جامعة ابن خلدون تيارت

كلية الحقوق والعلوم السياسية

قسم الحقوق

إجراءات التحقيق في الجرائم الإلكترونية

(دراسة مقارنة)

أطروحة لنيل شهادة دكتوراه الطور الثالث

تخصص القانون الجنائي والعلوم الجنائية

إعداد الطالبة:

حايطي فاطيمة

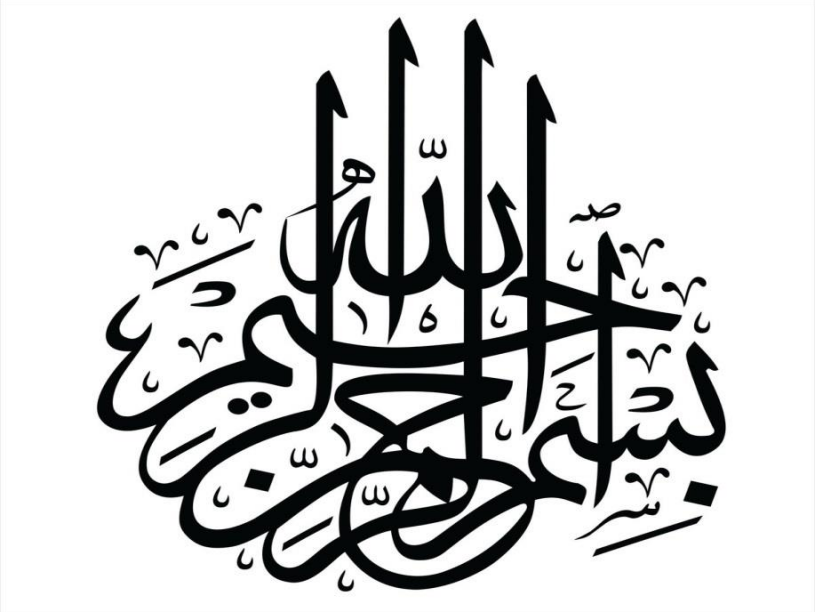
تحت إشراف:

أ.د: هروال نبيلة هبة

أعضاء لجنة المناقشة:

أ.د عليان بوزيان	أستاذ التعليم العالي	جامعة تيارت	رئيسا
أ.د/هروال نبيلة هبة	أستاذة التعليم العالي	جامعة تيارت	مشرفا ومقررا
أ.د/بوراس عبد القادر	أستاذ التعليم العالي	جامعة تيارت	ممتحنا
د.طالب خيرة	أستاذة محاضرة "أ"	جامعة تيارت	ممتحنا
أ.د بواب بن عامر	أستاذ التعليم العالي	جامعة البيض	ممتحنا
أ.دهنان مليكة	أستاذة التعليم العالي	جامعة البيض	ممتحنا

السنة الجامعية 2022/2023



﴿ قَالُوا سُبْحَانَكَ لَا عِلْمَ لَنَا إِلَّا مَا عَلَّمْتَنَا إِنَّكَ أَنْتَ الْعَلِيمُ الْحَكِيمُ ﴾

(سورة البقرة: الآية 32)

إهـــــداء

إلى من لا يمكن للكلمات أن توفي حقهما

والدي الكريمين

أبي العزيز ذا الروح الطيبة الذي لم يبخل يوما عني بشيء

أمي العزيزة التي علمتني العطاء وغمرتني من كرمها وحنانها بالكثير

أطال الله في عمرهما وأمدهما بالصحة والعافية

إلى إخوتي الأعزاء

إلى كل أفراد عائلتي الكريمة وخاصة جدتي الحنونة وأعمامي وعمتي

إلى كل أصدقائي وزملائي وأحبتي

إلى أساتذتي الأفاضل وخاصة الأستاذة هروال نبيلة هبة

إلى كل من قدم لي يد العون

إلى كل طالب علم

إليهم جميعا أهدي ثمرة جهدي هذا...

فاطيمة

كلمـــة شكـــر وتقدير

الحمد والشكر لله رب العالمين الذي بفضله تم إنجاز هذا العمل، والصلاة والسلام على أشرف الأنبياء والمرسلين سيدنا وحبيبنا محمد وعلى آله وصحبه ومن تبعهم بإحسان إلى يوم الدين، وبعد...

أتوجه بجزيل الشكر والامتنان إلى أستاذتي الكريمة هروال نبيلة هبة لقبولها الإشراف على هذه الأطروحة، إذ لم تبخل عليا بإرشاداتها وتوجيهاتها القيمة التي أثرت هذا العمل، فكانت لي معلمة ومشرفة وأختا، فلها مني وافر الشكر والتقدير وأسمى آيات المودة والاحترام

كما أتقدم بالشكر لأعضاء اللجنة الموقرة لقبولهم مناقشة هذا العمل المتواضع، وأتمنى الشفاء العاجل للأستاذة طالب خيرة.

كما أتقدم بشكر خاص إلى كل أساتذتي من كلية الحقوق والعلوم السياسية على دعمهم لي ومساندتي لإتمام هذا العمل.

وإلى كل أفراد عائلتي وأصدقائي

وإلى مصالح الشرطة التي لم تبخل بإمدادي بالمعلومات اللازمة.

ولا أنسى أن أشكر كل من قدم لي يد العون من قريب أو بعيد لإنجاز هذا العمل، ولو بالكلمة الطيبة.

فاطيمة

قائمة المختصرات

باللغة العربية:

ج رج ج: الجريدة الرسمية للجمهورية الجزائرية

ق إ ج ج: قانون الإجراءات الجزائية الجزائري

ق ع: قانون العقوبات

ق م: القانون المدني

الولايات م أ : الولايات المتحدة الأمريكية

م.م.م.ج.ت.إ.: المصلحة المركزية لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال

جريمة إ : جريمة إلكترونية

باللغة الأجنبية:

NCA : National Crime Agency

FBI : Federal Bureau Of Investigation

NC3 : The national cybercrime coordination unit

RCMP : Royal canadianmounted police

ECC : Electronic crime cyber council

CCCS : Canadian centre for cyber security

CAFC : Canadian anti-fraud centre

DCPJ : Direction centrale de la police judiciare

SDLC : Sous direction de la lutte contre la cybercriminalité

BEFTI : La Brigade d'enquètes sur les fraudes aux technologies de l'information

BFMD : La Brigade des fraudes liée aux moyens de paiement.

DGGN :Direction Générale de la Gendarmerie Nationale

LOCLCTIC : L'office central de lutte contre la cybercriminalité liée aux technologies de l'information

SDLC :Lasous direction de la lutte contre la cybercriminalité

DCRI : La direction centrale du renseignement intérieur

ANSSI : Agence nationale de la sécurité systèmes d'information

STRJD : Le service technique de recherche judicaire et de documentation

IRCGN : L'institut de recherche criminelles de la gendarmerie national

C3N : Le centre de lutte contre les criminalités numériques

CNAIP : Centre national d'analyse des photos

BKA : L'office fédéral de police criminelle

EC3 : European cybercrime center

J-CAT : Joint cybercrime action taskforce

IC3 : Internet Crime Complaint Center

IFCC : Internet Fraude Complaint Center

IOCE : International Organization On Computer Evidence

ANCE : Autorité Nationale de Certification Électronique

NWC : National White Collier Center

CA : Cour d'appel

CE : Conseil d'Europe

IP : Internet Protocol

CITC : Communication and information technology Commission

GDPR : General Data Protection Régulation

STAD : Système de traitement automatisé de données

TCP : Transmission Control Protocol

TIC : Technologies de l'information et de la communication

FBI : Federal Bureau of Investigation

INTERPOL : International Criminal Police Organization

US : United States

EUROJUST : European Union Agency for Criminal Justice Cooperation

EUROPOL : L'agence européenne de police criminelle

PHAROS : Portail officiel de signalement des contenus illicites de l'internet

JORF : Journal Officiel de la République Française

ARTP :L'Autorité de Régulation de la Poste et des Télécommunications

UPU : Universal Postal Union

ATU : Africain Télécommunication Union

ITU : International Télécommunication Union

مُقَدِّمَةٌ

مقدمة

شهد العالم منذ العقد الأخير من القرن العشرين، ثورة هائلة في مجال تقنية المعلومات سميت بالثورة المعلوماتية، حيث حققت هذه الأخيرة العديد من المزايا على جميع الأصعدة وفي شتى ميادين الحياة، إذ تلاشت معها الحدود السياسية والحواجز بين الدول والشعوب، نظرا لما تتميز به من عنصر السرعة والدقة في تجميع المعلومات وتخزينها ونقلها وتبادلها عن بعد داخل الدولة الواحدة أو بين عدة دول عبر العالم، الأمر الذي جعل العديد من العلماء والمفكرين يصفون هذه الثورة بالثورة الصناعية الثالثة، بالمقارنة مع الثورة الصناعية الأولى التي تحققت في أواخر القرن التاسع عشر، ففي حين كان الهدف من الثورة الأولى إحلال الآلة محل الجهد البدني للإنسان، فإن هدف الثورة المعلوماتية إحلال الآلة محل النشاط الذهني للإنسان.

وبالرغم من هذه المزايا التي حققتها هذه الثورة في مجال تقنية المعلومات إلا أنه قد رافقتها جملة من الانعكاسات السلبية الخطيرة نتيجة سوء استخدام هذه التقنية واستغلالها على نحو غير مشروع، وبطرق من شأنها المساس بمصالح الفرد والجماعة، إذ ازدادت هذه المخاطر تفاقما في ظل البيئة الافتراضية التي تمثلها شبكة الإنترنت، مما أدى إلى ظهور نمط جديد من الجرائم المستحدثة[1] والتي لم تكن معهودة من قبل، عرفت باسم "الجرائم الإلكترونية" أو "الجرائم المعلوماتية " أو جرائم الإنترنت" وغيرها من التسميات، [2] إذ بتعدد تسمياتها تعددت التعريفات التي أعطيت لها، وهذا ما انجر عنه عدم وضع تعريف موحد لها، [3]وتعرف الجريمة المعلوماتية على أنها كل سلوك إجرامي تكون المعلوماتية وسيلة

[1] يقصد بالجرائم المستحدثة الأنماط الإجرامية التي لم يألفها المجتمع في السابق، من حيث أسلوب ارتكابها ونوع الجناة فيها وحجمها، أو هي الجرائم المخطط لها والتي أفرزتها الثورة المعلوماتية والتطور في تكنولوجيات الإعلام والاتصال، يستعين فيها المجرم بتقنيات ومعطيات العلم الحديث، وتضم الجريمة المنظمة، جرائم الإرهاب، جرائم المخدرات، جرائم الإنترنت أو الجرائم الإلكترونية وغيرها. نقلا عن نبيلة هبة هروال، الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات، ط 1، دار الفكر الجامعي، الإسكندرية _مصر، سنة 2006، ص 21.

[2] تباينت المصطلحات الدالة على الجريمة الواقعة عبر الإنترنت وتعددت بين جرائم الإنترنت، وجرائم الكمبيوتر، والجرائم الالكترونية، و كذا الجرائم السيبرانية، والجرائم المعلوماتية وغيرها، وفي هذا يرى جانب من الفقه أن مصطلح الجرائم الالكترونية أوسع وأشمل من مصطلح الجرائم المعلوماتية وجرائم الكمبيوتر، ذلك أن الجرائم الإلكترونية تشمل كافة الجرائم التي تقع على الحاسبات أو بواسطتها سواء تمثلت في الحاسب الآلي أو مختلف الأجهزة الالكترونية الأخرى، بحيث يستخدم الحاسب في هذه الجرائم كأداة لارتكاب الجريمة أو محلا لها، أما عن مصطلح الجرائم المعلوماتية فيشمل مفهوم الاعتداء على المعلومات والبرامج الموجودة داخل الأجهزة الإلكترونية، بحيث يدخل في هذا المفهوم كل نشاط غير مشروع ناشئ في مكون أو أكثر من مكونات الإنترنت، كالتسلل إلى ملفات خاصة أو انتهاك حقوق الملكية الفكرية وغيراها، وتطلق تسمية جرائم الكمبيوتر فقط على الجرائم المرتكبة بواسطة أو على الكمبيوتر دون باقي الأجهزة، أما عن الجرائم السيبرانية فهي تسمية جاءت نتيجة العالم السيبراني أو الافتراضي.

[3] اختلفت تعريفات الجرائم الإلكترونية وتنوعت بين تعريفات فقهية وأخرى قانونية تستند كلها إلى عدة معايير وأسس، فهناك من عرفها على أساس وسيلة ارتكابها بأنها كل فعل إجرامي يستخدم الكمبيوتر أو الحاسب الآلي في ارتكابه كأداة رئيسية"، وطبقا لهذا التعريف يمكن أن ترتكب بعض الجرائم التقليدية بواسطة الحاسب الآلي، واتجاه آخر عرفها على أساس موضوعها أو محلها، على أنها كل سلوك غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب الآلي"، واتجاه عرفها على أساس معيار شخصي (الجاني)، من

في ارتكابه أو هدفا ومحلا له، حيث تتطلب لاقترافها أن تتوافر لدى فاعلها المعرفة بتقنية الحاسب الآلي والتكنولوجيات الحديثة.

ولعل خطورة هذا النوع من الجرائم نابعة من الطبيعة المتميزة والخاصة لها، من حيث ذاتية أركانها وحداثة أساليب ارتكابها وكذا البيئة الافتراضية التي تقع فيها، فهي جريمة تقنية تتميز بسهولة ارتكابها حيث لا تتطلب أي جهد عضلي ولا تخلف أي آثار محسوسة هذا من جهة، ومن جهة ثانية تتم من طرف شخص يتمتع بالذكاء والخبرة وله من المهارات التقنية العالية في التعامل مع التكنولوجيات الحديثة والتقنيات المتطورة للأجهزة الذكية، يطلق عليه اسم "المجرم المعلوماتي"[1]، فضلا عن ذلك فإنها من الجرائم العابرة للحدود إذ يتجاوز فيها السلوك الإجرامي الدولة الواحدة مما يخلق عدة إشكالات على المستويين الدولي والداخلي، الأمر الذي بات يثير بعض التحديات القانونية والعملية أمام السلطات والأجهزة المعنية بمكافحة الجرائم بصفة عامة، إذ أصبح من الصعب التعامل مع هذا النوع المستحدث من الجرائم وتكييفها على أساس النصوص الجناية التقليدية، سواء تلك النصوص الموضوعية التي تبين

بينهم الدكتور هشام رستم بقوله أنها "أية جريمة يكون متطلبا لاقترافها أن تتوافر لدى فاعلها معرفة بتقنيات الحاسب" ٬واتجاه أخير جمع بين عدة معايير في تعريفها بقوله أنها "الجريمة التي يستخدم فيها الحاسب الآلي كوسيلة أو أداة لارتكابها، أو يكون الحاسب الآلي نفسه ضحيتها. نقلا عن أحمد أمين أحمد الشوابكة، جرائم الحاسوب والأنترنت، مكتبة دار الثقافة للنشر والتوزيع، ط1، عمان، 2004، ص08

أما من الناحية القانونية فتعرف الجريمة الإلكترونية على أنها مجموعة الأنشطة المعاقب عليها قانونا والتي تربط بين الفعل الإجرامي والثورة التكنولوجية، والتي ينتج عنها حصول المجرم على فوائد مادية ومعنوية، مع تحميل الضحية خسارة مقابله، فبالنسبة للمشرع الجزائري وفي تعديله لقانون العقوبات بموجب القانون رقم 04-15 المتضمن قانون العقوبات، لم يعرّف الجريمة المعلوماتية بل اكتفى بالعقاب عليها تحت عنوان "الجرائم الماسة بنظام المعالجة الآلية للمعطيات" ونظرا للانتقادات الموجهة إليه على هذا القصور تدخل المشرع مرة أخرى لتدارك ذلك من خلال قانون رقم 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، وعرفها بموجب المادة الثانية منه بأنها: "جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات أو أية جريمة ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الالكترونية".

[1] يسمى الشخص الذي يرتكب الجريمة الإلكترونية بالمجرم المعلوماتي أو الإلكتروني، والذي يتميز عن غيره من المجرمين التقليديين بعدة خصائص، إذ يتمتع المجرم المعلوماتي بالمهارة والمعرفة الجيدة بمجال تكنولوجيا المعلومات والاتصالات والتي يكتسبها عن طريق الدراسة في هذا المجال أو عن طريق الخبرة المكتسبة في الحياة، كما يتمتع بالذكاء والاحترافية في تنفيذ جرائمه بما لا يدع مجالا لاكتشافه، ونظرا للتطور المستمر لتقنية المعلومات وسهولة التعامل مع الإنترنت اتسع نطاق وحجم المتعاملين مع الكمبيوتر مما أدى إلى ظهور عدة طوائف للمجرمين المعلوماتيين، فظهرت **طائفة المتطفلين**: وهم الذين يستهدفون الدخول إلى أنظمة الحواسب الآلية غير المصرح لهم بدخولها بغرض تحدي النظام واختراقه أو اكتساب الخبرة يطلق عليهم اسم Hachers، و**طائفة المخترقين**: تستهدف هذه الطائفة التسلل إلى أجهزة وأنظمة الحواسيب واختراقها والعبث بمحتوياتها بهدف إلحاق خسائر بالمجني عليه دون أن يكون بالضرورة هدفهم الحصول على مكاسب مالية، ويندرجون تحت طائفة مخترعي فيروسات الحاسبات الآلية وموزعها ويسمون "Malicieuses hackers"، و**طائفة الحاقدين**: وتسمى هذه الطائفة بـ"Crackers" حيث ترتكب اعتداءاتها الإجرامية بدافع الانتقام والثأر وتشويه السمعة، فليس لها أي هدف سياسي أو مادي من ارتكاب هذه الجريمة، بل تهدف إلى إلحاق الأذى بالمجني عليه.نقلا عن عبد الله دغش العجمي، المشكلات العملية والقانونية للجرائم الالكترونية، دراسة مقارنة، مذكرة لنيل شهادة الماجستير في القانون العام، جامعة الشرق الأوسط، 2014، ص22.

الفعل المجرم والعقوبة المقررة له، أو تلك النصوص الإجرائية التي تبين مراحل الدعوى الجزائية بما فيها مرحلة البحث والتحري ومرحلة التحقيق ، وكذا الأجهزة المنوط بها مباشرة هذه الإجراءات.

ولعل من الإشكالات الإجرائية التي تطرحها هذه الجرائم أن أجهزة البحث والتحري قد تعودت على التعامل مع الجريمة بصورتها التقليدية المعروفة التي يمكن إدراكها بالحواس واكتشاف آثارها في مسرح الجريمة، في حين أن الجرائم الإلكترونية ليس لها مسرح مادي ولا آثار مادية محسوسة، فضلا عن أن الدليل الناتج عنها سهل التدمير والمحو والتغيير مما يجعل أمر إثباتها صعبا ومعقدا، كما أن نقص خبرة ومعرفة المحقق بالمجالات التقنية يجعله يفشل في تتبعها وكشف مرتكبها.

ونتيجة لهذه الثغرات التي تثيرها المواجهة الإجرائية لهذه الجرائم زاد اهتمام الحكومات والهيئات الدولية بمكافحتها، إذ بدأت بتطوير أساليبها القانونية والفنية للوقاية من هذه الجرائم أولا ومن ثم القضاء عليها، فظهرت عدة جهود دولية وداخلية تسعى كلها لمكافحة هذا الإجرام تجلت في العديد من الاتفاقيات والمعاهدات ذات الصلة والتي أرست آليات جديدة لمتابعة هذه الجرائم، وعملت على تعزيز التعاون القضائي الدولي الذي اتخذ مظهر التعاون الأمني (الشرطي) الدولي من خلال تكاثف الأجهزة المكلفة بمتابعة هذه الجريمة في مختلف الدول، وتطوير الإمكانيات البشرية والمادية المؤهلة لتجسيد هذا الغرض، من خلال تخصيص وحدات مختصة بمباشرة أعمال التحري والتحقيق في هذه الجرائم، لديها من الخبرة والمعرفة القانونية والتقنية اللازمة لفك شفرة الجريمة الإلكترونية.

هذا من جهة، ومن جهة ثانية عملت معظم التشريعات الداخلية الأجنبية منها والعربية بما فيها المشرع الجزائري، على تعديل نصوص القوانين الإجرائية بما يتلاءم وخصوصية التحقيق في هذه الجرائم، عن طريق استحداث آليات وأساليب خاصة تعتمد بالضرورة على التقنيات الحديثة.

تتجلى أهمية موضوع "**إجراءات التحقيق في الجرائم الإلكترونية**" وتحديدا "**إجراءات البحث والتحري عن الجرائم الإلكترونية**" في أنه من المواضيع المستجدة والتي لا تزال محل نقاش وبحث مستمر نتيجة ارتباطها بمجال تقنيات المعلومات والتكنولوجيات الحديثة، التي لا تنفك في تطور مستمر يوم عن يوم، هذا ما جعل أساليب الجريمة بحد ذاتها في تطور مستمر، إذ أصبحت تهدد الأفراد والجماعات وأمن الدول، ولهذا أصبح من الضروري إعادة النظر في السياسة التشريعية الجنائية وخاصة ما تعلق منها بالجانب الإجرائي، الذي لقي العديد من التحديات والإشكالات القانونية والعملية التي وقفت عائقا أمام أجهزة التحري والتحقيق في الجرائم الإلكترونية، نظرا للخصوصية التي تتمتع بها هذه الأخيرة من حيث

أساليب ارتكابها ومرتكبها والآثار الناتجة عنها، ومن هنا ظهرت أهمية استحداث إجراءات وقائية وأخرى ردعية لمواجهة هذا النوع من الإجرام، بما يتماشى مع خصوصيته وطبيعته التقنية البحتة.

كما تكمن أهمية هذا الموضوع في أنه يثير عدة نقاط حساسة جدا تتعلق بمدى مساس هذه الإجراءات المستحدثة بخصوصية الأفراد وحقوقهم وحرياتهم المكفولة دستوريا، والتي تتطلب وجود مجموعة من الضوابط والضمانات الواجب مراعاتها من قبل القائم بالتحقيق، فضلا عن مدى مشروعية الأدلة الجنائية الإلكترونية المستمدة من هذه الإجراءات والأساليب الخاصة، ومدى تأثيرها على الاقتناع الشخصي للقاضي عند إثبات هذه الجريمة أمام القضاء.

ولعل هذه الأهمية البالغة لموضوع الدراسة وما يثيره من إشكالات قيمة تستحق المعالجة هو السبب في اختيارنا له ورغبة منا في الوقوف على حقيقة التعامل مع الجريمة الإلكترونية من الناحية الإجرائية، وخاصة معرفة الخصوصية التي تميز إجراءات التحري فيها عن إجراءات التحري في الجرائم التقليدية، وبالتالي معرفة السياسة التشريعية الجنائية الدولية والداخلية في مكافحة هذه الجرائم.

وهو ما ينبني عليه هدف هذه الدراسة والذي يتمثل في الإلمام بالجوانب الإجرائية الخاصة بمتابعة الجريمة الإلكترونية، وبالتحديد مرحلة البحث والتحري عن هذه الجرائم، أو كما تسمى بمرحلة "التحقيق الأولي" أو مرحلة "جمع الاستدلالات"، وذلك من حيث التطرق للوحدات المختصة في التحري عن هذه الجرائم على الصعيدين الدولي والداخلي، وتبيان الدور الوقائي لها في منع وقوع هاته الجرائم، وكذا الدور الردعي الذي يتجسد من خلال الضبط القضائي المختص في متابعة هذه الجرائم، كما تهدف الدراسة إلى إبراز خصوصية إجراءات البحث والتحري في الجرائم الإلكترونية وطرح أهم التحديات التي تثيرها أو تعترضها، محاولين من خلال هذه الدراسة معالجتها وتحليلها لإيجاد حلول لهذه العقبات.

وبالعودة للدراسات التي اهتمت بموضوع إجراءات التحقيق في الجرائم الإلكترونية نجد من بينها:

دراسة للأستاذة هروال نبيلة هبة والمعنونة بـ: "الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات" المطبوعة سنة 2006، وهي من بين أهم الدراسات كونها قريبة جدا من دراستنا حيث تضمنت مختلف الأجهزة القضائية المكلفة بالبحث والتحري عن الجرائم الإلكترونية وكذا إجراءات التحري التقليدية والمستحدثة، وذلك على المستويين الدولي والداخلي.

ودراسة أخرى للأستاذ يزيد بوحليط المعنونة بـ : "الجرائم الإلكترونية والوقاية منها في القانون الجزائري في ضوء الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، وقانون العقوبات، وقانون الإجراءات الجزائية"، المطبوعة سنة 2019، والتي تناولت بالدراسة الجوانب الموضوعية والإجرائية للجرائم الإلكترونية من حيث مفهوم الجريمة الإلكترونية وأركانها وأنواعها، وكذا المعالجة التشريعية الموضوعية لها في القانون الجزائري، وإجراءات التحقيق فيها التقليدية منها والمستحدثة أو الخاصة، وبهذا اختلفت هذه الدراسة عن دراستنا كون أنها واسعة ضمت الجانبين الموضوعي والإجرائي في حين اقتصرت دراستنا على الجانب الإجرائي فقط.

ودراسة ثالثة تمثلت في أطروحة دكتوراه في القانون العام للباحث براهيمي جمال المعنونة بـ : "التحقيق الجنائي في الجرائم الإلكترونية" الصادرة عن جامعة مولود معمري _ تيزي وزو التي نوقشت في 2018/06/27، عالجت هذه الدراسة مختلف إجراءات التحقيق في الجريمة الإلكترونية مع التفصيل في ماهية الدليل الإلكتروني ومدى مشروعية الحصول عليه وحجيته أمام القاضي الجزائي، كما تعرضت للإشكالات التي تطرحها المواجهة الإجرائية للجرائم الإلكترونية في مرحلة التحقيق الأولي، وهنا تكمن نقطة التشابه بين دراستنا وهذه الدراسة، واختلفتا في مواضع أخرى كون هذه الأخيرة لم تتطرق للأجهزة المعنية بالتحري في هذه الجرائم واكتفت بشرح الإجراءات وتحليلها وصولا إلى إيجاد حلول لأهم العقبات التي تعترض هذه الإجراءات.

من خلال استقرائنا لهذه الدراسات تبين لنا أن هناك مواضع تشابه كثيرة بينها وبين دراستنا خاصة أنها عالجت مسألة المواجهة الإجرائية للجرائم الإلكترونية بغض النظر عن ما إذا اقتصرت على مرحلة التحقيق الأولي أو امتدت لمرحلة التحقيق الابتدائي، إلا أنها لم تعالج مسألة دور وحدات مكافحة الجريمة الإلكترونية كضبطية إدارية وقائية، والوسائل التي تتدخل بها من أجل وقاية الأفراد والجماعات ومصالح الدول من الهجمات الإلكترونية، وهو ما حولنا تداركه في هذه الدراسة من خلال الإلمام بجميع جوانبها، بدء بمعرفة الأجهزة التي يناط بها مهمة البحث والتحري عن هذه الجرائم وذلك قبل وقوع الجريمة وبعد وقوعها، ومن ثم التطرق لمختلف الإجراءات التقليدية والمستحدثة مع إبراز خصوصيتها في مواجهة الجريمة الإلكترونية وعرض الإشكالات التي تطرحها محاولين بذلك إيجاد حلول لها.

وأما عن الإشكالية التي يدور حولها موضوع دراستنا، فتنصب أساسا حول معرفة السياسة الجنائية الإجرائية التي رصدها المشرع للبحث والتحري عن الجرائم الإلكترونية، وما مدى استجابتها للخصوصية والطابع التقني لهذه الجرائم؟

وتندرج تحت هذه الإشكالية الرئيسية جملة من التساؤلات الفرعية تتم الإجابة عليها من خلال فصول ومباحث هذه الدراسة، منها:

- فيما يتمثل الدور الوقائي لأجهزة مكافحة الجريمة الإلكترونية؟
- هل توجد شرطة مختصة بالتحري في الجرائم الإلكترونية ؟ وبما تتميز عن الشرطة التقليدية؟
- ما مدى قابلية القواعد الإجرائية التقليدية للتطبيق على الجرائم الإلكترونية في مرحلة التحري الأولي؟
- ما مدى فعالية وخصوصية إجراءات البحث والتحري المستحدثة، وفيما تتمثل أهم الإشكالات التي يطرحها تطبيق هذه الإجراءات على الجرائم الإلكترونية؟

وفي إطارنا للإجابة عن هذه الإشكاليات والإلمام بموضوع إجراءات التحقيق في الجرائم الإلكترونية، قد واجهنا عدة صعوبات لعل أهمها ضبط خطة متوازنة تعالج جميع جوانب الموضوع خاصة أننا اقتصرنا هذه الدراسة على مرحلة واحدة من مراحل التحقيق ألا وهي مرحلة التحقيق الأولي والتي كثيرا ما تتشابه إجراءاتها مع إجراءات التحقيق الابتدائي، هذا من جهة.

ومن جهة أخرى اتجاه أغلب الدراسات لمعالجة الظاهرة من الناحية الموضوعية، وإن كانت البعض منها تطرقت للجوانب الإجرائية للجرائم الإلكترونية إلا أنها لم تلم بجميع الوحدات والأجهزة وجميع الإجراءات التي تتعلق بمتابعة الجريمة الإلكترونية بل ذكرتها في شكل جزئيات مما جعل الباحث أمام حتمية تجميع كل هذه المعلومات بشكل متناسق وفق خطة متوازنة، فضلا عن قلة الدراسات التي عالجت موضوع الضبط الإداري في الجرائم الإلكترونية.

كما واجهت كباحثة صعوبات أثرت على مسار هذا البحث العلمي، نتيجة ظروف صحية صعبة.

للإجابة عن الإشكال المطروح اعتمدنا المنهج الوصفي لوصف خصوصية الجرائم محل الدراسة والأجهزة المكلفة بالبحث والتحري عنها وما يجب أن تتمتع به في سبيل التصدي الأمثل لهذه الجرائم، والمنهج التحليلي لتحليل المعلومات والنصوص القانونية ذات الصلة مع إبراز الإشكالات التي تطرحها

المواجهة الإجرائية في مرحلة البحث والتحري وتحليلها، وعلى المنهج الإستقرائي من خلال دراسة الجزئيات وصولا إلى نتائج عامة أو حلول مناسبة لهذه الإشكالات، كما كان للمنهج المقارن نصيب وافر من الاستعمال في دراستنا حيث استعنا به في جميع أطوار بحثنا من خلال مقارنة الأنظمة والتشريعات الداخلية والدولية التي أولت أهمية لموضوع إجراءات التحري في الجرائم الإلكترونية، متبعين في ذلك خطة ثنائية تتضمن بابين رئيسيين:

تضمن **الباب الأول الوحدات المختصة بالبحث والتحري عن الجرائم الإلكترونية**، والذي قسمنها بدوره إلى فصلين أساسيين: خصصنا **الأول** لدراسة دور وحدات البحث والتحري عن الجريمة الإلكترونية كضبطية إدارية (وقائية)، في حين خصصنا **الفصل الثاني** لمعالجة دور وحدات البحث والتحري عن الجريمة الإلكترونية كضبطية قضائية (ردعية).

أما عن **الباب الثاني فيعالج خصوصية إجراءات البحث والتحري عن الجريمة الإلكترونية**، والذي قسمناه إلى فصلين أساسيين: خصصنا **الأول** لمعالجة خصوصية إجراءات البحث والتحري التقليدية، في حين خصصنا **الفصل الثاني** لمعالجة خصوصية إجراءات البحث والتحري المستحدثة في الجريمة الإلكترونية.

وأنهينا دراستنا بخاتمة ضمناها أهم النتائج والتوصيات المقترحة.

الباب الأول

الوحدات المختصة بالبحث والتحري عن الجرائم الإلكترونية

نتيجة الثورة الرقمية التي اجتاحت العالم اليوم ظهرت العديد من الشبكات والمواقع الإلكترونية التفاعلية التي سهلت تواصل الأفراد عبر العالم، وكان لها من الآثار الإيجابية الكثيرة إلا أن مخاطرها عديدة أيضا، حيث أصبحت تهدد النظام العام على مستوياته المختلفة، هذا ما فرض تحديا جديدا على المفاهيم التقليدية للضبط لكي تواكب المستجدات الحاصلة في المجال الرقمي والتكنولوجي، وتتلاءم مع التهديدات الإلكترونية التي فرضتها مخاطر تلك الشبكات على النظام العام، وهنا برزت جهود الدولة في الوقاية والحيلولة دون وقوع هذه التهديدات والجرائم الإلكترونية، عن طريق ممارستها لوظيفتين: وظيفة الضبط الإداري والتي تمارس قبل وقوع الجريمة للحيلولة دون وقوعها وتفادي أخطارها، حيث تقوم بها عدة أجهزة وعن طريق وسائل معينة، وثانيا وظيفة الضبط القضائي والتي يباشرها أعوان متخصصين لهم صفة الضبط القضائي، إذ يعد ضباط الشرطة القضائية أصحاب الاختصاص العام في مكافحة الجرائم بأنواعها، إلا أن الجرائم الإلكترونية وما تتميز به من طبيعة خاصة قد فرضت تحديات كبيرة على أجهزة البحث والتحري إذ أصبحت عاجزة على مكافحة هذه الجرائم، ولهذا أصبح لزاما على الدول تطوير أجهزتها وتجهيزها للتصدي الأمثل لهذه التهديدات، عن طريق تنظيم الدورات التدريبية لهذه الفئات هذا من جهة، ومن جهة أخرى استحداث فرق خاصة ومتخصصة لها من الخبرة والدراية بمجال التحقيق والتعامل مع هذه الجرائم، وعليه ما مدى توفير الدول لأجهزة متخصصة في البحث والتحري عن الجرائم الإلكترونية؟ وما مدى فعالية وسائل الضبط في الوقاية وردع هذه الجرائم؟

للإجابة عن هذا الإشكال ارتأينا معالجة هذا الباب من خلال فصلين رئيسيين: خصصنا الأول لدراسة دور وحدات البحث والتحري عن الجرائم الإلكترونية كضبطية إدارية (وقائية)، في حين خصصنا الفصل الثاني لدراسة دور وحدات البحث والتحري عن الجرائم الإلكترونية كضبطية قضائية (ردعية).

الفصل الأول

دور وحدات البحث والتحري عن الجرائم الإلكترونية كضبطية إدارية (وقائية)

الفصل الأول: دوروحدات البحث والتحري عن الجرائم الإلكترونية كضبطية إدارية (وقائية)

نظرا لأن الدور الوقائي في التصدي للجرائم أهم وأسبق من متابعتها بعد وقوعها، تضطلع سلطات الضبط الإداري بمهمة المحافظة على النظام العام والوقاية من مختلف أشكال التهديدات التي قد تقع عليه، ونتيجة للتطور التكنولوجي وظهور المخاطر الإلكترونية تطورت نظرية الضبط الإداري التقليدي وامتد نطاقها لضبط الأنشطة في العالم الرقمي الإلكتروني، وأصبح بموجب هذه النظرية للجهات الإدارية المختصة اتخاذ جميع إجراءات الضبط الإداري الإلكتروني من خلال تقييد نشاط الأفراد داخل هذا العالم أو البيئة الجديدة، [1] حيث تتمتع في إطار المحافظة على النظام العام داخل البيئة الإلكترونية بعدة وسائل وأساليب قانونية ومادية وبشرية متنوعة خولها لها المشرع ذلك عن طريق إصدار اللوائح والقرارات التنظيمية التي تنظم سلوكات ونشاطات الأفراد في العالم الرقمي، واتخاذ الإجراءات التي تتناسب وهذه البيئة مثل فرض الرقابة الإلكترونية وحظر المواقع التي تشكل تهديدا للنظام العام بمختلف عناصره وكذا حجب خدمة الإنترنت وما إلى ذلك، وتضم هذه السلطات عددا من المتدخلين العموميين والخواص، الذين يباشرون مهامهم على المستويين الوطني والمحلي، إلى جانب سلطات إدارية مستقلة والتي جاء إنشائها في ظل عجز السلطات العمومية على ضبط بعض الأنشطة التي أفرزها هذا التطور التكنولوجي، ولفعالية حماية النظام العام من المخاطر الناجمة عن استخدام الشبكات الإلكترونية لابد من تكامل مجهودات الهيئات العمومية المختصة مع مجهودات الفاعلين في هذا المجال، والذين يقومون بدور مساعد لهذه السلطات والمتمثلين في مقدمي الخدمات بصفة عامة ومقدمي خدمات الإنترنت بصفة خاصة، وعليه فيما تتمثل هذه السلطات وما مدى صلاحياتها في مجال الضبط الإداري الإلكتروني؟

للإجابة عن هذا التساؤل ارتأينا معالجة هذا الفصل من خلال مبحثين رئيسيين: خصصنا الأول لدراسة دور الضبط الإداري التقليدي في الوقاية من الجرائم الإلكترونية، في حين خصصنا الثاني لدراسة دور الضبط الإداري الإلكتروني في الوقاية من الجرائم الإلكترونية.

[1] مصطفى جمال حنفي زينو، دور الضبط الإداري في مجال الجرائم الإلكترونية المخلة بالأمن العام (دراسة تحليلية)، مذكرة مقدمة لنيل شهادة الماجستير في القانون العام، كلية الحقوق، جامعة الأزهر، غزة فلسطين، 2017، ص 113-114.

المبحث الأول: دور سلطات الضبط الإداري التقليدي في الوقاية من الجرائم الإلكترونية

يعتبر الضبط الإداري أهم صور النشاط الإداري، فهو مجموعة الإجراءات والتدابير التي تتخذها الإدارة لتنظيم مختلف النشاطات والتي تسعى من خلالها إلى حفظ النظام العام بمختلف عناصره، [1] وتعتبر إجراءات الضبط من أخطر الوظائف لأنها ترتبط بحريات الأفراد لذلك حصر القانون السلطات والهيئات التي تقوم بهذه الوظيفة، إذ يتمتع البعض منها بسلطات الضبط الإداري العام الذي تمتد لتشمل جميع المجالات سواء كان ذلك على مستوى الدولة كلها أم على مستوى إحدى وحداتها الإقليمية، حيث يمارس الضبط الإداري في الحالة الأولى أعضاء السلطة المركزية (رئيس الجمهورية والوزير الأول)، في حين يمارسه في الحالة الثانية رؤساء الوحدات المحلية (الوالي ورئيس المجلس الشعبي البلدي)[2] أما عن

[1] يعرف الضبط الإداري التقليدي من الناحية العضوية على أنه: "الهيئات والأجهزة الإدارية التي تمارس هذه الوظيفة في إطار السلطة التنفيذية، ومجموع الموظفين المكلفين بمهمة الضبط"، كما عرفه الفقيه موريس هوريو من الناحية الوظيفية على أنه: "كل ما يستهدف به المحافظة على النظام العام في الدولة"، كما عرفه الأستاذ عمار عوابدي على أنه: "كالأعمال والإجراءات والقواعد التي تقوم بها السلطة الإدارية المختصة، على الأفراد لتنظم نشاطهم وتحدد مجاله، ولتقيد جرياتهم في حدود القانون، بقصد حماية النظام العام ووقاية المجتمع ضد كل ما يهدده"، لمزيد من التفاصيل ينظر عمار عوابدي، القانون الإداري، الجزء الثاني:(النشاط الإداري)، ط 04، ديوان المطبوعات الجامعية، الجزائر، 2007، ص 10.

ولعل من أهم مميزات الضبط الإداري مرونته في تنظيم نشاطات الأفراد وفرض القيود على بعض الحريات التي من شأنها المساس بالنظام العام، إضافة إلى تمتعه بالطابع الوقائي إذ يعمل على منع وقوع الجريمة باتخاذ تدابير وقائية للحفاظ على الأمن والسلامة والسكينة داخل المجتمع.

[2] تتمثل السلطة اللامركزية أو المحلية في الجزائر في كل من الوالي على مستوى إقليم الولاية ورئيس المجلس الشعبي البلدي على مستوى البلدية، حيث يقابلها في التنظيم الإداري الفرنسي ما يسمى بالمحافظة، يتولى الوالي أو المحافظ في فرنسا وكذا رئيس المجلس الشعبي البلدي في البلدين جملة من الصلاحيات والمهام تهدف لضمان التسيير الحسن للمرافق العمومية في حدود الولاية أو البلدية، كما يحوز على سلطات واسعة في مجال الضبط بنوعيه الإداري والقضائي، ولقد نصت المادة 114 من قانون الولاية 07/12 على أن الوالي مسؤول عن حفظ النظام العام والأمن والسكينة والسلامة، حيث توضع تحت تصرفه مصالح الأمن كما له أن يطلب تدخل الشرطة والدرك الوطنيين المتمركزة على إقليم الولاية عن طريق التسخير في حالة وجود خطر أو ظرف استثنائي معين، ويلزم مصالح الأمن بإعلامه بكل القضايا والجرائم الماسة بالنظام والأمن العموميين للتدخل وضمان سلامة الأشخاص والممتلكات عن طريق وسائل ضبطية تتمثل في جملة من القرارات الفردية والتعليمات التي تنظم سلوك الأفراد، ونفس المهام والصلاحيات أوكلت للمحافظ في فرنسا، لعل من بين كل ما سبق ومن استقرائنا لنصوص قانوني الولاية والبلدية نستخلص أن دور كل من الوالي ورئيس م ش ب في المحافظة على النظام العام بعناصره المختلفة يظهر جليا من خلال الصلاحيات والسلطات الواسعة التي منحهما إياها القانون، لكن ما يهمنا في هذا المقام هل يتدخل كل من الوالي ورئيس م ش ب في ضبط الجرائم الإلكترونية؟ وهنا نجد أن دورهما ضئيل جدا إن لم نقل منعدم لأن القانون لم ينص صراحة على ذلك بل اكتفى بالنص على التزام الوالي ورئيس م ش ب بالحفاظ على الأمن والنظام العام، أي منع كل الجرائم الماسة والمخلة بهما ولم يحدد نوع الجرائم أو التهديدات أو الأخطار لهذا نقول أن القانون لم ينص صراحة على ضبط الوالي ورئيس م ش ب للجرائم الإلكترونية وحتى الواقع يقول ذلك، لكن يمكننا القول بأنه قد يكون دور كلاهما ثانوي وذلك من خلال تنفيذهما للقوانين والتنظيمات الصادرة من السلطة التشريعية والسلطة التنفيذية ممثلة في كل من رئيس ج والوزير الأول والوزراء، عندما تكون هذه القوانين والتنظيمات أو المراسيم تعالج مسألة متعلقة بأخطار الإنترنت أو التهديدات السيبرانية المختلفة، أو ما يتعلق منها بتنظيم شبكات الإنترنت أو الاتصالات وغيرها. لمزيد من التفاصيل ينظر عمار عوابدي، القانون الإداري، الجزء الأول:(النظام الإداري)، ديوان المطبوعات الجامعية، الجزائر، 2000. وأيضا عمار عوابدي، القانون الإداري، الجزء الثاني:(النشاط الإداري)، المرجع السابق، وينظر أيضا نوال لصلج، صلاحيات رئيس المجلس الشعبي البلدي والولائي في ظل القوانين -...

النوع الثاني من أشكال الضبط وهو الضبط الإداري الخاص والذي ينظم مجال معين أو نشاط محدد ويخول بذلك هيئاته سلطات أقوى وأعمق من تلك التي يخولها الضبط الإداري العام، وسواء كان الضبط الإداري عاما أو خاصا فإن أهدافه واحدة فهو ينظم النشاطات الفردية والجماعية من بينها النشاطات التي تتم في البيئة الرقمية والتي تنظم الاتصالات وتبادل المعلومات، وعليه فما هو الدور الذي تلعبه سلطات الضبط الإداري العام والخاص على السواء في ضبط هذه الشبكات الإلكترونية؟

المطلب الأول: دور السلطة التنظيمية في الوقاية من الجرائم الإلكترونية.

تضطلع السلطة التنفيذية في الدولة بممارسة صلاحيات الضبط الإداري العام في تنظيم نشاطات الأفراد وحماية النظام العام، حيث يختلف أعضاء السلطة التنفيذية حسب النظام في كل دولة، وفي أغلب الدول يوزع المجال التنظيمي بين كل من رئيس الجمهورية والوزير الأول أو رئيس الحكومة، وعليه سوف نتطرق بالتفصيل للدور التنظيمي لهما في مجال الوقاية من الجرائم الإلكترونية.

الفرع الأول: دور رئيس الجمهورية في الوقاية من الجرائم الإلكترونية.

يعتبر رئيس الجمهورية أعلى هرم في هيكل النظام الإداري باعتباره رئيس السلطة التنفيذية في البلاد، يضطلع بمهام ومسؤوليات إدارية ويملك صفة وسلطة إصدار القرارات الإدارية التنظيمية العامة والقرارات الفردية بخصوص الوظيفة الإدارية باسم ولحساب الدولة وفي الحالات العادية والاستثنائية التي تمر بها الدولة، وذلك في نطاق الوظائف والاختصاصات الإدارية المقررة له بموجب الدستور والعرف الدستوري،[1] إذ يمارس سلطته التنظيمية في المسائل غير المخصصة للقانون وفقا للمادة 141 من التعديل الدستوري لسنة 2020[2] والتي تقضي بأن: "يمارس رئيس الجمهورية السلطة التنظيمية في المسائل غير المخصصة للقانون. يندرج تطبيق القوانين في المجال التنظيمي الذي يعود للوزير الأول أو لرئيس الحكومة حسب الحالة "وهذا ما يعني أنه يعود لرئيس الجمهورية الاختصاص في جميع المسائل التي لا تندرج ضمن اختصاص السلطة التشريعية، ولكن ما يهمنا في هذه الدراسة هل أقر الدستور لرئيس

=...الجديدة، مجلة هيرودوت للعلوم الإنسانية والاجتماعية، العدد السادس، جوان 2018. يراجع أيضا قانون الولاية رقم 07/12 المؤرخ في 21 فبراير 2012، ج ر ج ج عدد 12، الصادرة بتاريخ 29 فبراير 2012، وقانون البلدية رقم 10/11 المؤرخ في 22 جوان 2011، ج ر ج ج عدد 37، الصادرة بتاريخ 03 يوليو 2011.

[1] عمار عوابدي، القانون الإداري، الجزء الأول: (النظام الإداري)، المرجع السابق، ص 218.

[2] المرسوم الرئاسي رقم 20-442 المؤرخ في 15 جمادى الأولى عام 1442 الموافق 30 ديسمبر 2020، يتعلق بإصدار التعديل الدستوري الجزائري، ج.ر.ج.ج، عدد 82 الصادرة في 30 ديسمبر 2020

الجمهورية صلاحية ممارسة صفة الضبطية الإدارية؟[1] هنا يمكننا القول أن الدستور الجزائري لم ينص صراحة على اختصاص رئيس السلطة التنفيذية بوظيفة الضبط الإداري ومثله الدستور الفرنسي[2]غير أنه وبالرجوع لأحكام كلا الدستورين نجد أن رئيس الجمهورية وباعتباره المسؤول الأول على الحفاظ على استقرار وأمن الدولة ونظامها العام له صلاحية إصدار اللوائح الإدارية أو ما يسمى بلوائح الضبط(البوليس) الإداري على كامل التراب الوطني في الظروف العادية أو الاستثنائية التي تمر بها البلاد، [3]على عكس المؤسس الدستوري المصري[4] إذ نص صراحة على اختصاص رئيس الجمهورية بإصدار لوائح الضبط الإداري إلى جانب لوائح تنظيم المرفق العام وتسييره.[5]

يتمثل الاختصاص الضبطي لرئيس الجمهورية في الظروف العادية في إصدار المراسيم الرئاسية التي تهدف إلى حماية النظام العام وصونه من مختلف أشكال التهديدات[6] والتي من بينها الاعتداءات الإلكترونية، ففي الجزائر مثلا نجد أن سلطة رئيس الجمهورية في ضبط الاعتداءات الإلكترونية (الجرائم الإلكترونية) ضيقة نسبيا نظرا لاختصاص السلطة التشريعية بضبط هذا المجال لاسيما القواعد العامة لقانون العقوبات وقانون الإجراءات الجزائية حسب أحكام المادة 139 من الدستور الجزائري[7] وما يشرعه البرلمان بقوانين عضوية في بعض المجالات مثل القانون المتعلق بالإعلام وما ينصب تحته من اعتداءات إلكترونية متعلقة بمجال الصحافة والإعلام حسب أحكام المادة 140 من الدستور ج، [8] ومن بين اللوائح التنظيمية الصادرة عن رئيس الجمهورية في مجال ضبط الجرائم الإلكترونية نجد المرسوم الرئاسي رقم 15-261 الذي يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة

[1] سليماني هندون، سلطات الضبط في الإدارة الجزائرية، أطروحة مقدمة لنيل شهادة الدكتوراه في القانون العام، تخصص إدارة ومالية، كلية الحقوق، جامعة الجزائر 1، 2013/2012، ص 82.

[2]Le constitution française du 04 octobre 1958 avec sa derniére mise à jour de 20 aout 2008.

[3] عمار عوابدي، القانون الإداري، الجزء الثاني: (النشاط الإداري)، المرجع السابق، ص 28.

[4] دستور جمهورية مصر العربية الصادر في 13 أفريل 2019.

[5]ينظر المادة 150 من دستور جمهورية مصر سالف الذكر.

فقير محمد، علاقة رئيس الجمهورية بالوزير الأول في النظامين الجزائري والمصري، دراسة مقارنة، مذكرة لنيل شهادة الماجستير في القانون العام، تخصص إدارة ومالية، كلية الحقوق، جامعة أمحمد بوقرة، بومرداس، ب س، ص 87.

[6] اسماعيل جابوربي، الضبط الإداري في مجال المحافظة على الأمن العام في الظروف الاستثنائية، دراسة مقارنة في النظام الإسلامي والنظام القانوني الجزائري، أطروحة مقدمة لنيل درجة الدكتوراه في علوم الشريعة والقانون، تخصص مؤسسات سياسية وإدارية، كلية الشريعة والاقتصاد، جامعة عبد القادر للعلوم الإسلامية، قسنطينة، 2018/2017، ص 155.

[7] ينظر المادة 139 من التعديل الدستوري الجزائري لسنة 2020.

[8] ينظر المادة 140 من التعديل الدستوري الجزائري لسنة 2020.

بتكنولوجيات الإعلام والاتصال ومكافحتها[1] والمعدل بالمرسوم الرئاسي رقم 439/21 المؤرخ في 2021/11/07[2] هذه الهيئة التي تم إنشائها مؤخرا بهدف وقاية النظام والأمن العام من مختلف التهديدات ذات الطابع الإلكتروني والتي ستكون محل دراسة مفصلة لاحقا، أيضا المرسوم الرئاسي رقم 20-05 المتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية على مستوى وزارة الدفاع الوطني،[3] التي تتولى إعداد الإستراتيجية الوطنية لأمن الأنظمة المعلوماتية والموافقة عليها وتنفيذها، والتي ستكون أيضا محل تفصيل لاحق، وفي نفس السياق أصدر الملك خادم الحرمين الشريفين بالمملكة العربية السعودية أمرا ملكيا يقضي بإنشاء الهيئة الوطنية للأمن السيبراني عام 2017 في مجال المحافظة على أمن المجتمع السعودي واستقراره وتأمين سلامة عمل القطاعات المختلفة داخله، من خلال تأمينها من الهجمات والاختراقات السيبرانية.[4] كما أصدر رئيس سلطنة عمان في 10 يونيو 2020 مرسوما بإنشاء مركز للدفاع الإلكتروني الذي يستهدف المعاملات الإلكترونية ومكافحة جرائم تقنية المعلومات والتابع لجهاز الأمن الداخلي.[5]

إلى جانب هذه المراسيم يظهر دور رئيس الجمهورية في مجال الوقاية من الجرائم الإلكترونية في سلطة إبرامه ومصادقته على الاتفاقيات والمعاهدات الدولية المختلفة ذات الصلة بمكافحة هذا النوع من الإجرام، من بينها الاتفاقية العربية لمكافحة جرائم تقنية المعلومات والتي صادقت عليها الجزائر بموجب المرسوم الرئاسي رقم 14-252[6] حيث تهدف هذه الاتفاقية إلى تعزيز سبل التعاون بين الدول الأطراف في مجال التصدي للجرائم الإلكترونية بمختلف أشكالها، وتوحيد الجهود الرامية لمكافحتها لضمان أمن الدول وسلامتها، نجد أيضا اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية التي صادقت

---

[1] المرسوم الرئاسي رقم 15-261 المؤرخ في 2015/10/08، يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج ر ج ج عدد 53، المؤرخة في 2015/10/08.

[2] المرسومالرئاسي رقم 439/21 المؤرخ في 2021/11/07، يتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج ر ج ج عدد 05، المؤرخة في 2021/11/11.

[3] المرسوم الرئاسي رقم 20-05 المؤرخ في 24 جمادى الأولى عام 1441 الموافق 20 جانفي 2020، يتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية، ج ر ج ج عدد 04 المؤرخة في 26 جانفي سنة 2020.

[4] مقال حول "الأمن السيبراني حماية وطنية لأمن الفرد والمجتمع في المملكة"، منشور على موقع وكالة الأنباء السعودية، الأربعاء 2017/11/01 ، متاح على الرابط التالي: https://www.spa.gov.sa/1683272تاريخ الاطلاع: 2021/02/17 على الساعة 18:22،

[5] سيف إبراهيم، "لصد الهجمات هل ينشئ الخليج مركز موحد للأمن السيبراني"، نشر في2020/12/27، على 20:58سا، متاح على الرابط التالي: https://allkhaleejonline.net ، تاريخ الاطلاع: 2021/02/10 على الساعة 18:38،

[6] الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، المحررة بالقاهرة بتاريخ 2010/12/21، التي صادقت عليها الجزائر بموجب المرسوم الرئاسي رقم 14-252 المؤرخ في 2014/09/08، ج ر ج ج عدد 57، المؤرخة في 2014/09/28.
ينظر الملحق رقم 11.

عليها الجزائر بموجب المرسوم الرئاسي رقم 02-55 المؤرخ في 05 فيفري 2002 [1] والتي دخلت حيز التنفيذ في 29 سبتمبر 2003، حيث تهدف إلى مكافحة كل جريمة عابرة للحدود الوطنية من بينها الجريمة الإلكترونية، جاءت هذه الاتفاقية لتعزيز التعاون بين سلطات إنفاذ القانون والأجهزة القضائية لدى الدول الأعضاء وتقديم المساعدة التقنية للتصدي لهذه الجرائم.

الفرع الثاني: دور الوزير الأول في الوقاية من الجرائم الإلكترونية.

يمارس السلطة التنظيمية إلى جانب رئيس الجمهورية الوزير الأول أو ما يعرف برئيس الحكومة يتولى مهمة تسيير الحكومة والإدارة العامة وذلك عن طريق إصداره مراسيم تنفيذية، وقد خول الدستور الجزائري للوزير الأول صلاحيات عديدة إلا أنه لم يشر صراحة إلى اختصاصه بممارسة سلطة الضبط الإداري على غرار المؤسس الدستوري الفرنسي الذي نص على اختصاص الوزير الأول بإصدار اللوائح في المادة 21 من دستور 1958 [2] وكذا المؤسس الدستوري المصري الذي نص بصريح العبارة على ذلك في المواد 171 و172 [3] منه، ولكن بالرجوع لأحكام الدستور الجزائري وبعض النصوص القانونية التنظيمية لاسيما المادة141 منه والتي تنص في فقرتها الثانية على: "... يندرج تطبيق القوانين في المجال التنظيمي الذي يعود للوزير الأول أو رئيس الحكومة، حسب الحالة" والمادة 112 من الدستور نفسه [4] والتي حددت صلاحيات الوزير الأول من بينها أنه يقوم بتطبيق القوانين والتنظيمات، كما يوقع المراسيم التنفيذية.

من خلال استقراء هذه المواد نجد أن سلطة تنفيذ القوانين هي جزء من التنظيم الذي يمتد ليشمل النشاطات التي لا تندرج ضمن اختصاصات السلطة التشريعية، والتي من بينها المحافظة على النظام العام، إذ نجد المؤسس الدستوري الجزائري أعطى للوزير الأول صلاحية تطبيق أو تنفيذ القوانين

---

[1] اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية، التي صادقت عليه الجزائر بموجب المرسوم الرئاسي رقم 02-55 المؤرخ في 2002/02/05، ج ر ج ج عدد 09، المؤرخة في 2002/11/15.

ينظر الملحق رقم 10.

[2] Article 21 de la constitution français : " Le premier ministre dirige l'action du gouvernement. Il est responsable de la défense nationale. Il assure l'exécution des lois. Sous réserve des dispositions de l'article 13, il exerce le pouvoir réglementaire et nomme aux emplois civils et militaires…"

ينظر إبراهيم يامة، لوائح الضبط الإداري بين الحفاظ على النظام العام وضمان الحريات العامة، أطروحة مقدمة لنيل شهادة الدكتوراه في القانون العام، كلية الحقوق والعلوم السياسية، جامعة أبي بكر بلقايد، تلمسان، 2015/2014، ص 60.

[3] ينظر المادة 171 من دستور جمهورية مصر العربية.

[4] ينظر المادة 112 من التعديل الدستوري الجزائري لسنة 2020 والتي تقابلها المادة 167 من دستور جمهورية مصر العربية، التي تنظم صلاحيات الوزير الأول والسلطات المخولة له.

والتنظيمات ذلك أن بعض النصوص والتشريعات لا يتم تنفيذها بمجرد إصدارها بل تتطلب صدور مراسيم تنفيذية لإبراز الجزئيات اللازمة لنفاذها، وبهذا يمكن القول أن سلطة الوزير الأول في إصدار لوائح الضبط تقتصر كما أشرنا سابقا في تنفيذ القوانين والمراسيم الرئاسية[1]، وما يهمنا في هذه الدراسة دور الوزير الأول في ضبط الاعتداءات الإلكترونية والوقاية منها حفاظا على النظام العام بمختلف عناصره.

ففي الجزائر يظهر هذا الدور في إصداره لبعض المراسيم التنفيذية لعل أبرزها المرسوم التنفيذي رقم 98-257 المؤرخ في 25 أوت 1998 الذي يضبط شروط وكيفيات إقامة خدمات "أنترنات" واستغلالها، المعدل بموجب المرسوم التنفيذي رقم 2000-307 المؤرخ في 14 أكتوبر 2000[2] والذي نظم خدمة تقديم الترخيصات لمقدمي خدمات الإنترنت، ومسؤوليتهم عن المحتويات التي يقومون بإتاحتها للجمهور من خلال دورهم الرقابي على الموزعات التي تتضمن بيانات تتعارض مع النظام العام والأخلاق والآداب العامة.

نجد أيضا المرسوم التنفيذي رقم 15-320 المؤرخ في 13 ديسمبر 2015[3] الذي يحدد نظام الاستغلال المطبق على كل نوع من أنواع الشبكات بما فيها اللاسلكية الكهربائية وعلى مختلف خدمات المواصلات السلكية واللاسلكية الذي صدر تطبيقا للمادة 31 من القانون 2000-03[4] الذي يحدد القواعد العامة المتعلقة بالبريد وبالمواصلات السلكية واللاسلكية، حيث جاء هذا المرسوم لتنظيم استغلال شبكات الاتصال المختلفة وذلك عن طريق ترخيص أو رخصة تقدمها سلطة ضبط البريد والاتصالات السلكية واللاسلكية للمستفيد أو المتعامل معها، كما يحدد هذا المرسوم شروط وكيفيات منح هذه التراخيص واستغلال الشبكات الإلكترونية، علاوة على أن هذا الترخيص يمكن سلطة الضبط من ممارسة الرقابة على إنشاء واستغلال خدمات الإنترنت المختلفة، من أجل منع وحظر النشاطات إذا ما رأت أنها لا تستوفي الشروط أو تمس بالنظام العام، مع العلم أن هذه السلطة ستكون محل تفصيل لاحقا، كما قام الوزير

[1] بلخير محمد آيت عودية، الضبط الإداري للشبكات الاجتماعية الإلكترونية، أطروحة مقدمة لنيل شهادة دكتوراه في العلوم، تخصص قانون عام، كلية الحقوق والعلوم السياسية، جامعة باتنة 1، 2019/2018، ص 196_197.

[2] المرسوم التنفيذي رقم 98-257 المؤرخ في 25 أوت 1998 الذي يضبط شروط وكيفيات إقامة خدمات "أنترنات" واستغلالها، ج ر ج ج عدد 63 المؤرخة في 1998/08/26، المعدل بموجب المرسوم التنفيذي رقم 2000-307 المؤرخ في 14 أكتوبر 2000، ج ر ج ج عدد 60 المؤرخة في 2000/10/15.

[3] المرسوم التنفيذي رقم 15-320 المؤرخ في 13 ديسمبر2015 الذي يحدد نظام الاستغلال المطبق على كل نوع من أنواع الشبكات بما فيها اللاسلكية الكهربائية وعلى مختلف خدمات المواصلات السلكية واللاسلكية، ج ر ج ج عدد 68 المؤرخة في 2015/12/27.

[4] القانون 2000-03 المؤرخ في 2000/08/05 الذي يحدد القواعد العامة المتعلقة بالبريد وبالمواصلات السلكية واللاسلكية، ج ر ج ج عدد 48 المؤرخة في 2000/08/06.

الأول بإصدار العديد من المراسيم التنفيذية الأخرى والتي لا يسعنا ذكرها كلها بهدف ضبط قطاعي البريد والاتصالات وكل ما يندرج تحتهما من خدمات إلكترونية.[1]

أما عن التشريعات المقارنة نجد أنه قام رئيس مجلس الوزراء المصري بإصدار جملة من اللوائح التنفيذية لضبط هذا النوع من الجرائم من أبرزها صدور اللائحة التنفيذية التي توضح آليات تطبيق القانون رقم 175 لسنة 2018 بشأن مكافحة جرائم تقنية المعلومات،[2] إذ جاءت هذه اللائحة لتبين بشكل أكبر كيفيات تطبيق هذا القانون وتأهيل الجهات المختصة بتنفيذه بحيث تكون قادرة فنيا وعمليا على تطبيقه وتكييف جرائمه،[3] إلى جانب التشريع المصري يتضح دور رئيس مجلس الوزراء الفلسطيني في ضبط الجرائم الإلكترونية من خلال إصدار بعض القرارات من بينها القرار رقم 74 لسنة 2005 بشأن الإستراتيجية الوطنية للاتصالات وتكنولوجيا المعلومات، والذي حرص من خلاله رئيس مجلس الوزراء على حماية الآداب العامة من المخاطر والتهديدات الإلكترونية وحظر كل نشاط من شأنه المساس بقيمتها، حيث قضى هذا القرار حظر إرسال أو محاولة إرسال أي إشارات مخالفة للنظام العام والأمن العام والآداب العامة[4]، كما يظهر جليا دور رئيس مجلس الوزراء من خلال قراره الخاص بحظر استخدام الأجهزة التقنية بما يتنافى مع التعاليم الدينية والعادات والحياء العام أو استخدامها لأغراض ارتياد المواقع الإباحية وغيرها من المواقع الإلكترونية ذات المحتوى السيئ والمخالف للقانون.[5]

ونظرا لأن التكنولوجيا تتطور بشكل يومي وسريع جدا في حين أن القانون لا يتطور بنفس الوتيرة المتسارعة فقد استحدثت لجنة تشريعية خاصة على مستوى مجلس الوزراء للمملكة العربية السعودية تضم مجموعة من المختصين والتقنيين ذوي المعرفة بمهارات التكنولوجيا الحديثة[6]، وفي نهاية عام 2020 اعتمدت أيضا دولة الإمارات إنشاء مجلس للأمن السيبراني يختص باقتراح وإعداد التشريعات

---

[1] لمزيد من التفاصيل يراجع الموقع الرسمي لوزارة البريد والمواصلات السلكية واللاسلكية المتاح على الرابط التالي: https://www.mpt.gov.dz

[2] القانون رقم 175 لسنة 2018 بشأن مكافحة جرائم تقنية المعلومات، المؤرخ في 14 أوت 2018، ج ر ج م عدد 32 مكرر (ج).

[3] حسام أبو غزالة، "صدور اللائحة التنفيذية لقانون جرائم المعلومات"، مقال منشور على جريدة الوطن المصرية، السبت 02 ماي 2020، على الرابط التالي: https://www.elwatannews.com/news/details/4731772 تاريخ الاطلاع: 03 فيفري 2021 .

[4] قرار مجلس الوزراء رقم 74 لسنة 2005، بشأن الاستراتيجية الوطنية للاتصالات وتكنولوجيا المعلومات، منشور على جريدة الوقائع الفلسطينية، العدد 61، مارس 2006.

[5] قرار مجلس الوزراء بشأن المصادقة على السياسات العامة لاستخدام الحاسوب وشبكة الإنترنت في المؤسسات العامة، منشور على جريدة الوقائع الفلسطينية العدد 65، بتاريخ 2006/06/14.

[6] مقال حول "الجعيد يدعو لمنظمة عالمية خاصة بالأمن السيبراني"، منشور على جريدة الشرق، الاثنين 2021/02/08، متاح على الرابط التالي: https://www.middle-east-online.com تاريخ الاطلاع: الأربعاء 2021/02/10 سا 17:40

والسياسات اللازمة لتعزيز الأمن السيبراني من أجل المشاركة في إصدار القوانين والتشريعات الكفيلة والملائمة لطبيعة الجرائم الإلكترونية، كما يختص بإعداد وتطوير وتحديث إستراتيجية للأمن السيبراني ومواجهة التحديات الرقمية محليا ودوليا، في نفس السياق وافق مجلس الوزراء القطري على مشروع قرار أميري يقضي بإنشاء وكالة وطنية للأمن السيبراني تهدف لتوحيد جهود تأمين الفضاء السيبراني والمحافظة على الأمن الوطني بصفة عامة، ولهذا يعد استحداث هذه المجالس قفزة نوعية جد هامة في مجال التصدي لهذه الجرائم.[1]

المطلب الثاني: دور الوزارات في الوقاية من الجرائم الإلكترونية.

كأصل عام لا يتمتع الوزراء بوسائل الضبط العام لأنها من اختصاص رئيس الجمهورية والوزير الأول، ولا يمكنهم اتخاذ القرارات الضبطية القابلة للتطبيق على مستوى أنحاء التراب الوطني إلا في حدود معينة يسمح بها القانون، إذ لا يتمتعون سوى بوسائل ضبط مخصصة ضمن نطاق الوزارة التي يتولى نشاطها كل وزير في إطار ما يعرف بالضبط الإداري الخاص، لكن كاستثناء قد يجيز القانون لبعض الوزراء بحكم مراكزهم وحساسية القطاع الذي يشرفون عليه ممارسة بعض أنواع الضبط العام، فيما يلي سوف نتطرق لدور أهم الوزراء في مجال ضبط الجرائم الإلكترونية.

الفرع الأول: دور وزارة الداخلية في الوقاية من الجرائم الإلكترونية.

يعد وزير الداخلية من أكثر الوزراء احتكاكا وممارسة لإجراءات الضبط على المستوى الوطني، فباعتباره الرئيس الإداري المباشر للولاة بإمكانه إصدار تعليمات وقرارات متعلقة بالضبط الإداري العام تطبق على مستوى جميع ولايات الوطن، [2] حيث يقوم باتخاذ جملة من القرارات التي من شأنها الحفاظ على النظام والأمن العموميين وذلك عبر هيئات ومديريات تعمل في هذا المجال أبرزها المديرية العامة للأمن الوطني التابعة لوزارة الداخلية والتي تعرف في بعض الدول بوزارة حفظ النظام العام[3] وجاء المرسوم التنفيذي رقم 94- 247 المؤرخ في 10 أوت 1994[4] والنصوص اللاحقة له ليحدد مهام وزير الداخلية

[1] سيف إبراهيم، "لصد الهجمات هل ينشئ الخليج مركز موحد للأمن السيبراني"، مقال مشار إليه سابقا.

[2] عليان بوزيان، أثر حفظ النظام العام على ممارسة الحريات العامة، دراسة مقارنة بين الشريعة الإسلامية والقانون الجزائري، أطروحة مقدمة لنيل شهادة الدكتوراه، تخصص الشريعة والقانون، كلية العلوم الإنسانية والحضارة الإسلامية، جامعة وهران، 2007/2006، ص 191.

[3] إسماعيل جابوربي، الضبط الإداري في مجال المحافظة على الأمن العام في الظروف الاستثنائية، المرجع السابق، ص 160.

[4] المرسوم التنفيذي رقم 94-247 المؤرخ في 02 ربيع الأول عام 1415 الموافق ل 10 أوت 1994 الذي يحدد صلاحيات وزير الداخلية والجماعات المحلية والتهيئة العمرانية.

والجماعات المحلية والتي تتمثل أساسا في المحافظة على النظام العام والأمن العمومي والحريات العامة وتسيير أعمال الوقاية والمراقبة بما يضمن أمن الإقليم الوطني، وكذا تحديد السياسة الوطنية في مجال الأمن الداخلي للإقليم، وفي هذا تسهر الوزارة على احترام القوانين والتنظيمات وضمان حماية الأشخاص والممتلكات وضمان السكينة والصحة العامة.[1]

أما عن دور وزارة الداخلية في مجال الوقاية من الجرائم الإلكترونية بصفة خاصة فيبرز فيما تصدره من قرارات وتعليمات للهيئات الواقعة تحت سلطتها بهدف وقاية النظام العام من مخاطر الاعتداءات الإلكترونية، وذلك عن طريق ما تبذله المديرية العامة للأمن الوطني من جهود للتصدي لهذا النوع من الإجرام، حيث وضعت أجهزة للشرطة مسخرة للقيام بدوريات في مواقع التواصل الاجتماعي وغرف الدردشة لتتبع النشاطات غير القانونية ومراقبة ما يحدث داخلها، ولها في ذلك جميع الصلاحيات اللازمة للوقاية من كافة صور الإجرام، من بين هذه الصلاحيات التفتيش الذي يقوم به ضابط الشرطة داخل أجهزة الكمبيوتر في مقاهي الإنترنت أو في إحدى المؤسسات للتأكد من صلاحية البرمجيات المستعملة وكشف الخروقات غير المشروعة، مثل ما هو منتشر في الآونة الأخيرة من تداول لإشاعات ومعلومات مغلوطة، [2] وتجدر الإشارة إلى أن أجهزة المديرية العامة للأمن الوطني وفي سبيل مراقبة هذه الفضاءات الإلكترونية تعقد عدة اتفاقات مع شركات الاتصال لتزويدها ببيانات المستخدمين والمعلومات الخاصة بهم والتي تساعدهم في التحري عن الجرائم الواقعة داخل هذه الفضاءات، وعلى الرغم من صلاحية أجهزة إنفاذ القانون في مراقبة الفضاءات الإلكترونية لضمان الحفاظ على الأمن العام إلا أنها تثير بعض الإشكاليات حول مشروعية هذه المراقبة وضوابطها، لاسيما وأن هدفها الحصول على المعلومات الشخصية للأفراد.[3]

أما عن دور وزارة الداخلية في مجال التعاون الدولي فقد شاركت هاته الأخيرة في جميع دورات مجلسي وزراء الداخلية والعدل العرب اللذان يعتبران من أهم هيئات جامعة الدول العربية، واللذان يهدفان إلى ترقية التعاون بين الدول العربية في مجال الأمن ومجابهة الجريمة بأنواعها، وذلك من خلال وضع الاستراتيجيات والخطط لمكافحة الجريمة المنظمة والجريمة الإلكترونية، إذ نجد في هذا الإطار أن

[1] لمعرفة المزيد عن مهام الوزارة ينظر الموقع الرسمي لوزارة الداخلية والجماعات المحلية والتهيئة العمرانية الجزائرية المتاح على الرابط التالي https://www.interieur.gov.dz تاريخ الاطلاع: 20جانفي 2021.

[2] نبيلة هبة هروال. الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات، (دراسة مقارنة)، المرجع السابق، ص 87.

[3] فاطمة الزهراء عبد الفتاح، آليات وضوابط مراقبة مواقع التواصل الاجتماعي، مقال منشور الخميس 23 فيفري 2017، على الرابط التالي: https://futureuae.com/ar/Mainpage/Item تاريخ الاطلاع: 2021/02/19 على الساعة 10:30.

وزارة الداخلية وقعت العديد من الاتفاقيات التي ترمي إلى مكافحة الجرائم من بينها الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، والاتفاقية العربية لمكافحة الجريمة المنظمة العابرة للحدود، وكذا الاتفاقية العربية لمكافحة الفساد، وليس هذا فقط بل شاركت وزارة الداخلية في الملتقيات المنظمة من طرف وزراء الداخلية لبلدان اتحاد المغرب العربي وكذا لبلدان غرب الحوض المتوسط والاتحاد الأوروبي بحيث تهدف إلى تضافر جهود الدول الأعضاء من بينهم الجزائر إلى تكثيف التعاون الأمني في مواجهة الجرائم المنظمة من بينها الجرائم الإلكترونية وجرائم غسيل الأموال والإرهاب الإلكتروني وغيرها.

يتجلى دور وزارة الداخلية لمملكة البحرين في مكافحة الجرائم الإلكترونية من خلال إصدار المرسوم رقم (24) لسنة 2010 المعدل للمرسوم رقم (69) لسنة 2004 الذي أنشأ الإدارة العامة لمكافحة الفساد والأمن الاقتصادي والإلكتروني التي يتبعها ست إدارات من بينها إدارة مكافحة الجرائم الإلكترونية، حيث تتلقى هذه الأخيرة البلاغات من خلال الموقع الإلكتروني لمكتب الشكاوى وحقوق الانسان والبلاغات من قبل المواطنين على مدار اليوم، كما تمكنهم من الحضور مباشرة للإدارة مع الاحتفاظ بالسرية التامة والخصوصية اللازمة لسير التحقيقات من أجل زرع الثقة لدى المواطنين، وتقوم إدارة مكافحة الجرائم الإلكترونية بالتعاون والتنسيق مع المؤسسات الحكومية ذات الصلة باستخدام وسائل الاتصال وخدمات الإنترنت من شركات الاتصال والشركات المزودة بخدمات الإنترنت في مجال تبادل المعلومات والكشف عن الجرائم الإلكترونية ومرتكبيها، كما تقوم الإدارة أيضا بالتنسيق مع وزارة الإعلام من أجل حصر المواقع المشبوهة المنتشرة على شبكة الإنترنت مثل المواقع الإباحية وغيرها ومنع الاطلاع عليها.[1]

في نفس الإطار حرصت وزارة الداخلية المصرية على مواكبة التطورات التقنية من أجل التصدي للجرائم الإلكترونية من خلال استحداثها لقطاع نظم الاتصالات وتكنولوجيا المعلومات المختص بتتبع هذا النوع من الجرائم وملاحقة مرتكبيها، إذ أصدر وزير الداخلية القرار رقم 13507 القاضي بإنشاء إدارة مكافحة جرائم الحاسبات وشبكات المعلومات تماشيا مع مشروع الحكومة الإلكترونية، وتعمل هذه الإدارة على ضبط ومواجهة الجرائم الإلكترونية بمختلف أنماطها، فضلا عن دورها في متابعة مقاهي الإنترنت

[1] عادل الأبيوكي، دور وزارة الداخلية في تفعيل قانون جرائم تقنية المعلومات، مقال منشور على الجريدة اليومية الأولى في البحرين، العدد 13456 الجمعة 56 ديسمبر 2014، متاح على الرابط التالي: http://www.akhbar-alkhaleej.com/13426/article/60714.html تاريخ الاطلاع: 20 جانفي 2021 الساعة 18:00،

ووضع الضوابط لتسجيل بيانات المستخدمين،[1] كما استحدثت في هذا المجال موقع إلكتروني للوزارة بحيث يستطيع المواطنين تقديم بلاغاتهم من خلاله وذلك بالدخول إلى الموقع ثم الضغط على نافذة " شكاوى وبلاغات المواطنين" ومن ثم إضافة مضمون الشكوى والبيانات اللازمة[2]، وخط هاتفي مخصص لتلقي البلاغات " الخط الساخن 15008"[3]، وهذا على غرار وزير الداخلية للمملكة العربية السعودية والذي بادر بإنشاء نموذج على موقع الوزارة الإلكتروني لاستقبال الشكاوى والبلاغات حول الإساءات التي يتعرض لها الأشخاص عبر شبكة الإنترنت حيث يتيح الموقع إمكانية التقدم عبر التسجيل بخدمات الموقع أولا من ثم التقدم بتعبئة النموذج المخصص لذلك والموجود بقسم الجرائم الإلكترونية، يطلب من المستخدم إضافة عنوان الموقع الإلكتروني الذي أساء إليه واسم المشارك واسم المسيء الذي قام بالاعتداء، وكذا تاريخ المشاركة ووقتها، وإدراج جميع المعلومات المطلوبة من خلال النموذج.[4]

وإلى جانب هذا تعمل وزارة الداخلية الفرنسية على تطبيق الإستراتيجية الوطنية للأمن الرقمي التي أعلن عنها رئيس الوزراء وذلك من قبل المندوب الوزاري للصناعات الأمنية ومكافحة التهديدات السيبرانية DMISC[5] المسؤول عن تنفيذ هذه الإستراتيجية، حيث تقوم الوزارة وفقا لهذه الإستراتيجية بتأمين الشبكات المعلوماتية للحكومة والمؤسسات الفاعلة مع ضرورة توقع التهديدات السيبرانية الممكن التعرض لها، وتعزيز مستوى أمن أنظمة المعلومات الخاصة بالوزارة، وتطوير وسائل الوقاية وتعزيز قدرات الاستجابة لهذه التهديدات مع مواكبة التطور التكنولوجي للوسائل الإلكترونية، كما تعتمد الوزارة في مجال الوقاية من الجرائم الإلكترونية على زيادة مستوى الوعي لدى المواطنين والجهات الفاعلة

---

[1] مصطفى زكي، خدمات الداخلية الإلكترونية. كيف تعاقب المتحرش عبر رسائل "فايسبوك"؟، مقال منشور على جريدة بوابة الأهرام، في 2018/11/28، على الساعة 21:23، متاح على الرابط التالي: http://gate.ahram.org.eg/News/2060253.aspx تاريخ الاطلاع: الأحد 31 جانفي 2021 على الساعة 18:15.

[2] وذلك بالدخول على بوابة شكاوى المواطنين الموجودة على مستوى الموقع الرسمي لوزارة الداخلية المصرية المتاح على الرابط التالي: https://www.egypt.gov.eg/services/default.aspx?section=citizens تاريخ الاطلاع: الأحد 31 جانفي 2021 على الساعة 19:00.

[3] دينا الحسيني، "تعرف على دور وزارة الداخلية في مواجهة جرائم الإنترنت"، الأحد 25 نوفمبر 2018 الساعة 07:00، ، مقال منشور على الرابط التالي: http://www.dotmsr.com/news/196/1268350/ تاريخ الإطلاع: 20 جانفي 2021، على الساعة 12:30.

[4] مشعل الحميدان، "الداخلية تتصدى لإساءات مواقع التواصل الاجتماعي إلكترونيا"، مقال منشور على جريدة العرب الاقتصادية الدولية، الأربعاء 08 أغسطس 2012، متاح على الرابط التالي: https://www.aleqt.com/2012/08/08/article_681378.html تاريخ الاطلاع: 20 جانفي 2021، على الساعة 13:36.

[5] DMISC : Délégué ministériel aux industries de sécurité et a la lutte contre les cybermenaces, Disponible sur le lien suivant : https://www.interieur.gouv.fr/Le-ministere/Organisation/Delegue-ministeriel-aux-industries-de-securite-et-a-la-lutte-contre-les-cybermenaces consulté le 20/02/2021 a 09:30 H

الاقتصادية وغيرها ورفع مستوى يقظتهم في مواجهة هذه التهديدات، ومن جانب آخر تعمل الوزارة وفقا لهذه الإستراتيجية على دعم ومساعدة ضحايا الجرائم الإلكترونية، وأخيرا تعزيز التعاون الفني الدولي في هذا المجال نظرا لطبيعة الجريمة السيبرانية العابرة للحدود الوطنية.[1]

تضم وزارة الداخلية الفرنسية عدة مديريات وأجهزة أمنية على رأسها المديرية المركزية للشرطة القضائية(DCPJ)[2]والتي تتفرع عنها المديرية الفرعية لمكافحة الجريمة الإلكترونية [3](SDLC) هذه الأخيرة هي المسؤولة عن محاربة الجرائم الإلكترونية بمختلف أصنافها، ومديرية للدرك الوطني[4] والتي تضم قوات للدرك مسؤولة عن مراقبة الفضاءات الإلكترونية وإجراء التحقيقات بشأن الجرائم الواقعة، كما تشرف وزارة الداخلية الأمريكية على مجموعة من المديريات والأجهزة لعل أهمها وكالة الأمن القومي الأمريكية والتي تضم داخلها وكالة للأمن السيبراني مهمتها ضبط الجرائم السيبرانية وتأمين الشبكات المعلوماتية للوقاية من هذه التهديدات، إضافة إلى هذا يعمل مكتب التحقيقات الفيديرالي (FBI) التابع لوزارة الأمن الداخلي (DHS) على تأطير وتطوير تدابير الوقاية للاستجابة المستمرة لجرائم الإنترنت.[5]

تجدر الإشارة إلى أن كل من أجهزة الأمن الوطني والدرك الوطني تملك صفتي الضبط الإداري الوقائي والضبط القضائي الردعي، حيث تقوم في سبيل منع وقوع الجرائم الإلكترونية بتأمين شبكات المعلوماتية ومراقبة الفضاءات الإلكترونية كمواقع التواصل الاجتماعي مثلا، بحيث تقوم بالتفتيش داخل غرف الدردشة ومنصات المحادثة الإلكترونية، أو داخل مقاهي الإنترنت بهدف منع أي نشاط غير قانوني يتم داخلها فإذا ما وقع هذا النشاط أو الجريمة فإن أجهزة الأمن في هذه الحالة تقوم باستكمال مهمتها بصفتها كضبطية قضائية.

---

[1]Ministère de l'intérieur, Cybersécurité la stratégie du ministère de l'intérieur, 25 /01/2016, Article Disponible sur le lien suivant :https://www.interieur.gouv.fr/Archives/Archives-des-dossiers/2016-Dossiers/Securite-les-grands-plans-d-action/Cybersecurite-la-strategie-du-ministere-de-l-Interieu consulté le 20/02/2021, a 10 :00H

[2] DCPJ : Direction centrale de la police judiciaire, Disponible sur le lien suivant : https://www.police-nationale.interieur.gouv.fr/Organisation/Direction-Centrale-de-la-Police-Judiciaire

[3] SDLC : Sous direction de la lutte contre la cybercriminalité, Disponible sur le lien suivant : https://www.police-nationale.interieur.gouv.fr/Organisation/Direction-Centrale-de-la-Police-Judiciaire/Lutte-contre-la-criminalite-organisee/Sous-direction-de-lutte-contre-la-cybercriminalite

[4] La gendarmerie nationale disponible sur le lien suivant : https://www.gendarmerie.interieur.gouv.fr/

[5] المرجع نفسه.

في نفس إطار الوقاية والمراقبة القبلية للفضاءات الإلكترونية تقوم الأجهزة الأمنية من شرطة ودرك وطني بالحملات التحسيسية لصالح المواطنين والمؤسسات كافة للتعريف بمخاطر الفضاء السيبراني وتقديم الإرشادات اللازمة لتفادي الوقوع ضحية لهذه الجرائم.

الفرع الثاني: دوروزارة الدفاع الوطني في الوقاية من الجرائم الإلكترونية.

يبرز دور وزارة الدفاع من خلال حماية أنظمتها الرقمية من مختلف الهجمات السيبرانية حيث قامت بعض الدول في العالم في السنوات الأخيرة بتطوير استخدام مهارات الإنترنت والحواسيب كأدوات هجوم ودفاع واستخبارات، إذ أنشأت العديد من الدول من بينها الولايات المتحدة الأمريكية وبريطانيا وفرنسا والجزائر وحدات خاصة في قواتها المسلحة مسئولة عن ما يسمى بالحرب الإلكترونية أو حرب المعلومات مهمتها صد الهجمات الإلكترونية، وقد عرف الدكتور Paul Rosenevier أستاذ القانون في جامعة جورج واشنطن بأمريكا في بحث له عن قانونية هذه الحروب، الحرب الإلكترونية على أنها حرب ذكية أقوى من أي هجوم بري أو جوي وأكثر ذكاء وأقل تكلفة، فهي كما قال لا تحتاج إلى معدات حربية وعتاد وجنود بل كل ما تحتاجه قدرات علمية عالية.[1]

تطبيقا لما ذكر سابقا فقد تم إنشاء دائرة الإشارة وأنظمة المعلومات والحرب الإلكترونية على مستوى وزارة الدفاع الوطني بالجزائر والتي تهدف إلى معالجة أنظمة المعلومات الإلكترونية ومراقبة نشاط شبكات التواصل الاجتماعي، في إطار الحفاظ على الأمن الوطني ضد الهجمات الإلكترونية التي تستهدف الأنظمة المعلوماتية للجيش نفسه أو التي تخص مؤسسات سيادية في الدولة، كما استحدثت مصلحة جديدة تسمى" مصلحة الدفاع السيبراني ومراقبة أمن الأنظمة" على مستوى دائرة الاستعمال والتحضير لأركان الجيش الوطني وذلك منذ سنة 2015 تهدف إلى تأمين وحماية المنظومات والمنشآت الحيوية للبلاد ضد التهديدات الإلكترونية كالإرهاب الإلكتروني والتجسس الإلكتروني، من خلال متابعة ومراقبة حالة تقدم نشاطات تجسيد السياسة الشاملة للدفاع السيبراني الرامية لضمان الحماية ضد التهديدات السيبرانية التي تستهدف أنظمة المعلومات ومنظومات الاتصال ومنظومة الأسلحة للجيش الوطني،

[1] عمر نجيب، "الحرب السيبرانية تقود العالم إلى واقع جديد ...استهداف البنية التحتية والقطاعات العسكرية والحكومية والاقتصادية وتغيير البيئة الثقافية والفكرية"، مقال منشور على صحيفة رأي اليوم، 2020/12/22 سا 09:56، على الرابط التالي: https://www.raialyoum.com/index.php/ تاريخ الاطلاع: 2021/02/13 سا 19:30.

[1]وتتضمن هذه الإستراتيجية عدة جوانب أولها أن تكون منفذة وموجهة في إطار وظيفي تنظيمي تحت سلطة مباشرة للقيادة العليا للجيش الوطني الشعبي، والجانب الثاني القانوني المكلف بتحيين وتعزيز الإطار القانوني المتعلق باستعمال تكنولوجيات الإعلام والاتصال مع تحيين مستمر للنصوص القانونية، وكذا المساهمة في إعداد القوانين والقرارات المتعلقة بالدفاع السيبراني، كما تتضمن هذه الإستراتيجية جانب الموارد البشرية حيث يتطلب وجود مورد بشري تقني " جيش افتراضي" ذو كفاءة عالية في مجال الدفاع السيبراني والتعامل مع الفضاء الرقمي بصفة عامة، فضلا عن وضع سياسة للبحث والتطوير من خلال استخدام وسائل تقنية خاصة ومتطورة مثل وسائل وتقنيات الكشف عن الهجمات وحماية الأنظمة.

إلى جانب هذا تتضمن الإستراتيجية جانبا آخر يتعلق بوقاية وتحسيس مستخدمي الجيش الوطني الشعبي من المخاطر والتهديدات الإلكترونية التي تواجههم، [2] وذلك من خلال تنظيم المؤتمرات والندوات التي تهتم بهذا الموضوع فقد نظمت مديرية الاتصال والإعلام والتوجيه لأركان الجيش الوطني في السنوات الأخيرة عدة ملتقيات حول تحقيق الأمن السيبراني، من بينها الملتقى الموسوم "بالجيش الوطني الشعبي ورهانات تداول المعلومة عبر شبكات التواصل الاجتماعي" حيث أجمع المحاضرون فيه على ضرورة تحلي العقيدة الأمنية الجزائرية باليقظة والتحكم في التكنولوجيات الحديثة، مع ضرورة تحسيس الأفراد بأهميتها ودورها في تحصين وتطوير الاتصال العسكري، فضلا عن ترقية مستوى تكوين القطاع العسكري في مجال أمن وحماية المعلومة، والتنبيه بمخاطر الحروب والتهديدات السيبرانية، [3] [4].

---

[1] مقال حول "الدعوة لإستراتيجية وطنية ناجعة لمكافحة الجريمة الإلكترونية الجيش، الوطني الشعبي بالمرصاد للتهديدات السيبرانية"، منشور على موقع المجلس الشعبي الوطني في 2021/02/09، على الرابط التالي:http://www.apn.dz/ar/plus-ar/actualite-speciale-ar/6429-2021-02-09-19- تاريخ الاطلاع: 2021/02/13 سا 18:30.

[2] حول "الدعوة لإستراتيجية وطنية ناجعة لمكافحة الجريمة الإلكترونية الجيش، الوطني الشعبي بالمرصاد للتهديدات السيبرانية"، المرجع السابق.

[3] بن مرزوق عنترة، البعد الإلكتروني للسياسة الأمنية الجزائرية في مكافحة الارهاب، مجلة العلوم الإنسانية والاجتماعية، العدد 38، جوان 2018، ص46.

[4] مقال حول "وزارة الدفاع الوطني تنظم الطبعة الثانية لملتقى الأمن والدفاع السيبراني"، منشور يوم الاثنين 25 مارس 2019، على الساعة 13:30، متاح على الرابط التالي: https://www.aps.dz/ar/algerie/68706-2تاريخ الاطلاع :2021/02/17 على الساعة 18:00. كما نظمت وزارة الدفاع الوطني في مارس 2019 الطبعة الثانية لملتقى "الأمن السيبراني والدفاع السيبراني" بغرض مناقشة الأشكال الجديدة للتهديدات السيبرانية والطرق الفعالة لمجابهتها، حيث دعا رئيس دائرة الاستعمال والتحضير لأركان الجيش الوطني إلى ضرورة تأمين البنى التحتية والرقمية الحساسة، وأكد على أن تأتي حماية هذه البنى القاعدية على رأس أولويات القيادة العليا للجيش الوطني، كما دعا للتنسيق الوطني الدولي في مجال الحفاظ على الأمن وتعزيز الدفاع السيبراني

أيضا نظمت لجنة الدفاع الوطني بالمجلس الشعبي الوطني بالنادي الوطني للجيش يوما برلمانيا حول " الجريمة الإلكترونية وتداعياتها على أمن الوطن والمواطن" وذلك يوم 09 فيفري 2021، حيث أجمع خبراء ومختصون على ضرورة تبني إستراتيجية وطنية ناجعة لمكافحة هذا النوع من الإجرام باعتباره عابرا للقارات، وكذا تعزيز المنظومة القانونية لردع المتورطين فيه بهدف حماية الأمن والاستقرار الوطنيين، من خلال مشاركة الفاعلين فيه من ضباط شرطة ودرك وطني وضباط في الجيش الوطني وممثلي عن وزارة الاتصال ووزارة العدل ووزارة الدفاع بعدة مداخلات أثرت هذا الملتقى، مؤكدين على حجم المخاطر والتهديدات الإلكترونية وأسبابها ودوافعها وإعطاء الحلول الناجعة للتصدي لها، ودعوة مختلف المصالح والمؤسسات للتعاون مع بعضها لمجابهة هذه الجرائم، فضلا عن دعوة السلطات لمراجعة الإستراتيجية الوطنية المقررة لمكافحتها من أجل الحفاظ على سلامة الوطن والمواطن، ومن جانب آخر عرض مدير المدرسة العليا للقضاء في مداخلته مختلف الاتفاقيات العربية والإفريقية والدولية الرامية لتعزيز التعاون في هذا المجال، كما دعا إلى زيادة عملية التحسيس بخطورتها وإشراك المؤسسات التربوية والتكوينية في هذه العملية.[1]

من جانب آخر وتعزيزا للدور الوقائي للوزارات في التصدي للجريمة الإلكترونية صرح المتحدث باسم الحكومة وزير الاتصال بأن الحكومة الجزائرية تشهد في السنوات الأخيرة هجوما سيبرانيا وصفه بالحرب الإلكترونية يستهدف مؤسسات الدولة على رأسها مؤسسة الجيش، يقوم به معارضين بالخارج عن طريق نشر تسريبات تخص الجيش والأجهزة الأمنية ومؤسسات الدولة الأخرى عبر الفضاء المفتوح، داعيا المختصين والمجتمع المدني إلى بناء سيادة سيبرانية للدولة على فضائها الإلكتروني وتأمين شبكة الاتصالات لمواجهة هذه الخروقات.[2]

في نفس إطار الحماية المؤسساتية للأنظمة الرقمية وكون قضايا الأمن السيبراني تمس سيادة الدولة فقد تدخل المشرع الجزائري بآليات مستحدثة من خلال إنشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال بموجب القانون رقم 04/09[3] المتضمن القواعد الخاصة للوقاية

[1] مقال حول "الدعوة لإستراتيجية وطنية ناجعة لمكافحة الجريمة الإلكترونية الجيش الوطني الشعبي بالمرصاد للتهديدات السيبرانية"، المشار إليه سابقا.

[2] عثمان لحياني، "وزير جزائري نتعرض لحرب إلكترونية خارجية تستهدف أمن البلاد"، مقال منشور يوم 2021/02/09، متاح على الرابط التالي: https://www.alaraby.co.uk تاريخ الاطلاع: 2021/02/18 على الساعة 18:40.

[3] القانون رقم 04/09 المؤرخ في 14 شعبان عام 1430، الموافق 05 أوت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج ر ج ج عدد 47، الصادرة بتاريخ 16 أوت 2009.

من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها السالف ذكره، الموضوعة تحت سلطة رئيس الجمهورية والتي تتولى تنشيط وتنسيق عمليات الوقاية من الجرائم الإلكترونية ومساعدة السلطات المختصة في التصدي لها، إلى جانب هذه الهيئة استحدث المشرع الجزائري مؤخرا منظومة وطنية لأمن المعلوماتية موضوعة لدى وزارة الدفاع الوطني بموجب المرسوم الرئاسي رقم 20-05[1] المتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية، حيث تضم هذه المنظومة مجلس أمن يكلف بإعداد الإستراتيجية الوطنية لأمن الأنظمة المعلوماتية والموافقة عليها، ووكالة الأمن للأنظمة المعلوماتية تكلف بتنسيقها وتنفيذها، يعمل هذان الأخيران بالتنسيق والتعاون مع باقي أجهزة وزارة الدفاع الوطني في مجال محاربة التهديدات الإلكترونية، [2] وعليه فإن دور وزارة الدفاع الوطني في صد الهجمات الإلكترونية ساعد كثيرا على إجهاض العديد من محاولات اختراق المواقع وقيادات الدول ومؤسساتها قبل حدوثها.

كما يبرز دور وزارة الدفاع الوطني فيما يقوم به الدرك الوطني من إجراءات وقائية وردعية للتصدي لهذه الجرائم حيث يشارك الدرك الوطني في مهمة الدفاع عن الوطن وحمايته من الأخطار التي تواجهه طبقا للخطط المقررة من قبل وزير الدفاع الوطني وبهذا يتولى ممارسة مهام الشرطة الإدارية والشرطة القضائية والشرطة العسكرية، إذ يسهر الدرك الوطني في مجال الشرطة الإدارية على حفظ النظام العام والسكينة العامة وتطبيق القوانين والتنظيمات التي تحكم الشرطة العامة، عن طريق مراقبة عامة ومتواصلة من خلال الوحدات الإقليمية والمتخصصة والتي من بينها وحدات حفظ النظام العام والتي تمتاز بالاحترافية والكفاءة المهنية في تنفيذ مهامها إذ تضطلع هذه الأخيرة بالتدخل لحفظ النظام العام وإعادته من خلال تدعيمها للوحدات الإقليمية للدرك لمكافحة مختلف أشكال الإجرام من بينها الإجرام المعلوماتي من أجل تأمين حياة الأشخاص والممتلكات، وضمان حرياتهم دون الاعتداء عليها، [3] إذ تعتبر حماية المواطن في الفضاء السيبراني جزءا لا يتجزأ من مهام الدرك الوطني وهذا ما أكده العقيد جمال بن رجم رئيس مركز مكافحة الجرائم الإلكترونية بالدرك الوطني حيث أكد على أن جميع المهام الموكلة لقوات الدرك الوطني تقليديا تمارس أيضا في الفضاء السيبراني، كما أن مركز مكافحة الجرائم الإلكترونية بالدرك الوطني والذي أنشئ منذ سنة 2004 يواكب التحديات والمستجدات وفي هذا يضطلع بمهمتين

[1] المرسوم الرئاسي رقم 20-05، يتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية، المشار إليه سابقا.

[2] حزام فتيحة، الحماية المؤسساتية للأنظمة الرقمية في الفترة التشريعية الممتدة من 2009 إلى 2020، مجلة الأكاديمية للدراسات الاجتماعية والإنسانية، المجلد 13، العدد 01، 2020/10/31، ص 280.

[3] لمعرفة المزيد عن مهام الدرك الوطني ينظر الموقع الرسمي لوزارة الدفاع الوطني الجزائري المتاح على الرابط التالي: https://www.mdn.dz تاريخ الاطلاع: 2021/02/14 على الساعة 10:17.

ينظر الملحق رقم 01.

أساسيتين أولهما قبلية وقائية تتعلق بالتحسيس والوقاية من خلال وحدة الحماية والتحليل التي تسهر على تحليل المخزون المعلوماتي على مدار 24 ساعة وحماية بنوك المعلومات المفتوحة على الإنترنت، وخلية المساعدة ومعالجة الحوادث المعلوماتية التي تسهر على حماية وتقديم المساعدة لتخطي وتفادي الوقوع في الجرائم الإلكترونية، أما المهمة الثانية فهي مهمة ردعية بعدية أي بعد وقوع الجريمة، مشيرا في هذا الصدد إلى مساهمة المركز في برنامج وطني سطرته وزارة التربية ووزارة البريد وتكنولوجيات الاتصال وكذا وزارة الأسرة لحماية الطفل من مخاطر الإنترنت والفضاء الافتراضي والذي تم من خلاله تنظيم عملية تحسيسية كبرى لإرشاد الأطفال والأولياء لوقاية أطفالهم وزيادة الرقابة عليهم في هذا الفضاء، فضلا عن إلقاء محاضرات توعوية بالمؤسسات التعليمية والتكوينية بمختلف أطوارها عن طريق إجراء تدخلات عبر وسائل الإعلام المختلفة للتنبيه بمخاطر الإنترنت بصفة عامة،[1] وتقديم النصائح والإرشادات لتفادي الوقوع ضحية للجريمة الإلكترونية أو حتى التورط فيها من بينها عدم الاحتفاظ بالملفات الشخصية على جهاز الهاتف أو الكمبيوتر مثل الصور والفيديوهات، عدم فتح ملفات أو رسائل من طرف أشخاص مجهولين وغيرها.

من جانب آخر لم تسلم الولايات م أ هي الأخرى من هذه الهجمات حيث شهدت مواقعها الحكومية والأمنية هجمات سيبرانية في عام 2010 وفي الفترة الأخيرة من عام 2020 وبداية عام 2021، استهدفت عدة مواقع حكومية من بينها وزارة الدفاع ووزارة الخارجية، كان هدفها زعزعة الثقة العامة في البنية التحتية للحكومة الأمريكية في مجال الأمن السيبراني، فرغم أن الولايات م أ تعتبر من الدول المتطورة جدا في جميع المجالات وتمتلك قوة سيبرانية هائلة مقارنة بدول العالم الأخرى بما تملكه من وسائل وتقنيات تجسس ومراقبة إلا أنها في ظل السنوات الأخيرة وقعت ضحية حرب إلكترونية، وخاصة بعد تدشين قيادة عسكرية للفضاء الإلكتروني عام 2009، وكذا القيادة للفضاء الخارجي في عام 2018 لتصبح الفرع السادس للجيش، تتولى تعزيز التدخل العسكري في حماية المواقع الإلكترونية للجيش وممارسة الأنشطة الاستخبارية وحماية الأمن القومي، والعمل على ردع القوى الدولية المنافسة، ومواجهة كل عمل يهدد البنية التحتية المعلوماتية، من خلال تبني إستراتيجية تحديد السلوكيات المزعزعة لاستقرار الحكومة الأمريكية ومحاولة تعطيلها وإحباطها قبل الوصول إلى الشبكات الأمريكية، حيث أشار بيان البانتاغون إلى أن وزارة الدفاع تعمل أيضا على تعزيز موقفها الدفاعي من خلال تقوية الشبكة وتحسين مستوى الأمن

[1] مباركية بن عمراوي، "العقيد في الدرك الوطني جمال بن رجم للإذاعة: 95 بالمائة من الجرائم الإلكترونية تم حلها بنجاح"، مقال منشور على موقع الإذاعة الجزائرية، في 2018/02/14، سا 21:30، متاح على الرابط التالي: https://www.radioalgerie.dz/news/ar/article/20180214/133919.html تاريخ الاطلاع 2021/02/12 سا 11:00.

السيبراني من خلال تأمين المعلومات السرية وكذا البنى التحتية للمؤسسات الحيوية في الدولة، لضمان قدرة الحكومة والأجهزة الأمنية والجيش الأمريكي على القتال في مجال الفضاء السيبراني والاستجابة السريعة للهجمات وردعها.[1]

على غرار الحكومات السابقة قامت الحكومة الفرنسية بإنشاء الوكالة الوطنية لأمن أنظمة المعلومات (ANSSI)[2] بموجب المرسوم رقم (2009-834) عام 2009 لدى الأمانة العامة للدفاع والأمن القومي لوزارة الدفاع الوطني والقوات المسلحة، يتولى إدارة الوكالة مدير عام يعين بمرسوم من قبل رئيس الوزراء ويساعده في مهامه نائب مدير عام، تتولى مهام الوكالة خمس مديريات فرعية تتمثل في المديرية الفرعية للعمليات التي تضم مركز المراقبة الحكومي، المديرية الفرعية للإستراتيجية، مديرية الخبرة، المديرية الفرعية للإدارة، حيث تعمل كلها في مجال التصدي للهجمات الإلكترونية التي تستهدف المؤسسات والوقاية من حدوثها، إذ تلعب دورا مهما في منع هذه الهجمات من خلال اكتشافها والتنبيه بها ودعم المؤسسات والشركات التي تقع ضحية لهذه الهجمات وتقديم المشورة لها، وتعمل على تدريب وكلائها على استخدام التقنيات الحديثة وتطويرها، مزودة بوسائل الرصد والكشف والإنذار والاستجابة للهجمات السيبرانية المختلفة.[3]

إلى جانب الوكالة السابقة قامت الحكومة الفرنسية بإنشاء ما يسمى بقيادة الدفاع السيبراني Comcyber تحت سلطة رئيس أركان القوات المسلحة في جانفي 2017[4] مسؤولة عن حماية أنظمة المعلومات على مستوى وزارة الدفاع الفرنسية كما تقدم المشورة لوزير القوات المسلحة في مجال اختصاصه، تضم هذه الهيئة ثلاثة مصالح رئيسية أولها مركز التدقيق في أمن أنظمة المعلومات ومراجعتها، مركز التحليل الدفاعي للهجمات الإلكترونية وهو المركز الخبير في مكافحة جرائم الكمبيوتر

[1] S.Nielsen, The role of the U.S military in cyberspace , Journal of information warfare , vol 15, N 02 ; 2016, p 30 ; The link : https://www.jstor.org/stable/26487529

[2] ANSSI : Agence nationale de la sécurité des systémes d'information.

[3] لمزيد من التفاصيل يراجع الموقع الرسمي لوكالة الوطنية لأمن أنظمة المعلومات على الرابط التالي:
https://www.ssi.gouv.fr/agence/organisation/les-sous-directions/centre-operationnel-de-la-securite-des-systemes-dinformation-cossi

[4] Le commandement de cyberdéfense, disponible sur le lien suivant : https://fr.wikipedia.org/wiki/Commandement_de_cyberd%C3%A9fense consulté le 15/02/2021 à 12 :00 h

والرد على الهجمات على مدار 24 ساعة، تضم أيضا المركز الاحتياطي للدفاع السيبراني المسؤول عن تدريب موظفي الإدارة بالوزارة من خلال إعداد وتنظيم تمارين الدفاع السيبراني وطنيا ودوليا.[1]

الفرع الثالث: دور وزارتي الاتصال والبريد والمواصلات السلكية واللاسلكية في الوقاية من الجرائم الإلكترونية.

مع اتساع مضمون النظام العام وشموليته لمجالات جديدة ومتنوعة كان لزاما التوجه نحو التوسع في هيئات الضبط الإداري بحيث يتولى كل وزير ممارسة إجراءات الضبط على مستوى قطاعه بهدف الحفاظ على النظام العام، [2] ولعل دور كل من وزير الاتصال ووزير البريد والمواصلات السلكية واللاسلكية يبرز بشكل كبير في مجال الوقاية من الجرائم المتعلقة بالمحتوى الرقمي نظرا لطبيعة هذه الأخيرة وعلاقتها بشبكة الاتصالات العالمية ومختلف التكنولوجيات الناتجة عنها، ولمعرفة كيفية ذلك سوف نتطرق لدور كلا الوزارتين بالتفصيل من خلال النقطتين التاليتين:

أولا: دوروزارة البريد والمواصلات السلكية واللاسلكية في الوقاية من الجرائم الإلكترونية.

منح القانون لوزير البريد والمواصلات السلكية واللاسلكية عدة صلاحيات من خلال المرسوم التنفيذي رقم 20-178[3] الذي يحدد صلاحيات وزير البريد والمواصلات السلكية واللاسلكية، فوفقا لهذا المرسوم يتولى الوزير إعداد وتنفيذ السياسة الوطنية لترقية وتطوير البريد والمواصلات وتكنولوجيات الإعلام والاتصال، وتحسين الخدمات والاتصالات الإلكترونية، المشاركة في تحديد عناصر الإطار القانوني والتنظيمي للحفاظ على الحقوق والحريات الأساسية في الفضاء السيبراني، واحترام أخلاقيات تكنولوجيات الإعلام والاتصال والنفاذ إلى الخط، أيضا يقوم الوزير في نفس الإطار بإعداد الشروط العامة لإقامة شبكات المواصلات واستغلالها ويسهر على مراقبتها، بحيث يقوم بحماية شبكات النفاذ إلى الإنترنت وحفظ المعطيات ذات الطابع الشخصي وحماية الطفولة في العالم السيبراني.[4]

---

[1] Aude Géry,La stratégie française de cyber défense, centre de doctrine et d'enseignement du commandement, mars 2020, p3.

[2] عليان بوزيان، أثر حفظ النظام العام على ممارسة الحريات العامة، دراسة مقارنة بين الشريعة الإسلامية والقانون الجزائري، المرجع السابق، ص 190.

[3] المرسوم التنفيذي 20-178 المؤرخ في 14 ذي القعدة 1441 الموافق 06 يوليو 2020، يحدد صلاحيات وزير البريد والمواصلات السلكية واللاسلكية، ج ر ج ج العدد 40، الصادرة بتاريخ 18 يوليو 2020.

[4] ينظر المواد من 02 إلى غاية المادة 11 من المرسوم التنفيذي 20-178 المشار إليه سابقا والتي تتضمن مهام وصلاحيات وزير البريد والاتصالات السلكية واللاسلكية.

هذا ويوضع تحت سلطة وزير البريد والمواصلات السلكية واللاسلكية الإدارة المركزية لوزارة البريد تشتمل على عدة أجهزة وهياكل أولها الأمين العام ، رئيس الديوان، المفتشية العامة، وبعض المديريات من بينها[1] المديرية العامة لتكنولوجيات الإعلام والاتصال، المديرية العامة لمجتمع المعلومات، مديرية الإحصاء والدراسات والاستشراف، مديرية الشؤون القانونية...الخ، حيث تتولى المديرية العامة لمجتمع المعلومات حسب نص المادة 04 من المرسوم اقتراح عناصر السياسة والإستراتيجية الوطنية لتأمين أنظمة الإعلام وتطويرها وكذا اقتراح الإطار القانوني المتعلق بمجتمع المعلومات لاسيما في مجال الإنترنت والتصديق الإلكتروني والأمن السيبراني، وكذا الجريمة الإلكترونية، والحقوق والحريات الأساسية داخل الفضاء السيبراني.[2]

بالإضافة لهذا تكلف المديرية بضمان يقظة تكنولوجية للوقاية من مخاطر استعمال تكنولوجيات الإعلام والاتصال، والقيام بالعمليات التحسيسية لحماية المواطن والطفل من مختلف التهديدات السيبرانية التي يتعرض لها داخل هذا الفضاء، لهذا الغرض أتاحت الوزارة جملة من التدابير والإجراءات الوقائية لحماية هذه الفئات الهشة كالحملات التوعوية التي تقوم بها سنويا بهدف تسليط الضوء على هذه الجرائم، توفير أدوات الرقابة الأبوية مجانا للوالدين لفرض الرقابة على الأبناء، من خلال تشجيعهم على تحميل تطبيقات وبرامج الرقابة الأبوية لتصفية إمكانية الولوج إلى بعض المحتويات، وذلك للحد من خطر التعرض للمحتويات غير الملائمة كالأشرطة الإباحية والتي تشجع على التطرف والعنف وغيرها، [3] وتحقيقا لهذه الأهداف قامت الوزارة مؤخرا بوضع دليل عملي للأولياء والمربين لحماية الأطفال عبر الإنترنت على مستوى موقعها الرسمي، حيث يقدم هذا الدليل معلومات حول المخاطر التي يمكن أن يتعرض لها الأطفال على الإنترنت وكذا الإجراءات التي يجب أن يتخذها الأولياء والمربين من أجل حماية أطفالهم وتوفير بيئة آمنة لهم في هذا الفضاء.[4]

---

[1] المرسوم التنفيذي رقم 20-179 المؤرخ في 14 ذي القعدة الموافق 06 يوليو 2020، يتضمن تنظيم الإدارة المركزية لوزارة البريد والمواصلات السلكية واللاسلكية، ج ر ج ج العدد 40، الصادرة بتاريخ 18 يوليو 2020.

[2] ينظر المادة 04 من المرسوم التنفيذي رقم 20-179 يتضمن تنظيم الإدارة المركزية لوزارة البريد والمواصلات السلكية واللاسلكية سابق الذكر.

[3] مقال حول" مهام مديرية أمن مجتمع المعلومات" منشور على الموقع الرسمي لوزارة البريد والمواصلات السلكية واللاسلكية على الرابط التالي: https://www.mpt.gov.dz تاريخ الاطلاع 2021/02/20 على الساعة 18:00.

[4] ينظر "دليل حماية الأطفال عبر الإنترنت" المتاح من طرف وزارة البريد والمواصلات السلكية واللاسلكية عبر الموقع التالي: https://www.mpt.gov.dz/sites/default/files/guide_0.pdf تاريخ الاطلاع: 2021/02/20 على الساعة 14:55.

ثانيا: دور وزارة الاتصال في الوقاية من الجرائم الإلكترونية.

أما عن وزارة الاتصال فلها دور فعال في مجال الوقاية من الجرائم الإلكترونية حيث يسهر وزير الاتصال على ضبط نشاطات الاتصال بما فيها المتصلة بالوسائل الإلكترونية وفقا للمرسوم التنفيذي رقم 11-216[1] الذي يحدد صلاحيات وزير الاتصال، إذ توضع تحت سلطته عدة هياكل أهمها الإدارة المركزية للوزارة والتي تضم أجهزة ومديريات عديدة من الأمين العام فرئيس الديوان فالمفتشية العامة، إلى جانب مديرية وسائل الإعلام، مديرية الاتصال المؤسساتي، مديرية التطوير والتعاون والتكوين، مديرية الشؤون القانونية والتوثيق وغيرها، تقوم الوزارة من خلال هذه الأجهزة بضبط نشاطات الاتصال المختلفة، وتسليم رخص ممارسة أنشطة الاتصال بما فيها الصحافة الإلكترونية من جرائد وتلفزيون وإذاعات، كما تحرص على ضمان احترام أخلاقيات وآداب المهنة وعدم تجاوز الشروط المحددة لهذه النشاطات.[2]

إن مهمة ضبط نشاطات الصحافة الإلكترونية والتي أصبحت إعلاما بديلا تعد من الأولويات التي أكد رئيس الجمهورية على ضبطها وتسوية وضعيتها القانونية كون أنها مصدر الأخبار والأحداث التي تقع في البلاد، لهذا ونظرا لما أصبحت تنشره هذه الوسائل من معلومات وأخبار مغلوطة أدت إلى نشر الفتنة وزعزعة وحدة البلاد، ونظرا لسرعة وصول هذه الأخبار للمتلقي وسهولة الاطلاع عليها فإنه كان لزاما ضبطها ومراجعتها، وفي ذلك نجد وزير الاتصال قد أكد على التعاون بين وزارته ووزارة البريد والمواصلات السلكية واللاسلكية وكذا مصالح محاربة الجريمة الإلكترونية للحد من هذه الممارسات وتحديد أصحاب المواقع الإلكترونية التي تساهم في نشر هذه الإشاعات ومتابعتهم جزائيا، كما أوضح الوزير في كلمة ألقاها خلال مشاركته في اليوم البرلماني حول " الجريمة الإلكترونية" بالنادي الوطني للجيش أن 70% من الجزائريين يتصفحون الإعلام الإلكتروني وهم بذلك معرضين دائما للاستدراج خاصة الشباب عبر غسل الأدمغة والتحريض على العنف وزعزعة القيم والأخلاق، لهذا بات من الضروري والمستعجل التصدي للجريمة الإلكترونية بمختلف أشكالها وذلك بالتركيز على ضمان سيادة سيبرانية تقوم على إنتاج محتوى

[1] المرسوم التنفيذي رقم 11-216 المرخ في 2011/06/12، الذي يحدد صلاحيات وزير الاتصال، ج ر ج ج عدد 33، المؤرخة في 2011/06/12.

[2] مقال حول "مهام الإدارة المركزية لوزارة الاتصال" منشور على الموقع الرسمي لوزارة الاتصال الجزائرية على الرابط التالي: http://www.ministerecommunication.gov.dz تاريخ الاطلاع 2021/01/01 على الساعة 15:00.

وطني نوعي على المواقع الإلكترونية وتأمين الشبكة، حيث طالب الوزير بتوطين هذه المواقع في نطاق DZ من أجل السيطرة على المحتوى الذي تعرضه للجمهور ولضمان وتحقيق الأمن السيبراني خاصة.[1]

يبرز دور كلا الوزارتين في تنظيم والمشاركة في الدورات والمؤتمرات، حيث نظمت وزارة البريد والمواصلات السلكية واللاسلكية بالتعاون مع وزارة الاتصال وبدعم من شركة قوقل بمقر مؤسسة اتصالات الجزائر يوم 03 فيفري 2021 دورة تكوينية افتراضية لفائدة الصحافيين وصانعي المحتوى حول موضوع " الذكاء الاصطناعي"[2] سعيا منها إلى تكوين الصحفي بشكل احترافي لمعالجة والتحقق من الأخبار الصحيحة من المغلوطة، بحيث تساعد تقنية الذكاء الاصطناعي هذه في التقليل من الإشاعات والأخبار الزائفة وترفع نسبة التحقق من صحتها مما يزيد من مصداقية الصحفي والمؤسسة الإعلامية، [3] ولهذا نجد معظم الدول قد تبنت إستراتيجية الذكاء الاصطناعي من ذلك وزارة الاتصالات المصرية، ففي سبيل تعزيز التعاون المصري الفرنسي في مجال الاتصال والبحث والتطوير في مجال الذكاء الاصطناعي عقدت الوزارة اتفاقا تعاونيا مع نظيرتها الفرنسية لتنفيذ مشاريع تكنولوجيات الذكاء الاصطناعي.[4]

و لعل أبرز مثال على ما تقدم ذكره ما يحصل في الآونة الأخيرة بعد انتشار جائحة كورونا حيث أصبح اهتمام الناس حول معرفة المعلومات والأخبار المتعلقة بتطورات هذه الجائحة، سواء حول معرفة مصدرها أو نسبة ارتفاعها عبر العالم، أو حتى حول اللقاح مما شهد بعض الاختراقات من طرف مقدمي المعلومة من صحفيين وإعلامين وغيرهم، من خلال المبالغة في التهويل بالوضع الوبائي وتقديم إحصائيات مغلوطة ومخوفة للجمهور مما يزيد من حدة القلق والإصابة بالأمراض الخطيرة، في هذا نجد وزارة

---

[1] بلحيمر: "الجزائر مستهدفة بحرب إلكترونية تقودها جهات أجنبية راهنت على فشل المسار الديمقراطي"، مقال منشور على الموقع الرسمي لوزارة الاتصال الجزائرية، في 2021/02/09 على الساعة 13:27، متاح على الرابط التالي: http://www.ministerecommunication.gov.dz/ar/node/9683 تاريخ الاطلاع: 2021/03/09 على الساعة 21:21.

[2] يعتبر الذكاء الاصطناعي (Artificial Intelligence) الذي يشار إليه باختصار:(AI) أحد فروع علم الحاسوب وإحدى الركائز التي تقوم عليها صناعة التكنولوجيا في العصر الحالي، ويعني قدرة الحواسيب والآلات الرقمية على القيام بمهام تحاكي وتشابه مهام الكائنات الحية الذكية، كاقدرة على التفكير والتعلم والفهم...الخ، بحيث تقدم هذه الأنظمة الذكية لمستخدميها خدمات متنوعة، ويعود تاريخ ظهور مصطلح الذكاء الاصطناعي إلى العقد الخمسين من القرن العشرين عام 1950م عندما قام العالم آلانتورينغ بتقديم ما يعرف باختبار تورنغ الذي يعنى بتقديم الذكاء لجهاز الكمبيوتر وتصنيفه ذكيا في حال قدرته على محاكاة العقل البشري، وتوالت التجارب حول هذا الاختراع ولاتزال إلى يومنا هذا، ومن بين تطبيقات الذكاء الاصطناعي الألعاب الإلكترونية مثل لعبة الشطرنج وغيرها، الروبوتات الذكية...الخ.

[3] هند دلالي، "وزارة البريد تنظم دورة تكوينية للصحفيين حول الذكاء الاصطناعي"، مقال منشور يوم 2021/02/03 على الساعة 15:30، متاح على الرابط التالي: https://www.elikhbaria.com تاريخ الاطلاع 2021/02/24 على 19:00 سا.

[4] هبة السيد، "وزير الاتصالات يبحث مع نظيره الفرنسي تعزيز التعاون المشترك بمجالات الذكاء الاصطناعي"، مقال منشور يوم الثلاثاء 2020/10/06 على الساعة 11:41، متاح على الرابط التالي: https://www.youm7.com/story/2020/10/6/ تاريخ الاطلاع: 2021/03/08 على الساعة 19:50.

الاتصال تحذر وبشكل مستمر من التضليل الإعلامي وخطاب التهويل الصادر من بعض وسائل الإعلام، فيعتبر نشر الإشاعة والأخبار المغلوطة جريمة تمس بالنظام والأمن العموميين معاقب عليها قانونا.[1]

دائما في الحديث عن جائحة كورونا وما شهده العالم من انتعاش كبير في عدة مجالات كالقطاع الصحي والتعليم الإلكتروني حيث دعم قطاع الاتصالات وتكنولوجيا المعلومات الخدمات الصحية كالمساعدة في تشخيص المصابين عن بعد والتطبيب عن بعد، وكذا التنبؤ عن تفشي الوباء، وما أتاحته الشبكة العنكبوتية للطلاب والمتمدرسين في جميع الأطوار من التعلم عن بعد، وإتاحة النفاذ المجاني إلى المنصات والمواقع الإلكترونية المختلفة، [2]بالإضافة إلى تخصيص خدمات مجانية لطواقم القطاع الصحي، [3] حيث تعتبر هذه المبادرات إيجابية جدا لتطوير الخدمات ولكن من جانب آخر أتاحت الفرصة لعدة اختراقات وهجمات سيبرانية خاصة المتعلقة بالأطفال إذ أتاحت لهم فرصة التعرض لمخاطر المحتوى الرقمي عبر المواقع المختلفة والتي كانت لها أضرار كبيرة على المستوى النفسي والاجتماعي وحتى الجسدي.

ولنفس الهدف وإيمانا بضرورة تعزيز التعاون في مجال حماية الأطفال من هذا الفضاء الرقمي عقد الاتحاد الدولي للاتصالات [4](ITU)شراكة إستراتيجية مع الهيئة الوطنية للأمن السيبراني في المملكة العربية السعودية(NCA) حيث أطلقا برنامجا عالميا بشأن إنشاء فضاء سيبراني آمن ومزدهر للأطفال، يهتم بإنشاء التدابير والبرامج الوطنية والدولية التي ستضمن حماية الأطفال عبر الإنترنت وتزويدهم هم

[1] مقال حول "كوفيد 19: وزارة الاتصال تحذر من التضليل الإعلامي وخطاب التهويل"، مقال منشور على الموقع الرسمي لوزارة الاتصال، يوم 2020/07/11 على الساعة 19:53، متاح على الرابط التالي http://www.ministerecommunication.gov.dz/ar/node/9257 تاريخ الاطلاع 2021/03/06 على الساعة 20:30.

[2] مقال حول"مناقشات رفيعة المستوى خلال حدث العالم الرقمي الافتراضي للاتحاد لعام 2020 تركز على التكنولوجيا الرقمية في مواجهة جائحة فيروس كورونا"، مقال منشور على الموقع الرسمي للاتحاد الدولي للاتصالات، يوم 2020/11/04، متاح على الرابط التالي: https://www.itu.int/ar/mediacentre/Pages/pr24-2020-Virtual-Digital-World-technology-COVID-19.aspx تاريخ الاطلاع: 2021/03/07 على الساعة 19:00.

[3] هبة السيد، "تنظيم الاتصالات: زيادة باقات الإنترنت المنزلي أبرز إجراءات مواجهة كورونا"، مقال منشور يوم الجمعة 2020/07/10 على الساعة 03:06، متاح على الرابط التالي: https://www.youm7.com/story/2020/7/10/ تاريخ الاطلاع: 2021/03/07 على الساعة 14:30.

[4] يعتبر الاتحاد الدولي للاتصالات (ITU): International Télécommunication Union الهيئة الأساسية المتخصصة لمنظمة الأمم المتحدة في مجال تكنولوجيات الإعلام والاتصال، حيث تم إنشاؤه عام 1869 مقره جنيف بسويسرا، ويضم أكثر من 193 بلدا عضوا، إلى جانب موظفي قطاع تكنولوجيات الإعلام والاتصال كسلطات الضبط والمؤسسات العمومية والخاصة والهيئات الجامعية والأكاديمية، تتمثل مهمة الاتحاد في تشجيع التطور والتنمية لشبكات الاتصالات وتسهيل وتعميم الوصول لمشاركة الأشخاص في مجتمع المعلومات وكذا تقليص الفجوة الرقمية عن طريق تشجيع دعم الكفاءات ورفع مستوى الثقة في استعمال الفضاء الرقمي السيبراني وتأمين الأنترنت، وينقسم الاتحاد إلى ثلاثة مجالات أو قطاعات للنشاط تتمثل في : قطاع الاتصالات الراديوية، قطاع تقييس الاتصالات، قطاع تنمية الاتصالات.

والمدرسين والأولياء بمهارات السلامة الرقمية اللازمة لمواجهة أخطار الإنترنت، وقد ساهمت هذه الشراكة على تعزيز المبادرات المتعلقة بحماية الأطفال في الفضاء الرقمي خاصة لدى الدول الأعضاء وبناء على المبادئ التوجيهية الجديدة للاتحاد الدولي للاتصالات لعام 2020.[1] وبهذا تعتبر المملكة العربية السعودية من بين الدول الأولى عربيا وعالميا الأكثر استعدادا لمواجهة الهجمات السيبرانية بأنواعها، وليس هذا وفقط بل يقوم الاتحاد الدولي للاتصالات دائما بعقد شركات دولية ومذكرات تفاهم مع عدة دول ومنظمات وشركات رائدة في مجال توفير الأمن على الإنترنت، مثل شركة (Symantec) للاستفادة من خبراتها في تحليل وفهم أخطار الإنترنت، وتقديم الحلول اللازمة لها فضلا عن زيادة الوعي حول هذه المخاطر.[2]

تعزيزا للأمن السيبراني وحماية البنى التحتية المعلوماتية الحساسة يضع الاتحاد الدولي للاتصالات معايير دولية تساعد الدول الأعضاء في تحديد استراتيجياتها الأمنية السيبرانية وإنشاء فرق معينة خاصة بالاستجابة لحوادث الحاسوبية من بين هذه الدول مصر، حيث تم تشكيل المركز الوطني للاستعداد لطوارئ الحاسبات والشبكات(EG Cert) التابع للجهاز القومي لتنظيم الاتصالات في أبريل 2009، ودولة الإمارات التي أسست الفريق الوطني للاستجابة لطوارئ الحاسب الآلي (AeCert)من أجل تقديم الدعم الفني على مدار 24 ساعة لحماية ودعم البنى التحتية القومية للاتصالات لمواجهة الهجمات السيبرانية، والتوعية المجتمعية بأهمية الأمن السيبراني في قطاعات الدولة المختلفة، ناهيك عن تدريب الكوادر البشرية لتفعيل منظومة الأمن السيبراني والارتقاء بها نحو الأفضل، كما يسعى الفريق إلى تعزيز قوانين مكافحة الجرائم الإلكترونية والمساعدة في استحداث أخرى تواكب التطورات الحاصلة في مجال أمن المعلومات، وبناء خبرات وطنية مجهزة ومتخصصة،[3] على غرار استحداث دولة الإمارات العربية لهذا المركز تساهم في العديد من المبادرات الرامية لمحاربة والوقاية من هذه الجرائم، إذ أطلقت الهيئة العامة

---

[1] مقال حول "الاتحاد الدولي للاتصالات والهيئة الوطنية للأمن السيبراني في المملكة العربية السعودية يطلقان برنامجا عالميا جديدا للحفاظ على سلامة الأطفال على الأنترنت"، مقال منشور على الموقع الرسمي للاتحاد الدولي للاتصالات، في 2020/12/17 متاح على الرابط التالي: https://www.itu.int/ar/mediacentre/Pages/cm11-2020-ITU-SaudiArabia-partnership-COP-guidelines.aspx تاريخ الاطلاع: 2021/03/07 على الساعة 18:30.

[2] مقال حول "الاتحاد الدولي يتخذ إجراءات فاعلة لمكافحة جرائم الأنترنت"، مقال منشور على الموقع الرسمي لوزارة الاتصالات وتكنولوجيا المعلومات المصرية، يوم 2019/05/25 متاح على الرابط التالي: https://mcit.gov.eg/Ar/Media_Center/Latest_News/News/1913 تاريخ الاطلاع: 2021/03/08 على الساعة 19:00.

[3] مقال حول "السلامة السيبرانية والأمن الرقمي"، منشور على الموقع الرسمي لحكومة دولة الإمارات، متاح على الرابط التالي: https://u.ae/ar-ae/information-and-services/justice-safety-and-the-law/cyber-safety-and-digital-security تاريخ الاطلاع 2021/03/07 على الساعة 20:00.

للاتصالات مبادرة " سفراء الإمارات للأمن الإلكتروني" والتي تهدف إلى تدريب نخبة من الطلبة في الدولة لتمثيل فريق (AeCert)كسفراء في تعزيز ونشر الوعي الأمني الإلكتروني في جميع أنحاء الدول، كما أطلقت مبادرة سايبر سي 3 (Cyber C3) التي تهدف إلى تطوير المواطن وتدريبه على امتلاك مهارة القراءة والكتابة الرقمية وفهم العواقب المحيطة به على شبكة الإنترنت وتوعيته بها وتوجيهه إلى حسن استعمالها.[1]

فضلا عن كل هذه الجهود التي يقوم بها الاتحاد الدولي للاتصالات يبرز دوره أيضا من خلال إصداره " للرقم القياسي العالمي للأمن السيبراني(GCI)" الذي من خلاله يلزم الدول الأعضاء في الاتحاد بتحقيق الأمن السيبراني من أجل خلق فضاء آمن لمستخدمي الإنترنت، حيث يقوم هذا المؤشر بقياس مدى وجود هياكل أمنية وطنية تعمل على تطبيق الأمن السيبراني، وذلك عن طريق قيامه برصد خمس نقاط أساسية في تقييمه هذا: التدابير القانونية، التدابير التقنية، التدابير التنظيمية، بناء القدرات، التعاون الدولي، كما يجري الاتحاد تدريبات سيبرانية إقليمية ووطنية بهدف تعزيز التعاون الوطني والدولي بين الدول الأعضاء على مكافحة التهديدات السيبرانية.[2]

في سياق التعاون الدولي بين وزارات البريد والاتصالات وتكنولوجيا المعلومات والذي يشكل محورا مهما في تحسين وتطوير إستراتيجية أمن المعلومات والاتصالات، تقوم الوزارات بعقد عدة اتفاقيات وشراكات مع بلدان ومنظمات تعمل على تحديد هذه الاستراتيجيات، فعلى غرار منظمة الاتحاد الدولي للاتصالات يوجد عدة منظمات أخرى في هذا المجال من أبرزها منظمة الاتحاد الإفريقي للاتصالات(ATU)[3]والتي تضم عدة بلدان من بينها الجزائر تعمل على تطوير منشآت وخدمات تكنولوجيات الإعلام والاتصال في القارة الإفريقية وعصرنتها، يوجد أيضا الاتحاد البريدي العالمي[4] (UPU)

---

[1] المرجع السابق.

[2] مقال حول "دور الاتحاد الدولي للاتصالات في بث الاطمئنان وبناء الثقة فيما يتعلق باستخدام تكنولوجيا المعلومات والاتصالات"، مقال منشور على الموقع الرسمي للاتحاد الدولي للاتصالات، متاح على الرابط التالي: https://www.itu.int/ar/mediacentre/backgrounders/Pages/role-of-ITU-in-building-confidence-and-trust-in-the-use-of-ICTs.aspx تاريخ الاطلاع: 2021/03/08 على الساعة 21:00.

[3] تأسس الاتحاد الإفريقي للاتصال (ATU) Africain Télécommunication Union : في عام 1977 كمؤسسة متخصصة في مجال الاتصالات لمنظمة الوحدة الإفريقية مقرها في نيروبي كينيا، يضم الاتحاد 44 بلدا عضوا حيث تعتبر الجزائر عضوا فيه منذ تأسيسه، و24 عضوا منتسبا، هدفه هو ضمان السهر على تقوية المنشآت وعصرنة خدمات الاتصال وتطوير تكنولوجيات المعلومات والاتصالات.

[4] يعد الاتحاد البريدي العالمي (UPU) Universal Postal Union : ثاني أقدم منظمة دولية بعد الاتحاد الدولي للاتصالات، تأسس عام 1874 مقره بمدينة برن السويسرية، يضم 192 بلدا عضوا كما يعد المنتدى الرئيسي للتعاون بين الفاعلين في قطاع البريد مما يضمن وجود شبكة عالمية للمنتجات وخدمات المتطورة في هذا المجال.

والذي يعد من أقدم المنظمات الدولية بعد الاتحاد الدولي للاتصالات تعد الجزائر عضوا فعالا فيه يعمل على ضمان جودة الخدمات البريدية المقدمة للزبائن، إلى جانب هذا يوجد الاتحاد الإفريقي للبريد (Papu)[1]، الاتحاد الأوروبي والمنظمات العربية الأخرى.

المبحث الثاني: دور سلطات الضبط الإداري الإلكتروني في الوقاية من الجرائم الإلكترونية

تتمثل سلطات الضبط الإداري الإلكتروني في السلطات الإدارية المستقلة أو ما يعرف بسلطات الضبط المستقلة، وهي الوجه الجديد لتدخل الدولة في ضبط الاقتصاد[2]، تتميز عن السلطات التقليدية في أنها لا تخضع لرقابة إدارية أو وصائية كما لا تخضع لمبدأ التدرج الهرمي الذي تتميز به الإدارة، وسميت بهذه التسمية نظرا لطبيعتها الخاصة ونوعية وظائفها، حيث خولها القانون صلاحيات واسعة في مجال ضبط مختلف النشاطات وخصها بقانون خاص وسلطة تقديرية واسعة لضرورات مرونة العمل الإداري، بحيث تختلف عن الإدارات التقليدية في أن لها القدرة على التوغل داخل العالم الإلكتروني وفرض إجراءات الضبط على النشاطات التي تتم بداخله، وتتعدد سلطات الضبط المستقلة بتعدد النشاطات التي تدخل ضمن اختصاصها، حيث تنشأ استجابة لحاجة الدولة لهذه الخدمات خاصة في ظل التطور الحاصل في مختلف الميادين منه تطور تكنولوجيات الإعلام والاتصال وما تمخض عنها من اعتداءات في مجال الاتصالات الإلكترونية وكل ما يرتبط بها من نشاطات إلكترونية، إذ زادت الحاجة إلى تأمين وضبط هذه النشاطات فظهرت العديد من السلطات الإدارية المستقلة والتي تعددت صلاحياتها بين الضبط، الرقابة، القمع وحتى تسوية المنازعات المتعلقة بها.[3] ففيما يتمثل دور هذه السلطات المستقلة في مجال ضبط النشاطات غير المشروعة ذات الطابع الإلكتروني؟

---

[1] تم إنشاء الاتحاد الإفريقي للبريد عام 1980م في أروشا تنزانيا، يهدف لتنسيق أنشطة تطوير الخدمات البريدية في إفريقيا، يضم الاتحاد 44 دولة عضوا بما في ذلك الجزائر البلد المؤسس للاتحاد.

[2] إذ ظهر هذا المفهوم لأول مرة في السبعينيات في فرنسا من خلال انشاء "اللجنة الوطنية للإعلام الآلي والحريات" كأول سلطة إدارية مستقلة في التنظيم الإداري الفرنسي، والتي تهدف للموازنة بين تنظيم تطور استغلال الإعلام الآلي في الإدارات العمومية وبين مقتضيات حماية الحريات العامة لاسيما فيما يتعلق بالمعالجة الآلية للمعطيات الشخصية للأفراد، والتي جاءت كاستجابة لحاجة الدولة في الاستعانة بوسائل الإعلام الآلي في الإدارات، أما في التشريع الجزائري فأول سلطة إدارية مستقلة تم إنشاؤها هي المجلس الأعلى للإعلام بموجب القانون رقم 70/90 المتعلق بالإعلام المؤرخ في 03 أفريل 1990 وبعدها توالى إنشاء هذه السلطات منها على سبيل المثال: مجلس النقد والقرض، اللجنة المصرفية، مجلس المنافسة، سلطة ضبط البريد والمواصلات السلكية، سلطة ضبط الغاز والكهرباء...الخ.

[3] Rachid Zouaimia, Réflexions sur le pouvoir réglementaire des autorités administratives indépendantes, Revue critique de droit et sciences politiques,volume n° 06 ; N°02 2011 ; p 10-11.

المطلب الأول: دور سلطات ضبط تكنولوجيات الإعلام والاتصال الإلكتروني في الوقاية من الجرائم الإلكترونية.

استحدثت جل التشريعات المقارنة سلطات مستقلة تتمتع بصلاحيات الضبط الإداري الإلكتروني، حيث تتولى مهمة ضبط النشاطات ذات الصلة بتنظيم قطاع الاتصالات وتكنولوجيات الإعلام والاتصال، وفرض الرقابة عليها والتصدي لمختلف الانتهاكات التي تقع بشأنها وبمساعدة بعض الفاعلين في هذا المجال ألا وهم مقدمي خدمات الإنترنت، وعليه سوف نتعرض بالشرح لكل من هذه السلطات ونحاول من خلال ذلك إبراز الدور التي تضطلع به في مجال ضبط الجرائم الإلكترونية والوقاية منها.

الفرع الأول: دور سلطة ضبط البريد والاتصالات الإلكترونية في الوقاية من الجرائم الإلكترونية

شهد قطاع المواصلات السلكية واللاسلكية إصلاحات واسعة نتج عنها استحداث مؤسسات جديدة على رأسها سلطة ضبط البريد والمواصلات السلكية واللاسلكية (ARTP)[1] والتي تعتبر هيئة إدارية مستقلة تم إنشاؤها بموجب القانون رقم 2000-03[2] الذي يحدد القواعد العامة المتعلقة بالبريد والمواصلات السلكية واللاسلكية، المعدل والمتمم بالقانون رقم 04/18[3] يحدد القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية، حيث جدد هذا الأخير إنشاء هذه السلطة لتصبح تسمى بسلطة ضبط البريد والاتصالات الإلكترونية (ARPCE)[4]، وعلى هذا سنتطرق فيما يلي للتعريف بهذه السلطة وتحديد تشكيلتها ثم إلى عرض أبرز المهام التي تضطلع بها في سبيل المنع من وقوع الجريمة الإلكترونية وكل ما يدخل في محتواها من أنشطة إلكترونية غير مشروعة.

---

[1] ARTP :L'Autorité de Régulation de la Poste et des Télécommunications سلطة ضبط البريد والمواصلات السلكية واللاسلكية

[2] القانون رقم 2000-03 المؤرخ في05 جمادى الأولى عام 1421 الموافق ل 05 أوت 2000، الذي يحدد القواعد العامة المتعلقة بالبريد والمواصلات السلكية واللاسلكية، المشار إليه سابقا.

[3] القانون رقم 04/18 المؤرخ في 24 شعبان 1439 الموافق ل 10 مايو 2018، يحدد القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية، الجريدة الرسمية للجمهورية الجزائرية، العدد 27 الصادرة بتاريخ 13 ماي 2018.

[4] ARPCE :L'Autorité de Régulation de la Poste et des communications Électronique سلطة ضبط البريد والاتصالات الإلكترونية

أولا: التعريف بسلطة ضبط البريد والاتصالات الإلكترونية وتحديد تشكيلتها

نشأت سلطة ضبط البريد والاتصالات الإلكترونية بموجب المادة 11 من القانون رقم 04/18 التي قضت بأن: " تنشأ سلطة ضبط مستقلة للبريد والاتصالات الإلكترونية تتمتع بالشخصية المعنوية والاستقلال المالي، وتدعى في صلب النص " سلطة الضبط " يكون مقر سلطة الضبط بمدينة الجزائر ".[1]

من استقرائنا لنص هذه المادة نرى أن المشرع الجزائري قد اعترف لهذه السلطة بالاستقلالية العضوية والتي تفهم من عبارة " سلطة ضبط مستقلة"[2] وذلك من أجل ممارسة وظائفها الضبطية بشكل مستقل عن جهاز الدولة وهذا ما لا يتأتى إلا عن طريق إنشاء أجهزة تتولى تسيير هذه السلطة بكل حرية واستقلالية[3]، تقابلها هيئة الاتصالات وتقنية المعلومات في دولة السعودية (CITC)[4] والتي تم إنشائها بموجب قرار مجلس الوزراء رقم 133 الصادر بتاريخ 1424/05/21هـ، تتمتع بالشخصية المعنوية والاستقلال المالي والإداري لتحقيق أهدافها، مقرها مدينة الرياض، والتي تضم مجلس إدارة برئاسة وزير الاتصال وعضوية من ممثلي عن وزارة المالية والاقتصاد والتجارة وغيرها، ومحافظ يتم تعيينه بأمر ملكي وهو المسئول التنفيذي عن إدارة الهيئة.[5]

أما عن المشرع الجزائري فقد نص بموجب المادة 19 من القانون 04/18 على تشكيلة أجهزة سلطة الضبط بحيث تضم كل من مجلس ومدير عام ويضم كلا الجهازين أجهزة فرعية أخرى، فأما عن مجلس سلطة الضبط فيتشكل بناء على المادة 20 من القانون 04/18[6] من سبعة (7) أعضاء من بينهم الرئيس يتم

---

[1] ينظر المادة 11 من القانون رقم 04/18 يحدد القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية، المشار إليه سابقا.

[2] يقصد بالاستقلالية التي تتميز بها السلطات الإدارية التقليدية، عدم خضوع السلطات إلى رقابة رئاسية مع عدم تلقيها لأية تعليمة من جهة أخرى، ولقد اعتبر الأستاذ "رشيد زوايمية" أن المقصود بالاستقلالية هو عدم خضوع لأية رقابة سلمية سواء كانت السلطة المعنية تتمتع بالشخصية المعنوية أم لا، ومعيار تمتع هذه السلطات بالاستقلالية التامة تمتعها بالاستقلالية العضوية أي الاعتراف لها بالتشكيلة الجماعية من ناحية وتنوع جهات تعيين أعضائها، وكذا تحديدها لمهام مستخدميها، بالإضافة للاستقلالية العضوية يجب ان تتمتع هذه السلطات بالاستقلالية الوظيفية أي استقلالها إداريا وماليا وذلك عن طريق عدم إلغاء القرارات والتعليمات التي تصدرها وعدم تعديلها من سلطا عليا، ومدى حريتها في وضع الأنظمة الداخلية الخاصة بها، إضافة إلى استقلالها المالي، ومثال للسلطات الإدارية المستقلة نجد سلطة ضبط البريد والمواصلات السلكية وسلطة ضبط الكهرباء والغاز، وكذا لجنة تنظيم عمليات البورصة...الخ.

[3] عائشة نشادي، إعادة هيكلة قطاع البريد والمواصلات السلكية واللاسلكية، مذكرة ماجستير، كلية الحقوق، جامعة الجزائر، 2004/|2005، ص106.

[4] CITC : Communication and information technology Commission هيئة الاتصالات وتقنية المعلومات

[5] ينظر المواد 02 ، 04 ، 08 من تنظيم هيئة الاتصالات وتقنية المعلومات ، الصادر بقرار مجلس الوزراء رقم 120 بتاريخ 1440/02/21هـ

[6] ينظر المادة 20 من القانون رقم 04/18 يحدد القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية، المشار إليه سابقا.

تعيينهم من طرف رئيس الجمهورية بناء على اقتراح من الوزير الأول[1]، إذ نلاحظ أنه اعتمد في تشكيلة مجلس سلطة الضبط على الصفة الجماعية والتي تتميز بها السلطات الإدارية المستقلة بحيث تعتبر ضمانة للاستقلالية العضوية لهذه السلطة[2]، أما عن جهاز المدير العام يتكون من مدير عام وفقا لنص المادة 25 من القانون 04/18، ومديريات عامة كطرف ثاني في هذا الجهاز تعمل تحت سلطة المدير العام والتي كان عددها ستة (6) ليصبح بعد تعديل النظام الداخلي لسلطة الضبط تسعة (9) مديريات من بينها[3] مديرية الإدارة والموارد البشرية، مديرية التصديق الإلكتروني، مديرية الإعلام الآلي والأنظمة المعلوماتية، مديرية المتعاملين ومزودي الخدمات، وغيرها...الخ.

من الملاحظ من هذه التشكيلة تنوع مديريات جهاز المدير العام واتسام أغلبها بالطابع التقني الذي يتطلبه ضبط الاتصالات، هذا التنوع في المناصب والاختصاصات من شأنه تنويع المهام المسندة لسلطة الضبط[4]، وتحقيق الفعالية في الحفاظ على النظام العام بمختلف عناصره باعتباره الهدف الأساسي التي تسعى مختلف أجهزة الضبط إلى حمايته.

ثانيا: مهام أجهزة سلطة الضبط

خول المشرع الجزائري تماشيا مع التشريعات الأخرى لسلطة ضبط البريد والاتصالات الإلكترونية صلاحيات واسعة ومتنوعة تمثلت في آليات وقائية وأخرى قمعية تهدف من خلالها إلى المحافظة على النظام والأمن العموميين، وذلك بممارستها الدور التنظيمي من خلال اقتراح القوانين والتنظيمات المتعلقة بقطاعي البريد والاتصالات، والدور الرقابي من خلال مراقبة النشاطات وإجراء التحريات واتخاذ التدابير الوقائية ضد المخالفات[5] سيتم معالجة هذه المسألة من خلال التطرق للدور التنظيمي لسلطة الضبطثم إلى الدور الرقابي لها وذلك في النقاط التالية:

---

[1] يتم تعيين أعضاء مجلس سلطة الضبط من طرف رئيس الجمهورية بموجب المرسوم الرئاسي رقم 01-109 المؤرخ في 09 صفر 1422 الموافق ل 03 ماي 2001 يتضمن تعيين أعضاء مجلس سلطة ضبط البريد والمواصلات، الجريدة الرسمية للجمهورية الجزائرية، العدد 26 الصادرة بتاريخ 09 ماي 2001.

[2] سهام صديق، مظاهر استقلالية السلطات الإدارية المستقلة في الجزائر، المجلة الجزائرية للحقوق والعلوم السياسية، المركز الجامعي أحمد بن يحي الونشريسي تيسمسيلت، العدد الرابع، ديسمبر 2017، ص 197.

[3] يراجع تشكيلة سلطة ضبط البريد والاتصالات على الموقع الرسمي لسلطة ضبط البريد والاتصالات السلكية واللاسلكية المتاح على الرابط التالي: https://www.arpce.dz تاريخ الاطلاع 2021/03/03 على الساعة 9:00.

[4] عائشة نشادي، إعادة هيكلة قطاع البريد والمواصلات السلكية واللاسلكية، المرجع السابق، ص 106-107.

[5] سهام صديق، دور سلطات الضبط الإداري في الحفاظ على النظام العام الاقتصادي، دراسة مقارنة، أطروحة مقدمة لنيل شهادة الدكتوراه في العلوم، تخصص القانون العام، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد، تلمسان، 2019/2018، ص 75.

أ) الدور التنظيمي لسلطة الضبط

تمارس سلطة الضبط اختصاصها التنظيمي عن طريق اقتراح القوانين والتنظيمات المتعلقة بتسيير قطاع البريد والاتصالات وبالرجوع للقانون 04/18 سالف الذكر وتحديدا المادة 13 منه[1] والتي تقابلها المادة 03 من تنظيم هيئة الاتصالات وتقنية المعلومات للمملكة العربية السعودية، فتتمثل صلاحياتها في المجال التنظيمي في السهر على وجود منافسة فعلية ومشروعة في سوقي البريد والاتصالات الإلكترونية باتخاذ كل التدابير الضرورية لترقية واستعادة المنافسة في هاتين السوقين، بالإضافة إلى منحها التراخيص العامة لإنشاء و/أو استغلال شبكات الاتصالات الإلكترونية وتوفير خدمات الاتصالات الإلكترونية والبريد، كما تسهر على احترام متعاملي البريد والاتصالات الإلكترونية للأحكام القانونية والتنظيمية المتعلقة على الخصوص بهذه الاتصالات وبالأمن السيبراني.

نلاحظ من خلال ما جاء في نص هذه المواد أن سلطة الضبط تتولى صلاحيات واسعة تنصب كلها في إطار تطوير خدمات البريد والاتصالات بما يضمن خدمة ذات جودة وفي نفس الوقت حماية المصلحة العامة، وأما عن دورها في مجال ضبط الأنشطة الإلكترونية غير المشروعة (الجرائم الإلكترونية) فيتجسد من خلال صلاحيتها في منح التراخيص للمتعاملين ومن بينهم مقدمي خدمات الإنترنت وتحديد الشروط الواجب إتباعها في ذلك من خلال دفتر شروط تضعه السلطة نفسها يتضمن تحديد شروط إنشاء واستغلال الشبكات الإلكترونية[2] والتي يلتزم الأشخاص بالتقيد بها من أجل التمكن من مزاولة الأنشطة ذات الصلة بهذه الشبكات والنفاذ إليها، كما يتضمن هذا الدفتر بيان كيفيات تصفح الويب والمواقع، تخزين البيانات، تسيير عناوين البريد الإلكتروني[3]، وفي هذا يخضع صاحب الترخيص خلال ممارسته لنشاطه إلى جملة من الالتزامات لمساعدة سلطة الضبط في عملها الوقائي من بينها الحفاظ على سرية المعلومات والمراسلات الخاصة للمشتركين ومنع الاطلاع عليها أو إفشائها، ووضع البرامج التي تسمح بتحديد

[1] ينظر المادة 13 من القانون 04/18 الذي يحدد القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية، سالف الذكر والتي عددت المهام الموكلة لسلطة ضبط البريد والاتصالات الإلكترونية، تقابلها المادة 03 من نظام الاتصالات وتقنية المعلومات الصادر بقرار مجلس الوزراء رقم 74 وتاريخ 1422/03/05هـ والمعدل بموجب المرسوم الملكي رقم (م/15) وتاريخ 1440/02/22هـ..

[2] تنص المادة 03 من المرسوم 15-320 الذي يحدد نظام الاستغلال المطبق على كل نوع من أنواع الشبكات بما فيها اللاسلكية الكهربائية وعلى مختلف خدمات المواصلات السلكية واللاسلكية على: " يخضع لترخيص تمنحه سلطة ضبط البريد والمواصلات السلكية واللاسلكية، إنشاء واستغلال ما يأتي:...خدمات توفير النفاذ إلى الإنترنت...".

[3] القرار رقم 51/أخ/رم/س ض ب م/ 2016 المؤرخ في 03أفريل 2016 المتضمن دفتر الشروط الذي يحدد شروط وكيفيات إقامة واستغلال خدمات توفير النفاذ إلى الإنترنت. بالرجوع للمادة 05 منه نجدها تنص على الخدمات الوسيطة التي تقدمها سلطة الضبط وتشمل ما يلي: تصفح الويب، تسيير عنوان بريد إلكتروني، النفاذ إلى المواقع الإخبارية ومنتديات النقاش، استضافة المواقع، بث عبر الصوت/ الفيديو (البث التدفقي)، تخزين البيانات، اسم النطاق، المراجع.

هوية المستخدمين وغيرها[1]، وفي حالة عدم احترام المتعامل هذه الشروط فإنه يتعرض للعقوبات المنصوص عليها في هذا القانون، أما عن دور هيئة الاتصالات وتقنية المعلومات السعودية في مجال ضبط الاتصالات والنشاطات الإلكترونية فقد أعدت إستراتيجية واضحة تهدف إلى حماية المستخدمين وضمان توفير خدمات ذات جودة لهم، والإشراف على الأمن السيبراني وحماية البيانات،[2] من خلال الحد من حوادث الاختراق لشبكات الاتصال والانترنت واتخاذ الإجراءات اللازمة لذلك، بحيث ألزمت الهيئة كل مقدم خدمة أو مستخدم أن يضع الاحتياطات الضرورية للحد من الاختراقات واستعمال أحدث الوسائل والتقنيات التي تتناسب وأهمية شبكته وأنظمته وتحديثها بشكل دوري،[3] كما توفر الهيئة خدمة الإبلاغ عن الحوادث السيبرانية عن طريق تخصيص نماذج للإنذار عن المخاطر وللإبلاغ عنها من طرف مستخدمي خدمات الاتصال، كما خصصت سلطة ضبط البريد والاتصالات الإلكترونية بالجزائر هي الأخرى موقعا لتقديم الشكاوى وذلك عن طريق ملأ مجموعة من الاستمارات وإرسالها لموقع هذه الهيئات للنظر فيها من طرف مديريها.[4]

إلى جانب هذه المهام تمارس سلطة الضبط صلاحية التنظيم عن طريق الاستشارة وذلك بإبداء الرأي في جميع القضايا المتصلة بمجال تدخلها وكذا حول مدى ملائمة اعتماد نص قانوني مرتبط بقطاع البريد والاتصالات[5] وهذا ما جاء به المشرع في نص المادة 14 من القانون 04/18 سالف الذكر، فضلا عن هذا تضطلع سلطة الضبط وهيئة الاتصالات وتقنية المعلومات بمهمة مراقبة سوقي البريد والاتصالات والتحري والتحقيق في المخالفات المرتكبة من قبل المستخدمين، واتخاذ التدابير الوقائية اللازمة، سنقوم بالتفصيل في الدور الرقابي لهذه السلطات في النقطة الموالية.

---

[1] ينظر المادة 12 من دفتر الشروط الذي يحدد شروط وكيفيات إقامة واستغلال خدمة توفير النفاذ إلى الإنترنت، المشار إليه أعلاه، والمواد 54، 55 من اللائحة التنفيذية لنظام الاتصالات الصادرة بالمرسوم الملكي رقم (م/12) بتاريخ 1422/03/12هـ، الصادرة بموجب قرار وزير الاتصالات وتقنية المعلومات رقم 4 وتاريخ 1442/01/29هـ.

[2] ينظر الخطة السنوية لعام 2021، المنشورة على الموقع الرسمي لهيئة الاتصالات وتقنية المعلومات للمملكة العربية السعودية، المتاح على الرابط التالي: file:///C:/Users/dell/Downloads/Citc-2021Annualplan.pdf تاريخ الاطلاع: 2021/03/05 على الساعة 10:19.

[3] ينظر المادة 87 من اللائحة التنفيذية لنظام الاتصالات السعودي سالف الذكر.

[4] تتاح خدمة تقديم الشكاوى على الموقع الرسمي لسلطة ضبط البريد والاتصالات الإلكترونية الجزائرية، على الرابط التالي: https://www.arpce.dz/ar/claim وأيضا على الموقع الرسمي لهيئة الاتصالات وتقنية المعلومات السعودية، المتاح على الرابط التالي: https://www.citc.gov.sa/ar/RulesandSystems/CyberSecurity/Pages/default.aspx تاريخ الاطلاع : 2021/03/05 على الساعة 10:19.

ينظر الملحق رقم02.

[5] سهام صديق، دور سلطات الضبط الإداري في الحفاظ على النظام العام الاقتصادي، المرجع السابق، ص 71-72.

ب) الدور الرقابي لسلطة الضبط

تمارس سلطة الضبط دورا رقابيا من خلال مراقبة أنشطة المتعاملين معها وإجراء التحريات اللازمة لضبط المخالفات والمنع من وقوعها[1]، وهذا ما يعني أن حريات وأنشطة المتعاملين داخل هذا القطاع ليست مطلقة وإنما يقيدها القانون برقابة تمنع إهدار المصالح المحمية، وذلك بعد منح التراخيص للمتعاملين الذين تتوافر فيهم الشروط، [2] بحيث يمكن الترخيص سلطة الضبط من ممارسة الرقابة على إنشاء واستغلال خدمات الإنترنت المختلفة، من أجل منع وحظر النشاطات إذا ما رأت أنها لا تستوفي الشروط أو تمس بالنظام العام والأمن العمومي[3]، وتتخذ هذه الرقابة صورا عديدة لعل ما يهمنا في هذه الدراسة هي التدابير المتعلقة بضبط النفاذ إلى شبكات الإنترنت والاتصالات وذلك عن طريق إجراء الحجب الكلي أو الجزئي لها، أو من خلال ضبط المحتويات المحظورة المنشورة على هذه الشبكات والمواقع الإلكترونية[4]، كما لسلطة الضبط صلاحية فرض العقوبات على المستخدمين في حالة عدم الالتزام بالشروط المفروضة، سوف نتعرض بالتفصيل لهذه الصلاحيات فيما يأتي:

- **الدور الرقابي لسلطة الضبط عن طريق اتخاذ تدابير حجب الشبكات والمواقع الإلكترونية:**

يعتبر الحجب من التدابير الوقائية المانعة لممارسة النشاط والتي تملكها سلطات الضبط حيث تمنع من خلاله المستخدمين من الوصول إلى موقع أو شبكة اتصال معينة بصفة دائمة أو مؤقتة من أجل حماية النظام العام بمختلف عناصره، كحجب المواقع الإلكترونية الإباحية أو المروجة للإرهاب وما شابه ذلك، إذ يتخذ نظام الحجب إحدى الصورتين إما أن يكون حجبا كليا أو جزئيا، ويقصد **بالحجب الكلي** التقييد الدائم والمستمر للنفاذ إلى موقع أو أكثر، ومن أبرز الدول التي تفرض الحجب الكلي لبعض المواقع الإلكترونية: الصين وإيران بحيث اتخذت الدولتين قرارات بغلق مواقع التواصل الاجتماعي "Facebook"

---

[1] تمارس سلطة الضبط إجراءات التحري والتحقيق طبقا لنص المادة 36 من المرسوم التنفيذي رقم 01-219 المتضمن الموافقة على رخصة لإقامة واستغلال شبكة عمومية للمواصلات الخلوية من نوع GSM ولتوفير خدمات المواصلات اللاسلكية للجمهور تنص على: " عندما ...=يرخص التشريع والتنظيم المعمول بهما لذلك يمكن لسلطة الضبط أن تجري لدى صاحب الرخصة تحقيقات بما فيها تلك التي تستلزم تدخلات مباشرة أو تستلزم ربط تجهيزات خارجية على شبكته الخاصة إما عن طريق أعوانها المكلفين بذلك وإما عن طريق أي شخص مؤهل قانونا من طرفها، وذلك وفق الشروط المحددة في هذا التنظيم وهذا التشريع، ولا تكتفي سلطة الضبط بصلاحية التحقيق وإنما تمتد إلى حد تفتيش المواقع في بعض الأحيان طبقا للمادة 32 من دفتر الشروط سالف الذكر.

[2] ينظر المادة 34 من القانون رقم 04/18 الذي حدد القواعد المتعلقة بالبريد والاتصالات الإلكترونية، سالف الذكر والتي تقابلها المادة 10 من الفصل الثاني المعنون بالتراخيص من اللائحة التنفيذية لنظام الاتصالات السعودي سالفة الذكر.

[3] بلخير محمدآيت عودية، الضبط الإداري للشبكات الاجتماعية الإلكترونية، المرجع السابق، ص 257.

[4] المرجع نفسه، ص 268.

و"Twitter" إلى جانب مواقع أخرى اعتبرتها منافية للأخلاق والنظام العام[1]، كما جاء قانون تنظيم قطاع الاتصالات السلكية واللاسلكية الفلسطيني بإجراء حجب الخدمة أو الاتصال أو الأنترنت عن المستخدمين في حالة وجود مخالفة للقوانين والنظام العام والآداب العامة، كما منح للإدارة المختصة ممارسة أعمال التفتيش والضبط للمواقع والشبكات الإلكترونية[2].

أما عن نظام **الحجب الجزئي** فيتمثل في حظر بعض المواقع الإلكترونية مؤقتا لمواجهة ظرف معين بحيث قد يمتد الحجب لأيام أو ساعات معدودة بحسب كل حالة، ومن أمثلة الدول التي فرضت هذا النظام مثلا أستراليا حيث قامت الهيئة الأسترالية للاتصالات والإعلام بإعداد قائمة من عناوين مواقع إلكترونية يجب حجبها من طرف مقدمي خدمات الإنترنت تسمى القائمة السوداء، كما تم إنشاء هذا النوع من القوائم من طرف المركز الوطني لمكافحة الجرائم الإلكترونية بالدنمارك، [3] أما على المستوى العربي فقد فرضت المملكة العربية السعودية ودولة الكويت أيضا نظام الحجب الجزئي، بحيث تهدف الإستراتيجية التي قررتها هيئة الاتصالات وتقنية المعلومات في السعودية إلى حماية المستخدمين بالدرجة الأولى من كل الاحتيالات التي يتعرضون لها في مجال الاتصالات وداخل الفضاءات الرقمية، ذلك من خلال محاربة كل المكالمات والرسائل الاحتيالية والعمل على الحلول الاستباقية لمنع هذا الاحتيال حيث يجوز للمستخدم أن يطلب من الهيئة تكليف مقدم الخدمة بمراقبة ورصد المكالمات الهاتفية الواردة إلى هاتفه، ويقوم بتقديم نتائج مراقبته للاتصالات إلى الهيئة متضمنة أرقام هذه الهواتف وتواريخها وعدد مرات الازعاج لتتخذ الهيئة الإجراء المناسب لذلك من حجب لهذه الاتصالات والأرقام أو إحالة الموضوع إلى السلطات المختصة إن لزم الأمر، [4] ومن أمثلة ذلك قامت الهيئة بحجب أكثر من 73 مليون رسالة و82 مليون مكالمة احتيالية وتعليق أكثر من 246 ألف رقم خلال عام 2020/2021.

نجد أيضا دولة الجزائر تعتمد هذا النوع من الحجب إذ بالرجوع للقانون الجزائري نجد أن المشرع لم ينظم قانونا واضحا وموحدا يحكم عمليات حجب المواقع والشبكات من حيث جهة الاختصاص وحالات الحجب، إلا أن هناك بعض النصوص المتفرقة التي عالجت هذه المسألة[5] من بينها المرسوم رقم

[1] إيهاب خليفة، حروب مواقع التواصل الاجتماعي، ط 01، دار العربي للنشر والتوزيع، القاهرة، 2016، ص 137 نقلا عن بلخير محمد آيت عودية، الضبط الإداري للشبكات الاجتماعية الإلكترونية، المرجع السابق، ص 273.

[2] مصطفى جمال حنفي زينو، دور الضبط الإداري في مجال الجرائم الإلكترونية المخلة بالأمن العام، المرجع السابق، ص 135.

[3] بشيخ محمد حسين، مراقبة الإنترنت وأثرها على الحريات العامة، ط 01، المكتب العربي للمعارف، القاهرة مصر، 2019، ص 141-142.

[4] ينظر المادة 55 من اللائحة التنفيذية لنظام الاتصالات السعودي سالفة الذكر.

[5] بلخير محمد آيت عودية، الضبط الإداري للشبكات الاجتماعية الإلكترونية، المرجع السابق، ص 275.

98-257 الذي يضبط شروط وكيفيات إقامة خدمات الإنترنت واستغلالها[1] في المادة 14 منه حيث يلزم مقدمي خدمات الإنترنت خلال ممارسة مهامهم بمنع النفاذ إلى الموزعات التي تحتوي معلومات تتعارض مع النظام العام أو الأخلاق والآداب العامة، لعل من أهم تطبيقات نظام الحجب الجزئي أو المؤقت بالجزائر ما قامت به من حجب لمواقع التواصل الاجتماعي خلال فترة الامتحانات بهدف منع تسريب المواضيع وذلك بالتعاون مع سلطات ضبط البريد والاتصالات.

إضافة إلى المرسوم 98-257 سالف الذكر، جاء في قرار سلطة ضبط البريد والاتصالات الإلكترونية رقم 51/أخ/رم/س ض ب م/2016 المتضمن دفتر الشروط المذكور سابقا وتحديدا في المادة 13 منه أنه يجب على صاحب الترخيص اتخاذ جميع التدابير الضرورية لضمان مراقبة محتوى الإنترنت المتاحة للمشتركين[2]، وإزالة المحتوى الضار المخالف للنظام العام أو الذي يشكل جرائم إلكترونية.

من الملاحظ أن إجراءات الحجب وإزالة المحتوى المخل بالنظام العام من الشبكات الإلكترونية هي تدابير تقوم بها سلطة الضبط عن طريق مساعدة مقدمي الإنترنت لها، بحيث تمنح لهم تراخيص بذلك وتلزمهم في المقابل بجملة من الشروط لأداء مهامهم لهذا سنفصل أكثر في هذه النقطة عند التطرق لمسؤولية مقدمي خدمات الإنترنت لاحقا.

- **الدور الرقابي لسلطة الضبط عن طريق فرض الجزاءات :**

تمارس سلطة ضبط البريد والاتصالات الإلكترونية عدة صلاحيات من بينها توقيع الجزاءات الإدارية على المتعاملين معها في حال إخلالهم بالالتزامات القانونية والتعاقدية لاسيما في مجال ضبط التعامل بشبكات الاتصال والإنترنت، فكما ذكرنا سابقا تمنح سلطات وهيئات الضبط هذه التراخيص للمتعامل معها تلزمه بموجبها بمجموعة من الشروط التي يجب عليه احترامها، فإذا أخل المتعامل بإحدى هذه الشروط تقوم السلطة بإعذاره للامتثال لها وذلك في أجل معين لا يتعدى في القانون الجزائري ثلاثين (30) يوما، وفي حالة عدم امتثاله للإعذار تتخذ السلطة ضده عقوبات مالية معينة طبقا للمادة 36 من القانون 04/18، وإذا تمادى في عدم الامتثال لشروط الاعذار مرة أخرى رغم تطبيق العقوبات المالية عليه فتتخذ السلطة ضده عقوبة التعليق الكلي أو الجزئي للترخيص وذلك على نفقته وبموجب قرار مسبب،

[1] المرسوم التنفيذي رقم 98- 257 المؤرخ في 25 أوت 1998، الذي يضبط شروط وكيفيات إقامة خدمات "أنترنات" واستغلالها، المشار إليه سابقا.

[2] ينظر قرار سلطة ضبط البريد والاتصالات الإلكترونية رقم 51/أخ/رم/س ض ب م/2016 المتضمن دفتر الشروط المذكور سابقا.

وصولا إلى قرار السحب النهائي للترخيص، علما أنه لا تطبق هذه العقوبات على المعني إلا بعد إخطاره بما عليه واطلاعه على الملف.[1]

الفرع الثاني: دور سلطة ضبط السمعي البصري في الوقاية من الجرائم الإلكترونية.

يندرج إنشاء سلطة ضبط السمعي البصري في إطار التحولات التي شهدتها الجزائر منذ بداية التسعينات، والتي دفعتها لتبني أسلوب جديد لضبط القطاعات بواسطة السلطات الإدارية المستقلة، إذ استحدث المشرع هذه السلطة من خلال قانون الإعلام رقم 12-05[2] الذي نص على سلطتي ضبط في قطاع الإعلام والاتصال هما سلطة ضبط الصحافة المكتوبة بموجب المادة 40[3] وسلطة ضبط السمعي البصري والمستوحاة من المجلس الأعلى للسمعي البصري الفرنسي "CSA"[4] والذي يقابله لجنة الاتصال الفيدرالية الأمريكية[5] (FCC)والهيئة العليا للاتصال السمعي البصري في المغرب (HACA)[6]والهيئة العليا المستقلة للاتصال السمعي البصري في تونس (HAICA)[7]، والهيئة العامة للإعلام المرئي والمسموع بالسعودية[1](GCAM).

---

[1] ينظر المادة 36 من القانون رقم 04/18 الذي يحدد القواعد المتعلقة بالبريد والاتصالات الإلكترونية سالف الذكر.

[2] القانون العضوي رقم 12-05 المؤرخ في 18 صفر 1433 الموافق 12 يناير 2012، يتعلق بالإعلام، ج ر ج ج عدد 02 الصادرة في 2012/01/15.

[3] ينظر المادة 40 من القانون رقم 12-05 المتعلق بالإعلام المشار إليه أعلاه.

[4] تعتبر أول هيئة إدارية مستقلة في مجال الإعلام هي المجلس الأعلى للإعلام الذي أنشئ بموجب القانون رقم 07/90 المؤرخ في 1990/04/23 المتعلق بالإعلام، لكنه لم يدم طويلا حيث تم حله بعد الظروف التي مرت بها الدولة الجزائرية بموجب المرسوم الرئاسي رقم 93-252 المؤرخ في 1993/10/26 المتعلق بالمجلس الأعلى للإعلام، أما عن تجربة فرنسا في مجال ضبط السمعي البصري فقد مرت بعدة مراحل بداية من سنة 1982 حيث تم إنشاء السلطة العليا للاتصالات السمعية البصرية "HACA" ثم ألغيت بموجب القانون رقم 1986-1067 المؤرخ في 1986/09/30 المتعلق بحرية الاتصال بما يسمى باللجنة الوطنية للاتصالات "CNCL" والتي عوضت بصدور القانون رقم 89-25 المؤرخ في 1989/01/17 بالمجلس الأعلى للسمعي البصري "CSA" حيث تميز هذا المجلس بالاستقلالية والنفوذ وأصبحت مهامه تكتسي طابع الإلزام تجاه المحطات الإذاعية والتلفزيونية العمومية والخاصة .لمزيد من التفاصيل أنظر:

J.Chevallier, de la cncl au csa, AJDA, 20-02-1989, p 66 ;J.chevallier, le nouveau statut de la liberté, AJDA, 20-02-1987, p 59 ;J.chevallier, les instances de régulation de l'audiovisuel, regards sur l'actualité la documentation française, n° 147, janvier 1989, pp 39-54.

[5] FCC : Federal communication commission لجنة الاتصالات الفيدرالية

تعتبر لجنة الاتصالات الفيدرالية من أولى التجارب في العالم في مجال تنظيم الإعلام السمعي المرئي، أحدثت في مارس 1927 بهدف تنظيم الإذاعة وتوزيع الترددات على طالبي التراخيص.

[6] HACA : Haute Autorité de la communication Audiovisuelle الهيئة العليا للاتصال السمعي البصري

استحدثت الهيئة العليا للاتصال السمعي البصري بموجب المرسوم الملكي رقم 212-02-1 الصادر في 31 أوت 2002 والذي تم دسترتها في سنة 2011 بموجب القانون 11-15 وأصبحت تعتبر بموجبه مؤسسة دستورية مستقلة في مجال ضبط الاتصال السمعي البصري.

[7] HAICA : Haute Autorité Indépendante de la communication Audiovisuelle الهيئةالعليا المستقلة للاتصال السمعي البصري

تقضي المادة 64 من قانون الإعلام الجزائري: "تؤسس سلطة ضبط السمعي البصري وهي سلطة مستقلة تتمتع بالشخصية المعنوية والاستقلال المالي"، وقد أحال هذا القانون تحديد مهام سلطة ضبط السمعي البصري وصلاحياتها وكذا تشكيلتها للقانون رقم 14-04 المؤرخ في 24 فبراير 2014[2] والذي يهدف إلى تحديد القواعد المتعلقة بممارسة النشاط السمعي البصري وتنظيمه، سوف نتعرض بالتفصيل إلى كل من تشكيلة سلطة ضبط السمعي البصري (أولا) ثم إلى أبرز مهامها وصلاحياتها في مجال ضبط وسائل الإعلام والاتصال (ثانيا).

أولا: التعريف بسلطة ضبط السمعي البصري وتحديد تشكيلتها

طبقا لنص المادة 64 من القانون العضوي رقم 12-05 المتعلق بالإعلام تعتبر سلطة ضبط السمعي البصري سلطة إدارية مستقلة تتمتع بالشخصية المعنوية والاستقلال المالي والإداري والقانوني، مقرها الجزائر العاصمة، تضم تشكيلة جماعية حسب نص المادة 57 من القانون رقم 14-04 المتعلق بالنشاط السمعي البصري، حيث تتضمن تسعة (9) أعضاء يعينون بمرسوم رئاسي، [3] بناء على كفاءتهم وخبرتهم واهتمامهم بالنشاط السمعي البصري[4] يتمثلون في خمسة (5) أعضاء من بينهم الرئيس يختارهم رئيس الجمهورية، عضوان (2) غير برلمانيين يقترحهما رئيس مجلس الأمة، وعضوان (2) غير برلمانيين يقترحهما رئيس المجلس الشعبي الوطني، وقد حدد المشرع مدة عضويتهم بستة (6) سنوات غير قابلة للتجديد، [5]كما بين العقوبات التي تطبق على الأعضاء في حالة إخلالهم بمهامهم داخل السلطة، [6] إلى جانب هذه العضوية توجد مجموعة من المصالح الإدارية والتقنية لسلطة ضبط السمعي البصري موضوعة تحت سلطة رئيسها ويتم تسييرها من قبل أمين عام، لكن ما يلاحظ على هذه التشكيلة أنها تضم السلطتين التنفيذية ممثلة في رئيس الجمهورية والسلطة التشريعية ممثلة في رئيس مجلس الأمة ورئيس المجلس الشعبي الوطني في حين تخلو التشكيلة من العنصر القضائي رغم أنها تملك سلطة توقيع العقوبات، أما

استحدثت الهيئة العليا المستقلة للاتصال السمعي البصري في 30 جانفي 1989 وهي مؤسسة لها ذاتيتها واستقلالها المالي والإداري تهدف لتطوير وتعزيز خدمات الاتصال والممارسة الإعلامية التونسية وخاصة المتصلة بقطاع السمعي البصري.

[1] GCAM : General commission for audiovisual media الهيئة العامة للإعلام المرئي والمسموع

تأسست الهيئة العامة للإعلام المرئي والمسموع بموجب قرار مجلس الوزراء رقم 236 بتاريخ 21 رجب 1433 كهيئة ذات شخصية اعتبارية مستقلة تتمتع بالاستقلال المالي والإداري، تعنى بتنظيم قطاع الإعلام المرئي والمسموع والإشراف عليه.

[2] القانون رقم 14-04 المؤرخ في 24 فبراير 2014، المتعلق بالنشاط السمعي البصري، ج ر ج ج عدد 16 المؤرخة في 2014/03/23.

[3] ينظر المادة 57 من القانون رقم 14-04 المتعلق بالنشاط السمعي البصري المشار إليه أعلاه.

[4] ينظر المادة 59 من نفس القانون.

[5] ينظر المادة 60 من نفس القانون .

[6] ينظر المادة 66 وما يليها من نفس القانون.

عن التشريعات المقارنة فقد استحدثت كل من دولة تونس[1] والمغرب ما يسمى بالهيئة العليا المستقلة للاتصال السمعي البصري وهي هيئات عمومية مستقلة تتمتع بالشخصية المعنوية والاستقلال المالي، تكلف بالسهر على ضمان حرية الاتصال وتعدديته، تسيرها هيئة جماعية تتكون من عدة أعضاء إدارية وتقنية مستقلة.[2]

ثانيا: مهام سلطة ضبط السمعي البصري

بالرجوع للمادة 54 من القانون رقم 14-04 نجد أن مهام سلطة الضبط تندرج كلها ضمن تنظيم ممارسة النشاط السمعي البصري وتسهيل وصول الجمهور إلى خدماتها،[3] وفي سبيل أداء مهامها هذه تتمتع السلطة بعدة صلاحيات في المجال الاستشاري ومجال الضبط والمراقبة،[4] وعليه سوف نتناول هذه الصلاحيات من خلال النقاط التالية.

أ) صلاحيات السلطة في المجال الاستشاري:

طبقا لنص المادة 55 من القانون رقم 14-04 تتمتع سلطة الضبط بعدة صلاحيات تهدف كلها لتنظيم نشاط وسائل الإعلام وتوفير خدمات جيدة للجمهور، إذ تبدي رأيها في الإستراتيجية الوطنية لتنمية النشاط السمعي البصري، وفي كل مشروع نص تشريعي أو تنظيمي يتعلق بالنشاط السمعي البصري، وفيما يخص طلب جهة قضائية رأيها في كل نزاع يتعلق بممارسة النشاط السمعي البصري، كما تقوم بالتعاون مع السلطات والهيئات الوطنية والأجنبية التي تنشط في نفس المجال[5]، كما تكتسي الهيئة العليا المستقلة للاتصال السمعي البصري التونسي والمغربي الصبغة الاستشارية التي تسيطر على عملهما من خلال إعداد التقارير وجمع المعطيات والدراسات وإبداء الرأي حول مشاريع القوانين والتنظيمات ورفعها للجهات المعنية، وتنظيم الندوات المتعلقة بمواضيع الاتصال بين مختلف المؤسسات.[6]

---

[1] لمزيد من التفاصيل ينظر الفصل السادس والسابع من الباب الثاني من المرسوم رقم 116 المتعلق بحرية الاتصال السمعي البصري.

[2] لمزيد من التفاصيل ينظر الموقع الرسمي للهيئة العليا للاتصال السمعي البصري للمغرب، المتاح على الرابط التالي: https://www.haca.ma/ar

[3] ينظر المادة 54 من القانون رقم 14-04 المتعلق بالنشاط السمعي البصري المشار إليه أعلاه.

[4] Rachid Zouaimia, L'autorité de régulation de l'audiovisuel, Revue Académique de la recherche juridique, volume 17, n° 01, 2018, p 768.

[5] ينظر المادة 55 من القانون رقم 14-04المتعلق بالنشاط السمعي البصري سالف الذكر.

[6] سفيان السهيلي، "كيف يمكن تطوير مهام المجلس الأعلى للاتصال وتنويع تركيبته"، مقال منشور يوم 2019/01/11، على الرابط التالي: https://www.turess.com/assabah/4782 تاريخ الاطلاع: 2021/03/25 على الساعة 20:00، ينظر أيضا الفصل 19 و20 من المرسوم رقم 116 المؤرخ في 2011/11/02 المتعلق بحرية الاتصال السمعي البصري التونسي.

ب) صلاحيات السلطة في مجال الضبط والمراقبة:

طبقا لنص المادة 55 من القانون رقم 14-04 سالف الذكر تقوم السلطة في مجال الضبط بدراسة طلبات إنشاء خدمات الاتصال السمعي البصري والبت فيها، وتحديد شروط استخدام وسائل الاتصال، كما تعد وتصادق بنفسها على نظامها الداخلي، [1] أما عن دورها في مجال مراقبة النشاطات فتسهر سلطة الضبط على احترام مطابقة أي برنامج سمعي بصري كيفما كانت وسيلة بثه (تقليدية أو إلكترونية) للقوانين والتنظيمات سارية المفعول، كما تمارس الرقابة بكل الوسائل المناسبة على المواضيع والمضامين التي تتطرق لها الحصص التلفزيونية والإذاعية وتضمن احترامها للمبادئ المطبقة على خدمات الاتصال السمعي البصري وكذا تطبيقها لما جاء في دفاتر الشروط.[2]

لكن لا يقتصر نشاط سلطة ضبط السمعي البصري على وسائل الإعلام التقليدية فحسب بل يمتد أيضا إلى النشاط السمعي البصري عبر الإنترنت وهذا ما نجد التأكيد عليه بموجب المادة 56 من القانون 14-04 والتي تقضي: "تمتد مهام وصلاحيات سلطة الضبط السمعي البصري إلى النشاط السمعي البصري عبر الإنترنت"[3]، فعلاوة على المهام والصلاحيات الممنوحة لهذه السلطة بموجب القانون رقم 14-04 سالف الذكر تمارس مهمة ضبط هذا النشاط في البيئة الرقمية، حيث يقصد بخدمة السمعي البصري عبر الإنترنت طبقا للمادة 69 من القانون رقم 12-05 المتعلق بالإعلام كل خدمة اتصال سمعي بصري عبر الإنترنت (واب_ تلفزيون، واب_ إذاعة) موجهة للجمهور أو فئة منه، وتنتج وتبث بصفة مهنية من قبل شخص طبيعي أو معنوي يخضع للقانون الجزائري، ويتحكم في محتواها الافتتاحي، بحيث تحتوي هذه الخدمة على أخبار ذات صلة بالأحداث اليومية، [4] فمن خلال هذه الوسائل الإلكترونية تسعى المؤسسات الإعلامية لنشر محتوياتها عبر كل الوسائل الممكنة والمتاحة للوصول إلى أكبر عدد ممكن من الجمهور، بحيث صارت اليوم مثلا الصحيفة الورقية توجد ورقيا وإلكترونيا وتتصل بقرائها عبر مختلف الشبكات الاجتماعية الإلكترونية، وتجاوزت بهذا وسائل الإعلام الإلكتروني الدور الإخباري لتنتقل إلى خلق التواصل والتفاعل بين الناس للمشاركة بأنفسهم في صنع الخبر ونشره خاصة ما يتداول عبر مواقع التواصل

[1] ينظر المادة 55 من القانون رقم 14-04 المتعلق بالنشاط السمعي البصري سالف الذكر.

[2] ينظر المادة 55 من القانون رقم 14-04 سالف الذكر والتي تقابلها المواد من 06 إلى 10 من الظهير الشريف رقم 257-04-1 الصادر في 07 يناير 2005 بتنفيذ القانون رقم 03-77 المتعلق بالاتصال السمعي البصري المغربي، والمواد 03 إلى 06 والمواد 10 و11 من قانون نظام الإعلام السعودي، والفصول 15 و16 و19 و20 من القسم الثاني من الباب الثاني 02 من المرسوم رقم 116 المؤرخ في 2011/11/02 المتعلق بحرية الاتصال السمعي البصري التونسي، والتي تبين مهام والتزامات هذه الهيئات والمؤسسات الإعلامية التابعة لها.

[3] ينظر المادة 56 من القانون رقم 14-04 المتعلق بالنشاط السمعي البصري سالف الذكر.

[4] ينظر المادة 69 من القانون رقم 12-05 المتعلق بالإعلام المشار إليه سابقا.

الاجتماعي من فيسبوك وتويتر وغيرها[1]، كما نجد المشرع السعودي قد نص بصراحة على تنظيم جميع الأنشطة الإعلامية التقليدية والإلكترونية والتي عددها على سبيل المثال لا الحصر من خلال المادة 03 من قانون نظام الإعلام السعودي[2]، ولكن ماذا عن المخالفات التي قد تنجم عن هذه النشاطات؟

نجد أن المشرع الجزائري قد أكد على ضرورة احترام النشاط السمعي البصري التقليدي وعبر الإنترنت لمبادئ الدستور والدين الإسلامي، ومتطلبات النظام العام، في كل من قانون الإعلام من خلال المادة 02 منه[3] والقانون المتعلق بالنشاط السمعي البصري من خلال المادة 54 منه[4] والتي أكدت على ضرورة احترام الكرامة الإنسانية وحماية الطفل المراهق، [5] كما أكد المشرع الجزائري على احترام هذه المبادئ من خلال

[1] بلخير محمد آيت عودية، الضبط الإداري للشبكات الاجتماعية الإلكترونية، المرجع السابق، ص 207.

[2] تنص المادة 03 من قانون نظام الإعلام السعودي على: " تخضع لأحكام هذا النظام جميع الأنشطة الإعلامية التقليدية والإلكترونية ومنها على سبيل المثال لا الحصر ما يلي:

- الصحف الورقية والإلكترونية
- النشر الإلكتروني بكلفة أنواعه ومنصاته ووسائله
- الألعاب الإلكترونية بكافة أشكالها ووسائلها
- الدعاية التقليدية والإلكترونية..."

[3] تنص المادة 02 من القانون رقم 12-05 المتعلق بالإعلام على: "يمارس نشاط الإعلام بحرية في إطار أحكام هذا القانون العضوي والتشريع والتنظيم المعمول بهما، وفي ظل احترام:

- الدستور وقوانين الجمهورية.
- الدين الإسلامي وباقي الأديان.
- الهوية الوطنية والقيم الثقافية للمجتمع.
- السيادة الوطنية والوحدة الوطنية.
- متطلبات أمن الدولة والدفاع الوطني.
- متطلبات النظام العام.
- .المصالح الاقتصادية للبلاد.
- مهام والتزامات الخدمة العمومية.
- حق المواطن في إعلام كامل وموضوعي.
- سرية التحقيق القضائي.
- الطابع التعددي للآراء والأفكار
- كرامة الإنسان والحريات الفردية والجماعية."

[4] تنص المادة 54 فقرة 07 و08 من القانون رقم 14-04 المتعلق بالنشاط السمعي البصري على: "...السهر على احترام الكرامة الإنسانية. السهر على حماية الطفل المراهق"

[5] مثال ذلك ما سجلته سلطة ضبط السمعي البصري من تجاوزات متعلقة بالأطفال والماسة بحياتهم الخاصة وكرامتهم وسلامتهم المعنوية بحيث نبهت السلطة إلى عدم تداول الفيديوهات على مواقع التواصل الاجتماعي أو القنوات التلفزيونية التي يكون مضمونها الطفل وشددت على منع استعماله في ومضات اشهارية أو أفلام أو تسجيلات إلا بترخيص من ممثله الشرعي وطبقا للتشريع والتنظيم المعمول به، ومعاقبة كل من يستغل الطفل عبر وسائل الاتصال مهما كان شكلها في مسائل منافية للآداب العامة والنظام العام. لمزيد من التفاصيل ينظر: مقال

المرسوم التنفيذي رقم 16-222 المؤرخ في 11 أوت 2016 والذي يتضمن دفتر الشروط العامة الذي يحدد القواعد المفروضة على كل خدمة للبث التلفزيوني أو للبث الإذاعي من خلال مادته الثامنة (08) والتي تلزم مسئولي خدمات الاتصال السمعي البصري بالسهر على احترام الوحدة الوطنية والأمن والدفاع الوطنيين،[1] والتي تقابلها المادة 03 من القانون المغربي رقم 257-04-1 الصادر في 2005 المتعلق بالاتصال السمعي البصري، [2] والفصل الخامس من الباب الأول من المرسوم رقم 116 المؤرخ في 2011/11/02 المتعلق بحرية الاتصال السمعي البصري التونسي، [3] والمادة 09 من قانون نظام الإعلام السعودي.[4]

وفي حالة عدم احترام هذه المبادئ والنصوص التشريعية والتنظيمية يتعرض صاحب الخدمة أو النشاط إلى عقوبات إدارية وجزائية طبقا لما جاء في المواد من 98 إلى المادة 111 من القانون رقم 14-04 سالف الذكر، فوفقا لهذه المواد يتعرض كل شخص طبيعي أو معنوي مستغل لخدمة الاتصال السمعي البصري إلى الاعذار أولا وفي حالة عدم امتثاله للإعذار في الأجل المحدد له تسلط عليه العقوبات المالية المقررة في هذا القانون، وفي حالة عدم امتثاله لمقتضيات الإعذار رغم العقوبة المالية فتسلط عليه السلطة عقوبة التعليق الجزئي أو الكلي للبرنامج الذي يبثه أو تعليق الرخصة أو سحبها إلى جانب العقوبات الجزائية المنصوص عليها وفقا للمواد من 107 إلى المادة 111 من القانون 14-04، [5] وهو نفس الحال بالنسبة للهيئات العليا للاتصال السمعي البصري في كل من تونس والمغرب والمجلس الأعلى للسمعي البصري

حول "متابعات قضائية ضد القنوات التلفزيونية التي تمس بالحياة الخاصة للأطفال"، منشور على موقع وزارة الاتصال يوم 2021/01/25 ...=على الساعة 19:47، متاح على الرابط التالي: http://www.ministerecommunication.gov.dz/ar/node/9664تاريخ الاطلاع: 2021/03/01 على الساعة 12:00.

[1] تنص المادة 08 من المرسوم التنفيذي رقم 16-222 على: "يسهر مسؤولوا خدمات الاتصال السمعي البصري على تصميم وإعداد القواعد المتعلقة بالبرمجة وبث البرامج خصوصا على تطبيق المبادئ الآتية:

- احترام القيم الوطنية ورمز الدولة كما هي محددة في الدستور،
- احترام متطلبات الوحدة الوطنية والأمن والدفاع الوطنيين، والنظام العام وكذا المصالح الاقتصادية والدبلوماسية للأمة،
- احترام الثوابت والقيم الدينية والأخلاقية والثقافية للأمة،
- احترام المرجعيات الدنية والمعتقدات والديانات الأخرى،
- احترام الحق في الشرف وستر الحياة الخاصة للمواطن وكذا حماية الأسرة،
- حماية الفئات الضعيفة "

[2] الظهير الشريف رقم 257-04-1 الصادر في 07 يناير 2005 بتنفيذ القانون رقم 03-77 المتعلق بالاتصال السمعي البصري، المشار إليه سابقا.

[3] المرسوم رقم 116 المؤرخ في 2011/11/02 يعلق بحرية الاتصال السمعي البصري وبإحداث هيئة عليا مستقلة للاتصال السمعي والبصري، المشار إليه سابقا.

[4] قانون نظام الإعلام السعودي، المشار إليه سابقا.

[5] ينظر المواد من 98 إلى 111 من القانون رقم 14-04 الذي يحدد القواعد المتعلقة بالبريد والاتصالات الإلكترونية سالف الذكر.

الفرنسي وكذا لجنة الاتصال الفيدرالية الأمريكية ففي حالة عدم الالتزام ببنود دفتر الشروط أو كما يسمى في بعض التشريعات "كراس الشروط" وعدم احترام القواعد العامة للممارسة الإعلامية وأخلاقيات المهنة يتم سحب رخصة البث بصفة جزئية أو نهائية، إضافة إلى اتخاذ العقوبات الجزائية اتجاه المخالفين لهذه القواعد.[1]

من جانب آخر راعى المشرع الجزائري بروز هذا النوع الهجين من الإعلام الذي يجمع الإعلام التقليدي وتقنيات الإعلام الإلكتروني والصحافة الإلكترونية من خلال إصدار المرسوم التنفيذي رقم 20-332 المؤرخ في 22 نوفمبر 2020[2] والذي يحدد كيفيات ممارسة نشاط الإعلام عبر الإنترنت ونشر الرد أو التصحيح عبر الموقع الإلكتروني، حيث يهدف هذا المرسوم إلى محاربة كل أشكال تزييف المعلومة والتي أصبح لها أثر بالغ في تشويه سمعة الأشخاص بأصنافهم وذلك من خلال تركيب الصور والأصوات وتغيير مضمون الحقيقة خاصة ما يتم تداوله عبر مواقع التواصل الاجتماعي المختلفة، وفي هذا أكد وزير الاتصال على ضرورة إنتاج مضمون وطني قوي لمكافحة الأخبار المغلوطة، وقام بتنظيم ورشات لفائدة الصحفيين متخصصة في مجال الكشف عن الأخبار الكاذبة ومحاربة هذا التزييف للمعلومة، كما ألزم المشرع من خلال هذا المرسوم وطبقا للمواد من 13 إلى المادة 21 منه المدير المسئول عن جهاز الإعلام الإلكتروني بضرورة اتخاذ جميع التدابير اللازمة لمكافحة المحتوى غير القانوني في إطار احترام أحكام المادة 02 من قانون الإعلام ولا سيما كل محتوى يتضمن التحريض على الكراهية والعنف والتمييز، كما يجب عليه إخطار الجهات المعنية بكل محتوى غير قانوني للقيام بسحبه أو تعديله، [3] كما يلتزم أيضا المدير بضمان أمن تكنولوجيا المعلومات[4] إذ في حالة وجود محتوى ناجم عن قرصنة أو اختراق لموقع إلكتروني يتعين على المسئول إثباته بكل الوسائل وتبليغ السلطات المعنية بذلك، وتوقيف هذا الموقع مؤقتا لغاية تصحيح هذا الاختراق.[5]

---

[1] ينظر المواد 70 من الظهير الشريف رقم 257-04-1 سابق الذكر والمادة 15 من قانون نظام الإعلام السعودي، والفصول من 27 إلى 41 من القسم الثاني من الباب الثاني من المرسوم رقم 116 المتعلق بحرية الاتصال السمعي البصري المشار إليهما سابقا، والتي تبين الجزاءات الإدارية والعقوبات الجزائية المطبقة في حالة عدم الالتزام بشروط الخدمة الإعلامية.

[2] المرسوم التنفيذي رقم 20-332 المؤرخ في 08 ربيع الثاني عام 1442 الموافق 22 نوفمبر 2020، الذي يحدد كيفيات ممارسة نشاط الإعلام عبر الإنترنت ونشر الرد أو التصحيح عبر الموقع الإلكتروني، ج ر ج ج عدد 70 الصادرة في 25 نوفمبر 2020.

[3] ينظر المادة 13 من المرسوم التنفيذي رقم 20-332 الذي يحدد كيفيات ممارسة نشاط الإعلام عبر الإنترنت ونشر الرد أو التصحيح عبر الموقع الإلكتروني سالف الذكر.

[4] ينظر المادة 16 من المرسوم التنفيذي سالف الذكر.

[5] ينظر المادة 17 من المرسوم التنفيذي سالف الذكر.

وفي حالة الإخلال بالالتزامات السابقة يتعرض جهاز الإعلام عبر الإنترنت للإعذار من قبل السلطة المكلفة بالصحافة الإلكترونية أو السلطة المكلفة بخدمة السمعي البصري عبر الإنترنت وفي حالة عدم الامتثال يتم التعليق المؤقت للنشاط لمدة 30 يوم وفي حالة عدم الامتثال مرة ثانية فيتم سحب شهادة التسجيل والتي تسلم لمستضيف الخدمة عند الموافقة على ممارسته لنشاط معين عبر الإنترنت، دون الإخلال بالعقوبات المنصوص عليها في القانون المتعلق بالإعلام، [1] فبموجب هذا المرسوم أتاح المشرع الفرصة لكل شخص طبيعي أو معنوي تم ذكره اسميا أو تحديده ضمنيا في محتوى الإعلام عبر الإنترنت أن يستعمل حقه في الرد والتصحيح اتجاه كل اتهامات كاذبة أو ماسة بشرفه وسمعته أو أي وقائع وآراء أوردتها وسيلة الإعلام المعنية بصورة غير صحيحة، وتحدد كيفيات وآجال الرد والتصحيح بموجب المواد من 103 إلى 114 من القانون 12-05 المتعلق بالإعلام، والمواد 36 إلى 40 من المرسوم التنفيذي 20-332 سالف الذكر.[2]

وتجدر الإشارة إلى أن دور هذه السلطات والهيئات يتمثل في إنذار المتعامل واقتراح طبيعة العقوبة المفروضة عليه، أما عن مهمة توقيع هذه العقوبات فتوكل إلى الوزير المكلف بهذا القطاع دون المساس بالمتابعات القضائية اللازمة، كون أن توقيع العقوبات مهمة الجهات القضائية وبالرجوع إلى القانون المقارن نجد أن المجلس الدستوري الفرنسي قد أجاب عن هذه المسألة حيث وضع شروطا لممارسة السلطات الإدارية المستقلة هذه الوظيفة، إذ جاء في قرار أصدره بتاريخ 23 جويلية 1996 بأنه يجب أن لا تمس العقوبة بالحرية بل تهدف السلطة من خلال فرضها إلى حماية الحقوق والحريات المضمونة دستوريا.[3]

الفرع الثالث: دور سلطات التصديق الإلكتروني في الوقاية من الجرائم الإلكترونية.

إن الثقة والأمان لدى المتعاملين عبر شبكة الإنترنت هما أهم ضمانات نجاح وازدهار التعاملات الإلكترونية لذلك تم إسناد حماية هذه البيانات والمعلومات المتبادلة بين المتعاملين وتأكيد صحتها إلى جهات محايدة وموثوقة، حيث استحدث التشريعات المقارنة الأجنبية منها والعربية جهات تصديق موثوقة من بينها المشرع السعودي والمشرع السوري باستحداث المركز الوطني للتصديق الإلكتروني، والمشرع

[1] ينظر المواد 32 33 34 35 من المرسوم التنفيذي سالف الذكر.

[2] لمزيد من التفاصيل يراجع المواد من 36 إلى 40 من المرسوم التنفيذي رقم 20-332 سالف الذكر والمواد من 103 إلى 114 من القانون 12-05 المتعلق بالإعلام.

[3] Décision n° 96-378 DC de 23 juillet 1996, a propos de l'autorité de régulation des télécommunications, JORF du 27 juillet 1996.

لمزيد من التفاصيل حول دور المجلس الدستوري الفرنسي في إرساء نظرية الجزاء الإداري ينظر الشوا محمدسامي، القانون الإداري الجزائي، دار النهضة العربية، مصر، 1996، ص 82 وما بعدها.

المصري باستحداث سلطة التصديق الجذرية والحكومية، أما عن المشرع الجزائري فقد استحدث من خلال القانون رقم 04/15 المؤرخ في فبراير 2015 الذي يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين[1] ما يسمى بجهات التصديق الإلكتروني والتي تعمل على خلق بيئة إلكترونية آمنة للتعامل، وهذا عن طريق مخطط وطني وضعته جل التشريعات يتعلق بالتصديق الإلكتروني يتكون من السلطة الرئيسية الوطنية وسلطتين ملحقتين بها، إحداهما مخصصة للفرع الحكومي والأخرى للفرع الاقتصادي أو التجاري سوف نتطرق بالتفصيل لكل منها.

أولا: دور السلطة الوطنية للتصديق الإلكتروني[2] (ANCE)

وفقا لنص المادة 16 من القانون رقم 04/15 تعتبر السلطة الوطنية للتصديق الإلكتروني سلطة إدارية مستقلة تتمتع بالشخصية المعنوية والاستقلال المالي، وتدعى في صلب النص " السلطة"، تنشأ لدى الوزير الأول ويحدد مقرها بالجزائر العاصمة ويمكن نقله لأي مكان آخر من التراب الوطني، وتتشكل السلطة الحكومية للتصديق إ من مجلس يضم 5 أعضاء من بينهم الرئيس يعينهم رئيس الجمهورية على أساس كفاءاتهم في مجال العلوم التقنية وتكنولوجيات الاتصال، ومصالح تقنية وإدارية يسيرها مدير عام يعينه أيضا رئيس الجمهورية، [3] يقابلها في التشريع السعودي المركز الوطني للتصديق الإلكتروني الذي تم إنشائه وفقا لقرار اللجنة الدائمة للتجارة الإلكترونية في 1422/01/10، والذي يحتوي على مركز للتصديق الجذري السعودي ومراكز التصديق المندرجة تحته، [4] أما عن المشرع المصري هو الآخر قام باستحداث سلطة تدعى "سلطة الجذر المصرية".[5]

تتولى كل من السلطة الوطنية للتصديق إ طبقا للمادة 18 من القانون رقم 04/15 والمركز الجذري السعودي والمصري إعداد سياسة التصديق والسهر على تطبيقها والموافقة على سياسات التصديق إ الصادرة عن السلطتين الحكومية والاقتصادية والتدقيق فيها، كما تقوم هذه الهيئات باقتراح مشاريع

[1] القانون رقم 04/15 المؤرخ في 11 ربيع الثاني عام 1436 الموافق 01 فبراير 2015، يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، ج ر ج ج عدد 06، الصادرة بتاريخ 10 فبراير 2015.

[2] ANCE : Autorité Nationale de Certification Électronique

[3] ينظر المواد 16، 17، 19 من القانون رقم 04/15 يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، سالف الذكر.

[4] لمزيد من التفاصيل يراجع الموقع الرسمي للمركز الوطني للتصديق الرقمي السعودي، المتاح على الرابط التالي: https://www.ncdc.gov.sa/?page_id=1893 تاريخ الاطلاع: 2021/03/22 على الساعة 11:00

[5] لمزيد من التفاصيل يراجع الموقع الرسمي للسلطة الحكومية للتصديق الإلكتروني المصرية، المتاح على الرابط التالي: http://www.govca.gov.eg/services.php تاريخ الاطلاع: 2021/03/22 على الساعة 12:00.

القوانين والتنظيمات المتعلقة بخدمات التوقيع والتصديق إ، أما عن المصالح التقنية للسلطة الوطنية فقد أحال المشرع الجزائري تنظيمها للمرسوم التنفيذي رقم 16-134 المؤرخ في 25 أفريل 2016[1] وبناء على هذا المرسوم وطبقا لنص المواد 03 و04 فإنه توضع هذه المصالح تحت سلطة مدير عام الذي يتولى إعداد برامج نشاط السلطة وتقديم دفتر الشروط الذي يحدد كيفيات تأدية خدمات التصديق إ وتساعده في ذلك خلية للتدقيق تكلف بالتدقيق الداخلي للسلطات الثلاث، [2] وتتشكل هذه المصالح من دائرة تقنية تبدي رأيها في سياسات التصديق للسلطات الثلاث وفي دفتر الشروط وكل مسألة تتصل بالتصديق إ، [3] ودائرة أمن البنى التحتية والتي تتولى إعداد مشروع السياسة الأمنية للسلطات الثلاث وضمان اليقظة فيما يخص الأمن التنظيمي والتقني والمادي وأمن الأنظمة والشبكة المعلوماتية، [4] أما عن إدارة الشؤون القانونية فهي مسؤولة عن تنظيم الجوانب القانونية المتعلقة بتسيير هذه السلطة.[5]

ثانيا: دور السلطة الحكومية للتصديق الإلكتروني[6](AGCE)

نظم المشرع الجزائري هذه السلطة ضمن أحكام القانون رقم 04/15 سالف الذكر في المواد من 26 إلى المادة 28 منه، بموجب المادة 26 تنشأ لدى الوزير المكلف بالبريد وتكنولوجيات الإعلام والاتصال سلطة حكومية للتصديق الإلكتروني تتمتع بالاستقلال المالي والشخصية المعنوية، كما صدر بشأنها المرسوم التنفيذي رقم 16-135[7] الذي حدد طبيعة هذه السلطة وتشكيلتها وكيفيات سيرها، فطبقا للمادة 02 منه تدعى هذه السلطة بالسلطة الحكومية [8] ويقع مقرها بمدينة الجزائر[9]، يتولى إدارة هذه السلطة مدير عام ويزود بمجلس التوجيه وهياكل تقنية وإدارية حيث يتشكل هذا المجلس من المدير العام وممثل عن رئاسة الجمهورية وممثلين عن وزير الدفاع ووزير الداخلية ووزير العدل والمالية وكذا وزير تكنولوجيات الإعلام

[1] المرسوم التنفيذي رقم 16-134 المؤرخ في 17 رجب 1437 الموافق 25 أفريل 2016، يحدد تنظيم المصالح التقنية والإدارية للسلطة الوطنية للتصديق الإلكتروني وسيرها ومهامها، ج ر ج ج عدد 26، الصادرة بتاريخ 28 أفريل 2016.

[2] ينظر المادة 05 من المرسوم التنفيذي رقم 16-134 سالف الذكر.

[3] ينظر المادة 08 من المرسوم التنفيذي رقم 16-134 سالف الذكر.

[4] ينظر المادة 09 من المرسوم التنفيذي رقم 16-134 سالف الذكر.

[5] ينظر المادة 10 من المرسوم التنفيذي رقم 16-134 سالف الذكر.

[6] AGCE : Autorité Gouvernementale de Certification Électronique

لمزيد من التفاصيل يراجع الموقع الرسمي للسلطة الحكومية للتصديق الإلكتروني المتاح على الرابط التالي: https://agce.dz

[7] المرسوم التنفيذي رقم 16-135 المؤرخ في 17 رجب عام 1437 الموافق 25 أبريل 2016، يحدد طبيعة السلطة الحكومية للتصديق الإلكتروني وتشكيلها وتنظيمها وسيرها، ج ر ج ج عدد 26 الصادرة بتاريخ 28 أفريل 2016.

[8] ينظر المادة 02 من التنفيذي رقم 16-135 سالف الذكر.

[9] ينظر المادة 03 من التنفيذي رقم 16-135 سالف الذكر.

والاتصال،[1] ويساعد المدير العام في مهامه خلية تدقيق تتولى عملية التدقيق الداخلي للسلطة وأمانة تقنية[2] إضافة إلى هياكل تقنية وإدارية من بينها مديرية الأنظمة المعلوماتية وأمن البنى التحتية،[3] أما عن المشرع السعودي فقد استحدث مركز التصديق الحكومي[4] الذي يتولى مهام إصدار الشهادات الرقمية والخدمات الاستشارية، وكذا سلطة التصديق الحكومية المصرية التابعة لوزارة المالية والمسؤولة عن أعمال التوقيع والختم الإلكترونيين للموظفين والجهات الحكومية.[5]

تتولى السلطة الحكومية طبقا للمادة 28 من القانون 04/15 سالف الذكر متابعة ومراقبة نشاط التصديق الإلكتروني للأطراف الثالثة الموثوقة والتي يقصد بها في مفهوم هذا القانون كل شخص معنوي يقوم بمنح شهادات تصديق إلكتروني موصوفة أو خدمات لفائدة المتدخلين في الفرع الحكومي،[6] بحيث يقوم المدير العام للسلطة على إعداد برنامجها وتنفيذه، أما عن الهياكل التقنية والمديريات فإنها تقوم بمهام التدقيق في الشهادات الإلكترونية وضمان استغلال الأنظمة والشبكات الإلكترونية والمعلوماتية.[7]

ثالثا: دور السلطة الاقتصادية للتصديق الإلكتروني[8] (AECE)

عين القانون رقم 04/15 المتعلق بالتوقيع والتصديق الإلكترونيين سلطة ضبط البريد والاتصالات الإلكترونية بصفتها السلطة الاقتصادية للتصديق الإلكتروني، إذ نظمها وفقا لأحكام هذا القانون في المواد 29 و30 منه بحيث تكلف بمتابعة مؤديي خدمات التصديق الإلكتروني الذين يقدمون خدمات التوقيع والتصديق لصالح الجمهور،[9] والذي اختلفت جل التشريعات الدولية والداخلية على تسميتهم، حيث استخدم قانون الأونسيترال النموذجي المتعلق بالتوقيع الإلكتروني تسمية مقدم خدمات التصديق إ، أما عن المشرع الفرنسي استخدم مصطلح مزود خدمات التصديق إ، وعلى المستوى العربي فقد أطلق عليها

[1] ينظر المواد 04 و05 من المرسوم التنفيذي رقم 16-135 سالف الذكر.

[2] ينظر المادة 15 من المرسوم التنفيذي رقم 16-135 سالف الذكر.

[3] ينظر المادة 18 من المرسوم التنفيذي رقم 16-135 سالف الذكر.

[4] لمزيد من التفاصيل يراجع الموقع الرسمي للمركز الوطني للتصديق الرقمي السعودي، المتاح على الرابط التالي: https://www.ncdc.gov.sa/?page_id=1893 تاريخ الاطلاع: 2021/03/22 على الساعة 12:30

[5] لمزيد من التفاصيل يراجع الموقع الرسمي للسلطة الحكومية للتصديق الإلكتروني المصرية، المتاح على الرابط التالي: http://www.govca.gov.eg/services.php تاريخ الاطلاع: 2021/03/22 على الساعة 14:35

[6] ينظر المادة 02 فقرة 11 من القانون رقم 04/15 الذي يحدد القواعد المتعلقة بالبريد والاتصالات الإلكترونية، سالف الذكر.

[7] ينظر المواد من 16 إلى 26 من المرسوم التنفيذي رقم 16-135 سالف الذكر.

[8] AECE : Autorité Economique de Certification Électronique

لمزيد من التفاصيل يراجع الموقع الرسمي للسلطة الاقتصادية للتصديق الإلكتروني المتاح على الرابط التالي: www.aece.dz

[9] ينظر المواد 29 30 من القانون رقم 04/15 الذي يحدد القواعد المتعلقة بالبريد والاتصالات الإلكترونية، سالف الذكر.

المشرع المصري اسم جهات إصدار شهادة التصديق، أما عن المشرع الجزائري فقد اعتمد تسمية مؤدي خدمات التصديق الإلكتروني وعرفهم من خلال المادة 02 فقرة 12 من ذات القانون على أنهم أشخاص طبيعيين أو معنويين يقومون بمنح شهادات تصديق إلكتروني موصوفة أو خدمات أخرى في مجال التصديق الإلكتروني[1] وهم بذلك يختلفون عن الأشخاص الثالثة الموثوقة الذين توكل لهم أيضا مهمة خدمات التصديق إ لكن للهيئات العامة الحكومية فقط، كما يختلفون في أن مؤديي خدمات التصديق إ قد يكونون أشخاص طبيعية أو معنوية على غير الأشخاص الثالثة الموثوقة التي تكون دائما أشخاص معنوية لعل ذلك راجع لكون أنه ليس من السهل والمتاح للشخص الطبيعي أن يقوم بهذه الخدمات لكونها تحتاج إمكانيات مادية وبشرية وتقنية كبيرة لا يستطيع القيام بها إلا الشخص المعنوي.[2]

تقوم السلطة الاقتصادية بمنح هذه الفئات ما يسمى بالتراخيص لمباشرة نشاطهم بعد التحقق من مطابقة طلباتهم مع سياسة التصديق إ المعتمدة من طرف هذه السلطة، [3] كما فرض هذا القانون جملة من الشروط الواجب توافرها في مؤدي خدمات التصديق كأن يكون من جنسية جزائرية ويتمتع بقدرة مالية ومؤهلات وكذا خبرة في ميدان تكنولوجيات الاتصال وغيرها، [4] كما تقوم السلطة الوطنية في التشريع المغربي أيضا بتقديم اعتمادات لمقدمي خدمات التصديق لمزاولة نشاطهم، أما عن المشرع الفرنسي فيمكن مزودو هذه الخدمات من تقديم الشهادات دون ضرورة الحصول على ترخيص مسبق إعمالا لمبدأ حرية ممارسة نشاط التصديق الإلكتروني وهذا ما نجده في المادة 3 فقرة 1 من قانون التوجيه الأوروبي رقم 93-1999.

يرفق هذا الترخيص بدفتر شروط يحدد شروط وكيفيات تأدية خدمات التصديق إ ومنح شهادة التصديق الإلكتروني للمتعامل، هذه الشهادة التي تعتبر بمثابة الهوية الرقمية للشخص والتي عرفها المشرع الجزائري في المادة 02 فقرة 07 من القانون 04/15 والمشرع الفرنسي في المادة 01 فقرة 09 من المرسوم رقم 2001-272 المتعلق بالتوقيع الإلكتروني على أنها وثيقة إلكترونية تثبت الصلة بين بيانات التحقق من التوقيع الإلكتروني والموقع، [5] بحيث يصبح أمر التحقق منها متاح لجميع المتعاملين والمؤسسات في العالم

[1] ينظر المادة 2 فقرة 12 من نفس القانون.

[2] رضوان قرواش، هيئات التصديق في ظل القانون رقم 04/15 المتعلق بالقواعد العامة للتوقيع والتصديق الإلكترونيين(المفهوم والالتزامات)، مجلة العلوم الاجتماعية، العدد 24 جوان 2017، ص 413.

[3] ينظر المادة 33 من القانون رقم 04/15 الذي يحدد القواعد المتعلقة بالبريد والاتصالات الإلكترونية، سالف الذكر.

[4] ينظر المادة 34 من نفس القانون .

[5] Article n° 01 paragraphe 09 de décret n° 2001-272 du 30 mars 2001 pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique certificat électronique "

وهذا نتيجة الاعتراف الدولي لها والذي جاء متأخرا مقارنة مع دول أخرى حيث تم إطلاق العمل بخدمات التصديق الإلكتروني في 13 مارس 2021 للشروع في مهامها اعتبارا للأهمية البالغة التي تكتسيها عمليات التصديق الإلكتروني في إضفاء الحجية والرسمية للمحررات الإلكترونية.

كما يلتزم مؤدي الخدمة قبل منح شهادة التصديق من التحقق من تطابق المعلومات والبيانات التي تتضمنها الشهادة مع بيانات الموقع[1] حيث يكون مؤدي الخدمة هو المسئول عن الضرر الذي يلحق بأي هيئة أو شخص اعتمد على هذه الشهادة فيما يخص صحة المعلومات الواردة فيها، [2] ويجب على مؤدي خدمة التصديق إ الحفاظ على سرية هذه البيانات والمعلومات وعدم استعمالها إلا لأغراضها التي منحت من أجلها وهذا ما لا يتأتى إلا بوجود تقنيات تكنولوجية متطورة في حفظ البيانات وذلك من خلال تقنية التشفير المعتمدة من طرف هذه الهيئات كوسيلة تضمن سرية البيانات وعدم التعدي عليها، فنجد مثلا المشرع الفرنسي من خلال المادة 5 من المرسوم 535-2002 ألزم مقدمي الخدمات ضمان الأمان القانوني للمعلومات، [3] كذلك ما نصت عليه المادة 2 من اللائحة التنفيذية لقانون التوقيع الإلكتروني المصري بأن يحوز كل من يزاول تقديم خدمات التصديق إ على نظلم تأمين المعلومات وحماية البيانات، ولكن في حالة ما إذا قام مؤدي الخدمات بانتهاك سرية هذه البيانات أو التلاعب فيها بتزويرها وتغيير محتواها أو تزوير التوقيع الخاص به فإنه زيادة على العقوبات المالية والإدارية من غرامات وسحب ترخيص تطبق عليه عقوبة الحبس، كما يلتزم أيضا مقدم خدمات التصديق في حالة الخطأ في المعلومات التي تتضمنها الشهادة كأن يقوم بإعطاء شهادة غير الشهادة الخاصة بالشخص المعني مثلا لتشابه الأسماء، بتعليق العمل بها أو إلغائها نهائيا.[4]

أما في حالة المعلومات المزيفة فإن صاحب شهادة التصديق إ سواء كان شخصا معنويا أو طبيعيا فإنه هو الآخر مسئول عن ما يدلي به من معلومات حيث يعاقب بالحبس والغرامة في حالة إدلائه بإقرارات كاذبة

---

un document sous électronique attestant du lien entre les données de vérification de signature électronique et un signataire"

[1] ينظر المادة 44 من القانون 04/15 الذي يحدد القواعد المتعلقة بالبريد والاتصالات الإلكترونية سالف الذكر.

[2] ينظر المادة 53 من نفس القانون.

[3] Article 5 décret n° 2002-535 du 18 Avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produit et les systèmes des technologies de l'information : " L'agence nationale de la sécurité des systèmes d'information veille à la bonne exécution des travaux ou à obtenir des information sur leur déroulement"

[4] ينظر المادة 45 من القانون رقم 04/15 الذي يحدد القواعد المتعلقة بالبريد والاتصالات الإلكترونية، سالف الذكر.

للحصول على الشهادة أو استعماله بيانات مزيفة خاصة بالغير كأن ينتحل شخصية الغير مثلا، [1] كما تترتب في ذمته مسؤولية مدنية اتجاه مقدم الخدمات نتيجة المسؤولية العقدية التي أخل بها والتي قد ينجم عنها التشكيك في مصداقية مقدم الخدمات، ولهذا الأخير إلغاء الشهادة فور العلم بهذا التلاعب.

إلى جانب مقدمي خدمات التصديق الإلكتروني هناك نوع ثاني من مقدمي الخدمات سوف نتطرق إليهم بالتفصيل في النقطة الموالية.

الفرع الرابع: دور مقدمي خدمات الإنترنت في الوقاية من الجرائم الإلكترونية.

نظرا للتطور السريع في مجال تقنية المعلومات والاتصالات الإلكترونية والذي قد يؤدي إلى ظهور عدة أشخاص يقومون بأدوار ينطبق عليها وصف مقدمي خدمات الإنترنت، فإنه يصعب حصر الوسطاء بين المستخدم والشبكة إذ نجد على سبيل المثال: متعهدي الوصول، متعهدي الإيواء، ناقلي المعلومة، موردي المحتوى، مقدمي خدمة التصديق...الخ، ونظرا للتباين الموجود بين التشريعات المقارنة حول مفهوم مقدمي خدمات الإنترنت ودورهم في ضبط الجرائم الإلكترونية وجب أولا التعريف بهم قبل التطرق للدور الذي يضطلعون به.

أولا: التعريف بمقدمي خدمات الإنترنت

تطرقت العديد من التشريعات إلى تعريف مقدمي خدمات الإنترنت نجد من بينها القانون الفرنسي حول الثقة في الاقتصاد الرقمي في مادته 6-1/2 [2] والتوجيه الأوروبي حول التجارة الإلكترونية [3] في مادته 14 حيث عرفا مقدمي الخدمات على أنهم: "الأشخاص الطبيعيون أو المعنويون الذين يتولون ولو بالمجان تخزين البيانات والسجلات المعلوماتية لعملائهم، ويضعون تحت تصرفهم الوسائل التقنية والمعلوماتية التي تمكنهم من الوصول إلى هذا المخزون الإلكتروني على مدار الساعة"، كما عرفهم قانون تنظيم الاتصالات

[1] ينظر المواد 64 65 من القانون رقم 04/14 التي تنص على العقوبات المالية والإدارية المطبقة على مؤدي خدمات التصديق الإلكتروني، والمواد من 66 إلى المادة 75 منه والتي تنص على العقوبات الجزائية المطبقة على كل من مؤدي خدمات التصديق وصاحب شهادة التصديق في حالة ارتكاب بعض المخالفات التي تم ذكرها في المتن.

[2] Loi n° 2004/575 du 21juin 2004 sur la confiance dans l'économie numérique ;JO, 22 juin 2004 , p 11168.

[3] Directive n° 2000/ 31/CE du parlement européen et du Conseil du 08 juin 2000 relative a certains aspecte juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur.

المصري رقم 10 لسنة 2003 بأنهم: "أي شخص طبيعي أو اعتباري يستعمل خدمات الاتصال أو يستفيد منها ويقوم بتوفير أو تشغيل الاتصالات أيا كانت الوسيلة المستعملة"[1].

أما عن المشرع الجزائري فقد عرف مقدمي خدمات الإنترنت في القانون رقم 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، وذلك بموجب المادة الثانية منه بأنهم: "أي كيان عام أو خاص يقدم لمستعملي خدماته القدرة على الاتصال بواسطة منظومة معلوماتية و/أو نظام للاتصالات، وأي كيان آخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الاتصال المذكور أو لمستعمليها"[2]، وهو نفس التعريف الذي استمده المشرع من مضمون اتفاقية بودابست لمكافحة الجريمة الإلكترونية[3]، والذي تبناه في نص المادة 08 في فقرتها 8 من القانون 2000-03 سابق الذكر[4].

من خلال هذه التعريفات نستخلص أنه يوجد عدة فئات من مقدمي الخدمات كل له دور معين يقوم به في مجال تقديم هذه الخدمات، وبالرغم من هذا التعدد إلا أنه في مجال مكافحة الجرائم الإلكترونية والضبط الإداري في الفضاء الرقمي يتم التركيز على فئتين من مقدمي الخدمات وهما : مقدم خدمة الوصول للإنترنت، ومقدم خدمة الإيواء، وهذا ما نجد التأكيد عليه في العديد من التشريعات المقارنة من بينها التشريع الجزائري، [5] حيث خص المشرع الجزائري مقدمي خدمات الوصول للإنترنت بنظام قانوني خاص تمثل في المرسوم التنفيذي رقم 98-257 الذي يضبط شروط وكيفيات إقامة خدمات "أنترنات" واستغلالها، [6] ويكون مقدم خدمة الوصول شخصا طبيعيا أو معنويا دوره ربط مستخدمي الإنترنت بالشبكة وتمكينهم من الوصول إلى المواقع والحسابات التي يريدونها في أي مكان من العالم، أما عن الفئة الثانية أي مقدمي خدمة الإيواء فيقصد بهم حسب نص المادة 14 من التوجيه الأوروبي حول التجارة الإلكترونية والمادة 6-1/2 من القانون الفرنسي حول الثقة في الاقتصاد الرقمي كل شخص طبيعي أو

[1] عبد الفتاح محمد كيلاني، المسئولية المدنية الناشئة عن المعاملات الإلكترونية عبر الإنترنت، دار الجامعة الجديدة، مصر، 2011، ص 188.

[2] ينظر المادة 2 من القانون رقم 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها سالف الذكر.

[3] اتفاقية بودابست بشأن مكافحة الجريمة الإلكترونية المعتمدة من قبل لجنة وزراء مجلس أوروبا في دورتها التاسعة بعد المائة، بتاريخ 08 نوفمبر 2001 وتم التوقيع عليها في 23 نوفمبر 2001.

[4] عرفت المادة 08 فقرة 08 من القانون رقم 2000-03 الذي يحدد القواعد العامة المتعلقة بالبريد والمواصلات السلكية واللاسلكية، موفري الخدمات بأنهم:" كل شخص معنوي أو طبيعي يقدم خدمات مستعملا وسائل المواصلات السلكية واللاسلكية".

[5] بلخير محمد آيت عودية، الضبط الإداري للشبكات الاجتماعية الإلكترونية، المرجع السابق، ص 215.

[6] المرسوم التنفيذي رقم 98-257 الذي يضبط شروط وكيفيات إقامة خدمات "أنترنات" واستغلالها، سالف الذكر.

معنوي يهدف إلى تخزين مواقع إلكترونية وصفحات ويب على حساباته الآلية الخادمة بشكل مباشر ودائم مقابل أجر أو بالمجان، حيث يضع تحت تصرف عملائه الوسائل التقنية والمعلوماتية التي تمكنهم من بث ما يريدون على شبكة الإنترنت، وتربطه بعملائه رابطة تعاقدية يتم تنظيمها من خلال عقد خاص يسمى عقد الإيواء[1].

ثانيا: التزامات مقدمي خدمات الإنترنت ومسؤوليتهم عن الجرائم الالكترونية.

ألقت التشريعات المقارنة الدولية والداخلية عدة التزامات على عاتق مقدمي خدمات الإنترنت بمختلف فئاتهم، إذ تعد اتفاقية بودابست بشأن مكافحة الجريمة الإلكترونية لسنة 2001 من أولى هذه النصوص والتي اعتبرت دور مقدمي الخدمات من بين أهم الوسائل الإجرائية الوقائية من الجرائم الإلكترونية، كما نجد من بين التشريعات العربية التشريع المصري من خلال إصدار قانون مكافحة جرائم تقنية المعلومات الصادر برقم 157 لسنة 2018[2] والذي رتب التزامات عديدة على مقدمي الخدمات بصفة عامة، وبدوره المشرع الجزائري ألقى على عاتق مقدمي الخدمات بصفة عامة ومقدمي خدمات الإنترنت بصفة خاصة عدة التزامات تعتبر من بين وسائل الضبط الإداري الوقائي، وذلك بموجب المرسوم التنفيذي رقم 98-257 المتعلق بضبط شروط وكيفيات إقامة خدمات "أنترنات" واستغلالها[3]، وكذا القانون رقم 04/09 المشار إليهما سابقا[4]، فطبقا للمرسوم السابق يجب على مقدمي الخدمات تسهيل النفاذ إلى خدمات الإنترنت وذلك باستعمال أنجع الوسائل التقنية وتقديم المعلومات الواضحة والدقيقة حول موضوع النفاذ إليها لكافة المستخدمين[5]، إضافة إلى هذا فقد رتب القانون رقم 04/09 على عاتق هؤلاء التزاما بتقديم المساعدة للسلطات المكلفة بالتحري والتحقيق القضائي عن طريق جمع وتسجيل المعطيات المتعلقة بمحتوى الاتصالات التي يجريها المستخدمين، وهذا طبقا لما جاء في المادة 10 من ذات القانون.

وكوجه ثاني لهذه المساعدة ومن أجل تحديد هوية المستخدمين ومعرفة نشاطهم في البيئة الرقمية وضبطه، ألزم المشرع الجزائري مقدمي الخدمات بوضع المعطيات المجمعة تحت تصرف هذه السلطات

[1] ينظر المادة 14 من التوجيه الأوروبي والمادة 6-1/2 من القانون الفرنسي حول الثقة في الاقتصاد الرقمي والمذكورين سابقا.

[2] قانون رقم 185 لسنة 2018 بشأن مكافحة جرائم تقنية المعلومات، الجريدة الرسمية، العدد 32 (ج) الصادرة في 14 أغسطس 2018.

[3] المرسوم التنفيذي رقم 98-257 الذي يضبط شروط وكيفيات إقامة خدمات "أنترنات" واستغلالها، سالف الذكر.

[4] القانون رقم 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها سالف الذكر.

[5] ينظر المادة 14 من المرسوم التنفيذي رقم 98-257 الذي يضبط شروط وكيفيات إقامة خدمات "أنترنات" واستغلالها، سالف الذكر.

وذلك بعد التحفظ عليها[1]، إذ نصت المادة 11 من ذات القانون على نوعية المعطيات الواجب حفظها والمتمثلة في المعطيات التي تسمح بالتعرف على مستعملي الخدمة، والمعطيات المتعلقة بالتجهيزات الطرفية المستعملة للاتصال وكذا مكان ووقت الاتصال، المعطيات التي تسمح بالتعرف على المرسل إليه الاتصال وكذا عناوين المواقع المطلع عليها، بحيث تحدد مدة حفظ هذه المعطيات بسنة واحدة من تاريخ تسجيلها، وهو نفس الالتزام الذي جاءت به المادة 26 من القانون المتعلق بالتجارة الإلكترونية والتي ألزمت المورد الإلكتروني الذي يقوم بجمع المعطيات ذات الطابع الشخصي ويشكل ملفات الزبائن ألا يجمع إلا البيانات الضرورية لإبرام المعاملات التجارية، كما يجب عليه الحصول على موافقة المستهلكين قبل جمعها ويضمن سرية هذه الأخيرة، [2] كما تقوم المسؤولية الجزائية هنا في حالة عدم الالتزام بحفظ هذه المعطيات بما يسبب عرقلة في حسن سير التحريات القضائية، وأيضا في حالة تجاوز مدة الحفظ أو استعمال هذه المعطيات لغير الأغراض التي جمعت لأجلها، وهذا تحت طائلة العقوبات المنصوص عليها في المادة 11 من ذات القانون في فقرتها الأخيرة.[3]

كما أوجب المشرع مقدمي خدمات الإنترنت المحافظة على سرية المعلومات المتعلقة بالمستخدمين وعدم إفشائها إلا في الحالات المنصوص عليها قانونا[4]، وإلا ترتب على ذلك العقوبات المتعلقة بإفشاء السر المهني والمقررة في المواد 301 و303 مكرر 3 من قانون العقوبات الجزائري.[5]

إلى جانب هذه الالتزامات خص المشرع الجزائري مقدمي خدمات الإنترنت بالتزامين أوردهما بالذكر أولا في المرسوم التنفيذي رقم 98-257 سالف الذكر في المادة 14 منه، وثانيا في القانون رقم 04/09 في المادة 12 منه، حيث ألزم هذه الفئة بالتدخل الفوري لسحب المحتويات التي يتيحون الاطلاع عليها متى كانت مخالفة للنظام العام، بحكم أنهم هم من يمتلكون القدرة على السيطرة على منافذ الإنترنت، كما ألزمهم بوضع ترتيبات تقنية تسمح بحصر إمكانية الدخول إلى الموزعات التي تحوي مواد مخالفة للنظام العام

[1] ينظر المادة 10 من القانون رقم 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها سالف الذكر.

[2] حدة بوخلفة، المسؤولية الجنائية لمقدمي خدمات الإنترنت، دار هومه للطباعة والنشر، الجزائر، ديسمبر 2019، ص 50.

[3] ينظر المادة 11 من القانون رقم 04/09 سالف الذكر.

[4] ينظر المادة 10 فقرة 2 من نفس القانون.

[5] ينظر المواد من 301 إلى 303 مكرر 3 من القانون رقم 04- 15 المؤرخ في 27 رمضان عام 1425 الموافق 10 نوفمبر 2004، المعدل والمتمم للأمر رقم 66- 156 المؤرخ في 18 صفر عام 1386 الموافق 08 يونيو سنة 1966، المتضمن قانون العقوبات، ج ر ج ج عدد 71 الصادرة بتاريخ 10 نوفمبر 2004، والتي تبين العقوبات المقررة على كل من يفشي أسرار المهنة.

والآداب العامة وإخبار المشتركين بوجودها، [1] ونفس الشيء نجده في المرسوم 98-257 إذ حمل مقدمي الخدمات مسؤولية محتوى الصفحات التي يستخرجونها أو يقومون بإيوائها، كما أناط بهم واجب اتخاذ كل الإجراءات لتأمين مضمون هذه الموزعات قصد منع النفاذ إليها متى كانت تتعارض مع متطلبات النظام العام والقانون، وبالتالي يقع على كل مقدم خدمة عدم الاكتفاء بتوفير خدمة النفاذ للإنترنت فحسب، بل لابد من إعداد نظام بحث آلي قادر على التقاط كل محتوى غير مشروع واستبعاده[2]، وهو ما قرره التوجيه الأوروبي المتعلق بالتجارة الإلكترونية إذ ألزم مقدمي الخدمات أن يضعوا برامج لتصفية المحتويات التي يبثونها، ومن جهته نصت المادة 6 من القانون الفرنسي حول الثقة في الاقتصاد الرقمي أنه على مقدمي خدمات الإنترنت الإلتزام بتوعية المستخدمين بوجود برامج لتصفية المحتوى وتوفير واحد على الأقل على صفحات الويب، كما دعت لضرورة كشف مقدم الخدمة عن إسمه وإسم الشركة وعنوانها لسهولة الاتصال به عند حصول أي مخالفة للإبلاغ عن ذلك.[3]

أما عن مسؤوليتهم اتجاه ما يتيحونه من معلومات فقد ثار بشأنها اختلاف فقهي وقانوني كبير، إذ أن الدور التقني والفني الذي يقوم به كل من مقدم خدمة الوصول والإيواء وناقل المعلومة يجعله يتسم بالحياد إذ لا يكون محل مساءلة قانونية لأنه لا علاقة له بالمحتوى غير المشروع الذي تم بثه، على العكس تقوم مسؤولية كل من مقدمي خدمات الانترنت المعلوماتية كالناشر والمؤلف والمنتج لأنهم على اطلاع دائم بما ينشر عبر الشبكة، وفي هذه الحالة نستنتج أنه يكون مقدم خدمات الإنترنت مسئولا عن المحتوى غير المشروع إذا كان على علم بوجوده ولم يتدخل لسحبه وهو ما أكد عليه كل من التوجيه الأوروبي المتعلق بالتجارة الإلكترونية وكذا القانون الفرنسي حول الثقة في الاقتصاد الرقمي في المادة 6 فقرة 1 منه، وكذا القانون الأمريكي المتضمن حقوق الطبع والنشر الرقمية للألفية، [4] والذي تناول الاعتداءات على حقوق الملكية الفكرية، بموجب الباب الثاني منه الذي تناول مسؤولية مقدمي الخدمات حيث اشترط لقيام مسؤوليتهم علمهم بعدم مشروعية المحتوى المعلوماتي، وعدم شطبهم لهذا المحتوى غير المشروع.[5]

[1] ينظر المادة 12 من القانون رقم 04/09 سالف الذكر.

[2] بلخير محمد آيت عودية، الضبط الإداري للشبكات الاجتماعية الإلكترونية، المرجع السابق، ص 224.

[3] حدة بوخلفة، المسؤولية الجنائية لمقدمي خدمات الإنترنت، المرجع السابق، ص 46.

[4] القانون الأمريكي رقم 304- 105 الصادر في 28 أكتوبر 1998، المتضمن حقوق الطبع والنشر الرقمية للألفية.

[5] حدة بوخلفة، المسؤولية الجنائية لمقدمي خدمات الإنترنت، المرجع السابق، ص 45- 46.

المطلب الثاني: دور الهيئات الوطنية لأمن الأنظمة المعلوماتية في الوقاية من الجرائم الإلكترونية.

استحدثت التشريعات الدولية والعربية هيئات وطنية ضمن قوانينها الإجرائية الخاصة بالوقاية والتصدي للجرائم الإلكترونية، تتمتع بسلطات الضبط الإداري الإلكتروني، مهمتها تأمين الأنظمة المعلوماتية بما يضمن قلة الانتهاكات والاعتداءات التي تحدث في البيئة الرقمية والعالم السيبراني، وعليه سوف نتعرض فيما يلي لهذه الهيئات بالتفصيل محاولين في ذلك إبراز الدور الوقائي لها في التصدي لهذا النوع من الإجرام.

الفرع الأول: دور الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال

أنشأت أغلب تشريعات الدول هيئات تتولى مهمة الوقاية من الهجمات الإلكترونية التي قد تتعرض لها سلطات كل دولة، فقد قام المشرع الجزائري بإنشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها بموجب المادة 13 من القانون رقم 04/09 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، والتي تنص : " تنشأ هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.تحدد تشكيلة الهيئة وتنظيمها وكيفيات سيرها عن طريق التنظيم"، والتي يقابلها في التشريع المقارن المكتب المركزي لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال[1] (OCLTIC) والذي أنشأ في فرنسا بموجب المرسوم رقم 2000-405 المؤرخ في 15 ماي 2000، [2] بحيث تهدف هذه الهيئات إلى تنسيق عمليات الوقاية ومكافحة الجرائم الإلكترونية بين كل القطاعات والسلطات المختصة في هذا المجال، تحدد تشكيلة ومهام وكيفيات سير هذه الهيئات عن طريق التنظيم، لذا سوف نتطرق بالتفصيل فيما يأتي لكل من تشكيلة الهيئة وكيفية سيرها (أولا) ثم إلى تعداد مهامها (ثانيا):

أولا: تشكيل الهيئة وكيفية سيرها

لم ينص القانون رقم 04/09 على تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وإنما أحال ذلك للتنظيم، حيث أصدر رئيس الجمهورية مرسوما رئاسيا خاصا المرسوم

[1] OCLCTIC : Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication, Disponible sur le lien suivant : https://www.police-nationale.interieur.gouv.fr/Actualites/L-actu-police/Plateforme-Signalement-sur-Internet/Decouvrez-l-OCLCTIC.

[2] Décret n°2000-405 du 15 mai 2000, portant création d'un office central de lutte contre la criminalité liée aux technologies de l'information et de la communication.

رقم 15/ 261 المؤرخ في 10/08/2015[1] والذي ألغي عن طريق إصدار عدة مراسيم بعده والتي كان آخرها المرسوم الرئاسي رقم 439/21 المؤرخ في 2021/11/07 الذي يتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، [2] نصت المادة 02 من المرسوم الرئاسي رقم 439/21 سالف الذكر أن الهيئة سلطة إدارية مستقلة تتمتع بالشخصية المعنوية والاستقلال المالي، تدعى "الهيئة" توضع تحت سلطة رئيس الجمهورية بعدما كانت تحت سلطة وزير الدفاع الوطني ووزير العدل حسب المراسيم السابقة، ويحدد مقرها بمدينة الجزائر كما يمكن نقله لأي مكان آخر من التراب الوطني بموجب مرسوم من رئيس الجمهورية، [3] أما عن المكتب المركزي لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال فهو هيكل مشترك بين كل الوزارات بالرغم أنه موضوع تحت سلطة وزارة الداخلية، حيث يضم كل من وزارة الدفاع ووزارة الاقتصاد ووزارة المالية، وهو بذلك يضم تشكيلة كبيرة من الشرطة القضائية والدرك الوطني والجمارك طبقا لنص المادة 01 من المرسوم 2000-405 سالف الذكر.

وتضم تشكيلة الهيئة وفقا للمرسوم رقم 439/21 مجلس توجيه ومديرية عامة تتفرع عنها عدة مصالح أخرى، [4] يعتبر مجلس التوجيه الجهاز الأعلى على مستوى الهيئة يرأسه الأمين العام لرئاسة الجمهورية، كما يتولى المدير العام أمانة المجلس، [5] حيث نرى أن المشرع أعاد تنظيم تشكيلة المجلس من خلال إضافة عدة أعضاء من بينهم الأمين العام لوزارة الشؤون الخارجية والجالية الوطنية بالخارج، المدير المركزي لأمن الجيش لأركان الجيش الوطني الشعبي، رئيس مصلحة الدفاع السيبراني ومراقبة أمن أنظمة التابع لأركان الجيش الوطني وغيرهم، فمن خلال هذه التشكيلة نرى اختلاف كبير في عضوية الهيئة بين ما جاء في

---

[1] المرسوم الرئاسي رقم 15-261 المؤرخ في 2015/10/08، الذي يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، المشار إليه سابقا.

[2] حيث ألغي المرسوم الرئاسي رقم 261/15 سالف الذكر بالمرسوم الرئاسي رقم 19- 172 المؤرخ في 03 شوال عام 1440 الموافق 2019/06/06، الذي يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج ر ج ج عدد 37 الصادرة في 09 يونيو 2019، والذي ألغي بالمرسوم رقم 183/20 المؤرخ في 21 ذي القعدة عام 1441 الموافق 13 يوليو سنة 2020، يتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج ر ج ج عدد 40، الصادرة في 18 يوليو 2020، والذي ألغي بالمرسوم الرئاسي رقم 439/21 المؤرخ في 02 ربيع الثاني عام 1443 الموافق 07 نوفمبر سنة 2021، المتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج ر ج ج عدد 86، الصادرة في 11 نوفمبر 2021.

[3] ينظر المواد 01 02 و03 من المرسوم الرئاسي رقم 439/21 سالف الذكر.

[4] تنص المادة 05 من المرسوم رقم 439/21 على: " تتكون الهيئة من مجلس توجيه ومديرية عامة يوضعان تحت سلطة رئيس الجمهورية، ويقدمان له عرضا عن نشاطاتهما".

[5] ينظر الفقرة الأخيرة من المادة 06 من نفس المرسوم.

المرسومين السابقين، وهذا يعد تداركا من المشرع الجزائري ونقطة تحسب له، فكلما كان أعضاء الهيئة من مختلف المجالات تنوعت بذلك المهام وزادت السيطرة على تفشي الهجمات الإلكترونية في مختلف المجالات، إلا أننا نجد غياب لبعض الأطراف الفاعلة والتي كان من اللازم ضمها للهيئة من بينها ممثل عن وزارة المالية المكلف بالاقتصاد الرقمي الذي أصبح مستهدفا كثيرا في الآونة الأخيرة، بما يتعرض له من جرائم ومهددات تنقص من تطوره وتأثر على عجلة التنمية الوطنية، ولهذا يكون دور ممثل وزارة المالية والاقتصاد وقائيا بامتياز لتفادي هذه الهجمات والتصدي لها من خلال هذه الهيئة.

وفقا للمرسوم القديم 15-261 كانت تضم تشكيلة الهيئة إلى جانب اللجنة المديرة عدة مديريات من بينها مديرية عامة كان يديرها مدير عام يعين بموجب مرسوم رئاسي يتولى السهر على حسن سير الهيئة وتنفيذ برامجها، وهذا ما أبقى عليه المشرع في المرسوم الجديد رقم 439/21 إذ صنف وظيفة المدير العام على أنها وظيفة عليا في الدولة، [1] إلى جانب مديرية المراقبة الوقائية واليقظة الإلكترونية، مديرية التنسيق التقني، مركز للعمليات التقنية، ملحقات جهوية أخرى لم يعرفها القانون ولم يحدد تشكيلتها بل اكتفى بتعداد مهامها في مجال الوقاية من الجرائم الإلكترونية، أما عن تشكيلة المرسوم الجديد فقد أبقت على جهاز المديرية العامة في المادة 09 منه إذ تضطلع المديرية بالسهر على حسن سير الهيئة وإعداد مشروع ميزانيتها وتنشيط أعمال المراقبة والوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، وهي بذلك لها نفس المهام الموكلة للمديرية السابقة، [2] إلى جانب هذا تضم المديرية العامة وفقا للمرسوم الأخير عدة مديريات فرعية تتمثل في كل من مديرية المراقبة الوقائية واليقظة الإلكترونية، مديرية الإدارة والوسائل، مصلحة للدراسات والتلخيص، مصلحة للتعاون واليقظة التكنولوجية، إضافة إلى ملحقات جهوية أخرى، [3] حيث تعد وظائفهم وظائف عليا في الدولة، [4] كما أضاف المرسوم الأخير شرط أداء اليمين بالنسبة لمستخدمي الهيئة من ضباط وأعوان والذين يسمح لهم بالاطلاع على المعلومات السرية المتعلقة بعمليات المراقبة والوقاية وذلك أمام المجلس القضائي المختص إقليميا قبل تنصيبهم في مهامهم داخل الهيئة وفقا للمادة 22 من هذا المرسوم.

[1] ينظر المادة 09 من المرسومين رقم 15-261 والمرسوم رقم 439/21 سالفي الذكر.

[2] ينظر المادة 09 من المرسوم الرئاسي رقم 19-172 وكذا المرسوم الرئاسي رقم 439/21 سالف الذكر.

[3] ينظر المادة 11 من المرسوم الرئاسي رقم 439/21 سالف الذكر.

[4] ينظر المادة 12 من نفس المرسوم

ثانيا: مهام الهيئة

بالرجوع للقانون رقم 04/09 المتضمن القواعد العامة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال نجد أن المشرع قد عدد مهام وصلاحيات الهيئة الوطنية للوقاية من هذه الجرائم في المادة 14 منه والتي تقابلها المادة 03 من المرسوم رقم 2000-405 الفرنسي حيث تتولى هذه الهيئات خصوصا تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم الإلكترونية بما في ذلك تجميع المعلومات وإنجاز الخبرات القضائية، تبادل المعلومات مع نظيراتها في الخارج قصد جمع كل المعطيات المفيدة في التعرف على مرتكبي هذا النوع من الجرائم وتحديد مكان تواجدهم، [1] وكذا تكوين الضباط والقضاة في هذا المجال إلى جانب القيام بحملات التوعية والتحسيس بمخاطر هذه الجرائم.[2]

بالرجوع لأحكام المادة 07 من المرسوم الرئاسي 439/21 والتي تبين المهام الموكلة لمجلس التوجيه فإنه يتولى هذا الجهاز على الخصوص عملية التداول حول الإستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، لاسيما توافر شروط اللجوء للمراقبة الوقائية للاتصالات الإلكترونية، والقيام دوريا بتقييم حالة التهديد في مجال الجرائم الإلكترونية للتمكن من تحديد مضامين عمليات المراقبة الواجب القيام بها والأهداف المنشودة بدقة، وغيرها من المهام الإدارية الأخرى.[3]

أما بالنسبة للمهام التي أوكلت للجهاز الثاني من الهيئة ألا وهو المديرية العامة فحسب المادة 10 من المرسوم الرئاسي رقم 439/21 [4] تتولى هذه الهيئة عدة صلاحيات تتمثل أساسا في السهر على حسن سير الهيئة، وتنشيط وتنسيق عمليات الوقاية من الجرائم الإلكترونية، وتبادل المعلومات مع مثيلاتها الأجنبية بغرض تجميع كل المعطيات المتعلقة بتحديد مكان مرتكبي هذه الجرائم والتعرف عليهم، وكذا تمثيل الهيئة لدى السلطات الوطنية والدولية والقضاء، كما تتولى القيام بإجراءات التأهيل وأداء اليمين فيما يخص المستخدمين المعنيين في الهيئة، كما يلتزم المدير العام للهيئة بإخطار رئيس الجمهورية فورا عن كل

[1] ينظر المادة 14 من القانون رقم 04/09 المتضمن القواعد العامة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال سالف الذكر.

[2] Art n° 03 du décret n° 2000-405 précédent.

[3] ينظر المادة 07 من نفس المرسوم الرئاسي رقم 439/21 سالف الذكر.

[4] ينظر المادة 10 من نفس المرسوم.

حادثة من شأنها المساس بأمن الدولة أو المرتبطة بالأعمال الإرهابية أو التخريبية، والملاحظ من هذه المادة أنها وسعت من اختصاصات المديرية العامة وأعطت لها صلاحيات كثيرة في مواجهة أي تهديد إلكتروني.

يعتبر جهاز مديرية المراقبة الوقائية واليقظة الإلكترونية من بين المديريات التي تتفرع عن المديرية العامة للهيئة وفقا لأحكام المرسوم الرئاسي رقم 439/21 حيث كان يقابلها في المرسوم القديم المديرية التقنية وبالرجوع للمادة 14 من المرسوم الجديد والتي تقابلها المواد 11 و12 و13 و14 من المرسوم القديم [1]نجد أن المديرية التقنية تكلف بمهمة المراقبة الوقائية للاتصالات الإلكترونية في إطار الوقاية من الجرائم الموصوفة بالأفعال الإرهابية والتخريبية والاعتداء على أمن الدولة وهي ذات المهام التي أوكلت لمديرية المراقبة الوقائية وفقا للمرسوم الأخير. حيث تتولى أيضا مهمة جمع واستغلال كل المعلومات التي تسمح بالكشف عن الجرائم الإلكترونية، وتزويد السلطات القضائية ومصالح الشرطة القضائية بناء على طلبها بالمعلومات والمعطيات المتعلقة بهاته الجرائم، وكذا تنفيذ طلبات المساعدة القضائية الأجنبية و تبادل الخبرات القضائية في إطار مكافحة هذا النوع من الإجرام الذي يتطلب اللجوء إلى أساليب التحري الخاصة، بما أن طبيعة هذه الجرائم تحتاج حتما إلى أشخاص تقنيين لهم من الكفاءة والخبرة بما يساعد السلطات في مكافحة هذه الجرائم، وتوفير الموارد البشرية المتخصصة وتسييرها لتنفيذ عمليات المراقبة الإلكترونية.[2] وجمع وتسجيل وحفظ المعلومات الرقمية وتحديد مصدرها من خلال القيام بعمليات تفتيش المنظومة المعلوماتية ومراقبة الاتصالات الإلكترونية وحجز كل الأدلة الرقمية المتحصل عليها وتقديمها للسلطات المختصة من أجل مباشرة الإجراءات القضائية اللازمة، فهي بذلك تعتبر الجهاز الذي يتولى متابعة الجرائم الإلكترونية ومراقبة أنشطة المجرم داخل العالم الافتراضي، فهي بذلك تتولى الدور الوقائي الذي يكون قبل ارتكاب السلوك والدور الردعي من خلال تسهيل الإجراءات وتبادلها مع السلطات المختصة كقناة اتصال بينهم، شرط أن يكون ذلك بناء على إذن من السلطة القضائية المختصة.[3]

إضافة لما سبق يتيح المكتب المركزي الفرنسي (OCLTIC) منصة للإبلاغ عن المحتوى غير القانوني عبر الإنترنت[4] والتي تهدف إلى تزويد مستخدمي الإنترنت بنموذج إبلاغ للقيام بملئه وإرساله عبر المنصة ليقوم

[1] ينظر المواد 11 12 13 14 من المرسوم رقم 15-261 والتي تقابلها المواد 11 و12 من المرسوم رقم 19-172 سالف الذكر.

[2] يقصد بعمليات المراقبة الإلكترونية كل من مراقبة الاتصالات وتجميعها وإجراء التفتيش المعلوماتي وحجز المعطيات المتحصل عليها والتي نص عليها القانون رقم 04/09 سالف الذكر في المادة 03 منه والتي حصر المشرع مجالات اللجوء إليها بحيث يتم القيام بها إما لحماية النظام العام أو لمستلزمات التحريات والتحقيقات القضائية الجارية.

[3] تحدد المادة 14 من المرسوم الرئاسي 439/21 المهام الموكلة لجهاز مديرية المراقبة الوقائية واليقظة الإلكترونية.

[4] Voir la plateforme de signalement sur le lien suivant : www.internet.signalement.gouv.fr

المكتب بالنظر فيه وتدقيق المعلومات التي يحتويها وتوجيهها إلى السلطات المختصة بالتحقيق فيها سواء على المستوى الوطني أو الدولي، وهو بذلك يعتبر نقطة الاتصال المركزية في التبادلات الدولية من خلال وسيط المكتب المركزي الوطني للإنتربول، ووحدة التنبيه الوطنية للأوروبول، ونقطة اتصال لجميع الدول التي وقعت على اتفاقية مكافحة الجرائم الإلكترونية والتي من بينها الجزائر.[1]

مما سبق التطرق إليه يمكن القول أنه بالرغم من أن الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال هي هيئة إدارية مستقلة تتمتع بالشخصية المعنوية والاستقلال المالي والإداري والتي تعتبر من هيئات الإدارة التابعة للدولة وليس للسلطة القضائية، إلا أن هذا لا يمنع من وجود تنسيق دائم وتعاون بينها وبين السلطات القضائية وأجهزة الضبط القضائي، فقد حرص المشرع الجزائري على هذا التعاون لضمان فعالية التدخلات التي تحتاجها الهيئة في مكافحة هذا النوع من الجرائم وهذا ما يظهر من خلال المهام التي توكل إليها من مساعدة السلطات القضائية وتزويدها بالمعلومات الضرورية، والسهر على تنفيذ طلبات المساعدة القضائية الدولية وتبادل المعلومات والإجراءات على المستوى الوطني والدولي، [2] حيث استحدث المشرع الجزائري بموجب المادة 18 من المرسوم 439/21 مصلحة للتعاون واليقظة التكنولوجية التي تتولى تنسيق التعاون بين السلطات فيما يخص تنفيذ عمليات الوقاية من هذه الجرائم، وباعتبار أن دور الهيئات الإدارية في مجال الضبط الإداري يعتبر دورا وقائيا يهدف إلى وضع إجراءات استباقية تمنع وقوع الجريمة فإنه بالرجوع لمهام الهيئة دائما نجد أن هدفها الأساسي يتمحور حول الوقاية من هذه الجرائم وهو ما يظهر من خلال إعدادها للإستراتيجية الوطنية للوقاية من الجرائم الإلكترونية وضمان المراقبة الوقائية الفعالة للاتصالات الإلكترونية قصد كشف مختلف التهديدات قبل وقوعها أو أثناء ذلك للتخفيف من حدتها ومنع تفاقمها، كما يتضح دور هذه الهيئة في مجال ضبط هذه الجرائم من خلال ما تقوم به المديرية التقنية من عمليات المراقبة كما سبق ذكرها، وكذا من خلال عمليات التوعية حول استعمال تكنولوجيات الاتصال والمخاطر المتصلة بها.

الفرع الثاني: دور السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي في الوقاية من الجرائم الإلكترونية.

[1] Voir le point de contact sur le lien suivant ; www.pointdecontact.net

[2] ينظر المادة 18 من المرسوم الرئاسي 439/21، والمادة 07 من المرسوم رقم 2000-405 الفرنسي سالفي الذكر.

نظرا لتأثير التطور السريع في مجال تكنولوجيات الإعلام والاتصال على خصوصية البيانات والمعطيات الشخصية للأفراد[1] اتسعت دائرة الاعتداء على حق الأفراد في الحياة الخاصة، إذ أن المعلومات المتعلقة بجميع جوانب حياة الفرد الشخصية يمكن جمعها وتخزينها لفترة غير محدودة من الزمن هذا ما يشكل تهديدا لهذه الخصوصية، ولهذه الأسباب أصبحت حمية المعطيات الشخصية والمعالجة الكترونيا تحظى بأهمية كبيرة على المستوى الدولي حيث كرس الإعلان العالمي لحقوق الإنسان[2] وكذا الاتفاقية الدولية للحقوق المدنية والسياسية لسنة 1966 [3] هذا الحق، كما قدم الاتحاد الأوروبي عدة أدلة توجيهية حول حماية البيانات أبرزها دليل عام 1995 بشأن حماية الأفراد فيما يتصل بمعالجة البيانات الشخصية وحرية نقلها، [4] أما على مستوى التشريعات فتعتبر دولة السويد سباقة في تبني إطار حمائي من خلال إصدار قانون حماية المعطيات سنة 1973، ثم الولايات المتحدة الأمريكية من خلال سنها العديد من القوانين لحماية المعطيات الشخصية من بينها قانون الخصوصية الفيدرالي لسنة 1974[5]، وكذا فرنسا من خلال قانون رقم 77-78 الذي عدل بالقانون رقم 2004-801 لسنة 2004، [6] حيث أنشأ هذا القانون هيئة مستقلة تسهر على حسن تطبيقه وهي اللجنة الوطنية للمعلوماتية والحريات (CNIL)والتي تقوم بتنظيم عمليات معالجة البيانات الشخصية وتسجيلها وتخزينها وتقدم تراخيص لكل من يرغب في معالجة

[1] عملت جل التشريعات المقارنة على تعريف المعطيات ذات الطابع الشخصي حيث عرفتها الاتفاقية الأوروبية رقم 108 الصادرة عن مجلس أوروبا للبيانات الخاصة وكذا التوجيه الأوروبي رقم 46/95 الصادر بتاريخ 1995/10/24 في مادتهما 02 على أنها كل المعلومات المتعلقة بشخص طبيعي معرف أو قابل للتعرف عليه، وبنفس المعنى عرفها التشريع الفرنسي في المادة 02 من قانون 06 يناير 1978 المتعلق بالمعلومات والحريات، وأما بالنسبة لبعض التشريعات العربية فقد عرفها التشريع الجزائري في المادة 03 من القانون رقم 07/18 على أنها كل معلومة بغض النظر عن دعامتها متعلقة بشخص معرف أو قابل للتعرف عليه والمشار إليه أدناه "الشخص المعنوي" بصفة مباشرة أو غير مباشرة، لاسيما بالرجوع إلى رقم التعريف أو عنصر أو عدة عناصر خاصة بهويته البدنية أو الفيزيولوجية أو الجينية أو البيومترية أو النفسية أو الاقتصادية أو الثقافية أو الاجتماعية، والملاحظ أن جل التعريفات متقاربة إلى حد كبير.

[2] تنص المادة 02 من الإعلان العالمي لحقوق الإنسان المعتمد من طرف قرار الجمعية العامة 217 ألف (د-3) المؤرخ في 10 ديسمبر 1948 على: "لا يجوز تعريض أحد لتدخل تعسفي في حياته الخاصة أو في شؤون أسرته او مسكنه او مراسلاته أو لحملات تمس شرفه وسمعته ولكل شخص الحق في أن يحميه القانون من مثل هذا التدخل أو تلك الحملات".

ينظر الملحق رقم 09.

[3] الاتفاقية الدولية للحقوق المدنية والسياسية المعتمدة بموجب قرار الجمعية العامة للأمم المتحدة 2200 ألف (د-21) المؤرخ في 16 ديسمبر 1966، وبدأ العمل بها في 23 مارس 1976.

[4] يراجع الدليل الأوروبي الصادر في 24 نوفمبر 1995 المعتمد من طرف الجمعية العامة للاتحاد الأوروبي بشأن حماية الأفراد فيما يتصل بمعالجة البيانات الشخصية وحرية نقلها.

[5] القانون رقم 579/93 الصادر سنة 1974 المسمى بقانون الخصوصية الأمريكي، الذي ينظم جمع ومعالجة وتخزين وتشغيل واستخدام البيانات الشخصية في القطاع العام.

[6] Loi n° 2004-801 du 06 Aout 2004 relative à la protection des personnes physique a l'égard des traitements de donnée à caractère personnel et modifiant la loi n° 78-17 du 06 janvier 1978 relative à l'informatique aux fichiers et aux libertés.

هذه البيانات كما تفرض عقوبات معينة على كل من يخالف هذه القواعد، أما على المستوى العربي وضعت تونس نظام حماية ملائم لقواعد التوجيه الأوروبي من خلال القانون رقم 63-2004 المتعلق بحماية المعطيات ذات الطابع الشخصي بتاريخ 27 يوليو 2004، [1] كما سارع المشرع المغربي لمواكبة هذه التوجهات من خلال سنه القانون رقم 08-09 بتاريخ 18 فبراير 2009 المتعلق بحماية الأشخاص الذاتيين اتجاه معالجة المعطيات ذات الطابع الشخصي والذي أحدث لجنة وطنية لمراقبة حماية المعطيات الشخصية.[2]

أما بالنسبة للمشرع الجزائري وعلى غرار هذه التشريعات أولى أهمية كبيرة للحياة الخاصة للأفراد لاسيما المعطيات الشخصية وذلك من خلال المادة 47 من الدستور الجزائري[3] وكذا القانون رقم 18-07 المؤرخ في 10 جوان 2018[4] المتعلق بحماية الأشخاص الطبيعيين في مجال المعطيات ذات الطابع الشخصي والذي ضم من خلاله عدة آليات لضبط الممارسات المنافية لاحترام الحياة الخاصة للأفراد من خلال إنشاء سلطة إدارية مستقلة أسندت إليها مهمة معالجة وحماية هذه المعطيات، فيما يلي سوف نتطرق بالتفصيل لتنظيم ودور هذه الهيئة في الوقاية من الجرائم الإلكترونية.

أولا: التعريف بالسلطة

تعد الهيئة الوطنية لحماية المعطيات ذات الطابع الشخصي سلطة إدارية مستقلة تتمتع بالشخصية المعنوية والاستقلال المالي والإداري تحدث لدى رئيس الجمهورية ويحدد مقرها بالجزائر العاصمة، [5] تتكون هذه السلطة من ستة عشرة (16) عضوا يعينون حسب اختصاصهم القانوني والتقني في مجال معالجة المعطيات الشخصية بموجب مرسوم رئاسي لمدة خمسة (5) سنوات قابلة للتجديد، حيث تضم هذه التشكيلة ثلاثة شخصيات من بينهم الرئيس وثلاثة قضاة يقترحون من قبل المجلس الأعلى للقضاء من بين قضاة المحكمة العليا ومجلس الدولة، وعضو من كل غرفة من البرلمان يتم اختياره من قبل رئيس كل

[1] القانون الأساسي عدد 63 لسنة 2004 المتعلق بحماية المعطيات الشخصية المعدل بالقانون الأساسي عدد 25 لسنة 2018.

[2] ظهير شريف رقم 15-09-1 صادر في 22 صفر 1430 الموافق 18 فبراير 2009 بتنفيذ القانون رقم 09-08 المتعلق بحماية الأشخاص الذاتيين تجاه المعطيات ذات الطابع الشخصي، ج ر عدد 5711 بتاريخ 27 صفر 1430 الموافق 23 فبراير 2009.

[3] تنص المادة 47 من الدستور الجزائري لسنة 2020 على: "لكل شخص الحق في حماية حياته الخاصة وشرفه. لكل شخص الحق في سرية مراسلاته واتصالاته الخاصة في أي شكل كانت. لا مساس بالحقوق المذكورة في الفقرتين الأولى والثانية إلا بأمر معلل من السلطة القضائية. حماية الأشخاص عند معالجة المعطيات ذات الطابع الشخصي حق أساسي. يعاقب القانون على كل انتهاك لهذه الحقوق."

[4] القانون رقم 18-07 المؤرخ في 10 جوان 2018 ، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، ج ر ج ج عدد 34 الصادرة بتاريخ 10 جوان 2018.

[5] ينظر المادة 23 من القانون رقم 18-07 سالف الذكر.

غرفة، ممثل عن المجلس الوطني لحقوق الانسان، ممثل عن وزير الدفاع الوطني، ممثل عن وزير العدل، ممثل عن الوزير المكلف بالبريد والمواصلات السلكية واللاسلكية...وغيرهم، كما يمكن للسلطة الاستعانة بأي شخص مؤهل لمساعدتها في أعمالها، إلى جانب هذا تزود السلطة بأمانة تنفيذية يساعدها في تأدية مهامها مجموعة من المستخدمين،[1] أما عن اللجنة الوطنية لمراقبة حماية المعطيات ذات الطابع الشخصي التي أحدثها المشرع المغربي بموجب القانون رقم 09-08 فتوضع لدى رئيس الحكومة وتتألف من رئيس يعينه الملك وعدة أعضاء منهم من يقترحهم رئيس الحكومة ومنهم من طرف رئيس مجلس النواب أو رئيس مجلس المستشارين.[2]

ثانيا: مهام السلطة

أوكلت جل التشريعات الدولية والوطنية للسلطات والهيئات المختصة بحماية ومراقبة المعطيات ذات الطابع الشخصي عدة مهام في إطار السهر على مطابقة معالجة هذه المعطيات الشخصية لأحكام القوانين والتشريعات المعمول بها، وضمان عدم الاعتداء على حقوق وحريات الأشخاص أثناء هذه المعالجة وعلى غرار المشرع التونسي والمغربي وكذا المشرع الفرنسي قيد المشرع الجزائري عمليات المعالجة بعدة وسائل قانونية وقائية وردعية للحيلولة دون إلحاق الضرر بصاحبها، تضمنها القانون رقم 18-07 سالف الذكر سوف نقوم فيما يلي بتحديد الدور الوقائي والردعي للسلطة الوطنية لحماية المعطيات ذات الطابع الشخصي مع الوقوف على مدى فعاليتها في تحقيق أهداف الضبط الإداري في حماية هذه المعطيات.

1) الدور الوقائي للسلطة:

أخضع القانون 18-07 كل عملية معالجة للمعطيات ذات الطابع الشخصي لتصريح مسبق يقوم المسئول عن المعالجة بإرساله للسلطة الوطنية وقد حددت المادة 14 من نفس القانون البيانات الواجب توافرها في هذا التصريح من بينها اسم وعنوان المسئول عن المعالجة، طبيعة المعالجة والغرض منها...الخ،[3] لتقوم هذه السلطة بمنحه ترخيصا بمزاولة عملية معالجة المعطيات، حيث تقرر السلطة ضرورة الحصول على هذا الترخيص كلما رأت أن المعالجة المعتزم القيام بها تتضمن أخطارا على احترام الحياة الخاصة

[1] ينظر المادة 23 من نفس القانون.

[2] ينظر المادة 02 من المرسوم رقم 15-09-1 القاضي بتطبيق القانون رقم 09-08 سالف الذكر.

[3] ينظر المادة 13 من القانون رقم 18-07 والتي تقابلها المادة 27 من القانون رقم 09_08 المغربي سالف الذكر.

والحريات الأساسية للأشخاص، [1] كما تتولى السلطة إعلام الأشخاص المعنيين والمسئولين عن المعالجة بحقوقهم وواجباتهم، إذ اشترطت المادة 07 من نفس القانون ضرورة الحصول على الموافقة المسبقة والصريحة للشخص المعني قبل القيام بمعالجة المعطيات الخاصة به، وفي حال كان هذا الشخص عديم أو ناقص أهلية فإن الموافقة تخضع لقواعد القانون العام، وكاستثناء عن هذه القاعدة يمكن معالجة المعطيات الخاصة بشخص معين دون الموافقة المسبقة له وذلك في حالات معينة من بينها حماية حياته أو تحقيقا لمصلحته الشخصية، [2] كما يلتزم المسئول عن المعالجة بسرية وسلامة المعطيات حيث يجب عليه وضع التدابير التقنية والتنظيمية الملائمة لحماية المعالجة من الإتلاف أو القرصنة الإلكترونية وكل ما يهدد الحياة الخاصة للأشخاص.[3]

كما أقر المشرع من خلال هذا القانون لأصحاب المعطيات الشخصية إمكانية السيطرة على بياناتهم والتدخل في حالة الاعتداء عليها، إذ نص على الحق في إعلامهم من قبل المسئول عن المعالجة بأي تجميع لمعطياتهم وبهوية المسئول عن المعالجة وكذا الغرض منها، وتنبيه الشخص المعني بحقه في رفض السماح بمعالجة بياناته أو طلب تعديلها أو محوها تماما، [4] إلى جانب حق الإعلام أقر المشرع للشخص المعني حقه في الولوج من خلال طلب معلومات من الشخص المسئول عن المعالجة لمعرفة ما إذا تمت معالجة معطياته أم لا وكذا أغراض المعالجة...الخ، [5] أيضا للشخص المعني حق تصحيح معطياته الشخصية أو مسحها أو إغلاقها في حالات معينة، [6] وحق الاعتراض عن كل عملية معالجة لمعطياته الشخصية خاصة إذا تعلق الأمر بأغراض دعائية أو تجارية ويبقى هذا الحق مقيدا بوجود مبررات مشروعة للاعتراض، [7] كما له الحق في منع الاستكشاف المباشر لبياناته الشخصية بواسطة أي وسيلة ودون موافقته ومثال ذلك الرسائل الدعائية التي تصل زبائن الهاتف النقال بدون معرفة كيفية وصول أرقامهم للمرسلين ولا معرفة هويتهم للاعتراض عن هذه الرسائل وطلب إيقافها.[8]

---

[1] ينظر المادة 17 من القانون رقم 18-07 سالف الذكر.

[2] ينظر المادة 12 من القانون رقم 18-07 والتي تقابلها في التشريع المغربي المادة 12 من القانون رقم 09-08 سالف الذكر.

[3] ينظر المادة 38 من القانون رقم 18-07 سالف الذكر.

[4] ينظر المادة 32 من نفس القانون .

[5] ينظر المادة 34 من نفس القانون .

[6] ينظر المادة 35 من نفس القانون

[7] ينظر المادة 36 من نفس القانون .

[8] ينظر المادة 37 من نفس القانون

يقابل هذه المواد في التشريع المغربي المواد من 05 إلى المادة 11 من القانون رقم 09-08 سالف الذكر والتي تحدد حقوق الشخص المعني بمعالجة المعطيات.

2) الدور الردعي للسلطة

إلى جانب الآليات الوقائية التي تفرضها السلطة الوطنية لحماية المعطيات الشخصية تملك أيضا عدة آليات ووسائل ردعية تتمثل في اتخاذ الجزاءات المناسبة لمواجهة كل حالات انتهاك الأحكام والشروط القانونية المقررة لحماية هذه المعطيات، حيث تلجأ السلطة لإنذار المسئول عن المعالجة بمخالفته للأحكام القانونية المعمول بها وتذكره بضرورة مطابقة عمله لحقوق الشخص المعني، وفي حالة ارتكاب المسئول عن المعالجة أفعالا من شأنها الإضرار بالشخص المعني توجه له السلطة إعذارا قانونيا مع تحديد أجل لوضع حد لهذه التجاوزات، وفي حالة عدم امتثاله للإعذار الموجه إليه تتخذ السلطة تجاهه إجراء السحب المؤقت لوصل التصريح أو الترخيص لمدة لا تتجاوز سنة واحدة، كما يمكن لها اتخاذ قرار السحب النهائي للترخيص في حالة جسامة هذه الانتهاكات،[1] وفي حالة ما رأت أنها تمس بالنظام والأمن العموميين أو منافية للأخلاق والآداب العامة،[2] كما تفرض عقوبة الغرامة المالية ضد كل مسئول عن المعالجة يرفض دون سبب شرعي حقوق الإعلام والولوج والتصحيح أو الاعتراض أو لم يقوم بتبليغ السلطة الوطنية بالمعالجات المزعم القيام بها.[3]

إلى جانب هذه الإجراءات الإدارية تتمتع السلطة الوطنية باتخاذ إجراءات جزائية ضد كل من يخالف القواعد المعمول بها والتي تهدف أساسا لحماية المعطيات الشخصية، بحيث أقر القانون لهذه السلطة القيام بالتحريات اللازمة ومعاينة المحلات والأماكن التي تتم فيها المعالجة والولوج إلى المعطيات وجمعها بمساعدة أعوان وضباط الشرطة القضائية،[4] وتوقيع العقوبات الجزائية المنصوص عليها في الفصل الثالث من القانون رقم 18-07 سالف الذكر.[5]

الفرع الثالث: دور المنظومة الوطنية لأمن الأنظمة المعلوماتية في الوقاية من الجرائم الإلكترونية.

حاول المشرع الجزائري التدخل من جديد بآليات مستحدثة ترعاها وزارة من بين الوزارات السيادية وهي وزارة الدفاع الوطني كون أن قضايا الأمن السيبراني تمس بالسيادة الوطنية للدولة وتهدد كافة قطاعات

[1] ينظر المادة 46 من القانون رقم 18-07 سالف الذكر.

[2] ينظر المادة 48 من نفس القانون

[3] ينظر المادة 47 من نفس القانون

[4] ينظر المادة 49 من نفس القانون والتي تقابلها المادة 53 وما يليها في القانون المغربي رقم 09-08 سالف الذكر.

[5] ينظر المادة 54 ومايليها من القانون رقم 18-07 سالف الذكر والتي تقابلها المواد 53 وما يليها من القانون المغربي سالف الذكر.

ومجالات الحياة، وذلك من خلال إصدار المرسوم الرئاسي رقم 20-05 المؤرخ في 20 جانفي[1]2020 حيث بناء على هذا المرسوم استحدث ما يسمى ب "المنظومة الوطنية لأمن الأنظمة المعلوماتية" والتي تعتبر أداة الدولة في مجال أمن الأنظمة المعلوماتية، [2] وتشمل هذه المنظومة طبقا لنص المادة 03 من المرسوم سالف الذكر مجلس وطني لأمن الأنظمة المعلوماتية ووكالة لأمن الأنظمة المعلوماتية ويساعد هذه الأجهزة هياكل أخرى مختصة تابعة لوزارة الدفاع الوطني، سنتعرض بالتفصيل لكل من تشكيلة هذه المنظومة ومهامها في مجال الأمن المعلوماتي.

أولا: دور المجلس الوطني لأمن الأنظمة المعلوماتية

يعتبر المجلس الوطني هيئة مستحدثة في مجال تأمين الأنظمة المعلوماتية المختلفة، سنتناول من خلال هذه النقطة تحديد تشكيلته ثم أبرز مهامه في ضبط الأنظمة المعلوماتية.

1) تشكيلة المجلس الوطني لأمن الأنظمة المعلوماتية

تضم تشكيلة المجلس حسب نص المادة 05[3] من المرسوم الرئاسي رقم 20-05 رئيسا يتمثل في وزير الدفاع الوطني أو ممثله وممثل عن رئاسة الجمهورية، ممثل عن الوزير الأول، الوزير المكلف بالشؤون الخارجية، الوزير المكلف بالداخلية، الوزير المكلف بالعدل، الوزير المكلف بالمالية، الوزير المكلف بالطاقة، الوزير المكلف بالاتصالات، الوزير المكلف بالتعليم العالي، كما يمكن أن يستعين المجلس بأي شخص أو مؤسسة من شأنه تنويره في أعماله، كما يتوفر المجلس لأداء مهامه على أمانة تقنية توضح تحت سلطة رئيس المجلس أي وزير الدفاع، [4] يقوم بتسييرها أمين عام يعين من طرف وزير الدفاع الوطني، [5] تكلف الأمانة التقنية بعدة مهام من بينها إعداد مشروع النظام الداخلي للمجلس وجمع أي معلومات ووثائق ذات صلة بأشغال المجلس، كما تتولى تسيير الموارد البشرية والمادية والتنسيق مع مختلف الأجهزة الأخرى التابعة لوزارة الدفاع الوطني.[6]

[1] المرسوم الرئاسي رقم 20-05 المؤرخ في 24 جمادى الأولى 1441 الموافق 20 جانفي 2020، يتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية، المشار إليه سابقا.

[2] ينظر المواد 01 و02 من نفس المرسوم .

[3] ينظر المادة 05 من نفس المرسوم.

[4] ينظر المادة 07 من المرسوم الرئاسي رقم 20-05 المتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية المشار إليه سابقا.

[5] ينظر المادة 08 من نفس المرسوم

[6] ينظر المادة 09 من نفس المرسوم.

من خلال التمعن في تشكيلة المجلس يرى الباحث أن التشكيلة متنوعة تضم ممثلين ووزارات سيادية بما يحقق فكرة الأمن المعلوماتي أو الأمن السيبراني في مختلف القطاعات كقطاع التعليم العالي مثلا والذي يعتبر من أهم القطاعات التي تحتاج إلى أنظمة معلوماتية حمائية تمنع وتقلل من حجم التهديدات التي تقع عليه، كما تفيده هذه الأنظمة في تطوير خدماته الرقمية بما يحقق جودة الخدمة وسرعتها وأمانها أيضا وبالتالي تعود الفائدة على الطلبة والأساتذة في تقديم المعلومات والاستفادة منها بطرق سهلة وسريعة ومؤمنة، على غرار قطاع التعليم العالي فإن إشراك الوزارات في هذا المجلس يعتبر قفزة نوعية للجزائر من أجل تأمين أنظمتها من التهديدات السيبرانية واللحاق دائما بالركب التكنولوجي المتطور.

2) مهام المجلس الوطني لأمن الأنظمة المعلوماتية

قد عدد المرسوم الرئاسي رقم 20-05 في المادة 04[1] منه مهام وصلاحيات المجلس الوطني لأمن الأنظمة المعلوماتية حيث يتولى هذا الأخير إعداد الإستراتيجية الوطنية لأمن الأنظمة المعلوماتية المقترحة من قبل الوكالة وتحديدها، الموافقة على سياسة التصديق الإلكتروني للسلطة الوطنية للتصديق الإلكتروني وتصنيف الأنظمة المعلوماتية، كما يبدي رأيه في أي مشروع نص تشريعي أو تنظيمي ذي صلة بأمن الأنظمة المعلوماتية.

ثانيا: دور وكالة أمن الأنظمة المعلوماتية

تعتبر وكالة أمن الأنظمة المعلوماتية الجهاز الثاني للمنظومة الوطنية لأمن الأنظمة المعلوماتية الموضوعة لدى وزارة الدفاع الوطني، يقابلها في التشريع التونسي الوكالة الوطنية للسلامة المعلوماتية[2] (ANSI) التي استحدثت بموجب القانون عدد 05 المؤرخ في 03 فيفري 2004[3] المتعلق بالسلامة المعلوماتية، والوكالة الوطنية لسلامة الأنظمة المعلوماتية (ANSSI) التي أنشأت في فرنسا في 07 جويلية 2009 التي مقرها باريس[4]، حيث كان للمشرع التونسي والفرنسي السبق في إنشاء هذه الوكالة على عكس تبني المشرع

[1] ينظر المادة 04 من نفس المرسوم

[2] ANSI : Agence National de Sécurité Informatique الوكالة الوطنية للسلامة المعلوماتية

[3] القانون عدد 05 المؤرخ في 03 فيفري 2004 المتعلق بالسلامة المعلوماتية، الرائد الرسمي للجمهورية التونسية العدد 10 الصادر في 03 فيفري 2004.

[4] ANSSI : Agence national de la sécurité des systèmes d'information الوكالة الوطنية لسلامة الأنظمة المعلوماتية الفرنسية

الجزائري لها والذي جاء متأخرا لغاية عام 2020، [1] إذ تعتبر الوكالة حسب نص المادة 17 من المرسوم الرئاسي رقم 20-05 [2] مؤسسة ذات طابع إداري تتمتع بالشخصية المعنوية والاستقلالية المالية ويحدد مقرها بمدينة الجزائر، كما يحدد تنظيم مكونات هذه الوكالة وكيفيات سيرها وكذا مهامها وصلاحياتها بموجب قرار من وزير الدفاع الوطني، [3] أما عن الوكالة الوطنية للسلامة المعلوماتية التونسية فتعتبر مؤسسة عمومية لا تكتسي صبغة إدارية تتمتع بالشخصية المعنوية والاستقلال المالي يطلق عليها اسم الوكالة وتخضع للتشريع التجاري ويكون مقرها بتونس العاصمة، وتقع تحت إشراف وزارة تكنولوجيا المعلومات والاتصال والاقتصاد الرقمي، [4] وعليه سنتناول بالشرح كل من تشكيلة هذه الوكالات ومهامها في النقاط التالية:

1) تشكيلة وكالة أمن الأنظمة المعلوماتية

تضم الوكالة الوطنية للسلامة المعلوماتية بتونس في تشكيلتها إدارة عامة مسئولة عن الإستراتيجية الوطنية لتأمين النظم المعلوماتية وهياكل ووحدات ثانوية تتمثل في وحدة الإشراف واليقظة التكنولوجية، إدارة تكنولوجيات سلامة الأنظمة المعلوماتية، إدارة التدقيق في سلامة الأنظمة، وإدارة الاستجابة للطوارئ المعلوماتية، [5] وعن تشكيلة الوكالة الوطنية لسلامة الأنظمة المعلوماتية الفرنسية فتضم إدارة تتكون من مكتب وخلية للأمن السيبراني، تتفرع عنهما عدة أجهزة مسئولة عن عمليات المراقبة والخبرة التقنية وكذا الاستراتيجيات المتبعة في تحقيق أمن الأنظمة المعلوماتية. [6]

أما عن الوكالة الوطنية بالجزائر فيتولى إدارتها وفقا لنص المادة 20 من المرسوم 20-05 لجنة توجيه وتزود بلجنة علمية، يقوم بتسييرها مدير عام كما تتوفر الوكالة على مركز وطني عملياتي لأمن الأنظمة المعلوماتية ومديريات ومصالح تقنية وإدارية موضوعة تحت سلطته، فأما عن لجنة التوجيه فلها تشكيلة خاصة تتمثل في رئيس لجنة التوجيه الذي يتم تعيينه طبقا للتنظيم المعمول به في وزارة الدفاع الوطني، [7]

---

[1] حزام فتيحة، حماية الأنظمة الرقمية بين الآليات التقنية وأجهزة الحماية(قراءة في أحكام المرسوم الرئاسي 20-05)، مجلة الحقوق والعلوم الإنسانية، العدد الثالث، أكتوبر 2020، ص 182.

[2] ينظر المادة 17 من المرسوم الرئاسي رقم 20-05 المتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية المشار إليه سابقا.

[3] ينظر المادة 34 من نفس المرسوم

[4] ينظر الفصل الأول من الباب الأول من القانون عدد 05 لسنة 2004 سالف الذكر.

[5] لمزيد من التفاصيل يراجع الموقع الرسمي للوكالة الوطنية للسلامة المعلوماتية التونسية، المتاح على الرابط التالي: https://www.ansi.tn/ar

[6] لمزيد من التفاصيل يراجع الموقع الرسمي للوكالة الوطنية لسلامة الأنظمة المعلوماتية الفرنسية، المتاح على الرابط التالي: https://www.ssi.gouv.fr/agence/organisation/organigramme-general/

[7] ينظر المادة 21 من المرسوم الرئاسي رقم 20-05 المتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية المشار إليه سابقا.

إلى جانب الرئيس تتكون اللجنة من كل من ممثلي وزارة الدفاع الوطني، الوزارة المكلفة بالشؤون الخارجية، الوزارة المكلفة بالداخلية، الوزارة المكلفة بالعدل، الوزارة المكلفة بالمالية، الوزارة المكلفة بالطاقة، الوزارة المكلفة بالتعليم العالي، الوزارة المكلفة بالصناعة، الوزارة المكلفة بالاتصالات، الوزارة المكلفة بالتجارة، مصالح الأمن، سلطة ضبط البريد والاتصالات الإلكترونية، السلطة الوطنية للتصديق الإلكتروني، الهيئة الوطنية لحماية البيانات ذات الطابع الشخصي، السلطة الحكومية للتصديق الإلكتروني، وعلى سبيل الاستشارة المدير العام للوكالة، كما يمكن للجنة أن تستعين بأي شخص أو مؤسسة من شأنها تنويرها في أعمالها.[1]

نرى أنه قد وفق المشرع الجزائري من خلال تقريره لهذه التشكيلة المتنوعة والتي ضمت العديد من السلطات والوزارات ذات الصلة بالأمن المعلوماتي وتنظيم الاتصالات والبريد وحماية البيانات الشخصية والمعلومات الرقمية وضبط كل نشاط متعلق بها، لكن ما يثير التساؤل هنا، لماذا لم يضم المشرع الجزائري الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال المنصوص عليها بموجب القانون رقم 04/09 سالف الذكر بما أنها هي الأخرى تعتبر سلطة إدارية مستقلة مهمتها الوقاية من مختلف التهديدات المتعلقة بالفضاء السيبراني مثلها مثل كل من سلطة البريد والاتصالات الإلكترونية وكذا الهيئة الوطنية لحماية البيانات ذات الطابع الشخصي والسلطة الوطنية للتصديق الإلكتروني؟

يعتبر المدير العام الجهاز الثاني للوكالة يعين طبقا للتنظيم المعمول به في وزارة الدفاع الوطني وتنهى مهامه حسب الأشكال نفسها طبقا لنص المادة 27 من المرسوم السابق، ويسهر على تنسيق تنفيذ الإستراتيجية الوطنية لأن الأنظمة المعلوماتية وينفذ المخططات والبرامج المسطرة من طرف لجنة التوجيه، كما يعتبر مسئولا عن سير الوكالة حيث يتولى تسييرها في إطار احترام كل من التشريع والتنظيم المعمول بهما.[2]

تعزيزا لحسن سير الوكالة تم استحداث لجنة علمية بموجب المرسوم سالف الذكر، حيث من تسميتها نستنتج أنه يغلب عليها الطابع العلمي في عملها، تتكون هذه الأخيرة من عشرة (10) أعضاء يتم اختيارهم لمدة 03 سنوات قابلة للتجديد من قبل لجنة التوجيه من بين الأساتذة والباحثين والخبراء في مجال أمن الأنظمة المعلوماتية، كما ينتخب رئيس اللجنة العلمية من طرف زملائه الأعضاء وهذا ما نصت عليه المادة 31 من نفس المرسوم، [3] نجد من خلال هذه التشكيلة أنها تضم باحثين وأساتذة في مجال الأمن المعلوماتي

[1] ينظر المادة 22 من نفس المرسوم

[2] ينظر المواد 27 28 من المرسوم الرئاسي رقم 20-05 المتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية المشار إليه سابقا.

[3] ينظر المادة 31 من نفس المرسوم

وهذا ما يعتبر نقطة ايجابية وإضافة جد هامة للمشرع الجزائري، فمن خلال إشراك الباحثين في هذا المجال قد أعطى الفرصة لهم لإبداء مهاراتهم وتعزيز خبراتهم وكفاءتهم في هذا المجال فضلا عن ما يقدمونه من معلومات وإضافات جديدة ومستمرة تتطور بتطور التكنولوجيا والبحث العلمي، كما يمكن للجنة الاستعانة بأي شخصية علمية أو خبير بإمكانه المساهمة المفيدة بكفاءاته في تطوير أمن الأنظمة المعلوماتية.[1]

تجدر الإشارة إلى أن المشرع ترك تحديد تنظيم مكونات الوكالة وكيفيات سيرها وكذا مهامها وصلاحياتها بموجب قرار من وزير الدفاع الوطني.[2]

2) مهام وكالة أمن الأنظمة المعلوماتية

تتعدد وتتنوع المهام والصلاحيات التي أقرها المشرع لوكالة أمن الأنظمة المعلوماتية بموجب المرسوم رقم 20- 05 بحيث منح المشرع لكل جهاز في الوكالة صلاحيات معينة، إذ تكلف لجنة التوجيه[3] بدراسة واقتراح عناصر الإستراتيجية الوطنية لأمن الأنظمة المعلوماتية، تحديد الطرق والوسائل اللازم للاستجابة للحاجات الوطنية في مجال أمن الأنظمة وكذا ضبط الوسائل اللازمة لترقية البحث والتطوير في مجال أمن الأنظمة والتطبيقات ذات الصلة بالاحتياجات الوطنية وغيرها من المهام.

أما عن المدير العام للوكالة فيتولى تنسيق تنفيذ الإستراتيجية الوطنية لأمن الأنظمة المعلوماتية وهو بهذه الصفة يقوم[4] بإعداد مخطط عمل وبرامج نشاط الوكالة ويعرضها على لجنة التوجيه للموافقة عليها، ويتصرف باسم الوكالة ويمثلها أمام الهيئات القضائية، يبرم الصفقات ويوقع العقود والاتفاقيات والاتفاقات ذات الصلة بمهام الوكالة طبقا للتنظيم المعمول به، كما يعد المدير العام للوكالة تقريرا سنويا عن نشاطات الوكالة ويرسله إلى رئيس المجلس.

أما بالرجوع لمهام الوكالة الوطنية للسلامة المعلوماتية التونسية وطبقا للفصل 03 من الباب الأول من القانون عدد 05 لسنة 2004 سابق الذكر فإنها تضطلع بمهمة مراقبة النظم والشبكات الخاصة بمختلف الهياكل العمومية والخاصة من خلال السهر على ضمان اليقظة التكنولوجية، كما يهدف مركز الاستجابة

[1] ينظر المادة 33 من نفس المرسوم

[2] ينظر المادة 34 من نفس المرسوم

[3] ينظر المادة 24 من نفس المرسوم

[4] ينظر المادة 28 من المرسوم الرئاسي رقم 20-05 المتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية المشار إليه سابقا.

للطوارئ المعلوماتية داخل الوكالة إلى تعزيز سلامة المنظومات المعلوماتية والبنية التحتية للاتصالات والمعلومات بالجمهورية التونسية، وذلك من خلال اعتماد إجراءات استباقية وجمع وتحليل المعلومات المتعلقة بالحوادث السيبرانية والتنسيق بين الأطراف المعنية لمعالجتها والحد منها على المستويين الوطني والدولي، وهي نفس المهام التي تهدف الوكالة الوطنية لسلامة الأنظمة المعلوماتية إلى تحقيقها.[1]

[1] لمعرفة المزيد عن مهام الوكالة الوطنية للسلامة المعلوماتية، يراجع الموقع الرسمي للوكالة الوطنية للسلامة المعلوماتية، المتاح على الرابط التالي: https://www.ansi.tn/ar/node/50547 تاريخ الاطلاع: 2021/03/23 على الساعة 22:00.

الفصل الثاني

دور وحدات البحث والتحري عن الجرائم الإلكترونية كضبطية قضائية (ردعية)

الفصل الثاني: دوروحدات البحث والتحري عن الجرائم الإلكترونية كضبطية قضائية (ردعية)

كان للتزايد المستمر للجرائم الإلكترونية الأثر البالغ في تطوير أجهزة الضبط القضائي لتواكب التطور الحاصل في مجال مكافحة الجريمة، ونتيجة لهذا التحدي قامت معظم الدول بإحداث أجهزة متخصصة بمكافحة هذا النوع من الإجرام المستحدث، حيث تتولى مهمة البحث والتحري عنها وكشف غموضها، إذ سميت هذه الأخيرة بشرطة الإنترنت، تتميز بالخبرة والمعرفة بتقنيات التحقيق في هذه الجرائم، وتختلف تماما عن الشرطة التقليدية لكونها لا تعتمد على التدريبات المادية التي يتلقاها رجال الشرطة في الجرائم العادية، وإنما تعتمد على قوة تكوين البناء العلمي والتكنولوجي لهم لتولى مهمة البحث والتحري في العالم الافتراضي، على كلا الصعيدين الداخلي والدولي مجسدة بذلك مظاهر التعاون الشرطي الدولي من أجل التصدي الأمثل لهذه الجرائم، ففيما تتمثل هذه الوحدات والأجهزة؟

للإجابة عن هذا التساؤل ارتأينا معالجة هذا الفصل من خلال مبحثين رئيسيين: خصصنا الأول لدراسة وحدات البحث والتحري عن الجرائم الإلكترونية على المستوى الداخلي، في حين خصصنا الثاني لدراسة وحدات البحث والتحري عن الجرائم الإلكترونية على المستوى الإقليمي والدولي.

المبحث الأول: وحدات البحث والتحري عن الجرائم الإلكترونية على المستوى الداخلي

تسعى كل دولة لمحاربة الجرائم الإلكترونية داخل إقليمها راصدة لذلك عتادها الفني التقني والبشري، فعلى المستوى التقني قد قامت أغلب الدول بتوفير أساليب وطرق حديثة ومتطورة لحماية مجتمعاتها من مختلف الانتهاكات التي تحدث نتيجة التطور التكنولوجي، أما على المستوى البشري فقد أسست أغلب دول العالم الأجنبية منها والعربية وحدات خاصة تعمل على مكافحة الجرائم الإلكترونية، وتتولى مسائل التحري والتحقيق بشأنها والتي سنتطرق لها بالدراسة من خلال المطالب الآتية:

المطلب الأول: وحدات البحث والتحري عن الجرائم الإلكترونية على مستوى الدول الأجنبية

نتيجة تطور أغلب الدول الأجنبية في المجال التكنولوجي والذي أسفر عن ظهور وتنامي الجرائم والانتهاكات الإلكترونية كما سبق وأشرنا، فإنه قد سعت أغلب هذه الدول إلى تحديث تشريعاتها الداخلية بما فيها الإجرائية عن طريق استحداث بعض الأجهزة والوحدات المختصة بمتابعة هذا النوع من الجرائم والتحري بشأنها وذلك على مستوى كل من الدول الأنجلوساكسونية وكذا اللاتينية.

الفرع الأول: على مستوى الدول الأنجلوساكسونية

من أبرز الدول الأنجلوساكسونية التي بادرت بإنشاء شرطة متخصصة في مكافحة جرائم الإنترنت نجد المملكة المتحدة أو انجلترا، الولايات المتحدة الأمريكية، وكندا، سنتطرق لكل منها فيما يأتي:

أولا: المملكة المتحدة (انجلترا)

قامت المملكة المتحدة كغيرها من الدول المهددة بالاعتداءات السيبرانية بتخصيص وحدة تضم نخبة من رجال الشرطة المتخصصين في مجال البحث والتحري عن الجرائم الإلكترونية، حيث تضم هذه الوحدة نحو 80 مفتشا من رجال شرطة وجمارك ذو درجة عالية من الخبرة والكفاءة في المجال التقني والمعلوماتي، يتمركز هؤلاء الضباط في مدينة لندن وفي جميع المفتشيات الإقليمية التقليدية المتواجدة في انجلترا، حوالي 40 منهم يمارسون مهامهم ضمن الوحدة الوطنية لمكافحة جرائم التقنية العالية،[1] والباقي مقسمون على الوحدات المحلية الأخرى، حيث بدأت هذه الوحدة عملها في سنة 2001 ويتمثل دورها في متابعة مرتكبي الجرائم الإلكترونية بصفة عامة والجرائم الجنسية الواقعة على الأحداث والقصر بصفة خاصة،[2] إلى جانب هذه الوحدة تم إنشاء وحدة أخرى تختص بمكافحة الجريمة الإلكترونية على مستوى الشرطة المركزية "PCEU" والتي تختص بتحليل وتطوير المعلومات الاستخباراتية حول الجرائم الإلكترونية، وإنشاء شبكة تعاونية بين مؤسسات الدولة لتبادل المعلومات بشأن تطور هذه الجرائم، كما تقوم بالتحقيق في الحوادث الإلكترونية وتقديم الدعم والمشورة لسلطات إنفاذ القانون والأجهزة الشرطية في انجلترا.[3]

ومن جهة أخرى قامت المملكة المتحدة بتأسيس وكالة وطنية لمكافحة الجريمة أطلق عليها اسم "NCA"[4] تختص بمكافحة الجريمة المنظمة والاتجار بالبشر والأسلحة، والجريمة الاقتصادية، وجرائم الاحتيال الدولي، وجرائم المخدرات، وكذا الجرائم الإلكترونية، حيث تم تأسيسها نتيجة تصاعد الجرائم خاصة المرتبطة باستخدام التكنولوجيات الحديثة والجرائم المنظمة وذلك في 07 أكتوبر 2013 لتحل بذلك محل وكالة مكافحة الجريمة المنظمة والخطيرة "SOCA"، وهي تضم ثمانية فروع يشرف عليها سبعة مديرين يرأسهم مدير عام يساعده في مهامه نائبه، إذ تضم بذلك أكثر من 4000 ضابط، ونظرا لأهمية ما

---

[1] L'unité nationale de crime high-tech الوحدة الوطنية لمكافحة جرائم التقنية العالية

[2] نبيلة هبة هروال، الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات، المرجع السابق، ص 111.

[3] حسام محمد نبيل الشنراقي، الجرائم المعلوماتية، جرائم الاعتداء على التوقيع الإلكتروني(دراسة مقارنة)، دار الكتب القانونية، مصر-الإمارات، 2013، ص 747.

[4] NCA : National Crime Agency الوكالة الوطنية لمكافحة الجريمة

تقوم به هذه الوكالة من عرقلة أنشطة المجرمين وتقديمهم للعدالة فإنها تعتبر نقطة اتصال للمملكة المتحدة مع وكالة الإنتربول الدولية والأورو بول وكذا وكالات إنفاذ القانون الدولية الأخرى، ولعل من أبرز الأمثلة عن هذا التعاون هي عملية كاثريك"Catterick" والتي تتعلق بالابتزاز الذي قامت به شركات القمار عبر الإنترنت في الفترة الممتدة من ماي إلى أكتوبر 2004، حيث تلخصت وقائع هذه القضية في مجموعة أشخاص قاموا بإرسال رسائل لإحدى الشركات مطالبين بأموال مهددين إياها بأن يشنوا هجمات حجب الخدمة الموزعة على مواقع هذه الشركات في حالة امتناعها عن الدفع[1]، حيث تم تدمير العديد من المواقع الإلكترونية في جميع أنحاء العالم، منها 10 شركات بالمملكة المتحدة تجاوزت خسائرها 30 مليون جنيه إسترليني وأخرى من الولايات المتحدة الأمريكية، بالإضافة للأثر الذي تعرضت له المواقع نفسها من تعطيل، ومع مباشرة التحقيقات وعمليات المراقبة السرية للمواقع أسفرت عن إلقاء القبض على 10 أشخاص يشتبه في تورطهم وتم تحديد موقع جهاز كمبيوتر تم اختراقه في مدينة بالاكوفيا بروسيا، بدأت الشرطة الروسية على إثره بإجراء تحقيق مشترك مع الدولتين السابقتين أسفر عن توقيف عدد من الأشخاص وضبط عدد من أجهزة الكمبيوتر، والحكم على هؤلاء الأشخاص بالسجن ثماني سنوات بتهمة الابتزاز ونشر الفيروسات على أجهزة الكمبيوتر.[2]

ثانيا: الولايات المتحدة الأمريكية

نتيجة تزايد جرائم الإنترنت في الولايات المتحدة الأمريكية سارعت هي الأخرى بإنشاء عدة أجهزة ووحدات شرطة متخصصة في مكافحة هذا النوع من الإجرام والحد من خسائره، تتمثل فيما يلي:

[1] هجمات الحرمان من الخدمات أو هجوم حجب الخدمة: (Denial of Service Attacks) هي هجمات تتم عن طريق إغراق المواقع بكم هائل من البيانات غير اللازمة يتم إرسالها عن طريق أجهزة أو برامج *تسمى*(DDOS Attacks) تعمل على نشر هذه الهجمات، بحيث يتحكم فيها القراصنة الإلكترونيون أو المعلوماتيون لمهاجمة شبكة الإنترنت عن بعد بإرسال تلك البيانات إلى المواقع بشكل كثيف مما يسبب بطء الخدمات أو زحاماً بهذه المواقع ويسبب صعوبة وصول المستخدمين لها نظراً لهذا الاكتظاظ، خصوصاً وأنه يبدو وباعتراف الكثير من خبراء الأمن على الشبكة أنه لا يوجد علاج في الوقت الحالي لهذا الأسلوب في الهجوم على مواقع الشبكة (الإنترنت)، وعلى هذا الأساس فإن هذا النوع من الهجمات يُدعى في بعض الأوساط "بإيدز الإنترنت"ويتم هذا الهجوم بدون كسر ملفات كلمات السر أو سرقة البيانات السرية، بل يتم ببساطة بأن يقوم المهاجم أو المجرم بإطلاق أحد البرامج التي تزحم المرور للموقع الخاص بأي شخص أو مؤسسة وبالتالي تمنع أي مستخدم آخر من الوصول إليه.

[2] ليندا بن طالب، الدليل الإلكتروني ودوره في الإثبات الجنائي، أطروحة مقدمة لنيل شهادة الدكتوراه، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، 2019، ص 213.

1) مكتب التحقيقات الفيدرالي[1] (FBI)

يعتبر مكتب التحقيقات الفيدرالي وكالة حكومية تابعة لوزارة العدل الأمريكية تعمل كوكالة استخباراتية داخلية وقوة لتطبيق القانون في الدولة، حيث تأسست هذه الوكالة عام 1908 تحت اسم مكتب التحقيقات وتم تغييره إلى الاسم الحالي في عام 1935، مقره بواشنطن عاصمة أمريكا ويضم أكثر من 400 مكتب تحقيق مركزي منتشرة عبر عدة مدن داخل الو م أ، بالإضافة إلى 60 مكتب تحقيق دولي في القنصليات والسفارات الأمريكية حول العالم، يعمل هذا الجهاز على حماية الو م أ والدفاع عنها وتحقيق العدالة الجنائية، ذلك من خلال مكافحة الهجمات الإرهابية والإلكترونية والمنظمات الإجرامية المختلفة،[2] ونظرا للطابع التقني للجرائم الإلكترونية عني هذا المكتب بتوفير التدريب اللازم لمكافحة هذه الجرائم من خلال تنظيم دورات متخصصة مدة كل منها أربعة (04) أسابيع تعقدها أكاديمية هذا المكتب في كوانتيكو وفيرجينيا، تقوم من خلالها بتزويد محققي الشرطة والعاملين في سلطات إنفاذ القانون بصفة عامة بمهارات ومعارف حول البرمجة والحوسبة وكيفية التعامل مع هذا النوع من المسارح الافتراضية.[3]

ومن أشهر العمليات التي قام بها هذا المكتب العملية المعروفة باسم "I LOVE YOU"التي وقعت في 04 ماي عام 2000 حيث تم هجوم الشركات والأفراد في جميع أنحاء العالم من قبل فيروس "أنا أحبك" والذي تسبب في عدة خسائر كبيرة، حيث يستهدف هذا الفيروس البريد الإلكتروني للضحية والذي يحمل ملفا مرفقا يسمى "Love Letter For You" هو في الأصل عبارة عن فيروس خبيث وليست رسالة حب، يقوم بسرقة كلمات المرور ونسخ الملفات المتواجدة على جهاز الضحية، كما يرسل نسخ منه تلقائيا إلى جميع جهات الاتصال الموجودة في دفتر عناوين Microsoft Outlook، وعلى إثر هذا الهجوم تم التعاون بين كل من المركز القومي الأمريكي ومكتب التحقيقات الفيدرالي وكذا مكتب التحقيقات الفلبيني بالتحقيق في الحادث وتم التعرف على المشتبه فيه والذي يدعى "أونيل دي جوزمان" وهو رجل فليبيني الأصل وطالب مختص في التعامل مع الحواسيب الآلية.[4]

---

[1] FBI : Federal Bureau Of Investigation مكتب التحقيقات الفيدرالي

[2] مقال حول "مكتب التحقيقات الفيدرالي"، منشور على موقع الموسوعة الحرة "ويكيبيديا"، متاح على الرابط التالي: https://ar.wikipedia.org/wiki/ تاريخ الاطلاع: 2021/06/06 على الساعة 14:00.

[3] هشام محمد فريد رستم، الجوانب الإجرائية لجرائم المعلوماتية (دراسة مقارنة)، مكتبة الآلات الحديثة، مصر، 1994، ص 48.

[4] محمد سيد سلطان، قضايا في أمن المعلومات وحماية البيئة الإلكترونية، دار ناشري للنشر الإلكتروني، الإمارات المتحدة، سنة 2012، ص 49.

2) قسم جرائم الحاسوب والعدوان على حقوق الملكية الفكرية

تم إنشاء قسم جرائم الحاسوب سنة 1991 كوحدة تابعة لوزارة العدل الأمريكية ثم أصبح قسما مستقلا في عام 1996 نتيجة لتضخم أعماله، فقد بدأ عمله بخمسة وكلاء نيابة ليصبح في عام 2000 أكثر من 20 وكيلا، ويختص هذا القسم بالكشف عن الجرائم المرتبطة بالحاسوب الآلي وكذا جرائم الاعتداء على حقوق الملكية الفكرية وملاحقة مرتكبيها[1].

3) المركز الوطني لحماية البنية التحتية

تم إنشاء هذا المركز التابع للمباحث الفيدرالية الأمريكية في 1998/02/28 بحيث يتقاسم مهامه مع وزارة الدفاع الأمريكية، يتكون من فريق سري يصل عدد أعضائه إلى 125 رجل حكومي، تعود نشأة هذا الفريق إلى تقرير جمعية العمل حول جرائم الإنترنت والمقدم إلى الرئيس الأمريكي "بيل كلينتون" والذي حددت من خلاله البنى التحتية التي تعتبر محلا للهجمات والاعتداءات عبر الإنترنت منها قطاع الاتصالات، الغاز، البترول، البنوك والمؤسسات الاقتصادية...الخ.[2]

إضافة إلى هذه الأجهزة تم إنشاء وكالة متخصصة في مكافحة القرصنة المعلوماتية تابعة لمكتب التحقيقات الفيدرالي، مهمتها التنسيق مع المركز الوطني لحماية البنية التحتية ومحاربة جميع أشكال القرصنة والاحتيال المعلوماتي، [3]وكذا نيابة جرائم الحاسوب والاتصالات تتألف من مجموعة من قضاة

---

[1] نبيلة هبة هروال، الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات، المرجع السابق، ص108.

ويقصد بحقوق الملكية الفكرية Propriété intellectuelleحق المؤلف في حماية المبتكرات الفنية المتمثلة في المعارف والاختراعات التي يبتكرها، ويعتبر حق الملكية الفكرية أحد الحقوق المعنوية أو الأدبية التي تعرف على أنها قدرة يقرها ويحميها القانون لشخص على إنتاجه الفكري أو الذهني أو الفني أيا كان نوعه، فله بذلك احتكار المنفعة المالية التي تنتج من استغلاله، ومع التطور التكنولوجي الذي يشهده العالم باستمرار ظهرت أنماط جديدة من المصنفات سميت بمصنفات تقنية المعلومات مثل البرمجيات والخوارزميات وقواعد البيانات ، وسهلت شبكة الإنترنت نقل الملفات والصور والأفلام وتداولها ونشرها والترويج لها وحتى نسخها وتحميلها، مثل قيام الشخص بإنزال نسخة من مقال أو كتاب خاص بمؤلف ما عبر الإنترنت والقيام بترويجها عبر مجموعة إخبارية أو الترويج لفكرة للغير ونسبتها لنفسه وهذا كله لتحقيق أغراض خاصة دون علم أو موافقة المالك أو صاحب هذه المصنفات والابداعات والابتكارات، وهذا ما يعرف بجريمة الاعتداء على الملكية الفكرية عبر الإنترنت والتي تعاقب عليها أغلب تشريعات دول العالم. لمزيد من التفاصيل أنظر نبيلة هبة هروال، جرائم الإنترنت (دراسة مقارنة)، المرجع السابق، ص 204 وما بعدها.

[2] نبيلة هبة هروال، الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات، المرجع السابق، ص 109.

[3] كما تم تأسيس عدة هيئات غير قضائية تقوم بدعم الوحدات المخصصة بالتحقيق على مكافحة الجرائم الإلكترونية، من بينها هيئة الإنترنت للأسماء والأرقام المخصصة " Internet corporation for assignednames and numbers" والتي تعرف بالاسم المختصر "هيئة الأيكان "ICANN"، وهي منظمة غير ربحية تم تأسيسها دوليا سنة 1998 يقع مقرها مدينة كاليفورنيا بالولايات المتحدة الأمريكية أسندت لها مسؤولية توزيع العناوين وبروتوكولات الإنترنت"IP Adress" وإدارة نظام سجلات المواقع العامة عالية المستوى وسجلات المواقع عالية المستوى لرمز الدولة، كما أنها تضطلع بمسؤولية إدارة نظام الخوادم المركزية، وهي بذلك تساعد هيئات مكافحة

النيابة العامة مختصين ومدربين على التعامل مع نظم المعالجة الآلية للمعطيات والبيانات الرقمية، بحيث يتمتعون بصلاحيات واسعة في مجال التحقيق في الجرائم الإلكترونية بمختلف أصنافها، إلى جانب هذا هناك وحدة متخصصة تابعة لقسم العدالة الأمريكي مكلفة بمكافحة الإجرام المعلوماتي، تتكون من خبراء في تقنيات الحوسبة والإنترنت ومن مستشارين وقانونيين.[1]

كما نجد في ولاية أوهايو في الولايات م أ إحدى المنظمات الدولية التي تهدف إلى حماية المواقع الإلكترونية من عمليات الاختراق يطلق عليها اسم شرطة الإنترنت "Internet police" حيث تعمل هذه المنظمة على حماية المواقع التي تتعاقد معها رسميا مقابل مبلغ مالي من أي محاولة اختراق وإذا ما تم تكرار المحاولة أكثر من مرة من طرف المجرم أو الهاكر يتم تجميد الجزء المسئول عن التواصل مع شبكة الإنترنت بحيث يفشل نظام الحاسب في التواصل معها، ومن بين المواقع المحمية من قبل هذه المنظمة نجد بعض مواقع التجارة الإلكترونية ومواقع المباحث الفيدرالية، ومواقع الوزارات لكونها أكثر المؤسسات الحساسة والمسئولة عن الدولة.[2]

ومن أشهر الاختراقات الإلكترونية التي تعرضت لها الو م أ ودول العالم تقريبا الهجوم الذي أطلق عليه تسمية دودة موريس "Moris Worm" البرمجية الخبيثة التي صممها العالم الأمريكي روبرت تابان موريس وأطلقها في 02 نوفمبر 1988 بهدف معرفة حجم الإنترنت عن طريق تحديد عدد الأجهزة المتصلة بها، حيث أصابت هذه الدودة حوالي 6000 جهاز من أصل 60000 جهاز متصل بالإنترنت، أي حوالي 10% من إجمالي عدد هذه الأجهزة، فهي تقوم بنسخ نفسها على جهاز الحاسب الآلي وهكذا أصابت الآلاف من الأجهزة في ظرف زمني قياسي هذا ما أدى إلى عدة خسائر قدرت بما يقارب نصف مليون دولار، وكانت أغلب الأجهزة المستهدفة تابعة لجامعات ناسا وبيركلي وستانفورد ومعهد للتكنولوجيا والبنتاغون، والتي بقيت مصابة لمدة 72 ساعة تقريبا، إلى غاية تدخل عدد من الفرق الأمنية المختصة التي ضمت مجموعة من الخبراء والمبرمجين لإيقاف هذا الهجوم، وتم القبض على موريس ومقاضاته كأول شخص بموجب

...=الجريمة الإلكترونية من خلال توفير المعلومات الإلكترونية التي تحتاجها الدول سواء على صعيد الوكالات أو الأجهزة الحكومية أو على صعيد التعاون الدولي، كما تشارك الهيئة في دراسة وتحليل وتحديد الاستخدام غير المشروع للنطاقات على شبكة الإنترنت، إضافة إلى أنها تساهم في دعم تحديث الخطط الأمنية للبنوك التي تشرف على مواقعها وحل النزاعات المتعلقة بأسماء المواقع، حيث تم استخدامها لحل أكثر من 5000 نزاع على حقوق وأسماء المواقع الإلكترونية، وهي بهذه المهام والجهود تعتبر من أبرز الأمثلة على التعاون في مجال مكافحة الجرائم الإلكترونية. لمزيد من التفاصيل يراجع الموقع الرسمي لهيئة الأيكان المتاح على الرابط التالي:https://www.icann.org

[1] نبيلة هبة هروال، الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات، المرجع السابق، ص 110

[2] عبد الحليم بوقرين، حتمية إنشاء ضبطية خاصة بالجرائم الإلكترونية، مجلة العلوم القانونية والسياسية، المجلد 05، العدد 01، سنة 2016، ص 156.

قانون الاحتيال الإلكتروني الأمريكي، بالسجن لمدة ثلاث سنوات مع وقف التنفيذ وإيقافه تحت المراقبة بالإضافة لغرامة قدرت ب 10000 دولار أمريكي و400 ساعة عمل في خدمة المجتمع.[1]

إلى جانب هذا قد تعرضت بعض المرافق الحكومية للو م أ في السنوات الأخيرة ابتداء من عام 2016 إلى هجمات عديدة استهدفت كل من مواقع الوزارات والمؤسسات الرسمية، والتي تزامنت مع موعد الانتخابات بغية التأثير على الحملات الانتخابية، ما نتج عنه الكثير من الخسائر المادية.

ثالثا: كندا

قامت الحكومة الكندية كغيرها من الحكومات السابقة باستحداث عدة وحدات متخصصة في مكافحة الجرائم الإلكترونية والجرائم الخطيرة والعابرة للحدود، حيث أنشأت قوة شرطة وطنية متخصصة سميت "الوحدة الوطنية لمكافحة الجرائم السيبرانية"NC3"[2] تضم عدة ضباط متخصصين في مجال التحقيق في هذا النوع من الجرائم، حيث تعمل هذه الوحدة وفقا للإستراتيجية الوطنية للأمن السيبراني الموضوعة من طرف الحكومة الكندية، بالتنسيق مع وكالات إنفاذ القانون كالشرطة الكندية والإدارات والوكالات الفيدرالية، وكذا المركز الكندي لمكافحة الاحتيال، المركز الكندي للأمن السيبراني ووزارة العدل، واللجنة الكندية للإذاعة والتلفزيون والاتصالات اللاسلكية، وتقوم هذه الوحدة في سبيل التصدي لهذه الجرائم بمتابعتها وجمع المعلومات الاستخبارية بشأنها وتقديمها للشرطة الكندية.[3]

---

[1] تعتبر دودة موريس أول ديدان المعلومات التي انتشرت عبر الإنترنت في 02 نوفمبر 1988 من طرف روبرت تابان موريس الذي ولد في 08 نوفمبر 1965 بأمريكا وهو عالم كمبيوتر ورجل أعمال أمريكي وخبير تشفير ومحترف في الكمبيوتر والبرمجيات حيث كان يعمل في مختبرات "بيل" أين قدم إسهامات عديدة إلى شركة (Unix) مثل لغة البرمجة (bc) ونظام التشفير (el) المستخدم بواسطة كلمات المرور في نظام التشغيل هذا، ويقال أن موريس تابان الابن قد ورث هذه المهارات من موريس روبرت الأب الذي كان هو أيضا أحد مبتكري (CoreWar) وهي لعبة تستخدم لغة التجميع لترك الكمبيوتر خارج الذاكرة والتي تعتبر أحد فيروسات الكمبيوتر، وقد اشتهر موريس الابن بتصميمه لهذه الدودة والتي اعتمدت على فكرة بسيطة يطلق عليها تقنيا (Buffer Overflow) أي تجاوز سعة المخزن المؤقت، وهو مصطلح يستخدم في البرمجة للإشارة إلى خطأ برمجي يسبب تجاوز قدرة الذاكرة على التعامل مع البيانات المرسلة إليها، وفي بعض الحالات تعتبر مثل هذه الأخطاء البرمجية ثغرات أمنية تعطي للمخترق مساحة لزرع البرمجيات الخبيثة، وقد تطورت هذه التقنية سريعا بعد عدة أشهر من إطلاق دودة موريس ليشهد العالم فيروسات أخرى أطلق عليها اسم "هجمات الحرمان من الخدمات" حيث تعتبر "الفدية" أحدث فيروس يعمل بنفس الطريقة. لمزيد من التفاصيل ينظر مقال حول "دودة موريس"، على موقع الموسوعة الحرة "ويكيبيديا"، المتاح على الرابط التالي: https://ar.wikipedia.org/wiki تاريخ الاطلاع 2021/11/30 على الساعة 18:38.

[2] NC3 : The national cybercrime coordination unit, Disponible sur le site suivant : https://www.rcmp-grc.gc.ca/en/nc3 Consulté le 12/10/2021 à 17h15

[3] المرجع نفسه.

إلى جانب هذه الوحدة توجد "وحدة الدرك الملكي الكندي RCMP"[1] والتي تتكون من حوالي 18500 ضابط يمارسون مهامهم على المستوى الدولي والفيدرالي والإقليمي، بحيث يندرج اختصاصهم في متابعة الجرائم الإلكترونية، الجرائم المنظمة والعابرة للحدود والجرائم المالية، وكذا جرائم المخدرات والجرائم الخطيرة،[2] كما تجدر الإشارة إلى أنه تقوم هذه الوحدة والشرطة الملكية الكندية بدورات متخصصة مدة كل منها أربعة (04) أسابيع للتدريب على تقنيات وأساليب التحقيق في الجرائم الإلكترونية والتعامل مع الأدلة الرقمية، والتي يقوم بها مجموعة من المتخصصين في هذا المجال من خبراء وحتى ضباط شرطة ومحققين، إذ يتم تلقي هذه الدورات بكلية الشرطة في مدينة أوتاوا.[3]

وفي نفس إطار التحري في الجرائم الإلكترونية تم إنشاء ما يسمى "بمجلس الجريمة الإلكترونية ECC"[4] حيث يضم هو الآخر عدة ضباط شرطة وأشخاص مراقبين أكاديميين وحكوميين يعملون في الإدارات الحكومية والوزارات والوكالات على مستوى المقاطعات الفيدرالية لكندا، حيث يقوم هذا المجلس بدراسة قضايا الجرائم الإلكترونية والتحقيق فيها من طرف الضباط والخبراء الذين ينتمون إليه وتقديم نتائج هذه التحقيقات للجنة المعنية بالجرائم الإلكترونية (CACP)، كما يعمل هذا المجلس على ضمان عالم إنترنت آمن لمواطني كندا وحكوماتها، إذ يعمل بشكل جماعي وتعاوني مع مختلف الوحدات لتحديد الاحتياجات التكنولوجية داخل هذه الوحدات والأقسام لتطوير عمليات التحقيق ووسائل الكشف عن هذه الجرائم والتقليل من حدتها، علاوة على هذا يقوم المجلس بتقديم المشورة والدعم لضحايا هذه الجرائم.

ولعل من أبرز القضايا التي عالجتها هذه الوحدات الهجوم الذي تعرضت له مواقع إلكترونية في فبراير عام 2000 من بينها موقع السي إن إن(CNN)[5] وياهو (YAHOO)[6] وموقع الأمازون

---

[1] RCMP : Royal canadianmounted police, Disponible sur le site suivant : https ://www.rcmp-grc.gc.ca/ consulté le 12/10/2021 à 19h22

[2] المرجع نفسه.

[3] هشام محمد فريد رستم، الجوانب الإجرائية لجرائم المعلوماتية (دراسة مقارنة)، المرجع السابق، ص 49.

[4] ECC : Electronic crime cyber council, Disponible sur le site suivant : https://cacp.ca/e-crime-cyber-council-ecc-fr.htmlconsulté le 12/10/2021 à 19h45

[5] **السي إن إن كوم** يرمز له (CNN.COM) هو موقع إخباري تديره شركة السي إن إن، بدأ كأول موقع إخباري على شبكة الإنترنت، في 30 أغسطس 1995، يستلم هذا الموقع الأخبار من عدة وكالات إخبارية بالإضافة إلى التقارير التي تكتب من قبل موظفي السي إن إن، وبتاريخ 24 فبراير2003 أطلقت النسخة العالمية منه، والتي تركز على أخبار العالم بالإضافة إلى وجود فريق إخباري في كل من لندن وهونغ كونغو سيدني وأتلانتا.، كما تمت إعادة تصميم النسخة الإنجليزية من موقع سي إن إن كوم في 26مارس 2006.

[6] **شركة ياهو**Yahooهي شركة خدمات حاسوبية أمريكية مقرها في مدينة سانيفال بولاية كاليفورنيا، وتملكها شركة فرايزون ميديا، تأسست شركة ياهو الأصلية على يد جيري يانغو ديفيد فيلو في يناير 1994 وتم دمجها وإعلانها كشركة رسمية في 2 مارس 1995، حيث كان ياهو أحد رواد عصر الإنترنت المبكر في التسعينيات، وتقوم شركة ياهو بإدارة بوابة الشبكة العالمية إنترنت ودليل للشبكة، كما تقدم

(AMAZON)[1]من خلال رفض الخدمة الموزعة لهذه المواقع، ومن خلال التحقيقات التي أجرتها الشرطة الملكية الكندية بالتعاون مع المركز القومي الأمريكي تم تحديد مرتكبي هذا الهجوم والذين كانوا مجموعة تطلق على نفسها اسم "مافيا الأولاد" وتم القبض عليهم.[2]

ولنفس الهدف قامت حكومة كندا بإنشاء وحدة جديدة أطلق عليها اسم "المركز الكندي للأمن السيبراني[3]CCCS" في 01 أكتوبر 2018 موضوعة تحت مؤسسة أمن الاتصالات، والتي تعمل بالتعاون مع المركز الكندي للاستجابة لحوادث أمن الحاسوب Cert-Ca، وفرع أمن تكنولوجيا المعلومات بكندا، بحيث يهدف هذا المركز إلى ضمان الأمن الإلكتروني للكنديين سواء الأفراد أو المؤسسات وذلك من خلال التوجيه وتقديم المشورة في مجال التحقيق الرقمي إلى أجهزة إنفاذ القانون الكندية، وإنشاء آلية وطنية للإبلاغ عن حوادث جرائم الإنترنت للمواطنين الكنديين، إضافة إلى القيام بالحملات التوعوية والمنشورات الإرشادية التي يصدرها هذا المركز عن طريق القنوات ووسائل الإعلام أو عن طريق موقعه الرسمي.

تجدر الإشارة إلى أن هذا المركز لا يعتبر مركزا شرطيا لعدم توافره على ضباط شرطة قضائية بل يعتبر من قبيل المراكز التي تدعم عمل الشرطة في التحقيقات التي تقوم بها، بحيث يهدف أولا وأخيرا للوقاية من

منتجات ...=وخدمات أخرى من أشهرها خدمة" البريد الإلكتروني"، "محرك بحث"، و"خدمة إخبارية"، "ياهو" " ماسنجر"، "مشاركة الفيديو"، وموقعها على وسائل التواصل الاجتماعي في أوجها كان أحد أشهر المواقع في الولايات المتحدة الأمريكية، كما تعتبر بوابة ياهو من أكثر المواقع زيارة على الإنترنت، بأكثر من 130 مليون زائر مختلف شهريا، ومتوسط الزيارات لصفحات شبكة ياهو العالمية وصل ل 3,4 مليار زيارة يوميا منذ أكتوبر 2007، مما يجعلها واحدة من أكثر المواقع الأمريكية زيارة، حيث احتل المرتبة السادسة بين أكثر مواقع الويب زيارة على مستوى العالم في عام 2016.

[1]**أمازون كوم** Amazon.comصمم هذا الموقع للتجارة الإلكترونية والحوسبة السحابية حيث تأسس في 5 تموز1994 من قبل جيف بيزوسو يقع مقره في سياتل واشنطن، وهو أكبر متاجر التجزئة القائمة على الإنترنت في العالم من حيث إجمالي المبيعات والقيمة السوقية. بدأAmazon.comكمكتبة على الإنترنت، وتنوع لاحقا لبيع أقراص الفيديو الرقمية، وأقراص بلو-راي، والأقراص المدمجة، تنزيل وبث الفيديو، تنزيل وبث ملفاتMP3 ، وتنزيل الكتب الصوتية، والبرمجيات، وألعاب الفيديو، والإلكترونيات، والملابس، والأثاث، والمجوهرات. وتنتج الشركة أيضا الإلكترونيات الاستهلاكية، ولا سيما جهاز القراءة الإلكتروني كيندل، جهاز كيندلفاير وتلفاز فاير، وهو أكبر مزود في العالم لخدمات البنية التحتية السحابية، يوجد لأمازون مواقع منفصلة للبيع بالتجزئة في الولايات المتحدة والمملكة المتحدةوأيرلنداوفرنساوكنداوألمانياوإيطالياوإسبانياوهولنداوأستراليااوالبرازيلواليابانوالصينوالهندوالمكسيك، كما يقدم أمازون خدمة الشحن الدولي لبعض البلدان الأخرى لبعض المنتجات.، وفي عام 2016، تم إطلاق إصدارات اللغات الهولندية والبولندية والتركية لموقع أمازون الألماني في عام 2015 حيث تجاوز أمازون شركة وول مارت باعتبارها متاجر التجزئة الأكثر قيمة في الولايات المتحدة من حيث القيمة السوقية، وكان في الربع الثالث من عام 2016 رابع أكبر شركة عامة.

[2]محمد سيد سلطان، قضايا في أمن المعلومات وحماية البيئة الإلكترونية، المرجع السابق، ص 48.

[3] CCCS : Canadian centre for cyber security, Disponible sur le site suivant : https://cyber.gc.ca/en/guidance/cybercrime-0consulté le 23/10/2021 à 13h22

هذه الجرائم والهجمات الإلكترونية وتقديم الدعم والمشورة والمعلومات اللازمة لأجهزة الشرطة من أجل مساعدتها في ردع هذه الجرائم.

كما قامت الحكومة الكندية أيضا بتأسيس المركز الكندي لمكافحة الاحتيال المعلوماتي CAFC[1] والذي تتولى الشرطة الملكية الكندية ومكتب المنافسة في كندا، وشرطة مقاطعة أونتاريو إدارته بشكل مشترك، والمسئول عن مكافحة الاحتيال والغش عبر الإنترنت وذلك بمجرد تلقيه الشكاوى والتبليغات بشأن جرائم الاحتيال المختلفة، ليقوم فيما بعد بتحليلها وتجميع البيانات والوثائق المتعلقة بها من أجل الوصول إلى مرتكبيها، ويكون تقديم الشكوى أو البلاغ إما عن طريق موقع المركز على شبكة الإنترنت www.antifraudcentre.ca أو عن طريق الهاتف عبر الرقم التالي:(1-888-495-8501).[2]

[1] CAFC : Canadian anti-fraud centre, Disponible sur le site suivant : https://www.antifraudcentre-centreantifraude.ca/index-eng.htmconsulté le 23/10/2021 à 13h47

[2] لمزيد من التفاصيل يراجع الموقع الرسمي للمركز الكندي لمكافحة الاحتيال المعلوماتي المتاح على الرابط التالي:https://www.antifraudcentre-centreantifraude.ca/index-eng.htm تاريخ الاطلاع 2021/10/23 على الساعة 17:00.

من جانب آخر نجد دولة الصين والتي تعتبر من بين أول الدول التي بادرت بإنشاء وحدات متخصصة في التحقيق بالجرائم الإلكترونية وتطوير الوسائل والإمكانيات للتصدي لهذا الإجرام، إذ قامت بتأسيس وحدة شرطة متخصصة تدعى "**القوة المضادة للهكرة**" "The anti- haking syste" في 2000/08/22 والتي تتخذ من المعهد العالي للطاقة الفيزيائية مقرا لها، بحيث تختص بمراقبة عمليات الاحتيال الواقعة عبر الإنترنت إذ تلزم مستخدم شبكة الإنترنت بتسجيل نفسه لدى مكاتب الشرطة من أجل فرض رقابتها على كل مواطن والسماح له بالولوج إلى عالم الإنترنت، كما تقوم هذه الوحدة بتدريب العديد من حراس الأمن الإلكتروني على معرفة التقنيات وكيفية التعامل مع الهجمات الممكن حدوثها، كما تقوم بالتعاون مع أجهزة الإعلام المحلية في نشر معلومات حول الجرائم الإلكترونية التي تهددهم وكيفية التعامل معها، ومع معاهد البحوث المختلفة لتطوير برامج وقائية ضد تلك الفيروسات والهجمات.، وفي هذا الصدد أنشأت وزارة الأمن العام الصينية برنامجا مصمما لمحاربة العنف والتطرف عبر الإنترنت أطلق عليه اسم "**شرطة الإنترنت**" لمنع المستخدمين من تلقي معلومات ضارة من مواقع إلكترونية مشبوهة، بحيث يمكنه منع أو إلغاء الرسائل التي يكون مصدرها غير مشروع، كما خصصت رقما "110" لتقديم الشكاوى والبلاغات المتعلقة بالاعتداءات الإلكترونية، كما تم إنشاء 139 حسابا رسميا على الإنترنت على مستوى شرطة المقاطعات أو المدن وتم تكليف أصحاب تلك الحسابات من ضباط وخبراء بمراقبة نشاط المستخدمين في الفضاء الافتراضي، خاصة داخل مواقع التواصل الاجتماعي، حيث يعمل هذا الفريق على مدار الساعة على منع انتشار معلومات غير قانونية أو ألفاظ وعبارات غير لائقة ومكافحة جميع أشكال وصور الجريمة الإلكترونية التي قد تقع داخل هذه الفضاءات، بالإضافة إلى نشر كيفية التعامل مع هذه التهديدات والإنترنت بصفة عامة، وقد تلقى هذا الفريق حوالي 2000 بلاغ حول جرائم الإنترنت في نفس سنة إنشائه 2015 وقام بحذف أكثر من 200 ألف منشور غير لائق وكذا توجيه أكثر من 10 آلاف مستخدم بسبب عباراتهم ومنشوراتهم غير اللائقة، لمزيد من المعلومات ينظر هروال نبيلة هبة، الجوانب الإجرائية لجرائم الإنترنت، المرجع السابق، ص 107، وأيضا فيروز عوض الكريم ميرغني، إجراءات التحري والضبط في الجرائم الإلكترونية، المرجع السابق، ص261.

الفرع الثاني: على مستوى الدول اللاتينية

من أبرز الدول اللاتينية التي بادرت بإنشاء شرطة متخصصة في مكافحة جرائم الإنترنت نجد كل من فرنسا، اسبانيا، ألمانيا، وروسيا، سنتطرق بالتفصيل لكل منها فيما يلي:

أولا: فرنسا

يعتبر النظام الفرنسي من الأنظمة الأكثر تطورا وتماشيا مع الجرائم المستحدثة والجرائم الإلكترونية، من خلال تبني الحكومة الفرنسية إستراتيجية أمنية حديثة ومتطورة لمواجهة هذه التهديدات، وهذا من خلال العمل على تقوية القدرات الخاصة في مجال الأمن السيبراني وهو ما تجسد في إنشاء وحدات متخصصة في مجال مكافحة الجرائم الإلكترونية إلى جانب الوحدات التقليدية الأخرى،[1] ومن أبرز هذه الوحدات نجد:

[1] نظم المشرع الفرنسي الضبطية القضائية بموجب قانون الإجراءات الجزائية رقم 1426/57 المؤرخ في 1957/12/31، الجريدة الرسمية للجمهورية الفرنسية عدد 20، الصادرة بتاريخ 1958/01/08، والمعدل والمتمم بالقانون رقم 1109/2021 المؤرخ في 2021/08/24، حيث تنص المادة 12 منه على: "تمارس الشرطة القضائية تحت إشراف النائب العام، بواسطة ضباط وموظفين ووكلاء معينون في هذا الفصل".
كما حدد هذا القانون أعضاء الضبط القضائي في ثلاث فئات في المادة 15 منه، وذلك على النحو التالي:
الفئة الأولى تضم ضباط الضبط القضائي.
الفئة الثانية تضم معاوني الضبط القضائي.
الفئة الثالثة تضم الموظفون الذين منحوا بعض اختصاصات الضبط القضائي.
ولقد حددت المادة 16 من نفس القانون الفئة الاولى وهم:

1. العمد ومعاونوهم .
2. الضباط والرتباء من الحرس الإداري و الدركيون الذين امضوا في وظيفتهم خمس سنوات على الاقل ولا سيما الذين عينوا بقرارات من وزيري العدل و الدفاع بعد اخذ رأي لجنة معينة.
3. مفوضو الشرطة بالبوليس القومي وتضم هذه الفئة عدة أنواع:
   أ. مفوضي شرطة المدن و المحليات.
   ب. مفوضي الشرطة للمعلومات العامة
   ت. مفوضي الشرطة القضائية
   ث. مفوضيات المراقبة الإقليمية
4. ضباط الشرطة في البوليس القومي
5. المراقبين العموميين

أما الفئة الثانية فقد حددت أعضائها المادتان 20 و 21 من قانون الإجراءات الجنائية الفرنسي وهم ينقسمون الى قسميين:

1. عمال الضبط القضائي الذين أحصتهم المادة 20 من ذات القانون وهم:
   أ. الدركيون من غير مأموري الضبط القضائي
   ب. مفتشو الشرطة بالبوليس القومي الذين لم يمض على وجودهم بالخدمة أكثر من عامين.
2. عمال الضبط القضائي المعاونون والذين أحصتهم المادة 21 وهم:
   أ. العاملون في الإدارات البوليسية من غير من حددتهم المادة 20.

1) الوحدات التابعة للشرطة القضائية

نجد على مستوى مصالح الشرطة القضائية الفرنسية الوحدات التالية:

أ) المركز الوطني لمكافحة الجرائم المتصلة بتكنولوجيا المعلومات والاتصالات: L'office central de lutte contre la cybercriminalité liée aux technologies de l'information (L.O.C.L.C.T.I.C)

يعتبر هذا المكتب من أقدم المكاتب المختصة بمكافحة الجرائم الإلكترونية حيث تم إنشائه بموجب المرسوم البيوزاري رقم 2000-405 المؤرخ في 2000/05/15[1] على مستوى المديرية المركزية للشرطة القضائية التابعة لوزارة الداخلية، يساعده في نشاطه كل من وزارة الدفاع ووزارة الاقتصاد والمالية والصناعة، المديرية العامة للجمارك، وكذا المديرية العامة للمنافسة والاستهلاك وقمع الاحتيال وفقا لما جاء في المادة 01 من المرسوم سالف الذكر،[2] كما يتمتع باختصاص وطني يتحدد نطاقه في الجرائم المرتبطة بتكنولوجيات الإعلام والاتصال،[3] كما أنه يضم مجموعة كبيرة من ضباط الشرطة القضائية الذين يتمتعون بالخبرة الكافية في مجال الأنظمة المعلوماتية، وهم مقسمون على الوحدات التالية:

- **وحدة العمليات: La section opérationnelle**

تختص هذه الوحدة بالتحري في القضايا الإجرامية ذات الصلة بكل ما هو معلوماتي والكشف عن مرتكبي هذه الجرائم عن طريق تنسيق وتنشيط عمليات ملاحقة هؤلاء المجرمين، وتنقسم بدورها إلى أربع فرق من المحققين المختصين كالآتي:

ب. أفراد شرطة البلديات.

[1] المرسوم رقم 2000-405 المؤرخ في 2000/05/15، ويقصد بالمرسوم البيوزاري قرار تشترك في إصداره عدة وزارات.

[2] هذا ما تنص عليه المادة 01 من المرسوم الوزاري رقم 2000-405 المؤرخ في 2000/05/15 والتي تقضي :

"Il est crée au ministère de l'intérieur (direction générale de la police nationale, direction centrale de la police judiciaire) un office central de lutte contre la criminalité liée aux technologie de l'information et de la communication, sont associés aux activités de cet office le ministère de la défense (direction générale de la gendarmerie nationale) et le ministère de l'économie, des finances et de l'industrie (direction générale de la concurrence de la consommation et de la répressions des fraudes)."

[3] تنص المادة 02 من المرسوم رقم2000-405 سالف الذكر على:

"L'office a pour domaine de compétence les infractions spécifiques à la criminalité liée aux technologies de l'information et de la communication, dans les conditions fixées a l'article 3, sa compétence s'etend également aux infrations dont la commission est facilité ou liée à l'utilisation de ces technologies."

- فرقة البحث والتحري في الجرائم المتعلقة ببطاقات الدفع الإلكترونية.
- فرقة البحث والتحري في جرائم الاحتيال ضد موردي خدمات الاتصال.
- فرقة البحث والتحري في جرائم القرصنة الإلكترونية.
- فرقة البحث والتحري في جرائم النصب والاحتيال المعلوماتي[1]

- **وحدة المساعدات التقنية: . La plateforme d'assistance technique**

وهي عبارة عن بنية مجهزة ومزودة بأحدث التجهيزات الإلكترونية المتطورة والوسائل ذات المستوى التكنولوجي العالي، حيث تعمل على مساعدة مصالح التحري والتحقيق في الكشف عن الأدلة الإلكترونية وتحليلها وكذا توفير الرقابة التكنولوجية، كما تقوم بتكوين الضباط والمحققين في مجال التحقيق في الجرائم الإلكترونية.[2]

- **وحدة التحليل والتوثيق العملي: La cellule d'analyse et de documentation opérationnelle**

تعمل هذه الوحدة في معالجة البلاغات وتحليلها لمساعدة المصالح القضائية الأخرى في نشاطها، حيث تتكون هذه الوحدة من منصتين منصة فاروس(Pharos)، ومنصة (Info- Escroqueries) سيتم التفصيل فيهما في الباب الثاني من الدراسة بالتحديد في مرحلة تلقي البلاغات والشكاوى.

- **وحدة العلاقات الدولية:**

تعمل هذه الوحدة على ربط الاتصالات مع مختلف المصالح التي تعمل بالاشتراك مع هذا المركز من خلال تقديم وتبادل كل المعلومات اللازمة للتعرف أو البحث عن مرتكبي هذه الجرائم، [3] كما تجدر الإشارة إلى أن هذا المركز يمثل لفرنسا نقطة الاتصال المركزية في التبادلات الدولية، فهو من جهة يشارك على المستوى الوطني في تحريك وتنسيق الأعمال التحضيرية اللازمة، ومن جهة أخرى فهو يشارك في نشاطات المنظمات

[1] Adeline champagnat, L'office central de lutte contre la criminalité liée aux technologies de l'information et de la communication, revue de cybercriminalité cybermenace et cyberfraude, sous la direction de Irénebouhadana et William grilles, Edition IMODEV, paris, France, 2012, p 164

[2] نبيلة هبة هروال، الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات، المرجع السابق، ص 129.

[3] ينظر المادة 06 من المرسوم البيووزاري رقم 2000-405 سالف الذكر.

الدولية ومع كل المصالح المتخصصة في التحري في هذا النوع من الجرائم، كما أنه يقدم المساعدة للاتفاقيات الدولية في بحثها عن المعلومات المرتبطة بهذه الجرائم.[1]

ب) المديرية الفرعية لمكافحة الجريمة الإلكترونية: La sous direction de la lutte contre la cybercriminalité (S.D.L.C)

تضم وزارة الداخلية الفرنسية عدة مديريات وأجهزة أمنية على رأسها المديرية المركزية للشرطة القضائية (DCPJ)[2] والتي تتفرع عنها المديرية الفرعية لمكافحة الجريمة الإلكترونية هذه الأخيرة هي المسئولة عن محاربة الجرائم الإلكترونية بمختلف أصنافها، تم إنشاؤها بموجب مرسوم من رئيس الجمهورية في أفريل 2014، تضم هي الأخرى عدة أجهزة متخصصة تقوم كل منها بنشاط معين، أولها مكتب للتنسيق الاستراتيجي مسئول عن الاتصالات الداخلية والخارجية في مجال مكافحة الجرائم الإلكترونية، ومكتب الإنترنت مسئول عن جمع المعلومات من مقدمي الخدمات لصالح أجهزة الشرطة الوطنية، ومكتب التدريب الأولي على مكافحة هذه الجرائم، بالإضافة إلى قسم للتحليل الفني للهجمات السيبرانية يعتمد في عمله على التقنيات المتطورة لتحليل واكتشاف الدليل الإلكتروني والتنبيه بمخاطر الإنترنت بصفة عامة[3]

ج) المديرية العامة للاستخبارات الداخلية: La direction centrale du renseignement intérieur (D.C.R.I)

تختص هذه المديرية بقمع الجرائم على مستوى كامل التراب الوطني الفرنسي، وتلك التي تنشأ أو تكون مدعومة من قبل قوى خارجية أجنبية، والتي من شأنها الإضرار بأمن البلاد والمصالح الأساسية فيها، كالتجسس المعلوماتي والإرهاب المعلوماتي.[4]

---

[1] ينظر المادة 07 من نفس المرسوم.

[2] DCPJ : Direction centrale de la police judiciaire, Disponible sur le lien suivant : https://www.police-nationale.interieur.gouv.fr/Organisation/Direction-Centrale-de-la-Police-Judiciaireconsulté le 30/10/2021 à 18h56

[3] SDLC : Sous direction de la lutte contre la cybercriminalité, Disponible sur le lien suivant : https://www.police-nationale.interieur.gouv.fr/Organisation/Direction-Centrale-de-la-Police-Judiciaire/Lutte-contre-la-criminalite-organisee/Sous-direction-de-lutte-contre-la-cybercriminaliteconsulté le 01/11/2021 à 13h00

[4] Myriam Quémnéner, la coopération entre les organes de lutte contre la cybercriminalité, pour une stratégie de cyber sécurité français, revue de lamy droits des affaires, num° 87, France, 2013, p 02.

د) الوكالة الوطنية لأمن الأنظمة المعلوماتية: Agence nationale de la sécurité des systèmes d'information (A.N.S.S.I)

أنشأت هذه الوكالة في فرنسا في 07 جويلية 2009 مقرها باريس، وتعتبر وكالة وزارية تخضع لمصالح الوزير الأول، أما عن تشكيلة هذه الوكالة فهي تضم إدارة تتكون من مكتب وخلية للأمن السيبراني، تتفرع عنهما عدة أجهزة مسئولة عن عمليات المراقبة والخبرة التقنية وكذا الاستراتيجيات المتبعة في تحقيق أمن الأنظمة المعلوماتية، وتتمتع هذه الأخيرة بصلاحيات الضبط الإداري والقضائي معا، إذ تختص باقتراح القوانين والتنظيمات الخاصة بأمن الأنظمة المعلوماتية وتسهر على ضمان تطبيق النصوص حسب المعايير المحددة سلفا، كما تعمل على كشف الهجمات السيبرانية التي تستهدف هذه النظم والوقاية منها من خلال تطوير برامج حماية أمنية، وتحليل هذه الهجمات والتحري عن مرتكبيها وتقديم نتائج هذه التحقيقات إلى السلطات المختصة، كما أنها تقوم دائما بتوعية أفراد المجتمع كافة بخطورة هذه الجرائم وضرورة التبليغ عنها، [1] وبهذا فهي تلعب الدورين الوقائي والردعي معا.

هـ) فرق البحث والتحري عن جرائم الغش المعلوماتي:

زيادة على ما تقدم توجد هناك فرق مختصة بالبحث والتحري عن بعض الجرائم الإلكترونية، والتابعة لمحافظة شرطة باريس وضواحيها، أولها فرقة البحث والتحري عن الجرائم الماسة بالبرمجيات والاعتداء على حقوق المؤلف والملكية الفكرية[2](B.E.F.T.I) إذ تضم هذه الفرقة حوالي 30 شرطيا في صفوفها يختصون بمهمة التحري عن الجرائم الماسة بحقوق المؤلف وجرائم التقليد، وتنقسم بدورها إلى ثلاثة فرق أو خلايا تتمثل في خلية البحث والتحقيق، خلية المبادرة، خلية الدعم حيث تدعم أي جهة أخرى تتولى مسألة البحث والتحري في المسائل الإلكترونية.

إلى جانب هذه الفرقة توجد أيضا تحت سلطة محافظة باريس فرقة لمكافحة جرائم الغش المتعلقة بوسائل الدفع الإلكتروني[3](B.F.M.D) حيث تضم هي الأخرى حوالي 50 شرطيا مختص بمهمة التحري

[1] حسين ربيعي، آليات البحث والتحقيق في الجرائم المعلوماتية، آليات البحث والتحقيق في الجرائم المعلوماتية، أطروحة مقدمة لنيل شهادة الدكتوراه، تخصص قانون العقوبات والعلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة باتنة 1، 2016/2015، ص 161.

[2] BEFTI : La Brigade d'enquètes sur les fraudes aux technologies de l'information.

[3] BFMD : La Brigade des fraudes liée aux moyens de paiement.

في الجرائم المتعلقة بوسائل الدفع الإلكتروني بمختلف أنواعها كجرائم تزوير بطاقات الائتمان وكذا الاحتيال المالي...الخ.[1]

2) الوحدات التابعة لمصالح الدرك الوطني

لقد سخرت الحكومة الفرنسية إلى جانب رجال الشرطة القضائية، قوات درك وطنية لمواجهة الجرائم الإلكترونية، حيث ينعقد اختصاصها على كل من المستويين الوطني المركزي والإقليمي:

أ) على المستوى الوطني أو المركزي:

نجد على هذا المستوى وحدات الدرك الوطني التالية:

- **قسم الأنترنت التابع للمصلحة التقنية للبحوث القانونية والوثائقية: Le service technique de recherche judicaire et de documentation (S.T.R.J.D)**

يعتبر هذا القسم إحدى الوحدات الرئيسية في فرنسا تم إنشاؤه سنة 1998 في قلعة (Rosney – sous- bois)، ويتكون من عدة فرق للدرك الوطني، ويختص بجمع وتحليل الأدلة الرقمية المضبوطة من الجرائم الإلكترونية وتسهيل عملية التحقيق على المحققين من خلال عدة وحدات فرعية تتواجد داخله تتمتع باختصاص إقليمي وطني في مجال البحث والتحري عن الجرائم الإلكترونية، أهمها وحدة قمع الجرائم الماسة بالقصر عبر شبكة الإنترنت، وحدة التحقيقات بشأن جرائم الإنترنت، ووحدة الدعم والإسناد، [2] إذ تتمثل أغلب مهامها فيما يلي:

- معالجة المعلومات وتحليلها بطريقة علمية من خلال الخبراء والتقنيين وإعداد تقارير بذلك بناء على طلب وحدات الدرك الوطني أو القضاة.
- مساندة الوحدات السابقة على أرض الميدان وخاصة في حالات التفتيش المعقدة، وتقديم الدعم التقني لهم.
- البحث والتطوير من أجل فهم الوسائل والتقنيات الجديدة ومواكبة التطور التكنولوجي في مجال محاربة هذه الجرائم.[3]

[1] Myriam Quémnéner, la coopération entre les organes de lutte contre la cybercriminalité, op.cit, p 189-190.

[2] حسين ربيعي، آليات البحث والتحقيق في الجرائم المعلوماتية، المرجع السابق، ص 166.

[3] نبيلة هبةهروال، الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات، المرجع السابق، ص 134.

- **القسم المعلوماتي الإلكتروني التابع لمعهد البحوث الجنائية للدرك الوطني: L'institut de recherche criminelles de la gendarmerie national (I.R.C.G.N)**

تم إنشاء هذا القسم سنة 1992 على مستوى معهد البحوث الجنائية للدرك الوطني، حيث يخضع في عمله للإدارة العامة للدرك الفرنسي، تتمثل مهامه في تحليل البيانات المدمجة في الحواسيب الآلية والمتعلقة خاصة بالأعمال الاقتصادية والمالية خاصة المرتبطة بأرصدة المؤسسات وكذا أعمال قرصنة البرامج، وتقديمها للوحدات المختصة بالتحقيق في إطار المتابعات القضائية، كما يقوم بإنجاز الخبرات العلمية لمختلف مصالح الدرك الوطني، [1] وفضلا عن هذا يقوم أيضا بتكوين الضباط والمختصين في مجال التحقيق الجنائي بصفة عامة والتحقيق الإلكتروني بصفة خاصة.

- **المركز الوطني لتحليل الصور الإباحية: Centre national d'analyse des photos (C.N.A.I.P)**

تم إنشاء هذا المركز في أكتوبر 2003 بقلعة Rosney – sois – Bois وهو مركز مختص بجمع وترتيب الصور التي يتم ضبطها أثناء عمليات التفتيش والتحقيقات القضائية داخل الأنظمة المعلوماتية، حيث يعتمد في تحليل هذه الصور على عدة برامج مساعدة من بينها برنامج كشف الصور المسمى ب "Logiciel image seeker"[2] المصمم من الشركة الفرنسية التكنولوجية (LTU).[3]

- **مركز مكافحة الجرائم الرقمية: (CN3) Le centre de lutte contre les criminalités numériques**

تضم قوات الدرك وحدات مسئولة عن مراقبة الفضاءات الإلكترونية وإجراء التحقيقات بشأن الجرائم الواقعة داخلها، من خلال مراكز مختصة في مجال مكافحة هذا النوع من الإجرام على رأسها مركز مكافحة الجريمة الرقمية[4] المسئول عن تحديد الهجمات الإلكترونية والتحقيق فيها، فضلا عن أنه يقوم

---

[1] المرجع نفسه، ص 137.

[2] برنامج Logiciel image seeker هو عبارة عن برنامج لكشف الصور عبر إدخال أي صورة في الخانة المخصصة للبحث ليقوم هذا البرنامج بالبحث عن المعلومات والبيانات المتعلقة بها، واستخراجها جميعا، تم تصميمه من طرف الشركة الفرنسية التكنولوجية (LTU) ونظرا لأهميته البالغة أصبح يعتمد من طرف الخبراء في جميع المجالات وخاصة مجال التحليل الجنائي والتحقيقات القضائية

[3] Gendarmerie nationale : Gendarmerie vers cybercriminalité, Article disponible sur le site suivant : http://cyberpolice.over-bloc.comconsulté le 18/11/2021 à 15h30

[4] C3N : Le centre de lutte contre les criminalités numériques, Disponible sur le lien suivant : https://www.gendarmerie.interieur.gouv.fr/pjgn/scrcgn/le-centre-de-lutte-contre-les-criminalites-numeriques-c3nconsulté le 18/11/2021 à 19h26

بعمليات المراقبة المستمرة لهذه الفضاءات، وإجراء العمليات الاستباقية لمنع ووقاية الأفراد والمؤسسات من مخاطر الإنترنت.

ب) على المستوى الإقليمي

نجد على هذا المستوى ما يسمى بقسم الاستعلامات والتحقيقات القضائية (B.D.R.I.J) والذي يختص بتبادل الخبرات التقنية والاختصاصات بين رجال الدرك الوطني، ووحدات البحوث الإقليمية والتي تقوم بالمساهمة في مكافحة الجرائم الإلكترونية جنبا إلى جنب مع الوحدات المركزية السابقة، حيث تقوم بمعالجة الجرائم الخاصة المتعلقة بالمساس بالنظام المعلوماتي، كما أنها تمارس رقابة مشددة على مواقع الإنترنت وذلك بمشاركة قسم الإنترنت التابع للمصلحة التقنية للبحوث القانونية والوثائقية السابق.

وتجدر الإشارة أنه إلى جانب هذه الأقسام والمديريات قامت الحكومة الفرنسية بتحديث قوات الأمن الفرنسية لتصبح أكثر فعالية في مواجهة الجرائم الإلكترونية، حيث قام وزير الداخلية الفرنسي بتأسيس ما يسمى بتطبيقي الشرطة الرقمية والدرك الرقمي، حيث تعتبر هذه التقنية الجديدة وسيلة من خلالها يمكن لأي شخص استدعاء الشرطة أو الدرك عبر التطبيق المخصص لذلك، كما أن هذا التطبيق مسجل عليه بيانات ورخص السياقة ويمكنه التحقق من الهوية أيضا، وفي هذا الإطار تم توزيع نحو 60 ألف هاتف لوحي وهواتف ذكية لدى ضباط الدرك، ونحو 50 ألف لدى ضباط الشرطة، مزودة ببرامج متطورة وتطبيقات تعقب المجرمين، كما أن هذه التطبيقات ستكون متاحة أيضا عبر مواقع التواصل الاجتماعي، كما تجدر الإشارة إلا أن هذه الخدمات تم بداية العمل بها منذ فبراير 2018 إلى يومنا هذا.[1]

[1] هايدي صبري، "الشرطة الرقمية...أحدث وسائل مكافحة الجريمة في فرنسا"، مقال منشور يوم الخميس 2018/02/08، سا 07:40، على الرابط التالي: https://al-ain.com/article/digital-police-france تاريخ الاطلاع: 2021/06/11 سا 20:00.

يجدر القول أنه تعمل كل هذه الوحدات والأجهزة التابعة للشرطة والدرك الفرنسي معا لمكافحة جميع أشكال الإجرام بما فيه الإجرام المعلوماتي، ونتيجة هذا التعاون شرعت هذه الوحدات في إجراءات مراقبة الشبكات المعلوماتية منذ سنة 1998 من خلال تجنيد أكثر من 120 عون للقيام بهذه المهمة، بعد القيام بتكوينهم في مجال التحريات الخاصة بالجرائم المتصلة بالتكنولوجيات الحديثة، إذ خصصت نظاما خاصا يعمل بدعم من برنامجSimanalystلمراقبة المعاملات الخاصة بالبطاقات الإلكترونية وتحديد الجرائم المتعلقة بها، لتتطور فيما بعد الوسائل المستعملة في هذا المجال من خلال تجسيد مشروع بنك معلومات يجمع كل صور النشاطات الإجرامية الواقعة على الشبكات وبالخصوص جرائم الاستغلال الجنسي للأطفال، من خلال الاستعانة ببرامج معدة خصيصا لذلك كبرامج LOG IRC وp2p log وهو ما سمح لها سنة 2003 بتحصيل أكثر من 600,000 ألف معلومة حول جرائم الإنترنت، لمزيد من التفاصيل ينظر:

EricFiliol et Philippe Richard ; Cyber Criminalité-enquête sur les mafias qui envahissent le web, Edition Dunod, paris –France, 2006, p 149-150.

3) الوحدات التابعة للجمارك:

تعتبر الجمارك هيئة إدارية ضريبية تلعب دورا رئيسيا من خلال عمليات الرقابة الدائمة ومكافحة الجرائم الجمركية والغش الجمركي على المستوى الوطني والدولي، وفي ظل التطور التكنولوجي وما أفرزه من جرائم مستحدثة مست جميع القطاعات من أهمها القطاع الاقتصادي، برز دور الجمارك في مكافحة الجرائم الإلكترونية الماسة بهذا القطاع، حيث منحها القانون سلطات قضائية ودعمها بوسائل وأساليب متطورة من أجل التحري وضبط هذا النوع من الجرائم، مثل تدخلها في حجز البضائع المقلدة على مستوى مخازن البريد ومخازن التوصيل السريع التي تعتبر أفضل مكان يلجأ إليه المقلدون لإرسال سلعهم المباعة عبر شبكة الإنترنت والذي هو في تزايد مستمر في فرنسا، [1] لهذا السبب تم إسناد مهام قضائية لإدارة الجمارك الفرنسية فأصبح بذلك بمقدور بعض أعوان الجمارك المختصين مباشرة متابعات قضائية بموجب طلب من وكيل الجمهورية أو قاضي التحقيق، وهذا ما تقرر بموجب صدور القرار المؤرخ في 2002/12/05 المتضمن إنشاء الإدارة المركزية للجمارك القضائية، التي تضم أعوان جمارك مؤهلين اصطلح عليهم اسم "ضباط الجمارك القضائية" وهم تابعون للمديرية العامة للجمارك الفرنسية، وقد تدعم عمل هذه الهيئة بصدور قانون (Per Ben 2) الصادر في 2004/03/04 المتعلق بضرورة تطوير مرفق العدالة وفق تطور الجريمة، وهذا ما أعطى حرية كبيرة لمصالح الجمارك بممارسة أعمال التصدي للجرائم المنظمة، وبتاريخ فيفري 2009 تم صدور قرار آخر يقضي بإنشاء ما سمي ب "خلية الجمارك المعلوماتية" هذا ما شكل نقطة تحول في عمل واختصاص هذه الفئة بدخولها عالم البحث والتحري عن الجرائم الإلكترونية، إذ تم الإطاحة بشبكة دولية مختصة بتقليد المنتجات القادمة من الصين وبيعها في أوروبا والتي جنى أفرادها ما يقارب 4 مليون أورو تم تبييضها بسويسرا[2]، وغيرها من العمليات التي قامت بها هذه الخلية وهذا من خلال إتباع أساليب خاصة أقرها لها القانون الفرنسي تتمثل في:

- **أسلوب التدخل في عمليات الشراء عبر شبكة الإنترنت:**

أعطى القانون لخلية الجمارك المعلوماتية صلاحيات واسعة لكشف هذا النوع من الجرائم، إذ تقوم في سبيل ذلك بمراقبة عمليات التبادل الإلكتروني للسلع والمنتجات، وكذا القيام بعمليات الشراء مباشرة من

[1] Myriam Quéméner, la coopération entre les organes de lutte contre la cybercriminalité, pour une stratégie de cyber sécurité français, op.cit, p 03.

[2] حسين ربيعي، آليات البحث والتحقيق في الجرائم المعلوماتية، المرجع السابق، ص 169.

المواقع الإلكترونية محل المراقبة وذلك بهدف تحديد طبيعة المنتوجات المقلدة أو المحظورة والوصول إلى بائعيها وتحديد مسارهم.

- **أسلوب التسرب ضمن مواقع القمار الإلكترونية:**

سمح القانون الصادر في 2012/05/12 لضباط الجمارك القضائية بالمشاركة في ألعاب القمار الإلكترونية التي تتم عبر الإنترنت[1]، وذلك بأسماء مستعارة لعدم كشف هويتهم، بهدف كشف عمليات تبييض الأموال والاحتيال الإلكتروني وكل الجرائم ذات الصلة بذلك.

- **أسلوب الاتصال بالغير:**

يتمثل هذا الأسلوب في اتصال أعوان الجمارك بأي شخص يحوز على معلومات أو أدلة من شأنها الكشف عن عمليات احتيال أو أي نشاطات غير مشروعة تتم عبر شبكة الإنترنت، بحيث تعمل خلية الجمارك المعلوماتية على تجميع هذه المعلومات وتحديد مسار البضاعة محل الجريمة وتحديد مسار الأموال المستعملة أو الناتجة عن هذه الجرائم.[2]

وفي سبيل التصدي الأمثل لهذا النوع من الإجرام المستحدث تتشارك خلية الجمارك المعلوماتية تبادل المعلومات بشأن هذه الجرائم مع العديد من الإدارات الأخرى من بينها المركز الوطني لمكافحة الجرائم المتصلة بتكنولوجيا المعلومات والاتصالات (L.O.C.L.C.T.I.C)، المديرية العامة للمنافسة والاستهلاك وقمع الاحتيال(D.G.C.C.R.F)، وكذا الإدارة الوطنية للتحقيقات الضريبية (D.N.E.F)، وهذا من خلال منصة فاروس(PHAROS)، وأيضا قامت هذه الخلية بتوقيع العديد من بروتوكولات التعاون مع مقدمي خدمات الإنترنت وشركات الاستضافة.

---

[1] يعتبر القمار الإلكتروني من أخطر أنواع القمار حيث يتم عن طريق الولوج إلى مواقع إلكترونية مخصصة لألعاب القمار، إما بغرض الترفيه أو كسب الأموال، وقد يتطور ليصبح عند البعض من الشباب إدمانا خطيرا بحث يقضي جلهم أغلب أوقاتهم أمام أجهزة الكمبيوتر أو الهاتف للعب والمقامرة، وقد أكدت عدة دراسات أنه يمكن أن يسبب حالة مرضية تسمى (Pathologicalgambling) أي المقامرة المرضية، حيث يؤثر على الجانب النفسي والجسدي والمادي للإنسان، ومن الناحية القانونية فإن بعض الدول تعاقب على القمار مهما كانت وسيلته مثل المملكة العربية السعودية التي تعتبر القمار مخالفا للقانون وتعاقب عليه بالسجن والتعزير وذلك وفقا لأحكام الشريعة الإسلامية.

[2] Gérard Schoen, La douane face a la cybercriminalité, Revue de cybercriminalité cybermenave et cyberfraude, sous la direction de Irène bouhadana et William dgilles, editionImodev, paris, France, 2012, pp 169 -170.

لمزيد من التفاصيل ينظر حسين ربيعي، آليات البحث والتحقيق في الجرائم المعلوماتية، المرجع السابق، ص 169- 170.

كما تلتزم خلية الجمارك المعلوماتية بالحفاظ على علاقاتها مع الإدارات في البلدان الأخرى من خلال الاجتماعات التي تنظمها دوريا ومن خلال الدورات التدريبية التي يخضع لها الضباط المنتمين لهذه الخلية والتي تكون عادة في بلدان أخرى، وهذا كله لتعزيز التعاون بين الدول وكذا إيجاد أساليب ناجعة لمكافحة الإجرام المعلوماتي، ومن بين أشهر العمليات أو القضايا التي عالجتها هذه الخلية عملية "بانجيا السادسة" التي جرت في الفترة من 18 إلى 25 يونيو 2013 وشاركت فيها 99 دولة، حيث تم ضبط أكثر من 300812 سلعة مهربة بما فيها أدوية صيدلانية مقلدة.[1]

ثانيا: على مستوى بعض الدول اللاتينية الأخرى

في إسبانيا تشكل إجراءات مكافحة الجرائم الإلكترونية جزءا مهما من الإستراتيجية الأمنية الوطنية التي اعتمدتها الدولة في ديسمبر 2013 والتي يجري تحديثها باستمرار، فنتيجة لذلك قامت الحكومة الاسبانية باستحداث وحدة التحريات المركزية لأمن معلومات جرائم الإنترنت التي تعمل مع الإدارة المركزية لوزارة الداخلية الإسبانية، حيث تهدف إلى مراقبة مرتكبي الجرائم المستحدثة والعمل على إحباط مخططاتهم الإجرامية، [2] كما استحدث مكتب المدعي العام الإسباني تخصصا في مجال الجريمة الإلكترونية إذ منذ عام 2011 قامت الشبكة الوطنية للمدعين العامين المختصة تحديدا بملاحقة هذا النوع من الجرائم بنشر قرابة 150 مدعيا عاما على الأراضي الوطنية في عواصم المقاطعات وفي عدد من المدن المختارة، بحيث تكون هذه الوحدات التابعة للمدعي العام على اتصال دائم بالشرطة القضائية وكذا مع غيرها من الهيئات المختصة بمكافحة الجرائم الإلكترونية، وتشمل هذه الهيئات الهيئة الإسبانية لحماية البيانات، المركز الوطني لحماية البنى التحتية الحيوية، والمعهد الوطني للأمن السيبراني، المركز الوطني لعلوم التشفير، القيادة المشتركة للدفاع السيبراني، وكذلك منظمات وكيانات من القطاع الخاص مثل الهيئات المصرفية والأخرى المسئولة عن خدمات الاتصالات وغيرها.[3]

وعن ألمانيا التي تزداد فيها الجرائم الإلكترونية بوتيرة مرتفعة حيث تم زيادة معدل الجريمة عام 2020 بنسبة 80% وهذا راجع بشكل كبير إلى انتشار جائحة كورونا وما خلفته من آثار سلبية على جميع

[1] مقال منشور على الموقع الرسمي للمنظمة الدولية للشرطة الجنائية (للإنتربول)، متاح على الرابط التالي: https://www.interpol.int/ar/1/1/2012/54 consulté le 18/11/2021 à 16h00 تاريخ الاطلاع: 2021/06/17 على الساعة 19:00.

[2] نبيلة هبةهروال، الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات، المرجع السابق، ص 108

[3] قرار الجمعية العامة للأمم المتحدة رقم 73/187، حول مكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية، الدورة الرابعة والسبعون، البند 109، الصادر بتاريخ 30 جويلية 2019، ص 90-91.

الميادين، [1] ونتيجة لهذا الارتفاع وضعت الحكومة الألمانية عدة أقسام متخصصة في الإجرام المعلوماتي داخل وحدات ومكاتب الشرطة التقليدية، حيث استحدثت وزارة الداخلية قسم مكافحة جرائم الإنترنت والتابع للمكتب الاتحادي للشرطة الجنائية [2](BKA)، وكذا المركز الأوروبي للجرائم الإلكترونية[3](**EC3**)، كما قامت بإنشاء فرقة للعمل المشترك لمكافحة الجرائم الإلكترونية [4](J-CAT)، حيث تعمل هذه الفرق والأقسام بالتنسيق مع مختلف مراكز الشرطة القضائية في مختلف المدن الألمانية، وذلك من خلال التحري في الجرائم التي تصل إلى علمها ومحاولة الوصول إلى المجرمين ومتابعتهم، [5] كما تم تخصيص الرقم الموحد التالي (01608000116) للتواصل مع هذه الأجهزة وتقديم البلاغات بشأن كل الجرائم بما فيها الجرائم الإلكترونية.[6]

أما عن روسيا فقد قامت بإنشاء وحدة للشرطة القضائية الإلكترونية تابعة لوزارة الداخلية الروسية في عام 2018، تضم عددا من الضباط المختصين في معالجة الجرائم الإلكترونية، كما يعمل المكتب المركزي الوطني للإنتربول الروسي(NCB)على متابعة هذه الجرائم بصفة خاصة.[7]

مما تقدم ذكره نرى أنه نتيجة تطور الدول الأجنبية في مجال الإلكترونيات والتعامل مع الأجهزة الإلكترونية وخاصة بعد الهجمات الشهيرة التي تعرضت لها هذه الدول من قبل أشخاص على قدر كبير من المعرفة والذكاء والمهارة في هذا المجال، فإنها لا تزال في استحداث دائم ومستمر لأجهزة ووحدات شرطية مختصة في التحري والتحقيق في الجرائم الإلكترونية أو المعلوماتية وهذا بالتنسيق دائما مع الوحدات التقليدية، إلا أنه يوجد بعض التفاوت بين هذه الدول في عدد الأجهزة المختصة ومدى توفير الدورات التكوينية

[1] Oliver Noyan, Montée en flèche de la cybercriminalité en Allemagne,12/05/2021, Article disponible sur le site suivant :https://www.euractiv.fr/section/economie/news/dramatischer-anstieg-der-cyberkriminalitaet-in-deutschland/,Consulté le 16/06/2021, a 18h00

[2] BKA : L'office fédéral de police criminelle.

[3] EC3 : Europeancybercrime center.

[4] J-CAT : Joint cybercrime action taskforce.

[5] La chasse aux criminels sur internet, Article disponible sur le site suivant :https://www.deutschland.de/fr/topic/politique/lutter-contre-la-cybercriminalite-la-police-allemande-et-europol2021/04/18 Consulté le 16/06/2021 à 18h19

[6] La police Allemagne, Article disponible sur le site suivant : https://handbookgermany.de/fr/rights-laws/police.html le 16/06/2021, à 18h30

[7] How interpol supports Russia to tackle international crime, Article disponible sur le site suivant :https://www.interpol.int/Who-we-are/Member-countries/Europe/RUSSIAconsulté le 16/06/2021, à 19h00

والتدريبية لهؤلاء الضباط، وهذا لا ينقص من المجهودات التي بذلتها هذه الدول في سبيل محاربة هذا النوع من الإجرام إذ تعتبر من الدول السباقة في هذا المجال.

المطلب الثاني: وحدات البحث والتحري عن الجرائم الإلكترونية على مستوى الدول العربية

ناهيك عن الدول الأجنبية والتي استحدثت عدة وحدات وفرق مختصة في متابعة الجرائم الإلكترونية قد تفطنت بعض الدول العربية لخطورة هذا النوع من الإجرام وسارعت لإيجاد سبل للتصدي له من خلال سن بعض التشريعات والقوانين التي تهدف لتجريم مختلف أشكال الإجرام المعلوماتي ومعاقبة مرتكبيه هذا من جهة، ومن جهة أخرى قامت باستحداث فرق خاصة مؤهلة علميا وعمليا لمتابعة هذه الجرائم والتحري فيها، ومن هذا المنطلق سوف نتطرق بالدراسة أولا لبعض الدول العربية بصفة عامة، ثم إلى ما استحدثته دولة الجزائر بصفة خاصة.

الفرع الأول: على مستوى الدول العربية بصفة عامة

كما أشرنا سابقا فإن معظم الدول العربية سارعت لإنشاء فرق وأجهزة مختصة للتصدي الأمثل للجرائم الإلكترونية، وهذا سواء كانت من الدول المتقدمة أو حتى النامية باعتبارها ليست بمنء عن هذا الإجرام، ولعل أبرز هذه الدول نجد الإمارات المتحدة، المملكة العربية السعودية، مصر، والأردن.

أولا: الإمارات المتحدة

تسعى دولة الإمارات العربية المتحدة لأن تكون من أكثر البلدان أمانا من خلال نصها لقوانين اتحادية تحافظ على حقوق وحريات المواطنين وتحميهم من مختلف أشكال الجرائم والتي من بينها الجرائم الإلكترونية، حيث أصدرت القانون الاتحادي رقم (35) لسنة 1992 المتضمن قانون الإجراءات الجزائية[1]، والذي نظم من خلال نصوصه الضباط الذين تعهد لهم صفة الضبطية القضائية والمسمون في هذا القانون بمأموري الضبط القضائي، والمنصوص عليهم بموجب المادة 33 من هذا القانون، [2] كما بين المهام

[1] القانون الاتحادي رقم (35) لسنة 1992 المتضمن قانون الإجراءات الجزائية، الجريدة الرسمية عدد 233 مكرر الصادرة بتاريخ 1992/01/26.

[2] تنص المادة 33 من هذا القانون على ما يلي: "يكون من مأموري الضبط القضائي في دوائر اختصاصهم:

1. أعضاء النيابة العامة.
2. ضباط الشرطة وصف ضباطها وأفرادها.
3. ضباط وصف ضباط وأفراد حرس الحدود والسواحل.
4. ضباط الجوازات.
5. ضباط الموانئ البحرية والجوية من رجال الشرطة أو القوات المسلحة.
6. ضباط وصف ضباط الدفاع المدني.
7. مفتشو البلديات.

الموكلة لهؤلاء الضباط بشأن متابعة الجرائم بمختلف أشكالها من بينها الجرائم الإلكترونية، وتأكيدا على هذا أصدرت الحكومة الإماراتية القانون الاتحادي رقم (5) لعام 2012 المعدل والمتمم بالقانون الاتحادي رقم (12) لعام 2016 المتعلق بمكافحة جرائم تقنية المعلومات[1]، إذ بين هذا القانون أنواع الجرائم وكذا العقوبات المقررة لها، وكيفيات التبليغ عنها لدى السلطات والوحدات المختصة بهذا النوع من الجرائم، ومن بين هذه الوحدات قد أنشأت إمارة دبي قسما مختصا بنظر الجرائم الإلكترونية موجود على مستوى كل من الإدارة العامة للتحريات والمباحث الجنائية و إدارة المباحث الإلكترونية لدى مراكز شرطة دبي، حيث يقوم هذا القسم بالتحري عن هذه الجرائم من خلال ما يصله من معلومات وبلاغات حولها، فهو يتيح إمكانية تقديم الشكاوى والبلاغات بخصوص الجرائم المرتكبة عبر الإنترنت من خلال أرقام ومواقع إلكترونية مخصصة لهذا الغرض، فقد أشار نائب القائد العام لشرطة دبي بأن الجرائم إ والاقتصادية تعتبر أبرز الظواهر الإجرامية الحديثة على المجتمعات الخليجية وتحديدا المجتمع الإماراتي، [2] حيث لم يكن هذا النوع من الجرائم معروفا قبل 40 عاما، وقد تضاعف خلال السنوات الماضية والحالية، حيث استقبلت إدارة مكافحة الجريمة إ 278 بلاغا في عامها الأول 2008 وارتفع إلى 436 بلاغ في عام 2009 ليتصاعد العدد إلى 445 بلاغ عام 2010، و588 بلاغ عام 2011، أما في عام 2012 وصل العدد إلى 772 وفي عام 2013 تجاوز العدد 1000 بلاغ.[3]

كما قامت هذه الوحدة بمعالجة العديد من هذه البلاغات والقضايا من بينها قضية اختلاس أموال تعد الأولى من نوعها، تمثلت في سرقة أموال طائلة من حسابات لعملاء في 13 بنك محلي وعالمي، قام بارتكابها مهندس حاسوب آسيوي يبلغ من العمر 31 عاما، وذلك بعد توصل إدارة مكافحة الجرائم الإلكترونية على 14 بلاغ من بنوك محلية أفادت عن تعرض بعض عملائها لاختلاسات مالية من حساباتهم الشخصية وتحويل هذه المبالغ على حسابات وهمية له ودفعها في مشتريات خارجية دون علمهم، وعلى إثر هذه البلاغات انتقلت مصالح شرطة دبي متمثلة في فرقة مكافحة الجرائم الإلكترونية وخبراء في جرائم

8. مفتشو وزارة الصحة.

9. الموظفون المخولون صفة مأموري الضبط القضائي بمقتضى القوانين والمراسيم والقرارات المعمول بها".

[1] القانون الاتحادي رقم (5) لعام 2012 المعدل والمتمم بالقانون الاتحادي رقم (12) لعام 2016 المتعلق بمكافحة جرائم تقنية المعلومات، الجريدة الرسمية عدد 597 الصادرة في 2016/05/31، المعدل بالقانون الاتحادي رقم (2) لعام 2018، ج ر عدد 633 الصادرة في 2018/07/31.

[2] احتلت الإمارات المتحدة طليعة دول الشرق الأوسط الأكثر استهدافا وعرضة للجرائم المالية الإلكترونية بنسبة تقدر ب 38,8 % تليها المملكة العربية السعودية بنسبة تقدر ب 29,3 %، تليهم دولة قطر بنسبة 09,64%، والكويت بنسبة 06,92%.

[3] مجمع البحوث والدراسات، الجريمة الإلكترونية في المجتمع الخليجي وكيفية مواجهتها، أكاديمية السلطان قابوس لعلوم الشرطة، جامعة نايف بن عبد العزيز للبحوث الأمنية، عمان، 2016، ص ص 37-38-40.

الحاسوب إلى البنوك المحلية المستهدفة وقاموا بفحص الحاسبات الآلية بها حيث تبين أن شخصا استطاع الدخول على شبكات البنوك الإلكترونية وتمكن من تحويل بعض المبالغ المالية عن طريق الإنترنت، كما توصل الخبراء إلى أن الجاني قام باستغلال أحد مقاهي الإنترنت لتنفيذ هذه العمليات، وبعد جهود وتحريات كبيرة تم ضبط المتهم واتضح أنه تمكن من الدخول لهذه الحسابات عن طريق اختراقها وزرع برامج خاصة لتسهيل الدخول لحسابات العملاء مع العلم أن المتهم قد ضبط سابقا في جرائم مماثلة من بينها قضية بيع مصنفات وبرامج فنية.[1]

إلى جانب هذا تم تخصيص فرقة شرطة إلكترونية لمكافحة الابتزاز الإلكتروني والتي تختص بالتحري في جرائم التهديد والابتزاز الإلكتروني تابعة لكل مدن الإمارات العربية المتحدة (دبي، أبو ظبي، الشارقة، عجمان...)،[2] حيث تتميز هذه الفرق بالمعرفة الجيدة بمهارات الكمبيوتر والتعامل مع الفضاءات الإلكترونية، إذ استقطبت الإمارات كفاءات بشرية عديدة ومؤهلة للتعامل مع هذه الجرائم علاوة على قيامها بإعداد وتنظيم ورشات ومؤتمرات علمية وعملية حول مناقشة السبل الكفيلة بمواجهة هذه الجرائم، وفي هذا الصدد قامت بالتنسيق مع الشرطة الاتحادية الأمريكية (FBI)من أجل تنظيم دورات تكوينية لفائدة ضباط الشرطة القضائية وتأهيلهم على الطرق المستجدة والحديثة في كيفية التحقيق في الجرائم الإلكترونية.[3]

ولم تتوقف جهود الحكومة الإماراتية على تخصيص وحدات ومواقع إلكترونية لمكافحة هذه الجرائم، بل أطلقت النيابة العامة الاتحادية الإماراتية في يونيو 2018 تطبيق لحماية المواطنين من مختلف أشكال التهديدات الإلكترونية أطلق عليه اسم: **"مجتمعي آمن"** بحيث يتميز هذا التطبيق بسهولة التحميل سواء على جهاز الهاتف المحمول أو حتى جهاز الكمبيوتر، يتيح للجميع إمكانية الإبلاغ عن أي جريمة أو اشتباه عن وقوعها عبر مواقع التواصل الاجتماعي وكل شبكات ومواقع الانترنت والذي من شأنه أن يهدد أمن

[1] مجمع البحوث والدراسات، الجريمة الإلكترونية في المجتمع الخليجي وكيفية مواجهتها، المرجع السابق، ص 45.

[2] حيث يتم التواصل مع هذه الفرق إلكترونيا أو عبر الخط التالي (4444)، لمزيد من التفاصيل ينظر الموقع الرسمي لهيئة تنظيم الاتصالات والحكومة الرقمية لدولة الإمارات العربية المتحدة، المتاح على الرابط التالي: https://www.tdra.gov.ae/ar/media-hub/cyber-blackmailing.aspx تاريخ الاطلاع 2021/06/13 على الساعة 20:15.

[3] فايز خليفة بن يعروف، المواجهة التشريعية والأمنية للجرائم المتصلة بمواقع التواصل الاجتماعي، مذكرة مقدمة لنيل شهادة الماجستير في البحث الجنائي، أكاديمية شرطة دبي، الشارقة، الإمارات، 2019، ص 179.

وسلامة المجتمع، كما يضمن هذا التطبيق السرية التامة لهوية المبلغ ليتخذ الإجراءات المناسبة والسريعة من خلال مكتب التحقيقات الاتحادي التابع للنائب العام.[1]

ثانيا: المملكة العربية السعودية

في إطار تنامي ظاهرة الإجرام الإلكتروني في المملكة العربية السعودية بشكل كبير ومستمر، ونتيجة لضعف السلطات القضائية التقليدية[2] في مواجهة هذا النوع من الإجرام، قامت الحكومة السعودية بتأسيس وحدات وفرق مختصة لمحاربة هذا النوع من الجرائم هذا من جهة، ومن جهة ثانية استحدثت تطبيقات وأرقام متعددة لاستقبال بلاغات المواطنين حول هذه التهديدات وهي في تحيين دائم ومستمر لهذه التطبيقات، من بين أهم هذه الوحدات والأقسام نجد قسم مكافحة الجرائم الإلكترونية التابع لمديرية الأمن العام للمملكة، والذي يختص باستقبال البلاغات والتحري في هذه الجرائم وذلك نظرا لخبرة موظفيه في التعامل مع هذه التهديدات والطبيعة التقنية لها، وتعقبه للمجرمين المعلوماتيين والكشف عنهم وتوجيههم للقضاء، كما أسست الحكومة السعودية هيئة لمكافحة الابتزاز الإلكتروني وهي عبارة عن

[1] وقد اختلفت تسميات هذه التطبيقات عبر إمارات الدولة، فأطلق اسم "الأمين" في إمارة دبي واسم "أمان" في إمارة أبو ظبي، واسم "نجيد" في إمارة الشارقة، وهذا لتشجيع المواطنين على المبادرة بالتبليغ عن مختلف التهديدات الإلكترونية حماية لهم ولمصالحهم، وكذا إبراز الدور الإيجابي للمجتمع في التعاون مع الأجهزة الأمنية للتصدي لهذه الجرائم. لمزيد من التفاصيل ينظر المواقع الرسمية لهذه التطبيقات والأرقام المخصصة للاتصال على الروابط التالية:

- موقع الأمين للقيادة العامة لشرطة دبي http://www.alameen.ae/ar/والرقم المجاني: 8004888
- موقع الأمان للقيادة العامة لشرطة أبو ظبي mailto:aman@adpolice.gov.ae والرقم المجاني: 8002626.
- موقع نجيد للقيادة العامة لشرطة الشارقةhttp://moi.gov.ae/ar/media.center/news/news2105.aspx والرقم المجاني: 800151.

[2] المنصوص عليها بموجب نظام الإجراءات الجزائية السعودي والصادر سنة 2013، والذي ينظم إجراءات رفع الدعوى الجزائية وكذا إجراءات الاستدلال والتحقيق في الجرائم، والأشخاص الذين يتمتعون بصفة الضبطية القضائية والمسمون في هذا النظام ب "رجال الضبط الجنائي"، حيث نصت المادة 24 من هذا النظام على: "رجال الضبط الجنائي هم الأشخاص الذين يقومون بالبحث عن مرتكبي الجرائم وجمع المعلومات والأدلة اللازمة للتحقيق وتوجيه الاتهام".

وجاءت المادة 26 من ذات القانون لتبين من يقوم بأعمال الضبط الجنائي إذ تنص على: "يقوم بأعمال الضبط الجنائي - بحسب المهمات الموكولة إليه – كل من:

1. أعضاء هيئة التحقيق والادعاء العام في مجال اختصاصهم.
2. مديري الشرط ومعاونيهم في المدن والمحافظات والمراكز.
3. الضباط في جميع القطاعات العسكرية – كل بحسب المهمات الموكولة إليه – في الجرائم التي تقع ضمن اختصاص كل منهم.
4. محافظي المحافظات ورؤساء المراكز.
5. رؤساء المراكب السعودية البحرية والجوية في الجرائم التي ترتكب على متنها.
6. رؤساء مراكز هيئة الأمر بالمعروف والهي عن المنكر في حدود اختصاصهم.
7. الموظفين والأشخاص الذين خولوا صلاحيات الضبط الجنائي بموجب أنظمة خاصة.
8. الجهات واللجان والأشخاص الذين يكلفون بالتحقيق بحسب ما تقضي به الأنظمة".

هيئة حكومية متخصصة في متابعة جرائم الابتزاز الواقعة من داخل المملكة أو خارجها، وذلك من خلال فريق كبير من المختصين في معالجة الابتزاز والتهديد بطريقة تقنية، كما تمتلك فريق تقني يعمل على تعقب المجرمين والقبض عليهم وإحالتهم للنيابة العامة، بحيث تتيح هذه الهيئة رقما خاصا للمواطنين لتقديم بلاغاتهم كما تتيح لهم إمكانية التواصل مع محامي مختص في الجرائم الإلكترونية وعرض مشكلتهم عليه للتمكن من مساعدتهم وتقديم الاستشارة القانونية لهم بخصوص هذه الجرائم.[1]

فوفقا لتقارير عديدة قامت بها الأجهزة الأمنية فإن قضايا الابتزاز والتهديد الإلكتروني وكذا قضايا تخزين المواد الإباحية تحتل نسبة 76% من الجرائم الإلكترونية الواقعة بالسعودية تليها قضايا التحويلات البنكية غير المشروعة والاستخدام غير المشروع لبطاقات الائتمان وتزويرها، تليها جرائم الفدية التي تمس المؤسسات والشركات الكبرى، [2]فقد تعرضت المملكة العربية السعودية ودولة قطر عام 2013 إلى هجمات إلكترونية استهدفت كل من شركة أرامكو السعودية للنفط وشركة رأس غاز القطرية، وهجمات أخرى على مواقع إلكترونية حكومية منها وزارة الداخلية أدت إلى تعطيل بعض المرافق مؤقتا.

ثالثا: مصر

يتولى عملية التحري والتحقيق بصفة عامة مأموري الضبط القضائي والمنصوص عليهم في قانون الإجراءات الجنائية رقم 150 لسنة 1950 المعدل بالقانون رقم 189 لسنة 2020، حيث تنص المادة 21 من هذا القانون[3]أنه يقوم مأمور الضبط القضائي بالبحث عن الجرائم ومرتكبيها وجمع الاستدلالات بشأنها

[1]مقال حول "هيئة مكافحة جرائم الابتزاز الإلكتروني" منشور على الموقع الرسمي لوزارة الداخلية للمملكة العربية السعودية، والمتاح على الرابط التالي: https://www.moi.gov.sa تاريخ الاطلاع 2021/06/15 على الساعة 18:00

[2]جدة عبد القادر محمد، "الشرطة السعودية تستعد لمواجهة ملف الجرائم الإلكترونية"، مقال منشور على الرابط التالي: https://www.alarabiya.net/saudi-today/2013/12/05/تاريخ الاطلاع 2021/06/15 على الساعة 20:23.

[3]ميز المشرع المصري داخل **طائفة مأموري الضبط القضائي ذوي الاختصاص العام** بين مجموعتين، الأولى تضم مأموري الضبط القضائي الذين يباشرون الاختصاص العام في نطاق اختصاص إقليمي محدود، والثانية تضم مأموري الضبط القضائي الذين يباشرون الاختصاص العام في جميع أنحاء الجمهورية، وهذا ما نصت عليه المادة 23 من قانون الإجراءات الجنائية رقم 150 لسنة 1950 المعدل بالقانون رقم 189 لسنة 2020، والتي تقضي :

أ. **يكون من مأموري الضبط القضائي في دوائر اختصاصهم:**

1. أعضاء النيابة العامة ومعاونوها.
2. ضباط الشرطة وأمناؤها والكونستابلات والمساعدون.
3. رؤساء نقط الشرطة.
4. العمد ومشايخ البلاد ومشايخ الخفراء.
5. نظار ووكلاء محطات السكك الحديدية الحكومية.

لمباشرة التحقيق فيها، ونظرا لظهور نوع مستحدث من الجرائم ألا وهو الجرائم الإلكترونية، كان لزاما على الحكومة المصرية استحداث وحدات وأجهزة متخصصة في هذا النوع من الإجرام، استحدثت بذلك وزارة الداخلية المصرية جهازا متخصصا في هذه الجرائم سمي "بإدارة مكافحة جرائم الحاسبات وشبكات المعلومات "بموجب القرار الوزاري رقم (13507) المؤرخ في 2002/07/07[1] والذي حدد اختصاصات هذه الإدارة في مجال ضبط الجرائم الإلكترونية، حيث تعد هذه الإدارة جديدة في تكوينها ونوعيتها تختص بمكافحة هذه الجرائم من خلال مجموعة ضباط متخصصين في تكنولوجيا الحاسبات والاتصالات وشبكة الإنترنت، مقسمين على أجهزتها المختصة وذلك كما يلي:[2]

- **قسم العمليات:**

وهو قسم يختص بمكافحة الجرائم التي تقع باستخدام أجهزة الحاسب الآلي وتمس بقواعد ونظم البيانات المعلوماتية، وذلك بالاشتراك مع الأجهزة المختصة بهذه الجرائم سواء من داخل الوزارة أو خارجها وفقا للتعليمات المنظمة لذلك، كما يقوم هذا القسم بإخطار الأجهزة الأخرى المختصة بالتحري في هذه الجرائم بالمعلومات المتوصل إليها، والتنسيق معها لإجراء التحريات وأعمال الضبط في تلك الجرائم، كما

...= ولمديري أمن المحافظات ومفتشي مصلحة التفتيش العام بوزارة الداخلية أن يؤدوا الأعمال التي يقوم بها مأمور الضبط القضائي في دوائر اختصاصهم.

ب. **ويكون من مأموري الضبط القضائي في جميع أنحاء الجمهورية:**

1. مدير وضباط إدارة المباحث العامة بوزارة الداخلية وفروعها بمديريات الأمن.
2. مديرو الإدارات والأقسام ورؤساء المكاتب والمفتشون والضباط وأمناء الشرطة والكونستابلات والمساعدون وباحثات الشرطة العاملون بمصلحة الأمن العام وفي شعب البحث الجنائي بمديريات الأمن.
3. ضباط مصلحة السجون.
4. مدير الإدارة العامة لشرطة السكة الحديد والنقل والمواصلات وضباط هذه الإدارة.
5. قائد وضباط أساس هجانة الشرطة.
6. مفتشو وزارة السياحة.

أما عن **الطائفة الثانية من مأموري الضبط القضائي** فحددتهم المادة 23 فقرة 3 و4 من نفس القانون والتي تقضي ب: "ويجوز بقرار من وزير العدل بالاتفاق مع الوزير المختص تخويل بعض الموظفين صفة مأموري الضبط القضائي بالنسبة إلى الجرائم التي تقع في دائرة اختصاصهم وتكون متعلقة بأعمال وظائفهم.

وتعتبر النصوص الواردة في القوانين والمراسيم والقرارات الأخرى بشأن تخويل بعض الموظفين اختصاص مأموري الضبط القضائي بمثابة قرارات صادرة من وزير العدل بالاتفاق مع الوزير المختص" ومن أمثلة هؤلاء الموظفين مهندسو التنظيم ومفتشو صحة المحافظات ومساعديهم ومفتشو صحة الأقسام والمراكز ومراقبو الأغذية ومفتشو المأكولات، ومدير إدارة الملاهي ومفتشوها ومدير السجل التجاري ووكيل ومفتشو هذه الإدارة ورؤساء مكاتب السجل التجاري.

[1] القرار الوزاري رقم 13507 المؤرخ في 2002/07/07 نشر في الأوامر العمومية لوزارة الداخلية المصرية، العدد 07، القاهرة.

[2] نبيلة هبة هروال، الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات، المرجع السابق، ص 143.

يقوم أيضا بإنشاء ملفات وسجلات بجميع عمليات التحري التي قام بها وذلك من خلال إعداد قائمة بيانات تضم الجرائم وكذا الأحكام الصادرة بشأنها ومرتكبيها.[1]

- **قسم التأمين:**

يختص هذا القسم بوضع الأساليب والخطط اللازمة من أجل تأمين الأنظمة المعلوماتية والشبكات الخاصة بأجهزة الوزارة وتنفيذها بعد اعتمادها، وذلك بالتنسيق مع الأجهزة المختصة بذلك، كما يقوم هذا القسم بتقديم يد العون لكافة أجهزة الوزارة التي تطلب تأمين نظمها المعلوماتية حماية للمعلومات السرية وضمانا لعدم الاعتداء عليها، ومتابعة التراخيص الصادرة عن الشركات الخاصة في مجال تأمين النظم والشبكات والأجهزة الخاصة بها وذلك دائما بالتنسيق مع الجهات المعنية.[2]

- **قسم البحوث والمساعدات الفنية:**

يختص هذا القسم بالقيام بإعداد البحوث الفنية والقانونية في مجال تأمين نظم وشبكات المعلومات والحاسبات الآلية، وبدراسة الظواهر الإجرامية المتعلقة بها واستخلاص النتائج للاستفادة منها في أساليب المكافحة، كما يقوم ببحث مدى ملائمة التشريعات الجنائية لمواجهة مثل هذه الجرائم، ضف إلى ذلك فهو يقوم بتقديم الدعم الفني وتوفير المساعدات الفنية وإبداء الرأي والمشورة بخصوص القضايا المرتبطة بهذا النوع المستحدث من الإجرام للجهات المختصة بذلك.[3]

إلى جانب هذه الوحدات والأقسام أنشأت وزارة الداخلية المصرية إدارات أمنية أخرى أوكلت لها مهمة ضبط الجرائم الإلكترونية، حيث تم إنشاء الإدارة العامة لمباحث الأموال العامة التي تضطلع بمكافحة الجرائم الاقتصادية التقليدية بصفة عامة والجرائم المستحدثة بصفة خاصة، خاصة جرائم تحويل الأموال وجرائم بطاقات الدفع الإلكتروني والجرائم المصرفية وجرائم تزوير العملات الورقية وغيرها، كما تعتبر الإدارة العامة للتوثيق والمعلومات من أكبر الإدارات بوزارة الداخلية تعاملا مع الجرائم المستحدثة، بحيث تختص بعمليات المتابعة الفنية لهذه الجرائم بعد التبليغ عنها من قبل الإدارات الأخرى، هذا من جهة، ومن جهة أخرى تقوم هذه الإدارة بتحديد شخص المتهم من خلال عمليات المتابعة حيث يعتمد

[1] المرجع نفسه، ص 143.

[2] فيروز عوض الكريم صالح الميرغني، إجراءات التحري والضبط في الجرائم الإلكترونية، أطروحة مقدمة لنيل شهادة الدكتوراه في القانون العام، كلية الدراسات العليا والبحث العلمي، جامعة شندى، 2017، ص 253.

[3] المرجع نفسه، ص 258.

أسلوب عمل هذه الإدارة في معرفة مرتكب الجريمة على استخدام البرامج الحديثة والمتطورة مثل الاعتماد على رقم البروتوكول(IP) الذي يتعامل من خلاله الشخص مع شبكة الإنترنت، ولهذا الغرض خصصت إدارة مكافحة جرائم الحاسبات مجموعة من المواقع والأرقام لتلقي البلاغات حول هذه الجرائم، حيث يمكن للمواطنين التواصل عبر الرقم "108" الذي أنشئ خصيصا للتبليغ عن الجرائم الإلكترونية دون غيرها، أو عبر الموقع الإلكتروني لإدارة مكافحة جرائم الحاسبات مرورا بالموقع الرسمي لوزارة الداخلية www.egypt.gov.eg.

وإلى جانب هذه الوحدات نجد الإدارة العامة للمصنفات الفنيةوالتي تهتم بحماية الملكية الفكرية وحرية الإبداع والتعبير من أي أعمال غير مشروعة كجرائم النسخ والتقليد، وذلك من خلال تلقيها إخطارا أو بلاغا عن وقوع جريمة من بين هذه الجرائم لتبدأ الإدارة بعملية التحري والتفتيش والتحفظ على الأدلة المتحصل عليها مثل الوسائط الإلكترونية وغيرها من الأدوات المستعملة في النسخ والطباعة.[1]

وقد كشفت العديد من الدراسات الزيادة الهائلة في حجم الجرائم الإلكترونية في السنوات الأخيرة، من بينها دراسة أعدتها لجنة الاتصالات وتكنولوجيا المعلومات والتي تبين من خلالها ارتفاع هذه الجرائم في شهري سبتمبر وأكتوبر من سنة 2019 إلى 1038جريمة إلكترونية، نجحت وزارة الداخلية في ضبط غالبية المتهمين في هذه الجرائم، إذ تم القبض على 300 متهم منهم، كما أكد رئيس لجنة الاتصالات أن أغلب هذه الجرائم كانت جرائم نصب واحتيال وابتزاز وتشهير، وكذا بيع أدوية ومواد صيدلانية غير صالحة للاستخدام ومنتهية الصلاحية، إلى جانب تجارة آثار مزورة عبر صفحات الإنترنت، وفي دراسة أخرى أعدتها شركة "ترينـد مايكرو إنكوربوريتد"[2] للنصف الأول لعام 2021 بينت حجم الجرائم التي واجهتها هذه السنة، حيث تصدت الشركة ل 40,9 مليار هجمة إلكترونية بزيادة سنوية بلغت نسبة 47%، أغلبها تمثل في جرائم الفدية التي استهدفت شركات كبرى، وخاصة القطاع المصرفي حيث تأثر هذا الأخير بنسبة 1,318

[1] نبيلة هبة هروال، الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات، المرجع السابق، ص 141-142.

[2] تعد شركة "**ترينـد مايكرو**" من أبرز الشركات في مجال الوقاية من التهديدات الرقمية إذ تقوم بالتعاون مع كلا القطاعين العام والخاص لرفع مستوى الوعي بمخاطر الإنترنت وسد فجوة المعرفة بالأمن السيبراني، بما يعزز من أمن الخدمات الإلكترونية الخاصة بجميع مؤسسات مصر، وتحتل هذه الشركة موقع الصدارة من حيث تقديم حلول أمنية مبتكرة للشركات تتميز بقدرتها على توفير الأمن لها وكل المعلومات الخاصة بالتهديدات والاستجابة لها قبل حدوثها، وهذا ما ساعد على تفادي العديد منها.

كما أكد المؤسس والرئيس التنفيذي **لشركة "ديجيتال بلانتس"** في ملتقى نظمته الشركة بالتعاون مع شركة "سوفوس" العالمية وشركة الاتصالات المصرية على أنه يتوقع أن يبلغ حجم خسائر العالم من هذه الهجمات الإلكترونية حوالي 10,5 تريليون دولار بحلول سنة 2025، فيما أظهرت بعض الدراسات والإحصائيات أن الجرائم إ هي الأسرع انتشارا حول العالم، حيث يشهد العالم جريمة واحدة كل 11 ثانية خلال 2021.

% من هذه الجرائم خلال النصف الأول من عام 2021، كما قامت الشركة بحجب ما يزيد عن 13 مليون هجمة إ عبر البريد الإلكتروني في مصر، فضلا عن الحيلولة دون وقوع ما يزيد عن 1,4 مليون هجمة عبر الروابط الضارة، وأكثر من 5,23 هجمة عبر الروابط المضيفة، بالإضافة إلى أكثر من 681 ألف هجمة عبر البرامج الضارة تم تحديدها وإيقافها قبل حدوثها.[1]

رابعا: الأردن

تناط مهمة الضبط القضائي في الأردن بجهاز الضابطة العدلية طبقا لقانون أصول المحاكمات الجزائية[2] وينقسم موظفو الضابطة العدلية إلى طائفتين تبعا لنوع الجريمة أو طبيعتها، الطائفة الأولى هي من أوكل لها ممارسة الضبط في جميع أنواع الجرائم ويطلق عليها أعضاء الضابطة العدلية ذو الاختصاص العام، وهم من ورد ذكرهم في المادتين 08 و09 من قانون أصول المحاكمات الجزائية[3]، أما الطائفة الثانية وهي من خصها القانون بضبط بعض الجرائم دون غيرها، ويطلق عليها أعضاء الضابطة العدلية ذو الاختصاص الخاص، وهم من ورد ذكرهم في المادة 10 من ذات القانون، [4] من بينهم الأعضاء

[1] تقرير من شركة "تريند مايكرو" حول الهجمات الإلكترونية في النصف الأول من عام 2021، منشور على الرابط التالي: https://almalnews.com في 2021/10/27، تاريخ الاطلاع 2021/11/10 على الساعة 15:40.

[2] قانون أصول المحاكمات الجزائية رقم 09 لسنة 1961، الجريدة الرسمية الأردنية عدد 2539 الصادرة بتاريخ مارس 1961، ص 311، المعدل والمتمم بالقانون رقم 16 لسنة 2001 والقانون رقم 32 لسنة 2017.

[3] حيث تنص المادة 08 فقرة 2 من قانون أصول المحاكمات الجزائية على أنه: "يقوم بوظائف الضابطة العدلية المدعي العام ومساعدوه ويقوم بها أيضا قضاة الصلح في المراكز التي لا يوجد فيها مدعي عام، كل ذلك ضمن القواعد المحددة في القانون"

وتنص المادة 09 من ذات القانون على أن: "يساعد المدعي العام في إجراء وظائف الضابطة العدلية:

- الحكام الإداريون.
- مدير الأمن العام.
- مديرو الشرطة.
- رؤساء المراكز الأمنية.
- ضباط وأفراد الشرطة.
- الموظفون المكلفون بالتحري والمباحث الجنائية.
- المخاتير.
- رؤساء المراكب البحرية والجوية.

وجميع الموظفين الذين خولوا صلاحيات الضابطة العدلية بموجب هذا القانون والقوانين والأنظمة ذات العلاقة.

يقوم كل من الموظفين المذكورين بوظائف الضابطة العدلية في نطاق الصلاحيات المعطاة لهم في هذا القانون والقوانين الخاصة بهم"، لمزيد من التفاصيل ينظر حسن الجوخدار، البحث الأولي أو الاستدلال في قانون أصول المحاكمات الجزائية، ط 01، دار الثقافة للنشر والتوزيع، الأردن، 2012، ص 68-69.

[4] حيث تنص المادة 10 من ذات القانون على: "لنواطير القرى العموميين والخصوصيين وموظفي مراقبة الشركات ومأموري الصحة ومحافظي الجمارك ومحافظي الحراج ومراقبي الآثار الحق في ضبط المخالفات وفقا للقوانين والأنظمة المنوط بهم تطبيقها ويودعون إلى المرجع القضائي

المختصون في التحري وضبط الجرائم الإلكترونية، حيث استجابة للتسارع والتطور الكبير الذي يشهده العالم في مجال الجريمة وخاصة الإلكترونية أنشأت مديرية الأمن العام بالمملكة الهاشمية الأردنية إدارة مخصصة للبحث الجنائي عام 1948 وكانت أولى مهامها منع الجرائم والقبض على المجرمين وحراسة السجناء، حيث كانت تعرف باسم دائرة تحري المجرمين[1]، وقد تم دمج عدة أقسام ضمنها واستحداث أخرى إلى غاية عام 2008 استحدثت المديرية على مستوى إدارة البحث قسما للجرائم الإلكترونية وطورته عام 2015 ليصبح وحدة مكافحة الجرائم الإلكترونية، إذ تضم هذه الوحدة مجموعة من الضباط والخبراء المدربين والمؤهلين لملاحقة هذا النوع من الإجرام والتصدي له، من خلال الكشف عن الجناة وملاحقتهم عن طريق التحقق من الحسابات والمواقع والبرامج التي استخدمها المجرمين في تنفيذ جرائمهم، إذ تعتمد هذه الوحدة في تحرياتها على وسائل جد متطورة تمكنها من معرفة صاحب الحساب أو الموقع ومكان تواجده.

كما تعمل هذه الوحدة وفق نهج تشاركي مع المؤسسات الخاصة والعامة وشركات الاتصالات في تتبع هذا النوع من الجرائم والتحقيق فيها، كما تقوم بتعزيز التعاون الدولي مع الجهات الدولية الأخرى في العديد من البلدان في مجال مكافحة هذا النوع من الإجرام، ومن مهامها أيضا القيام بدوريات إلكترونية متجددة

...=المختص المحاضر المنظمة بهذه المخالفات"، وينحصر اختصاص هؤلاء في الجرائم المحددة على سبيل الحصر وفقا للقانون والنظام، إذ لا يمكنهم اتخاذ أي إجراء في شأن جرائم لا تدخل ضمن اختصاصهم المحدد، وتكمن علة تخصيص بعض الموظفين بجرائم محددة وذات طبيعة خاصة بضرورة توافر الخبرة والكفاءة فيهم، ومعرفتهم الجيدة بهذه الجرائم، وتدريبهم على استخدام أساليب ووسائل علمية وتقنية في الكشف عن هذه الجرائم، لمزيد من التفاصيل ينظر حسن الجوخدار، البحث الأولي أو الاستدلال في قانون أصول المحاكمات الجزائية، المرجع السابق، ص 69-70.

[1] وفي عام 1948 انقسمت دائرة تحري المجرمين إلى قسمين القسم السياسي ودائرة سجلات الجرائم، وفي عام 1953 تم دمج القسمين معا تحت اسم دائرة المباحث العامة، ليعاد تقسيم هذه الدائرة في عام 1961 إلى قسمين، احتفظ القسم الأول باسمه الأساسي (الاستخبار السياسي وقسم الجرائم)، وفي عام 1968 تم تنظيم قسم الجرائم وأصبح يعرف باسم فرع التحقيقات الجنائية، أما في عام 1974 تم عقد المؤتمر الثاني لقادة الشرطة العرب في عمان وأطلق على الفرع السابق اسم إدارة التحقيقات، وفي عام 1976 ظهرت فكرة انشاء جهاز متخصص في البحث الجنائي في الأمن العام الأردني، وتم استحداث مفارز للبحث الجنائي على مستوى مديريات الشرطة في كل محافظة واستمر ذلك لغاية 1984 تم تغيير مسمى شعبة البحث الجنائي إلى فرع التحقيق والبحث الجنائي ويتبع قسم الشرطة القضائية في مديريات الشرطة في جميع أنحاء المملكة باستثناء مديرية شرطة العاصمة فقد أصبحت الشعبة قسم بحث جنائي، وفي عام 1996 تم استحداث منصب مساعد مدير شرطة العاصمة للبحث الجنائي وبقيت الأقسام في المديريات الشرطة كما هي، وفي عام 2004 تقرر استحداث إدارة للبحث الجنائي تضم شعب البحث الجنائي في كل من العاصمة والضواحي تتبع لمساعد مدير الأمن العام للبحث الجنائي، وبتاريخ 2005/02/03 تم ربط باقي شعب المملكة بإدارة البحث الجنائي وباشرت عملها على مستوى المملكة منذ ذلك التاريخ، وفي عام 2008 أنشأت المديرية العامة قسم الجرائم الإلكترونية وطورته عام 2015 ليصبح وحدة مكافحة الجرائم الإلكترونية، ولحقه عام 2012 استحداث وحدة مكافحة الاتجار بالبشر والتي باشرت أعمالها في 2013/01/01، لمزيد من التفاصيل راجع الموقع الرسمي لمديرية الأمن العام للمملكة الهاشمية الأردنية، على الرابط التالي: https://psd.gov.jo/index.php/ar/2015-01-19-08-25-06/2015-03-17-09-14-06

وبشكل دائم على المواقع الإلكترونية ومواقع التواصل الاجتماعي لمراقبة أي منشور من شأنه أن يشكل جريمة إلكترونية، كالعبارات الماسة بالآداب والأخلاق العامة، أو خطابات الكراهية والخطابات الماسة بأمن الدولة وغيرها، وفي سبيل التواصل مع هذه الوحدة قد خصصت مديرية الأمن العام الرقم التالي "065633404" للإجابة عن جميع استفسارات المواطنين واستقبال بلاغاتهم المتعلقة بالجرائم الإلكترونية، والرقم "192" للتبليغ عن جرائم الابتزاز الإلكتروني خصيصا، أو عن طريق التواصل مع مديرية الأمن العام عبر بريدها الإلكتروني التالي "jenaee.dept@psd.gov.jo"[1]

وقد عالجت هذه الوحدة منذ إنشائها العديد من قضايا الإجرام الإلكتروني فبحسب إحصائيات مقدمة من طرف هذه الوحدة أنها تلقت العديد من البلاغات حيث وصل عدد الجرائم إ في سنة 2012 حوالي 1139 جريمة، في حين بلغ عددها عام 2013، 1599 جريمة، حيث تصدرت جرائم الابتزاز والتشهير هذه الجرائم ب 387 قضية، ووصل عدد الجرائم إ عام 2014 حوالي 1865 جريمة من بينها 641 جريمة ابتزاز، فيما بلغت عدد القضايا خلال عام 2015 حوالي 2305 قضية.[2]وارتفعت لتبلغ 7500قضية عام 2019 في حين سجلت 9500 قضية عام 2020، إذ تتصدر هذه القضايا دائما جرائم التهديد والابتزاز الإلكتروني، تليها جرائم انتحال الشخصية، ثم جرائم الاحتيال واختراق الأنظمة وسرقة البيانات وكذا البريد الإلكتروني، ثم تليها الجرائم المتعلقة بالإرهاب والتطرف، وأخيرا تأتي جرائم الاستغلال الجنسي للأطفال،[3] ومن بين هذه القضايا تمكنت وحدة مكافحة ج إ على مستوى إدارة البحث الجنائي بإلقاء القبض على أحد الأشخاص بعد أن ثبت تورطه في إنشاء صفحات وهمية على مواقع التواصل إ واستخدامها للإساءة للمواطنين والشخصيات العامة والتشهير بهم ونشر الاشاعة والأكاذيب عليهم، وهذا بعد تلقي الإدارة عدة بلاغات وشكاوى ضد شخص مجهول ينشر هذه التهديدات عبر صفحات الإنترنت، وبعد تشكيل فريق من المختصين تم تتبع منشورات هذا الشخص لغاية الوصول إليه وتحديد مكانه وتم القبض عليه.[4]

---

[1] لمزيد من التفاصيل يراجع الموقع الرسمي لمديرية الأمن العام للمملكة الهاشمية الأردنية، المتاح على الرابط التالي: https://www.psd.gov.jo/index.php/ar/2020-02-05-08-20-44 تاريخ الاطلاع 2021/06/30 على الساعة 20:30

[2] غادة الشيخ، الفضاء الإلكتروني مسرح جديد للجرائم ضحاياه مراهقون، مقال منشور في جريدة الغد على الرابط التالي: https://alghad.com تاريخ الاطلاع 2021/07/20، على الساعة 19:12.

[3] غادة الشيخ، الفضاء الإلكتروني مسرح جديد للجرائم ضحاياه مراهقون، المرجع السابق.

[4] مقال حول "البحث الجنائي يلقي القبض على منشأ صفحات وهمية على الفايس بوك قام بالإساءة والتشهير بمواطنين"، منشور على الموقع الرسمي لمديرية الأمن العام للمملكة الأردنية الهاشمية، صفحة الأخبار، يوم 2017/04/03، على الرابط التالي: https://www.psd.gov.jo/index.php/ar/2015-07-07-17-14-02/76-arabi-part/2015-03-10-09-41-44/2015-04-12-05-16-34/3670-1491197263 تاريخ الاطلاع: 2021/10/31 على الساعة 12:00.

كما تجدر الإشارة أنه تقوم هذه الوحدة في سبيل التحذير من الجرائم الإلكترونية على نشر الوعي والثقافة الإلكترونية والدعم والإرشاد عن طريق موقعها الإلكتروني أو صفحتها على مواقع التواصل الاجتماعي، أو عن طريق المحاضرات التي يتم إلقائها من طرف الضباط والخبراء في الجريمة الإلكترونية وذلك على مستوى كل من المدارس والمعاهد والجامعات وحتى الجمعيات، تجنبا لوقوع المواطنين وخاصة فئة الأطفال ضحية لهذه الجرائم.

الفرع الثاني: على مستوى الجزائر بصفة خاصة

تناط مهمة البحث والتحري في الجرائم بصفة عامة إلى جهاز الضبطية القضائية، حيث عني قانون الإجراءات الجزائية الجزائري بتحديد الأشخاص الموكل إليهم مهام الضبط القضائي، فوفقا للمادة 12 فقرة 01 من ق إ ج ج[1] يقوم بمهمة الضبط القضائي رجال القضاء والضباط والأعوان والموظفون المنوط بهم بعض مهام الضبط القضائي، وقد جاءت المادة 15 من ذات القانون[2] محددة لمن تثبت لهم صفة

[1] تنص المادة 12 من القانون رقم 22/06 المؤرخ في 20 ديسمبر 2006 المعدل والمتمم للأمر رقم 66_155 المتضمن قانون الإجراءات الجزائية، ج ر العدد 84، الصادرة بتاريخ 24 ديسمبر 2006، علىمايلي: " يقوم بمهمة الشرطة القضائية، القضاة والضباط والأعوان والموظفون المبينون في هذا الفصل.

توضع الشرطة القضائية بدائرة اختصاص كل مجلس قضائي، تحت إشراف النائب العام، ويتولى وكيل الجمهورية إدارتها على مستوى كل محكمة، وذلك تحت رقابة غرفة الاتهام.

ويناط بالشرطة القضائية مهمة البحث والتحري عن الجرائم المقررة في قانون العقوبات وجمع الأدلة عنها والبحث عن مرتكبيها ما دام لم يبدأ فيها تحقيق قضائي.

يحدد النائب العام التوجيهات العامة اللازمة للشرطة القضائية لتنفيذ السياسة الجزائية بدائرة اختصاص المجلس القضائي."

[2] تنص المادة 15 من القانون رقم 10/19 المؤرخ في 14 ربيع الثاني عام 1441 الموافق 11 ديسمبر 2019، المعدل والمتمم للأمر رقم 66-155 المؤرخ في 18 صفر عام 1386 الموافق 08 يونيو سنة 1966 والمتضمن قانون الإجراءات الجزائية، ج ر ج ج عدد 78، الصادرة في 18 ديسمبر 2019، على مايلي: " يتمتع بصفة ضابط الشرطة القضائية:

1. رؤساء المجالس الشعبية البلدية
2. ضباط الدرك الوطني
3. الموظفون التابعون لأسلاك الخاصة للمراقبين، ومحافظي وضباط الشرطة للأمن الوطني
4. ضباط الصف الذين أمضوا في سلك الدرك الوطني ثلاث (3) سنوات على الأقل، وتم تعيينهم بموجب قرار مشترك صادر عن وزير العدل حافظ الأختام، ووزير الدفاع الوطني، بعد موافقة لجنة خاصة،
5. الموظفون التابعون للأسلاك الخاصة للمفتشين وأعوان الشرطة للأمن الوطني الذين أمضوا ثلاث سنوات على الأقل بهذه الصفة والذين تم تعيينهم بموجب قرار مشترك صادر عن وزير العدل ووزير الداخلية والجماعات المحلية، وبعد موافقة لجنة خاصة،
6. ضباط وضباط الصف التابعين للمصالح العسكرية للأمن الذين تم تعيينهم خصيصا بموجب قرار مشترك صادر عن وزير الدفاع الوطني ووزير العدل.

يحدد تكوين اللجنة المنصوص عليها في هذه المادة وتسييرها بموجب مرسوم."

الضبطية القضائية، وجاءت المادتان 21 و28[1] محددة للموظفين الموكل إليهم بعض مهام الضبط القضائي الخاص، بحيث قسم القانون هؤلاء الضباط إلى فئتين أساسيتين تتمتع الأولى بمتابعة جميع أنواع الجرائم وتعرف بالضبطية القضائية ذات الاختصاص العام، في حين تتمتع الفئة الثانية بالتحري في بعض الجرائم الخاصة وتعرف بالضبطية القضائية ذات الاختصاص الخاص،[2] وبظهور الجرائم المستحدثة والإلكترونية أصبح جهاز الضبطية القضائية غير قادرا على التصدي لمثل هذه الجرائم نظرا لضعف خبرته ومعرفته في هذا المجال، لهذه الأسباب ونظرا للخصوصية التي تتمتع بها هذه الجرائم أصبح لزاما العمل على تكوين وتأهيل الضباط في مجال التحري عن الجرائم الإلكترونية لتطوير كفاءاتهم ومهامهم من أجل التصدي الأمثل لهذه الجرائم ومحاربة مرتكبيها، وفي هذا الإطار قامت الحكومة الجزائرية بإنشاء واستحداث أجهزة خاصة للبحث والتحري في الجرائم الإلكترونية وذلك على مستوى كل من مديرية الأمن الوطني، والقيادة العامة للدرك الوطني، وكذا المديرية العامة للجمارك، سنتعرف عليها بالتفصيل في النقاط الآتية:

أولا: الوحدات التابعة للمديرية العامة للأمن الوطني

في إطار تجسيد سياسة أمنية فعالة للتصدي للجرائم الإلكترونية بادرت المديرية العامة للأمن الوطني بتحديث بنيتها الهيكلية والعمل على استحداث وحدات متخصصة تعمل على مكافحة هذا النوع من الجرائم، حيث استحدثت أربع (04) مصالح مختصة في شكل نيابة تمثلت في نيابة مديرية الشرطة العلمية والتقنية، نيابة المديرية الاقتصادية والمالية، نيابة القضايا الجنائية، مصلحة البحث والتحليل.

[1] تنص المادة 21 من ق ا ج ج على: " يقوم رؤساء الأقسام والمهندسون والأعوان الفنيون والتقنيون المختصون في الغابات وحماية الأراضي واستصلاحها بالبحث والتحري ومعاينة جنح ومخالفات قانون الغابات وتشريع الصيد ونظام السير وجميع الأنظمة التي عينوا فيها بصفة خاصة وإثباتها في محاضر ضمن الشروط المحددة في النصوص الخاصة."

كما تنص المادة 28 من ذات القانون على فئة معينة منح لها القانون صفة الضبطية القضائية في بعض الحالات، ألا وهي فئة الولاة، إذ جاء في نص المادة: " يجوز لكل وال في حالة وقوع جناية أو جنحة ضد أمن الدولة وعند الاستعجال فحسب، إذا لم يكن قد وصل إلى علمه أن السلطة القضائية قد أخطرت بالحادث أن يقوم بنفسه باتخاذ جميع الإجراءات الضرورية لإثبات الجنايات أو الجنح الموضحة أنفا أو يكلف بذلك كتابة ضباط الشرطة القضائية المختصين.

وإذا استعمل الوالي هذا الحق المخول له فإنه يتعين عليه أن يقوم فورا بتبليغ وكيل الجمهورية خلال 48 ساعة التالية لبدء هذه الإجراءات وأن يتخلى عنها السلطة القضائية ويرسل الأوراق لوكيل الجمهورية ويقدم له جميع الأشخاص المضبوطين.

يتعين على كل ضابط من ضباط الشرطة القضائية تلقى طلبات من الوالي حال قيامه بالعمل بموجب الأحكام السابقة وعلى كل موظف بلغ بحصول الإخطار طبقا لهذه الأحكام ذاتها أن يرسل الأول هذه الطلبات وأن يبلغ الثاني هذه الإخطارات بغير تأخير إلى وكيل الجمهورية."

[2] نبيلة هبةهروال، الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات، المرجع السابق، ص 95.

وقد أسندت مهمة مكافحة الجرائم الإلكترونية لنيابة مديرية الشرطة العلمية والتقنية، والتي تتولى أعمال البحث والتحري من خلال وحدات متخصصة تتمثل في كل من المخبر المركزي للشرطة العلمية بشاطوناف بالجزائر العاصمة والذي يضم 15 مصلحة حيث يحتل المرتبة الثانية إفريقيا والأولى عربيا بين مخابر الشرطة، إضافة إلى إنشاء مخبرين جهويين بكل من قسنطينة ووهران و03 مخابر أخرى على مستوى كل من ولاية ورقلة وبشار وتمنراست، [1] إذ تحتوي هذه المخابر على عدة فروع تقنية تتولى مهمة التحري في الجرائم الإلكترونية، وجمع الأدلة الرقمية وتحليلها، إذ يضم كل مخبر دائرتين هما:

- الدائرة العلمية والتي تتولى أعمال تحليل الأدلة المتصلة بالمجال البيولوجي والطب الشرعي والكيمياء، وكذلك المتعلقة بمجال التسميم والحريق والمتفجرات...الخ.
- الدائرة التقنية وتتولى مهام البحث والتحقيق وتحليل الأدلة الجنائية الناتجة عن الجرائم التي تستعمل فيها الأسلحة وكذا جرائم التزوير والجرائم المعلوماتية، وتباشر الإجراءات الخاصة بكل جريمة على مستوى دائرة مستقلة عن الأخرى.

كما يضم المخبر الجهوي للشرطة العلمية على مستوى ولاية قسنطينة وولاية وهران، مخبرا خاصا يتولى مهمة التحقيق بشأن الجرائم الإلكترونية وذلك تحت تسمية "**دائرة الأدلة الرقمية والآثار التكنولوجية**" والتي تم استحداثها سنة 2004 حيث عملت في بداياتها كقسم وبعد الارتفاع الهائل في عدد الجرائم الإلكترونية تم ترقيتها إلى دائرة وتضم هذه الأخيرة ثلاث (03) أقسام فرعية:

- قسم استغلال الأدلة الرقمية الناتجة عن الحواسيب والشبكات.
- قسم استغلال الأدلة الناتجة عن الهواتف النقالة.
- قسم تحليل الأصوات.

[1] يعود عمل الشرطة العلمية والتقنية بالجزائر إلى سبعينيات القرن الماضي على المستوى الوطني، حيث كان مقرها على مستوى المدرسة العليا للشرطة من خلال إنشاء مخبر علمي ومصلحة للطب الشرعي، تدعما لاحقا بملحقتين إقليميتين بوهران وقسنطينة، فبالنسبة للمخبر المركزي فهو يعمل بتقنيات عالية وجد متطورة ومتحصل على مقياس الجودة من المنظمة الدولية للمعايير (ايزو/ آي إي سي 17025) التي تقوم بتصنيفه عالميا ضمن المنطقة الزرقاء، وذلك وفق مقاييس خاصة تتطلب أن يكون المحلل حائزا على باكالوريا زائد أربع سنوات دراسة في الجامعة في تخصص الكيمياء أو البيولوجيا، ولديه مهارات في العلوم التحليلية والفيزيائية والعضوية والبيولوجية، ومتمكن من الأجهزة المستخدمة في التحليل ومتقنا لفن الإحصاء ولديه مكتبة من الوثائق التي يعتمد عليها.
أما بالنسبة للمخبر الجهوي بوهران يمتلك 08 فروع تقنية وعلمية إضافة إلى فرع الكحوليات الملحق بدائرة التسممات، وهو يشرف على 15 ولاية بالجهة الغربية حيث كانت بداية انطلاقته في الثمانينات بالأمن الحضري الثالث على مستوى حي (أش أل أم) إلى غاية فتح مقر الأمن الولائي سنة 1987.

وتضم الدائرة ثمانية (08) أعضاء محققين، أربعة (04) منهم أعوان شرطيون رسميون يتمتعون بصفة ضابط شرطة قضائية، والبقية أعوان شبيهون، يحمل كل منهم شهادة جامعية في تخصص الإعلام الآلي، إضافة إلى إلمامهم بالجانب القانوني، كما يخضعون بصفة دورية لدورات تكوينية لأجل الاطلاع على المستجدات القانونية والتقنية في مجال التحقيق في الجرائم الإلكترونية.

وتضطلع هذه الدائرة بأقسامها ومخابرها بضمان الدعم التقني لمصالح الشرطة والأجهزة القضائية في مجال التحريات الإلكترونية، بحيث يستجيب أعضاء هذه المخابر للطلبات المقدمة لهم من طرف أعوان الشرطة التابعون لوحدات وفرق مكافحة الجرائم الإلكترونية الموزعة على كل مديريات الأمن الوطني أو لطلبات وكيل الجمهورية أو قاضي التحقيق التي تردهم في شكل إنابة قضائية من أجل دعمهم في مرحلة معاينة مسرح الجريمة والحجز على الأدلة المتواجدة فيه، وذلك من خلال القيام بعمليات التحليل الفني للمعطيات الرقمية والأدلة الإلكترونية بمختلف أشكالها وباستعمال برامج ووسائل خاصة تساعد في تحليل محتوى الوسائط الرقمية واسترجاع المعلومات المحذوفة وغيرها، أما أثناء مرحلة التحقيق القضائي فإن دور هذه الدائرة لا يتعدى لأن يكون دور خبير وذلك من خلال إعداد تقارير خبرة وتقديمها لقضاة التحقيق أو قضاة الحكم للاستناد عليها في تسبيب أحكامهم وقراراتهم، وبالرجوع للمعطيات الإحصائية المقدمة فإن سنة 2014 شهدت ما يقارب 250 قضية محل تحقيق من قبل أعضاء الدائرة، أبرزها قضيتان وردتا على سبيل الإنابة القضائية الدولية وبالتحديد عن طريق مكتب الإنتربول تتعلق كلاهما بقيام شابين من ولاية قسنطينة بالاعتداء على الأنظمة المعلوماتية الخاصة بموقع وزارة الخارجية الكويتية وتعطيلها، والقيام بالاحتيال الإلكتروني على مجموعة أشخاص من الولايات المتحدة الأمريكية، في حين تم تسجيل 60 قضية في الثلاثي الأول من سنة 2015 قام محققي دائرة الأدلة الرقمية بالنظر فيها، حيث تتعلق أغلبها بسوء استخدام مواقع التواصل الاجتماعي من خلال قضايا المساس بالأشخاص عن طريق السب والقذف والتشهير وكذا الابتزاز...الخ.[1]

إضافة إلى هذه الوحدات تم إنشاء المصلحة المركزية لمكافحة الجريمة المعلوماتية على مستوى المديرية العامة للأمن الوطني والتي كانت عبارة عن فصيلة شكلت النواة الأولى لمحاربة الجريمة الإلكترونية والتي أنشأت سنة 2011، ليتم بعدها إنشاء المصلحة المركزية لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام

[1] حسين ربيعي، آليات البحث والتحقيق في الجرائم المعلوماتية، المرجع السابق، ص 181.

والاتصال (م.م.م.ج.ت.إ.إ) بقرار من المدير العام للأمن الوطني وذلك سنة 2015[1] وتعمل هذه المصلحة بالتنسيق مع جهاز الشرطة القضائية والشرطة العلمية على المستوى المركزي، كما تم إنشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها بموجب القانون رقم 04/09 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، مقرها الجزائر العاصمة، حيث تتولى هذه الأخيرة الوقاية من الجرائم الإلكترونية والتصدي لها، مع مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها في هذه الجرائم.[2]

أما **على المستوى المحلي** فقد تم استحداث فرق متخصصة في محاربة الجريمة الإلكترونية على مستوى كافة ولايات الوطن. إذ تم انتقاء مجموعة عناصر شرطة ممن تتوفر فيهم شروط الميول والكفاءة والاطلاع الدائم على التكنولوجيات الحديثة، أسفر عن استحداث 48 فصيلة تابعة للمصالح الولائية للشرطة القضائية لأمن الولايات، بحيث يشترط في هؤلاء الضباط خبرتهم الكافية بالمعلوماتية والتعامل مع الأجهزة الإلكترونية باحترافية، إذ يخضع عناصر كل فرقة إلى دورات تكوينية منها دورات ابتدائية تكون قبل مزاولة الضابط لمهنته وهذا لامتحانه ومعرفة مدى إلمامه بالتقنيات والتكنولوجيات الحديثة، ودورات متواصلة تكون دورية ومتخصصة في كيفية التحري في الجرائم الإلكترونية، تكون موجهة عادة للرتب والإطارات، كما قد تتم هذه الدورات التكوينية على مستوى مديرية الشرطة القضائية من طرف عدة خبراء وضباط مختصين، كما قد تتم في بلدان أخرى عربية أو أجنبية في إطار تبادل الخبرات وتعزيز التعاون الدولي في هذا المجال.[3]

ومن بين أهم القضايا التي قامت المصلحة المركزية لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال بمعالجتها كانت أولها قضية ذات بعد دولي جاءت إثر بلاغ من مكتب التحقيقات الفيدرالية "أف بي آي" للسلطات الجزائرية بسبب تعرض شركة أمريكية إلى عملية قرصنة بخصوص بيانات بنكية، إذ تبين من التحقيق أنها منظمة إجرامية تنشط في مجال الاختراق والقرصنة ولها شريك بالجزائر، وبعد وصول البلاغ الأجنبي تم توجيه الملف إلى مصالح مديرية الشرطة القضائية لتقوم بتشكيل فريق متخصص للتحري في هذه القضية، وهنا كانت الانطلاقة الأولى للمصلحة المركزية لمحاربة الجريمة

[1] مقال حول "كلمة المدير العام للأمن الوطني"، منشور على الموقع الرسمي لمديرية الأمن الوطني الجزائري، متاح على الرابط التالي:https://www.algeriepolice.dzتاريخ الاطلاع 2021/11/20 على الساعة 18:48.

[2] لمزيد من التفاصيل حول تشكيلة ودور الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، ينظر الفصل الأول من هذا الباب، ص 54 وما بعدها.

[3] مقال حول "كلمة المدير العام للأمن الوطني"، منشور على الموقع الرسمي لمديرية الأمن الوطني الجزائري، المشار إليه سابقا.

الإلكترونية ذات البعد الدولي، [1] ومن الأمثلة أيضا توقيف مصالح الأمن الجزائرية لشاب جزائري صاحب مقهى للإنترنت ببلدية بومرداس إثر ورود شكوى ضده من مكتب التحقيقات الفيدرالي الأمريكي، عن طريق مكتب الإنتربول بالجزائر مفادها أنها تلقت رسالة إلكترونية باللغة الإنجليزية مجهولة الهوية مصدرها جهاز يقع في هذا المقهى، تضم تهديدا بوضع قنبلة لإحدى أحياء مدينة جوهانسبورغ بجنوب إفريقيا تستهدف المناصرين الأمريكيين قبيل انطلاق مباراة كرة القدم بين المنتخب الجزائري والأمريكي في كأس العالم، والأمثلة كثيرة.[2]

كما سجلت هذه الفرق العديد من القضايا على المستوى المحلي التي بينت أن معدل الجريمة الإلكترونية في تزايد يوما بعد يوم، خاصة في السنوات الأخيرة، إذ سجلت فرقة مكافحة الجرائم المعلوماتية بأحد ولايات الوطن تطور الجريمة الإلكترونية بمعدل 280% خلال السنوات (2020، 2021، 2022)، إذ سجلت 35% قضية نصب واحتيال عبر مواقع التواصل الاجتماعي، وحوالي 40% قضية قذف وتشهير وابتزاز إلكتروني، وحوالي 05% قضية الإخلال بالنظام العام والآداب العامة، و09 %قضية المساس بحرمة الحياة الخاصة وغيرها من القضايا، [3] في حين سجلت الفرقة المختصة بمكافحة الجرائم المعلوماتية التابعة للمصلحة الولائية للشرطة القضائية بولاية تيارت تطور ملحوظ في معدل الجريمة خلال السنوات الأربع الأخيرة، وتجدر الإشارة إلى أن هذه الحالات التي تم التبليغ عنها أو اكتشفت عن طريق السلطات فقط، فهي لا تعكس الأرقام الحقيقية لذلك الشبح الذي يرعب دول العالم سواء كانت متقدمة أو حتى نامية، لأن الكثير منها يبقى في طي الكتمان.[4]

ثانيا: الوحدات التابعة للقيادة العامة للدرك الوطني

[1] مقال حول "المصلحة المركزية للجريمة الإلكترونية في مواجهة مجرمي العالم الافتراضي"، مقال منشور علىجريدة السلام يوم2016/02/13، متاح على الرابط التالي:https://www.djazairess.com/essalam/52564تاريخ الاطلاع: 2021/06/27 على الساعة 18:20.
وفي سنة 2017 تم تعيين عميد الشرطة رئيس المصلحة على رأس مجموعة خبراء الإنتربول المختصة في مكافحة الجريمة الإلكترونية وذلك من قبل الأمين العام لمنظمة الشرطة الدولية، حيث جاء هذا التعيين بمناسبة أشغال الاجتماع ال10 لرؤساء المصالح المختصة في مكافحة الجرائم الإلكترونية لدول الشرق الأوسط وشمال إفريقيا المنعقد يومي 10 و11 ماي 2017 بفرنسا، وهذا ما يعد اعترافا بالمستوى العالي والاحترافية التي أضحت تتميز بها الشرطة الجزائرية في مجال محاربة الجرائم الإلكترونية. ينظر بلقاسم بحري، "جزائري يرأس خبراء "الإنتربول" في مكافحة الجريمة المعلوماتية "مقال منشور يوم 2017/05/29، متاح على الرابط التالي: https://www.sabqpress.dz/nationalتاريخ الاطلاع: 2021/06/27 على الساعة 18:30.

[2] جمال براهيمي، التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص 301.

[3] معلومات مقدمة من طرف الملازم الأول التابع للمصلحة الولائية للشرطة القضائية بولاية الأغواط حول "تطور الجريمة المعلوماتية في السنوات الأخيرة"، مقابلة إذاعية منشورة على الموقع الرسمي للمديرية العامة للأمن الوطني، المتاح على الرابط التالي:https://www.algeriepolice.dz–تاريخ الإطلاع 2022/09/12 على الساعة 10:17.

[4] ينظر الملحقين رقم 07 و08.

بما أن الدرك الوطني أحد الأجهزة الأمنية المكلفة بردع وضبط الجريمة، والمحافظة على الأمن والنظام العموميين، فقد ساير التطور الإجرامي الذي يشهده العالم اليوم من خلال توفير الوسائل المادية وتأهيل الضباط المختصين في مكافحة الإجرام المعلوماتي وذلك بإنشاء العديد من الهياكل والوحدات المتخصصة في التحري والتحقيق في هذا النوع من الجرائم، إلى جانب بعض المصالح التي تختص بالتحري في جميع الجرائم بصفة عامة نذكر من بينها، المصالح والمراكز العلمية والتقنية، المصلحة المركزية للتحريات الجنائية، هياكل التكوين، الوحدات المتخصصة ووحدات الإسناد، والوحدات الإقليمية.

إضافة إلى هذه المصالح وفي سبيل مكافحة الجريمة الإلكترونية يضع الدرك الوطني بعض الوحدات والمراكز المتخصصة في هذا النوع من الجرائم، وذلك على كل من المستوى المركزي والجهوي والمحلي:

1) على المستوى المركزي:

فعلى المستوى المركزي تم إنشاء المصالح التالية:

أ) المعهد الوطني للأدلة الجنائية وعلم الإجرام:

يعد المعهد الوطني للأدلة الجنائية وعلم الإجرام مؤسسة عمومية ذات طابع إداري، تم إنشاؤه بموجب المرسوم الرئاسي رقم 04-432 المؤرخ في 29 ديسمبر 2004[1] ببوشاوي بالجزائر العاصمة وذلك في إطار عصرنة قطاع الدرك الوطني، يتكون هذا المعهد من (11) إحدى عشرة دائرة متخصصة في مجالات مختلفة، تهدف جميعها إلى إنجاز عمليات الخبرة والتكوين والتعليم وتقديم المساعدات التقنية وغيرها، ومن بين هذه الدوائر **دائرة الإعلام والإلكترونيك** التي أوكلت لها مهام تحليل الأدلة الرقمية المتحصلة من الجرائم الإلكترونية، حيث تنقسم هذه الدائرة إلى ثلاث مخابر وذلك حسب نوع المعلومات أو الأدلة[2]، تتمثل هذه المخابر في:

- **مخبر الإعلام الآلي:**

يقوم هذا المخبر بتحليل ومعالجة حوامل المعطيات الرقمية الموجودة بالأجهزة الإلكترونية مثل الهاتف، الشريحة، القرص الصلب، ذاكرة الفلاش...الخ، والقيام بتحديد التزوير الرقمي للبطاقات البنكية

[1] المرسوم الرئاسي رقم 04-432 المؤرخ في 29 ديسمبر 2004، يتضمن إنشاء المعهد الوطني للبحث في علم التحقيق الجنائي، ج ر جج عدد 84، المؤرخة في 29 ديسمبر 2004، ص 24.

[2] هواري عياش، مداخلة حول مسار التحقيقات الجنائية في مجال الجريمة المعلوماتية، المعهد الوطني للأدلة الجنائية وعلم الإجرام، كلية الحقوق، جامعة بسكرة، 2016، ص 03.

وبطاقات الائتمان وغيرها، حيث يستعين في تحليله هذا بعدة وسائل وتجهيزات لاستخراج المعلومات من الهواتف والحواسيب، وكذا محطات لترميم وتصليح الأجهزة والحوامل المعطلة والشبكات الإعلامية، ومحطات ثابتة ومحمولة لإجراء خبرات الإعلام الآلي.[1]

- **مخبر الفيديو:**

يختص هذا المخبر بمقارنة الصور والفيديوهات وإعادة بناء مسرح الجريمة بالتشكيل ثلاثي الأبعاد، وذلك عن طريق أجهزة فيديو بوكس وحوامل الفيديو الرقمية والممغنطة (كونيتك استوديو، ماكس ثلاثة أبعاد) وموزع لحفظ شرائح الفيديو، كما يحتوي مخبر الفيديو على أربع قاعات، قاعتان للتحليل، قاعة للتخزين، وقاعة موزع.[2]

- **مخبر الصوت:**

يختص هذا المخبر بتحسين نوعية إشارة الصوت بنزع التشويش وتعديل السرعة، كما يقوم بتحديد الشخص المتكلم وتحديد شرعية التسجيلات الصوتية، وذلك عبر أجهزة الازدواجية والتنصت والحبكات الإعلامية المختصة بمعالجة وتحسين التسجيلات الصوتية، وكذا أجهزة نسخ الأقراص المضغوطة وأجهزة التصليح، ويحتوي هو الآخر على 05 قاعات، ثلاثة منها مخصصة للتحليل، وقاعة للتخزين، وقاعة موزع.[3]

من خلال ما يحتويه هذا المعهد من دوائر ومخابر فرعية مختصة تقنيا فإنه يساهم بشكل فعال في مكافحة الجرائم الإلكترونية وذلك لما يقوم به من مهام حيث يتولى في هذا الشأن القيام بالخبرات العلمية والتقنية لدعم أجهزة التحري والتحقيق وذلك بطلب منها، إذ تساعد الخبرات والتحليلات التي يقوم بها هذا المعهد على تحديد هوية مرتكبي هذه الجرائم، كما يقوم بدعم هذه الوحدات عن طريق الخبراء المؤهلين بمعاينة هذه الجرائم، إذ يتم التواصل بين أجهزة الشرطة القضائية وهذه المخابر عن طريق إرسالية تتضمن طلب تحليل الأجهزة المتحصل عليها من طرف الشرطة والتي قد تتمثل في دعائم تخزين رقمية مثل القرص المرن والقرص المضغوط، أو الهواتف النقالة أو الحواسيب أو أجهزة التصوير وغيرها من الأجهزة الرقمية، ليقوم الخبراء على مستوى هذه المخابر بتحليلها واستخراج المعطيات المخزنة بداخلها، وذلك بالاستعانة بمجموعة من الأدوات والوسائل المتطورة في سبيل الوصول إلى تحديد هوية

[1] المرجع نفسه، ص 04.

[2] المرجع نفسه، ص 07.

[3] هواري عياش، مداخلة حول مسار التحقيقات الجنائية في مجال الجريمة المعلوماتية، المرجع السابق، ص 08.

الأجهزة أو مرتكبيها أو أماكن تواجدها والتي من شأنها مساعدة الضباط في عملية التحقيق، مع الإشارة إلى أن نتائج هذه الخبرة قد تأخذ وقتا طويلا يدوم لعدة أشهر، وفي هذه المدة يواصل ضباط الشرطة التحري في الجريمة في انتظار وصول نتائج الخبرة.

فضلا عن هذا يشارك المعهد في الأبحاث والدراسات المتعلقة بالوقاية من جميع أشكال الإجرام بما فيها المعلوماتي، وبهذا يكون المعهد قد ساهم في وضع واقتراح سياسة ناجعة لمكافحة الإجرام بأنواعه.

ب) المركز الوطني لمكافحة الجريمة الإلكترونية:

جاء هذا المركز نتيجة إستراتيجية مؤسسة الدرك الوطني في تعقب الجرائم والإسراع في صدها إيمانا منها بأن المعلوماتية أصبحت وسيلة لتطور بعض الجرائم، وقد تم إنشاؤه في الجزائر العاصمة سنة 2004،[1] يضم هذا الأخير مجموعة من الوحدات والأقسام تقوم بمهام التحري في هذا النوع من الجرائم، وهي كالتالي:

- **وحدة الحماية والتحليل (Unité de veille et analyse)**

تسهر هذه الوحدة على تحليل المخزون المعلوماتي على مدار 24سا، وحماية بنك المعلومات المفتوحة والمتداولة عبر شبكة الإنترنت، وهي تضمن بهذا مهمة المراقبة العامة للمضمون المعلوماتي.

- **خلية المساعدة ومعالجة الحوادث المعلوماتية (Cellule d'assistance et de réponse aux incidents informatique):**

تسهر هذه الخلية على الوقاية من مخاطر المعلوماتية وتقديم المساعدة للمواطنين في تخطي الجرائم الإلكترونية على مستوى المؤسسات والمرافق الحكومية للدولة.

- **الوحدة المركزية للتنسيق والتعاون (Unité centrale de coordination et de lutte contre la cybercriminalité):**

[1] مباركة بن عمراوي، "العقيد في الدرك الوطني جمال بن رجم للإذاعة 95 بالمائة من الجرائم الإلكترونية تم حلها بنجاح"، مقال مشار إليه سابقا.

وتتفرع عن هذه الوحدة عدة وحدات فرعية موجودة على مستوى المجموعات الولائية والمتمثلة في الوحدات المحلية لمحاربة الجريمة الإلكترونية، إذ تعمل بالتنسيق مع الوحدة المركزية في مجال تبادل المعلومات والخبرات في التحري عن هذه الجرائم وتحليل الأدلة الرقمية.[1]

من خلال هذه الوحدات والمهام المنوطة بها نستنتج أن المركز الوطني لمكافحة الجرائم الإلكترونية يضطلع بمهمتين أساسيتين أولهما قبلية وتتعلق بالوقاية من مخاطر المعلوماتية وتجنب الوقوع فيها إضافة إلى عمليات التوعية والتحسيس التي يقوم بها المركز، والثانية بعدية تتمثل في ردع الجرائم بأنواعها.

وتجدر الإشارة أنه قد تم إنشاء مكتب خاص بمكافحة الجريمة الاقتصادية على مستوى هذا المركز، عالج من خلاله حوالي 20 جريمة اقتصادية ومالية خلال سنة 2017، إلى جانب هذا المكتب وعلى مستوى نفس المركز تم إنشاء مكتبا آخرا خاصا بحماية الأحداث عبر الإنترنت ليكمل مهام الفرق الخاصة بحماية الأطفال التي استحدثتها قيادة الدرك الوطني، حيث يقوم هذا المكتب بتقديم الدعم التقني للوحدات الإقليمية في مجال التحري عن الجرائم الواقعة على الأطفال، وقد عالج هذا الأخير حوالي 100 جريمة إلكترونية كان ضحاياها أطفال ومراهقين من ضمن 1000 قضية تمت معالجتها سنة 2017.[2]

ت) مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية:

يعتبر مركز الوقاية من جرائم الإعلام الآلي نقطة اتصال وطنية في مجال دعم أعمال البحث والتحري عن الجرائم الإلكترونية وجرائم الإعلام الآلي، وهو هيئة تقنية تعمل تحت وصاية مديرية الأمن العمومي والاستعمال لقيادة الدرك الوطني، تم إنشاؤه سنة 2015 ببئر مراد رايس بالجزائر العاصمة، حيث يتولى المهام التالية:

- القيام بمراقبة الاتصالات الإلكترونية بما يسمح به القانون لفائدة وحدات الدرك الوطني والجهات القضائية.
- مساعدة الوحدات الإقليمية للدرك الوطني في معاينة الجرائم المرتبطة بتكنولوجيا الإعلام والاتصال، والبحث عن الأدلة عبر شبكة الإنترنت والأجهزة الإلكترونية.

[1] نبيل. ق، "إنشاء مركز لمكافحة الجريمة المعلوماتية في الجزائر"، مقال منشور على الموقع الإخباري جزايرس، في 2008/05/17، متاح على الرابط التالي: https://www.djazairess.com/alfadjr/71333 تاريخ الاطلاع 2021/11/20 على الساعة 19:05.

[2] مباركة بن عمراوي، العقيد في الدرك الوطني جمال بن رجم للإذاعة 95 بالمائة من الجرائم الإلكترونية تم حلها بنجاح، المرجع السابق.

- المشاركة في عمليات التحري من خلال التسرب عبر شبكة الانترنت لفائدة مصالح الدرك الوطني والسلطات القضائية.
- العمل على ضمان المراقبة الدائمة والمستمرة لشبكة الإنترنت.[1]

وفي إطار مكافحة الجرائم الإلكترونية عالج هذا المركز سنة 2015 ما يقارب 240 قضية متعلقة بالجرائم الإلكترونية تنوعت بين جرائم التهديد والتحريض، جرائم الاختراق والقرصنة، جرائم التحرش الجنسي بالأطفال وتحريضهم على الفسق والدعارة، جرائم إهانة رموز وطنية وهيئات حكومية، جرائم النصب والاحتيال، جرائم الاعتداء على حرمة الحياة الخاصة...الخ.[2]

كما تم إنشاء بعض المصالح الأخرى على نفس المستوى المركزي من بينها مديرية الأمن العمومي والاستغلال وهي عبارة عن هيئة تعمل على التنسيق بين مختلف الوحدات الإقليمية والمركز التقني العلمي في مجال البحث والتحري عن الجرائم الإلكترونية، وكذا المصلحة المركزية للتحريات الجنائية والتي تعمل على التحري في جميع أنواع الجرائم بما فيها الجرائم الإلكترونية والجرائم المرتبطة بتكنولوجيات الإعلام والاتصال.[3]

2) على المستوى الجهوي:

تختص المصالح الجهوية التابعة للدرك الوطني بمهمة التنسيق بين مختلف الوحدات التابعة للشرطة القضائية وتقديم الدعم لها بخصوص الوسائل والإمكانيات الخاصة بالتحريات في الجرائم الإلكترونية، حيث يلعب الدرك الوطني دورا هاما في مكافحة الإجرام المعلوماتي نظرا لانتشار وحداته على مستوى كامل التراب الوطني بما يتوفر عليه من وسائل مادية وأفراد مؤهلين للتحري عن هذا النوع من الإجرام الخطير والمعقد.

3) على المستوى المحلي:

يحوز الدرك الوطني على عدة فرق فرعية تتمتع بالكفاءة والاختصاص الواسع في مجال التحري في الجرائم الإلكترونية، تتولى مهمة مكافحة جميع الجرائم بما فيها الجريمة الإلكترونية، وذلك عن طريق القيام

[1] حسين ربيعي، آليات البحث والتحقيق في الجرائم المعلوماتية، المرجع السابق، ص 185.

[2] عزالدين عزالدين، قيادة الدرك الوطني، الإطار القانوني للوقاية من الجرائم المعلوماتية ومكافحتها، بحث مقدم إلى أعمال الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة، 16-17 نوفمبر 2015، جامعة بسكرة، الجزائر، ص 29.

[3] حسين ربيعي، آليات البحث والتحقيق في الجرائم المعلوماتية، المرجع السابق، ص 183.

بتحقيقات تتطلب تحريات معقدة، وهي بذلك تساهم في تدعيم نشاط الأبحاث والتحريات التي تقوم بها الفرق الإقليمية للدرك الوطني، حيث أعيد تنظيم هذه الفرق بتاريخ 21 جويلية 2004بموجب التعليمة رقم 223-04 الصادرة عن ديوان قيادة الدرك الوطني، وذلك تماشيا مع طبيعة الجرائم محل المعاينة، إذ تم إنشاء خلية متخصصة لمكافحة الجرائم المتعلقة بتكنولوجيا الإعلام والاتصال في سبعة عشر (17) مجموعة ولائية، كل هذا لضمان التصدي الفعال لهذه الجرائم.[1]

مما تقدم ذكره يمكن القول بأنه كنتيجة لزيادة معدلات الجريمة الإلكترونية التي أصبحت تهدد جميع ميادين الحياة، سارعت الدول العربية على غرار الدول الأجنبية باستحداث العديد من الأجهزة والفرق المعنية بمحاربة هذه الجرائم والتحري فيها والتي رأيناها سابقا، حيث كانت دولة الإمارات العربية المتحدة من الدول السباقة التي عرفت تطورا كبيرا في مجال الإلكترونيات، تليها المملكة العربية السعودية ثم تأتي بعض الدول العربية الأخرى ومن بينها الجزائر، فرغم تأخر الحكومة الجزائرية عن الالتحاق بالركب المتطور إلا أنها عرفت سن بعض القوانين واستحداث بعض الوحدات لتختص بمتابعة هذا النوع من الإجرام، كما تقوم هذه الدول بدورات تكوينية لتدريب الضباط وتأهيلهم في مجال التعامل مع الأجهزة الإلكترونية والفضاءات الافتراضية والأدلة الرقمية وغيرها، ولكن من خلال دراستنا توصلنا لنتيجة مفادها أنه رغم وجود هذه الوحدات لكن بمقارنتها مع التزايد الهائل للجرائم الإلكترونية وكذا تطور أساليب مجرمي الإنترنت لا زالت قاصرة نوعا ما عن ضبط ومحاربة هذه الجريمة بشكل فعال، لذا أصبح لزاما على الدول العربية بصفة عامة والجزائر بصفة خاصة أن تكثف التدريب في هذا المجال وتطور من وسائل وأساليب التحقيق في هذه الجرائم، ولما لا تصبح الدول العربية أفضل من الدول الأجنبية في التصدي لهذه الجرائم.

[1] المرجع نفسه، ص 186-187.

إضافة للوحدات التابعة لمديرية الأمن والدرك الوطنيين نجد أن المديرية العامة للجمارك لا تحوز لحد الساعة على خلية أو فرقة مختصة بمعالجة الجرائم الإلكترونية، وإنما توفر لجميع مرتفقيها وكل المواطنين خلية إلكترونية للإعلام والاتصال على مستوى المديرية العامة للجمارك، وخلية الإصغاء والتوجيه خاصة بدراسة انشغالات الجمركيين وحل مشاكلهم، وخلية على مستوى المديريات الجهوية تسمى بخلية الصحافة يتم من خلالها إرسال البيانات الصحفية والعمليات المنجزة من هذه المصلحة مرفقة بالصور والفيديوهات للعمليات الهامة والحساسة التي أنجزتها المديرية، وإرسالها للقنوات الإعلامية والصحفيين من أجل تسجيل الحدث، وأما فيما يخص خلية مختصة بمعالجة الجرائم الإلكترونية فقط تم إثارة هذا الموضوع مؤخرا من طرف المدير العام للجمارك لكن لم يتم استحداثها لحد اليوم، معلومات مقدمة من طرف الملازم الأول لمصلحة الجمارك، بتيارت، بتاريخ 2021/11/01.

المبحث الثاني: وحدات البحث والتحري عن الجرائم الإلكترونية على المستوى الإقليمي والدولي

نتيجة للانتشار الواسع للجرائم الإلكترونية التي أصبحت تتميز بالطابع العالمي والبعد الدولي قد أثبت الواقع العملي أنه لا تستطيع أي دولة بجهودها المنفردة وأجهزتها الداخلية القضاء على هاته الجرائم بل تحتاج إلى تعاون دولي يتفق والطبيعة الخاصة لهذه الجرائم، حيث يكفل هذا الأخير كيفيات سير إجراءات البحث والتحري فيها ويسمح بالاتصال المباشر بين أجهزة الشرطة في الدول المختلفة، وهذا ما لا يتأتى إلا عن طريق إنشاء هيئات أمنية إقليمية ودولية ومكاتب متخصصة لجمع المعلومات عن مرتكبي هذه الجرائم، وخلق قنوات اتصال لتبادل الخبرات والمعارف الفنية في مجال التحري في الجرائم الإلكترونية عن طريق عقد الدورات التدريبية، فلا تكفي المساعدة الأمنية الدولية وحدها للتصدي لهذه الجرائم بل لابد من مصاحبتها بالمساعدة الفنية وتبادل الخبرات لأن سلطات الأمن والأجهزة الشرطية ليست بذات الجاهزية والكفاءة لمواجهة الجرائم الإلكترونية في جميع الدول إنما تختلف من دولة لأخرى حسب درجة تقدمها وتطورها في هذا المجال، من هذا المنطلق ناشدت معظم الاتفاقيات الدولية والإقليمية ذات الصلة بضرورة إنشاء وحدات وهيئات مختصة بالبحث والتحري في هذه الجرائم، وهذا ما سنتطرق له بالدراسة من خلال المطالب التالية:

المطلب الأول: وحدات البحث والتحري عن الجرائم الإلكترونية على المستوى الإقليمي

لعل من مظاهر التعاون الشرطي الإقليمي ما جسدته العديد من الاتفاقيات الإقليمية والتي نادت بضرورة توحيد جهود الدول في مكافحة الجرائم العابرة للحدود من بينها الجرائم الإلكترونية، إذ تم إنشاء الشرطة الأوروبية (الأوروبول)، وكذا جهاز الأوروجست على المستوى الأوروبي، في حين أنشأ الاتحاد الإفريقي للتعاون الشرطي على مستوى الدول الإفريقية، كما بادرت أغلب الدول العربية بإنشاء وحدات وأجهزة أمنية للتصدي لهذه الجرائم، أهمها المكتب العربي للشرطة الجنائية وغيرها من الأجهزة التي سوف نتطرق لها بالتفصيل في النقاط التالية.

الفرع الأول: على المستوى الأوروبي

من أبرز الهياكل أو الأجهزة الشرطية على المستوى الأوروبي نجد مركز الشرطة الأوروبية (جهاز الأوروبول) وجهاز (الأوروجست).

أولا: جهاز الأورو بول أو مركز الشرطة الأوروبية

أنشئ جهاز الأورو بول على مستوى الاتحاد الأوروبي عام 1992 بمدينة لاهاي بلكسمبورغ[1]، ليكون حلقة وصل بين أجهزة الشرطة الوطنية للدول الأعضاء في مجال محاربة الجرائم الخطيرة كالجرائم الإرهابية، وجرائم المخدرات والجريمة المنظمة، وكذا الجرائم المعلوماتية، إذ يتكفل هذا الجهاز بمكافحة هذه الجرائم عن طريق معالجة المعلومات المرتبطة بالأنشطة الإجرامية على مستوى الاتحاد الأوروبي، كما يقوم بدعم وتشجيع سلطات التحقيق في تحديث وسائلها وتطويرها لتصبح أكثر فعالية في التصدي للإجرام بصفة عامة، ويقوم أيضا بتسهيل تبادل المعلومات عن طريق تزويد المحققين بتحاليل علمية ودعمهم بالخبرات والمساعدات التقنية اللازمة والتي تساعدهم في التحري حول الجرم ومرتكبه، ومدهم بمختلف التقارير حول هوية المتهمين والأدلة المحصلة من هذه الجرائم، [2] ويرصد هذا الجهاز هيكلا بشريا يضم أكثر من 600 شخص يضمنون التنسيق والدعم للمحققين الميدانيين سواء تعلق الأمر بدعمهم بالبيانات اللازمة أو التقنيات في مجال التحقيق.[3]

وقد شهد الأورو بول سنة 2008 طفرة نوعية غيرت من وسائل عمله وصلاحياته، فبتاريخ 24 أكتوبر 2008 تقرر بلكسمبورغ إنشاء قاعدة بيانات[4] أوروبية مشتركة تخضع لتسيير منظمة الأورو بول وتضمن التنسيق بين عمل جهات الشرطة للدول الأعضاء من خلال إحصاء وجمع كافة القضايا الإجرامية التي لها علاقة بالمعلوماتية، وتطبيقا لذلك فقد اعتمد مجلس الوزراء الأوروبي المنعقد ببروكسل بلجيكا في 22 نوفمبر 2000 بمناسبة مناقشة مشروع(Télécom Paquet)فكرة منح الأورو بول صلاحية ومهمة

[1] ترجع فكرة إنشاء هذا الجهاز إلى اقتراح تقدم به المستشار الألماني "Helmut Kohl" أثناء قمة لكسمبورغ في 1991/06/23، كنموذج للشرطة الفيدرالية الألمانية أي بمثابة "FBI" مكتب فيدرالي أوروبي للتحقيقات، غير أن هذا المكتب أو الجهاز تجسد فعليا سنة 1995 وذلك بعد مصادقة دول المجلس الأوروبي على اتفاقية ماستريخت في 1995/07/29 واتخذ من لاهاي مقرا له.

[2] نبيلة هبة هروال، الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات، المرجع السابق، ص 158.

[3] حسين ربيعي، آليات البحث والتحقيق في الجرائم المعلوماتية، المرجع السابق، ص 152.

[4] قاعدة البيانات هي مجموعة منظّمة من المعلومات المهيكلة أو البيانات المخزّنة عادةً بصيغة إلكترونيّة أو في نظام كمبيوتر. عادةً ما تكون قاعدة البيانات تحت تحكم نظام إدارة قاعدة بيانات(DBMS) ووفقا لهذا النظام تتم الإشارة إلى البيانات ونظام إدارة قواعد البيانات جنبًا إلى جنب مع التطبيقات المرتبطة بهما باعتبارها نظام قواعد بيانات وغالبًا ما يتم اختصاره إلى قاعدة بيانات فقط، وعادةً ما تتم صياغة البيانات ضمن الأنواع الأكثر شيوعًا من قواعد البيانات المستعملة اليوم على هيئة صفوف وأعمدة في سلسلة من الجداول لإضفاء الفاعلية على المعالجة والاستعلام عن البيانات .ويمكن حينئذٍ الوصول إلى البيانات وإدارتها وتعديلها وتحديثها والتحكم فيها وتنظيمها بسهولة تامة.

ملاحقة ومتابعة مجرمي المعلومات، من خلال اعتماد أسلوب الدوريات الإلكترونية وذلك بتجميع المعلومات التي يوفرها مزودو الخدمة بالإنترنت وقوات الشرطة.[1]

وللأورو بول دورا فعالا في مكافحة الجريمة الإلكترونية إذ تم اختياره من طرف الاتحاد الدولي للأمن المعلوماتي لإنجاز مختلف الدراسات الخاصة بالجريمة الإلكترونية، وذلك لغاية 2020 بهدف تحليل دوافع هذه الجرائم ووضع تصور مستقبلي لتطورها، وهو ما يفسر الثقة التي وضعتها فيه اللجنة الأوروبية باختيارها له كمركز إعلام حول موضوع الجرائم المعلوماتية، إذ تم استحداث جهاز على مستوى الأورو بول عام 2010 أطلق عليه اسم "ICROS : Internet Crime Reporting Online"مهمته توفير أكبر قدر من التعاون والتنسيق الأمني في مجال مكافحة الجرائم الإلكترونية بين دول الاتحاد الأوروبي، والذي تم تدعيمه في جويلية 2017 بهيئة أخرى متخصصة تدعى المركز الأوروبي للجريمة الإلكترونية "EC3" والذي اعتبر همزة وصل بين الدول الأعضاء ومركزا للدعم الاستخباراتي والتشغيلي والقضائي، بحيث يعمل على تزويد الشرطة وسلطات إنفاذ القانون في الدول الأعضاء بالمعلومات اللازمة حول اتجاهات هذه الجرائم.[2]

من جهة أخرى أنشأ الأورو بول مركزا آخرا خاصا بمكافحة الجريمة الإلكترونية وذلك سنة 2013، حيث يعتبر هذا المركز نقطة محورية على المستوى الأوروبي في مجال مكافحة الجرائم الإلكترونية، إذ يهدف لحماية المواطنين الأوروبيين والشركات من التهديدات عبر الإنترنت، وكذا حماية المعلومات الشخصية الخاصة بهم، كما يعمل على تحذير الدول الأعضاء في الاتحاد الأوروبي من التهديدات السيبرانية وتقديم الدعم التقني في التحقيقات الأمنية، سواء عبر تحليل المعلومات أو تشكيل فرق التحقق المشترك مع المؤسسات الأمنية الرئيسية.[3]

ليس هذا وحسب بل ولتفعيل وتوسيع التعاون الأمني عبر الحدود يتعامل الأورو بول مع وكالات استخباراتية متخصصة وأنظمة مراقبة ذات خبرة عالية، من بينها وكالة "فرونتكس Frontex" وهي وكالة

[1] ربيعي حسين، آليات البحث والتحقيق في الجرائم المعلوماتية، المرجع السابق، ص 153.

[2] جمال براهيمي، التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص 305- 306.

[3] لبيب فهمي، "مركز أوروبي لمكافحة الجريمة الإلكترونية"، 2012/03/28، مقال منشور على الرابط التالي: https://www.aljazeera.net/news/reportsandinterviews/2012/3/29/ تاريخ الاطلاع 2021/11/30 على الساعة 12:30.

أوروبية تعمل على إدارة التعاون العملياتي على الحدود الخارجية للدول أعضاء الاتحاد الأوروبي، [1] ونظام "الأورو داك Eurodac"[2] وهو نظام معلوماتي واسع النطاق يحوي على البصمات الرقمية لطالبي اللجوء والمهاجرين غير الشرعيين المتواجدين على إقليم الاتحاد الأوروبي، وكذا نظام "الأوروسير Eurosur" وهو نظام لتبادل المعلومات بخصوص مراقبة الحدود الأوروبية، يشتمل على برنامج مشترك لتكنولوجيا المعلومات ويعمل على تمكين السلطات المشاركة في تقييم الوضع على الحدود الخارجية للاتحاد.[3]

ومن بين أبرز العمليات التي قامت بها الأورو بول في مجال مكافحة جرائم الإنترنت، عملية "أوديسيوس Odysseus" التي تمت في 26 فبراير 2004 بمبادرة من الأورو بول، وقامت قوات الشرطة خلالها بعمليات شملت 10 دول هي (أستراليا، بلجيكا، كندا، ألمانيا، هولندا، النرويج، بيرو، اسبانيا، السويد، بريطانيا)، كذلك عملية أخرى اشتهرت باسم "محطم الجليد Icebreaker" في 14 يونيو 2005 والتي تم من خلالها مداهمة وتفتيش شبكات الحاسب الآلي وتوقيف أشخاص في ثلاثة عشرة دولة أوروبية هي (النمسا، بلجيكا، فرنسا، ألمانيا، المجر، ايسلندا، إيطاليا، هولندا، بولونيا، البرتغال، سلوفاكيا، السويد، بريطانيا العظمى).[4]

ثانيا: جهاز الأورو جست

جهاز الأورو جست هو جهاز يعمل على المستوى الأوروبي إلى جانب جهاز الأورو بول، في مجال مكافحة جميع أنواع الجرائم الخطيرة، حيث تم إنشاؤه من قبل مجلس الاتحاد الأوروبي في 2002/02/22، وينعقد اختصاصه إذا ما تعلق الأمر بجرائم يكون طرفا فيها على الأقل دولتين من دول الاتحاد الأوروبي أو دولة واحدة إذا ما تعلقت مصالحها بمصالح الاتحاد الأوروبي، [5] ويعمل جهاز الأورو جست على تطوير آلياته لمكافحة الجرائم الإلكترونية من خلال تبادل المعلومات بصفة دورية مع الأجهزة الأخرى من بينها جهاز

[1] "الفرونتكس" هي وكالة أوروبية تأسست في الفاتح من ماي 2005 ودخلت حيز الخدمة في أكتوبر 2005، مقرها بوار شو ببولندا، وهي مسؤولة عن تنسيق نشاطات الحدود الوطنية الخاصة بضمان أمن الحدود في أوروبا مع الدول غير الأعضاء.

[2] لمزيد من التفاصيل حول نظام الأورو داك ينظر الرابط التالي:
https://secure.edps.europa.eu/EDPSWEB/edps/Supervision/Eurodac تاريخ الاطلاع 2021/11/30 على الساعة 16:00.

[3] جمال براهيمي، التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص 305.

[4] جان فرانسوا هنروت، أهمية التعاون الدولي والتجربة البلجيكية في تبادل المعلومات بين عناصر الشرطة والتعاون القضائي، بحث مقدم إلى الندوة الإقليمية حول الجرائم المتصلة بالكمبيوتر ضمن برنامج تعزيز حكم القانون في بعض الدول العربية، المملكة المغربية، في 19- 20 يونيو 2007، ص 108.

[5] نعيم سعيداني، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة مقدمة لنيل شهادة الماجستير، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر باتنة، 2013/2012، ص 108.

الأورو بول، فهو على علاقة وثيقة به إذ يمده بالتحليلات اللازمة للقيام بالتحقيقات في الجرائم المنظمة والخطيرة والجرائم الإلكترونية، وهو يتكون من نواب عامين، ومستشارين قضائيين، وضباط شرطة قضائية للدول الأعضاء في الاتحاد الأوروبي ذوي الاختصاص والمندوبين من قبل كل دولة عضو في الاتحاد.[1]

وتتركز أهم نشاطاته في سبيل التصدي للجرائم الخطيرة بما فيها الجريمة الإلكترونية، في تطوير التنسيق والتعاون بين السلطات القضائية المختصة للدول الأعضاء، وكذا الاستجابة لطلبات المساعدة القضائية، تبادل المعطيات بين هذه الدول والتحفظ عليها، كما يمكن للوكلاء والنواب العامين ذوي الاختصاص الوطني إجراء تحقيقات أو ملاحقات أو التبليغ عن الجرائم إلى السلطات المختصة للدول الأعضاء.[2]

الفرع الثاني: على المستوى الإفريقي (آلية الاتحاد الإفريقي للتعاون الشرطي "أفريبول")

حظيت آلية الاتحاد الإفريقي للتعاون الشرطي "أفر يبول" باهتمام دولي كبير من طرف الدول المهتمة بتحقيق الأمن والسلم العالميين والتصدي للجرائم بأشكالها، ولا شك أن الوقوف حول مفهوم هذه الآلية _كآلية مستحدثة من بين أهم آليات التعاون الأمني الشرطي في مجال مكافحة الجريمة _ يتطلب بالدرجة الأولى تحديد نشأتها والهيكل التنظيمي لها، وكذا تبيان مهامها أو دورها في التصدي لمختلف أشكال الإجرام بما فيه الإجرام المعلوماتي.

---

[1] نبيلة هبة هروال، الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات، المرجع السابق، ص 160.

[2] نبيلة هبة هروال، الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات، المرجع السابق ، ص 160.

إلى جانب جهازي الأورو بول والأورو جست، لقد تم إنشاء فضاء جماعي من غير حدود سمي بفضاء شنجن (Espace communautaire sansfrontiéres – Schengen)وذلك بمناسبة التوقيع على معاهدة شنجن في 1985/06/14 وعلى اتفاقية تطبيق هذه المعاهدة في 1990/06/19، حيث استحدثت هذه الاتفاقية وسيلتين جديدتين لتعزيز التعاون الشرطي الأوروبي لمواجهة التحديات التي تفرضها الظروف الجديدة والتي من بينها الجريمة الإلكترونية أو جرائم الإنترنت، تمثلت في مراقبة المشتبه فيهم عبر الحدود وكذا ملاحقة المجرمين خارج الحدود الوطنية طبقا لنص المادتين 40 و41 من الاتفاقية، هذا من جهة ومن جهة أخرى فقد نصت الاتفاقية على إنشاء نظام لتسجيل المعلومات يسمى بنظام معلومات شنجن"Le systéme d'information Schengen " يمثل قاعدة تكنولوجية للمعلومات المتعلقة بالأشخاص المطلوبين والأموال والأسلحة وكل ما يتم البحث عنه، كما يساهم ها النظام في ملاحقة ومنع بث الصور الإباحية عبر الإنترنت في الدول الأطراف، ويتكون نظام معلومات شنجن من قسم مركزي ومقره ستراسبورغ وأقسام وطنية في كل دولة من دول المنظمة، ويحتوي على بنك معلومات كبير تسجل فيه المعلومات التي ترسلها إليه قوات الشرطة والسلطات القضائية في كل دولة، ومن بين هذه المعلومات عناوين الأفراد المطلوب تسليمهم والممنوعين من دخول أراضي دولة ما، أو المعلن اختفاؤهم أو المطلوبين أمام العدالة.

أولا: نشأة الآلية وهيكلها التنظيمي

الأفريبول أو منظمة الشرطة الجنائية الإفريقية هي أكبر منظمة شرطة في القارة الإفريقية ترجع فكرة إنشائها لسنة 2013 بمناسبة انعقاد المؤتمر الإقليمي الإفريقي الثاني والعشرون(22) للإنتربول والمنعقد في الفترة الممتدة من 10 إلى 12 سبتمبر 2013 بوهران (الجزائر) والذي شهد حضور كافة قادة الشرطة الأفارقة الواحد والأربعون، وفي فيفري 2014 تم اعتماد إعلان الجزائر بخصوص إنشاء آلية للاتحاد الإفريقي للتعاون الشرطي، وخلال المؤتمر التاسع والثلاثون (39) لقادة الأمن والشرطة العرب المنعقد يومي 9 و10 ديسمبر 2015 بتونس تبنى المشاركون بإجماع المبادرة التي تقدمت بها الجزائر حول إنشاء هذه الآلية وذلك باعتبار عشرة (10) دول عربية تقع بالقارة الإفريقية، وحدد مقرها بالجزائر العاصمة.[1]

وبتاريخ 13 ديسمبر 2015 تم الافتتاح الرسمي لمقر الأفريبول الذي أقيم بالعاصمة الجزائرية بحضور ممثلي أجهزة الشرطة ل 41 بلدا إفريقيا، وبتاريخ 30 يناير 2017 تم اعتماد النظام الأساسي لآلية الأفريبول من قبل مؤتمر الاتحاد الإفريقي في دورته العادية رقم 28 المنعقدة بباديس أبابا- اثيوبيا ليدخل حيز النفاذ بهذا التاريخ.[2]

أما عن هيكلها التنظيمي فقد نصت المادة السابعة (7) من النظام الأساسي لآلية الاتحاد الإفريقي للتعاون الشرطي "أفريبول" على أنها تضم في تشكيلتها كل من الجمعية العامة، لجنة التوجيه، الأمانة، ومكاتب الاتصال الوطنية، سنتعرف عليها فيما يأتي:

1) الجمعية العامة:

هي السلطة العليا للأفريبول، والهيئة الفنية والتقنية المكلفة بإدارة شؤون الشرطة في إفريقيا على المستوى الاستراتيجي والعملياتي، حيث تتمثل مسؤوليتها في توفير التوجيه القيادي فيما يتعلق بالتعاون

[1] انعقاد المؤتمر التاسع والثلاثون (39) لقادة الشرطة والأمن العرب حول تبني مبادرة الجزائر حول إنشاء منظمة الشرطة الإفريقية (أفريبول)، المنعقد بتونس، بتاريخ 2015/12/10. لمزيد من التفاصيل يراجع موقع مديرية الأمن الوطني المتاح على الرابط التالي: https://www.algeriepolice.dz/IMG/pdf/communiqarr10122015.pdf تاريخ الاطلاع 2021/11/20 على الساعة 19:50.

[2] تم تدشين مقر آلية التعاون للشرطة الإفريقية (أفريبول) يوم الأحد 13 ديسمبر 2015، تحت إشراف معالي وزير الداخلية والجماعات المحلية السيد نور الدين بدوي رفقة اللواء عبد الغني هامل المدير العام للأمن الوطني، وممثلي أجهزة الشرطة لأزيد من أربعين (40) بلدا افريقيا. لمزيد من التفاصيل يراجع موقع مديرية الأمن الوطني المتاح على الرابط التالي: https://www.algeriepolice.dz/IMG/pdf/communiqar13122015-2.pdf تاريخ الاطلاع 2021/11/22 على الساعة 22:17.

الشرطي في إفريقيا[1]، ويتشكل مكتب الجمعية العامة من خمسة أعضاء: الرئيس، وثلاث نواب ومقرر واحد، يتم انتخابهم على أساس التناوب لولاية مدتها سنتين غير قابلة للتجديد، يمثلون الأقاليم الخمسة وفقا لما حدده الاتحاد الإفريقي وهذا ما نصت عليه المادة الثامنة في فقرتها الثالثة "ي" من النظام الأساسي لآلية الاتحاد الإفريقي للتعاون الشرطي.[2]

تضطلع الجمعية العامة للأفريبول بعدة مهام فهي المسئولة عن وضع السياسات وإعداد الخطوط التوجيهية وتحديد أولويات عمل الأفريبول والإشراف على تنفيذها، والحرص على تنفيذ النظام الأساسي للمنظمة[3]، وكذا إعداد التقارير السنوية عن عملها وتقديمها إلى أجهزة صنع السياسة للاتحاد الإفريقي[4]، بالإضافة إلى هذه المهام فلها أن تقوم بوظائف أخرى بغية ضمان تنفيذ النظام الأساسي لهذه الآلية وكذا الصكوك والسياسات الأخرى ذات الصلة[5]، وتجدر الإشارة إلى أنه تجتمع الأفريبول في دورة عادية كل سنة كما لها أن تعقد دورات استثنائية بناء على طلب مقدم من طرف الجمعية العامة أو أجهزة صنع السياسة للاتحاد الإفريقي أو أي دولة من الدول الأعضاء بشرط موافقة الأغلبية البسيطة من الدول الأعضاء على ذلك، [6] وفي هذا الصدد تم انعقاد الجمعية العامة الأولى لآلية الاتحاد الإفريقي بالجزائر العاصمة في الفترة الممتدة من 14 إلى 16 ماي 2017، والتي تم فيها انتخاب السيد اللواء المدير العام للأمن الوطني كمدير تنفيذي لآلية الأفريبول لمدة سنتين، وانبثق عن أشغال هذه الجمعية المصادقة على البرنامج الثلاثي للأفريبول 2019/2017 الذي تمثلت أهم أهدافه في خلق مكاتب الاتصال الوطنية في مجال التعاون الشرطي الإفريقي، ووضع نظام الاتصال المسمى "أف. سي. كوم" كوسيلة اتصال حديثة وآمنة تمكن من ربط هذه المكاتب من الأمانة العامة للأفريبول في كل ما يتعلق بالمعلومات المرتبطة بمكافحة مختلف أشكال الجريمة في القارة الإفريقية، وكذا التعاون مع المنظمات الأخرى وتعزيز قدرات الهيئات الشرطية الإفريقية.[7]

---

[1] ينظر المادة 08 فقرة 01 من النظام الأساسي لآلية الاتحاد الافريقي للتعاون الشرطي "أفريبول".

[2] ينظر المادة 08 فقرة 03 "ي" من نفس النظام الأساسي

[3] ينظر المادة 08 فقرة 03 "أ" و"ب" من نفس النظام الأساسي

[4] تنص المادة 01 من النظام الأساسي لآلية الاتحاد الافريقي للتعاون الشرطي "أفريبول": تعني كلمة أجهزة صنع السياسة "أجهزة صنع السياسة للاتحاد الافريقي كما هو محدد في القانون التأسيسي"، ويقصد بها الأجهزة الحكومية التي تتخذ القرارات داخل الاتحاد.

[5] ينظر المادة 08 فقرة 03 "م" من نفس النظام الأساسي

[6] ينظر المادتين 15 و16 من نفس النظام الأساسي

[7] عميد الشرطة القضائية تابع لمكتب التعاون الدولي بمديرية الشرطة القضائية، "البعد الدولي للشرطة الجزائرية في مكافحة الجريمة المنظمة العابرة للحدود الوطنية"، مداخلة مقدمة للندوة الوطنية حول التعاون الشرطي في مجال مكافحة الجريمة المنظمة، جامعة تبسة، 16 أفريل 2018، ص 08.

2) لجنة التوجيه:

تعد لجنة التوجيه الجهاز التنفيذي لآلية الاتحاد الإفريقي للتعاون الشرطي وتتشكل من أعضاء مكتب الجمعية العامة (رئيس وثلاث نواب ومقرر) ومن مفوض السلم والأمن للاتحاد الإفريقي، ورؤساء المنظمات الإقليمية للتعاون الشرطي، والمدير التنفيذي لآلية الاتحاد الإفريقي، حيث يترأس لجنة التوجيه رئيس الجمعية العامة.[1]

أما عن وظائف لجنة التوجيه فيتم النص عليها في قواعد الإجراءات المطبقة في الاتحاد الإفريقي وفقا للمادة 09 فقرة 3 من النظام الأساسي لآلية الاتحاد الإفريقي للتعاون الشرطي "أفريبول".[2]

3) الأمانة:

تتشكل أمانة آلية الأفريبول من المدير وهو المسئول التنفيذي للأفريبول والذي يتم تعيينه بناء على توصية مقدمة من لجنة التوجيه للجمعية العامة، ويساعده في مهامه عدد من العاملين ذوي الخبرة والمؤهلات المناسبة، الذين يتم تعيينهم وفقا لقواعد ولوائح العاملين في الاتحاد الإفريقي، أما عن مهام أمانة الأفريبول فنجد المادة 10 فقرة 7 من النظام الأساسي قد حصرت المهام المنوطة بالأمانة نذكر من بينها[3]:

- ضمان الإدارة الفعالة للأفريبول
- عقد وخدمة اجتماعات آلية الأفريبول بما فيها اجتماعات الجمعية العامة ولجنة التوجيه، وكتابة محاضر بذلك وحفظها.
- تنفيذ قرارات الجمعية العامة ولجنة التوجيه.
- الإبقاء على اتصالات مع سلطات إنفاذ القانون الوطنية والدولية.
- الاضطلاع بأي وظيفة أخرى يتم تكليفها بها من قبل الجمعية العامة أو أي جهاز من الأجهزة ذات الصلة.

[1] ينظر المادة 09 فقرة 2 من النظام الأساسي لآلية الاتحاد الافريقي للتعاون الشرطي "أفريبول".
[2] ينظر المادة 09 فقرة 3 من نفس النظام الأساسي
[3] ينظر المادة 10 فقرة 7 من نفس النظام الأساسي

4) مكاتب الاتصال الوطنية:

تنشئ كل دولة عضو في الاتحاد الإفريقي للتعاون الشرطي "أفريبول" مكتب اتصال وطني للأفريبول وفقا لما تنص عليه تشريعاتها الوطنية، وهذا لضمان سلامة وسهولة سير وتنفيذ أنشطة هذه المنظمة، وكذا تبادل المعلومات[1]، حيث قد بلغ عدد هذه المكاتب تقريبا أكثر من 30 مكتبا.[2]

ثانيا: مهام المنظمة

في إطار تنفيذ إستراتيجية الاتحاد الإفريقي للتعاون الشرطي "أفريبول" في مواجهة الجرائم الخطيرة سطرت هذه الآلية جملة من الأهداف التي تصب كلها في مجال التعاون الشرطي وذلك على كل من المستوى الوطني والإقليمي والدولي، حيث حصرت المادة الثالثة (3) من النظام الأساسي للاتحاد الإفريقي هذه الأهداف، وقد عملت هذه الآلية على تحقيقها إذ يقوم الأفريبول لمواجهة هذه التهديدات والجرائم الخطيرة بعدة مهام يمكن إجمالها فيما يلي:

- خلق مجال للتعاون بين مؤسسات الشرطة للدول الأعضاء على المستويات الوطنية والإقليمية والدولية، ومساعدتها على تحسين كفاءتها وفعاليتها من خلال تعزيز قدراتها التنظيمية والفنية والإستراتيجية والعملياتية، وهذا ما يتحقق بالقيام بدورات تكوينية لأجهزة الشرطة للدول الأعضاء بهدف تطوير خبراتهم وكفاءاتهم في مجال التحقيق ومتابعة الجرائم والتصدي الأمثل لها[3]، وفي هذا الصدد تم فعلا تنظيم عدة نشاطات تكوينية خلال سنة 2017 من أهمها تنظيم الدورة التكوينية الأولى حول تعزيز القدرات في مجال مكافحة الجريمة المنظمة العابرة للحدود الوطنية، والجريمة السيبرانية، وجرائم الإرهاب، والتي تم تنظيمها بتاريخ 24 و25 أكتوبر 2017 بمقر المراقبة التابع للمديرية العامة للأمن الوطني بالجزائر[4]، حيث ارتكزت هذه الدورة على ضرورة تكوين أجهزة الشرطة وتدعيم قدراتهم في مجال التحقيق والتحليل الجنائي، فضلا عن اعتماد مراكز خاصة بالشرطة العلمية والتقنية، أما عن الدورة التكوينية الثانية فكانت بتاريخ 14 مارس 2018 خاصة برؤساء المكاتب الوطنية للاتصال والتي كان هدفها الأساسي تكوين رؤساء

[1] ينظر المادة 11 من النظام الأساسي لآلية الاتحاد الافريقي للتعاون الشرطي "أفريبول".

[2] خديجة خالدي، آلية الاتحاد الافريقي للتعاون الشرطي " أفريبول"، مجلة العلوم الاجتماعية والانسانية، المجلد 11، العدد 01، سنة 2018، ص 76.

[3] ينظر المادة 04 فقرة "أ" و"ب" من النظام الأساسي لآلية الاتحاد الافريقي للتعاون الشرطي "أفريبول".

[4] خديجة خالدي، آلية الاتحاد الافريقي للتعاون الشرطي " أفريبول"، المرجع السابق، ص 70.

هذه المكاتب حتى تتمكن من مباشرة تنفيذ مهامها الشرطية، حيث أبرز عميد الشرطة ومدير مكتب التعاون الدولي بالمديرية العامة للأمن الوطني أن برنامج هذه الدورة ينقسم إلى محورين أولهما جاء ليبرز الصلاحيات والمهام المنوطة بمكاتب ارتباط الأفريبول، والثاني تقني يتعلق بنظام اتصال الأفريبول المسمى "أف. سي. كوم" كما ذكرنا سابقا[1]، والذي يجمع كافة أجهزة الشرطة الإفريقية في مجال تبادل المعلومات وقواعد البيانات، حيث أوصت الجمعية العامة للأفريبول بتدعيم وتسريع تفعيل هذا الجهاز.[2]

- العمل عند الاقتضاء ووفقا للقوانين الوطنية والدولية المعمول بها على تسهيل المساعدات القانونية المتبادلة، أو ترتيبات تسليم المجرمين بين الدول الأعضاء، وكذا تيسير تبادل أو تقاسم المعلومات أو الاستخبارات لمكافحة الجرائم المنظمة عبر الوطنية وجرائم الإرهاب والجريمة الإلكترونية[3]، وهذا ما لا يتأتى إلا عن طريق التعاون والتنسيق بين أجهزة الشرطة والوكالات الوطنية والإقليمية والدولية المعنية بإنفاذ القانون[4]، وفي هذا الصدد قررت الجمعية العامة الثانية للأفريبول في ختام أشغالها بالجزائر العاصمة في 18 أكتوبر 2018 إنشاء ثلاث فرق عمل تتكفل بمكافحة الجريمة العابرة للحدود والجريمة السيبرانية وكذا مكافحة الإرهاب والتطرف والوقاية منهما، حيث تم خلال أشغال هذه الجمعية تقديم مسح كامل لقضايا الإرهاب والتطرف والجرائم الإلكترونية بالقارة الإفريقية مع تسجيل بعض المقترحات حول كيفية التعامل مع هذه التهديدات والتصدي لها.[5]
- مساعدة الدول الأعضاء على تطوير وتحسين عمل الشرطة وأدوات ووسائل منع الجريمة، وتأهيل الكفاءات من أجهزة الشرطة الإفريقية من خلال المساعدة التقنية المتبادلة في مجالات التكوين وتبادل التجارب والخبرات في علم الإجرام والتحقيق الجنائي، وهذا باستعمال تكنولوجيات جديدة وناجعة، [6] وكذا تنظيم الاجتماعات التي تدرس كيفيات مكافحة هذه الجرائم نذكر من

---

[1] مقال حول "مدير مكتب التعاون الدولي بالمديرية العامة للأمن الوطني...تعزيز التعاون الشرطي الإفريقي أولويات الأفريبول"، مقال منشور بتاريخ 2018/03/14، متاح على الموقع التالي: https://elmaouid.dz، تاريخ الاطلاع 2021/08/25 على الساعة 18:00.

[2] أحلام بوكربوعة، آلية الاتحاد الإفريقي للتعاون الشرطي "أفريبول" ودورها في مكافحة ظاهرة الإرهاب، حوليات جامعة الجزائر 1، المجلد 34، العدد 04، سنة 2020، ص 615.

[3] ينظر المادة 04 فقرة "ج" و"د" من النظامالأساسي لآلية الاتحاد الافريقي للتعاون الشرطي "أفريبول".

[4] ينظر المادة 04 فقرة "د" من النظام الأساسي لآلية الاتحاد الافريقي للتعاون الشرطي "أفريبول".

[5] أحلام بوكربوعة، "آلية الاتحاد الإفريقي للتعاون الشرطي "أفريبول" ودورها في مكافحة ظاهرة الإرهاب"، المرجع السابق، ص 615. لمزيد من التفاصيل يراجع الموقع التالي: http://www.elmassar elarabi.com

[6] ينظر المادة 04 فقرة "ز" من النظام الأساسي لآلية الاتحاد الافريقي للتعاون الشرطي "أفريبول".

بينها، تنظيم اجتماع حول تعزيز التعاون في مجال مكافحة الجريمة الإلكترونية بتاريخ 13 و14 ديسمبر 2017 بمقر الأفريبول والذي خرج بعدة توصيات تهدف أساسا إلى الوقاية من الجرائم الإلكترونية ومكافحتها خاصة إنشاء فريق خبراء مختص في هذا النوع من الإجرام،[1] كما تعمل آلية الأفريبول كحلقة وصل مؤسسات الشرطة في الدول الأعضاء مع فريق الدعم الاستراتيجي الشرطي الذي أنشئ مؤخرا داخل قسم عمليات دعم السلام في إدارة السلم والأمن للاتحاد الإفريقي، وذلك في مجالات التخطيط والتعبئة ونشر الموظفين المكلفين بإنفاذ القانون وضباط الشرطة في عمليات دعم السلام التي يقودها الاتحاد الإفريقي، كما يمكن لها القيام بأية مهام أخرى في إطار التعاون الشرطي الإفريقي.[2]

- في إطار تعزيز قدرة القارة الإفريقية على مكافحة جرائم الإرهاب والجريمة المنظمة والجريمة السيبرانية، وقع الاتحاد الإفريقي للتعاون الشرطي "أفريبول" اتفاقا مع منظمة الشرطة الجنائية الدولية "الإنتربول" لتوفير منصة تعاون يتم من خلالها تبادل المعلومات والخبرات، هذا التحالف الذي تم إطلاقه في بداية سنة 2020 تنفيذا لخطة عمل مشتركة بين المنظمتين والتي حددت من 2020 إلى 2024، ونتيجة لهذا التحالف منح الأفريبول حق الوصول إلى مجموعة واسعة من قواعد بيانات الإنتربول الجنائية العالمية وإلى شبكة المنظمة للاتصالات الشرطية المأمونة المعروفة باسم (I-7/24) ما يتيح له العمل مباشرة مع أجهزة إنفاذ القانون في كل من البلدان ال 194 الأعضاء في منظمة الإنتربول، وفي يناير 2016 فتح الإنتربول مكتب ممثل خاص للمنظمة لدى الاتحاد الإفريقي لتعزيز فرص الاستفادة من إمكانات مكاتبه الإقليمية (زمبابوي، الكاميرون، كوت ديفوار، كينيا)، ومكاتبه المركزية الوطنية في إفريقيا.[3]

كما قام الإنتربول بتنفيذ مشروعا يدعى "I-One" في أرجاء إفريقيا سنة 2020[4] يرمي إلى تجهيز المكاتب المركزية الوطنية بأحدث معدات تكنولوجيا المعلومات وتدريبها حرصا على استدامة قدرات أجهزة إنفاذ

[1] خديجة خالدي، آلية الاتحاد الافريقي للتعاون الشرطي " أفريبول"، المرجع السابق، ص 70.

[2] ينظر المادة 04 من النظام الأساسي لآلية الاتحاد الافريقي للتعاون الشرطي "أفريبول".

[3] مقال حول "التحالف بين الإنتربول والأفريبول يدخل حيز النفاذ"، مقال منشور على الموقع الرسمي للمنظمة الدولية للشرطة الجنائية (الإنتربول)، متاح على الرابط التالي: https://www.interpol.int/ar/1/1/2020/20 تاريخ الاطلاع 2021/11/20 على الساعة 11:00

[4] حيث تغطي مثل هذه المشاريع ومبادرات التدريب وبناء القدرات التي ننفذها الإنتربول جميع مجالات الإجرام ومناطق العالم كافة، وتتمحور أنشطة التدريب التي نقدمها حول مبادرتين رئيسيتين تستندان إلى معايير الجودة وأفضل الممارسات:

القانون، وفي نفس الصدد يتيح برنامج منظومة المعلومات الشرطية لغرب إفريقيا (برنامج وابيس)[1] الذي ينفذه الإنتربول، جمع المعلومات الشرطية على نحو فعال بفضل منظومة وطنية مركزية ويساعد أجهزة إنفاذ القانون في إفريقيا على تعميم هذه المعلومات على المستوى الوطني والإقليمي والدولي.[2]

المطلب الثاني: وحدات البحث والتحري عن الجرائم الإلكترونية على المستوى الدولي

لقد دفعت زيادة التهديدات الإلكترونية أغلب الدول إلى تفعيل دور التعاون الشرطي أو الأمني الدولي، سعيا منها إلى تجاوز الصعوبات التي تطرحها عملية البحث والتحري عن هذه الجرائم وجمع الأدلة خارج الإقليم الوطني، كون هذه الجرائم تمتاز بالطابع العالمي العابر للحدود، وقد تجسد هذا التعاون في إنشاء واستحداث هيئات ووحدات دولية خاصة بمكافحة الجرائم الإلكترونية، تضمن الاتصال المباشر بين سلطات الأمن في الدول والتبادل السريع للمعلومات والخبرات بينها من أجل تحقيق أهداف لا قبل للشرطة الإقليمية بتحقيقها، ومن أبرزها المنظمة الدولية للشرطة الجنائية (الإنتربول)، والمنظمة الدولية للشرطة السيبرانية (سيباربول).

- أكاديمية الإنتربول الافتراضية: وهي المنصة الرقمية للتعليم
- أكاديمية الإنتربول العالمية: وهي شبكة شركاء الإنتربول الإقليميين في التدريب.

كما تقيم الإنتربول أيضا شراكات مع منظمات عامة وخاصة للاستفادة من خبراتها المتطورة، ومعرفة وسائل جديدة للتدريب لكي يعم بالفائدة على جميع الأعضاء ومن أجل التصدي الأمثل للمجرمين والجريمة بصفة عامة. لمزيد من التفاصيل يراجع الرابط التالي:https://www.interpol.int/ar/2/6

[1] ينفذ الإنتربول برنامج منظومة المعلومات الشرطية لغرب افريقيا (برنامج وابيس) بتمويل من الاتحاد الأوروبي، ويهدف البرنامج إلى تحسين تبادل المعلومات والتنسيق بين مختلف أجهزة إنفاذ القانون في المنطقة عبر:

- تمكين أفراد الشرطة في الدول في غرب أفريقيا من الوصول إلى المعلومات الشرطية الحساسة من قواعد البيانات الجنائية لدى أجهزتهم الوطنية ومن قواعد بيانات الدول في المنطقة، بما يحسّن الكشف عن المجرمين ويدعم التحقيقات الجارية.
- تحسين عملية تحليل التحديات الناجمة عن الجريمة المنظمة عبر الوطنية والإرهاب اللذين يتهددان المنطقة، وتكوين فهم أفضل عن الجرائم الناشئة في غرب أفريقيا.
- إتاحة المجال للتعاون القضائي والشرطي في المسائل الجنائية في الإقليم والاتحاد الأوروبي وفي سائر أنحاء العالم.

ويدعم برنامج وابيس الجهود المبذولة من الأجهزة الوطنية والجماعات الاقتصادية لدول غرب إفريقيا لتحسين الوضع الأمني للمواطنين في غرب أفريقيا، ويجري تنفيذه على ثلاثة أصعدة، وطني وإقليمي وعالمي. لمزيد من التفاصيل يراجع الرابط التالي: https://www.interpol.int/ar/2/6/6تاريخ الاطلاع 2021/11/21 على الساعة 13:10.

[2] لمزيد من التفاصيل يراجع الموقع الرسمي للمنظمة الدولية للشرطة الجنائية (الإنتربول)، المتاح على الرابط التالي: https://www.interpol.int تاريخ الاطلاع 2021/11/21 على الساعة 13:30.

الفرع الأول: المنظمة الدولية للشرطة الجنائية (الإنتربول)

تعد المنظمة الدولية للشرطة الجنائية "الإنتربول" من أقدم صور التعاون الشرطي في مكافحة الجريمة بأنواعها، وهي منظمة دولية حكومية ذات طبيعة اجتماعية كونها تضم العديد من الدول، تهدف إلى تتبع وملاحقة المجرمين على المستوى الدولي، وتشجيع سلطات وأجهزة الشرطة في الدول الأعضاء على التصدي لمختلف أشكال الإجرام بما فيه الإجرام المعلوماتي، وهذا من خلال تبنيها مجموعة من المبادئ التي تساعدها في تحقيق أهدافها، وقبل التطرق لأهداف هذه المنظمة ودورها في مكافحة الجرائم وجب علينا التطرق لمراحل نشأة الإنتربول والأجهزة التي تضمها هذه المنظمة.

أولا: نشأة المنظمة وهيكلها التنظيمي

لقد اقترنت نشأة المنظمة الدولية للشرطة الجنائية مع البدايات الأولى للتعاون الدولي في المجال الشرطي سنة 1904 والتي تظهر ملامحه ضمنا في الاتفاقية الدولية المتعلقة بالرقيق الأبيض المبرمة في 18 ماي 1904 والتي دعت الدول إلى إنشاء سلطة مركزية تختص بشِؤون استخدام النساء والفتيات لغرض الدعارة في الخارج، ومع نهاية سنة 1905 اتجهت العديد من الدول الأمريكية إلى إنشاء مثل هذه الأجهزة بغرض تبادل المعلومات المتعلقة باستخدام النساء لأغراض الدعارة محاولة منهم القضاء على هذه الجريمة.[1]

ومن هنا بدأت ملامح التعاون الشرطي الدولي في الظهور حيث أخذت شكل المؤتمرات الدولية، وكان أولها وأسبقها تاريخيا مؤتمر موناكو المنعقد في الفترة من 14إلى 18 أفريل 1914 والذي ضم رجال الشرطة والقضاء والقانون من 14 دولة لمناقشة وضع أسس التعاون الدولي في بعض المسائل الشرطية، حيث نتج عنه إنشاء جهاز دولي يختص بالتعاون في مكافحة الجريمة وتعقب المجرمين، إلا أنه ونتيجة لقيام الحرب العالمية الأولى لم يحقق المؤتمر أي نتائج عملية تذكر،[2] وبعد انتهاء الحرب وتحديدا عام 1919 حاول الكولونيل "فان هوتين" أحد ضباط الشرطة الهولندية إحياء فكرة التعاون الدولي الشرطي وذلك بالدعوة لعقد مؤتمر دولي لمناقشة هذه المسألة غير أنه لم يوفق في مسعاه، وفي عام 1923 نجح الدكتور "جوهانو سويرا" مدير شرطة فيينا في عقد مؤتمر دولي يعد الثاني على المستوى الدولي للشرطة الجنائية وذلك في

[1] عبد المالك بشارة، آلية الإنتربول في مكافحة الجريمة، مذكرة لنيل شهادة الماجستير في القانون الجنائي الدولي، كلية الحقوق والعلوم السياسية، المركز الجامعي عباس لغرور، خنشلة، 2010/2009، ص 10.

[2] لينا محمد الأسدي، مدى فاعلية أحكام القانون الجنائي في مكافحة الجريمة المعلوماتية، دار الحامد للنشر والتوزيع، الأردن عمان، 2015، ص 101.

الفترة من 03 إلى 07 سبتمبر 1923، ضم مندوبي تسعة عشر (19) دولة، تمخض عنه ولادة اللجنة الدولية للشرطة الجنائية (ICPO) والتي كان مقرها فيينا، إلا أنها توقفت عن عملها مع اندلاع الحرب العالمية الثانية إلى حين انتهاء الحرب سنة 1946، تم بعدها عقد مؤتمر دولي في بروكسل ببلجيكا في الفترة من 06-09 جوان 1946 بهدف إحياء مبادئ التعاون الأمني ووضعها موضع التنفيذ بدعوة من المفتش العام للشرطة البلجيكية، وانتهى المؤتمر بإحياء اللجنة الدولية للشرطة الجنائية ونقل مقرها إلى باريس بفرنسا، وفي عام 1956 تغير اسم اللجنة إلى المنظمة الدولية للشرطة الجنائية (الإنتربول) وأصبح مقرها في مدينة ليون بفرنسا.[1]

تضم المنظمة حاليا 194 بلدا عضوا فيها من بينهم الجزائر التي انضمت لها سنة 1963 مباشرة بعد الاستقلال الوطني، حيث تولت الجزائر منصب نيابة رئاسة المنظمة في سنة 1974، إذ يعمل لدى هذه المنظمة 541 موظف من 79 جنسية مختلفة، وتباشر مهامها بأربع لغات رسمية (الانجليزية، الفرنسية، الإسبانية، العربية)، وتتكون من عدة أجهزة تباشر مهامها بالتنسيق مع بعضها البعض ومع نظيراتها في الدول الأطراف بصفة متكاملة،[2] فقد أخذت الإنتربول كغيرها من المنظمات الدولية بمبدأ تعدد الأجهزة ذلك بموجب نص المادة الخامسة (05) من القانون الأساسي للمنظمة والتي تنص على أنه تتكون المنظمة من الأجهزة التالية[3]:

[1] عبد المالك بشارة، آلية الإنتربول في مكافحة الجريمة، المرجع السابق، ص 12-13.

[2] لمزيد من التفاصيل يراجع الموقع الرسمي للمنظمة الدولية للشرطة الجنائية (الإنتربول)، المتاح على الرابط التالي: https://www.interpol.int/ar/3/3 تاريخ الاطلاع 2021/11/12 على الساعة 17:56.

[3] المادة 05 من القانون الأساسي للمنظمة الدولية للشرطة الجنائية والتي تنص على: " تتكون المنظمة الدولية للشرطة الجنائية (الإنتربول) من:

- الجمعية العامة،
- اللجنة التنفيذية،
- الأمانة العامة،
- المكاتب المركزية الوطنية،
- المستشارين،
- لجنة الرقابة على المحفوظات."

1) **الجمعية العامة:**

وتعتبر هي أعلى هيئات المنظمة، تتكون من مندوبي أعضاء المنظمة، وتعقد اجتماعاتها بمقرها في دورة عادية مرة واحدة كل سنة، ولها أن تجتمع في دورة استثنائية بناء على طلب اللجنة التنفيذية أو بطلب من أغلبية أعضائها، ويترأس دورات الجمعية العامة واللجنة التنفيذية معا رئيس المنظمة ويدير مناقشاتها.[1]

وتختص هذه الجمعية بتحديد السياسة العامة للمنظمة وإصدار القرارات المتعلقة بالمسائل التي تختص المنظمة بمعالجتها، والعمل على تحقيق أهداف المنظمة المنصوص عليها في المادة 02 من القانون الأساسي لها، كما تقوم بدراسة الاتفاقات مع المنظمات الأخرى والموافقة عليها، بحيث تقوم بجمع كافة البلدان الأعضاء مرة في السنة لاتخاذ القرارات اللازمة.[2]

2) **اللجنة التنفيذية:**

تتكون اللجنة التنفيذية للمنظمة حسب المادة 15 من القانون الأساسي، [3] من رئيس المنظمة وثلاثة نواب للرئيس وتسعة مندوبين، حيث يكون هؤلاء الأعضاء من بلدان مختلفة، ويتولى رئيس المنظمة ترأس دورات اللجنة التنفيذية ويدير مناقشاتها، فيما تشرف اللجنة التنفيذية على تنفيذ قرارات الجمعية العامة وكذا إعداد جدول أعمال دورات الجمعية ومراقبة إدارة الأمين العام للمنظمة، وتمارس كافة السلطات التي توكلها إليها الجمعية العامة، [4]

3) **الأمانة العامة:**

تتكون الأمانة العامة من الأمين العام وموظفين فنيين وإداريين مكلفين بالاضطلاع بأعمال المنظمة موزعين على بعض الإدارات الدائمة داخل المنظمة، [5] ومن أهم هذه الإدارات:

- **إدارة التنسيق الشرطي:** وتضم شعبة مكافحة الإجرام العام، شعبة مكافحة الاتجار غير المشروع بالمخدرات، شعبة الإجرام الاقتصادي والمالي، شعبة الاستخبار الجنائي.

[1] ينظر المادتين 06 و10 من القانون الأساسي للمنظمة الدولية للشرطة الجنائية.
[2] ينظر المادة 08 من نفس القانون والتي تحدد مهام ووظائف الجمعية العامة.
[3] ينظر المادة 15من نفس القانون.
[4] ينظر المادة 22 من نفس القانون والتي تحدد مهام ووظائف اللجنة التنفيذية.
[5] ينظر المادة 27 من نفس القانون.

- **إدارة القضايا القانونية:** تختص بتقديم الخبرة القانونية في جميع مجالات التعاون الأمني وصياغة الأنظمة والتوصيات وقرارات المنظمة، وجمع المعلومات المتعلقة بالإجرام الدولي وتحليلها.
- **إدارة الدعم التقني:** تضم هذه الإدارة شعبة الاتصالات وشعبة الحاسب الآلي، شعبة البحث والتطوير وفرع التقصي الآلي.[1]

4) المكاتب المركزية الوطنية:

وهي المكاتب التي يتم إنشاؤها في الدول الأعضاء لتكون حلقة وصل بين الأجهزة الشرطية في الدولة وبين المكاتب الوطنية، حيث يعين كل بلد هيئة تعمل كمكتب مركزي وطني يؤمن الاتصال بين مختلف أجهزة البلد وبين هذه المكاتب، وتكون هذه المكاتب بمثابة نقطة الاتصال بين الأمانة العامة للمنظمة وبين المكاتب المركزية الأخرى،[2] كما تسهر هذه المكاتب المركزية على تنفيذ العمليات وإجراءات التحقيق على أراضي دولتها، وتلتزم بإرسال نتائج التحقيقات للسلطات القضائية المعنية أو للأمانة العامة للمنظمة، ويعد مسئول المكتب المركزي الوطني عضوا في المنظمة وممثلا لوفد بلاده في اجتماعات الجمعية العامة، بحيث يتولى بالخصوص نشر الوثائق والإرساليات الصادرة من المنظمة والمتعلقة بمكافحة الجرائم والقبض على المجرمين، ويقوم بإبلاغ المنظمة بالإرساليات الصادرة عن بلده أيضا.[3]

5) المستشارون:

تستعين المنظمة بعدد من المستشارين ذوي الخبرة من أجل دراسة بعض المسائل العلمية المتعلقة بعمل هذه المنظمة، ويتمثل هؤلاء في الاستشاريين الدوليين المتخصصين في مكافحة الجرائم، يتم تعيينهم من قبل اللجنة التنفيذية لمدة ثلاث سنوات ولا يكتسب تعيينهم الصفة القطعية إلا بعد أن تسجله الجمعية العامة، وتجدر الإشارة إلى أنهم يختارون من بين الأشخاص الذين اكتسبوا شهرة ونفاذ رأي دوليين نتيجة قيامهم بأبحاث في أحد المجالات التي تهم المنظمة.[4]

---

[1] أسامة غربي، المنظمة الدولية للشرطة الجنائية (الإنتربول) ودورها في مكافحة الجريمة المنظمة، مجلة دراسات وأبحاث، المجلد 03، العدد 03، 2011، ص 162.

[2] ينظر المواد 31 و 32 من القانون الأساسي للمنظمة الدولية للشرطة الجنائية.

[3] رحموني محمد، منظمة الشرطة الجنائية الدولية (الإنتربول) آلية لمكافحة الجريمة المنظمة، مجلة آفاق علمية، المجلد 11، العدد 04، سنة 2019، ص 69.

[4] ينظر المواد 34 و35 من القانون الأساسي للمنظمة الدولية للشرطة الجنائية.

6) لجنة الرقابة على المحفوظات:

وهي هيئة مستقلة تحرص على أن تكون معاملة المنظمة للمعلومات ذات الطابع الشخصي موافقة للأنظمة التي وضعتها المنظمة لنفسها في هذا الخصوص، كما تقدم هذه اللجنة المشورة للمنظمة فيما يخص أي مشروع أو عملية أو مسألة تتطلب معاملة أو معالجة معلومات ذات طابع شخصي، ولهذا يتمتع أعضاء هذه اللجنة بالخبرة اللازمة التي تتيح لهم الاضطلاع بهذه المهام.[1]

ثانيا: مهام المنظمة

تهدف منظمة الشرطة الجنائية الدولية إلى تشجيع وتعزيز التعاون المتبادل بين سلطات وأجهزة الشرطة في الدول الأعضاء، وذلك عن طريق الوصل بينها لمنع الجريمة ومكافحتها عالميا، وهي في سبيل تحقيق ذلك تباشر وظيفتين رئيسيتين: تتمثل الأولى في تجميع كافة البيانات والمعلومات المتعلقة بالمجرم والجريمة من خلال مكاتب الشرطة المتواجدة على أقاليم الدول الأعضاء، أما الثانية فتتمثل في التعاون على ضبط وملاحقة المجرمين الفارين وتسليمهم إلى الدول الطالبة، [2]حيث يتجسد دورها في مكافحة هذه الجرائم في عقد المؤتمرات والاتفاقيات من جهة**(أولا)**، والعمل على تجسيد ذلك ميدانيا من خلال دعم إجراءات المتابعة والتحقيق في الجرائم من جهة أخرى**(ثانيا)**.

1) دور المنظمة من خلال عقد المؤتمرات والاتفاقيات:

ففي سبيل مكافحة الجريمة الإلكترونية والمعلوماتية قامت المنظمة بما يلي:

أ. عقد المؤتمر الدولي الأول بشأن الجرائم الحاسوبية في عام 1995 والذي أنشئ من خلاله وحدة مركزية وأربعة فرق عاملة معنية بمتابعة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال مثلت كل من إفريقيا، الأمريكتين، آسيا، وأوروبا، حيث تختص هذه الفرق بإتاحة التدريب والتعاون على المستوى الإقليمي لدولة كل قارة، [3]كم قام الإنتربول بخلق ثلاث هياكل خاصة تمثلت في الندوة الإقليمية الأوروبية، اللجنة التقنية الأوروبية، والأمانة الإقليمية الأوروبية، والتي من خلالها

[1] ينظر المادة 36 من نفس القانون.

[2] نبيلة هبة هروال، الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات، المرجع السابق، ص ص 150- 151.

[3] نادر عبد الكريم الغزواني، الحماية الجنائية من جرائم الإنترنت (دراسة مقارنة)، مكتبة نور للنشر، الاسكندرية مصر، 2017، ص 142.

استطاع مد جسور التعاون الشرطي إلى أوروبا وجعلها شريكا مهما لمختلف الأجهزة الأمنية الناشطة على الإقليم الأوروبي في هذا المجال.[1]

ب. عقد مؤتمر جرائم الإنترنت عام 2000 بلندن، والذي أكد من خلاله سكرتير الأنتربول (Raymond Kendall) على ضرورة إيجاد تعاون دولي لمكافحة هذا النوع من الإجرام، كما دعى المجتمع الدولي إلى عدم الانتظار إلى حين عقد المؤتمرات والمعاهدات في هذا الإطار بل يجب الشروع فورا في إيجاد سبل لمكافحة هذه الجرائم، ناهيك عن تأسيس شراكات إستراتيجية مع منظمات دولية حكومية وغير حكومية ومع القطاع الخاص أيضا.[2]

ت. كما نظمت الإنتربول في فيفري 2005 المؤتمر الثاني للتنسيق بشأن جرائم الاحتيال المعلوماتي، والذي جاء بعد وقوع حوالي 2000 شخص من مجموع 60 دولة مختلفة ضحية للاحتيال المعلوماتي، قدرت خسائرهم بحوالي 166 مليون أورو، أين تولى الإنتربول التحقيق فيها بالتنسيق مع سلطات الأمن للدول المعنية وتوصل إلى الكشف عن المجرمين وتوقيفهم بدولة اسبانيا في ديسمبر 2004 بعد تقدم النائب العام الاسباني بطلب المساعدة الدولية من قبل الإنتربول،[3] وفي نفس الصدد قامت الإنتربول بالتنسيق والتعاون مع الشرطة الفيدرالية الأمريكية" FBI" وكذا الشرطة الفرنسية في إحدى قضايا مكافحة استغلال الأطفال في المواد الإباحية عبر الإنترنت والمسماة بعملية فالكون "Falcon" التي تمت في أفريل 2005، والتي سمحت بتفكيك شبكة إجرامية تنشط في العديد من الدول الأوروبية.[4]

من جانب آخر فإن سلطات الأمن الجزائرية باشرت هي الأخرى العديد من الأعمال الإجرائية في إطار المساعدة القضائية الدولية مع الإنتربول، ومن الأمثلة على ذلك قد تم فتح تحقيق قضائي في أكثر من 800 قضية متعلقة بالجريمة الإلكترونية منذ دخول القانون رقم 04/09 المتعلق بالقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال حيز التنفيذ، حيث تورط فيها جزائريون وأجانب وتم النظر فيها بالتنسيق والتعاون مع سلطات الأمن الأجنبية، وقد كانت أول هذه القضايا عندما تحركت سلطات أمن ولاية باتنة في عام 2010 بناء على معلومات كافية قدمت لها من طرف الشرطة الأمريكية حول تقني سامي في الإعلام الآلي عمره 21 سنة جزائري الجنسية قام باختراق موقع شركة أمريكية

[1] جمال براهيمي، التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص 299.

[2] حسين ربيعي، آليات البحث والتحقيق في الجرائم المعلوماتية، المرجع السابق، ص 149.

[3] المرجع نفسه، ص 150.

[4] جمال براهيمي، التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص 300.

متخصصة في حماية المعلومات والبرامج الإلكترونية للعديد من الشركات الأمريكية، ثم استغلال تلك المعلومات لصالح شركات منافسة مقابل مبالغ مالية ضخمة، والذي أحيل للقضاء بمحكمة الجنح بباتنة.[1]

ث. من جانب آخر نظم الإنتربول المؤتمر الدولي السادس بشأن الجرائم المعلوماتية المنعقد بالقاهرة أفريل 2005، وتأكيدا لما دعى إليه هذا المؤتمر انعقد المؤتمر الدولي المتعلق بتكوين المحققين في الجرائم المعلوماتية فيشهر سبتمبر من نفس السنة بمدينة ليون الفرنسية، والذي عرف مشاركة خبراء من 30 دولة من أجل الاستفادة من هذا التكوين.[2]

ج. أطلق الإنتربول عام 2008 المبادرة الأمنية العالمية للقرن الحادي والعشرين التي تلخص منظور المنظمة الاستراتيجي في بعض المسائل والتي يأتي على رأسها الإجرام المعلوماتي وإجرام الإنترنت، والعمل على مكافحتها من منظور عالمي، حيث تتضمن هذه الإستراتيجية خمسة مسارات عمل تهدف كلها لمساعدة الدول الأعضاء على الكشف عن الاعتداءات السيبرانية وعن مرتكبيها، إذ تقوم أولا بتقييم التهديدات وتحليلها للتوصل إلى نتائج بشأنها، تيسير الوصول إلى البيانات المتعلقة بهذه الاعتداءات والاستفادة منها بشكل أفضل بغية الوصول للأدلة والحفاظ عليها لتسليمها فيما بعد للعدالة، كما تعمل الإنتربول وفق هذه الإستراتيجية على تحسين مستوى العمل والتنسيق بين الدول الأعضاء والعالم بأسره وتحثهم على توحيد تشريعاتهم الداخلية لتتضمن وسائل فعالة لمكافحة هذا النوع من الإجرام.[3]

ح. إضافة لهذه الجهود ينظم الإنتربول بالشراكة مع الأورو بول مؤتمرا سنويا لمكافحة الجريمة السيبرانية، والذي أطلق عام 2013 حيث يجمع هذا الأخير خبراء من أجهزة إنفاذ القانون والقطاع الخاص والأوساط الأكاديمية لإجراء مناقشات معمقة بشأن أحدث التهديدات السيبرانية وكيفية التغلب عليها، وينظم هذا المؤتمر سنويا بالتناوب لدى كل من الأورو بول والإنتربول.[4]

2) دور المنظمة من خلال دعم إجراءات المتابعة والتحقيق في الجرائم:

[1] جمال براهيمي، التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص 301.

[2] حسين ربيعي، آليات البحث والتحقيق في الجرائم المعلوماتية، المرجع السابق، ص 150.

[3] لمزيد من التفاصيل يراجع الموقع الرسمي للمنظمة الدولية للشرطة الجنائية (الإنتربول)، مقال متاح على الرابط التالي: https://www.interpol.int/ar/4/6/4 تاريخ الاطلاع 2021/09/03 على الساعة 18:00

[4] المرجع نفسه.

كما قلنا سابقا فإنه لا يقتصر عمل الإنتربول في مجال مكافحة الجرائم الإلكترونية على عقد المؤتمرات والاتفاقيات الدولية، بل يعمل على تجسيد ذلك ميدانيا على أرض الواقع من خلال تعزيز إجراءات البحث والتحري عن هذه الجرائم وتبادلها مع الدول الأعضاء، حيث يقوم الإنتربول في سبيل ذلك بما يلي:

أ. جمع وتخزين المعلومات المتعلقة بالجرائم ومرتكبيها وتبادلها بواسطة منظومة اتصالات شرطية عالمية تتيح تبادل المعلومات بشكل مأمون وفعال بين أجهزة الشرطة في الدول الأعضاء، يرمز لها (I-24/7)الأمر الذي يتيح للمستخدمين المرخص لهم تبادل البيانات الشرطية الهامة فيما بينهم والوصول إلى قواعد بيانات المنظمة وخدماتها المتيسرة على مدار الساعة وطوال أيام الأسبوع، كما يمكنها تلقي أو تقديم المعلومات أو طلبات المساعدة[1]، وقد كانت كندا أول بلد يتم وصله بهذه المنظومة بتاريخ 29 جانفي 2003، وبالرغم من أن المنظومة تنصب أساسا في المكاتب المركزية الوطنية إلا أن العديد من الدول قررت وضعها أيضا في المواقع الإستراتيجية كمراكز الحدود والمطارات والجمارك...الخ، حيث توفر هذه الأخيرة مجموعة من قواعد البيانات من بينها قاعدة البيانات الإسمية التي تتضمن معلومات عن المجرمين المعروفين دوليا والأشخاص المفقودين ...الخ، وقاعدة وثائق السفر المسروقة والمفقودة، قاعدة سمات ADN، قاعدة بصمات الأصابع، وقاعدة صور الإساءة الجنسية للأطفال وغيرها، [2] ودعما لهذه الشبكة تم إنشاء منظومة أخرى تدعى (I-Link) التي تعتبر المركز الرئيسي لتبادل المعلومات الجنائية والتواصل بين الدول الأعضاء بشكل أفضل وأسرع مقارنة بالمنظومة السابقة، وتتضمن هي الأخرى جملة من الوظائف التي تضمن نقل وتبادل المعلومات الشرطية تبادلا فعالا من خلال إمكانية التحكم المباشر في البيانات والتدقيق فيها، وإمكانية تسجيل أحدث المعلومات مباشرة في قاعدة البيانات الجنائية، وكذا توفير أداة بحث قوية وسريعة تضمن حصول الشرطة على الإجابات الفورية والشاملة وتقصيها بشكل سهل وناجع[3]، علاوة على هذه الأنظمة والمختصة بالجرائم عامة، استحدثت الإنتربول منصتين مأمونتين تتيحان التواصل بين أجهزة الشرطة وسائر الجهات المعنية في مجال مكافحة الجريمة السيبرانية، تختص الأولى بتبادل المعارف المتصلة بالجريمة السيبرانية بحيث تتيح لمستخدميها من أجهزة إنفاذ القانون والحكومات والمنظمات الدولية مناقشة أحدث اتجاهات

[1] لمزيد من التفاصيل يراجع الموقع الرسمي للمنظمة الدولية للشرطة الجنائية (الإنتربول)، مقال متاح على الرابط التالي: https://www.interpol.int/ar/3/3 تاريخ الاطلاع 2021/09/08 على الساعة 19:30

[2] رحموني محمد، منظمة الشرطة الجنائية الدولية (الإنتربول) آلية لمكافحة الجريمة المنظمة، المرجع السابق، ص 74.

[3] حسين ربيعي، آليات البحث والتحقيق في الجرائم المعلوماتية، المرجع السابق، ص 151.

هذه الجرائم وكيفية الوقاية منها وأساليب التحقيق فيها، وهي بذلك تساهم في خلق شبكة دولية من الخبراء المختصين لتبادل المعارف والخبرات في هذا المجال، أما عن المنصة الثانية فتسمى بمنصة التعاون لمكافحة الجريمة السيبرانية (العمليات) وهي مركز للمعلومات تعمل على تنسيق عمليات أجهزة إنفاذ القانون على الصعيد العالمي، فهي تتيح للجهات المعنية تعميم المعلومات الاستخباراتية ضمن بيئة تفاعلية مأمونة لتكوين رؤية عن التهديدات السيبرانية.[1]

ب. من جهة أخرى تقوم الإنتربول بتنسيق الجهود بين الدول الأعضاء فيما يتعلق بالقبض على المجرمين من خلال المكاتب المركزية الوطنية التابعة للمنظمة، وذلك بتعيين مكان تواجد المجرم والإسراع في اتخاذ إجراءات القبض عليه وتسليمه وفقا لما تضمنته القوانين والنظم الداخلية للدول والاتفاقيات المبرمة بينها، ليس هذا وحسب بل تقوم أيضا في مجال مكافحة الجرائم الإلكترونية بوضع قائمة إسمية لضباط متخصصين تحت تصرف الدول الأعضاء للاستعانة بهم في عملية البحث والتحري عن هذه الجرائم.[2]

ت. كما استحدثت الإنتربول فرق إقليمية تعنى بمتابعة الجرائم الإلكترونية في كل من مناطق إفريقيا، والأمريكتين، وآسيا، وأوروبا، والشرق الأوسط، حيث تجتمع هذه الفرق العاملة مع فريق خبراء الإنتربول العالمي لمكافحة الجريمة السيبرانية من أجل دراسة التهديدات الواقعة وإسداء المشورة للمنظمة بشأن صياغة السياسات وتنفيذ المشاريع المتعلقة بمكافحة هذه الجرائم، وكمثال على الأنشطة المقدمة من قبل هذه الفرق ما قامت به الفرقة العاملة الأوروبية بإعداد "دليل الإنتربول بشأن جرائم تكنولوجيا المعلومات" الذي يجمع ويصف بالتفصيل أساليب التحقيقات الجنائية في هذه الجرائم.[3]

ث. نشر البحوث والدراسات من خلال مكتبة الإنتربول، وكذا نشر الإحصائيات الجنائية المتعلقة باتجاهات الجريمة ونشاطاتها ومعدلاتها.[4]

ج. في إطار تبادل المعلومات المتعلقة بالجريمة ومرتكبيها تقوم الإنتربول باستخدام النشرات الدولية التي تصدرها الأمانة العامة بناء على طلب يقدم لها من طرف المكاتب المركزية الوطنية للدول

---

[1] لمزيد من التفاصيل يراجع الموقع الرسمي للمنظمة الدولية للشرطة الجنائية (الإنتربول)، مقال متاح على الرابط التالي: https://www.interpol.int/ar/4/6/6 تاريخ الاطلاع 2021/09/03 على الساعة 22:00

[2] جمال براهيمي، التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص 300.

[3] مريم أحمد مسعود، آليات مكافحة جرائم تكنولوجيات الإعلام والاتصال في ضوء القانون رقم 04/09، مذكرة مقدمة لنيل شهادة الماجستير في القانون الجنائي، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح، 2013، ص 60.

[4] نادر عبد الكريم الغزواني، الحماية الجنائية من جرائم الإنترنت، المرجع السابق، ص 144.

الأعضاء، وهي تختلف حسب نوعية مضمونها والهدف من إصدارها، بحيث تعتبر هذه النشرات من قبيل الوسائل الفنية التي تستخدمها المنظمة في إنجاز مهامها،[1] كما تقوم المنظمة بتزويد الدول الأعضاء بكتيبات إرشادية حول جرائم الإنترنت وكيفية التدريب على مكافحتها والتحقيق فيها، مثال ذلك ما قدمته للشرطة الأوروبية والمسمى "بدليل جرائم الحاسب الآلي" "Computer crime manual".[2]

ح. إضافة لهذا فقد أنشأ الإنتربول بنكا للصور المتعلقة بالمواد الإباحية، حيث يكون في متناول جميع أجهزة وقوات الشرطة، ويحتوي على صور الأطفال الذين تم التعرف عليهم على مواقع إباحية عبر الإنترنت، إذ يقدم هذا البنك معلومات إلى الشخص المخول من قبل البلد التي ينتمي إليها هذا الطفل وكذا عناوين عناصر الشرطة المتخصصة مع مراعاة الحفاظ على سرية هوية الطفل وفي نفس الوقت حمايته من الاستغلال عبر الإنترنت،[3] من جانب آخر أنشأ الإنتربول أيضا مركزا متعدد الاختصاصات لمكافحة الجريمة السيبرانية والذي يضم خبراء في شؤون التعامل مع الإنترنت من أجهزة إنفاذ القانون والقطاع الخاص يقومون بجمع المعلومات والبيانات حول الأنشطة الإجرامية المرتكبة في الفضاء السيبراني بهدف تزويد البلدان الأعضاء بها، بحيث ينشر هذا المركز تقارير لتنبيه البلدان إلى التهديدات الإلكترونية المحتملة وقد تم إصدار ما يزيد عن

[1] حيث تعد النشرة الحمراء من أقوى أدوات الملاحقة الدولية التي يلاحق بها الأشخاص الخطرين المطلوب القبض عليهم لصالح الدول الأعضاء في المنظمة الدولية، تليها النشرة الدولية الخضراء والتي يتم إصدارها في حق الأشخاص الذين لا يتمتعون بخطورة إجرامية والأشخاص المقبوض عليهم، بحيث تتيح هذه النشرة لسلطات الدول المعنية العلم بخبر القبض على الشخص وإدراج بياناته في الحاسب الآلي للبلد ليكون معروفا للسلطات، أما عن النشرة الدولية الزرقاء لا تصدر للقبض على المجرم بل تقوم الدولة بالتبليغ على وجود الشخص على أراضيها والإخطار عند المغادرة وتحديد الجهة التي اتجه إليها، كما توجد النشرة الدولية الصفراء وتصدر للبحث عن الأشخاص الغائبين والتي تحمل بيانات عن الشخص المفقود، في حين تصدر النشرات الدولية السوداء للتبليغ عن الجثث المجهولة وكذا كل المعلومات والبيانات الخاصة بهه الجثث، ويتم توزيعها على مختلف المكاتب المركزية الوطنية والتي بدورها تقوم باتخاذ إجراءاتها الشرطية من أجل الكشف عن صاحب هذه الجثة، كما تتنوع النشرات حسب أهدافها إلى النشرة الدولية الفنية والتي تختص بوصف التحف والآثار الفنية المسروقة، والنشرة الدولية للأطفال للمفقودين التي تصف وقائع اختفاء الأطفال، وأخيرا نجد النشرة الدولية للنقد المزيف بحيث تقوم الأمانة العامة للإنتربول فور إصدار أي عملة جديدة في أي دولة بإجراء نشرة للعملة الصحيحة وتوضيح العلامات المميزة لها ويتم توزيع هذه النشرة على المكاتب المركزية الوطنية وأجهزة الشرطة في الدول الأعضاء، وهذا من أجل المحافظة على استقرار سوق التداول للعملات النقدية لمختلف الدول.

[2] نبيلة هبة هروال، الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات، المرجع السابق، ص 154.

[3] نادر عبد الكريم الغزواني، الحماية الجنائية من جرائم الإنترنت، المرجع السابق، ص 143.

800 تقرير موجه للشرطة في أكثر من 150 بلد، بهذا يساعد هذا المركز البلدان في وضع استراتيجيات للوقاية من هذه التهديدات والتصدي لها، والاستعداد لمواجهة أي تهديدات جديدة.[1]

خ. تقوم المنظمة بتنظيم دورات تدريبية للضباط والخبراء والمختصين بالتحقيق في الجرائم الإلكترونية، حيث تعقد سنويا دورات تدريبية لتجديد المعلومات عن أدوات الإنتربول والخدمات التي يقدمها، إذ تتيح للخبراء والضباط إمكانية التعرف على فرص جديدة لاستخدام الموارد بالشكل الأمثل، وتبادل المعارف والاطلاع على آخر المستجدات بشأن الجرائم التي يتوجب عليهم التصدي لها وكذا على أهم وأحدث الطرق والوسائل المستعملة في التحقيق بشأن هذه الجرائم المتطورة باستمرار،[2] ومن بين هذه الدورات نظمت الإنتربول دورة تدريبية إلكترونية عن بعد امتدت من 17 جوان إلى 09 سبتمبر 2019، حيث كان موضوعها الأساسي فهم الأدلة الرقمية وكيفية التعامل معها واستخدامها في التحقيقات القضائية موجهة لأجهزة إنفاذ القانون من شرطة وقضاة ومدعون عامون وغيرهم، إذ شارك في الدورة حوالي 65 شخصا من 30 بلدا، وقدم فيها خبراء في هذا المجال مجموعة دروس مختلفة كل أسبوع شملت أصول التحقيق الرقمي وعلوم الأدلة الجنائية الرقمية، كما اشترك في تقديم التدريب أصحاب مشروع "Scorpius" لمكافحة الإرهاب والجريمة المنظمة في جنوب وجنوب شرق آسيا، وأصحاب مشروع مكافحة الجريمة السيبرانية في الأمريكتين الممولان من طرف حكومة كندا، وذلك بالتعاون مع مركز الإنتربول العالمي للموارد ومختبر البحوث والتحقيقات والأدلة الجنائية الرقمية التابع لجامعة دبلن[3]،

[1] لمزيد من التفاصيل يراجع الموقع الرسمي للمنظمة الدولية للشرطة الجنائية (الإنتربول)، مقال متاح على الرابط التالي: https://www.interpol.int/ar/4/6/1 تاريخ الاطلاع 2021/09/17 على الساعة 11:30

[2] مقال حول "المكاتب المركزية الوطنية وتدريب أجهزة الشرطة"، مقال منشور على الموقع الرسمي للمنظمة الدولية للشرطة الجنائية (الإنتربول)، متاح على الرابط التالي: https://www.interpol.int/ar/2/6/2 تاريخ الاطلاع 2021/09/24 على الساعة 13:22

[3] من أشهر الأمثلة على ذلك ما حدث في مارس 2008 حيث طلبت كولومبيا من الإنتربول إجراء فحوص أدلة جنائية مستقلة على أجهزة ومعدات حاسبات تم ضبطها خلال عملية لمكافحة المخدرات والإرهاب نفذت ضد معسكر للقوات الثورية الكولومبية، وذلك لتحديد ما إذا كان قد جرى التلاعب بمضمون أي من المعدات أو المستندات أو المحررات المخزنة على الحاسب الآلي لوزارة الدفاع، وترتيبا على ذلك أجرى فريق خبراء الأدلة الجنائية التابع للإنتربول دراسة فنية لهذه الأجهزة وأصدر بشأنها تقريرا خلص إلى غياب أي دليل يشير إلى تعديل ملفات المستخدمين أو تحريفها أو تغيير محتواها. ينظر بن تركي ليلى، التعاون القضائي الدولي لمكافحة جرائم الاعتداء على التوقيع الإلكتروني (بطاقات الائتمان نموذجا)، مجلة بحوث، العدد 10، الجزء الأول، ص 87

إضافة إلى خبراء من مركز الابتكار ووحدة مكافحة الجريمة السيبرانية لدى الإنتربول والشرطة الاتحادية النمساوية وغيرها من الأجهزة.[1]

الفرع الثاني: المنظمة الدولية للشرطة السيبرانية (السايبربول)

إلى جانب المنظمات الإقليمية والدولية التي تطرقنا لها سابقا أنشئت مؤخرا منظمة دولية مختصة في مكافحة الجرائم السيبرانية أطلق عليها اسم المنظمة الدولية للشرطة السيبرانية، وتسمى اختصارا بالسايبربول، حيث تهدف هذه الأخيرة إلى تعزيز التعاون والمساعدة الدولية بين جميع سلطات الشرطة والمنظمات في دول العالم، والعمل على تطويرها من أجل التصدي الفعال لهذا النوع من الإجرام وقبل التطرق لمهام هذه المنظمة يجدر بنا التطرق أولا لنشأتها وكذا هيكلها التنظيمي.

أولا: نشأة المنظمة وهيكلها التنظيمي

[1] مقال حول "أول دورة تدريب إلكترونية بأكملها للإنتربول تركز على الأدلة الرقمية"، مقال منشور يوم 2019/09/19، على الموقع الرسمي للمنظمة الدولية للشرطة الجنائية (الإنتربول)، متاح على الرابط التالي:https://www.interpol.int/ar/1/1/2019/40تاريخ الاطلاع 2021/09/24على الساعة 17:30

بالإضافة لمنظمة الإنتربول توجد عدة منظمات وهيئات دولية أخرى لا يقل دورها عن دور الإنتربول في مواجهة الإجرام المستحدث على المستوى الدولي، أبرزها المجموعة الثمانية الاقتصادية (G8) والتي من أبرز جهودها في مكافحة هذا الإجرام المستحدث أنها قامت بإعداد ملتقى دولي في نهاية نوفمبر سنة 2000 في طوكيو لتكوين قوة دولية أطلق عليها اسم "The DigitalsOpportunityTaskForced" تختص بتحقيق أمن تكنولوجيا المعلومات، إلى جانبها نجد منظمة التعاون الاقتصادي والتنمية (OECD) والتي تهتم بالنمو الاقتصادي وتطور التنمية الاجتماعية، حيث بدأت الاهتمام بالجريمة المعلوماتية منذ عام 1978 من خلال وضعها لمجموعة من الأدلة والقواعد الإرشادية التي تتعلق بأمن المعلومات، إذ يعد دليل حماية الخصوصية وقواعد البيانات من أول الأدلة التي تم تبنيها من قبل مجلس المنظمة في عام 1980، والذي تلاه إصدار تقرير بعنوان الجرائم المرتبطة بالحاسوب وتحليل السياسة القانونية الجنائية سنة 1983، وقد استعرض هذا التقرير الحد الأدنى من أفعال سوء استخدام الحاسوب والتي على الدول تجريمها، وفي سنة 1992 وضعت المنظمة أيضا توصيات وإرشادات خاصة بأنظمة المعلومات وأوصت بضرورة أن تعطي التشريعات الجزائية للدول الأعضاء مبادئ عامة تمثلت في:

- حدود التجميع: يتعين فرض قيود على تجميع البيانات.
- نوعية البيانات: حيث تنص على أن تتعلق البيانات بالغاية والغرض الذي سوف تستخدم من أجله.
- تعيين الغرض: بحيث يكون الغرض الذي تستخدم فيه البيانات الشخصية محصور ومحدد سلفا.
- حدود الاستخدام: يقضي الالتزام بعدم إفشاء البيانات الشخصية ونشرها لغير المصرح له بذلك.
- الوقاية الأمنية: ضرورة اتخاذ تدابير وإجراءات أمنية ملائمة وحازمة في إحاطة البيانات.
- المشاركة الفردية: أي حق الأشخاص المعنية في الوصول والتعرف على البيانات التي تخصهم فضلا عن رقابة مدى صحتها.
- المسائلة : التي تقتضي محاسبة الأشخاص والجهات المرخص لها الوصول إلى المعلومات والاطلاع عليها في حالة تجاوز أي من الإجراءات التي تكفل حماية البيانات ذات الصفة الخاصة.

أما على المستوى العربي، يعد المكتب العربي للشرطة الجنائية أحد المكاتب الخمسة للأمانة العامة لمجلس الوزراء الداخلية العرب يهدف إلى تأمين وتنمية التعاون بين أجهزة الشرطة للدول الأعضاء في مجال مكافحة الجريمة بصفة عامة وملاحقة المجرمين في حدود القوانين والأنظمة المعمول بها في كل دولة، بالإضافة إلى تقديم المعونة في مجال دعم وتطوير أجهزة الشرطة في الدول الأعضاء. لمزيد من التفاصيل ينظر طالب ليندا، الدليل الإلكتروني ودوره في الإثبات الجنائي، المرجع السابق، ص 218-219.

أنشئت المنظمة الدولية للشرطة السيبرانية بموجب المرسوم الملكي رقم 22/595.16 وذلك بتاريخ 02 جويلية 2015، [1] في المملكة المتحدة ثم تم نقل مقرها إلى بلجيكا طبقا للمادة 01 من القانون الأساسي للمنظمة الصادر في 02 جويلية 2015، والذي يبين الأجهزة المكونة لها وكذا مهامها في مكافحة الجريمة السيبرانية، كما أنها تخضع في عملها للقانون البلجيكي المتعلق بالرابطات والمؤسسات الدولية التي لا تستهدف الربح المؤرخ في 27 جوان 1921، باعتبارها منظمة دولية غير ربحية بل تم إنشائها لهدف واضح ألا وهو مكافحة الجرائم الإلكترونية.[2]

أما عن الأجهزة التي تضمها هذه المنظمة فقد حددتها المادة 05 من النظام التأسيسي للمنظمة، حيث تتألف من كل من الجمعية العامة، اللجنة التنفيذية، الأمانة العامة، المكتب المركزي الوطني، المستشارون، وأخيرا لجنة مراقبة السجلات، [3] و يلاحظ أنها تتشابه كثيرا في عضويتها مع عضوية المنظمة الدولية للشرطة الجنائية (الإنتربول)، وفيما يلي سوف نتطرق بالتفصيل لكل جهاز على حدة.

1. الجمعية العامة

بالرجوع للمادة 06 من النظام الأساسي للمنظمة فإنه تعتبر الجمعية العامة هي الهيئة أو السلطة العليا في المنظمة وتتألف من الأعضاء التالية: المؤسسون، الرئيس، نائب الرئيس، الأمانة العامة، والمندوبين وهم أعضاء يتم اختيارهم من قبل رئيس الجمعية العامة إما من بين الأعضاء الوطنيين والحكوميين الأوروبيين أو من أعضاء الدول المنضمة لهذه المنظمة، [4] بحيث يمثل كل مندوب بلده، ونظرا للطابع التقني للمنظمة فإنه يلزم على الأعضاء تعيين مندوبين بحيث تتوافر فيهم بعض الشروط أهمها، أن يكونوا من كبار المسئولين في الدولة والذين لديهم معرفة وتخصص في المجال الإلكتروني وشؤون الشرطة الحاسوبية.[5]

أما عن رئيس الجمعية العامة فهو من يرأس المنظمة، ينتخب من طرف الجمعية العامة من بين المندوبين حيث يلزم أغلبية الثلثين لانتخابه، وفي حالة عدم بلوغ هذا العدد بعد الاقتراع الثاني فتكفي الأغلبية

[1] Royal Decree° WL 22/16.595, Dated 02 July 2015, State Gazette n° 635.897.257

ينظر الملحق رقم 12.

[2] لمزيد من التفاصيل يراجع الموقع الرسمي للمنظمة الدولية للشرطية السيبرانية (سايبربول)، المتاح على الرابط التالي: https://www.cyberpol.info/تاريخ الاطلاع 2021/11/25 على الساعة 18:00.

[3] ينظر المادة 05 من النظام الأساسي للمنظمة الدولية للشرطية السبرانية.

[4] ينظر المادة 06 من نفس القانون الأساسي للمنظمة.

[5] ينظر المادة 07 من نفس القانون.

البسيطة، [1] ونشير إلى أنه ينتخب الرئيس لمدة 05 سنوات كما ينتخب نائب الرئيس وكذا الأمين العام أيضا لنفس المدة، [2] وتقوم الجمعية بالاضطلاع بالواجبات المنصوص عليها في اللوائح التي يصدرها رئيس المنظمة، حيث تقوم بدراسة وإقرار البرنامج العام لأنشطة المنظمة وتبليغ الأعضاء بها.[3]

وتجتمع الجمعية العامة في دورة عادية كل عام كما يجوز لها أن تجتمع في دورة استثنائية بناء على طلب من رئيسها أو من اللجنة التنفيذية، [4] ولها أن تنشئ لجانا خاصة لمعالجة مسائل معينة بعد موافقة الرئيس، [5] بحيث لها أن تختار مكان انعقاد الدورات ويتم نشر قراراتها في غضون 21 يوما من تاريخ انعقاد الدورة على لوحة إشعار المنظمات على الموقع المخصص لذلك، وإذا رأى رئيس الجمعية أن هذه القرارات ليست في مصلحة المنظمة يقوم بالطعن فيها بحيث تتوقف الموافقة النهائية عليه.[6]

2. اللجنة التنفيذية

تتألف اللجنة التنفيذية من رئيس المنظمة، ونائب الرئيس، والأمين العام، والمندوبين الذين يتم اختيارهم دائما من قبل الرئيس، بحيث يشترط أن يكون جميع الوفود المنتمين للجنة من بين أعضاء المنظمة، كما يشترط أن يكون العدد الأدنى لأعضاء اللجنة ثلاثة (03) أعضاء ولا يحدد العدد الأقصى لهم، [7] أما عن كيفية تعيين المندوبين في اللجنة التنفيذية فطبقا للمادة 19 من النظام الأساسي للمنظمة فإنه تقوم الجمعية العامة بانتخابهم لمدة 04 سنوات.[8]

أما عن مهام اللجنة التنفيذية فهي تقوم بالإشراف عن تنفيذ قرارات الجمعية العامة وإعداد جدول أعمالها، كما لها الحق في تقديم برنامج عمل أو أي مشروع للجمعية العامة تجده مفيدا وضمن أهداف وإستراتيجية المنظمة.[9]

---

[1] ينظر المادة 16 من نفس القانون.
[2] ينظر المادة 17 من نفس القانون.
[3] ينظر المادة 08 من نفس القانون
[4] ينظر المادة 10 من نفس القانون.
[5] ينظر المادة 11 من نفس القانون.
[6] ينظر المواد 12 13 و14 من نفس القانون.
[7] ينظر المادة 15 من نفس القانون.
[8] ينظر المادة 19 من نفس القانون
[9] ينظر المادة 22 من نفس القانون

وأما عن اجتماعاتها فتجتمع اللجنة التنفيذية مرة واحدة على الأقل كل سنة عند استدعاء رئيس المنظمة لها، ويتم تبليغ جدول أعمالها ومكان وتاريخ انعقاد دورتها عن طريق إشعار عام أو رسائل مباشرة بأية وسيلة كانت كما هو محدد في المادة 20 من القانون الأساسي للمنظمة، ويلزم موافقة الرئيس والأمانة العامة على القرارات التي تصدرها اللجنة ومن ثم موافقة الجمعية العامة عليها لكي تنشر فيما بعد في لوحة الإشعارات كما أشرنا سابقا وذلك في غضون 21 يوما.[1]

3. الأمانة العامة

تتألف الأمانة العامة من الأمين العام وموظفين تقنيين وإداريين مكلفين بأعمال المنظمة، حيث تقترح اللجنة التنفيذية تعيين الأمين العام بعد موافقة الرئيس عليه لعضوية مدتها 05 سنوات، ويكون اختياره من بين الأشخاص ذوي الكفاءة العالية في مجال الأمن الإلكتروني والسيبراني والتحقيقات الشرطية، [2] كما للجنة أن تقترح أيضا عزله من منصبه في حالات استثنائية وبعد الموافقة الصريحة للرئيس دائما، [3] وأما عن صلاحيات الأمين العام فيتولى هذا الأخير تعيين الموظفين وتوجيههم، تنظيم عمل الإدارات التابعة للأمانة وللمنظمة تحت إشراف الرئيس والجمعية العامة للمنظمة، كما له الحق في المشاركة في مناقشات واجتماعات الجمعية العامة واللجنة التنفيذية، علاوة على ذلك يمثل المنظمة في جميع محافلها.[4]

كما تعمل الأمانة العامة كمركز دولي وتقني وإعلامي في مكافحة الجرائم السيبرانية يكفل الإدارة الفعالة للمنظمة والحفاظ على الاتصال بالسلطات الوطنية والدولية للدول الأعضاء من جهة، وبين أجهزة المنظمة بما فيها الجمعية العامة واللجنة التنفيذية ورئيس المنظمة من جهة ثانية.[5]

أما بالنسبة للموظفين التابعين للأمانة العامة فيتم اختيارهم من قبل رئيس المنظمة بحيث يمكن أن يكون هؤلاء الموظفون ممن يعملون في مجال إنفاذ القانون سواء في الهيئات التابعة للقطاع الخاص أو العام، ولا يعتبر هؤلاء الأعضاء نفس المندوبين الذين ورد ذكرهم سابقا والمنتمين لكل من الجمعية العامة واللجنة التنفيذية بل مجرد موظفين تقنيين وإداريين لدى الأمانة، ولا يجوز لأي دولة أو منظمة أو كيان أن يرشح أي موظف إداري تقني إلا بعد موافقة الرئيس على ذلك، ويقوم هؤلاء الموظفون بممارسة

[1] ينظر المادة 20 من نفس القانون.
[2] ينظر المادة 26 من نفس القانون.
[3] ينظر المادة 27 من نفس القانون.
[4] ينظر المادة 28 من نفس القانون.
[5] ينظر المادة 25 من نفس القانون

اختصاصات معينة من قبل الأمين العام إذ يتولون البحث والتحقيق حول التهديدات السيبرانية، كما يتولون عمل السكرتارية داخل الأمانة.[1]

تجدر الإشارة إلى أنه لا يجوز للأمين العام والموظفين التقنيين عند مباشرة مهامهم التماس أو قبول تعليمات من أي منظمة أو مؤسسة أو سلطة خارج نطاق عضوية المنظمة، كما يمتنعون عن أي عمل يضر بمهمتها الدولية، وفي هذا يتعهد كل عضو في المنظمة باحترام الطابع الدولي الخاص بها وبواجبات الأمين العام وكذا الموظفين الإداريين وعدم التأثير على أدائهم.[2]

4. المكاتب المركزية الوطنية

لضمان تحقيق التعاون والمساعدة الدولية في مجال مكافحة الجرائم السيبرانية يقوم كل عضو في المنظمة بتعيين مكتب أو هيئة محلية داخل بلده تكون بمثابة مكتب مركزي وطني للمنظمة، بحيث يكفل هذا الأخير الاتصال الدائم بالمنظمة عن طريق الأمانة العامة، والاتصال بالإدارات الأخرى في البلدان الأعضاء وتبادل المعلومات والوسائل بخصوص مكافحة هذه الجرائم.[3]

5. المستشارون

تعين اللجنة التنفيذية أو رئيس المنظمة فئة معينة من الأشخاص الذين يتمتعون بمؤهلات عالية وعالمية في مجال مكافحة الجرائم السيبرانية والتعامل مع الفضاءات الإلكترونية بصفة عامة، والذين يهتمون بمجالات عمل المنظمة وذلك لمدة 03 سنوات وبعد موافقة أو إخطار الجمعية العامة، [4] بحيث يكون عمل هؤلاء المستشارين عملا استشاريا بحتا، تستشيرهم المنظمة في المسائل العلمية والتحريات وكذا البحوث العلمية المختلفة التي تساعد في تطوير عمل هذه المنظمة.[5]

كما يجوز للمنظمة عزل المستشار من منصبه في ظروف معينة وعند الإخلال بالتزامات المنظمة، وذلك بقرار من الجمعية العامة.[6]

---

[1] ينظر المادة 26 من نفس القانون.

[2] ينظر المادة 29 من نفس القانون.

[3] ينظر المواد 30 31 32 من نفس القانون.

[4] ينظر المادة 34 من نفس القانون.

[5] ينظر المادة 33 من نفس القانون.

[6] ينظر المادة 34 من نفس القانون.

6. لجنة مراقبة السجلات

تعتبر لجنة مراقبة السجلات هيئة مستقلة تكفل تجهيز المنظمة بالمعلومات الشخصية للأنظمة المعلوماتية وتقديم المشورة لها بشأن أي مشروع أو عضو أو متطوع أو أي مسألة تنطوي على تجهيز المعلومات الشخصية،[1] ويتمتع أعضاء هذه اللجنة بالخبرة الفنية والمؤهلات اللازمة لإنجاز مهامها، ويخضع تشكيلها وعملها لقواعد محددة تضعها الجمعية العامة بعد موافقة رئيس المنظمة.[2]

كما تجدر الإشارة أنه تخضع لجنة مراقبة السجلات لتصريح أمني موافق عليه من قبل رئيس المنظمة قبل البدء في عملها وهذا لضمان توافر الثقة فيها والاطمئنان على السجلات والمعلومات المتعلقة بالمنظمة، بحيث لا تتاح هذه السجلات إلا لأعضاء المنظمة وموظفيها.[3]

وفي نفس الصدد تقوم المنظمة بإقامة علاقات تعاون مع العديد من المنظمات الدولية الحكومية وغير الحكومية مراعية في ذلك تحقيق أهدافها وأنشطتها المسطرة، وأهمها تعزيز التعاون بين الدول في مجال مكافحة الجرائم الإلكترونية، كما للمنظمة أن تأخذ بمشورة المنظمات الوطنية الحكومية وغير الحكومية في المسائل التي تختص بها وذلك بأمر من رئيسها، كما يجوز للجنة التنفيذية للمنظمة أو الأمين العام وفي حالات خاصة أو عاجلة أن يقبل طلبات المساعدة الواردة من المؤسسات والمنظمات الدولية الأخرى أو تطبيقا للاتفاقيات الدولية والتي تكون في نطاق اختصاصات المنظمة وكذا أنشطتها، وهذا بعد موافقة رئيس المنظمة أو الجمعية العامة[4]

ثانيا: مهام المنظمة

في سبيل التصدي الأمثل للجرائم الإلكترونية قامت المنظمة الدولية للشرطة السيبرانية بوضع إستراتيجية دولية لمنع تنامي هذه الجرائم، حيث ضمنتها العديد من الأهداف والمهام الموزعة على أعضاء وأجهزة هذه المنظمة، وعليه سنحاول التطرق بالتفصيل لمحاور هذه الإستراتيجية الدولية والمهام التي تضمنتها.

[1] ينظر المادة 35 من نفس القانون.

[2] ينظر المادة 36 من نفس القانون.

[3] ينظر المادة 35 من نفس القانون.

[4] ينظر المادة 40 من نفس القانون والتي تبين علاقة المنظمة الدولية للشرطة السيبرانية مع المنظمات الدولية الأخرى.

- تسهيل الوصول إلى البيانات والمعلومات المتعلقة بالجرائم السيبرانية، وضمان الاتصال السريع بجميع خدمات الشرطة السيبرانية وذلك عن طريق إتاحة مواقع وإنشاء منتديات ونقاط اتصال دائمة بين الدول الأعضاء في المنظمة.
- إنشاء برنامج يوفر الدعم الفني لأجهزة الشرطة في الدول الأعضاء، يعمل على مدار الساعة ويعتبر أول وسيلة دولية لإدارة المخاطر الإلكترونية، يطلق عليه اسم (Cyberwatch)، حيث يضم هذا الأخير قاعدة بيانات رقمية لمراقبة الحدود الدولية ورصد المخاطر الإلكترونية داخل الفضاءات السيبرانية.
- العمل على تنمية القدرات والمعارف والكفاءات اللازمة لتحقيق الفعالية في مواجهة الجرائم السيبرانية، وفي هذا الإطار قامت منظمة السايبربول بتوفير برامج تعليمية وأخرى تدريبية عالمية في مجالات الحوسبة والأمن السيبراني لتدريب العاملين في المنظمة وأجهزة الشرطة في الدول الأعضاء.
- الاستفادة من جهود ومساعدة السلطات التابعة للقطاعين الخاص والعام من أجل تعزيز ونشر مهمة وأهداف المنظمة وإستراتيجيتها في مكافحة هذا النوع من الجرائم، من خلال نشر برامجها التوعوية والتربوية (Cyberbook).
- كما يلتزم السايبربول بتوفير الوسائل الإلكترونية والخدمات الرقمية وتحديثها من حين لآخر من أجل تحقيق المعايير الدولية للشرطة السيبرانية والهياكل القاعدية للأمن الإلكتروني.
- تقوم المنظمة وفقا لهذه الاستراتيجية بمراقبة المواقع والعناوين الإلكترونية والشبكة المعلوماتية لرصد المواقع التي تقدم محتويات ضارة وغير قانونية م شأنها التأثير على الراحة النفسية والجسدية والعقلية مستخدمي الإنترنت بغية تحقيق شبكة أكثر أمانا.
- تعزيز وتقوية علاقات التعاون الدولية مع الهيئات والمنظمات الاقليمية والدولية الأخرى التي تسعى لمكافحة هذا النوع من الإجرام.
- السعي لزيادة البحث والدراسة في مجال الأمن والدفاع السيبراني لتطوير قدرات هذه المنظمة والأجهزة الشرطية في الدول الأخرى، بغية الوصول إلى عالم إلكتروني أو رقمي آمن.[1]

[1] Cyberpol strategic framework 2016-2025, Article disponible sur le site suivant : http://cyberpol.infoconsulté le 30/11/2021, à 19 :45

ينظر أيضا المادة 02 من القانون الأساسي للمنظمة.

وأخيرا ومما تم التطرق إليه في هذا الباب نخلص للقول بأن نتيجة الانتشار الواسع للجرائم الإلكترونية وتطور أساليب ارتكابها وكذا احترافية مرتكبيها، برزت جهود الدول في التصدي لها ومكافحتها، وذلك عن طريق أسلوبين أو وظيفتين: تتمثل الأولى في الضبط الإداري والذي يمارس قبل وقوع الجريمة للوقاية والحيلولة دون وقوعها، والذي يوكل إلى عدة جهات تشمل السلطات الإدارية التقليدية وكذا السلطات الإدارية الإلكترونية والتي جاء إنشائها في ظل عجز السلطات العمومية التقليدية على ضبط النشاطات الإلكترونية للأفراد داخل العالم الرقمي، إذ نجد منها سلطات ضبط البريد والاتصال وكذا الهيئات المستحدثة للوقاية من هذه الجرائم، والتي تقيد من نشاطات الأفراد داخل هذه البيئة من خلال وسائل قانونية ومادية وبشرية، كفرض الرقابة على بعض المواقع الإلكترونية وحظر الأخرى وحجب بعض الخدمات وغيرها، فضلا عن مقدمي خدمات الإنترنت والذين يقومون بدور مساعد لهذه السلطات ولسلطات التحقيق من خلال التزويد بالمعلومات اللازمة.

أما عن الوظيفة الثانية وتتمثل في الضبط القضائي الذي يباشرها أعوان متخصصين في مجال مكافحة الجرائم بأنواعها، إلا أن طبيعة الجرائم الإلكترونية وما تتميز به فرضت تحديا أمام هذه السلطات التي أصبحت عاجزة عن متابعة هذه الجرائم، مما حذا بأغلب الدول إلى تنظيم الدورات التكوينية والتدريبية من أجل تلقين ضباط الشرطة وكذا قضاة التحقيق والحكم أساليب ومهارات التحقيق في هذه الجرائم والتعامل معها، هذا من جهة، ومن جهة أخرى سارعت بعض الدول إلى استحداث فرق متخصصة بمتابعة هذه الجرائم كشرطة الإنترنت، وذلك على المستوى الداخلي سواء الدول الأجنبية أو العربية من بينها الجزائر، وعلى المستوى الإقليمي من خلال استحداث الشرطة الأوروبية "الأوروبول" والشرطة الإفريقية " أفريبول" وكذا على المستوى الدولي الشرطة الدولية "الإنتربول" والشرطة السيبرانية "السايبربول" والتي تتولى عدة مهام منها متابعة الجرائم الإلكترونية والعمل على تنسيق الجهود بين مختلف الدول لضمان فاعلية التحقيق والمكافحة.

الباب الثاني

خصوصية إجراءات البحث والتحري عن الجريمة الإلكترونية

كما سبق وذكرنا أن التطور الحاصل في مجال المعلوماتية قد رتب آثارا هامة انعكست على الجرائم من حيث الوسائل التي ترتكب بها، وكذا المحل الذي تقع عليه، ونوع الجناة الذين يرتكبونها، الأمر الذي أدى إلى تطوير وتحديث أحكام القانون الجنائي بشقيه الموضوعي والإجرائي، من أجل استيعاب هذه النوعية الجديدة من الجرائم، كون أنها جرائم مستترة لا يمكن اكتشافها بسهولة نظرا للطبيعة الخاصة للأدلة الناتجة عنها، الأمر الذي أصبح يشكل التحدي الأكبر الذي يواجه النصوص الجزائية الإجرائية، التي تنظم سير الإجراءات المتعلقة بالبحث والتحقيق وملاحقة المجرمين، حيث أصبحت القواعد التقليدية منها عاجزة على كشف غموض الجريمة الإلكترونية، وجمع الدليل الإلكتروني الذي يصعب التعامل معه نظرا للخصائص التقنية التي يتميز بها، مما جعل عملية إثباته أمام القضاء من المسائل الصعبة والمعقدة، إذ يثير عدة إشكالات حول مشروعية الحصول عليه، وكذا مدى مصداقيته في إثبات الواقعة الإجرامية، ولهذا كان لابد من وضع أطر قانونية ملائمة تتماشى مع طبيعة هذه الجرائم مع ضرورة مراعاة مدى احترامها لحقوق الإنسان وحرياته، والضمانات الممنوحة للمشتبه فيه أثناء إعمال هذه القواعد الإجرائية، إذ تدخل المشرع عن طريق إدخال تعديلات على القوانين الإجرائية السارية، واستحداث نصوص وقواعد خاصة للتحري والتحقيق في هذه الجرائم، بما يتلاءم مع طبيعتها الخاصة، وعليه فيما تتمثل خصوصية إجراءات التحري والبحث عن الجريمة الإلكترونية؟ وما مدى فعاليتها في مواجهة هذا النوع من الجرائم؟ وما هي أهم الإشكالات التي يثيرها تطبيق هذه الإجراءات؟

للإجابة عن هذه الإشكالات ارتأينا معالجة هذا الباب من خلال فصلين رئيسيين: خصصنا الأول لدراسة خصوصية إجراءات البحث والتحري التقليدية في الجريمة الإلكترونية، أما الثاني فخصص لدراسة خصوصية إجراءات البحث والتحري المستحدثة.

الفصل الأول

خصوصية إجراءات البحث والتحري التقليدية في الجريمة الإلكترونية

الفصل الأول: خصوصية إجراءات البحث والتحري التقليدية في الجريمة الإلكترونية

بظهور الجريمة الإلكترونية وانتشارها الواسع في جميع أنحاء العالم، سارعت الدول للتصدي لها بعدة طرق، إذ لم يكن لها خيار في البداية إلا الاعتماد على النصوص الإجرائية التقليدية، تفاديا لإفلات الجناة من العقاب والمتابعة، هذا من جهة، ولعدم وجود قواعد قانونية أخرى تتلاءم مع طبيعة هذه الجرائم المستحدثة من جهة أخرى، ومما لا شك فيه أن هذه القواعد عامة النطاق حيث تنظم إجراءات استخلاص الدليل في جميع الجرائم، سواء كانت تقليدية أم مستحدثة، إلا أنها في الأولى لا تثير أي إشكالات إجرائية على عكس الجرائم الإلكترونية، وذلك من حيث اختصاصات السلطات القضائية بهذه الجرائم اختصاصا محليا ونوعيا،[1] وكذا خصوصية هذه الإجراءات في متابعة هذا النوع من الجرائم، وعليه ما مدى إمكانية تطبيق القواعد الإجرائية التقليدية على هذه الجرائم المستحدثة؟

للإجابة عن هذا التساؤل ارتأينا معالجة هذا الفصل من خلال مبحثين رئيسيين: خصصنا الأول لدراسة خصوصية إجراءات البحث والتحري المادية، في حين خصصنا الثاني لدراسة خصوصية إجراءات البحث والتحري الشخصية.

المبحث الأول: خصوصية إجراءات البحث والتحري المادية

تتخذ سلطات التحري جملة من الإجراءات الأولية عقب تلقيها بلاغا عن وقوع جريمة ما، تهدف من خلالها للتأكد من وقوع هاته الجريمة والتحفظ على مسرحها، وتعتبر صلاحية تلقي البلاغات والشكاوى من المراحل المهمة في البدء في إجراءات التحري خاصة في الجرائم الإلكترونية التي تعتبر صعبة الكشف نتيجة طبيعتها المتميزة، هذه الطبيعة التي فرضت نوعا مختلفا من التعامل مع المسرح الذي وقعت فيه الجريمة، وعليه سوف نتطرق فيما يلي لمعرفة مدى إمكانية تلقي البلاغات في الجرائم الإلكترونية وكيفية

1يحدد القانون الاختصاص المحلي لضباط الشرطة القضائية في الحدود التي يباشرون ضمنها وظائفهم المعتادة، أي في دائرة اختصاص المحكمة وفي حالة الاستعجال يمدد اختصاصهم إلى كافة دائرة اختصاص المجلس القضائي التابعين له، وفي حالات عندما يتعلق الأمر ببعض الجرائم منها الجرائم الإلكترونية فيمدد الاختصاص إلى كافة التراب الوطني.

أما عن الاختصاص المحلي لوكيل الجمهوريةفطبقا للماده37من قانون الإجراءات الجزائيةيحدد بمكان وقوع الجريمة وبمحل إقامة أحد الأشخاص المشتبه في مساهمتهم فيها أو بالمكان الذي تم في دائرته القبض على أحد هؤلاء الأشخاص حتى لو حصل هذا القبض لسبب آخر، كما قام المشرع بتوسيع الاختصاص الإقليمي لوكيل الجمهورية ليشمل اختصاص محاكم أخرى كلما تعلق الأمر بالتحري والتحقيق بشان جرائم المخدرات والجريمة المنظمة عبر الحدود الوطنية والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبييض الأموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف، وهو نفس معيار تحديد الاختصاص لقاضي التحقيق وفقا المادة 40من قانون الإجراءات الجزائية.

ذلك؟ وإلى معرفة كيفية التعامل ومعاينة مسرح الجريمة الإلكترونية وأهم الضوابط الواجب مراعاتها في ذلك؟

المطلب الأول: تلقي البلاغات والشكاوى

تظل الجريمة مستترة عادة ما لم يتم التبليغ عنها إلى الجهات المختصة بالتحري وتحريك الدعوى العمومية، وبمجرد العلم بها من طرف هاته الأخيرة تتخذ بشأنها جملة من الإجراءات للتأكد من صحة الواقعة والكشف عن مرتكبيها، ويعد كل من الشكوى والبلاغ وسيلتين للإخبار عن الجريمة الواقعة إلا أنهما يختلفان في بعض النقاط وخاصة عندما يتعلق الأمر بالجرائم الإلكترونية والمرتكبة في العالم الرقمي، وعلى هذا سنحاول التعريج على مفهوم كل منهما وبيان الخصوصية التي يتمتعان بها في ظل الجرائم الإلكترونية وكذا المشاكل التي تطرحها، وأخيرا معرفة المراكز المتخصصة بتلقي الشكاوى والبلاغات في بشأن هذه الجرائم.

الفرع الأول: المقصود بالبلاغ والشكوى

يقصد **بالبلاغ** إخطار السلطات المختصة عن وقوع جريمة أو أنها على وشك الوقوع أو أن هناك اتفاقا جنائيا أو أدلة أو قرائن أو عزما على ارتكابها، أو وجود شك أو خوفا من أنها ارتكبت، [1] وهو إجراء يقوم بواسطته شخص لم يتضرر من الجريمة بالإبلاغ عنها لدى الجهات المختصة والتي تتمثل عادة في الضبطية القضائية كما جاء في الفقرة الأولى من المادة 17من ق ا ج ج والتي تقابلها المادة 17من ق ا ج الفرنسي والمادة 24من ق ا ج المصري، والمادة 27من نظام الإجراءات الجزائية السعودي.[2]

ويعد التبليغ عن الجريمة واجبا على كل من علم بوقوع جريمة ولم يكن متضررا منها أو له مصلحة فيها وهذا من أجل تقديم العون للسلطات في تحقيق الأمن ومتابعة المجرمين، وإن كان في القانون الجزائري جائزا إلا في جرائم معينة يستوجب التبليغ عنها كالجريمة المنصوص عليها في المادة 91من ق ع ج، [3] والجريمة المنصوص عليها في المادة 32من ق ا ج ج.[1]

1نبيلة هبة هروال، الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات، المرجع السابق، ص 177.

2حيث تنص المادة 17فقرة 01من ق ا ج ج على: "يباشر ضباط الشرطة القضائية السلطات الموضحة في المادتين 12و13ويتلقون الشكاوى والبلاغات ويقومون بجمع الاستدلالات وإجراء التحقيقات الابتدائية."

تقابلها المادة 17من ق ا ج الفرنسي والتي تنص على أنه يكون تلقي البلاغات من اختصاص الضابطة القضائية، وتجدر الإشارة هنا إلى أن المادة 17من ق ا ج ج تعتبر ترجمة حرفية لهذه المادة، أما عن ق ا ج المصري فينص في المادة 24منه على أنه: "يجب على مأموري الضبط القضائي أن يقبلوا التبليغات والشكاوى التي ترد إليهم بشأن الجرائم..."، ونفس الشيء بالنسبة لنظام الإجراءات السعودي.

3تنص المادة 91من ق ع ج على: "مع عدم الإخلال بالواجبات التي يفرضها سر المهنة، يعاقب بالسجن المؤقت لمدة لا تقل عن عشر سنوات ولا تجاوز عشرين سنة في وقت الحرب وبالحبس من سنة إلى خمس سنوات وبغرامة من 20.000إلى 100.000دينار في وقت السلم كل شخص

وتجدر الإشارة أن القانون لم يشترط أن يكون مصدر البلاغ معلوم الهوية ومن هذا المنطلق يمكن أن يكون المبلغ مجهولا وعلى ضابط الشرطة القضائية في كلتا الحالتين أن يأخذ هذا البلاغ بجدية كاملة.

أما عن **الشكوى** فيقصد بها الإخطار الذي يقدمه المجني عليه أو وكيله الخاص إلى السلطات المختصة مطالبا بتعويض الضرر الذي لحقه من الجريمة، وقد تقدم الشكوى أمام ضباط الشرطة القضائية طبقا للمادة 17من ق ا ج ج، [2] كما تقدم أمام قضاة النيابة طبقا للمادة 36من ق ا ج ج، [3] كما قد تكون في شكل شكوى مصحوبة بادعاء مدني أمام قضاة التحقيق طبقا لنص المادة 72من ذات القانون.[4]

وتجدر الإشارة إلى أنه لا يمكن تحريك الدعوى العمومية بشأن بعض الجرائم إلا بناء على شكوى مقدمة من طرف المتضرر أو وكيله الخاص، في حين يمكن تقديم شكوى في كل الجرائم الإلكترونية.[5]

ولا تختلف أحكام التبليغ والشكوى في الجرائم الإلكترونية عن ما هي عليه في الجرائم التقليدية غير أنهما تتمتعان بنوع من الخصوصية التي تتماشى وطبيعة هذه الجرائم، فبمجرد تلقي الجهة المختصة

علم بوجود خطط أو أفعال لارتكاب جرائم الخيانة أو التجسس أو غيرها من النشاطات التي يكون من طبيعتها الإضرار بالدفاع الوطني ولم يبلغ عنها السطات العسكرية أو الإدارية أو القضائية فور علمه بها...".

وذات الشأن بالنسبة للمشرع المصري إذ نجد أنه حدد في قانون العقوبات بعض الجرائم التي يجب الإبلاغ عنها وذلك في المواد 84و98منه، حيث أوجبت المادتين على كل من علم بارتكاب جريمة من الجرائم المضرة بأمن الحكومة من جهة الخارج أن يسارع إلى إبلاغ السلطات المختصة وإلا كان معرضا للعقوبة.

1تنص المادة 32من ق ا ج ج على: "يتعين على كل سلطة نظامية وكل ضابط أو موظف عمومي يصل إلى علمه أثناء مباشرته مهام خبر جناية أو جنحة إبلاغ النيابة العامة بغير توان، وأن يوافيها بكافة المعلومات ويرسل إليها المحاضر والمستندات المتعلقة بها"، وذات الشأن بالنسبة للقانون الإجرائي المصري إذ ينص في المادة 26منه على إلزام الموظفين العموميين بالتبليغ عن الجرائم التي يعلمون بها أثناء تأديتهم لعملهم أو بسبب تأديتهم لذلك الأخير.

2ينظر المادة 17من ق ا ج ج المشار إليها سابقا.

3تنص المادة 36من ق ا ج ج على: "يقوم وكيل الجمهورية بما يأتي: ...

- تلقي المحاضر والشكاوى والبلاغات ويقرر في أحسن الآجال ما يتخذه بشأنها...". وهذه المادة تقابلها المادة 25من ق ا ج المصري.

4تنص المادة 72من ق ا ج ج على: "يجوز لكل شخص متضرر من جناية أو جنحة أن يدعي مدنيا بأن يتقدم بشكواه أمام قاضي التحقيق المختص". وهذه المادة تقابلها المادة 27من ق ا ج المصري.

5حدد المشرع الجزائري بعض الجرائم التي تشترط لتحريك الدعوى بشأنها تقديم شكوى من الطرف المتضرر، وهي:

- جريمة الزنا المنصوص عليها في المادة 339من ق ع ج.
- جرائم السرقة التي تقع بين الأقارب والحواشي والأصهار لغاية الدرجة الرابعة، المنصوص عليها في المواد 368و369من ق ع ج.
- جرائم النصب المادة 372من ق ع ج، وجريمة خيانة الأمانة المادة 377ق ع ج، وجريمة إخفاء الأشياء المسروقة المادة 387ق ع.
- خطف أو ابعاد القاصر وزواجها من خاطفها المادة 326ق ع ج.
- نرك أحد الوالدين لأسرته أو الزوج الذي يتخلى عن زوجته مع علمه بأنها حامل المادة 330ق ع ج.

ولعل العلة في تطلب الشكوى في مثل هذه الجرائم هي تقدير المشرع أن المجني عليه في هذه الجرائم أقدر من النيابة العامة على تقدير ملائمة اتخاذ الإجراءات الجزائية.

والتي عادة ما تكون الضبطية القضائية بلاغا أو شكوى تشير إلى ممارسة أي شخص معروف أو مجهول لأنشطة تندرج ضمن الجرائم الإلكترونية، تنعقد لها جملة الاختصاصات العادية التي تمارسها بصدد الجرائم التقليدية.[1]

والبلاغ في الجرائم الإلكترونية قد يتم بعدة طرق وهنا تجدر الإشارة إلى أنه يمكن التبليغ عن الجرائم الإلكترونية بالطرق العادية، فقد يتم إما عن طريق توجه المبلغ بنفسه لأقرب جهة مختصة للإدلاء بتصريحاته وذلك إما كتابيا أو شفويا وهذا ما يسمى بالبلاغ المادي، كما يمكن أن يكون بلاغا معنويا عن طريق إرسال المبلغ بريدا أو اتصالا هاتفيا...الخ، وأخيرا يمكن أن يتم عن طريق الإنترنت أو ما يسمى بالبلاغ الرقمي وذلك إما عن طريق إرسال رسالة إلكترونية إلى عنوان البريد الإلكتروني للجهات المختصة بالتحري أو عن طريق ملء استمارات رقمية تكون متاحة في المواقع الرسمية الإلكترونية المخصصة لتلقي البلاغات والشكاوى، [2]وحتى يكون البلاغ جديا ومستوفيا لجميع أركانه لابد من أن تتوافر فيه جملة من العناصر من بينها، ذكر نوع الحادثة، تحديد المجني عليه، تحديد زمان ومكان وقوع الجريمة، بيان الإصابات ومعرفة السبب والدوافع التي حملت الجاني على الجريمة، معرفة المتهم، وهذا فيما يتعلق بالتبليغ عن الجرائم بصفة عامة، في حين يستحب إن لم نقل يتوجب أن يكون المبلغ في الجرائم الإلكترونية على درجة مقبولة من الإلمام والمعرفة بالجوانب الفنية للحاسوب حتى يتمكن من تقديم معلومات تصف الحادث بشكل جيد بحيث يساعد ضابط الشرطة على فهم محتوى التبليغ ومباشرة عملية التحري بشأنه، كما يفترض في ضابط الشرطة القضائية أو متلقي البلاغ بصفة عامة أن يكون ذو خبرة فنية بالجوانب التقنية والمعلوماتية حتى يستطيع فهم جوانب البلاغ وعناصره وبالتالي مناقشة المبلغ بشكل أفضل والوصول إلى معلومات أكثر دقة.[3]

الفرع الثاني: المراكز المتخصصة بتلقي الشكاوى والبلاغات

في إطار مكافحة الجرائم الإلكترونية أنشئ مكتب التحقيقات الفيدرالي FBIمركزا لتلقي ومعالجة شكاوى جرائم الإنترنت (IC3)[4]عام 2000، ثم قام بإنشاء موقعا لتلقي شكاوى وبلاغات الاحتيال عبر

1نبيلة هبة هروال، الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات، المرجع السابق، ص 181.

2المرجع نفسه، ص 182 -183.

3حسين ربيعي، آليات البحث والتحقيق في الجرائم المعلوماتية، المرجع السابق، ص 216.

4IC3 : Internet Crime Complaint Centerمركز معالجة شكاوى جرائم الإنترنت

الإنترنت (IFCC)[1]والذي تم تأسيسه عام 2003في فرجينيا الغربية بالولايات المتحدة الأمريكية، [2]حيث يعمل المركز وموقعه بصورة تشاركية مع مكتب التحقيقات الفيدرالي والمركز الوطني لجرائم الياقات البيضاء(NWC)[3]من أجل مكافحة ظاهرة الاحتيال عبر الإنترنت التي ازدادت بكثرة في السنوات الأخيرة، ويقوم هذا المركز (أي مركز تلقي شكاوى الإنترنت) بتلقي الشكاوى عبر الموقع مخصص لذلكhttp://www.ifccfbi.gov.frمن خلال قيام الشاكي أو الضحية بملء استمارة إلكترونية متاحة على الموقع، وبمجرد وصول تلك الشكاوى إلى عنوان هذا المركز يقوم الفريق المختص في هذه الجرائم بترتيب هذه الشكاوى وتحليلها لتحديد تكييفها القانوني ودرجة الإجرام وتقييمه لإرساله بعد ذلك إلى السلطات القضائية المختصة بالبحث والتحري.[4]

وكذلك الموقع الإلكتروني الذي خصصته إدارة العدل الأمريكية "USDOJ"من أجل تقديم البلاغات بخصوص جميع الجرائم، وكذا موقع البلاغات للمخابرات المركزية الأمريكية "CIA"بالإضافة إلى موقع هيئة حماية البرمجيات الأوروبية "APP"وغيرها.[5]

أما في فرنسا فقد أنشأت الحكومة الفرنسية عدة مراكز ووحدات لمكافحة الإجرام الإلكتروني من بينها المكتب المركزي لمكافحة الإجرام المرتبط بتكنولوجيا المعلومات والاتصالات والذي من بين اختصاصاته تلقي البلاغات والشكاوى وتحليلها، حيث تقوم بهذه المهمة وحدة التحليل والتوثيق العملي التي يضمها هذا المكتب والمشار إليها في الباب الأول من الدراسة، [6] إذ تعمل هذه الوحدة على تلقي الشكاوى والبلاغات من جهة عن طريق منصتين استحدثتا لهذا الغرض أولهما منصة فاروس (Pharos)والتي تم إنشائها في 06/01/2009والثانية منصة(Info- Escroqueries) والتي تعملان على استقبال بلاغات وشكاوى ضحايا هذه الجرائم عن المحتويات والنشاطات غير المشروعة المرتكبة عبر الإنترنت، ومن بينها وجود مواقع تنشر صورا للاستغلال الجنسي للأطفال والتي يعمل هذا المكتب بالخصوص على محاربتها، وذلك عن طريق ملء استمارة تبليغ إلكترونية متاحة على الموقع الإلكتروني

1IFCC : Internet Fraude Complaint Centerمركز معالجة شكاوى الاحتيال عبر الإنترنت

2لمزيد من التفاصيل حول مركز تلقي شكاوى وبلاغات الاحتيال عبر الإنترنت، يراجع الرابط التالي: http://www.ifccfbi.gov

3NWC : National White Collier Centerالمركز الوطني لجرائم الياقات البيضاء

4Service de presse national de FBI : Internet fraud center, disponible sur le lien suivant : http://www.ifccfbi.gov Consulté le 10/10/2021 à 14 :00h

ينظر نبيلة هبة هروال، الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات، المرجع السابق، ص 193.

5عمر محمدأبو بكر بن يونس، الجرائم الناشئة عن استخدام الإنترنت (الأحكام الموضوعية والجوانب الإجرائية)، ط 01، دار النهضة العربية، مصر، 2004، ص 825.

6يراجع الفصل الثاني من الباب الأول من الدراسة، ص 12وما بعدها.

التالي المخصص لاستقبال هذه البلاغات "www. internet-Signalement.gouv.fr"[1]أو الخط الهاتفي التالي "0805805 817"المخصص لاستقبال البلاغات بشأن هذه الجرائم،[2] حيث تلقى المركز من خلاله حوالي (23695) اتصالا سنة 2020يحمل شكاوى من ضحايا وقعوا في شبكة الإجرام المعلوماتي.[3]

وبعد وصول هذه البلاغات إلى المكتب أو وحدة التحليل والتوثيق العملي يتم تسجيلها أوتوماتيكيا أو آليا في قاعدة البيانات الخاصة بالمكتب، ليقوم بعد ذلك بتحليلها ومراجعتها عن طريق القيام بمراجعة أولية لمحتواها والتأكد من صحة ما ورد فيها من معلومات وتقييمها، حيث يكون هذا التحليل من طرف مختصين وخبراء ومحققين ذوي خبرة عالية في المجال المعلوماتي والجنائي، ليتم إرسالها فيما بعد لأجهزة الشرطة والدرك ذوي الاختصاص الإقليمي، والذي ينعقد للجهة المتواجد فيها مستخدم الإنترنت الذي شاهد أو علم بالواقعة الإجرامية أو تضرر منها.[4]

وفي نفس الصدد قامت مصالح الدرك الوطني الفرنسي بتوفير بريد إلكتروني Judiciare@gendaremeriedefense.gov.fr لتلقي جميع شكاوى وبلاغات المواطنين في فرنسا بشأن كافة الجرائم بما فيها الجرائم الإلكترونية.[5]

وفي دولة الإمارات المتحدة خصص قسم مكافحة الجرائم الإلكترونية التابع لشرطة دبي موقعا إلكترونيا لتلقي البلاغات والشكاوى الخاصة بهذه الجرائم وذلك بملء استمارة إلكترونية متواجدة عبر الموقع التالي mail@dubaipolice.gov.ae[6]أو عبر الاتصال بالرقم "999"أو الرقم "901"، وبالنسبة للأطفال قد خصص نفس الموقع رقما هاتفيا للتبليغ عن المضايقات التي يتعرض لها الأطفال عبر الإنترنت على الرقم "8002626/116111"وأيضا عن طريق ملأ استمارة متاحة عبر الموقع الإلكتروني السابق،[7] كما خصصت وزارة الداخلية منصة إلكترونية تسمى"E.crime"تابعة لشرطة دبي لاستقبال بلاغات

1 Patforme Pharos Disponible sur le lien suivant :https://www.interieur.gouv.fr/A-votre-service/Ma-securite/Conseils-pratiques/Sur-internet/Signaler-un-contenu-suspect-ou-illicite-avec-PHAROS consulté le 30/10/2021 à 13h12

ينظر الملحق رقم 05.

2Platforme Téléphonique INFO ESCROQUERIES(0805 805 817)

3لمزيد من التفاصيل حول هذا المركز يراجع الرابط التالي: https://www.gouvernement.fr/risques/cybercriminalite

4نبيلة هبة هروال، الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات، المرجع السابق، ص 187.

5 المرجع نفسه، ص 182.

6لمزيد من التفاصيل يراجع الموقع الرسمي لقسم شرطة الجرائم الإلكترونية لإمارة دبي، المتاح على الرابط التالي:mail@dubaipolice.gov.aeتاريخ الاطلاع 13/06/2021على الساعة 19:00.

7 المرجع نفسه، ص 02

ضحايا هذه الجرائم واستفساراتهم حول مخاطر مواقع الإنترنت وكذا كيفية التعامل مع هذه التهديدات وذلك عبر الموقع التالي: ecrime@adpolice.gov.ae، [1] وفي هذا الصدد قد أوضحت عدة تقارير أن مؤشر البلاغات التي تستقبلها هذه المنصة حول الجرائم الإلكترونية يتفاوت بين 600و800بلاغ سنويا في حين أنه تم تسجيل أكثر من 25ألف بلاغ واتصال في سنة 2020وخاصة بسبب جائحة كورونا وما خلفته من جرائم، وهذا ما يفسر مدى وعي الأشخاص بمدى خطورة هذا النوع من الجرائم وحرصهم على حماية أمنهم وأمن بلدهم.

إضافة إلى الوحدات السابقة شكلت شرطة أبو ظبي فرقا متخصصة تعمل على استقبال البلاغات بشأن الجرائم الإلكترونية وتحليلها، إذ يقوم المبلغ بتقديم بلاغه على مستوى إدارة التحريات والمباحث الجنائية قسم الجريمة المنظمة، فرع الجرائم الإلكترونية، عن طريق حضوره الشخصي للإدارة أو عن طريق تواصله مع غرفة العمليات المركزية عبر الرقم "999"أو الاتصال بالرقم (025127777)، [2] أو الاتصال على خدمة **"أمان"**الإلكترونية التي تعمل على مدار الساعة وبسرية تامة، وذلك على الرقم المجاني (8002626) أو بواسطة الرسائل النصية (2828) أو عبر البريد الإلكتروني (aman@adpolice.gov.ae).[3]

كما وفرت وزارة الداخلية السعودية خدمة للمواطنين لتقديم بلاغاتهم عن الجريمة الإلكترونية من خلال موقع **"أبشر"**المرتبط بحساب المواطن وذلك بالدخول لموقع الوزارة والتوجه إلى خدمات الأمن العام ثم إلى خانة الجرائم الإلكترونية، ومن ثم اختيار البلاغ عن الجرائم الإلكترونية ليظهر لك استمارة إلكترونية تحوي خانات معينة يتم ملأها من طرف الشاكي أو الضحية وإرسالها عبر هذا الموقع، وفي الأخير سيظهر لمقدم البلاغ رقم بلاغه والذي يجب عليه حفظه من أجل متابعته، كما أطلقت الحكومة السعودية مشروعا للاتصال الموحد الذي يمكن المواطنين من الوصول لكافة خدمات الرئاسة ومن بينها خدمات مكافحة الجرائم الإلكترونية وخدمات مكافحة الابتزاز وأخرى للتوجيه والتوعية، وهذا من خلال الاتصال على الرقم الموحد "1909"، أو على الرقم الدولي "00966114998666"والمختص باستقبال

1المرجع نفسه، ص 03.

2أحمد عبد العزيز، "شرطة أبو ظبي تشكل فرقا متخصصة لمكافحة الجرائم الإلكترونية"، مقال منشور يوم الإثنين13/02/2012، على الرابط التالي: https://www.alittihad.ae/article/15105/2012تاريخ الاطلاع 13/06/2021على الساعة 21:00.
ينظر الملحق رقم 03.

3شرطة أبو ظبي: ""أمان"طريق الحماية من الابتزاز الإلكتروني"، مقال منشور يوم 24/12/2020، على الرابط التالي: https://www.emaratalyoum.com/local-section/other/2020-12-24-1.1435848تاريخالاطلاع13/06/2021على الساعة 20:30.

البلاغات في حالة كان الشخص المبتز من خارج المملكة العربية السعودية، بحيث بمجرد الاتصال يتم تسجيل بيانات الشخص المتصل بما فيها اسم الشاكي واسم الجاني والمكان وغيرها وإدخال هذه البلاغات داخل الأنظمة المعلوماتية التي تحتوي على برامج متطورة وتقنيات وأدوات متخصصة في التحليل الفني لهذه المعلومات ومن ثم استخراج الأدلة الرقمية ومعرفة النشاطات المتعلقة بكل دليل رقمي، ليتم بعد ذلك إعداد تقارير وإرسالها للأجهزة الشرطية وأجهزة التحقيق عبر كافة المناطق تمهيدا لإحالتها على الجهات القضائية.[1]

إلى جانب هذه المواقع يمكن التواصل مع وحدة مكافحة الجرائم الإلكترونية المشار إليها سابقا من خلال تطبيق متطور جدا استحدثته الحكومة السعودية تحت اسم "**كلنا آمن** "حيث يعتبر من التطبيقات الحكومية المجانية المتميزة وسهلة التعامل إذ يمكن لأي شخص تحميله بكل سهولة من متجر "آبل" أو "جوجل بلاي"، وهو يدار من قبل قسم مكافحة الجرائم الإلكترونية الذي يستقبل البلاغات من خلاله، ويمكن الاستفادة من هذا التطبيق من خلال إتباع خطوات معينة، فأول ما يقوم به الشخص المبلغ تحميل هذا التطبيق في هاتفه أو جهازه الإلكتروني بصفة عامة، ثم القيام بإنشاء حساب على هذا التطبيق والتسجيل فيه، ومن ثم يتم الدخول إلى هذا التطبيق ليظهر لنا ثلاثة خانات يتم الضغط على خانة "الدوريات الأمنية" والبدء في كتابة مضمون البلاغ، كما يمكن إرفاقه بصور أو فيديوهات أو ملاحظات معينة وإرساله ليتم إحالته من طرف الموظفين إلى الجهات المختصة بالتحقيق لاتخاذ الإجراءات اللازمة، وتجدر الإشارة إلى أن هذا التطبيق يضمن سرية هوية المبلغ وبياناته دون حضوره لمراكز الشرطة وهذا ما يضمن الحفاظ على خصوصية الأشخاص.[2]

واستكمالا للسياسة الجنائية للمشرع الجزائري في مجال مكافحة الجرائم بصفة عامة والجريمة الإلكترونية خاصة، قامت المديرية العامة للأمن الوطني بتعزيز وسائل التبليغ والتواصل مع المواطنين وذلك عن طريق تخصيص خانة لتقديم البلاغات والشكاوى على مستوى موقعها الرسمي، وكذا استحداث تطبيق ذكي ومتطور يطلق عليه تسمية "ألو شرطة" بحيث يسمح للمواطن بالتبليغ عن جريمة

1المعرفة المزيد حول خدمات أبشر يراجع الموقع الرسمي لصفحة أبشر المتاح على الرابط التالي: https://www.absher.sa/wps/portal/individualsتاريخ الاطلاع 15/06/2021على الساعة 18:00

2المعرفة خدمة البلاغات الأمنية على تطبيق "كلنا آمن"يراجع الموقع الرسمي للمنصة الوطنية الموحدة للمملكة العربية السعودية للخدمات والمعلومات الحكومية، المتاح على الرابط التالي:

https://www.my.gov.sa/wps/portal/snp/servicesDirectory/servicedetails/10262تاريخالاطلاع 15/06/2021على الساعة 18:30.

ما بواسطة الهاتف المحمول إما بإرسال صورة أو فيديو للحادثة أو السلوك المجرم، إذ يتيح هذا التطبيق سرعة التبليغ ويساعد ضباط الشرطة على معرفة أماكن تواجد الحادثة عن طريق نظام تحديد المواقع GPSناهيك على أنه نظام جد آمن وسري يحفظ البيانات والمعلومات وهوية المبلغ أيضا.[1]

من جهة أخرى قامت قيادة الدرك الوطني بإنشاء وإطلاق خدمة عمومية جديدة عبر 48ولاية باستعمال تكنولوجيات الإعلام والاتصال تحت اسم "الشكوى المسبقة والاستعلام عن بعد "حيث تدخل هذه الخدمة في إطار عصرنة الخدمات التي تقدمها وحدات الدرك الوطني خاصة في ظل الانتشار الواسع لاستخدام الإنترنت وما خلفته من تهديدات، إذ يمكن هذا التطبيق المواطنين من إيداع البلاغات والشكاوى المسبقة عن طريق الإنترنت وتأكيدها بعد ذلك لدى وحدة الدرك الوطني المعنية في غضون 30يوما، [2] ناهيك عن استحداث خدمة النيابة الإلكترونية وذلك على مستوى وزارة العدل الجزائرية، والتي من خلالها يمكن للمواطن تسجيل شكوى أو عريضة ومعرفة مآل هاته الأخيرة.[3]

وعليه إذا كان هذا الإجراء مستحسنا بحيث يمكن الضحية أو المبلغ من سهولة تقديم البلاغ أو الشكوى خاصة في الجرائم الإلكترونية وحتى إمكانية تثبيت هذا التطبيق على الهواتف النقالة الذكية للوصول إلى أكبر شريحة من الناس، إلا أنه يبقى إجراء غير رسمي إلى غاية تأكيده من طرف الضحية في غضون 30يوما، وهو فارق زمني كبير يتيح للمجرم إمكانية محو الدليل والتلاعب بالمعطيات، ولذلك نرى إعادة النظر في هذا الإجراء باعتماده رسميا من لحظة إرساله من طرف المبلغ ربحا للوقت واستباقا للخطوات التي يمكن اتخاذها من الطرف المجرم.[4]

استنادا إلى ما سبق ذكره يمكننا القول أنه بالرغم من أن العديد من الدول استحدثت مواقع إلكترونية وتطبيقات ذكية لتلقي البلاغات والشكاوى إلا أن بعضها الآخر وخاصة الدول المتخلفة تكنولوجيا لا تزال متأخرة نوعا ما في هذا المجال، وذلك إما لعدم وجود أجهزة متخصصة بالتحري في هذه الجرائم أو عدم إتاحتها لمواقع معينة لاستقبال البلاغات وحتى في حالة وجود هذه المواقع لم يتم تفعيلها

1مقابلة مع نوري ميلود، الملازم الأول للشرطة، رئيس فرقة مكافحة الجرائم المعلوماتية للمصلحة الولائية للشرطة القضائية، بمقر المصلحة، بتاريخ 26/07/2021، على الساعة 10:30.

ينظر الملحق رقم 04.

2يزيد بوحليط، الجرائم الإلكترونية والوقاية منها في القانون الجزائري في ضوء الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، (قانون العقوبات، قانون الإجراءات الجزائية)، دار الجامعة الجديدة، مصر، 2019، ص 319.

ينظر الملحق رقم 01.

[3] حيث تتوفر خدمة النيابة الإلكترونية على الموقع التالي: https://e-nyaba.mjustice.dz/choix.php

4 يزيد بوحليط، الجرائم الإلكترونية والوقاية منها في القانون الجزائري في ضوء الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، ص 320.

والعمل بها لعدم وجود إطارات متخصصة في ذلك، أو نتيجة نقص خبرة ضباط الشرطة القضائية في التعامل مع متطلبات التحري في مثل هذه الجرائم.

ومن هذا المنطلق فلا مناص من القول بأنه لتلقي الشكاوى والبلاغات عبر الإنترنت أهمية بالغة في مجال مكافحة الجرائم إ إذ يوفر لضابط الشرطة القضائية السرعة اللازمة في مباشرة إجراءات البحث والتحري بما يمكنه من الكشف المبكر عن الجريمة ومرتكبها.[1] كما يساعد في إبقاء هوية المبلغ مخفية مما يشجعه على الإبلاغ دون خشية من تعرضه للاعتداء من طرف الجاني إذا ما تعرف عليه.[2]

كما تظهر أهميته أيضا في أنه يساعد رجال البحث والتحري على تحديد نوع الجريمة المبلغ عنها ما إذا كانت من ضمن الجرائم الإلكترونية أو لا، وكذا وضع تصور مبدئي لخطة العمل المناسبة للبحث والتحري بشأن هذه الجريمة وبالتالي تحديد نوع الخبرة المطلوبة لأجل المعاينة وتحريز الأدلة، [3] ويجب الإشارة إلى أنه وقبل إنهاء عملية تلقي البلاغات يجب على المبلغ القيام بتجهيز قائمة تضم أسماء العاملين في المؤسسة أو المشتبه فيهم ممن لهم علاقة بالأجهزة المتضررة، وتجهيز نسخ احتياطية من بيانات الأجهزة المتضررة لفحصها من قبل فريق التحري فور وصوله لموقع الجريمة، وأخيرا التأكيد على المبلغ بضرورة عدم تبليغ أي أحد آخر بالجريمة إلا لمن لزم الأمر.[4]

ولكن وبالرغم من هذه الأهمية إلا أن أغلب الجرائم إ لا تصل عادة لعلم السلطات المختصة وذلك لصعوبة اكتشافها بواسطة الأشخاص العاديين، وإما نتيجة إحجام العديد من الأشخاص وحتى المؤسسات عن التبليغ عنها خوفا عن سمعتها أو تحسبا لردود أفعال الناس، كما أن البلاغ الرقمي كثيرا ما يكون مقيد ضد مجهول وهذا لصعوبة تحديد شخصية الجاني في مثل هذه الجرائم، بالإضافة إلى هذا وكما سبق ذكره بخصوص الشكوى فلا تختلف أحكامها في الجرائم التقليدية عن تلك الإلكترونية إذ لا يجوز للجهات المختصة تحريك الدعوى العمومية في هذه الجرائم إلا بعد تقديم شكوى من المجني عليه أو المتضرر من الجريمة أو من وكيله الخاص ضد المتهم أو الجاني والذي كثيرا ما يصعب تحديد شخصيته في مثل هذا النوع من الجرائم، وهذا ما أدى ببعض الفقه المقارن إلى اعتبار مزود الدخول لخدمات الإنترنت

1المرجع نفسه، ص 316.

2حسام محمد نبيل الشنراقي، الجرائم المعلوماتية، دراسة تطبيقية مقارنة على جرائم الاعتداء على التوقيع الإلكتروني، المرجع السابق، ص 341.

3حسين ربيعي، آليات البحث والتحقيق في الجرائم المعلوماتية، المرجع السابق، ص 218.

4لحسن ناني، التحقيق في الجرائم المتصلة بتكنولوجيا المعلوماتية بين النصوص التشريعية والخصوصية التقنية، النشر الجامعي الجديد، الجزائر، سنة 2018، ص 65.

مسئولا عن هذه الجرائم في حال عدم معرفة شخصية الجاني على أساس مبدأ افتراض مسؤولية الغير، وهذا ما يجعل موضوع الشكوى محل جدل قانوني وخصوصا إذا تم تقديمها ضد مزودي خدمات الإنترنت، دون متابعة التحريات لمعرفة الجاني الحقيقي.[1]

ناهيك عن أن تقديم الشكوى والبلاغ عبر الإنترنت يمكن أن يكون من شخص يستعمل هوية مستعارة أو أن الواقعة وهمية وهذا ما يتعارض مع كون الشكوى لا تقبل إلا من طرف المضرور، وإن تم قبولها في هذه الحالة يصبح الجميع يتعامل بشخصيات وأسماء مستعارة وهذا غير مشروع، إلا في بعض الحالات التي يسمح بها القانون،[2] مثل ذلك ما نص عليه المشرع الجزائري بخصوص إجراء التسرب المتعلق بالبحث والتحري في بعض الجرائم الخاصة والتي من بينها الجرائم الإلكترونية.[3]

المطلب الثاني: المعاينة التقنية لمسرح الجريمة الإلكترونية

للمعاينة أهمية كبيرة في كشف غموض الكثير من الجرائم، وتختلف المعاينة في الجرائم التقليدية عنها في الجرائم الإلكترونية وهذا راجع لطبيعة البيئة والمسرح الافتراضي الذي تتميز به هذه الجرائم، وعليه سنتطرق فيما يلي إلى تعريف المعاينة وكيفية القيام بها في المسرح الافتراضي للجريمة الإلكترونية، وكذا أهم الضوابط التي يتعين على ضابط الشرطة القضائية التقيد بها خلال معاينته لهذا المسرح.

الفرع الأول: تعريف المعاينة التقنية.

تعتبر المعاينة كأصل إجراء من إجراءات التحقيق أي أنها من اختصاص قاضي التحقيق،[4] إلا أنها يمكن أن تأمر بها المحكمة من تلقاء نفسها أو بناء على طلب أحد الخصوم،[1] كما يجوز لضابط الشرطة

1نبيلة هبة هروال، الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات، المرجع السابق، ص 185.

يراجع الفصل الأول من الباب الأول ص 54وما بعدها بخصوص مسؤولية مقدمي خدمات الإنترنت. (تعديل ص فيما بعد)

2يزيد بوحليط، الجرائم الإلكترونية والوقاية منها في القانون الجزائري في ضوء الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، المرجع السابق، ص 318.

3ينظر المادة 65مكرر 12من القانون رقم 06/22المتضمن قانون الإجراءات الجزائية الجزائري المشار إليه سابقا.

4تنص المادة 79من ق ا ج ج على: "يجوز لقاضي التحقيق الانتقال إلى أماكن وقوع الجرائم لإجراء جميع المعاينات اللازمة أو القيام بتفتيشها، ويخطر بذلك وكيل الجمهورية الذي له الحق في مرافقته، ويستعين قاضي التحقيق دائما بكاتب التحقيق ويحرر محضرا بما يقوم به من إجراءات"، وتقابلها المادة 90من ق ا ج المصري بقولها: "ينتقل قاضي التحقيق إلى أي مكان كلما رأى ذلك ليثبت حالة الأمكنة والأشياء والأشخاص ووجود الجريمة ماديا وكل ما يلزم إثبات حالته"، وتقابلهما المادة 92من ق ا ج الفرنسي بقولها:

« Le juge d'instruction peut se transporter sur les lieux pour y effectuer toutes constatations utiles ou procéder à des perquisitions. Il en donne avis au procureur de la République, qui a la faculté de l'accompager.

القضائية في حالات التلبس وفي الأحوال العادية القيام بهذا الإجراء، [2] كما يجوز أن يقوم بإجراء المعاينة المحضر القضائي والخبير كما هو الشأن في القانون الفرنسي، وذلك بناء على طلب الشخص المعني بعد موافقة القاضي المختص، [3] كما أجاز القانون الأمريكي (1) 2703 18US code secلعضو النيابة المعلوماتية CTCأن يعجل بإجراء المعاينة خشية ضياع الأدلة وتلفها، وذلك عن طريق إرسال رسالة إلى مزود خدمة الإنترنت ملزما إياه بالتحفظ على السجلات المطلوبة إلى حين صدور أمر المحكمة باتخاذها لذلك الإجراء أو غيره. [4]

وعن تعريف المعاينة نجد أن أغلب التشريعات لم تقم بإعطاء تعريف لها وإنما تركت ذلك للفقه الجنائي، فقد عرفها الدكتور أحمد فتحي سرور على أنها: "إثبات مباشر ومادي لحالة شيء أو شخص معين ويكون ذلك من خلال الرؤية أو الفحص المباشر للشيء أو الشخص". [5] أي هي ملاحظة وفحص حسي مباشر لمكان أو شخص أو شيء له علاقة بالجريمة لإثبات حالته والكشف والتحفظ على كل ما قد يفيد من الأشياء في كشف الحقيقة، [6] وقد عرفها البعض بأنها "إجراء بمقتضاه ينتقل المحقق إلى مكان وقوع الجريمة ليشاهد بنفسه ويجمع الآثار المتعلقة بالجريمة وكيفية وقوعها وكذلك جمع الأشياء الأخرى التي تفيد في كشف الحقيقة". [7]

أما عن معاينة مسرح الجريمة الإلكترونية يقصد به معاينة الآثار التي يتركها مستخدم الشبكة المعلوماتية أو الإنترنت بصفة عامة، وتشمل هذه الآثار الرسائل المرسلة منه أو إليه، وكذا الاتصالات التي

Le juge d'instruction est toujours assisté d'un greffier, Il dresse un procés- verbal de ses opérations ».

1تنص المادة 235من ق ا ج ج على: "يجوز للجهة القضائية إما من تلقاء تفسها أو بناء على طلب النيابة العامة أو المدعي المدني أو المتهم أن تأمر بإجراء الانتقالات اللازمة لإظهار الحقيقة".

2تنص المادة 42من ق ا ج ج على: "يجب على ضابط الشرطة القضائية الذي بلغ بجناية في حالة تلبس أن يخطر بها وكيل الجمهورية على الفور ثم ينتقل بدون تمهل إلى مكان الجناية ويتخذ جميع التحريات اللازمة.

وعليه أن يسهر على المحافظة على الآثار التي يخشى أن تختفي...". والتي تقابلها المادة 31من ق ا ج المصري بقولها: "يجب على مأمور الضبط القضائي في حالة التلبس بجناية أو جنحة أن ينتقل فورا إلى محل الواقعة، ويعاين الآثار المادية للجريمة ويحافظ عليها، ويثبت حالة الأماكن والأشخاص، وكل ما يفيد في كشف الحقيقة...".

3نبيلة هبة هروال، الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات، المرجع السابق، ص 215.

4المرجع نفسه، ص 215، ينظر أيضا عمر محمد أبو بكر يونس، الجرائم الناشئة عن استخدام الإنترنت، المرجع السابق، ص 895.

5عماد محمد، "المعاينة في مجال الجرائم الإلكترونية"، مقال منشور على موقع حماة الحق، على الرابط التالي: https://jordan-lawyer.com/2022/01/02/inspection-in-cybercrime/تاريخ الاطلاع: 23/04/2022على الساعة 16:00.

6نبيلة هبة هروال، الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات، المرجع السابق، ص 213.

7عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في الإثبات الجنائي، (دراسة مقارنة)، مذكرة مقدمة لنيل شهادة الماجستير في الحقوق، كلية الحقوق، جامعة الإسكندرية، سنة 2009، ص 47.

تمت من خلال هذه الشبكات الرقمية، وكذا البيانات المحفوظة داخلها أيا كان نوع الجهاز، مثل رسائل البريد الإلكتروني وصفحات المواقع المختلفة، الفيديوهات والتسجيلات الرقمية والصور، الملفات المخزنة في الحاسب الآلي...الخ.[1]

وللمعاينة أهمية كبيرة في مجال التحقيق الجنائي لكونها مصدرا أصيلا للأدلة المادية والفنية التي طالما تكون محل ثقة لدى سلطات التحقيق والقضاء، [2] إلا أنها ليست بذات الأهمية في كل أنواع الجرائم، إذ يتضاءل دورها في مجال كشف غموض الجريمة الإلكترونية وضبط الأشياء الناتجة عنها ونسبتها إلى مرتكبيها، ومرد ذلك أن هذا النوع من الجرائم قلما يخلف عن ارتكابه آثارا مادية، وبالتالي يصعب ضبط الآثار اللامادية الناتجة عن هذه الجرائم، ومن جهة أخرى فإن مسرح الجريمة الإلكترونية مسرح يسمح بتردد الكثير من الأشخاص خاصة في الفترة الزمنية بين ارتكاب الجريمة وبين اكتشافها مما يسمح بالتلاعب بالدليل الإلكتروني وإتلافه وهذا ما يشكك في قيمة الدليل المستمد من المعاينة، [3]ولهذا الغرض ولتأتي المعاينة بأغراضها المنشودة أحاطتها بعض التشريعات بجزاءات جنائية توقع على كل من يقوم بإحداث تغيير على حالة الأماكن التي وقعت فيها الجريمة، باستثناء ما إذا كانت تلك التغييرات ضرورية لسلامة الضحية أو تستلزمها المصلحة العامة، [4] ومثال ذلك ما نصت عليه المواد 43من ق ا ج ج والمادة 55من ق ا ج ف، [5] حرصا منه على المحافظة على مسرح الجريمة قبل القيام بالإجراءات الأولية للتحقيق، والملاحظ أن أحكام هاته المواد وإن كانت تنصرف إلى أغلب الجرائم التقليدية إلا أنه يمكن تطبيقها عند معاينة مكونات الأجهزة الإلكترونية ذات الطابع المادي، بخلاف المكونات غير المادية والتي تحتاج إجراءات خاصة تنظمها من أجل ضمان قيمة ومشروعية الدليل الإلكتروني المستمد منها.

1خالد ممدوح براهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، ط 1، دار الفكر الجامعي، مصر، 2018، ص165.

2جمال براهيمي، التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص 57.

3خالد ممدوح براهيم، الإثبات الإلكتروني في المواد الجنائية والمدنية، ط 01، دار الفكر الجامعي، الاسكندرية، مصر، سنة 2020، ص 94.

4نبيلة هبة هروال، الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات، المرجع السابق، ص 215.

5تنص المادة 43من ق ا ج ج على:"يحظر في مكان ارتكاب جناية على كل شخص لا صفة له أن يقوم بإجراء أي تغيير على حالة الأماكن التي وقعت فيها الجريمة أو ينزع أي شيء منها قبل الإجراءات الأولية للتحقيق القضائي، وإلا عوقب بغرامة من 200إلى 1000دج.

غير أنه يستثنى من هذا الحظر حالة ما إذا كانت التغييرات أو نزع الأشياء للسلامة والصحة العمومية أو تستلزمها معالجة المجني عليهم...".

Article n° 55 du Code de procédure pénale Français ;Modifié par loi n° 92-1336 du 16 Décembre 1992- art 11 JORF 23 Décembre 1992en vigueur le 1er Maes 1994 ; Dispose que : « Dans les lieux ou un crime a été commis, il est interdit, sous peine de l'amende prévue pour les contraventions de la quatrième classe, à toute personne non habilitée, de modifier avant les premières opérations de l'enquête juridique l'état des lieux et d'y effectuer des prélèvements quelconques ».

الفرع الثاني: كيفيات وضوابط معاينة مسرح الجريمة الإلكترونية

وتتم المعاينة في الجرائم الإلكترونية كأي جريمة أخرى عن طريق الانتقال إلى مسرح الجريمة، إلا أن هذا الانتقال يختلف حسب طبيعة محل الجريمة الإلكترونية، فإذا كانت الجريمة واقعة على المكونات المادية للأجهزة الإلكترونية كجرائم الاعتداء على الحاسب الآلي وغيرها، ففي هذه الحالة يكون الانتقال ماديا بحيث يقوم ضابط الشرطة القضائية بمعاينة جميع المكونات المادية المتواجدة بمسرح الجريمة والتحفظ على الأشياء التي تعد أدلة مادية، ومن ثم ضبطها في أحراز مختومة لتقدم للنيابة العامة، [1] أما إذا كانت الجريمة واقعة على المكونات غير المادية للأجهزة الإلكترونية أو بواسطتها، كتلك الواقعة على برامج الحاسب الآلي وبياناته وشبكة الإنترنت فيكون الانتقال للمعاينة هنا إلكترونيا وذلك بأن يدخل الضابط أو قاضي التحقيق للعالم الافتراضي عبر الإنترنت سواء انطلاقا من مكتبه عن طريق الحاسوب المتواجد به، أو من خلال مقهى الإنترنت أو إحدى مقرات مزود خدمات الإنترنت، الذي يعتبر أفضل مكان يمكن من خلاله إجراء المعاينة، كما يستطيع المحقق أيضا الانتقال إلى مقر مكتب الخبير التقني المختص إذ سمح له القانون بذلك.[2]

وتجدر الإشارة إلى أنه يجب على ضباط الشرطة القضائية قبل الانتقال لمعاينة مسرح الجريمة الإلكترونية اتباع مجموعة من الخطوات والتدابير الفنية والتحفظية التي تساعدهم في القيام بمهامهم على أحسن وجه، أهمها:

- ضرورة الحصول أولا على إذن أو أمر قضائي للقيام بإجراء المعاينة، إذ نصت المادة 47من ق ا ج ج على وجوب صدور إذن مسبق من وكيل الجمهورية المختص، أو أمر من النيابة العامة أو القاضي الجزئي المختص طبقا لقانون الإجراءات الجزائية المصري.[3]
- توفير معلومات مسبقة عن مكان الجريمة، وكذا نوع وعدد الأجهزة المتوقع مداهمتها وملحقاتها، ونوع الشبكات المتصلة بها والنهايات الطرفية المتصلة بها، وذلك لتحديد خطة التعامل معها.[1]

1وذلك عن طريق فحص الحواسيب ومكوناتها وكذا ملحقاتها، ولهذا ينبغي القيام بفحص القطع الصلبة والقطع المرنة أو ما يسمى بالبرمجيات، ومن ثم المعطيات والبيانات المخزنة داخلها، وتعتمد عملية الفحص هذه على طريقتين: تتمثل الأولى في الفحص الذاتي من خلال قيام الجهاز ذاته بفحص مكوناته وتقديم تقرير كامل عنها إلى طالب الفحص، أما الطريقة الثانية فتتمثل في الفحص بواسطة جهاز آخر للبحث في جزئية معينة عبر الحاسب مثلا، لمزيد من التفاصيل ينظر جمال براهيمي، التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص 57وما يليها.

2خالد ممدوح ابراهيم، الإثبات الإلكتروني في المواد الجنائية والمدنية، المرجع السابق، ص 96.

3المرجع نفسه ، ص 158.

- إعداد خريطة الموقع الذي سيتم الانتقال إليه مع ضرورة وضع خطة وتقسيم الأدوار على فريق التحري والتحقيق وتحديد مهام واختصاص كل واحد منهم .

- تأمين مصدر التيار الكهربائي حتى لا يتم التلاعب به عن طريق قطعه أو تعديله بهدف تعطيل عمل فريق المعاينة.[2]

- توفير الوسائل والإمكانات اللازمة من أجهزة وبرامج وأقراص للاستعانة بها في الفحص والتشغيل، وكذا ضبط وتأمين وحفظ المعلومات، مثل برنامج معالجة الملفات (Xtree Pro Gold)، وبرنامج النسخ (Lap Link)وغيرها...[3]

- التأكد من خلو المحيط الخارجي لمسرح الجريمة الإلكترونية من أية مجالات لقوى مغناطيسية التي يمكن أن تتسبب في محو وإتلاف البيانات المسجلة.[4]

- اقتصار عملية المعاينة على ضباط الشرطة القضائية ممن تتوافر فيهم الكفاءة العلمية والخبرة الفنية في المجال المعلوماتي، وممن تلقوا تدريبا للتعامل مع الأدلة الرقمية ومع هذا النوع من الجرائم، ونظرا لكون هذه الجرائم ذات طبيعة تقنية وفنية فيمكن لضباط الشرطة الاستعانة بفريق من المختصين وأهل الخبرة في مجال تكنولوجيات الإعلام والاتصال والإعلام الآلي، فمثلا في فرنسا يقوم فريق التحقيق المتكون من ثلاث عشر (13) شرطيا بالإشراف على تنفيذ المهام التي يأمر بها وكيل الجمهورية أو قاضي التحقيق، عن طريق مرافقتهم للمحققين أثناء عمليات المعاينة ويعملون على فحص الأجهزة ونسخ محتوياتها وإعداد تقارير فنية بذلك.[5]

- الحفاظ على سرية المعاينة إلى غاية الانتهاء من هذا الإجراء، مع مراعاة عدم الإفصاح عن المعلومات والبيانات المتحصل عليها تجنبا لعدم إتلافها أو التغيير فيها من قبل المتهمين.[6]

كما يجب إتباع بعض الخطوات عند الوصول إلى مسرح الجريمة الإلكترونية والمتمثلة فيما يلي:

- ضرورة التزام القائم بالمعاينة بالسرعة في التنقل إلى مسرح الجريمة الإلكترونية والسيطرة عليه وعلى جميع المنافذ الموجودة به، وفي هذا نجد أن المشرع الجزائري قد وسع من النطاق المكاني للمعاينة في

1حسين ربيعي، آليات البحث والتحقيق في الجرائم المعلوماتية، المرجع السابق، ص 239.

2 نبيلة هبة هروال، الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات، المرجع السابق، ص 219.

3يزيد بوحليط، الجرائم الإلكترونية والوقاية منها، المرجع السابق، ص 326.

4المرجع نفسه، ص 326.

5خالد ممدوح ابراهيم، الإثبات الإلكتروني في المواد الجنائية والمدنية، المرجع السابق، ص 110.

6حسام محمد نبيل الشنراقي، الجرائم المعلوماتية، المرجع السابق، ص 354.

الجرائم الإلكترونية وكذا من المجال الزمني لها، فقد أجاز من خلال المادة 47من ق ا ج ج القيام بعملية المعاينة في كل ساعة من ساعات الليل أو النهار وفي كل محل سكني أو غير سكني تفاديا منه ضياع الدليل الإلكتروني من مسرح الجريمة، وهذا ما جاء به القانون رقم 175لسنة 2018في شأن مكافحة جرائم تقنية المعلومات المصري في المادة 06منه، حيث حدد مجال القيام بالمعاينة بثلاثين (30) يوما قابلة للتجديد مرة واحدة دونما تحديد لساعات القيام بذلك.[1]

- ضرورة وضع حراسة كافية على مكان المعاينة ومراقبة التحركات داخل مسرح الجريمة مع رصد الاتصالات الهاتفية من وإلى مسرح الجريمة مع إبطال مفعول الهواتف النقالة التي تساعد عن طريق تقنية الجيل الثالث في تدمير الأدلة من خلال اتصالها بالأجهزة محل المعاينة.[2]

- الملاحظة الجيدة للطريقة التي تم بها إعداد النظام والآثار الإلكترونية، وإثبات حالة التوصيلات والكابلات المتصلة بكل مكونات النظام، وخاصة السجلات الإلكترونية التي تتزود بها شبكات المعلومات لمعرفة موقع الاتصال ونوع الجهاز الذي تم عن طريقه الولوج إلى النظام أو الموقع الإلكتروني، حتى تكون عملية المقارنة والتحليل فيما بعد ممكنة عند عرض الأمر على المحكمة.

- تصوير الجهاز الإلكتروني الذي ارتكبت عن طريقه الجريمة وما قد يتصل به من أجهزة طرفية ومحتويات، وتصوير أوضاع المكان الذي تتواجد به هاته الأجهزة، مع ضرورة تسجيل وقت وتاريخ ومكان التقاط هذه الصور.[3]

- عدم التسرع في نقل أي مادة معلوماتية من مسرح الجريمة وذلك قبل إجراء الاختبارات اللازمة للتيقن من عدم وجود أي مجالات مغناطيسية في المحيط الخارجي حتى لا يحدث أي إتلاف للبيانات المخزنة.

- القيام بحفظ المستندات الخاصة بالإدخال وكذلك مخرجات الحاسب الورقية ذات الصلة بالجريمة، وكذا رفع ما قد يوجد عليها من بصمات أو آثار مادية تفيد في كشف الحقيقة.[4]

- الحرص على عدم إتلاف أي بيانات يتم استخراجها من الجهاز، والتأكد من وجود نسخة منها داخل الجهاز نفسه، مع الفحص الدقيق لكل الملفات للتعرف على جميع العمليات التي قام بها مستخدم

1خضرة شنتير، الآليات القانونية لمكافحة الجريمة الإلكترونية، أطروحة مقدمة لنيل شهادة الدكتوراه، تخصص القانون الجنائي، كلية الحقوق والعلوم السياسية، جامعة أحمد دراية، أدرار، 2020/2021، ص 69.

2حسين ربيعي، آليات البحث والتحقيق في الجرائم المعلوماتية، المرجع السابق، ص 240.

3عيدة بلعابد، خصوصية التحقيق في الجريمة المعلوماتية، مجلة الباحث الأكاديمي في العلوم القانونية والسياسية، العدد 06، مارس 2021، ص 140.

4حسام محمد نبيل الشنراقي، الجرائم المعلوماتية، المرجع السابق، ص 359.

الجهاز وكذا المواقع الإلكترونية التي ارتادها على شبكة الإنترنت، وكذا معرفة أسماء حساباته على هذه المواقع وكلمات المرور الخاصة به.[1]

- التحفظ على محتويات سلة المهملات من أوراق ممزقة وأوراق مستعملة أو شرائط وأقراص ممغنطة لفحصها ورفع ما قد يوجد عليها من بصمات التي قد تكون لها صلة بالجريمة المرتكبة.[2]

- ضبط وتحريز الدعائم الأصلية للبيانات وعدم الاكتفاء بضبط النسخ، كما يجب مراعاة ظروف تخزينها كعدم وضعها على مقربة من محطة إرسال لاسلكي أو غيرها مما يسبب تلفها.[3]

من بين الإجراءات الهامة في نهاية المعاينة ينبغي على ضابط الشرطة القضائية التحفظ على مسرح الجريمة وعلة ذلك هي إمكانية العودة إليه كلما دعت الضرورة ذلك، مع تدوين هذه الإجراءات كتابة ورسما وتصويرا في محضر خاص بذلك مع تحديد تاريخ ووقت بدأ المعاينة ونهايتها.[4]

المبحث الثاني: الاستعانة بالخبرة والشهادة الإلكترونية

يعتبر كل من إجراء الخبرة والشهادة من الإجراءات الشخصية التي يتدخل فيها بعض الأشخاص بحكم صفتهم، من أجل الحصول على الدليل وإثبات الجريمة الواقعة، ولعل الجرائم الإلكترونية بما تتميز به من جوانب تقنية وأدلة فنية فإنه من الضروري استعانة سلطات التحري والتحقيق بأصحاب الخبرة الفنية لكشف غموض الجريمة وتحليل الأدلة الناتجة عنها، هذا من جهة، ومن جهة ثانية قد يستعين الضابط بفئة أخرى من الفنيين الذين لهم صلة مباشرة بتقديم وتسهيل خدمات النفاذ إلى الإنترنت وغيرها، لسماعهم كشهود على الجريمة الواقعة، وعليه سنتطرق فيما يلي إلى معرفة مدى استعانة ضباط الشرطة القضائية بأصحاب الخبرة من خبراء وشهود لإثبات الجرائم الإلكترونية؟ ومدى فاعلية هذه الإجراءات في الوصول إلى الحقيقة خاصة في هذا النوع من الجرائم؟

المطلب الأول: الاستعانة بالخبرة التقنية

أصبحت الاستعانة بالخبرة التقنية في فحص الأدلة وتحليلها أمرا ملحا لإثبات الجرائم الإلكترونية، إذ لا يعقل أن يفصل القاضي في قضايا تقنية المعلومات دون استناده إلى آراء الخبراء الفنيين في هذا

1خضرة شنتير، الآليات القانونية لمكافحة الجريمة الإلكترونية، المرجع السابق، ص 70.

2هشام محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية، المرجع السابق، ص 60، ينظر أيضا نبيلة هبة هروال، الجوانب الإجرائية لجرائم الإنترنت، المرجع السابق، ص 220.

3يزيد بوحليط، الجرائم الإلكترونية والوقاية منها، المرجع السابق، ص 328.

4خالد ممدوح ابراهيم، الإثبات الإلكتروني في المواد الجنائية والمدنية، المرجع السابق، ص 101.

المجال، وعلى هذا الأساس سنحاول من خلال هذا المطلب معرفة المقصود بالخبرة التقنية، وبيان أهميتها في إثبات الجرائم الإلكترونية، وكذا أهم الضوابط التي تحكم عمل الخبير الفني.

الفرع الأول: تعريف الخبرة التقنية

تعتبر الخبرة القضائية عموما وسيلة قررها المشرع لمساعدة القاضي في تقدير المسائل التي يحتاج إثباتها إلى معرفة فنية خاصة، ولهذا فإن الخبرة تفترض وجود واقعة مادية أو شيء يصدر الخبير حكمه فيه، [1] وذلك عن طريق التفسير الفني للأدلة بالاستعانة بالمعلومات العلمية، فهي في حقيقتها ليست دليلا مستقلا عن الدليل القولي أو المادي، وإنما هي تقييم فني لهذه الأدلة.[2]

وتعرف الخبرة القضائية على أنها: "تنقيب وبحث يرتبط بمادة تتطلب معارف علمية أو فنية خاصة لا تتوافر سوى لدى المحقق أو القاضي".[3]

كما عرفها جانب من الفقه المقارن على أنها "الاستشارة الفنية التي يستعين بها القاضي أو المحقق في مجال الإثبات لمساعدته في تقدير المسائل الفنية التي يحتاج تقديرها إلى معرفة فنية أو دراية علمية لا تتوافر لدى عضو السلطة القضائية المختص بحكم عمله وثقافته"، [4] أو أنها إجراء من إجراءات التحقيق يتم بموجبه الاستعانة بشخص يتمتع بقدرات فنية ومؤهلات علمية لا تتوافر لدى جهات التحقيق والقضاء، من أجل الكشف عن دليل أو قرينة تفيد في معرفة الحقيقة بشأن وقوع جريمة أو نسبتها إلى المتهم.[5]

والعنصر المميز للخبرة عن غيرها من الإجراءات الأخرى كالمعاينة والشهادة والتفتيش، هو الرأي الفني للخبير في كشف الدلائل أو تحديد قيمتها في الإثبات، الأمر الذي يتطلب مهارات ومعارف فنية وعلمية خاصة في القائم بها، [6] والذي يعرف على أنه هو كل شخص مختص فنيا في مجال من المجالات الفنية والعلمية، إذ يستطيع بما له من معلومات ومعرفة وخبرة إبداء رأيه في أمر معين يتعلق بالقضية

1رشيدة بوكر، الحماية الجزائية للتعاملات الإلكترونية، المرجع السابق، ص 380.

2خالد ممدوح براهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص 283.

3المرجع نفسه، ص 284.

4دلال ملياني مولاي، إشكالية الإثبات في جرائم الإنترنت في التشريع الجزائري، أطروحة مقدمة لنيل شهادة الدكتوراه، تخصص قانون خاص، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد، تلمسان، 2017/2018، ص 161.

5جمال براهيمي، التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص 68.

6يزيد بوحليط، الجرائم الإلكترونية والوقاية منها، المرجع السابق، ص 329.

المطروحة أو الجريمة الواقعة التي تحتاج طبيعتها إلى خبرة فنية خاصة،[1] وتتعدد أصناف الخبراء الإلكترونيون حيث يمكن تقسيمهم إلى طائفتين: تشمل الطائفة الأولى الخبراء من ضباط الشرطة القضائية الذين ينتمون للمعامل الجنائية المختصة بتحليل الأدلة الجنائية، والذين يتلقون دورات تدريبية خاصة ومتخصصة في مجال معين من مجالات التحقيق الجنائي، أما الطائفة الثانية فتشمل الخبراء من خريجي الكليات، ككلية الطب، كلية الهندسة، وغيرها، حيث يتم تدريبهم وتلقينهم بعض المواد القانونية والمبادئ الشرطية بما يتفق واحتياجاتهم في مجال عملهم،[2] ولعل من أهم الخبراء في مجال التعامل مع الأدلة الإلكترونية نجد كل من المبرمجين ومهندسي الصيانة والاتصالات، ومشغلي الحاسوب وشبكاته، ومديري النظام المعلوماتي، كما أنه لا يكفي حصول الخبير على درجة علمية معينة، وإنما يجب أن تتوافر لديه الإمكانات والقدرات العلمية والفنية التي تمكنه من اكتساب الخبرة في مجال معين.[3]

ومن المتفق عليه أن للخبرة أهمية بالغة في إثبات الجرائم بأنواعها لأنها تنير الدرب لسلطات التحقيق والقضاء في الوصول إلى الحقيقة وتحقيق العدالة الجنائية، لذلك فقد اهتم المشرع الجزائري بتنظيم أعمال الخبرة في المواد من 143إلى 156من ق ا ج ج، والتي أجازت لجهات التحقيق والحكم تعيين خبراء في المسائل التي تستدعي ذلك، إذ تنص المادة 143من ق ا ج ج على: "لجهات التحقيق أو الحكم عندما تعرض لها مسألة ذات طابع فني أن تأمر بندب خبير إما بناء على طلب النيابة العامة وإما من تلقاء نفسها أو الخصوم..."[4]كما قام بتعزيز قدرات النيابة العامة في معالجة القضايا ذات الطابع التقني، وذلك باستحداث وظيفة المساعدين المتخصصين الدائمين بموجب المادة 35مكرر من الأمر رقم 15/02المعدل والمتمم لقانون الإ ج ج، حيث يكون هؤلاء المساعدون تحت تصرف النيابة العامة بشكل دائم للاستعانة بآرائهم وخبرتهم في مختلف المسائل الفنية أثناء التحريات الأولية.[5]

وهو ما أجازه المشرع الفرنسي في المواد من 156إلى 169من ق ا ج ف، والمشرع المصري في المواد 85إلى 89من ق ا ج م، التي سمحت لكل من مأموري الضبط والنيابة العامة وقاضي التحقيق الاستعانة

1خالد ممدوح براهيم، الإثبات الإلكتروني في المواد الجنائية والمدنية، المرجع السابق، ص 188.

2خالد ممدوح ابراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص 287.

3ليندا بن طالب، الدليل الإلكتروني ودوره في الإثبات الجنائي، المرجع السابق، ص 77.

4ينظر المادة 143من ق ا ج ج.

5رشيدة بوكر، الحماية الجزائية للتعاملات الإلكترونية، المرجع السابق، ص 381.

بالخبراء، والمادتين 292و293من ذات القانون التي أجازت للمحكمة ندب الخبراء بناء على طلب الخصوم أو من تلقاء نفسها.[1]

وإن كانت الاستعانة بخبير فني في المسائل الفنية البحتة في الجرائم التقليدية أمر واجب على جهة التحقيق والقاضي، فهي أمر لابد منه في مجال استخلاص الدليل التقني لإثبات الجرائم الإلكترونية، كونها تتعلق بمسائل تقنية وفنية معقدة تستلزم شخص ذو خبرة ودراية بهذه الأمور ليستطيع التعامل معها وكشف غموضها، إذ يصعب على جهات التحقيق والتحري فهم الدليل الإلكتروني خاصة أنه دليل غير مادي ذو طبيعة خاصة، كما أنه سهل التدمير والإتلاف وهذا ما يؤكد ضرورة وأهمية الاستعانة بالخبراء في مجال التحري عن هذا النوع من الإجرام، ولعل هذه الأهمية والدور الرئيسي الذي تلعبه الخبرة في مجال الإثبات الجنائي، جعلت بعض التشريعات المقارنة لا تكتفي بالنصوص التقليدية التي تنظم الخبرة، وإنما عملت على استحداث أحكام قانونية خاصة بتنظيم أعمال الخبرة في مجال الجرائم الإلكترونية،[2] فنجد على الصعيد الدولي مثلا المادة 27من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المحررة بالقاهرة في 2010، والمصادق عليها بالمرسوم الرئاسي رقم 14-252، والتي نصت على أنه تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين السلطات المختصة من إصدار الأوامر إلى أي شخص لديه معرفة بوظيفة تقنية المعلومات، من أجل تقديم المساعدة لها لإتمام إجراءات التحقيق.[3]

أما عن أهم التشريعات التي بادرت بتنظيم نصوص خاصة تحكم أعمال الخبرة، نجد التشريع البلجيكي الصادر في 23نوفمبر 2000، حيث أجازت المادة 88منه لقاضي التحقيق والشرطة القضائية أن يستعينا بخبير ليقدم وبطريقة مفهومة المعلومات اللازمة عن كيفية تشغيل النظام، وكيفية الدخول للبيانات المخزنة أو المعالجة أو المنقولة بواسطته، أو البحث داخل هذا النظام وعمل نسخة من البيانات المطلوبة للتحقيق على أن يتم ذلك تحت سلطة التحقيق.[4]

كما نظم المشرع المصري هو الآخر عمل الخبراء وذلك في القانون رقم 175لسنة 2018في شأن مكافحة جرائم تقنية المعلومات، حيث قرر في نص المادة 10منه إنشاء سجلان بالجهاز القومي لتنظيم الاتصالات لقيد الخبراء الفنيين والتقنيين للاستعانة بهم في تحري الجرائم الإلكترونية إذ خصص سجل

1خالد ممدوح ابراهيم، الإثبات الإلكتروني في المواد الجنائية والمدنية، المرجع السابق، ص 189.

2خضرة شنتير، الآليات القانونية لمكافحة الجريمة الإلكترونية، المرجع السابق، ص 111.

3ينظر المادة 27من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المحررة بالقاهرة في 2010، المشار إليها سابقا

4خالد حسن أحمد لطفي، الدليل الرقمي ودوره في إثبات الجريمة المعلوماتية، ط 1، دار الفكر الجامعي، مصر، 2020، ص 104.

للفنيين والتقنيين العاملين بالجهاز، والثاني لغير العاملين بهذا الجهاز، وتطبق عليهم في ممارسة مهامهم هذه نفس القواعد والأحكام الخاصة بتنظيم الخبرة أمام جهات القضاء.[1]

ولم يتخلف المشرع الجزائري عن هذه التشريعات، إذ لم يكتفي بهاته النصوص التقليدية و نظم أعمال الخبرة في بعض النصوص الخاصة مثل ما جاء في نص المادة 05من القانون رقم 09/04المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، [2] إذ سمح للسلطة المكلفة بتفتيش المنظومات المعلوماتية تسخير كل شخص له دراية بعمل المنظومة المعلوماتية محل البحث والتحري، لمساعدتها وتزويدها بكل المعلومات الضرورية لإنجاز مهامها، ولعل استخدام المشرع هنا لعبارة "أي شخص له دراية "أمر مقصود حتى يوسع من دائرة المساعدة القضائية في مجال مكافحة الجرائم الإلكترونية لتشمل إلى جانب الخبير، جميع المتخصصين والعاملين في مجال تكنولوجيا الإعلام والاتصال، مثل مهندسي الإعلام الآلي، ومزودي خدمات الإنترنت وغيرهم.[3]

ولم تتوقف هذه التشريعات عند هذا الحد، بل قامت بإنشاء هيئات متخصصة في مواجهة هذه الجرائم مزودة بوسائل وتقنيات متطورة مهمتها إنجاز الخبرات لمساعدة سلطات التحقيق، على رأسها الولايات م أ، التي أسست المعمل الإقليمي الشرعي للحاسب الآلي التابع للمباحث الفيدرالية والمسمى "The Regional computer forensicslaboratory" الكائن "بسان دييجو"، حيث أعد هذا الأخير ليكون مقرا للخبرة متعدد النواحي القضائية، يهدف لمكافحة الإجرام الخطير والإجرام المعلوماتي، من خلال قيامه بتصنيف وتحليل الأدلة الرقمية من طرف محللين ومختصين في هذا المجال يتمتعون بالخبرة العلمية والتقنية، والذين تلقوا تدريبا في مجال التعامل مع هذه الأدلة.[4]

وبدوره قام المشرع الجزائري بإنشاء هيئات متخصصة في هذا المجال، من بينها الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، حيث تتولى مديرية المراقبة الوقائية واليقظة الإلكترونية مهمة إنجاز الخبرات القضائية في مجال اختصاص الهيئة، [5] ومساعدة السلطات ومصالح الشرطة القضائية بناء على طلبها، طبقا للمادة 15من المرسوم الرئاسي رقم 439/21

1خالد ممدوح ابراهيم، الإثبات الإلكتروني في المواد الجنائية والمدنية، المرجع السابق، ص 189.

2ينظرالمادة 05من القانون رقم 09/04المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها المشار إليه سابقا.

3جمال براهيمي، التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص 71.

4حسام محمد نبيل الشنراقي، الجرائم المعلوماتية، المرجع السابق، ص 451.

5دلال ملياني مولاي، إشكالية الإثبات في جرائم الإنترنت في التشريع الجزائري، المرجع السابق، ص 164.

الذي يتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، كما نجد مركز الوقاية من جرائم الإعلام الآلي والجرائم الإلكترونية الذي أنشئ من قبل قيادة الدرك الوطني عام 2009والذي يتولى تحليل المعطيات الخاصة بالجرائم الإلكترونية وتحديد هوية مرتكبيها، فضلا عن تأمين الأنظمة المعلوماتية، والمعهد الوطني للبحث في علم التحقيق الجنائي الذي تم إنشاؤه بموجب المرسوم الرئاسي رقم 04-432[1]الذي تضمن مصلحة للخبرات الخاصة بالدلائل التكنولوجية، وكذا القسم الخاص بالخبرة التقنية التابع لنيابة الشرطة العلمية والتقنية بمديرية الشرطة القضائية، بالإضافة إلى قسم الأدلة الإلكترونية والرقمية الموجود على مستوى كل المخابر الجهوية، [2] كما قام المشرع بإنشاء المعهد الوطني للأدلة الجنائية وعلم الإجرام بموجب المرسوم الرئاسي رقم 04- 183، [3] والذي يدعم أجهزة التحري والتحقيق بما يقوم به من خبرات علمية وتقنية وتحاليل معقدة للأدلة والأجهزة الإلكترونية.[4]

الفرع الثاني: الضوابط القانونية والفنية التي تحكم الخبرة التقنية

باعتبار الخبرة التقنية إجراء من إجراءات التحقيق والإثبات الجنائي تم إخضاعها لمجموعة من الضوابط القانونية والفنية التي تعتبر كضمانات هامة تساعد في إنجاز أعمال الخبرة وتضمن مشروعية الحصول على الدليل الإلكتروني، وحجيته في إثبات الجرائم الإلكترونية، وتتمثل هذه الضوابط فيما يلي:

أولا: الضوابط القانونية التي تحكم الخبرة التقنية

تتمثل هذه الضوابط فيما يلي:

1) اختيار الخبير من جدول الخبراء

الأصل أن يختار الخبراء حسب التخصص من الجداول التي تعدها المجالس القضائية بعد استطلاع رأي النيابة العامة، ولكن كاستثناء في حالة ما لم يتضمن الجدول الخبراء المتخصصين في مجال الخبرة

1 نصت المادة 05 من المرسوم الرئاسي رقم 04- 432المؤرخ في 29/12/2004يتضمن إنشاء المعهد الوطني للبحث في علم التحقيق الجنائي على: "يتولى المعهد المهام التالية:...إعداد التقارير الخبرة بناء على طلب من السلطات المختصة المؤهلة قانونا، القيام بأعمال التكوين وتجديد المعارف وتحسين المستوى ...".

2جمال براهيمي ، التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص 72.

3المرسوم الرئاسي رقم 04- 183المؤرخ في 26/06/2004، يتضمن إحداث المعهد الوطني للأدلة الجنائية وعلم الإجرام المشار إليه سابقا.

4يراجع الفصل الثاني من الباب الأول لمزيد من التفاصيل، ينظر أيضا يزيد بوحليط، الجرائم الإلكترونية والوقاية منها، المرجع السابق، ص 338.

فإنه يجوز لجهات التحقيق اختيار خبراء ليسوا مقيدين في هذا الجدول،[1] وهذا ما نص عليه المشرع الفرنسي بموجب الفقرة الثانية من المادة 157من ق ا ج التي أجازت استثناء وبقرار مسبب للمحكمة أن تختار خبراء ليسو من هذه الجداول، وهو ما أكده المشرع الجزائري في المادة 144من ق ا ج ج،[2] وتبقى كيفية اختيار الخبير في المسألة المطروحة أمرا متروكا لجهات التحقيق، فطبقا لنص المادة 147من ذات القانون يمكن للقاضي أن يندب خبيرا واحدا أو عدة خبراء حسب الحاجة لذلك، حيث لا تهم طبيعة الخبير سواء كان شخصا طبيعيا أو معنويا كأن يكون مؤسسة متخصصة في مجال الخبرة التقنية مثلا،[3] ونحن نرى أنه حسن ما فعل المشرع هنا لاسيما أمام ما يثيره مجال تقنية المعلومات من جدل واسع حول كيفيات التعامل معه وكذا النتائج الممكن تحقيقها فيه، إلا أنه رغم ذلك يبقى هذا التوجه قاصرا ويحتاج إلى تطوير في مجال الجرائم الإلكترونية حتى يسمح بالاستعانة بخبراء الرقمنة والإعلام الآلي من الدول الأجنبية ولو عن بعد، سيما أن البيئة والعالم الذي يتم التعامل معه في هذه الجرائم هو عالم رقمي يسمح بالاتصال بين دول العالم، إذ نجد أن هذا الأسلوب من التعاون بين الخبراء موجود في العديد من الدول المتقدمة في حين لا نجد تطبيقه في الدول المتخلفة أو النامية، ولعل المشرع الجزائري أجاز للقضاة الاستعانة بجهات مماثلة عن طريق الهيئة الوطنية للوقاية من الجرائم الإلكترونية كما أشرنا سابقا، إذ تتولى إنجاز الخبرات القضائية لمساعدة السلطات القضائية، وتبادلها مع العديد من الدول في إطار التعاون والمساعدة القضائية، ولهذا حبذا لو تهتم جميع الدول خاصة التي تعاني من نقص الكفاءة في مجال تكنولوجيات الإعلام والاتصال، بإبرام اتفاقيات التعاون بين الدول الأجنبية للاستفادة من خبراتها في مكافحة الجرائم الإلكترونية.

2) واجبات الخبير التقني:

لضمان صحة تقرير الخبرة ونيل ثقة أطراف الدعوى، أوجب المشرع الجزائري على الخبير حلف اليمين القانونية قبل البدء في إنجاز الخبرة المطلوبة، وذلك في حدود ما نص عليه أمر أو حكم الندب ، وتحت رقابة قاضي التحقيق أو القاضي الذي أمر بإجراء الخبرة. ولعل العبرة من هذا هي حمل الخبير على

1نعيم سعيداني، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، المرجع السابق، ص 168.

2تنص المادة 144من ق ا ج ج على: "يختار الخبراء من الجدول الذي تعده المجالس القضائية بعد الاستطلاع رأي النيابة العامة".

أما بالنسبة للمشرع المصري فلم يعد يعمل بنظام الجداول وذلك بعد أن قفل المرسوم رقم 96لسنة 1952الخاص بتنظيم الخبرة أمام جهات القضاء هذه الجداول، ليقوم بأعمال الخبرة أمام جهات القضاء حسب المادة 2من هذا المرسوم خبراء وزارة العدل ومصلحة الطب الشرعي والمصالح الأخرى التي يعهد إليها بأعمال الخبرة، وكل من ترى جهات القضاء ضرورة الاستعانة برأيهم الفني من غير من ذكروا. لمزيد من التفاصيل ينظر بوكر رشيدة، الحماية الجزائية للتعاملات الإلكترونية، المرجع السابق، ص 384وما بعدها.

3ينظر المادة 147من ق ا ج ج.

الصدق والأمانة في عمله، وبث الطمأنينة في نتائج خبرته التي يقدمها سواء بالنسبة لتقدير القاضي أو الثقة ببقية أطراف القضية، [1] وهو ما نص عليه المشرع المصري بدوره بموجب المادة 86من ق ا ج م، هذا وقد استقر الفقه والقضاء عموما على أن أداء الخبير لليمين يوم تسلمه العمل يغني عن أدائه اليمين عند مباشرته لأعمال الخبرة، ولا مانع من إعادة استحلافه لليمين قبل أداء مهامه.[2]

كما يعد من واجب الخبير الاستجابة للطلبات التي يطلبها أطراف الدعوى أثناء إجراء أعمال الخبرة، ومن ذلك تكليف الخبير بإجراء أبحاث معينة ذات طابع فني تفيد في إجراءات التحري والتحقيق، هذا ما أجازته المادة 152من ق ا ج ج، والمادة 165من ق ا ج ف، [3] كما يلتزم أيضا بأداء مهمته المكلف بها بنفسه، فلا يصح أن يحيل غيره للقيام بذلك، إلا أن بعض التشريعات خرجت عن هذه القاعدة منها المشرع الفرنسي الذي نجده أجاز استعانة الخبير بغيره من الفنيين المختصين وهو ما أشارت له المادة 162من ق ا ج ف.[4]

كما أجاز المشرع الجزائري للخبير الاستعانة بأخصائي لمساعدته في إنجاز خبرته طبقا للمادة 149من ق ا ج ج، وإن كان يشترط أن يكون ذلك بتصريح من القاضي على أن يقوم هؤلاء الخبراء بحلف اليمين ويرفق تقريرهم مع تقرير الخبراء الأصليين، [5] وهذا ما لم يبينه المشرع المصري من خلال أحكام قانون الإجراءات الجزائية.

1يزيد بوحليط، الجرائم الإلكترونية والوقاية منها، المرجع السابق، ص 332.

2رشيدة بوكر، الحماية الجزائية للتعاملات الإلكترونية، المرجع السابق، ص 386.

3رشيدة بوكر، جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري والمقارن، ط 1، منشورات الحلبي الحقوقية، لبنان، 2012، ص 428.

4Article n° 162 modifié par loi n° 2004-130 du 11 février 2004 – art 56 JORF 12 février 2004 ;dispose que : «Si les experts demendent à être éclairés sur une question échappant à leur spécialité, le juge peut les autoriser à s'adjoindre des personnes nommément désignées, spécialement qualifiées par leur compétence. Les personnes ainsi désignées prètent serment dans les conditions prévues à l'article 160, leur rapport sera annexé intégralement au rapport mentionné à l'article 166. »

5تنص المادة 149من ق ا ج ج على: "إذا طلب الخبراء الاستنارة في مسألة خارجة عن دائرة تخصصهم فيجوز للقاضي أن يصرح لهم بضم فنيين يعينون بأسمائهم ويكونون على الخصوص مختارين لتخصصهم.

ويحلف الفنيون المعينون على هذا الوجه اليمين ضمن الشروط المنصوص عليها في المادة 145. ويرفق تقريرهم بكامله بالتقرير المنوه عنه في المادة 153."

كما وتجدر الإشارة إلى أنه يمكن للخبير الاستعانة بأقوال الجناة وشهاداتهم إذ كثيرا ما تتضمن عوامل تساعده في خبرته، ولذا يمكن أن يستعين بالمجرم المعلوماتي للتعرف على أسلوبه في ارتكاب تلك الجريمة.[1]

بعد انتهاء الخبير من أعماله التي كلف بها، يقوم بإيداع تقرير الخبرة التقنية لدى كتابة الجهة القضائية التي أمرت بالخبرة، خلال المدة المحددة في أمر أو حكم الندب ، مع تقديم نتائج هذه الخبرة وما قام به من أبحاث، وفي حالة مخالفته لهذه الشروط جاز للقاضي استبداله بغيره، أو حتى توقيع عقوبات تأديبية عليه تصل إلى شطب اسمه من جداول الخبراء بقرار من الوزير، في حالة وقوع إهمال منه.[2]

وبناء على ما سبق إذا توفرت الخبرة على هذه الشروط المذكورة أعلاه يكون لها حجية نسبية أمام القضاء، لأن نتائج الخبرة ما هي إلا مجرد استدلال يعتمده القاضي لإنارته في حكمه، ذلك لأن رأي الخبير يعطى بصفة استشارية وليس له قوة ملزمة، حيث لا يقيد هذا التقرير القاضي وإنما له أن يأخذ به على سبيل الاستدلال أو يطرحه، كما له أن يفاضل بين تقارير الخبراء ويأخذ منها ما يرتاح إليه ويطرح ما عداه، وله أن يأمر بإجراء خبرة إضافية إذا كان هذا التقرير ناقص أو غير كامل، [3]إلا أنه في حالة عدم موافقة القاضي على هذا التقرير يجب أن يقوم بتسبيب هذا الرفض.

ونفس الأمر يسري على الخبرة التقنية التي تكون في إطار الجرائم المتعلقة بتكنولوجيا المعلومات وشبكة الإنترنت، إلا أن إعمال مبدأ "القاضي خبير الخبراء "في مثل هذه الحالات أمر غير ممكن إذ لابد من تعيين خبير فني يجيد التعامل مع هذه التطورات والمعلومات، ذلك لأنه لا تسمح ثقافة القاضي المبنية على الدراسات القانونية من التفاعل مع هذه التطورات والبيئة الافتراضية الجديدة وما ينتج عنها من جرائم، وهذا لا يعني تغليب رأي الخبير على رأي القاضي فيبقى رأي الخبير مقتصر على المسائل الفنية فقط.

ثانيا: الضوابط الفنية التي تحكم الخبرة التقنية

تتمثل هذه الضوابط فيما يلي:

1) المواضيع التي يتعين على الخبير الإلمام بها:

1ليندا بن طالب، الدليل الإلكتروني ودوره في الإثبات الجنائي، المرجع السابق، ص 79.

2يزيد بوحليط، الجرائم الإلكترونية والوقاية منها، المرجع السابق، ص 330.

3رشيدة بوكر، جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري والمقارن، المرجع السابق، ص 429.

بالنظر للطبيعة الفنية والعلمية للدليل الإلكتروني ينبغي للخبير إلى جانب ما يتوفر فيه من شروط شكلية وموضوعية، الإلمام بالجوانب التقنية في مجال تكنولوجيا المعلومات، إذ يجب عليه:

- الإلمام بتركيب الحاسب وصناعته وطرازه، ونظم تشغيله الرئيسية والفرعية، وكذا الأجهزة الملحقة به، وكلمات المرور وأكواد التشفير.

- معرفة طبيعة البيئة الإلكترونية التي يعمل فيها هذا الجهاز الإلكتروني، وتوزيع الشبكة قفيها ونمط ووسائل الاتصالات.

- يجب أن تكون لديه المهارة التي تسمح له بعزل النظام المعلوماتي والحفاظ على الأدلة المتواجدة به، ونقلها من شكلها غير المرئي إلى أدلة مقروءة مادية دون إتلافها.[1]

- الالتزام بأحكام ونصوص القوانين التي تنظم عمل الخبراء وكذا القوانين الإجرائية وقوانين مكافحة الجرائم الإلكترونية.

- الإلمام بعلم وفن التحقيق الجنائي بصفة عامة، والتحقيق في الجرائم الإلكترونية بصفة خاصة.[2]

- معرفته لوسائل وطرق فحص النظام وتشغيله، مثل برامج كشف الفيروسات وإزالتها، وبرامج استرجاع البيانات والمعلومات التي تم محوها أو التغيير فيها.[3]

2) أساليب عمل الخبير في اكتشاف الدليل الإلكتروني والتعامل معه:

قد وضعت وزارة العدل الأمريكية إطارا عمليا يحدد خطوات أساسية لجمع الأدلة الإلكترونية ثم فحصها ومن ثم تحليلها وصولا إلى نتائج معينة يتم تدوينها في تقرير الخبرة، ولكن قبل التطرق إلى هذه المراحل على الخبير القيام ببعض الخطوات القبلية والتي تكون قبل تشغيل الجهاز الإلكتروني وفحصه، منها التأكد من مطابقة محتويات أحراز المضبوطات لما هو مدون عليها، التأكد من صلاحية وحدات نظام التشغيل، والقيام بتسجيل معطيات وحدات المكونات المضبوطة.[4]

وبعد تأكد الخبير التقني من هذه الأمور يبدأ في مرحلة التشغيل والفحص، وذلك عن طريق استكمال تسجيل باقي بيانات ومعطيات الوحدات من خلال قراءة الأجهزة الإلكترونية،[5] وعمل نسخ

1يزيد بوحليط، الجرائم الإلكترونية والوقاية منها، المرجع السابق، ص 334.

2رفاه خضير جياد العارضي، الدليل الإلكتروني وأثره في مجال نظرية الإثبات الجنائي، ط1، مكتبة زين الحقوقية والأدبية، 2019، ص 170.

3سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، المرجع السابق، ص 170.

4 المرجع نفسه، ص 171.

5يزيد بوحليط، الجرائم الإلكترونية والوقاية منها، المرجع السابق، ص 335.

مطابقة للأصل عن كل وسائط التخزين المضبوطة، كالقرص الصلب مثلا لحماية الأصل من التغيير أو التلف، ومن ثم البدء في إظهار واسترجاع الملفات والمعلومات المخفية أو التي تم محوها وذلك باستخدام برامج ووسائل متطورة مخصصة لاستخلاص الدليل الرقمي، نذكر منها:

- **بروتوكول الإنترنت (IP)**

أو ما يسمى بعنوان الإنترنت، وهو نظام يشبه عنوان البريد العادي يعمل على تراسل حزم البيانات عبر شبكة الإنترنت وتوجيهها إلى أهدافها، فهو موجود بكل جهاز إلكتروني مرتبط بشبكة الإنترنت، ويتكون من أربعة أجزاء كل جزء يتكون من أربعة خانات، حيث يشير الجزء الأول من اليسار إلى المنطقة الجغرافية، والجزء الثاني لمزود الخدمة، وأما الجزء الثالث لمجموعة الأجهزة الإلكترونية المرتبطة ، ويحدد الجزء الرابع الجهاز الذي تم الاتصال به، [1] وعليه في حالة وجود أي جريمة إلكترونية أو أعمال تخريبية فإن الخبير يقوم بالبحث عن رقم الجهاز وتحديد موقعه لمعرفة الجاني، كما يمكن لمزود خدمة الإنترنت أو خدمة الاتصال الهاتفي أن يراقب المشترك.

وتتعدد الطرق التي يتم من خلالها معرفة العنوان الخاص بجهاز الكمبيوتر في حالة الاتصال المباشر، فعلى سبيل المثال ما يستخدم في حالة العمل على نظام تشغيل Windowsحيث يتم كتابة كلمة Winpcfgفي أمر التشغيل ليظهر مربع حوار يبين فيه عنوان (IP) الخاص بذلك الجهاز، وبهذا يتتبع الخبير المسار التراسلي لغاية الوصول إلى عنوان بروتوكول الإنترنت.[2]

- **نظام البروكسي (PROXY)**

يعمل هذا النظام كوسيط بين الشبكة ومستخدميها، حيث يضمن توفير خدمات الذاكرة الجاهزة (Cache Memory)، وتقوم فكرة هذا النظام على تلقي مزود البروكسي طلبا من المستخدم للبحث عن صفحة ما ضمن الذاكرة الجاهزة، فيقوم هذا النظام بالتحقق فيما إذا كانت هذه الصفحة قد جرى تنزيلها من قبل أو لا، ويقوم بإرسالها للمستخدم دون الحاجة لإرسال الطلب إلى الشبكة العالمية مرة أخرى، وفي حالة ما لم يتم تنزيلها من قبل فيقوم بإرسال الطلب إلى الشبكة العالمية، [3]ونجد دولة الإمارات العربية المتحدة قد طبقت هذا النظام فعندما يطلب المشترك موقعا ما على الشبكة تصل الإشارة إلى

1جمال براهيمي، التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص 78.

2خالد ممدوح ابراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص 304.

3جمال براهيمي، التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص 79.

الرقيب الذي يقوم بدوره بعرض الموضوع على قائمة كبيرة من المواقع الممنوعة، فإذا تبين له أن الموقع المطلوب يدخل ضمن هذه المواقع المحظورة فلا يستطيع المشترك الحصول عليه.[1]

ومن مزايا هذا النظام أن الذاكرة المتوفرة لديه يمكنها الاحتفاظ بكل العمليات التي تمت عليها من قبل المستخدم، هذا ما يساعد الخبير في اكتشاف الدليل ويجعل دوره قوي في إثبات الجرائم الإلكترونية.[2]

- **برامج التتبع:**

تقوم هذه البرامج بالتعرف على محاولات الاختراق التي تتم وتقديم بيان شامل بها إلى المستخدم الذي تم اختراق جهازه، إذ يحتوي هذا البيان على اسم الحدث وتاريخ حدوثه وعنوان بروتوكول الإنترنت الذي تمت من خلاله عملية الاختراق، وكذا اسم الشركة المزودة لخدمة الإنترنت، [3] ولعل من أهم هذه البرامج يوجد برنامج (Trace Route) الذي يعتبر ذا أهمية بالغة في الكشف الجنائي، إذ يحدد بدقة متناهية الأجهزة الإلكترونية التي اشتركت في نقل البيانات على الإنترنت بتحديد مسارها وصولا إلى المرسل إليه، كما يستطيع أن يستدعي ويحيط بجميع الملفات التي تم الولوج إليها وكافة عمليات الاختراق والتجاوز التي تحدث أثناء تنفيذ الجريمة، والمعلومات المتعلقة بدخول الأشخاص المستخدمين لمواقع معينة وتحديد مسارات تنقلاتهم فيها إلى غاية خروجهم منها، فهو بهذا يستطيع جمع كل الأدلة الرقمية التي تساعد في الاستدلال على الجريمة.[4]

إلى جانب هذا نجد برنامج كشف الاختراق الذي يرمز له بالرمز (IDS)[5] يتولى مراقبة بعض العمليات التي يتم القيام بها على الأجهزة الإلكترونية المرتبطة بشبكة الإنترنت، وتسجيلها فور وقوعها في سجلات خاصة داخل هذه الأجهزة، ليقوم فيما بعد بمقارنتها بمجموعة من الصفات المشتركة للاعتداءات الحاسوبية والإلكترونية، وفي حال اكتشف النظام وجود أحد هذه الصفات يقوم بإنذار مدير النظام بشكل فوري.[6]

1رفاه خضير جياد العارضي، الدليل الإلكتروني وأثره في مجال نظرية الإثبات الجنائي، المرجع السابق، ص 176.

2خالد ممدوح ابراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص 305.

3المرجع نفسه، ص 306.

4جمال براهيمي، التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص 79.

5كلمة (IDS) هي عبارة عن اختصار لكلمة Intrusion Detectionأي نظام كشف الاختراق.

6كما يعتبر من برامج التتبع أيضا برنامج Hack Tracerوهو عبارة عن برنامج يتكون من شاشة رئيسية تقدم للمستخدم بيان شامل بعمليات الاختراق التي تعرض لها جهازه، يحتوي على اسم وتاريخ الواقعة وعنوان IPالذي تمت من خلاله، واسم الدولة التي تمت منها محاولة الاختراق

- **برامج مراجعة العمليات الحاسوبية واسترجاعها (Auditing Tools)**

وهي عبارة عن برامج تستعمل لمراقبة مختلف العمليات التي يجريها المستخدم على ملفات وأنظمة تشغيل الحاسب، والقيام بتسجيلها في ملفات تسمى (Logs) واسترجاع هذه الملفات في حالة محوها أو حذفها، ومن أمثلتها برنامج (Event Viewer) لبيئة النوافذ، وبرنامج (Syslogd) لبيئة يونيكس، وبرنامج (Recover)، وقد تأتي هذه البرامج مضمنة في أنظمة التشغيل أو كبرامج مستقلة تم تركيبها على أنظمة التشغيل، وفي كلتا الحالتين لابد من تفعيلها قبل العمل بها وذلك قبل وقوع الجريمة الإلكترونية حتى تتمكن من تسجيل كل المعلومات المتعلقة بها.[1]

- **برنامج الدمج وفك الدمج (PKZIP)**

تقوم هذه البرامج بفك البرامج التي قام المجرم الإلكتروني بدمجها قصد التعرف على طبيعة البيانات التي تحتويها وتحليلها، حيث يستعمل المجرم هذه البرامج لإخفاء معلومات معينة لا يمكن الاطلاع عليها إلا بعد فك الدمج.[2]

- **الذكاء الاصطناعي**

ويقصد بالذكاء الاصطناعي مجموعة التقنيات والبرامج الحاسوبية التي يستعين بها الخبير أو المحقق بصفة عامة لحصر الحقائق والاحتمالات والأسباب والفرضيات المتعلقة بالجريمة، وجمع الأدلة الجنائية والقيام بتحليلها واستخلاص الحقائق منها، [3] عن طريق عمليات ومعاملات حسابية يتم حلها بواسطة برامج مصممة لذلك موجودة بالحاسب الآلي، كبرنامج (XtreeProgold) الذي يستخدم للعثور على الملفات المبحوث عنها في أي مكان على الشبكة أو الأقراص الصلبة أو المرنة...وغيرها، ويقوم بقراءة محتوياتها الأصلية من أجل تحليلها والتوصل بذلك إلى الأدلة التي تثبت الجريمة.[4]

وعليه وبعد استخراج واسترجاع الخبير للمعلومات المطلوبة وتجميعه لمجموعة من المواقع التي تشكل جريمة أو ساعدت على ارتكابها، يقوم بتحليل رقمي لها عن طريق فحصها بدقة لمعرفة كيفية

وحتى اسم الشركة والشبكة المزودة لخدمة الإنترنت، وبيانات هذه الأخيرة من أرقام وهواتف وغيرها من المعلومات الخاصة بها، لمزيد من التفاصيل ينظر خالد ممدوح إبراهيم، الإثبات الإلكتروني في المواد الجنائية والمدنية، المرجع السابق، ص 204.

1جمال براهيمي، التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص 80.

2نعيم سعيداني، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، المرجع السابق، ص 173.

3خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص 206.

4جمال براهيمي، التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص 81.

إعدادها البرمجي ونسبتها إلى مسارها الذي أعدت فيه، ومن ثم التوصل إلى معرفة البروتوكول الخاص بالإنترنت والذي ينسب للجهاز الذي ارتكبت منه الجريمة،[1] وفي هذه المرحلة يجب على الخبير الالتزام بالتحفظ على الأدلة المتوصل إليها إذ تتم عملية حفظ الدليل داخل جهاز الحاسب الآلي بعدة أساليب، تتمثل في أبسط مظاهرها باستخدام أسلوب الحفظ العادي، وأقوى مظاهرها في عمليات حجز الحاسوب على الدليل الموضوع فيه، ذلك أن الدليل الإلكتروني يحتوي في العادة على بيانات رقمية غير قابلة للتحويل إلا في حالة القيام بإجراء تعديلات رقمية عليها،[2] كما أن وجود مجالات كهرومغناطيسية أو أجهزة ارسال يؤثر على البيانات المستمدة من الدليل إذ قد تحدث تغيرات في طبيعتها مما يتسبب في اتلافها، فضلا عن نقص الخبرة لدى بعض العاملين في الأجهزة الأمنية والخبراء، مثل ما حدث في واقعة إذ بلغت إحدى الشركات عن وجود قنبلة منطقية بنظام حاسبها الآلي، وعند التحقيق في الأمر تبين أن الشركة وقبل إبلاغ السلطات المختصة كانت قد استدعت خبيرا للتحقق من صحة الخبر، وبالفعل استطاع الخبير اكتشاف القنبلة وإزالتها من البرنامج الموضوعة فيه، لكن اتضح عند وصول مصالح الشرطة أنه تم اتلاف كل الأدلة الدالة على وجود الجريمة،[3] لهذا يجب على الخبير أن يكون حريصا في تعامله مع الدليل الإلكتروني وعلى قدر من المعرفة الفنية والتخصص في مجال البرمجيات والتكنولوجيات الحديثة.

وأخيرا يعد الخبير تقرير الخبرة مع تضمينه جميع خطوات وإجراءات البحث والفحص التي قام بها، مرفقا بالملاحق الإيضاحية مثل الصور والتسجيلات وغيرها، ليقوم في الأخير بتسليمه لجهة التحقيق أو الحكم التي طلبت إجراء الخبرة.

المطلب الثاني: الاستعانة بالشهادة الإلكترونية

تعد الشهادة من أهم وسائل الإثبات في جميع الجرائم، كونها عاملا حاسما يمكن تقديمه للقضاء، وهي لا تقل أهمية في الجرائم الإلكترونية عنها في الجرائم التقليدية، وإن كانت لا تختلف من حيث كيفية الاستعانة بها أو نظام أدائها أو أثرها بين الجرائم التقليدية والإلكترونية، إلا أنها تثير بعض الإشكالات أو التساؤلات خاصة ما يتعلق منها بمدى التزام الشاهد المعلوماتي بها؟ ومدى إمكانية الإدلاء بها عبر الوسائل الإلكترونية؟

1يزيد بوحليط، الجرائم الإلكترونية والوقاية منها، المرجع السابق، ص 336.

2ليندا بن طالب، الدليل الإلكتروني ودوره في الإثبات الجنائي، المرجع السابق، ص 85.

3خضرة شنتير، الآليات القانونية لمكافحة الجريمة الإلكترونية، المرجع السابق، ص 110.

الفرع الأول: مفهوم الشهادة الإلكترونية

سنحاول التطرق في هذا الفرع للمقصود بالشهادة الإلكترونية وتمييزها عن نظيرتها التقليدية، وكذا المقصود بالشاهد المعلوماتي والفئات التي تندرج تحت هذه الصفة.

أولا: تعريف الشهادة الإلكترونية

تعرف الشهادة على أنها إثبات حقيقة واقعة معينة، علم بها الشاهد من خلال ما شاهده أو سمعه أو أدركه بإحدى حواسه، كما يعرفها البعض على أنها: "الأقوال التي يدلي بها غير الخصوم أمام سلطة التحقيق أو القضاء بشأن جريمة وقعت سواء كانت تتعلق بثبوت الجريمة وظروف ارتكابها وإسنادها إلى المتهم أو براءته منها"،[1] وبهذا تعد الشهادة وسيلة إثبات أساسية في المسائل الجزائية، لأنها تنصب في الغالب على وقائع مادية تقع بشكل مفاجئ يتعذر إثباتها إلا عن طريق الشهادة، فغالبا ما يكون للشهادة وخاصة التي يدلي بها فور وقوع الحادث أو الجريمة أثرا كبيرا في الحكم بالإدانة أو البراءة.

وعليه للشهادة بصفة عامة أهمية بالغة في مجال الإثبات الجنائي باعتبارها أهم طرق الإثبات، حيث لا تقل أهميتها في مجال إثبات الجرائم الإلكترونية عنه في مجال الجرائم التقليدية كون أن الشاهد في كلتا الجريمتين يلتزم بالإدلاء بما يعلمه من معلومات بخصوص واقعة الجريمة والفاعلين فيها، بما يفيد في كشف الحقيقة، ولهذا قد عنيت جل التشريعات بتنظيم أحكام الشهادة وإحاطتها بضمانات عديدة،[2] من بينها المشرع المصري الذي نظمها في المواد 110إلى 122من ق ا ج م،[3] كما قام المشرع الجزائري بتنظيم أحكام الشهادة في القسم الرابع من الفصل الأول من الباب الثالث تحت عنوان: "سماع الشهود"في المواد من 88إلى 99من ق ا ج ج والتي تتلخص حول استدعاء الشهود وحضورهم وكيفية تلقي إفاداتهم وحلف اليمين...الخ.[4]

وأما عن الشهادة الإلكترونية أو ما يصطلح عليها بالشهادة عن بعد، فهي الشهادة التي لا يكون فيها الشاهد حاضرا جلسة التحقيق بشخصه، وإنما تتم عبر وسائل إلكترونية ورقمية متطورة، وقد كانت بداية الأخذ بنظام الشهادة الإلكترونية عن بعد في القضاء الأمريكي عندما واجه مشكلة إدلاء الشهادة من

1عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في الإثبات الجنائي، المرجع السابق، ص 77.

2رشيدة بوكر، الحماية الجزائية للتعاملات الإلكترونية، المرجع السابق، ص 364.

3إذ تنص المادة 112من ق ا ج م على : "يسمع القاضي كل شاهد على انفراد وله أن يواجه الشهود بعضهم ببعض وبالمتهم".

4ينظر المواد من 88إلى المادة 99من ق ا ج ج.

قبل أشخاص وضعوا في برنامج حماية الشهود، إذ قررت المحكمة الفيدرالية العليا آن ذاك قبول شهادتهم عبر وسائل التواصل عن بعد، طالما كانت هناك أسباب في القانون تدعو إليها، كما تم العمل بهذا النظام في قضية أخرى استلزمت إدلاء شخص محصن بسماع شهادته عبر دوائر تلفزيونية مغلقة[1] شريطة أن يكون حضور الشاهد عبر هاته الدوائر كما لو كان حاضرا بشخصه للجلسة، [2] وقد ميز القضاء الأمريكي والفقه الجنائي بين نوعين من الشهادة الإلكترونية أو الشهادة عن بعد: **الشهادة المرئية ذات الاتجاه الواحد** حيث أن الشاهد في هذه الحالة يدلي بشهادته بطريقة مرئية تخول أعضاء المحكمة رؤيته في حين لا يستطيع هو رؤيتهم، [3] إذ نجد أن هذا النوع من الشهادة رغم وجوده إلا أنه ينقص من القيمة القانونية للشهادة والتي تعتمد على أسلوب المواجهة.

أما عن النوع الثاني فيصطلح عليه الشهادة المرئية ذات الاتجاهين: وفي هذا النوع من الشهادة يرى الشاهد قاعة المحكمة ومن فيها كما يتمكن من بالمحكمة من قضاة وغيرهم من رؤيته، [4]

وبطبيعة الحال لا تقتصر الشهادة الرقمية أو الإلكترونية على الجرائم الإلكترونية فقط، فهي وسيلة لإثبات مختلف أنواع الجرائم خصوصا تلك الجرائم الخطيرة و العابرة للحدود، لذلك فان إتاحة هذا النوع من الشهادة لمثل هذه الجرائم أمر ضروري، وهو ما جسده المشرع الجزائري في إطار قانون عصرنة العدالة رقم 15/03[5]، من أجل إرساء مفهوم المحاكمة الإلكترونية أو التقاضي عن بعد، حيث نصت المادة 15منه على أنه يمكن لقاضي التحقيق أن يستعمل المحادثة المرئية عن بعد في استجواب أو سماع شخص وفي إجراء مواجهات بين عدة أشخاص، كما يمكن أيضا أن تستعمل المحادثات المرئية عن بعد لسماع الشهود والأطراف المدنية والخبراء.

كما أتاحت بعض الدول خدمة رقمية يستطيع الشاهد من خلالها تقديم شهادته عن طريق ملأ إستمارة رقمية متاحة على الموقع الخاص بمديرية الأمن الوطني مما يساعد على تشجع الشاهد والإقدام على الإدلاء بأقواله دون خوف من المتهم أو غيره، ورغم أن هذه الطريقة تعتبر من الطرق العملية والتي توفر

1يقصد بالدوائر المغلقة مجموعة دوائر اتصال تكون مغلقة بين اتجاهين فأكثر يتم تحديدها مسبقا بحيث لا يستطيع الغير الدخول عليها، إذ توفر بذلك نوع من الحماية والخصوصية.

2خالد ممدوح ابراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص 262.

3رشيدة بوكر، الحماية الجزائية للتعاملات الإلكترونية، المرجع السابق، ص 371.

4المرجع نفسه، ص 372.

5القانون رقم 15/03مؤرخ في 11ربيع الثاني عام 1436الموافق لأول نوفمبر 2015، يتعلق بعصرنة العدالة، ج ر ج ج عدد 06، الصادرة بتاريخ 10فبراير 2015.

حماية كبيرة لشخص الشاهد إلا أننا نرى أنها ليست من الطرق الموثوقة في إثبات الجرائم بصفة عامة، كونها قد تكون هذه الشهادة كاذبة أو تظليلية أو كيدية.[1]

ثانيا: تعريف الشاهد الإلكتروني

الشاهد هو ذلك الشخص الذي يقرر أمام القضاء أو سلطة التحقيق ما يكون قد سمعه أو رآه أو أدركه بإحدى حواسه، [2]أما الشاهد في الجريمة الإلكترونية فيقصد به ذلك الشخص الفني صاحب الخبرة والتخصص في مجال تقنية المعلومات، والذي يكون لديه معلومات جوهرية عن نظم التشغيل أو عمل الأجهزة الإلكترونية محل الجريمة، أو كان يتوفر على معلومات عن المجرم الإلكتروني أو شاهده وهو يقوم بالجريمة، وعليه فإن كانت شهادة الشهود تقبل من أي شخص بأي مستوى علمي أو اجتماعي، فهي ليست كذلك في جرائم الإنترنت أو الجرائم الإلكترونية، وهذا راجع لاختلاف مسرح هذه الجريمة وطبيعتها، وكذا الدليل الناتج عنها، الأمر الذي يؤدي إلى اختلاف فئات الشهود فيها وكذا اختلاف طرق أدائها، [3]وعليه يعتبر شاهد معلوماتي كل من:

- **القائم على تشغيل النظام:** وهو ذلك الشخص المسئول عن تشغيل الجهاز ومعداته والملحقات المتصلة به، حيث يتمتع هذا الأخير بالخبرة الفنية والتقنية في مجال التعامل مع الأجهزة الإلكترونية.[4]
- **خبراء البرمجة:** وهم الأشخاص المتخصصين في كتابة أوامر البرامج الخاصة بالحاسب الآلي، وهم فئتين: مخططو البرامج التطبيقية ومخططو برامج النظم، بحيث يقوم مخططو برامج التطبيقات بالحصول على خصائص ومواصفات النظام المطلوب من محلل النظم، ومن ثم تحويلها إلى برامج دقيقة وموثقة لتحقيق هذه المواصفات، [5] أما مخططو برامج النظم فيقومون باختبار وتعديل وتصحيح برامج نظام الحاسب الآلي الداخلية، أي أنهم يقومون بالوظائف الخاصة بتجهيز الحاسب بالبرامج والأجزاء الداخلية التي تتحكم في وحدات الإدخال والإخراج ووسائط التخزين.[6]
- **المحلل:** وهو الشخص الذي يقوم بتجميع بيانات ومعطيات النظام، ودراستها ثم تحليل النظام وتقسيمه إلى وحدات منفصلة، ومن ثم استنتاج العلاقات الوظيفة بين هذه الوحدات، كما يقوم بتتبع

[1] ينظر الملحق رقم 06.

2أحمد فتحي سرور، الوسيط في شرح قانون الإجراءات الجنائية، ج1، ب ط، مطبعة القاهرة، مصر، 1979، ص 498.

3دلال ملياني مولاي، إشكالية الإثبات في جرائم الإنترنت في التشريع الجزائري، المرجع السابق، ص 137.

4المرجع نفسه، ص 139.

5حسين ربيعي، آليات البحث والتحقيق في الجرائم المعلوماتية، المرجع السابق، ص 256.

6عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في الإثبات الجنائي، المرجع السابق، ص 79.

البيانات داخل النظام عن طريق ما يسمى بمخطط تدفق البيانات واستنتاج الأماكن التي يمكن ميكنتها بواسطة هذا النظام.[1]

- **مهندسو الصيانة والاتصالات:** وهم الأشخاص المسئولون عن أعمال الصيانة الخاصة بتقنيات الحاسب ومكوناته وشبكاته الاتصالية.[2].
- **مدير النظام:** وهو الشخص الذي توكل إليه مهمة إدارة النظام المعلوماتي.[3]

إضافة إلى هذه الفئات هناك بعض الأشخاص الذين يعدون بمثابة شهود في الجريمة الإلكترونية، ويعتبر دورهم مهم كثيرا في مجال إثبات هذا النوع من الجرائم، وقد تم الاشارة إليهم سابقا لعل من بينهم نجد، مقدمو الخدمات الوسيطة في مجال المعلوماتية والإنترنت، متعهدو الوصول والإيواء، وكذا المنتج وناقل المعلومات ، مسئول متعهد الخدمات...الخ.[4]

استنادا إلى ما سبق يمكن القول أن الشاهد المعلوماتي كما قد يكون أحد هذه الفئات السابقة كأن يكون أحد العاملين في إحدى الشركات التي تكلف عامليها بإرسال رسائل إلكترونية إلى الزبائن مثلا، يمكنه أن يكون أيضا شخص عادي عاين الجريمة، فإننا نرى أنه ليس من الضروري أن يكون الشاهد دائما ملم بجميع جوانب المعلوماتية وما يتعلق بها، فقد يكون شخص عادي شاهد الجريمة، كأن يكون مثلا صاحب مقهى الإنترنت أو ممن يرتادون هذا المقهى، فالشاهد العادي يلعب دور مهم ومكمل في عملية إثبات الجريمة الإلكترونية عندما يتعلق الأمر بالنشاط المادي الذي يرتكبه المجرم المعلوماتي في العالم المادي أو على الأجهزة الإلكترونية وملحقاتها.

الفرع الثاني: التزامات الشاهد الإلكتروني

تجدر الإشارة إلى أن هناك اختلافا واضحا بين الشاهد العادي أو التقليدي و الشاهد المعلوماتي، ففي الجرائم العادية كل شخص تنطبق عليه شروط أداء الشهادة هو أهل لها، في حين أن الشاهد في جرائم الإنترنت لابد أن يلتزم ببعض الضوابط الفنية التي تحكم الشهادة في هذا النوع من الجرائم، ودون الإخلال بالأحكام والشروط المنصوص عليها في القوانين الإجرائية، إذ يقع على عاتق الشاهد واجب التعاون

1رشيدة بوكر، الحماية الجزائية للتعاملات الإلكترونية، المرجع السابق، ص 365.

2فيروز عوض الكريم صالح ميرغني، إجراءات التحري والضبط في الجريمة الإلكترونية، المرجع السابق، ص 113.

3عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في الإثبات الجنائي، المرجع السابق، ص 79.

4رشيدة بوكر، الحماية الجزائية للتعاملات الإلكترونية، المرجع السابق، ص 366.

مع السلطات القضائية بإعلامها بكل ما وصل إلى علمه حول ارتكاب جريمة معينة. فما مدى التزام الشاهد المعلوماتي بتقديم كل ما لديه من معلومات بخصوص هذه الجرائم؟

أولا: حضور الشاهد أمام الجهة التي استدعته وحلف اليمين

مضمون هذا الالتزام حضور الشاهد بنفسه في المكان والوقت المحددين للاستماع إلى شهادته، [1] والذي يكون بناء على التكليف بالحضور عن طريق أحد المحضرين القضائيين أو رجال الضبط القضائي، فبالرجوع للمشرع الجزائري وتحديدا للمادة 97من ق ا ج ج نجده يلزم كل شخص استدعى لسماع شهادته بالحضور للجلسة، وفي حالة تخلفه عن ذلك يجوز لقاضي التحقيق بناء على طلب وكيل الجمهورية استحضاره جبرا بواسطة القوة العمومية والحكم عليه بغرامة من 200دج إلى 2000دج، غير أنه إذا حضر فيما بعد وأبدى أعذارا مقبولة جاز لقاضي التحقيق إعفائه من الغرامة كلها أو جزء منها.[2] وهو ما نص عليه المشرع الفرنسي في المادة 101من ق ا ج ف، [3] وكذا المشرع المصري في المادة 117من ق ا ج المصري[4] التي تلزم الشاهد الحضور متى تم استدعائه وإلا جاز تغريمه أو إصدار أمر بضبطه وإحضاره، كما يجب عليه الإدلاء بكل المعلومات التي يعرفها وفي حالة امتناعه عن ذلك يجوز للقاضي الحكم عليه بالغرامة في حالة الجنايات والجنح، كما يمكن إعفائه من بعض العقوبة أو كلها إذا عدل عن امتناعه.[5]

1رشيدة بوكر، الحماية الجزائية للتعاملات الإلكترونية، المرجع السابق ، ص 367.

2حيث تنص المادة 97من ق ا ج ج على:"كل شخص استدعي لسماع شهادته ملزم بالحضور وحلف اليمين وأداء الشهادة مع مراعاة الأحكام القانونية المتعلقة بسر المهنة".

3Article n° 101 Modifié par loi n°2000- 516 du 15 juin 2000 – art.31 JORF 16 juin 2000 en vigueur le 1er janvier 2001 : «…Les témoins peuvent aussi être convoqués par lettre simple, par lettre recommandée ou par la voie administrative ; ils peuvent en outre comparaitre volontairement.
Lorsqu'il est cité ou convoqué, le témoin est avisé que, s'il ne comparait pas ou s'il refuse de comparaitre, il pourra y être contraint par la force publique en application des dispositions de l'article 109. »

كما يعاقب الامتناع عن الإدلاء بما يعرفه والإجابة على ما يطرح عليه من أسئلة، طبقا للمواد 109و113من ق ا ج ج ف، وتضاعف العقوبة في حالة ما إذا كان الشاهد على علم بالجناة ورفض الإجابة على الأسئلة.

4تنص المادة 117من ق ا ج م على: "يجب على كل من دعي للحضور أمام قاضي التحقيق لتأدية شهادة أن يحضر بناء على الطلب المحرر إليه وإلا جاز للقاضي الحكم عليه بعد سماع أقوال النيابة العامة بدفع غرامة لا تجاوز خمسين جنيها ويجوز له أن يصدر أمرا بتكليفه بالحضور ثانيا بمصاريف من طرفه أو أن يصدر أمرا بضبطه وإحضاره".

5حسام نبيل محمد الشنراقي، الجرائم المعلوماتية، جرائم الاعتداء على التوقيع الإلكتروني، المرجع السابق، ص 418.

وفي حالة ما إذا قدم الشاهد أعذارا مقبولة عن عدم إمكانية حضوره فللمحكمة الانتقال إليه وسماع شهادته بعد إخطار النيابة العامة وباقي الخصوم، والذين لهم الحق في الحضور بأنفسهم أو بواسطة وكلائهم، وتوجيه الأسئلة إلى الشاهد طبقا لنص المادة 281من ق ا ج م، [1] والمادة 99من ق ا ج ج، [2] والمادة 112من ق ا ج ف.[3]

إلا أنه بعد ظهور الوسائل التقنية المتطورة وتفاديا لتنقل الشهود لمقر الشرطة القضائية أو المحاكم والمجالس القضائية، ظهر ما يسمى بالشهادة الإلكترونية وأصبحت أغلب الدول تعتمد هذه التقنية في سماع الشهود، حيث تضمن هذه الأخيرة حضور الشاهد للجلسة والإدلاء بشهادته دون أعذار، هذا من جهة، ومن جهة ثانية توفر له نوع من الحماية القانونية، إذ لا يفوتنا أن ننوه أنه تعزيزا لدور الشاهد في مسار الإجراءات والتحريات القضائية أقرت القوانين الإجرائية نوع من الحماية القانونية والإجرائية لمنع أي تهديد أو مساس بحياة الشاهد أو سلامته أو سلامة أحد أفراده أو أي مصلحة أساسية، وذلك بإخفاء هويته وكل المعلومات المتعلقة به، وكذا وضع أجهزة تقنية وقائية لمراقبته، وقد كان القانون الأمريكي أولى التشريعات بحماية الشهود من خلال الفصل الخامس من قانون الرقابة على الجريمة المنظمة الصادر في 1970، كما أدخل المشرع الفرنسي نصوصا خاصة تحمي الشاهد بمقتضى قانون الأمن اليومي 2001-1062المعدل لقانون الإجراءات الجزائية، وذلك من المواد 706-57إلى 706-63منه، [4] وكذلك فعل المشرع الجزائري حين أصدر الأمر رقم 15/02المعدل والمتمم للأمر 66-155المتضمن ق ا ج ج الذي أضاف بموجبه الفصل السادس من الباب الثاني من الكتاب الأول تحت عنوان "في حماية الشهود والخبراء

1تنص المادة 281من ق ا ج م على: "للمحكمة إذا اعتذر الشاهد بأعذار مقبولة عن عدم إمكانه الحضور أن تنتقل إليه وتسمع شهادته بعد إخطار النيابة العامة وباقي الخصوم، وللخصوم أن يحضروا بأنفسهم أو بواسطة وكلائهم، وأن يوجهوا للشاهد الأسئلة التي يرون لزوم توجيهها إليه".

2تنص المادة 99من ق ا ج ج على: "إذا تعذر على شاهد الحضور انتقل إليه قاضي التحقيق لسماع شهادته أو اتخذ لهذا الغرض طريق الإنابة القضائية فإذا تحقق من أن شاهدا قد ادعى كذبا عدم استطاعته الحضور جاز له أن يتخذ ضده الإجراءات القانونية طبقا لأحكام المادة 97".

3Article n° 112 dispose que : « Si un témoin est dans l'impossibilité de comparaitre, le juge d'instruction se transporte pour l'entendre, ou délivre à cette fin commission rogatoire dans les formes prévues à l'article 151 ».

كما تجدر الإشارة إلى ضرورة مراعاة الشاهد لواجب التحفظ على السر المهني كما أشرنا سابقا، إذ قد يستثنى من فئة الشهود بعض الطوائف التي تختلف من تشريع لآخر، ففي التشريع الفرنسي مثلا تنص المادة 378من ق ع ف على أنه يمنع من أداء الشهادة موظفي الدولة بشأن المعلومات التي يتحصلون عليها بحكم وظيفتهم، وكذا المحامين والأطباء، وهو ما جاء في كل من التشريعين الجزائري والمصري إذ يمنع كل من المحامين والأطباء وموظفي الدولة، والأزواج وبعض الأقارب، كأصول وفروع المتهم عن الشهادة ضده طبقا لما جاءت به المادة 286ق ا ج م.

4رشيدة بوكر، الحماية الجزائية للتعاملات الإلكترونية، المرجع السابق، ص 373- 374.

والضحايا "في المواد من 65مكرر 19إلى المادة 65مكرر 28منه، [1]إذ تعتبر هذه التدابير كلها إجراءات تحفيزية تعزز دور الشاهد في الكشف عن ملابسات القضية، وإن كانت لا تختلف بين الشاهد العادي والشاهد المعلوماتي، بل تعد الشهادة الإلكترونية أو ما يسمى بالشهادة عن بعد إحدى طرق الحماية التي يسمع بها الشاهد تفاديا لإظهار هويته أو تواجده بمقر المحكمة شخصيا.

إذن بعد حضور الشاهد أمام الجهة التي استدعته يصبح أمام التزام حلف اليمين القانونية، إذ يعد هذا الالتزام ضمانة تضفي الثقة على الشهادة لكي تكون دليلا يستمد منه القاضي اقتناعه، وقد نص على هذا الالتزام المشرع الجزائري في المادة 97و222من ق ا ج ج، كما نص عليه المشرع المصري في المادة 283من ق ا ج م، [2] غير أنه طبقا للمادة 29 /2من ق ا ج م فإن حلف الشاهد لليمين القانونية يعتبر إجراء وجوبي في مرحلة التحقيق دون مرحلة جمع الاستدلالات، إذ يبقى أمر تحليفه اليمين في هذه المرحلة أمر اختياري يعود لتقدير رجال الضبط القضائي، كما لا يحلف الشاهد القاصر اليمين عند أداء شهادته والتي تكون على سبيل الاستدلال فقط.

أما عن صيغة اليمين فقد حددها المشرع كل حسب تشريعه، إذ تؤدى في التشريع الجزائري طبقا للمادة 93/2من ق ا ج ج[3] وبعد رفع الشاهد ليده اليمنى بالصيغة التالية: "أحلف بالله العظيم أن أتكلم بغير حقد ولا خوف وأن أقول كل الحق ولا شيء غير الحق"، ومن جهته حدد المشرع المصري صيغة اليمين في المادة 283من ق ا ج م[4] إلا أنها تبقى غير إلزامية إذ يكفي حلف الشاهد بأن يشهد بالحق فقط، وعلى غرار ذلك أقر المشرع الفرنسي من جهته صيغة معينة لليمين وإن كانت تختلف باختلاف المحاكم إلا أنها تفيد كلها الوعد بقول الحقيقة وذلك في المواد 103- 446- 536من ق ا ج ف، كما أنه ليس من الضروري ذكر صيغة اليمين بأكملها في المحضر إلا أنه لابد من أن يثبت المحقق أو القاضي حلف الشاهد لليمين في المحضر وإلا ترتب على ذلك البطلان طبقا لكل من التشريعين الجزائري والفرنسي.[5]

1لمزيد من التفاصيل حول حماية الشهود والخبراء يراجع الفصل السادس من الباب الثاني من الكتاب الأول من الأمر رقم 15/02الصادر في 23جويلية 2015المعدل والمتمم لقانون الإجراءات الجزائية الجزائري، المواد من 65مكرر 19إلى 65مكرر 28منه، والتي تضمنت مجموعة من الإجراءات لحماية الشهود والخبراء والضحايا.

2تنص المادة 283من ق ا ج م على : "يجب على الشهود الذين بلغت سنهم أربع عشرة سنة أن يحلفوا يمينا قبل أداء الشهادة على أنهم يشهدون بالحق ولا يقولون إلا الحق، ويجوز سماع الشهود الذين لم يبلغوا أربع عشرة سنة كاملة بدون حلف يمين على سبيل الاستدلال".

3ينظر المادة 93فقرة 2من ق ا ج ج.

4ينظر المادة 283من ق ا ج م.

5رشيدة بوكر، الحماية الجزائية للتعاملات الإلكترونية، المرجع السابق، ص 368.

ثانيا: الإدلاء بالشهادة

في حالة حضور الشاهد وحلف اليمين وجب عليه أداء الشهادة، والتي تتضمن الحقيقة التي تعبر عن الواقعة أو الجريمة التي رآها أو أدركها بحواسه، فهو ملزم بقول الحقيقة وإلا اعتبرت شهادته شهادة زور ورد النص على العقاب عليها في المادة 332من ق ع ج، والمواد من 294إلى 298من ق ع المصري، وبالتالي يتعين على الشاهد بصفة عامة أن يلتزم بتقديم المعلومات التي تفيد في إظهار الحقيقة، ومن ثم يصبح الشاهد المعلوماتي ملزم بتقديم المعلومات اللازمة لإختراق النظم المعلوماتية بحثا عن أدلة الجريمة، وهذا ما يصطلح عليه "بالالتزام بالإعلام في الجرائم الإلكترونية "أي أن يقدم الشاهد المعلوماتي لسلطات التحري والتحقيق ما يحوزه من معلومات جوهرية لازمة لاختراق نظام المعالجة الآلية للبيانات بحثا عن أدلة الجريمة التي تتطلبها مصلحة التحقيق، [1] فيكون بذلك الشاهد مطالبا بأن يعلم بها سلطات التحقيق و التحري على سبيل الإلزام، فهل يعرض هذا الإلزام الشاهد للجزاءات في حالة عدم تأديته له، وفيما يتمثل هذا الالتزام؟ للإجابة عن هذا التساؤل اختلف الفقه المقارن بين مؤيد ومعارض حيث انقسم إلى قسمين:

1) الاتجاه الأول : يرى هذا الاتجاه أنه ليس من التزامات الشاهد المعلوماتي الإفشاء بما لديه من معلومات أو الإفصاح عن كلمات المرور، لأن شهادته تنصب على معرفة قائمة لديه بالفعل، ولاتشمل تقديم معلومات جديدة، كما أن هذا البحث يدخل في اختصاص الخبير القضائي وليس الشاهد، وهذا ما جسده كل من الفقه والتشريع الألماني حيث يرى عدم التزام الشاهد بطبع البيانات المخزنة في ذاكرة الحاسوب على أساس أن الالتزام بإدلاء الشهادة لا يتضمن هذا الواجب، وهو ما جسده التشريع التركي، [2]

2) الاتجاه الثاني :يرى أنصار هذا الاتجاه أن إفشاء كلمات السر و الإفصاح عنها لسلطات التحقيق هو التزام قانوني يتحمله الشاهد، خاصة وأن المؤتمر الدولي الخامس عشر للجمعية العامة لقانون العقوبات والذي عقد في ريودي جانيرو بالبرازيل في الفترة من (4 -9) سبتمبر، أوصى بواجب التعاون الفعال من جانب المجني عليهم والشهود وغيرهم من مستخدمي تكنولوجيات المعلومات، [3] إضافة إلى بعض التشريعات التي فرضت هذا الواجب على الشاهد في مجال الجرائم الإلكترونية، من بينها القانون الإنجليزي الصادر عام 1984بشأن البوليس والأدلة الجنائية، حيث يمكن المحقق من تكليف

1يزيد بوحليط، الجرائم الإلكترونية والوقاية منها، المرجع السابق، ص 345.

2رشيدة بوكر، الحماية الجزائية للتعاملات الإلكترونية، المرجع السابق، ص 366.

3عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في الاثبات، المرجع السابق، ص 79.

الغير من الدخول إلى المعلومات المخزنة في الحاسب الآلي أو الاطلاع عليها، [1] وكذا قانون الحاسب الآلي في هولندا الذي يتيح لسلطات التحري والتحقيق إصدار الأمر للقائم بتشغيل النظام المعلوماتي بتقديم المعلومات اللازمة لاختراقه أو الولوج إليه، والإفصاح عن الكلمات السرية وحل الشفرات الخاصة بتشغيل البرامج المختلفة.

كما يؤيد هذا الاتجاه بعض الفقهاء في فرنسا على أساس أن المشرع الفرنسي طالما لم ينظم هذه المسألة فإنه لا مناص من تطبيق القواعد العامة للشهادة، وبالتالي يلتزم الشهود بالكشف عن كلمات المرور السرية التي يعرفونها وشفرات تشغيل البرامج، [2] إذ يتعرضون لعقوبات جنائية في حالة رفض إعطاء كلمات السر التي يعلمونها وهذا في مرحلتي التحقيق والمحاكمة طبقا للمواد(109-138).[3]

وهذا ما أكدته اتفاقية بودابست في المادة التاسعة عشر في فقرتها الرابعة من خلال إلزام كل طرف تبني الإجراءات التشريعية وأية إجراءات أخرى يرى أنها ضرورية من أجل تخويل سلطاته المختصة سلطة إصدار الأمر لأي شخص لديه معلومات عن تشغيل النظام أو الإجراءات المطبقة من أجل حماية المعطيات التي تتضمن تقديم كل المعلومات الضرورية على نحو معقول يسمح بتطبيق الإجراءات القضائية اللازمة، وبهذا فهي تلزم مديري النظم بالتعاون مع السلطات القضائية وتقديم المعلومات التي من شأنها تسريع وتسهيل إجراءات التفتيش والضبط، وهذا ما ذهب إليه المشرع الجزائري في المادة 5من القانون رقم 09/04المشار إليه سابقا، هذا من جهة.

ومن جهة أخرى فقد جعل المشرع الجزائري كل من مزود خدمات الانترنيت من فئة الشهود الذين يقع على عاتقهم الالتزام بالإعلام في الجرائم الإلكترونية، طبقا لنص المادة 10من القانون رقم (09-04) وفي حالة الإخلال بهذا الالتزام يعتبر مزود الخدمات مرتكب لجريمة عرقلة حسن سير التحريات القضائية ويعاقب بالعقوبات المنصوص عليها في الفقرة الأخيرة من المادة 11من ذات القانون.

ثالثا: شروط الالتزام بالإعلام في الجر ائم الإلكترونية

لينشأ التزام الشاهد المعلوماتي بالإعلام في الجرائم الإلكترونية لابد من توافر شروط معينة حيث يعرضه الإخلال بها للمسائلة الجزائية، تتمثل هاته الشروط فيما يلي:

1 المرجع نفسه، ص 80.

2 المرجع نفسه، ص 81.

3عبد الفتاح بيومي حجازى، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت، المرجع السابق، ص 350.

1) أن نكون بصدد جناية أو جنحة من جرائم الإنترنت واقعة بالفعل وليست متوقعة الحدوث، لأن الإعلام يأتي مباشرة بعد العلم بوقوع السلوك الإجرامي.[1]

2) أن يكون الشاهد المعلوماتي على علم ودراية بالمعلومات المتصلة بالنظام المعلوماتي محل الواقعة، والتي تكون تحت سيطرته بالنظر إلى طبيعة نشاطه، كمزود خدمة الانترنت مثلا، أو أعضاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها ، باعتبارهم يمارسون مهام من شأنها أن تجعلهم من فئات الشاهد المعلوماتي السالفة الذكر.

3) أن تتطلب مصلحة التحري والتحقيق الحصول على هذه المعلومات، وخاصة إذا تطلب الأمر اختراق نظام معين باعتبار أن هذا التكليف الذي حدده القانون سوف يأتي في سياق البحث عن الدليل الجنائي الرقمي.[2]

1دلال ملياني مولاي، إشكالية الإثبات في جرائم الإنترنت في التشريع الجزائري، المرجع السابق، ص 146 -147.

2خالد ممدوح براهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص 265.

الفصل الثاني

خصوصية إجراءات البحث والتحري
المستحدثة في الجريمة الإلكترونية

الفصل الثاني: خصوصية إجراءات البحث والتحري المستحدثة في الجريمة الإلكترونية

نتيجة عدم كفاية وفاعلية الإجراءات التقليدية للبحث والتحري في الجرائم الإلكترونية، خاصة وأنها تتسم بالطابع العالمي، فقد اتجهت جهود المجتمع الدولي في تكثيف التعاون القضائي في هذا المجال، حيث تجلت هذه الجهود في عقد العديد من المؤتمرات والاتفاقيات الدولية والإقليمية والتي دعت صراحة إلى ضرورة وجود تعاون دولي في مجال التحري عن الجريمة المعلوماتية والتحقيق فيها، نذكر من بينها معاهدة بودابست لعام 2001بشأن مكافحة جرائم نظم المعلومات والاتصالات، وغيرها من الجهود التي برزت في هذا المجال، أما على المستوى الداخلي فقد استحدثت التشريعات الأجنبية منها والعربية آليات جديدة لمواجهة هذا النوع من الإجرام، إذ قامت بسن نصوص قانونية جديدة وإجراءات خاصة في مجال البحث والتحري عن الجرائم الإلكترونية، وتعديل أخرى بما يتناسب مع طبيعة الدليل الإلكتروني الناتج عنها، ففيما تتمثل هذه الإجراءات، وما مدى تلاؤمها مع خصوصية الجرائم الإلكترونية وفعاليتها في التصدي لها؟

للإجابة عن هذا التساؤل ارتأينا معالجة هذا الفصل من خلال مبحثين رئيسيين: خصصنا الأول لدراسة خصوصية إجراءات البحث والتحري المستحدثة وفقا للقوانين الإجرائية العامة، في حين خصصنا الثاني لدراسة خصوصية إجراءات البحث والتحري المستحدثة وفقا للقوانين الإجرائية الخاصة.

المبحث الأول: خصوصية إجراءات البحث والتحري المستحدثة وفقا للقو انين الإجر ائية العامة

تعتبر إجراءات البحث والتحري المستحدثة مكسبا هاما لسلطات التحقيق في الكشف عن بعض الجرائم من بينها الجرائم الإلكترونية، وكما سبق وذكرنا فإن أغلب تشريعات الدول سارعت لتبني جملة من الإجراءات والآليات المستحدثة ضمن قوانينها الإجرائية العامة، من أجل التصدي الأمثل لهذا النوع من الجرائم، من بينها آلية الترصد الإلكتروني بمختلف صورها كاعتراض المراسلات وتسجيل الأصوات، وكذا إجراء التسرب الإلكتروني داخل البيئة الافتراضية، وفي المقابل أحاطتها بجملة من الضوابط والضمانات التي تكفل عدم تعسف السلطات في استخدامها لهذه الأساليب كونها تشكل مساسا لحرمة الحياة الخاصة للأفراد، وعليه فيما تتمثل هذه الإجراءات؟ وماهي أهم هذه الضمانات والضوابط، وما مدى التزام سلطات البحث والتحري بها أثناء مباشرتهم لإجراء الترصد الإلكتروني؟

المطلب الأول: الترصد الإلكتروني في الجريمة المعلوماتية

نظرا لنجاعة آليات الترصد الإلكتروني في التصدي للجريمة الإلكترونية وجمع الأدلة الناتجة عنها، فقد اهتمت الاتفاقيات والمواثيق الدولية بالنص عليها، إذ تبنتها العديد من المواثيق الدولية على رأسها اتفاقية الأمم المتحدة لمكافحة الفساد في مادتها 50، [1] وكذا الاتفاقية الأوروبية حول الجرائم الإلكترونية لعام 2001من خلال نص المادة 21منها حيث أوصت جميع الدول الأعضاء بضرورة تبني إجراءات اعتراض المراسلات والمراقبة الإلكترونية للاتصالات ضمن تشريعاتها الداخلية، الأمر الذي لقي استجابة واسعة من طرف غالبية الدول الأوروبية، [2]كما نصت اتفاقية بودابست لعام 2001على هذه الإجراءات موجبة بذلك الدول الأعضاء باتخاذ إجراءات المراقبة والترصد بصدد التحري والتحقيق في الجرائم الخطيرة وخاصة الجرائم الإلكترونية و الجرائم المنظمة العابرة للحدود، إلا أنها لم تعرف هذه الآلية ولذلك أوجدت عدة تعريفات فقهية من بينها أنها عبارة عن"تتبع سوي ومتواصل للمجرم أو المشتبه فيه قبل وبعد ارتكابه لجريمة تم القبض عليه متلبسا بها"، وهناك من عرفها بصورها بقوله: "أن الترصد الإلكتروني هي تلك العملية التي تتم من خلالها اعتراض المراسلة أو تسجيل الأصوات أو التقاط الصور، وتثبيتها بغاية استغلالها في التحري والتحقيق في الجرائم"[3]

واستجابة للتوصيات التي قدمتها هاته الصكوك الدولية تبنت أغلب التشريعات المقارنة إجراءات اعتراض المراسلات وتسجيل الأصوات والتقاط الصور، إذ كان المشرع الفرنسي سباقا إلى تبني أسلوب اعتراض ومراقبة الاتصالات الإلكترونية ضمن إجراءات التحري من خلال القانون رقم 91- 649الصادر في 10يوليو 1991المتضمن قانون الإجراءات الجزائية الفرنسي، [4]حيث لم يرد في ق ا ج ج القديم نص واضح وصريح يجيز القيام بإجراءات التنصت الهاتفي وهذا ما أثاره القضاء الفرنسي حول مسألة شرعية هذه الإجراءات لتأتي فيما بعد محكمة النقض الفرنسية لتأكد شرعية التنصت التليفوني الذي يأمر به قاضي التحقيق بشرط ألا يقترن بحيلة فنية أو بمخالفة للحق في الدفاع.[5]وبقي الحال على هذا الشأن إلى أن أصدرت المحكمة الأوروبية لحقوق الإنسان حكمين صادرين في 24أفريل1990أدانت فيهما فرنسا إذ

---

[1] المادة 50 من اتفاقية الأمم المتحدة لمكافحة الفساد، المعتمدة من قبل الجمعية العامة للأمم المتحدة بنيويورك، بتاريخ 31 أكتوبر 2003، صادقت عليها الجزائر بموجب المرسوم الرئاسي رقم 128/06 المؤرخ في 2006/04/19، ج رج ج عدد 26 بتاريخ 2006/04/25.

2جمال إبراهيمي، التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص 88.

3خرشي عثمان، الترصد الإلكتروني كآلية لمكافحة الجرائم المعلوماتية، مجلة الدراسات الحقوقية، المجلد 07، العدد 03، سبتمبر 2020، ص 803- 804.

4Loi n° 91- 646 du 11 juillet 1991 ; JORF 13/07/1991.

5أحسن بوسقيعة، التحقيق القضائي، ط 2، الديوان الوطني للأشغال التربوية، الجزائر، 2002، ص 95.

أوضحت عدم كفاية الضمانات القانونية في القانون الفرنسي للتدخل في الحياة الخاصة للأفراد عن طريق مراقبة أحاديثهم واعتراضها مما يشكل مخالفة للمادة 08من الاتفاقية،[1] وهذا ما دفع المشرع الفرنسي إلى إصدار القانون رقم 91- 646في 10يوليو 1991الذي من خلاله نص على إمكانية اعتراض المراسلات والذي عدل فيما بعد بالقانون رقم 2019-222الصادر في 23/03/2019، حيث كرس المشرع الفرنسي هذه التقنية في المادة 100من هذا القانون والتي أجاز من خلالها لقاضي التحقيق باعتراض المراسلات وتسجيل الأحاديث الملتقطة ونقلها.[2]

وعلى غرار المشرع الفرنسي قام المشرع الأمريكي بمناسبة تعديل القانون الاتحادي الإجرائي الأمريكي عام 2000، بتوسيع مجال تطبيق إجراء الاعتراض والمراقبة ليشمل كل المراسلات السلكية واللاسلكية،[3] وبعد أحداث الحادي عشر (11) من شهر سبتمبر سنة 2001صدر قانون يبيح التنصت على المكالمات الهاتفية وتسجيلها كما أجاز اعتراض المراسلات بجميع أنواعها، حيث يعتبر المشرع الأمريكي هذا القانون بمثابة وسيلة إجرائية وقائية ضد جرائم الإرهاب الدولي، وليس انتهاكا للخصوصية، كما منح التشريع الأمريكي حق الاختصاص لمراقبة مدى صلاحية الإدارة في القيام بعمليات اعتراض المراسلات أو التنصت لبعض الجهات كمحكمة الاستخبارات الأجنبية التي تبحث في مدى توفر شروط مشروعية المراقبة من

1في 24أفريل صدر قرارين في قضية "كراستتان"و"ليفيغ"مسببين بشأن إجراءات التنصت الهاتفي الذي أجراه ضباط الشرطة القضائية في إطار تنفيذ إنابة قضائية، إذ أدانت المحكمة الأوروبية لحقوق الإنسان عمل السلطات الفرنسية هذا باعتباره لا يتماشى والمادة 08من =...الاتفاقية الأوروبية لحماية حقوق الانسان والحريات الفردية، حيث جاء في قرار المحكمة أن إجراء التنصت الهاتفي في قانون الإجراءات الفرنسي وأيضا في القضاء الفرنسي لم يوضح المشرع الفرنسي من خلالهما كيفية ممارسة هذا الإجراء، كما أصدرت وزارة العدل مذكرة في 28أفريل1990وجهتها إلى رؤساء المحاكم وقضاة التحقيق تدعوهم فيها إل ضرورة مراعاة م جاء في حكم المحكمة الأوروبية، ينظر حمزة قريشي، الوسائل الحديثة للبحث والتحري في ضوء قانون 06/22، مذكرة مقدمة لنيل شهادة الماجستير، دراسة مقارنة، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح، ورقلة، 2011/2012، ص 22.

2Article n° 100 du Loi n° 2019- 222 du 23/03/2019 ; JORF 25/03/2019 en vigueur le 01 juin 2019, code de procédure pénale dispose que : En matière criminelle et en matière correctionnelle, si la peine encourue est égale ou supérieure à trois ans d' emprisonnement, le juge d' instruction peut, lorsque les nécessités de m' information l' exigent, prescrire l' interception, l' enregistrement et la transcription de correspondances émises par la voie des communications électroniques, ces opérations sont effectuées sous son autorité et son contrôle.

La décision d'interception est écrite, Elle n'a pas de caractère juridictionnel et n'est susceptible d'aucun recours.

En cas de délit puni d'une peine d'emprisonnement commis par la voie des communications électronique sur la ligne de la victime, l'interception peut également être autorisée, selon les mêmes modalités, si elle intervient sur cette ligne à la demande de la victime. »

3جمال براهيمي، التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص 88.

طلب وشهادة مكتوبة وإذن بالعملية، [1]كما يجيز المشرع الإيطالي انتهاك الحق في سرية المراسلات لمصلحة العدالة في المادتين 226و338من قانون الإجراءات الجزائية الإيطالي رقم 517لسنة 1955، حيث أعطت هاتان المادتان للقضاء حق إصداره قرار بالاطلاع على المراسلات والتنصت على المكالمات الهاتفية في حالة ما إذا كان ذلك من شأنه أن يفيد السلطات القضائية في كشف الحقيقة.[2]

أما عربيا فقد أجازت بعض التشريعات اعتراض المراسلات من بينها المشرع الأردني[3]، المشرع السعودي، [4]وكذا المشرع المصري إذ سمح هذا الأخير لقاضي التحقيق بأن يأمر بمراقبة المحادثات السلكية واللاسلكية أو إجراء تسجيلات لأحاديث تجري في مكان خاص بموجب المادتين 95و206من ق ا ج م رقم 37لسنة 1972المعدل بالقانون رقم 189لسنة 2020[5]متى كانت هناك فائدة في إظهار الحقيقة، حيث نصت المادة 95على:"لقاضي التحقيق أن يأمر بضبط جميع الخطابات والرسائل والجرائد والمطبوعات والطرود لدى مكاتب البريد وجميع البرقيات لدى مكاتب البرق وأن يأمر بمراقبة المحادثات السلكية واللاسلكية أو إجراء تسجيلات لأحاديث جرت في مكان خاص متى كان لذلك فائدة في ظهور الحقيقة في جناية أو جنحة معاقب عليها بالحبس لمدة تزيد على ثلاثة أشهر، وفي جميع الأحوال يجب أن يكون الضبط أو الاطلاع أو المراقبة أو التسجيل بناء على أمر مسبب ولمدة لا تزيد على ثلاثين يوما قابلة للتجديد لمدة أو مدد أخرى مماثلة."[6]

1خضرة شنتير، الآليات القانونية لمكافحة الجريمة الإلكترونية، المرجع السابق، ص 124.

2المرجع نفسه، ص 125.

3تنص المادة 51فقرة 2من قانون الإجراءات الجزائية الأردني رقم (3) لسنة 2001على: "يجوز لضابط العدلية القضائية مراقبة المحادثات السلكية واللاسلكية وإجراء تسجيلات لأحاديث في مكان خاص بناء على إذن من قاضي الصلح متى كان لذلك فائدة في إظهار الحقيقة في جناية أو جنحة يعاقب عليها بالحبس لمدة ا تقل عن سنة".

4كما أجاز المشرع السعودي من خلال نظام الإجراءات الجزائية لعام 1435في المادة 57منه لرئيس النيابة العامة أن يأمر بضبط الرسائل والخطابات والمطبوعات وأن يراقب المحادثات الهاتفية وتسجيلها، متى كان في ذلك فائدة لإظهار الحقيقة في جريمة وقعت على أن يكون الأمر أو الإذن مسببا ومحدود المدة بمدة لا تزيد هن عشرة أيام قابلة للتجديد وفقا لمقتضيات التحقيق، كما أضافت اللائحة التنفيذية لهذا النظام بأن هذه المادة 57تشمل وسائل التواصل الإلكترونية بما يفيد أنه قد أجاز المشرع أيضا مراقبة وضبط الاتصالات الإلكترونية وفقا لنفس الشروط. لمزيد من التفاصيل ينظر خالد حسن لطفي، الدليل الرقمي ودوره في إثبات الجريمة المعلوماتية، المرجع السابق، ص 170.

5قانون الإجراءات الجنائية المصري رقم 37لسنة 1972الصادر بتاريخ 28سبتمبر 1972المعدل بالقانون رقم 189لسنة 2020الصادر بتاريخ 05سبتمبر 2020ج ر ج م عدد 36مكرر (ب).

6كما تنص المادة 206من قانون ا ج المصري رقم 189لسنة 2020على: "لا يجوز للنيابة العامة تفتيش غير المتهم أو منزل غير منزله إلا إذا اتضح من أمارات قوية أنه حائز لأشياء تتعلق بالجريمة.

ويجوز لها أن تضبط لدى مكاتب البريد الخطابات والرسائل والجرائد والمطبوعات والطرود ولدى مكاتب البرق جميع البرقيات وأن تراقب المحادثات السلكية واللاسلكية وأن تقوم بتسجيلات محادثات جرت في مكان خاص متى كان لذلك فائدة في ظهور الحقيقة في جناية أو جنحة معاقب عليها بالحبس لمدة تزيد على ثلاثة أشهر.

ولم يتخلف المشرع الجزائري عن هاته الدول فقد أشار لأول مرة لآلية الترصد الإلكتروني من خلال القانون 06/01 المتعلق بالوقاية من الفساد ومكافحته وذلك كأسلوب تحري خاص ضمن نص المادة م56منه، [1] دون إعطاء تعريف لهذه الآلية أو تنظيمها، ونظرا لهذا القصور تدخل مرة ثانية وذلك بموجب قانون الإجراءات ج ج رقم 06-22المؤرخ في 20/12/2006المعدل والمتمم، [2] حيث قام باستحداث الفصل الرابع من الباب الثاني تحت عنوان مغاير ضم جميع صور الترصد الإلكتروني ألا وهي: "اعتراض المراسلات وتسجيل الأصوات والتقاط الصور"بموجب المواد من المادة 65مكرر 5إلى المادة 65مكرر 10، تناول من خلالها المقصود بهذه الإجراءات ونطاقها وكذا ضوابط أو شروط استخدامها، وعلى هذا الأساس سنحاول معرفة المقصود بكل إجراء وكذا ضوابط وضمانات مباشرة هذه الإجراءات من قبل أجهزة البحث والتحري، وذلك في الفروع التالية:

الفرع الأول: تعريف اعتراض المراسلات وتسجيل الأصوات والتقاط الصور

بغرض البحث والتحري عن بعض الجرائم الخطيرة أجازت المادة 65مكرر5من قانون الإجراءات الجزائية الجزائري لضباط الشرطة القضائية القيام ببعض الإجراءات الخاصة والماسة بالحياة الخاصة للأفراد والمتمثلة في اعتراض المراسلات التي تتمعن طريق وسائل الاتصال السلكية واللاسلكية ، وتسجيل الأصوات وكذا التقاط الصور، حيث نصت المادة 65مكرر5على ما يلي:"إذا اقتضت ضرورات التحري في الجريمة المتلبس بها أو التحقيق الابتدائي في جرائم المخدرات أو الجريمة المنظمة العابرة للحدود الوطنية أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات أو جرائم تبييض الأموال أو الإرهاب أو الجرائم المتعلقة بالتشريع الخاص بالصرف وكذا جرائم الفساد يجوز لوكيل الجمهورية المختص أن يأذن بما يلي : اعتراض المراسلات التي تتم عن طرق وسائل الاتصال السلكية و اللاسلكية.

وضع الترتيبات التقنية دون موافقة المعنيين من أجل التقاط وتثبيت وبث وتسجيل الكلام المتفوه به بصفة خاصة أو سرية من طرف شخص أو عدة أشخاص في أماكن خاصة أو عمومية أو التقاط صور

...=ويشترط لاتخاذ أي إجراء من الإجراءات السابقة الحصول مقدما على أمر مسبب بذلك من القاضي الجزئي بعد اطلاعه على الأوراق، وفي جميع الأحوال يجب أن يكون الأمر بالضبط أو الاطلاع أو المراقبة لمدة لا تزيد على ثلاثين يوما ويجوز للقاضي الجزئي أن يجدد هذا الأمر لمدة أو مدد أخرى مماثلة...".

1تنصالمادة 56من القانون رقم 06-01المؤرخ في 20/02/2006، المتعلق بالوقاية من الفساد ومكافحته، ج ر ج ج عدد 14، الصادرة بتاريخ 08/03/2006.على: " من أجل تسهيل جمع الأدلة المتعلقة بالجرائم المنصوص عليها في هذا القانون يمكن اللجوء إلى التسليم المراقب أو اتباع أساليب تحر خاصة كالترصد الإلكتروني والاختراق، على النحو المناسب وبإذن من السلطة القضائية المختصة".

2القانون رقم 06- 22المتضمن ق ا ج ج المشار إليه سابقا.

لشخص أو عدة أشخاص يتواجدون في مكان خاص، يسمح الإذن المسلم بغرض وضع ترتيبات التقنية بالدخول إلى المحلات السكنية أو غيرها ولو خارج المواعيد المحددة في المادة 47من هذا القانون وبغير علم أو رضا الأشخاص الذين لهم حق على تلك الأماكن، تنفذ العمليات المأذون بها على هذا الأساس تحت مراقبة المباشرة لوكيل الجمهورية المختص، وفي حالة فتح تحقيق قضائي تتم العمليات المذكورة بناء على إذن من قاضي التحقيق وتحت مراقبته المباشرة"."[1]

وخلافا للمشرع الجزائري الذي جمع كل هذه الأساليب في مادة واحدة، فإن المشرع الفرنسي فرق بين هذه الأساليب حيث نص في المادة 706-95من ق ا ج ف رقم 2019- 222سالف الذكر على أسلوب اعتراض المراسلات، ونص في المادة 706-96منه على تسجيل الأصوات والتقاط الصور خاضعا كل واحد منهما لإجراءات خاصة.[2]

أولا: اعتراض المراسلات

يقصد باعتراض المراسلات كما عرفته لجنة الخبراء للبرلمان الأوروبي في اجتماعها المنعقد بستراسبورغ بتاريخ 06/10/2006حول أساليب التحري التقنية وعلاقتها بالأفعال الارهابية بأنه: "كل عملية مراقبة سرية للمراسلات السلكية واللاسلكية في إطار البحث والتحري عن الجريمة وجمع الأدلة أو المعلومات حول الأشخاص المشتبه فيهم في ارتكابهم أو في مشاركتهم في ارتكاب الجريمة"[3]، حيث تكون هذه المراقبة عن طريق اعتراض أو تسجيل أو نسخ المراسلات التي هي عبارة عن بيانات قابلة للتخزين والتوزيع والاتصال والاستقبال باستعمال وسائل سلكية كالهاتف أو لا سلكية كالهاتف النقال والبريد الالكتروني[4]وقد اقتبس المشرع الجزائري هذا التعريف بشيء من التفصيل في المادة 65مكرر 5المشار إليها أعلاه، وهو نفس ما اعتمده المشرع الفرنسي في المادة 100من ق إ ج ف،[5]إلا أنه لم يعرف المشرع الجزائري إجراء اعتراض المراسلات شأنه شأن المشرع الفرنسي، غير أن القضاء الفرنسي عرفها على أنها: تقنية يتم من خلالها الاعتراض عن طريق ربط خط هاتفي للمشتبه فيه مع اللجوء إلى تسجيل المكالمات في

1ينظر المادة 65مكرر 5من ق ا ج ج.

2يامة إبراهيم، أساليب التحري الخاصة بالجريمة المنظمة في القانونيين الجزائري والفرنسي، مجلة دفاتر السياسة والقانون، المجلد 11، العدد 02، جوان 2019، ص 153.

3-عبد الرحمان خلفي، الإجراءات الجزائية في التشريع الجزائري والمقارن، ط 4، دار بلقيس للنشر، الجزائر، 2018/2019، ص100.

4- المرجع نفسه، ص100.

5Voir l'article n° 100 du code de procédure pénale français.

أشرطة مغناطيسية.[1] وحسنا ما فعل المشرع عندما لم يقدم تعريفا محددا لعملية اعتراض المراسلات كما ورد في المادة 65مكرر5من قانون الإجراءات الجزائية وذلك لترك المجال مفتوحا لاحتواء أي تطور تكنولوجي في مجال وسائل الاتصال.

أما عن المقصود بالمراسلات السلكية واللاسلكية محل الاعتراض فقد عرفها المشرع الجزائري بموجب المادة 08فقرة 21من القانون رقم 2000-03المؤرخ في 05/08/2000الذي يحدد القواعد العامة المتعلقة بالبريد والمواصلات السلكية واللاسلكية والمعدل بالقانون رقم 18-04المحدد للقواعد العامة للبريد والاتصالات الإلكترونية، على أنها: "كل تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة عن طريق الأسلاك أو البصريات أو اللاسلكي الكهربائي أو أجهزة أخرى كهربائية مغناطيسية"[2] غير أنه بعد تعديل هذا القانون بالقانون رقم 18-04المشار إليه أعلاه، نجد بأنه ألغى هذه الفقرة وأضاف فقرة 16من المادة 09من القانون الجديد وعرف من خلالها "مادة المراسلة "على أنها: "اتصال مجسد في شكل كتابي على دعامة مادية مهما كانت طبيعتها يتم إيصاله وتسليمه إلى العنوان المبين من طرف المرسل نفسه أو بطلب منه. ولا تعد الكتب والفهارس والجرائد والدوريات كمادة مراسلات".[3]

وعليه فالملاحظ من هذه المواد أن المشرع الجزائري حدد المراسلات التي تصلح أن تكون محلا للاعتراض بتلك المراسلات التي تتم بواسطة وسائل الاتصال السلكية واللاسلكية دون الإشارة إلى طبيعة هذه المراسلات، إذ استعمل عبارة "مهما كانت طبيعتها "في المادتين مما يفتح المجال لمختلف الرسائل المكتوبة بغض النظر عن شكلها (كتابة، رموز، أشكال...) أو الدعامة التي تنصب عليها (ورقية أو رقمية)، أو الوسيلة المستعملة في إرسالها سلكية كانت كالفاكس مثلا او لاسلكية كالهاتف النقال والبريد الإلكتروني، كما يدخل أيضا ضمن المراسلات السلكية واللاسلكية كل المراسلات التي تتم بواسطة جهاز الإعلام الآلي والرسائل الصوتية المخزنة على الهاتف أو الرسائل القصيرة أو التسجيلات ضمن أشرطة

1خضرة شنتير، الآليات القانونية لمكافحة الجريمة الإلكترونية، المرجع السابق، ص 123.

2ينظر المادة 08فقرة 21من القانون رقم 2000- 03الذي يحدد القواعد العامة المتعلقة بالبريد والمواصلات السلكية واللاسلكية المشار إليه سابقا.

3ينظر المادة 09فقرة 16من القانون رقم 18-04المتعلق بالبريد والاتصالات الإلكترونية المشار إليه سابقا..

مرئية[1]، باستثناء الكتب والمجلات والدوريات التي لا تعد كمادة مراسلات طبقا لنص المادة 09فقرة 16من القانون رقم 18-04المحدد للقواعد العامة للبريد والاتصالات الإلكترونية.

كما تجدر الإشارة إلى أن الفقه فرق بين مصطلح اعتراض المراسلات أو المكالمات الهاتفية وما يسمى بوضع الخط التليفوني تحت المراقبة، فبينما يكون الأول دون رضا المعني، فالثاني يكون بطلب ورضا من صاحب الشأن و يخضع لتقدير الهيئة المختصة[2] بهدف إثبات الجريمة وخاصة في جرائم القذف والسب والتهديد الواقعة بواسطة الهاتف، كما لا يعتبر من قبيل الاعتراض قيام مأموري الضبط القضائي بتركيب جهاز على تليفون المجني عليه لتحديد وتسجيل رقم التليفون طالب المكالمة واليوم والساعة التي تم فيها الاتصال لأن الجهاز لا يسجل المكالمات ولا يتنصت عليها وإنما يسجل فقط أرقام الهواتف التي يستقبلها الشخص، وهذا ما أجازه القضاء الفرنسي لضباط الشرطة القضائية في مرحلة الاستدلال ودون اشتراط الحصول على إذن من وكيل الجمهورية، [3]كما لا يعتبر من قبيل الاعتراض قيام ضابط الشرطة بطلب المكالمات الصادرة والواردة والمدة التي تمت فيها وأماكن الاتصال وهوية المتصل من طرف وكالات المتعامل النقال، حيث أن هذا الإجراء يلجأ له الضابط بموجب تسخيرة أو مذكرة تقدم من قاضي التحقيق لجمع معلومات حول المشتبه فيهم ومعرفة هويتهم لفائدة التحقيق، وليس للتنصت على مكالماتهم واعتراضها.[4]

ثانيا: تسجيل الأصوات

يعرف التسجيل الصوتي بأنه التصنت على الأحاديث الخاصة وتسجيل المحادثات الشفوية التي يتحدث بها الأشخاص (المشتبه فيهم) بصفة سرية أو خاصة، "[5]كما قد عرف المشرع الأمريكي هذا الإجراء في الباب الثالث من القانون الفدرالي الأمريكي لسنة 1968على أنه الاكتساب السمعي عن طريق الاستماع لمحتويات أية أسلاك أو أية اتصالات شفوية عن طريق استخدام جهاز إلكتروني أو ميكانيكي أو أي جهاز آخر، [6]ويقصد بالمحادثة في مفهوم المادة كل صوت له دلالة التعبير عن معنى، بحيث لا يشترط فيه لغة معينة ولا دلالة معينة، إذ يمكن أن يكون مجرد صيحات، فالهدف من تسجيل الأصوات كأسلوب من

1مالك بن ذياب، حق الخصوصية في التشريع العقابي الجزائري، مذكرة مقدمة لنيل شهادة الماجستير، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، 2012/2013، ص 134.

2- عبد الرحمان خلفي، الإجراءات الجزائية في التشريع الجزائري والمقارن، المرجع السابق، ص 101.

3حمزة قريشي، الوسائل الحديثة للبحث والتحري في ضوء قانون 06/22، المرجع السابق، ص 23.

4المرجع نفسه، ص 24.

5علي شملال، المستحدث في قانون الإجراءات الجزائية الجزائري، الكتاب الثاني التحقيق والمحاكمة، ط2، دار هومه، الجزائر، 2017، ص77.

6حمزة قريشي، الوسائل الحديثة للبحث والتحري في ضوء قانون 06/22، المرجع السابق، ص 17.

أساليب التحري عن الجريمة هو متابعة المحادثات ومراقبتها وتسجيلها على أجهزة خاصة كدليل لإثبات هذه الجرائم.

وقد تبنت التشريعات المقارنة أسلوب تسجيل الأصوات من خلال قوانينها الإجرائية، بحيث أجازت لسلطات التحري والتحقيق اتخاذ هذا الإجراء بصدد التحري عن بعض الجرائم التي من بينها الجرائم الإلكترونية، إذ نجد المشرع الفرنسي قد نظم هذا الإجراء بموجب المادة 706- 96من ق ا ج ف التي أجازت نقل وتسجيل المكالمات التي يدلي بها الأشخاص بصفة خاصة أو سرية في أماكن عامة أو خاصة أو في مركبات، [1] كما نظمها المشرع المصري بموجب المادتين 95و206من ق ا ج المصري سالفتي الذكر، حيث أجاز لكل من قاضي التحقيق والنيابة العامة بإجراء تسجيل الأحاديث التي جرت في مكان خاص متى كان لذلك فائدة في ظهور الحقيقة.[2]

أما عن المشرع الجزائري فقد نص بموجب المادة 65مكرر 5فقرة (2) من قانون الإجراءات الجزائية على إمكانية اللجوء إلى تسجيل الأصوات والأحاديث وذلك كما يلي:" ...وضع الترتيبات التقنية دون موافقة المعنيين من أجل التقاط وتثبيت وبث وتسجيل الكلام المتفوه به بصفة خاصة أو سرية من طرف شخص أو عدة أشخاص في أماكن خاصة أو عمومية أو التقاط صور لشخص أو عدة أشخاص يتواجدون في مكان خاص".[3]

من خلال هذه المواد نلاحظ أنه قد سمح المشرع لضباط الشرطة القضائية وبمناسبة البحث والتحري عن إحدى الجرائم الواردة في نص المادة سابقة الذكر بتسجيل الكلام والأحاديث الخاصة التي تجري بين الأشخاص سواء في مكان عام أو خاص، بحيث يأخذ حكم الحديث الخاص ذلك الحديث الذي يجري بصفة سرية بين الأشخاص والذي يتضمن أسرارهم ومكنوناتهم بغض النظر عن مكان التسجيل كان عاما أو خاصا، غير أن قانون الإجراءات الجزائية الفرنسي كان أكثر دقة من نظيره الجزائري، حيث أباح تسجيل الكلام المتفوه به سواء في مركبات(Véhicule) أو في أماكن عمومية أو خاصة، وقد ذهبت

1Article n° 706- 96 modifié par loi n° 2019- 222 du 23 mars 2019, dispose que : Il peut être recouru à la mise en place d' un dispositif technique ayant pour objet, sans le consentement des intéressés, la captation, la fixation, la transmission et l' enregistrement de paroles prononcées par une ou plusieurs personnes à titre privé ou confidentiel, dans des lieux ou véhicules privés ou publics, ou de l' image d' une ou de plusieurs se trouvant dans un lieu privé ».

2ينظر المادتين 95و206من قانون الإجراءات الجزائية المصري رقم 189الصادر في 05سبتمبر 2020المشار إليه سابقا.

3ينظر المادة 65مكرر 5فقرة 2من ق ا ج ج.

محكمة النقض الفرنسية (الغرفة الجزائية) إلى أبعد من ذلك حيث سمحت في قرارها بتاريخ 01/03/2006بإمكانية التنصت على محادثات الموقوفين في المؤسسات العقابية مع زوارهم.[1]

كما أكدت هذه التشريعات على أن يكون هذا التسجيل دون علم ورضا المعنيين أو المشتبه في ارتكابهم لإحدى الجرائم السابقة، ونظرا للتطور التكنولوجي ظهرت العديد من الأجهزة الرقمية المختلفة التي تساعد على التقاط وتثبيت وتسجيل الصوت والكلام المتفوه به بجودة عالية، مثل الميكروفونات الحساسة ذات القدرة على التقاط الأصوات وتسجيلها منها ما يسمى بميكروفونات الليزر التي تقوم بالتقاط الأصوات من وراء النوافذ الزجاجية من خلال توجيه أشعة الليزر هاته إلى نافذة من نوافذ المكان ثم يتم تحويل هذه الذبذبات إلى أصوات واضحة، كما تستطيع هذه الأجهزة التقاط الإشارة الصادرة من أي جهاز إلكتروني موجود في المكان نفسه،[2] والتي قد توضع في مكتب المشتبه فيه أو في منزله أو حتى في مكان عمله، أو باستعمال الهاتف المحمول الذي باستطاعته تسجيل الصوت على نحو متناه في الدقة، وكذا استعمال أقلام الحبر أو الأزرار،[3] كما توجد أجهزة أخرى دقيقة في التقاط الأصوات تسمى Micro-direction حيث يمكنها تسجيل الأحاديث الخاصة على بعد مسافات طويلة وذلك بتوجيهها نحو فتحة معينة في مكان مثل النوافذ أو الشرفات ومنها ما هو قادر على التقاط الأحاديث من داخل المكان حتى لو كانت النوافذ مغلقة، وأخرى تدعى Micro Close تسمح بالتنصت على المحادثات التي تتم خلف حواجز أو جدار لمباني دون الحاجة لتثبيتها في المبنى المراد التنصت من خلاله، ومنها التي تأخذ شكل الرصاصة إذ

1Crim 01 mars 2006, n° 05- 87251, Jean Bradel, A. Varinard ; les grands arrêts de la procédure pénal, arrêt n° 17, Dalloz, 8 Edition, Paris, 2014, p 215 : Que d'autre part, les opérations, ordonnées par le juge d'instruction pour une durée limité, ont été placées en permanence sous son autorité et son contrôle et ont été justifiées par la nécessité de recherche la manifestation de la vérité, relativement à des infractions portant gravement atteinte à l'ordre public, telles celles prévues et définies par l'article 706- 73, alinéa 14, du code de procédure pénale.

Qu'enfin, la cour de cassation est en mesure de s'assurer que les garanties légales et conventionnelles reconnues aux personnes concernées par cette mesure ont été respectées, celles- ci ayant tout pouvoir d'en contrôler efficacement l'exécution.

2إن تسجيل الأصوات وإعادة إنتاجها هو عبارة عن كتابة كهربائية أو ميكانيكية للموجات الصوتية وإعادة تكوينها، ويتم ذلك بطريقتين: الأولى تسمى بالتسجيل التناظري والذي يتم بواسطة طبقة صغيرة يمكنها اكتشاف التغيرات في الضغط الجوي حيث تستشعر إبرة التسجيل الانخفاضات في التسجيل مسببة اهتزازات لطبقة الميكروفون ثم يتم تحويلها إلى تيار كهربائي متغير، والذي يتحول بعد ذلك إلى مجال مغناطيسي متغير بواسطة مغناطيس كهربائي، مما يؤدي إلى تمثيل للصوت، أما عن الطريقة الثانية لتسجيل الأصوات فتتمثل في التسجيل الرقمي الذي يتم عن طريق تخزين الصوت كمجموعة من الأرقام الثنائية ذات جودة عالية، ويعتبر التسجيل الرقمي أفضل من التسجيل التناظري، لمزيد من التفاصيل ينظر يزيد بوحليط، الجرائم الإلكترونية والوقاية منها في القانون الجزائري، المرجع السابق، ص 371.

3أمينة ركاب، أساليب التحري الخاصة في جرائم الفساد في القانون الجزائري، مذكرة مقدمة لنيل شهادة الماجستير، تخصص قانون عام معمق، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد، تلمسان، 204/2015، ص 61/62.

تطلق من بندقية لتستقر في حائط أحد المباني فترسل الأحاديث التي تلتقطها من داخل المبنى وتدعى هاته الأخيرة ب Micro Belles.[1]

ثالثا: التقاط الصور

لم يكتفي المشرع بالسماح لأجهزة التحري والتحقيق بتسجيل الأصوات بل مكنها أيضا من التقاط الصور وهذا لما تثبته عدسات الكاميرا من حقائق وتفاصيل تفيد في كشف الحقيقة، و كالعادة سمح المشرع الفرنسي لجهات التحقيق اتخاذ هذا الأسلوب في تحرياتها عن بعض الجرائم، وذلك بموجب المادة 706- 96من ق ا ج ف بالتقاط وتثبيت صور لشخص أو أكثر متواجد في مكان خاص، [2] في حين لم يأذن المشرع المصري لمأموري الضبط ق أو قاضي التحقيق بإجراء التصوير في مكان خاص، حتى لو كان ذلك بصدد جريمة واعتبر الدليل الناجم عن ذلك التصوير باطلا، وهذا ما أثار جدلا فقهيا حول مشروعية استخدام هذا الأسلوب في مواجهة الجرائم.[3]

كما تبنى المشرع الجزائري هذا الأسلوب في نص المادة 65مكرر 5فقرة 02من قانون الإجراءات الجزائية حيث أجاز لضباط الشرطة القضائية وضع الترتيبات التقنية اللازمة دون موافقة المعنيين من أجل التقاط صور لشخص أو عدة أشخاص يتواجدون في مكان خاص"، [4]ويتمثل هذا الأسلوب في وضع أجهزة تصوير صغيرة الحجم وإخفاؤها في أماكن خاصة لالتقاط صور تفيد في إجلاء الحقيقة وتسجيلها، وبالرجوع إلى المادة 65مكرر5من قانون الإجراءات الجزائية نجدها قد نصت على التقاط الصور في المكان الخاص وبمفهوم المخالفة فانه لا تخضع لأي ضابط من الضوابط المنصوص عليها في المواد سالفة الذكر مسألة التقاط الصور في المكان العام، فجهاز الأمن مثلا يعتمد على أسلوب المراقبة عن طريق استخدام أجهزة التصوير في الطرق العامة للحفاظ على النظام والأمن العموميين، وهذا ما يلاحظ على المشرع الجزائري والفرنسي أيضا من خلال أخذه بمعيار طبيعة المكان الخاص لا بحالة الخصوصية التي يكون عليها الأشخاص، إضافة إلى وجوب وضع هذه التقنيات بدون علم ورضا المعني أو الشخص المشتبه فيه.[5]

1حمزة قريشي، الوسائل الحديثة للبحث والتحري في ضوء قانون 06/22، المرجع السابق، ص 26.

2Voir l'Article n° 706- 96 du code de procédure pénale français.

3أشرف عبد القادر قنديل، الوسائل الإلكترونية ودورها في الإثبات الجنائي (دراسة مقارنة)، دار الجامعة الجديدة، مصر، 2018، ص 256.

4ينظر المادة 65مكرر 5فقرة 2من قانون ا ج ج.

5عاقلي فضيلة، الحماية القانونية للحق في حرمة الحياة الخاصة، دراسة مقارنة، أطروحة مقدمة لنيل شهادة الدكتوراه، كلية الحقوق، جامعة الإخوة منثوري، قسنطينة، 2011/2012، ص 190/ 191.

وبناء على ذلك فإن النص على وضع الترتيبات التقنية يفيد استخدام كل أنواع الأجهزة التصويرية ووسائل المراقبة المرئية المختلفة من وسائل الرؤية والمشاهدة التي تسهل عمليات الالتقاط والتثبيت وتسجيل الصور مثل الدوائر التلفزيونية المغلقة وآلات التصوير عن بعد وأجهزة التصوير بالأشعة الحمراء وغيرها من الأجهزة التي ساعد التطور التكنولوجي والتقني على ظهورها، إلا أنه من جهة أخرى ساعد هذا التطور على صنع التطبيقات والبرامج الخاصة بتركيب وتعديل الصور كالمونتاج إلى غير ذلك، مما يشكك في القيمة القانونية للدليل المستمد من هذه الإجراءات.

الفرع الثاني: مشروعية اللجوء لهذه الأساليب

لما كانت المراسلات والأحاديث الخاصة والصور الشخصية تعبر عن الحياة الخاصة للأفراد فإنها تستمد حصانتها من حرمة هذه الحياة الخاصة، ولهذا حرصت المواثيق الدولية والدساتير والتشريعات العقابية في جميع الدول على ضرورة احترام حرمة الحياة الخاصة وعدم المساس بها أو انتهاكها بأي شكل من الأشكال، فنجد من أهم هذه المواثيق الإعلان العالمي لحقوق الإنسان الصادر في 10ديسمبر 1948من قبل الجمعية العامة للأمم المتحدة، تضمن مجموعة من المبادئ الدولية التي تنادي باحترام الحقوق الأساسية للإنسان لاسيما حقه في حرمة حياته الخاصة، حيث نصت المادة 12منه على: "لا يتعرض أحد لتدخل تعسفي في حياته الخاصة أو أسرته أو مسكنه أو مراسلاته أو لحملات على شرفه وسمعته، ولكل شخص الحق في حماية القانون من مثل هذا التدخل أو تلك الحملات".[1]كما أكد العهد الدولي الخاص بالحقوق المدنية والسياسية الصادر في 16ديسمبر 1966من قبل الجمعية العامة للأمم المتحدة، في المادة 17منه على عدم التدخل في خصوصيات الأفراد وكل ما يتعلق بحياتهم الخاصة بقولها: "لا يجوز التدخل بشكل تعسفي أو غير قانوني بخصوصيات أحد أو بعائلته أو مراسلاته، ولا لأي حملات غير قانونية تمس شرفه أو سمعته، من حق كل شخص أن يحميه القانون من مثل هذا التدخل أو المساس"، [2]ومن جهة أخرى نادت الاتفاقية الأوروبية لحماية البيانات الشخصية في مجال المعلوماتية التي تبناها المجلس الأوروبي بمدينة ستراسبورغ الفرنسية سنة 2004، الدول الأعضاء بضرورة اتخاذ ما يجب من إجراءات للتصدي للإجرام الإلكتروني المهدد لسرية البيانات والمعلومات، [3]وهذا ما جرمته اتفاقية بودابست لسنة

1خلايفية هدى، الإطار الدولي والداخلي لحماية الخصوصية على الإنترنت (التشريع الجزائري نموذجا)، مداخلة مشارك بها في الملتقى الدولي الموسوم بـ: "الخصوصية في مجتمع المعلوماتية"، في طرابلس، لبنان، 19-20جويلية 2019، ص 43.

2المرجع نفسه، ص 44.

3، خلايفية هدى، الإطار الدولي والداخلي لحماية الخصوصية على الإنترنت (التشريع الجزائري نموذجا)، المرجع السابق، ص 46.

2001في مادتها الثالثة (03) إذ عاقبت على كل عملية اعتراض غير قانوني متعمد يكون بواسطة وسائل إلكترونية وتكنولوجية للبيانات المرسلة من وإلى الكمبيوتر.

وعلى غرار هذه المواثيق الدولية فقد ظهرت العديد من الاتفاقيات التي كرست حماية الحياة الخاصة للأشخاص، من بينها الاتفاقية الأوروبية لحقوق الإنسان 1950في مادتها الثامنة (08)، الاتفاقية الأمريكية لحقوق الإنسان لسنة 1969في مادتها الحادية عشر (11)، الميثاق الإفريقي لحقوق الإنسان والشعوب، والميثاق العربي لحقوق الإنسان في مادته الحادية والعشرين (21)، التي اتفقت جميعها على احترام خصوصية كل شخص وعدم التدخل في شؤون حياته الخاصة أو المساس بسرية مراسلاته واتصالاته، حتى وإن كان الهدف من ذلك التصدي للجريمة وحماية المجتمع.[1]

وعلى هدي هذه المواثيق والصكوك الدولية سارت الدساتير المقارنة، إذ أقر التعديل الرابع لدستور الو م أ حماية للحق في الحياة الخاصة وأضفى عليها طابع الحرمة إذ نص على: "حق الأفراد أو المواطنين في أن يكونوا آمنين في أشخاصهم ومنازلهم وأوراقهم ومستنداتهم من عمليات التفتيش والضبط غير المشروعة التي تقوم بها سلطات إنفاذ القانون بدون إذن قضائي..."، [2]وعلى غرار المشرع الأمريكي، كرس المشرع الجزائري حماية كبيرة للحق في الحياة الخاصة وذلك من خلال النص عليه في مختلف الدساتير التي عرفتها الجزائر منذ تاريخ استقلالها، فقد كفل المؤسس الدستوري حماية سرية المراسلات والاتصالات كصورة من صور الحق في الحياة الخاصة بحيث لا يجوز لأي كان الاعتداء عليها بأي شكل، بالإضافة إلى أنه أكد على حماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، وذلك من خلال نص المادة 39من التعديل الدستوري لسنة 2020 والتي تنص على: "تضمن الدولة عدم انتهاك حرمة الإنسان..."، وكذا نص المادة 47 منه والتي تنص على أنه: "لكل شخص الحق في حماية حياته الخاصة وشرفه. لكل شخص الحق في سرية مراسلاته واتصالاته الخاصة في أي شكل كانت، لا مساس بالحقوق المذكورة في الفقرتين الأولى والثانية إلا بأمر معلل من السلطة القضائية، حماية الأشخاص عند معالجة المعطيات ذات الطابع الشخصي حق أساسي، يعاقب القانون على كل انتهاك لهذه الحقوق".[3]

1حليم رامي، إجراءات استخلاص الدليل في الجرائم المعلوماتية، مجلة دفاتر البحوث العلمية، المجلد 09، العدد 01، سنة 2021، ص 236.

2حيث ينص التعديل الرابع للدستور الأمريكي على:

« The right of the people to be secure in their persons, houses, papers, and effects, againstunreasonablesearches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularlydescribing the place to besearched, and the persons or things to beseized ».

3ينظر المادتين 39و47من التعديل الدستوري الجزائري لسنة 2020.

كما نص الدستور المصري في المادة 57منه على أنه : "للحياة الخاصة حرمة، وهي مصونة لا تمس، وللمراسلات البريدية والبرقية والإلكترونية والمحادثات الهاتفية وغيرها من وسائل الاتصال حرمة وسريتها مكفولة ولا تجوز مصادرتها أو الاطلاع عليها أو رقابتها إلا بأمر قضائي مسبب ولمدة محددة وفي الأحوال التي يبينها القانون".[1]

والملاحظ من هذه النصوص الدستورية أنها كفلت الحماية للحياة الخاصة للأفراد بجميع أشكالها وأقرت العقاب على كل انتهاك لهذه الخصوصية وهو ما نجد تطبيقه في القوانين العقابية لأغلب الدول، فقد عاقب المشرع الجزائري على انتهاك حرمة الحياة الخاصة للأفراد في قانون العقوبات رقم 06-23المؤرخ في 20/12/2006[2] بموجب المادة 303منه حيث اعتبر المراسلات والرسائل من قبيل الخصوصيات ولا يجوز المساس بها أو الاطلاع على محتواها أو إتلافها وإلا توجب عقوبة الحبس والغرامة بقولها: "كل من يفض أو يتلف رسائل أو مراسلات موجهة إلى الغير وذلك بسوء نية وفي غير الحالات المنصوص عليها في المادة 137يعاقب بالحبس من شهر (1) إلى سنة (1) وبغرامة من 25.000دجإلى 100.000دج أو بإحدى هاتين العقوبتين فقط".

كما وشدد العقوبة إذا كان مرتكب الفعل موظف أو مستخدم أم مندوب عن مصلحة البريد وذلك بموجب المادة 137من ق ع ج والتي تقضي بما يلي: "كل موظف أو عون من أعوان الدولة أو مستخدم أو مندوب عن مصلحة البريد يقوم بفض أو اختلاس أو إتلاف رسائل مسلمة إلى البريد أو يسهل فضها أو اختلاسها أو إتلافها، يعاقب بالحبس من ثلاثة (3) أشهر إلى خمس (5) سنوات وبغرامة من 30.000دج إلى 500.000دج.ويعاقب بالعقوبة نفسها كل مستخدم أو مندوب في مصلحة البرق يختلس أو يتلف برقية أو يذيع محتواها، ويعاقب الجاني فضلا عن ذلك بالحرمان من كافة الوظائف أو الخدمات العمومية من خمس سنوات إلى عشر سنوات".

كما عاقب المشرع الجزائري على تسجيل المكالمات والأحاديث الخاصة والتقاط الصور بموجب المادة 303مكرر والتي تنص على: "يعاقب بالحبس من ستة (6) أشهر إلى ثلاث (3) سنوات وبغرامة من 50.000دج إلى 300.000دج، كل من تعمد المساس بحرمة الحياة الخاصة للأشخاص بأية تقنية كانت وذلك: بالتقاط أو تسجيل أو نقل مكالمات أو أحاديث خاصة أو سرية بغير إذن صاحبها أو رضاه. بالتقاط

1ينظر المادة 57من دستور الجمهورية المصرية المعدل بالفرار رقم 38لسنة 2019الصادر بتاريخ 23أبريل 2019.

2القانون رقم 06- 23المؤرخ في 29ذي القعدة عام 1427الموافق 20ديسمبر 2006، المعدل والمتمم للأمر رقم 66- 156المؤرخ في 18صفر عام 1386الموافق 08يونيو سنة 1966، المتضمن قانون العقوبات، ج ر ج ج عدد 84الصادرة بتاريخ 24ديسمبر 2006.

أو تسجيل أو نقل صورة لشخص في مكان خاص بغير إذن صاحبها أو رضاه، يعاقب على الشروع في ارتكاب الجنحة المنصوص عليها في هذه المادة بالعقوبات ذاتها المقررة للجريمة التامة..."، وهي نفس الجريمة التي عاقب عليها المشرع الفرنسي في المادة 226-1من ق ع ف رقم 92- 684لسنة 1992[1]، والمشرع المصري بموجب المادة 309مكرر من ق ع م رقم 58لسنة 1937[2]، حيث استعمل كل من المشرع الجزائري والفرنسي عبارة "بأية تقنية كانت "والتي تفيد أن تكون عملية تسجيل المكالمات والتنصت والتقاط الصور عن طريق الوسائل الإلكترونية، ما يسمح باستيعاب التقنيات الحاضرة والمستقبلية التي يفرزها التقدم العلمي، وكذلك فعل المشرع المصري في المادة 309مكرر من ق ع باستخدام عبارة "جهاز من الأجهزة أيا كان نوعه"والتي تفيد أن يكون الجهاز إلكتروني.

وتجدر الإشارة إلى أن المشرع الجزائري عند إقراره للحماية الجنائية للأحاديث والمكالمات الخاصة أخذ بمعيار طبيعة الحديث الخاص لا بمعيار المكان الذي يلتقط فيه الصوت أو الحديث فيستوي في ذلك أن يكون الحديث في مكان عام أو خاص، إلا أنه بخصوص التقاط الصور فقد اشترط أن تلتقط في مكان خاص لإضفاء الحماية عليها طبقا لنص المادة 303من ق ع ج، وهو ما أقره المشرع الفرنسي حيث أخذ بالمعيار الموضوعي المتمثل في طبيعة الحديث الخاصة دون المكان التي جرت فيه وفقا للمادة 226-

1Article n° 226-1 modifié par la loi n°2020- 936 du 30 juillet 2020- art 17 en vigueur le 01 Aout 2020; code pénal français, dispose que: Est puni d'un an d'emprisonnement et de 45.000 euros d'amande le fait au moyen d'un procédé quelconque, volontairement de porter atteinte à l'intimité de la vie privée d'autrui :

1° En captant, enregistrant ou transmettant, sans le consentement de leur auteur, des paroles prononcées à titre privé ou confidentiel ;

2° En fixant, enregistrant ou transmettant, sans le consentement de celle- ci, l'image d'une personne se trouvant dans un lieu privé.

3° En captant, enregistrant ou transmettant, par quelque moyen que ce soit, la localisation en temps réel ou en différé d'une personne sans le consentement de celle- ci.

Lorsque les actes mentionnés aux 1° et 2° du présent article ont été accomplis au vu et au des intéressées sans qu'il s'y soient opposés, alors qu'ils étaient en mesure de le faire, le consentement de ceux- ci est présumé.

Lorsque les actes mentionnés au présent article ont été accomplis sur la personne d'un mineur, le consentement doit émaner des titulaires de l'autorité parentale.

Lorsque les faits sont commis par le conjoint ou le concubin de la victime ou le partenaire lié à la victime par un pacte civil des solidarité, les peines sont portées à deux ans d'emprisonnement et à 60.000 euros d'amande. ».

2تنص المادة 309مكرر من القانون رقم 58لسنة 1937المؤرخ في 05أوت 1937، المتضمن قانون العقوبات المصري على: "يعاقب بالحبس مدة لا تزيد على سنة كل من اعتدى على حرمة الحياة الخاصة للمواطن، وذلك بأن ارتكب أحد الأفعال الآتية في غير الأحوال المصرح بها قانونا أو بغير رضا المجني عليه:

- استرق السمع أو سجل أو نقل عن طريق جهاز من الأجهزة أيا كان نوعه محادثات جرت في مكان خاص أوعن طريق التليفون.
- التقط أو نقل بجهاز أيا كان نوعه صورة شخص في مكان خاص".

1من ق ع ف، في حين أن المشرع المصري أخذ بطبيعة المكان لا الحديث باشتراطه المكان الخاص طبقا لما جاء في نص المادة 309مكرر من ق ع م[1]، وهو ما أخذ به المشرع الأردني في المادة 51فقرة 2من ق ا ج سالف الذكر.[2]

وخلاف لهاته التشريعات نجد أن المشرع الأمريكي نص بصريح العبارة بموجب القانون الجنائي الفيدرالي على أنه يعاقب على كل من يعترض أو يساعد غيره على اعتراض أي اتصال سلكي أو شفوي أو إلكتروني، وكل من يفشي أو يحاول أن يفشي محتوى اتصال هاتفي أو إلكتروني[3]، والتي تقابلها المادة 226-15من ق ع الفرنسي[4]، والمادة 303مكرر 1من ق ع ج التي تعاقب على الاحتفاظ بالمراسلات أو الصور أو استخدامها أو وضعها في متناول الجمهور.[5]

من زاوية أخرى فرض المشرع الجزائري نوعا من الحماية الجزائية للاتصالات بموجب القانون رقم 18-04المحدد للقواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية_ الذي عدل من خلاله القانون رقم 2000-03المؤرخ في 05/08/2000الذي يحدد القواعد العامة المتعلقة بالبريد والمواصلات السلكية واللاسلكية_ حيث ضمنه في المواد من المادة 164إلى المادة 188عدة عقوبات جزائية تفرض على المتعاملين في هذا المجال، أهمها ما جاء في المادة 164والتي تعاقب كل من ينتهك سرية المراسلات عبر البريد أو الاتصالات إ أو يفشي مضمونها أو ينشره أو يستعمله دون ترخيص من المرسل أو المرسل إليه، وذلك

1أشرف عبد القادر قنديل، الوسائل الإلكترونية ودورها في الإثبات الجنائي، المرجع السابق، ص 192وما بعدها.

2عاصف جودت أحمد النجاجره، خصوصية التحقيق في الجرائم الإلكترونية، رسالة مقدمة لنيل شهادة الماجستير، جامعة القدس، فلسطين، 2019، ص 39.

3رشيدة بوكر، الحماية الجزائية للتعاملات الإلكترونية، المرجع السابق، ص 316.

4Article 226-15 modifié par Ordonnance n° 2000- 916 du 19 septembre 2000, art 3, JORF 22/09/2000 en vigueur le 1 janvier 2002 dispose que : Le fait commis de mauvaise foi, d'ouvrir de supprimer de retarder ou de détourner des correspondances arrivées ou non à destination et adressées à des tiers, ou d'en prendre frauduleusement connaissance, est puni d'un an d'emprisonnement et de 45000 euros d'amende.

5تنص المادة 303مكر 1من ق ع ج على: "يعاقب بالعقوبات المنصوص عليها في المادة السابقة كل من احتفظ أو وضع أو سمح بأن توضع في متناول الجمهور أو الغير، أو استخدم بأية وسيلة كانت التسجيلات أو الصور أو الوثائق المتحصل عليها بواسطة أحد الأفعال المنصوص عليها في المادة 303مكرر من هذا القانون.

عندما ترتكب الجنحة المنصوص عليها في الفقرة السابقة عن طريق الصحافة تطبق الأحكام الخاصة المنصوص عليها في القوانين ذات العلاقة لتحديد الأشخاص المسؤولين.

يعاقب على الشروع في ارتكاب الجنحة المنصوص عليها في هذه المادة بالعقوبات ذاتها المقررة للجريمة التامة.

ويضع صفح الضحية حدا للمتابعة الجزائية".

بالحبس من سنة إلى خمس (5) سنوات والغرامة من 500.000دج إلى 1.000.000دج، [1] والمادة 165من نفس القانون والتي تعاقب كل متعامل للبريد يفتح أو يخرب البريد أو يساعد في ارتكاب هذه الأفعال بالحبس من سنة إلى ثلاثة سنوات وبغرامة من 1.000.000دج إلى 5.000.000دج أو بإحدى هاتين العقوبتين، وتطبق نفس الأحكام على كل متعامل للاتصالات الإلكترونية يحول بأية طريقة كانت المراسلات الصادرة أو المرسلة أو المستقبلة عن طريق الاتصالات الإلكترونية، [2] وهو ما يعاقب عليه المشرع الفرنسي بموجب نص المادة 432- 9من ق ع الفرنسي. [3]

واستنادا لما سبق ذكره فإنه في حقيقة الأمر ليست الحماية الجنائية للحياة الخاصة حماية مطلقة بل ترد عليها بعض الاستثناءات نظرا لتدخل المشرع بواسطة القواعد الإجرائية تغليبا منه للمصلحة العامة، ولتحقيق نوع من التوازن بين حماية الحق في الحياة الخاصة وبين حق المجتمع في العقاب بحيث لا يفلت

1تنص المادة 164من القانون رقم 18- 04المحدد للقواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية على: "يعاقب بالحبس من سنة (1) إلى خمس (5) سنوات وبغرامة من 500.000دج إلى 1.000.000دج كل شخص ينتهك سرية المراسلات المرسلة عن طريق البريد أو الاتصالات الإلكترونية أو يفشي مضمونها أو ينشره أو يستعمله دون ترخيص من المرسل أو المرسل إليه أو يخبر بوجودها".

2كما تنص المادة 165من ذات القانون على أنه : "يعاقب بالحبس من سنة (1) إلى ثلاث (3) سنوات وبغرامة من 1.000.000دج إلى 5.000.000دج أو بإحدى هاتين العقوبتين، كل متعامل للبريد يفتح أو يحول أو يخرب البريد أو يساعد في ارتكاب هذه الأفعال.

تسري نفس العقوبات على كل متعامل للاتصالات الإلكترونية يحول بأي طريقة كانت المراسلات الصادرة أو المرسلة أو المستقبلة عن طريق الاتصالات الإلكترونية أوامر أو ساعد في ارتكاب هذه الأفعال.

ويمكن الجهة القضائية أيضا النطق بواحدة أو أكثر من العقوبات التكميلية المنصوص عليها في المادة 09من قانون العقوبات".

كما عاقب المشرع الجزائري بموجب المادة 166من ذات القانون كل عون مستخدم من طرف متعامل للبريد يفتح أو يخرب البريد أو يساعد في ارتكاب هذه الأفعال في إطار ممارسة مهامه بعقوبة الحبس من ستة أشهر إلى سنتين وبغرامة من 500.000دج إلى 1.000.000دج، ويعاقب بنفس هاته العقوبات كل مستخدم لدى متعامل للاتصالات الإلكترونية يحول بأي طريقة كانت المراسلات الصادرة أو المرسلة أو المستقبلة عن طريق الاتصالات الإلكترونية أو أمر أو ساعد في ارتكاب هذه الأفعال.

ومن خلال هذه المواد نرى أن المشرع الجزائري قد أضفى حماية كبيرة للمراسلات والاتصالات ومنع الاطلاع عليها وفي هذا ضمانة للحياة الخاصة للأفراد، وقد واكب التطورات في مجال الاتصالات باستحداثه هذا القانون.

3Article n° 432- 9 modifié par loi n° 2004- 669 du 9 juillet 2004 art- 121 JORF 10 juillet 2004, code de procédure pénale ; dispose que : Le fait, par une personne dépositaire de l'autorité publique ou chargé d'une mission de service public, agissant dans l'exercice ou à l'occasion de l'exercice de ses fonctions ou de sa mission, d'ordonner, de commettre ou de faciliter, hors les cas prévus par la loi, le détournement, la suppression ou l'ouverture de correspondances ou la révélation du contenu de ces correspondances, est puni de trois ans d'emprisonnement et de 45.000 euros d'amende.

Est puni des mêmes peines le fait, par une personne visée à l'alinéa précédent ou un agent d'un exploitant de réseaux ouverts au public de communications électroniques ou d'un fournisseur de service de télécommunications, agissant dans l'exercice de ses fonctions, d'ordonner, de commettre ou de faciliter, hors les cas prévus par la loi, l'interception ou le détournement des correspondances émises, transmises ou reçues par la voie des télécommunications, l'utilisation ou la divulgation de leur contenu ».

الجاني بحجة حماية حرمة الحياة الخاصة ولا تهدد الحريات بحجة حق المجتمع في العقاب، [1] لعل أهم ضمانة هي تجسيد مبدأ الشرعية الإجرائية الذي يقضي باحترام الحقوق الفردية المقررة قانونا أثناء مراحل الدعوى العمومية، ومن خلال هذه المبادئ والأسس التي جاءت بها المواثيق الدولية اهتدت أغلب التشريعات الداخلية ومن بينها المشرع الوطني إلى تبني هذا المبدأ وتكريسه دستوريا باعتبار أن الدستور هو الذي يرسم حدود هذه الشرعية ويلزم المشرع باتباعها، إذ نص المشرع الدستوري الجزائري على هذا المبدأ في دساتيره المتعاقبة وأحاط بعض الإجراءات التي تباشرها السلطة التنفيذية في مجال الحريات، بقيود ونصوص دستورية نظرا لأهميتها وخطورتها على حقوق الإنسان وحرياته الفردية، وقد تجلى هذا التكريس في المواد 41 43 وما يليها من التعديل الدستوري لسنة 2020، [2] والتي أكدت على أنه لا يمكن إدانة أي شخص إلا بمقتضى قانون صادر قبل ارتكاب الجريمة، كما لا يجوز متابعة أي شخص إلا ضمن شروط وإجراءات محددة قانونا، وقد أقره المشرع الجزائري بصفة صريحة بعد صدور القانون رقم 17-07 الذي أدخل نصا جديدا على التقنين الإجرائي أثار مكانة هذا المبدأ في المادة الجزائية، وهو نص المادة الأولى (01) من قانون الإجراءات الجزائية، والذي قضى بتطبيق مبادئ الشرعية والمحاكمة العادلة وكذا احترام كرامة وحقوق الإنسان، وتكريس مبدأ أصل البراءة وما ينتج عنه من تفسير الشك لصالح المتهم، ومن جانب آخر نص المشرع على ضرورة السرعة في الفصل في القضايا وإعلام المتقاضين بحقوقهم أمام القضاء، إضافة إلى ضرورة تسبيب الأحكام والقرارات القضائية، [3] كما يحتاج ضمان حماية حريات وحقوق الأفراد إشرافا قضائيا، فالقضاء باعتباره الحامي لهذه الحقوق والحريات يعتبر الوسيلة لضبط القانون وفرض احترام تطبيقه، ولذلك نجد جل الدساتير والقوانين تعهد مهمة مراقبة مدى مشروعية الإجراءات إلى السلطة القضائية، وبالتالي فإن النظام القضائي يعد عنصرا مهما من عناصر الشرعية الإجرائية فمن خلاله يتم الموازنة بين المصلحة العامة أو مصلحة الدولة في تقرير العقاب من جهة، ومصلحة الفرد في حماية الحرية الشخصية له. [4] ومن هذا المنطلق قام المشرع بتحصين هذه الشرعية من

---

1 حمزة قريشي، الوسائل الحديثة للبحث والتحري في ضوء قانون 06/22، المرجع السابق، ص 30.

[2] تنص المادة 41 من التعديل الدستوري الجزائري لسنة 2020 على: " كل شخص يعتبر بريئا حتى تثبت جهة قضائية إدانته، في إطار محاكمة عادلة".

وتقضي المادة 43 من نفس القانون على: "لا إدانة إلا بمقتضى قانون صادر قبل ارتكاب الفعل المجرم".

وفي نفس الصدد وتكريسا لمبدأ الشرعية الإجرائية قضت المادة 44 من نفس القانون ب: " لا يتابع أحد ولا يوقف ولا يحتجز، إلا ضمن الشروط المحددة بالقانون، وطبقا للأشكال التي نص عليها...".

[3] ينظر المادة 01 من القانون رقم 17- 07 المتضمن قانون الإجراءات الجزائية الجزائري.

[4] كريمة علا، الشرعية الجنائية الإجرائية: نجاعة الصياغة وفعالية التطبيق، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، المجلد 05، العدد 02، سنة 2020، ، ص 1248.

خلال فرض جزاءات معينة في حالة عدم التطبيق أو التطبيق السيئ للإجراءات أو التعسف في استعمالها، ويتمثل هذا الجزاء الإجرائي في إلغاء الإجراء المخالف للقانون عن طريق تقرير ما يسمى بالبطلان، الذي يعد الوسيلة المثلى للرقابة القضائية على صحة الإجراءات المتخذة، وقد أخذ المشرع الجزائري بالبطلان القانوني من خلال نصوص قانونية محددة حصرا فلا يجوز لأي سلطة تقريره ما لم ينص القانون على ذلك استنادا إلى القول بأن لا بطلان إلا بنص، [1] وقد نظمه في قانون الإجراءات الجزائية في القسم العاشر تحت عنوان "في بطلان إجراءات التحقيق"، والمندرج ضمن الفصل الأول من الباب الثالث المعنون ب "في جهات التحقيق"، في المواد من 157 إلى 161.[2]

وقد أسند المشرع الجزائري لغرفة الاتهام صلاحية مراقبة الإجراءات على اعتبار أنها درجة ثانية للتحقيق وهذا في حد ذاته ضمانة للمتهم في احترام حقوقه وضمان لحماية الحق العام في سير إجراءات التحقيق، وتمارس الغرفة رقابتها هذه في جميع مراحل التحقيق منذ بدايته إلى غاية نهايته، كما يتعرض القائم بهذه الإجراءات غير المشروعة سواء كان ضابط شرطة قضائية أو قاضي تحقيق أو غيره، للمتابعة الجزائية نتيجة هذا الإخلال والانتهاك الصارخ لمبدأ الشرعية الإجرائية، فاحترام حقوق الأفراد وحرياتهم يقاس بمدى تطبيق الشرعية والضمانات المقررة قانونا، وليس بكمية الضمانات والمبادئ التي تتضمنها السلطة التشريعية.

ولهذا قد اشترطت أغلب التشريعات الجنائية لصحة هذه الإجراءات جملة من الضوابط و الشروط الموضوعية والشكلية التي تعد ضمانات قانونية تحول دون تعسف السلطات القضائية في اتخاذ هذه الإجراءات في مواجهة المشتبه فيهم، وتتمثل هذه الضوابط فيما يلي:

أولا: **الضوابط الموضوعية**

1. لقد اختلفت التشريعات المعاصرة في تحديد الجرائم التي تبرر اللجوء إلى أساليب التحري الخاصة، وذلك لاختلاف السياسة الجنائية المتبعة في كل دولة، ولكن ما يجمع هاته التشريعات أنها اتفقت في أن تكون هذه الأساليب بصدد مكافحة الجرائم الخطيرة في منظور كل دولة، حيث منها من لجأت في تحديد الجريمة التي تكون محل عمليات المراقبة إلى معيار جسامة العقوبة المقررة للجريمة، ومن بينها المشرع الفرنسي حيث أخذ بهذا المعيار بصدور قانون الإجراءات الجزائية رقم 91- 646سالف الذكر

[1] رميساء كحول، دور قانون الإجراءات في تحقيق الشرعية الجزائية، المجلة الجزائرية للأمن الإنساني، المجلد 07، العدد 01، جانفي 2020، ص 618.

[2] ينظر المواد من 157 إلى 161 من قانون الإجراءات الجزائية الجزائري المشار إليه أنفا.

والذي نظم من خلاله مراقبة الاتصالات بحيث حدد الجرائم التي تبرر اللجوء إلى المراقبة والاعتراض بالجنايات والجنح التي تساوي عقوبتها أو تزيد عن الحبس لمدة سنتين طبقا لنص المادة 100- 1من ق ا ج ف، وعليه فإنه بمفهوم المخالفة لا يجوز اللجوء لهذه الأساليب إذا ما كانت عقوبة الجريمة الحبس لمدة تقل عن سنتين، وهو نفس ما تبناه المشرع الأردني بموجب المادة 51فقرة 2من ق ا ج أ[1]، والمشرع المصري حيث أخذا بمعيار جسامة العقوبة إذ بالرجوع للمادة 95أو 206من ق ا ج م نجدها أجازت اللجوء لهذه الأساليب الخاصة في الجرائم المعاقب عليها بالحبس لمدة تزيد عن ثلاثة أشهر، [2]وهذا عكس ما ذهب إليه المشرع الجزائري إذ أخذ بمعيار طبيعة الجريمة لا بمعيار جسامة العقوبة، بحيث حدد الجرائم التي يجوز فيها اللجوء لاعتراض المراسلات وتسجيل الأصوات والتقاط الصور وذلك بموجب نص المادة 65مكرر5من ق ا ج والتي تتمثل في جرائم المخدرات، الجريمة المنظمة العابرة للحدود الوطنية، الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، جرائم تبييض الأموال أو الإرهاب، الجرائم المتعلقة بالتشريع الخاص بالصرف، وجرائم الفساد.[3]

ونرى أن المقاربة التي اعتمدها المشرع الجزائري بحصر الجرائم التي يتم اللجوء فيها لإجراءات المراقبة تحد من حرية السلطة القضائية في استعمال هذه الأساليب الخاصة في التحري، وبالتالي من فعالية التحقيق وذلك لصعوبة وصف الجريمة وتكييفها قبل اكتمال التحقيق، إضافة إلى تقييد سلطة قاضي التحقيق في اتخاذ هذا الإجراء بصدد جرائم أخرى خطيرة غير الجرائم التي حددها المشرع سابقا كجرائم اختطاف الأطفال والقتل ...الخ، في حين أن المشرع الفرنسي ترك المجال مفتوحا للسلطات القضائية لأن تحديد الجنايات والجنح بتحديد العقوبة المقدرة في قانون العقوبات أمر سهل وميسور.[4]

وعلى خلاف المشرع الفرنسي والمصري والجزائري قد أخذت بعض التشريعات الأخرى منها الأنجلوساكسونية مثل الولايات م أ وانجلترا بمعياري جسامة العقوبة وطبيعة الجريمة معا في تحديد الجرائم التي يجوز فيها إجراءات المراقبة، إذ يحدد المشرع الجرائم التي تجوز فيها المراقبة وفقا لعقوبتها، ثم يجيز إلى جانب ذلك المراقبة في جرائم أخرى محددة على سبيل الخطر استنادا إلى طبيعتها وبصرف النظر

1ينظر المادة 51فقرة 2من قانون الإجراءات الجزائية الأردني رقم (3) لسنة 2001.

2أشرف عبد القادر قنديل، الوسائل الإلكترونية ودورها في الإثبات الجنائي، المرجع السابق، ص 205.

3ينظر المادة 65مكرر 5من ق ا ج ج سالفة الذكر.

4وهيبة رابح، الإجراءات المتبعة أمام الأقطاب الجزائية المتخصصة، أطروحة مقدمة لنيل شهادة الدكتوراه في القانون الإجرائي، كلية الحقوق والعلوم السياسية، جامعة مستغانم، سنة 2015/2016، ص 237.

عن عقوبتها، [1] ولعل هذا الجمع يعتبر أفضل معيار لتحديد الجرائم التي تبرر اللجوء لإجراءات التحري الخاصة.

2. إن الناظر في التشريعات المعاصرة التي أجازت اللجوء إلى إجراءات المراقبة يلاحظ أنها تقيد مباشرة هذه الإجراءات بوجود فائدة منها في إظهار الحقيقة، وهو ما نص عليه المشرع الفرنسي صراحة في المادة 100من ق ا ج ف بعبارة "أن تكون المراقبة ضرورية لمصلحة التحقيق"وما أكدت عليه محكمة النقض الفرنسية، وكذلك فعل المشرع الأردني في المادة 51فقرة 2من ق ا ج[2]، والمشرع المصري إذ قرن مباشرة المراقبة بأن تكون لها فائدة في ظهور الحقيقة وذلك في المادة 206من ق ا ج م، [3] غير أنه أضاف المشرع المصري شرطا آخر يقضي أن تتخذ هذه الإجراءات بصدد جريمة وقعت بالفعل لاعتباره إجراءات المراقبة هذه من إجراءات التحقيق لا التحري أو الاستدلال وهذا ما أكدته محكمة النقض المصرية بقولها: "إن الأصل في الإذن بالتفتيش أو تسجيل المحادثات أنه إجراء من إجراءات التحقيق لا يصح إصداره إلا لضبط جريمة (جناية أو جنحة) وقعت بالفعل، وترجحت نسبتها إلى متهم معين، وهناك من الدلائل ما يكفي التصدي لحرمة مسكنه أو حريته الشخصية".[4]

وبالرجوع للمشرع الجزائري فقد اشترط لجواز اتخاذ إجراءات اعتراض المراسلات وتسجيل الأصوات والتقاط الصور أن تقتضيها ضرورة التحري في الجرائم المتلبس بها، أو التحقيق الابتدائي في الجرائم التي حددها حصرا في المادة 65مكرر 5من ق ا ج ج ومنها الجرائم الإلكترونية، حيث نجد المشرع الجزائري قد قيد اللجوء إلى هاته الأساليب بضرورة توافر حالة التلبس بالجريمة ما يعني أنه لا يجوز اتخاذها بصدد الجنايات أو الجنح غير المتلبس بها، وفي هذا تضييق على سلطة وكيل الجمهورية وفي نفس الوقت ضمانة للمشتبه فيه في عدم انتهاك خصوصياته إلا للضرورة التي تقتضيها عملية التحري، [5] ومن جانب آخر لا يجوز اللجوء إلى هاته الإجراءات إلا بصدد التحقيق الابتدائي في الجرائم التي حددتها المادة سالفة الذكر، وهذا ما يعني أنه لا يمكن الإذن بها إلى إذا وقعت الجريمة فعلا وأسندت التهمة إلى المتهم باعتبار وجود

1حمزة قريشي، الوسائل الحديثة للبحث والتحري في ظل قانون رقم 06- 22، المرجع السابق، ص 30.

2ينظر المادة 51فقرة 2من ق ا ج الأردني.

3رشيدة بوكر، الحماية الجزائية للتعاملات الإلكترونية، لمرجع السابق، ص 319.

4أشرف عبد القادر قنديل، الوسائل الإلكترونية ودورها في الإثبات الجنائي، المرجع السابق، ص 235.

5جزول صالح، ضمانات مشروعية التنصت التلفوني واعتراض المراسلات في القانون الإجرائي الجزائري، مجلة نوميروس الأكاديمية، المجلد 01، العدد 02، يونيو 2020، ص 163.

دلائل كافية وقوية ضده، وفي جميع الأحوال تبقى مسألة تقدير ضرورة اللجوء لهذه الإجراءات من عدمه للسلطة التقديرية للقاضي.

3. نظرا لخطورة إجراءات المراقبة ومساسها بحرمة الحياة الخاصة للأشخاص فقد اتجهت جل التشريعات إلى وضع هذه الإجراءات في يد السلطة القضائية وهو ما يعد تطبيقا لمبدأ الضمان القضائي في الإجراءات الجزائية وضمانة لمشروعية إجراءات المراقبة، حيث أجاز المشرع الفرنسي مراقبة المراسلات وتسجيل المكالمات بناء على إذن صادر عن قاضي الحريات والحجز أو الحبس في حالة التحقيق الأولي أو مرحلة الاستدلال، حيث له أن يأذن باعتراض المراسلات بناء على طلب وكيل الجمهورية، ويتوجب على هذا الأخير إطلاع القاضي بأي عمل يتم في هذا الإطار، وفي حالة التحقيق الابتدائي في الجرائم فإن قاضي التحقيق هو من له صلاحية إصدار الإذن بوضع الترتيبات الضرورية لتنفيذ إجراءات المراقبة طبقا لنص المادة 100- 1من ق ا ج ف، غير أنه إذا تعلق الأمر بوضع هذه الترتيبات في مكان معد للسكن _ والذي تتم فيه هذه العمليات خارج الساعات المبينة في المادة 59من ق ا ج ف_ فإن الإذن يمنح من طرف قاضي الحريات والحبس بناء على طلب من قاضي التحقيق، [1] وفي جميع الأحوال يخضع قاضي التحقيق لرقابة غرفة الاتهام أثناء مباشرة هذه الإجراءات، [2] كما يمكن للمحكمة الجنحية ومحكمة الجنايات في حالة

1Article n° 706- 95 modifié par Ordonnance n° 2019- 964 du 18 septembre 2019- art 35 en vigueur le 01/01/2020 ; code de procédure pénale ; dispose que : Si les nécessités de l'enquête de flagrance ou de l'enquête préliminaire relative à l'une des infractions entrant dans le champ d'application des articles 706- 73 et 706- 73-1 l'exigent, le juge des libertés et de la détention du tribunal judiciaire peut, à la requête du procureur de la république, autoriser l'interception, l'enregistrement et la transcription de correspondances émises par la voie des communications électronique selon les modalités prévues par les articles 100, deuxième alinéa, 100-1 et 100-3 à 100-7, pour une durée maximum d'un mois, renouvelable une fois dans les mêmes conditions de forme et de durée. Ces opérations sont faites sous le contrôle du juge des libertés et de la détention.
Les dispositions de l'article 100-8 sont applicables aux interceptions ordonnées en application du présent article.
Pour l'application des dispositions des articles 100-3 à 100-5 et 100-8, les attributions confiées au juge d'instruction ou à l'officie de police judiciaire requis par ce magistrat.
Le juge des libertés et de la détention qui a autorisé l'interception est informé sans délai par le procureur de la république des actes accomplis en application de l'alinéa précédent, notamment des procés- verbaux dressés en exécution de son autorisation, par application des articles 100-4 et 100-5 ».

2أشرف عبد القادر قنديل، الوسائل الإلكترونية ودورها في الإثبات الجنائي، المرجع السابق، ص 222.

التحقيق التكميلي أن تمنح الإذن بمباشرة عمليات المراقبة وهذا ما جاءت به المواد 205و283من ق ا ج ف.[1]

وعلى نهج المشرع الفرنسي سار المشرع المصري إعمالا لحكم المادة 57من الدستور التي حظرت المراقبة إلا بأمر قضائي مسبب[2]، إذ أجاز في المادة 95من ق ا ج م لقاضي التحقيق أو القاضي الجزائي بإصدار إذن بالمراقبة، [3] واستثناء سمح للنيابة العامة إذا ما تولت هي التحقيق في هذه الجرائم أن تمنح الإذن لمأموري الضبط القضائي لمباشرة عمليات المراقبة وبعد حصولها على إذن من قاضي التحقيق أو القاضي الجزائي طبقا لنص المادة 206من ق ا ج م، إذ يعد هذا التوسع في الاختصاص بالنسبة للنيابة العامة أمرا غير محمود لأنه يقلل من الضمانات التي تحول دون التعسف في انتهاك الحياة الخاصة للأفراد.[4]

وخلافا للمشرعين الفرنسي والمصري فقد انتهج المشرع الجزائري نهجا مختلفا في تحديد السلطة المختصة بإصدار الإذن، فبالرجوع للمادة 65مكرر 5من ق ا ج ج، فإنه يجوز اعتراض المراسلات وتسجيل الأصوات والتقاط الصور من طرف ضابط الشرطة القضائية بعد حصوله على إذن مكتوب من طرف وكيل الجمهورية المختص إقليميا في حالة البحث عن جريمة متلبس بها، أو من قاضي التحقيق في حالة فتح تحقيق قضائي في الجرائم المحددة سلفا بموجب المادة 65مكرر 5من ذات القانون، كما أجاز المشرع لقاضي التحقيق أن ينتدب ضابط من ضباط الشرطة القضائية لإجراء عمليات المراقبة ضمن نفس الشروط المنصوص عليها قانونا وهذا ما يستنتج من عبارة "ضابط الشرطة القضائية المأذون له أو المناب"الواردة في المادة 65مكرر 9من ذات القانون،

حيث تتم هذه العمليات تحت الرقابة المباشرة لكل من وكيل الجمهورية وقاضي التحقيق، وعلى هاذين الأخيرين قبل منح هذا الإذن تقدير فائدة هذه الإجراءات وجديتها وملائمتها لسير إجراءات الدعوى من خلال معطيات التحريات التي قامت بها الضبطية القضائية مسبقا،[5] ومعى ه ا أنه تل م الـ ة القـ ائة لة مـ الـ اجات ت اه و الـ هـ رة حـ تأخ مـ ه جـ ع الـ عل ات الـ اجـ ات اذها

1حمزة قريشي، الوسائل الحديثة للبحث والتحري في ظل قانون رقم 06- 22، المرجع السابق، ص 42.

2تنص المادة 57من دستور الجمهورية المصرية على: "للحياة الخاصة حرمة، وهي مصونة لا تمس، وللمراسلات البريدية والبرقية والإلكترونية والمحادثات الهاتفية وغيرها من وسائل الاتصال حرمة وسريتها مكفولة ولا تجوز مصادرتها أو الاطلاع عليها أو رقابتها إلا بأمر قضائي مسبب ولمدة محددة وفي الأحوال التي يبينها القانون"

3والتي تقابلها المادة 51فقرة 2من ق ا ج الأردني.

4أشرف عبد القادر قنديل، الوسائل الإلكترونية ودورها في الإثبات الجنائي، المرجع السابق، ص 232.

5ليندا بن طالب، الدليل الإلكتروني ودوره في الإثبات الجنائي، المرجع السابق، ص 108.

د إجراء معـ ، ومـ جهة ثانة قـ م الـائـ العام الإشـاف على مهام الـ ة ق وأ ا تـجـهه في مـاشـة ع لـه ، وفي حالة تقـ أحـ الـ ا ز للـائـ العام إحالـه إلى غـفة الاتهام غـض تـ الـ ع الـأدي ة ضـ ه، ا ع ضـا الـ ة القـ ائـة لقاة غـفة الاتهام فهي مـ ة ا ة أعـال الـ ق سـ اء قام بها ضـا الـ ة أو قاضي الـ ق لـعـفة مـ صـ ة ه ه الإجـاءات، وفي حالة الإجـاء الـ الـ للقاذ ن فإنه يـ تـ على ذلـ الـ لان قـا للـ اد 157 159 و160 مـ ق ا ج، و ع الـ لان ضـانة قاذ ن ة لـ ع القائـ الـ ق يل م أ الـ ة ع الـ ق بهـ ه الإجـاءات.

وتجدر الإشارة إلا أنه وفيما يتعلق بالجوانب التقنية لتنفيذ مثل هذه العمليات فقد أجازت المادة 65مكرر 8[1]من نفس القانون لكل من وكيل الجمهورية وقاضي التحقيق أو ضابط الشرطة القضائية المأذون له أن يسخر كل عون مؤهل لدى مصلحة أو وحدة أو هيئة عمومية أو خاصة مكلفة بالمواصلات السلكية واللاسلكية للتكفل بالجوانب التقنية للعمليات المذكورة في المادة 65مكرر5من نفس القانون، وذلك نظرا لكون هذه العمليات تقنية بحتة تستلزم أن يكون القائم بها ذو خبرة واختصاص في مجال تركيب الأجهزة والمعدات الخاصة بتسجيل الأصوات والتقاط الصور في أماكنها المناسبة، غير أن المشرع الجزائري لم يبين لنا طبيعة الأشخاص الذين يتم تسخيرهم للقيام بهذه الإجراءات التقنية التي تسمح باعتراض وتسجيل المراسلات هذا ما يجب تداركه من المشرع بشيء من التفصيل.

4. حرصت معظم التشريعات المقارنة على تحديد مدة معينة لإجراءات اعتراض المراسلات والتنصت التليفوني والتقاط الصور حيث حددها كل من المشرع الفرنسي في المادة 100- 2من ق ا ج ف، والمشرع الجزائري في المادة 65مكرر 7فقرة 2بأربعة (04) أشهر قابلة للتجديد ضمن نفس الشروط الشكلية والزمنية، [2] إلا أن المشرع الفرنسي اشترط أن لا تتجاوز المدة كاملة للمراقبة سنة واحدة، حسب ما جاء في نص المادة 100- 2من ق ا ج ف، وإذا ما تعلق الأمر بالجرائم المنصوص عليها في المواد 706-

1تنص المادة 65مكرر 8من ق ا ج ج على: "يجوز لوكيل الجمهورية أو ضابط الشرطة القضائية الذي أذن له، ولقاضي التحقيق أو لضابط الشرطة القضائية الذي ينيبه أن يسخر كل عون مؤهل لدى مصلحة أو وحدة أو هيئة عمومية أو خاصة مكلفة بالمواصلات السلكية واللاسلكية للتكفل بالجوانب التقنية للعمليات المذكورة في المادة 65مكرر 5أعلاه".

2تنص المادة 65مكرر 7فقرة 2من ق ا ج ج على: "...يسلم الإذن مكتوبا لمدة أقصاها أربعة (4) أشهر قابلة للتجديد حسب مقتضيات التحري أو التحقيق ضمن نفس الشروط الشكلية والزمنية".

73و706- 73- 1ومنها الاعتداء على نظم المعالجة الآلية للمعطيات[1]، فتكون مدة المراقبة سنتين كاملتين[2]، في حين نرى أن المشرع المصري قد حدد مدة المراقبة بأمد قصير يتمثل في ثلاثين يوما قابلة للتجديد لمدة أو مدد أخرى طبقا للمادتين 95و206من ق ا ج م، [3] بحيث يحق للقاضي الجزائي تجديد الإذن بالمراقبة بناء على طلب من النيابة العامة أو بأمر قضائي لمدة ثلاثين يوم أخرى ولم يحدد المشرع الحد الأقصى لهذا التجديد إذ أجازه لعدة مرات بشرط ألا تزيد المدة الواحدة عن ثلاثين يوما، [4] في حين حددها المشرع السعودي وفقا للمادة 57من نظام الإجراءات الجزائية بعشرة (10) أيام قابلة للتجديد.[5]

ونحن نرى أنه حبذا لو قلص المشرع الجزائري هذه المدة لأنها بقدر ما تعتبر تطبيقا لضمانة دستورية بعدم انتهاك حق الحياة الخاصة للأفراد، بقدر ما تتضمن مخاطر تكمن في إمكانية استغلال هذه المدة الطويلة من قبل ضابط الشرطة القضائية في التعسف والتمادي في التنصت ومراقبة محادثات الأشخاص وفي هذا انتهاك صارخ لحريات وخصوصيات الأفراد.[6]

أما عن المكان الذي تتم فيه عمليات المراقبة فلم يحدد المشرع الجزائري بدقة الأماكن التي يجوز فيها اعتراض المراسلات وتسجيل الأصوات والتقاط الصور، بل جاء النص على عمومه بحيث أجازت المادة 65مكرر 5اتخاذ هاته الإجراءات في أماكن عامة وخاصة دون استثناء، وذلك دون موافقة المعنيين أو أصحاب هذه الأماكن، وحتى خارج الآجال المنصوص عليها في المادة 47من ق ا ج ج، [7] بمعنى يمكن وضع الترتيبات التقنية (كوضع كاميرات مراقبة أو ميكروفونات لتسجيل الأصوات وغيرها) داخل المحلات

1Voir l'article n° 703-73 modifié par Ordonnance n°2020- 1733 du 16 décembre 2020 – art 11 en vigueur le 01/05/2021,code de procédure pénale français.

2Article n° 100-2 modifié par loi n°2016-731 du 03 juin 2016 –art 57 en vigueur le 05/06/2016, code de procédure pénale, dispose que : Cette décision est prise pour une durée maximum de quatre mois, Elle ne peut être renouvelée que dans les mêmes conditions de forme et de durée, sans que la durée totale de l'interception puisse excéder un an ou s'il s'agit d'une infraction prévue aux articles 706-73 et 706-73-1 , deux ans ».

3ينظر المادتين 95و206من ق ا ج المصري سالف الذكر.

4أشرف عبد القادر قنديل، الوسائل الإلكترونية ودورها في الإثبات الجنائي، المرجع السابق، ص 236.

5ينظر المادة 57من نظام الإجراءات الجزائية السعودي سالف الذكر.

6جزول صالح، ضمانات مشروعية التنصت التلفوني واعتراض المراسلات في القانون الإجرائي الجزائري، المرجع السابق، ص 168.

7تنص المادة 47من ق ا ج ج على: "...عندما يتعلق الأمر بجرائم المخدرات أو الجريمة المنظمة عبر الحدود الوطنية أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبييض الأموال والإرهاب وكذا الجرائم المتعلقة بالتشريع الخاص بالصرف فإنه يجوز إجراء التفتيش والمعاينة والحجز في كل مكان سكني أو غير سكني في كل ساعة من ساعات النهار أو الليل وذلك بناء على إذن مسبق من وكيل الجمهورية المختص.

عندما يتعلق الأمر بالجرائم المذكورة في الفقرة الثالثة أعلاه، يمكن قاضي التحقيق أن يقوم بأية عملية تفتيش أو حجز ليلا أو نهارا وفي أي مكان على امتداد التراب الوطني أو يأمر ضباط الشرطة القضائية المختصين للقيام بذلك...".

السكنية وغير السكنية في أي ساعة من ساعات النهار أو الليل وهذا ما ينطبق مع إجراءات التفتيش والمعاينة والحجز في كل محل سكني أو غير سكني المنصوص عليها في المادة سالفة الذكر، غير أنه أوجب المشرع في المادة 65مكرر 6فقرة 1من ق ا ج أن تتم هذه الترتيبات والعمليات دون المساس بالسر المهني المنصوص عليه في المادة 45من ق ا ج [1] والتي ترخص بتفتيش الأماكن التي يشغلها شخص ملزم قانونا بكتمان السر المهني منوهة على ضرورة اتخاذ جميع التدابير اللازمة لضمان احترام ذلك السر قبل مباشرة هذه العمليات، ومن الأشخاص الملزمين بكتمان السر المهني الأطباء، المحامون، الموثقون وغيرهم...الخ، [2] وخلافا لذلك سمح المشرع الفرنسي بموجب المادة 706- 96من ق ا ج ف بالمراقبة في بعض الأماكن العامة والخاصة وحتى داخل المركبات، ومنع الدخول لبعض الأماكن الأخرى كاستثناء [3] منها المؤسسات الإعلامية مثل مؤسسة الصحافة أو الاتصال السمعي البصري طبقا للمادة 56- 2من ق ا ج ف، والمحلات ذات الطابع المهني للأطباء، المحامين، الموثقين ، المحضرين القضائيين، إلا أنه بعد تعديل قانون الإجراءات الفرنسي بالقانون رقم 2004- 204الصادر في 09مارس 2004سمح المشرع بمراقبة مكتب المحامي والقاضي وكذا محل إقامتهم واعتراض مراسلاتهم لكن بعد إبلاغ نقيب المحامين، أو النائب العام بالولاية القضائية التي يقيم فيها القاضي طبقا للمادة 100- 7من ق ا ج ف. [4]

5. تتم إجراءات اعتراض المراسلات وتسجيل المحادثات الشخصية بين الأشخاص المشتبه في ارتكابهم بعض الجرائم الخطيرة، إلا أنه ليست كل الأحاديث محل اعتراض فهناك بعض الأحاديث الخاصة تتمتع بالحماية وتحول دون التنصت عليها وتسجيلها من بينها، الأحاديث التي تجري بين المتهم ومحاميه وهذا لطابع السرية الذي يتمتع به الحديث بين المحامي وموكله والذي يتفرع عن مبدأ سرية المهنة لأن حق الدفاع حق مقدس يجب احترامه، فقد نصت المادة 116من ق ا ج الفرنسي على حق المتهم

1تنص المادة 45من ق ا ج ج على: "...غير أنه يجب عند تفتيش أماكن يشغلها شخص ملزم قانونا بكتمان السر المهني أن تتخذ مقدما جميع التدابير اللازمة لضمان احترام ذلك السر".

2يامة ابراهيم، أساليب التحري الخاصة بالجريمة المنظمة في القانونين الجزائري والفرنسي، المرجع السابق، ص 156.

3رشيدة بوكر، الحماية الجزائية للتعاملات الإلكترونية، المرجع السابق، ص 239.

4Article n°100-7 modifié par loi n°2004-204 du 9 mars 2004 – art 5 JORF 10 mars 2004 en vigueur le 01/03/2004, code de procédure pénale, dispose que : Aucune interception ne peut avoir lieu sur la ligne d'un député ou d'un sénateur sans que le président de l'assemblée à laquelle il appartient en soit informé le juge d'instruction.
Aucune interception ne peut avoir lieu sur une ligne dépendant du cabinet d'un avocat ou de son domicile sans que le bâtonnier en soit informé le juge d'instruction.
Aucune interception ne peut avoir lieu sur une ligne dépendant du cabinet d'un magistrat ou de son domicile sans que le premier président ou le procureur général de la juridiction ou il réside en soit informé les formalités prévue par le présent article sont prescrites à peine de nullité ».

في الاتصال بمحاميه بحرية وسرية تامة، [1] وفي هذا الصدد حظرت محكمة استئناف باريس التنصت على المحادثات المتبادلة بين المتهم ومحاميه نزولا عن حق الدفاع، فألغت أمر الندب الذي صدر من قاضي التحقيق لضابط الشرطة القضائية بمراقبة تليفون أحد المحامين واعتبرت جميع الإجراءات باطلة، وبصدور القانون رقم 2004- 204الصادر في 09مارس 2004كما أشرنا سابقا فقد سمح المشرع بمراقبة الخط التليفوني الخاص بمكتب المحامي بعد إبلاغ نقيب المحامين طبقا للمادة 100- 7من ق ا ج ف.[2]

إضافة لهذا حظر القانون مراقبة أحاديث رؤساء الدول الأجنبية والدبلوماسيين والقناصلة باعتبارهم يتمتعون بالحصانة القضائية التي تعفيهم من الخضوع لقضاء الدولة المضيفة بصدد الجرائم التي يرتكبونها على إقليمها بحيث يمتنع أن يتخذ ضدهم إجراء من إجراءات الاستدلال أو التحقيق أو المحاكمة والتي منها مراقبة أحاديثهم الخاصة أو تسجيلها، لكن هذه الحماية ليست مطلقة بالنسبة لبعض هذه الفئات بل هناك بعض الاستثناءات.[3]

ثانيا: الضوابط الشكلية

1. لقد اشترطت غالبية التشريعات المقارنة وجوب الحصول على إذن من السلطات المختصة لمباشرة عمليات المراقبة والاعتراض كونها إجراءات تمس الحياة الخاصة للأفراد وتنتهك سرية مراسلاتهم وأحاديثهم الخاصة، وهذا ما أكدته جل الدساتير، فبالرجوع للدستور المصري النافذ نجده قد تطرق إلى ضرورة منح الإذن بالمراقبة ذلك في المادة 57منه بقولها: "...للمراسلات البريدية والهاتفية وغيرها من وسائل الاتصال حرمة وسريتها مكفولة، ولا تجوز مصادرتها أو الاطلاع عليها أو رقابتها إلا بأمر قضائي مسبب،

1Voir l'article n° 116 modifié par loi n°2019-222 du 23 mars 2019 – art 56 en vigueur le 01/06/2019, code de procédure pénale français.

2حمزة قريشي، الوسائل الحديثة للبحث والتحري في ظل قانون رقم 06- 22، المرجع السابق، ص 37وما بعدها.

3فبالنسبة للصفة الدبلوماسية العليا التي يتمتع بها رئيس الدولة فإنه يتمتع بالحصانات والامتيازات الدبلوماسية فلا يخضع بذلك لاختصاص محاكم الدولة المستقبلة ولا تتخذ الإجراءات ضده، فلا يجوز مراقبة أحاديث رئيس الدولة الأجنبية ولا تسجيلها وتعتبر هذه الحماية مطلقة لا تحمل أي استثناء، أما عن المبعوثين الدبلوماسيين فيتمتعون بحماية تحول دون خضوعهم للإجراءات الجزائية في إقليم الدولة المبعوثين إليها، حيث تمتد هذه الحماية إلى مراسلاتهم ومحادثاتهم سواء المتعلقة بالبعثة أو الخاصة بهم ولو كان ذلك لازما لكشف جريمة معينة، وخلافا لهؤلاء فإن القناصلة يتمتعون بحماية نسبية وليست مطلقة إذ تلتزم الدولة المستضيفة بحماية وصيانة مراسلاتهم وعدم الاطلاع عليها ولكن في حدود ضيقة إذ يتمتع القناصلة بالحصانة القضائية فيما يتعلق بأعمالهم الرسمية فقط ولا يتمتعون بهذه الحصانة بصدد أعمالهم الخاصة التي يقومون بها خارج الدوام الرسمي لهم، ومعنى هذا أنه إذا ارتكب أحد القناصلة جريمة تتعلق بعمله الرسمي فإنه لا تجوز محاكمته عنها لتمتعه بالحصانة القضائية، أما إذا ارتكب جريمة لا علاقة لها بعمله فإنه لا يتمتع بهذه الحصانة ويجوز محاكمته، وبالتالي يجوز اعتراض مراسلاته وتسجيل أحاديثه الخاصة في حالة ما إذا نتج تحقيق عن جريمة ما. أنظر قريشي حمزة، المرجع نفسه، ص 39.

ولمدة محددة وفي الأحوال التي يبينها القانون..."، [1] كما سار على هذا الطريق المؤسس الدستوري الجزائري إذ أكد على ضرورة وجود هذا الشرط لإمكانية المساس بالحياة الخاصة، إذ نصت المادة 47من دستور 2020على أنه: " ...لا مساس بالحقوق المذكورة في الفقرتين الأولى والثانية إلا بأمر معلل من السلطة القضائية..."، [2] وهذا ما يعد ضمانة إجرائية كبيرة لحماية الحياة الخاصة للأفراد من جهة وتمكين السلطات القضائية من التصدي للجرائم الخطيرة دون التعسف في استعمال حقها واتخاذ عمليات المراقبة هاته.

وتأكيدا لهذه الضمانات الدستورية التي جاءت بها هاته الدساتير، نصت القوانين الإجرائية على ضرورة حصول القائم بهذه العمليات على إذن أو أمر من السلطات القضائية، إذ أخذ المشرع المصري بشرط الإذن في المادة 95و المادة 206من ق ا ج م، [3] بقولها "...ويشترط لاتخاذ إجراء من الإجراءات السابقة الحصول مقدما على أمر مسبب بذلك من القاضي الجزائي بعد اطلاعه على الأوراق..."، [4] كما أوجب المشرع الجزائري وبموجب المادة 65مكرر5من قانون الإجراءات الجزائية الحصول على إذن قضائي للقيام بإجراءات التحري الخاصة أو عمليات المراقبة المذكورة سابقا، حيث يجب على ضابط الشرطة القضائية الحصول على إذن مكتوب مسبق من قبل وكيل الجمهورية أو قاضي التحقيق متى رأى وقدر ضرورة ذلك، [5] وأما عن المشرع الفرنسي فقد نظم هذا الشرط بموجب المادة 100- 1من ق ا ج ف، [6] حيث استلزمت هذه المادة أن يكون قرار قاضي التحقيق مكتوبا ومسببا أي أن يوضح فيه أن المراقبة استدعتها

1ينظر المادة 57من الدستور المصري لسنة 2019سالف الذكر.

2تنص المادة 47من التعديل الدستوري الجزائري لسنة 2020على:"لكل شخص الحق في حماية حياته الخاصة وشرفه.

لكل شخص الحق في سرية مراسلاته واتصالاته الخاصة في أي شكل كانت.

لا مساس بالحقوق المذكورة في الفقرتين الأولى والثانية إلا بأمر معلل من السلطة القضائية.

حماية الأشخاص عند معالجة المعطيات ذات الطابع الشخصي حق أساسي.

يعاقب القانون على كل انتهاك لهذه الحقوق".

3والتي تقابلها المادة 52فقرة 2من ق ا ج الأردني.

4ينظر المادتين 95و206من ق ا ج المصري سالف الذكر.

5ينظر المادة 65مكرر 5من ق ا ج الجزائري سالف الذكر.

6 Article n°100-1 modifié par loi n° 2019-222 du 23 mars 2019 –art 44 en vigueur le 01/06/2019, code de proc »dure pénale, dispose que : La décision prise en application de l’article 100 est motivée par référence aux éléments de fait et de droit justifiant que ces opérations sont nécessaires, Elle comporte tous les éléments d’identification de la liaison à intercepter, l’infraction qui motive le recours à l’interception ainsi que la durée de celle- ci ».

ضرورة التحقيق بمعنى أن تحديد الجناة وضبطهم أضحى مستحيلا أو على الأقل صعبا بوسائل التحري العادية أو التقليدية[1].

من استقرائنا لهاته النصوص القانونية نجد أن هاته التشريعات اشترطت وجوب الحصول على إذن من السلطة القضائية المختصة بالتحري والتحقيق وأن يكون هذا الإذن أو الأمر مسببا، إذ يعتبر التسبب وسيلة فعالة لتقييد السلطة التي أذنت به باعتبار أن هذه العمليات (اعتراض المراسلات وتسجيل الأصوات والتقاط الصور) تمس بالحريات والاتصالات الخاصة للأفراد ما يقتضي ضرورة مراقبتها من جهة قضائية أعلى من التي أصدرت الإذن، [2]وهذا ما نص عليه كل من المشرع المصري[3] والفرنسي صراحة في كل من دساتيرهم وقوانينهم الإجرائية، غير أن المشرع الجزائري لم يتطرق لمسألة تسبيب الإذن الصادر من السلطة القضائية بالرغم أن الدستور الجزائري لسنة 2016و2020أكد على عدم جواز المساس بسرية المراسلات والاتصالات الخاصة بكل أشكالها دون أمر معلل من السلطة القضائية وهنا يظهر التناقض بين ما جاءت به الدساتير المتعاقبة وبين ما هو منصوص عليه في ق ا ج ج، وهذا خلافا للمشرعين المصري والفرنسي، ولعل السبب في هذا التباين هو صدور تعديل قانون ا ج ج قبل صدور التعديل الدستوري وهذا ما يقتضي من المشرع تدارك هذا النقص وضبط المادة 65مكرر 5بما يتوافق مع ما جاء به الدستور الجديد.[4]

إضافة إلى هذا فقد اشترطت هاته التشريعات وجوب أن يتضمن الإذن الصادر مجموعة من العناصر الأساسية حيث تفاوتت هذه العناصر من مشرع لآخر، إذ نصت المادة 100 –1من ق ا ج ف على ضرورة شمول هذا الإذن كل العناصر التي تسمح بالتعرف على الاتصالات المطلوب التقاطها والأماكن المقصودة، وكذا الجريمة التي تبرر اللجوء إلى هذه التدابير، إضافة إلى المدة الزمنية لهذا الإذن والتي حددها بأربعة (04)أشهر قابلة للتجديد مع تحديد تاريخ بداية هذه العمليات ونهايتها، ولم يذهب المشرع الجزائري بعيدا عما قرره نظيره الفرنسي، حيث نص على نفس العناصر التي يجب أن يتضمنها الإذن طبقا

1أشرف عبد القادر قنديل، الوسائل الإلكترونية في الإثبات الجنائي، المرجع السابق، ص 224.

2رشيدة بوكر، الحماية الجزائية للتعاملات الإلكترونية، المرجع السابق، ص 323.

3وهذا ما قضت به محكمة النقض المصرية، إذ اعتبرت تسبيب الإذن الصادر بالمراقبة يقصد به اطلاع القاضي على التحريات التي أوردها الضابط في محضره وأفصح عن اطمئنانه عى كفايتها، بمعنى قد اتخذ القاضي من تلك التحريات أسبابا للإذن بالمراقبة، وهو ما أكد عليه المشرع الأردني في المادة 51فقرة 3من ق ا ج سالف الذكر الذي اشترطت أن يكون أمر الضبط أو إذن المراقبة أو التسجيل مسببا.

4جزول صالح، ضمانات مشروعية التصنت التلفوني واعتراض المراسلات في القانون الإجرائي الجزائري، المرجع السابق، ص 165.

لنص المادة 65مكرر7من ق ا ج ج[1] غير أنه لم يراع المشرع الجزائري العامل الزمني إذ لم يحدد عدد مرات قابلية هذا الإذن للتجديد، كما لم يرتب أي جزاء على مخالفة أحكام هذه المادة رغم أنه بدأها بعبارة "يجب" التي تفيد الإلزام وهذا ما يستدعي من المشرع تداركه في القريب العاجل، [2] أما عن المشرع المصري فلم يتضمن ق ا ج م البيانات التي يشملها الأمر بالمراقبة ولذلك يتم الرجوع للمبادئ العامة التي تحكم إجراءات التحقيق وبما لا يتعارض مع ذاتية وطبيعة المراقبة.[3]

2. يوجب قانون الإجراءات الجزائية على ضباط الشرطة القضائية تحرير محاضر بأعمالهم والتوقيع عليها مبينين من خلالها كافة الإجراءات التي قاموا بها في مرحلة البحث والتحري عن الجرائم، حيث أوجب المشرع المصري ضرورة تنظيم محضر يدون فيه جميع الإجراءات المتخذة وذلك في المادة 206من ق ا ج م بعبارة "...وتدون ملاحظاتهم عليها..."، ومن جهة أخرى تطرق المشرع الإماراتي إلى ضرورة تنظيم محضر بالعمليات التي يباشرها مأموري الضبط القضائي وذلك بموجب المادة 36من ق ا ج الإماراتي والتي تنص على أنه: "يجب أن تثبت جميع الإجراءات التي يقوم بها مأمور الضبط القضائي في محاضر موقع عليها من طرفهم يبين بها وقت اتخاذ الإجراءات ومكان حصولها...".[4]

وبالرجوع للمواد المنظمة لإجراءات التحري الخاصة وبالتحديد المادة 65مكرر9من قانون الإجراءات الجزائية [5] نجدها توجب على ضباط الشرطة القضائية المكلفين بالقيام بعمليات اعتراض المراسلات وتسجيل والتقاط الصوت والصورة بتحرير محاضر عن كل عملية يقومون بها حيث يشمل كل محضر تاريخ وساعة بداية العملية ونهايتها وكذا الظروف التي تمت فيها، كما يرفق بملف الدعوى محضر يتضمن وصفا أو نسخة من مضمون المراسلات المسجلة والصور والمحادثات المفيدة في إظهار الحقيقة وهذا ما

1- تنص المادة 65مكرر 7من ق ا ج ج على: "يجب أن يتضمن الإذن المذكور في المادة 65مكرر 5أعلاه، كل العناصر التي تسمح بالتعرف على الاتصالات المطلوب التقاطها والأماكن المقصودة سكنية أو غيرها والجريمة التي تبرر اللجوء إلى هذه التدابير ومدتها. يسلم الإذن مكتوب لمدة أقصاها أربعة(04)أشهر قابلة للتجديد حسب مقتضيات التحري أو التحقيق ضمن نفس الشروط الشكلية والزمنية. "

2فوزي عمارة، اعتراض المراسلات وتسجيل الأصوات والتقاط الصور والتسرب كإجراءات تحقيق قضائي في المواد الجزائية، المرجع السابق، ص 241.

3مصطفى طالب نعمة الجابري، استعمال كاميرات المراقبة بين التجريم والاباحة، رسالة مقدمة لنيل شهادة الماجستير في القانون العام، معهد العلمين للدراسات العليا، قسم القانون، العراق، سنة 2020، ص 85.

4مصطفى طالب نعمة الجابري، استعمال كاميرات المراقبة بين التجريم والاباحة، المرجع السابق، ص 87.

5- تنص المادة 65مكرر 9من ق ا ج ج على: "يحرر ضابط الشرطة القضائية المأذون له أو المناب من طرف القاضي المختص محضرا عن كل عملية اعتراض وتسجيل المراسلات وكذا عن عمليات وضع الترتيبات التقنية وعمليات الالتقاط والتثبيت والتسجيل الصوتي أو السمعي البصري.

يذكر بالمحضر تاريخ وساعة بداية هذه العمليات والانتهاء منها".

نصت عليه المادة 65مكرر10فقرة01من نفس القانون[1]، وما أكد عليه المجلس الدستوري الفرنسي في قراره الصادر بتاريخ 23مارس 2004، لتكون هذه المحاضر كدليل لتوجيه الاتهام ضد المشتبه فيه، [2] وعند الاقتضاء إذا كانت المكالمات التي تم اعتراضها والتسجيلات الصوتية أو السمعية البصرية بلغة أجنبية تتم ترجمتها بمساعدة مترجمين يتم تسخيرهم لهذا الغرض وذلك بموجب المادة 65مكرر10فقرة 02من قانون الإجراءات الجزائية[3]

3. تعتبر المراسلات و التسجيلات والصور التي تم تسجيلها والتقاطها بصدد التحري أو التحقيق في الجرائم المذكورة سابقا أدلة أصلية تفيد في إثبات هذه الجرائم ولهذا تقتضي الشرعية الإجرائية حفظها بطريقة خاصة بوضعها في أحراز مختومة بما يضمن عدم التلاعب بها أو العبث في الأشرطة المسجلة من حذف أو تغيير في الأصوات، [4] إلا أنه لم يبين المشرع الجزائري في النصوص المنظمة لهذه الإجراءات الخاصة كيفية حفظ هذه التسجيلات والنسخ التي ترفق بالملف، وفي هذا يتم الرجوع إلى الأحكام العامة في ق ا ج وتحديدا للمادة 45منه التي ينص من خلالها المشرع على أنه يتم غلق الأشياء والمستندات المتحصلة من الجرائم ويختم عليها، أو يتم وضعها في أكياس أو أوعية ويضع عليها ضابط الشرطة القضائية شريطا من الورق ويختم عليه بختمه، [5] ورغم هذا النص إلى أنه كان الأجدر من المشرع ج الأخذ

1تنص المادة 65مكرر 10من ق ا ج ج على: "يصف أو ينسخ ضابط الشرطة القضائية المأذون له أو المناب المراسلات أو الصور أو المحادثات المسجلة والمفيدة في إظهار الحقيقة في محضر يودع بالملف.

تنسخ وترجم المكالمات التي تتم باللغات الأجنبية عند الاقتضاء بمساعدة مترجم يسخر لهذا الغرض".

2 Article n°706-101 modifié par loi n°2016-731 du 03 juin 2016 –art 4 en vigueur du 05/06/2016 au 01/06/2019, code de procédure pénale, dispose que : Le procureur de la république, le juge d'instruction ou l'officier de police judiciaire requis en application des articles 706-96 et 706-96-1 décrit ou transcrit, dans procès-verbal qui versé au dossier, les images ou les conversation enregistrées qui sont utile à la manifestation de la vérité. Aucune séquence relative à la vie privée étrangère aux infractions vissées dans les décisions autorisant la mesure ne peut être conservée dans le dossier de la procédure.

Les conversations en langue étrangère sont transcrites en français avec l'assistance d'un interprète requis à cette fin ».

3- ينظر المادة 65مكرر 10من ق ا ج.

وتجدر الإشارة إلى أن المشرع الجزائري لم يحل إجراء إعداد محاضر هذه العمليات إلى المواد 94و95من ق ا ج ج المتعلقتين بالشروط الواجب توافرها في المحضر، وأيضا لم يحل إلى أحكام المادتين 91و92من ق ا ج ج المتعلقتين بالاستعانة بمترجم خاصة أن المادة 65مكرر 10فقرة 2من ق ا ج ج لم تشر إلى وجوب تحليف المترجم اليمين إذا لم يسبق له أداؤه.

4ليندا بن طالب، الدليل الإلكتروني ودوره في الإثبات الجنائي، المرجع السابق، ص 110.

5فوزي عمارة، اعتراض المراسلات وتسجيل الأصوات والتقاط الصور والتسرب كإجراءات تحقيق قضائي في المواد الجزائية، المرجع السابق، ص 244.

بعين الاعتبار خطورة هذه التسجيلات ومدى سريتها وإحاطتها بحماية خاصة كضمانة للحفاظ على حرمتها وبالتالي على مصلحة الفرد.

ولا بد من الإشارة أنه قد حددت بعض التشريعات المقارنة مصير هذه التسجيلات والنسخ المتحصل عليها نتيجة هذه العمليات، ومن بينها المشرع الفرنسي في المادة 706- 102من ق ا ج ف، [1] حيث أكد على ضرورة إتلاف هذه التسجيلات وإعدامها بعد انقضاء المدة المقررة لتقادم الدعوى العمومية، وهذا ما لم يفعله المشرع الجزائري إذ لم يبين مصير هذه التسجيلات والصور والمحادثات الملتقطة، [2] ولهذا يتعين عليه التنصيص عل ذلك لأن في هذا ضمانة لحماية مصلحة الأفراد في الحفاظ على خصوصياتهم بإعدامها بعد الانتهاء من استعمالها في الغرض الذي جمعت لأجله.

وعلاوة على ذلك يثار التساؤل عن من له الحق في الاطلاع على هذه التسجيلات والصور الملتقطة وبالرجوع للنصوص القانونية للتشريع الجزائري نجد أن المشرع قد خول لضباط الشرطة القضائية حق الاطلاع على مضمون التسجيلات أثناء عملية نسخها في محاضر وذلك بأنفسهم أو بتسخير خبير إذا كان الاطلاع عليها واستخلاص الدليل يقتضي خبرة فنية، وسواء كان ذلك في إطار تحقيق ابتدائي أو حالة تلبس بالجريمة أو الإنابة القضائية، وهذا لضمان عدم تحريف هذه التسجيلات أو إدخال أي مونتاج عليها، وكذلك الأمر بالنسبة للصور، كما رخص القانون للنيابة العامة والهيئة القضائية حق الاطلاع عليها على اعتبار أنها السلطة المخولة بمنح الإذن باتخاذ هذه العمليات، إلا أنه لم يشر صراحة إلى إمكانية عرض هذه التسجيلات والأدلة على المشتبه فيهم مثلما هو منصوص عليه في المادة 42من ق ا ج ج بصدد الجرائم العادية[3] ونحن نرى أنه حسن ما فعل المشرع الجزائري لأن هذه الإجراءات تتميز بالسرية التامة نظرا لخطورة الجرائم التي تتخذ بصددها ولذلك من الأحسن عدم عرضها على المشتبه فيهم.

4. الأصل أن تنصب إجراءات اعتراض المراقبة على الجرائم التي تبرر اللجوء إلى هذه التدابير والأشخاص الذين تضمن الإذن الإشارة إليهم دون غيرهم، غير أنه في بعض المرات يتم اكتشاف جرائم أخرى غير تلك الجرام المحددة سابقا والتي تجري بصددها عمليات المراقبة حيث يطلق عليها اسم

1Article n°706-102 création par loi n°2004-204 du 09 mars 2004 – art 1 JORF 10 mars 2004 en vigueur le 1 er octobre 2004, dispose que : Les enregistrements sonores ou audiovisuels sont détruits, à la diligence du procureur de la république ou du procureur général, à l'expiration du délai de prescription de l'action publique.
Il est dressé procès- verbal de l'opération de destruction ».

2جزول صالح، ضمانات مشروعية التصنت التلفوني واعتراض المراسلات في القانون الإجرائي الجزائري، المرجع السابق، ص 169.

3ليندا بن طالب، الدليل الإلكتروني ودوره في الإثبات الجنائي، المرجع السابق، ص 111.

"الجرائم العارضة"فقد قرر المشرع الجزائري بأن يتخذ الضابط بشأنها ما يراه مناسبا دون أن يكون ذلك سببا لبطلان هذه الإجراءات العارضة وهذا ما يستخلص من نص المادة 65مكرر 6فقرة 2من ق ا ج ج بقولها: "...إذا اكتشفت جرائم أخرى غير تلك التي ورد ذكرها في إذن القاضي، فإن ذلك لا يكون سببا لبطلان الإجراءات العارضة"، [1] وهذا ما أكدته الغرفة الجزائية بمحكمة النقض الفرنسية إذ أقرت بصحة الإجراءات في قرارها الصادر بتاريخ 21فيفري 1995وأطلقت عليه مصطلح "التنصت العارض Ecoute incidente".[2]

ويمكن أن نخلص في الأخير للقول أن هذه الإجراءات وإن كان لها دور كبير في الحد من الجرائم الخطيرة فهي في المقابل لها تأثير ومساس خطير بالحق في الخصوصية لذا كان على المشرع أن يقلل من حدة هذه الإجراءات وينص عليها في حدود ضيقة لضمان حماية أكبر لحق الخصوصية، كما أن مسألة مشروعية الأدلة المتحصل عليها من هذه العمليات لا زالت محل خلاف فقهي وقانوني كبير لذا سوف نتطرق لها بالتفصيل عند التطرق لمسألة ضبط الدليل الإلكتروني لاحقا.

المطلب الثاني: التسرب الإلكتروني

يعتبر أسلوب التسرب عملية ميدانية بالغة الخطورة تستخدم لمراقبة الأشخاص المشتبه في ارتكابهم للجريمة بصفة عامة (التسرب الكلاسيكي)، ونظرا لتطور الجريمة وظهور الجرائم الإلكترونية والمنظمة سارعت التشريعات إلى تكييف هذا الإجراء مع هاته التطورات واستحدث بذلك أسلوب التسرب الإلكتروني أو الرقمي الذي يستخدم للبحث عن دليل الجريمة داخل الشبكات الرقمية، ولما كان مفهوم التسرب لا يخرج عن كونه مراقبة فهو يحمل في طياته نوعا من التدخل في الحياة الخاصة للأفراد، ولذلك أحاطه المشرع بجملة من الشروط والضوابط التي تحد من تعسف السلطات المختصة في استعماله، وعليه سنحاول من خلال هذه الفروع معرفة المقصود بأسلوب التسرب بنوعيه الكلاسيكي والإلكتروني، وكذا الإشارة لأهم الضوابط التي وضعها المشرع لمباشرته.

الفرع الأول: مفهوم التسرب

يعد نظام التسرب إجراء من إجراءات التحري الخاصة التي أرستها معظم تشريعات العالم وقد كانت اتفاقية منظمة الأمم المتحدة المتعلقة بمكافحة الجريمة المنظمة سباقة إلى احتواء هذا الإجراء بنصها في المادة 20على أساليب التحري الخاصة بما فيها أسلوب التسرب، والذي عبرت عنه بمصطلح

1ينظر المادة 65مكرر 6فقرة 2من ق ا ج ج.

2ابراهيم يامة، أساليب التحري الخاصة بالجريمة المنظمة في القانونين الجزائري والفرنسي، المرجع السابق، ص 155.

"الأعمال المستترة"[1]، وأما عن المشرع الجزائري فقد تبنى هذا الإجراء عقب تصديق الجزائر على هذه الاتفاقية بموجب المرسوم الرئاسي رقم 02-05المؤرخ في 02/02/2002بتحفظ، واتفاقية مكافحة الفساد لسنة 2003المصادق عليها بتاريخ 19/04/2004.

ولقد ورد النص على هذا الأسلوب لأول مرة في الجزائر بمناسبة صدور القانون رقم 06-01المتعلق بالوقاية من الفساد ومكافحته عام 2006، تحت اسم "الاختراق"[2]وذلك في نص المادة 56منه: "من أجل تسهيل جمع الأدلة المتعلقة بالجرائم المنصوص عليها في هذا القانون يمكن اللجوء إلى التسليم المراقب وإتباع أساليب تحري خاصة كالترصد الإلكتروني أو الاختراق على النحو المناسب وبإذن من السلطة القضائية المختصة".[3]

ونظرا لغموض هذا النص بخصوص المقصود بالاختراق والتسرب وشروط وكيفيات مباشرتهما، بقيت هذه الإجراءات جامدة إلى غاية تعديل قانون الإجراءات الجزائية بموجب القانون رقم 06/22المؤرخ في 20/12/2006، أين تم تحديد معالم إجراء التسرب من خلال تعريفه وبيان شروطه وضوابطه، وذلك في المواد من 65مكرر 11إلى المادة 65مكرر 18من ق ا ج ج، أما عن المشرع الفرنسي فقد نظمه في المواد من 706-81إلى 706-87من ق ا ج الفرنسي، كما اعتمده المشرع المصري تحت اسم "الإرشاد الجنائي"[4]إذ أصدرت محكمة النقض المصرية عدة قرارات قضائية تبيح العمل مع المرشدين منها القرار الصادر في 09/06/1980الذي جاء فيه: "يستطيع مأمور الضبط أن يستعين بمعاونيه من رجال السلطة العامة أو

1جمال براهيمي، التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص 83.

2يعتبر كل من أسلوب التسرب والاختراق مصطلحين لهما نفس المدلول حيث اعتمد المشرع الجزائري تسمية هذا الإجراء بالاختراق في قانون مكافحة الفساد رقم 06-01في حين اعتمد تسمية "التسرب"في قانون الإجراءات الجزائية رقم 06-22الصادر في 20/12/2006.

3ينظر المادة 56من القانون رقم 06-01المؤرخ في 20/02/2006، المتعلق بالوقاية من الفساد ومكافحته سالف الذكر.

4يقصد بالإرشاد الجنائي تجنيد بعض عناصر الأمن للدخول مع جماعة إجرامية بصفتهم شركاء معهم في أنشطتهم الإجرامية من أجل الحصول على المعلومات التي تساعدهم في كشف الحقيقة والقبض على المجرمين، أما عن الإرشاد الجنائي عبر الإنترنت فيكون بتجنيد مأمور الضبط القضائي أو الغير للدخول إلى العالم الافتراضي عبر حلقات النقاش والدردشة والمواقع الإلكترونية مستخدمين في ذلك أسماء مستعارة لأشخاص أو هيئات مختلفة لعدم التعرف على هويتهم الحقيقية، وكما أشرنا فإن المرشد قد يكون أحد مأموري الضبط القضائي كما يمكن أن يكلف الضابط شخصا أخر من عامة الناس للقيام بهذه المهمة، ويشترط للقيام بعملية الارشاد الإلكتروني حصول المرشد على إذن من طرف سلطات التحقيق على أن يتضمن هذا الأخير رقم الحاسوب وصلاحيته للعمل، وخلوه من العوائق واحتوائه على برمجيات أصلية، فضلا عن ذكر أرقامها المتسلسلة ورقم وتاريخ الترخيص بها، وجهة إصدارها.

وبمجرد حصول المرشد على معلومات تفيده في إجلاء الحقيقة فإنه يسهر على توصيلها إلى جهات الضبط القضائي التي تكمل عملها من أجل القبض على المجرمين عن طريق الاستعانة بالوسائل التكنولوجية المتطورة كتتبع رقم البروتوكول IPالخاص بالحاسوب الذي يستخدمه المجرم. لمزيد من التفاصيل ينظر نبيلة هبة هروال، الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات، المرجع السابق، ص 195وما بعدها.

المرشدين السريين الذين يندسون بين المشتبه فيهم بقصد كشف الجرائم ومرتكبيها ولا يعيب الإجراءات أن تظل شخصية المرشد مجهولة.[1]

ويقصد بأسلوب التسرب حسب نص المادة 65مكرر12من ق ا ج ج، قيام ضابط أو عون الشرطة القضائية، تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية، بمراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة بإيهامهم أنه فاعل معهم أو شريك لهم أو خاف، وهو نفس التعريف الذي تبناه المشرع الفرنسي في المادة 706-81من ق ا ج الفرنسي.[2]

انطلاقا من هذا التعريف يتبين أن المشرع سمح لضابط الشرطة القضائية أو عون الشرطة بالتوغل داخل جماعة إجرامية وذلك تحت مسؤولية ضابط شرطة آخر مكلف بتنسيق عملية التسرب، بهدف مراقبة الجناة أو المشتبه فيهم وكشف أنشطتهم الإجرامية، وذلك بإيهامهم أنه فاعل أصلي أو شريك معهم أو خاف لمحصلات الجريمة، حتى يحظى بثقتهم من أجل الوصول إلى الحقيقة.

وفي سبيل الوصول لهذه الغاية سمح المشرع للمتسرب استعمال أساليب غير مشروعة، من إخفاء لهويته الحقيقية وانتحال هوية مستعارة، وكذا ارتكاب بعض الجرائم المنصوص عليها والمحددة في قانون إ ج في نص المادة 65مكرر 14من ق ا ج ج والتي تقابلها المادة 706-82من ق ا ج الفرنسي، والمتمثلة في حيازة أو نقل أو تسليم أو إعطاء مواد أو أموال أو منتوجات أو وثائق أو معلومات متحصل عليها من ارتكاب الجرائم أو مستعملة في ارتكابها، كما سمح للمتسرب وضع تحت تصرف مرتكبي هذه الجرائم الوسائل ذات الطابع القانوني أو المالي [3] وكذا وسائل النقل أو التخزين أو الإيواء أو الحفظ أو الاتصال، وذلك دون

1صالح شنين، التسرب في قانون الإجراءات الجنائية الجزائري حماية للنظام العام والحريات أم حماية للنظام العام، المجلة الجزائرية للقانون المقارن، المجلد 01، العدد 02، ديسمبر 2015، ص 120.

2 Article n° 706-81 de code de procédure pénale française:" Lorsque les nécessités de l'enquête ou de l'instruction concernant l'un des crimes ou délits entrants dans le champ d'application de l'article 706-73 le justifient , le procureur de la république, ou après avis de ce magistrat, le juge d'instruction saisi peuvent autoriser qu'il soit procédé, sous leurs contrôle respectif, a une opération d'infiltration dans les conditions prévues par la présente section.

L'infiltration consiste, pour un officier ou un agent de police judiciaire spécialement habilité dans des conditions fixées par décret et agissant sous la responsabilité d'un officier de police judiciaire chargé de coordonner l'opération, à surveiller des personnes suspectées de commettre un crime ou un délit en faisant passer, auprès de ces personnes, comme un des leurs, coauteurs, complices ou receleurs"

3يقصد بالوسائل ذات الطابع القانوني توفير الوثائق الرسمية للضابط المتسرب، مثل رخصة السياقة، بطاقة التعريف، جواز السفر، البطاقة الرمادية...الخ وكل ما يحتاج إليه في عملية التسرب، أما عن الوسائل ذات الطابع المالي فيقصد بها إمكانية استعمال الضابط المتسرب للأموال المتحصل عليها من ارتكاب الجرائم المنصوص عليها في هذا الفصل.

أن تشكل هذه الأفعال منه تحريضا على ارتكاب الجريمة، [1] وأن يكون تنفيذها عند الضرورة فقط وهذا ما يعني أنه لا يجوز اللجوء إلى أسلوب التسرب إلا في بعض الجرائم البالغة الخطورة والتي حددها المشرع الجزائري على سبيل الحصر في المادة 65مكرر 05، والمتمثلة في: جرائم المخدرات، الجريمة المنظمة، جرائم تبييض الأموال والإرهاب، الجرائم المتعلقة بالتشريع الخاص بالصرف، والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، [2] وخلاف للمشرع الجزائري فقد توسع المشرع الفرنسي في تحديد قائمة الجرائم التي من الممكن الترخيص فيها بعملية التسرب وذلك في المادة 706-73من ق ا ج الفرنسي. [3]

وعليه يتصور عملية التسرب في الجرائم الإلكترونية في ولوج ضابط أو عون الشرطة القضائية إلى العالم الافتراضي والمواقع الإلكترونية مثل مواقع التواصل الاجتماعي، ومشاركته في محادثات غرف الدردشة أو حلقات النقاش والاتصال مباشرة مع المشتبه فيهم، والظهور بمظهر الفاعل أو الشريك أو الخافي مستخدما في ذلك أسماء مستعارة لتجنب التعرف على هويته. [4] وتكون هذه المناقشة والحديث حول

1حيث تنص المادة 65مكرر 12فقرة 02من ق ا ج ج على: "...يسمح لضابط أو عون الشرطة القضائية أن يستعمل لهذا الغرض، هوية مستعارة وأن يرتكب عند الضرورة الأفعال المذكورة في المادة 65مكرر 14أدناه، ولا يجوز تحت طائلة البطلان أن تشكل هذه الأفعال تحريضا على ارتكاب جرائم"، ومما يستشف من نص المادة أنه قد سمح القانون للمتسرب استعمال هوية مستعارة وارتكاب بعض الجرائم ولكن دون أن يقوم بتحريض المشتبه فيهم على ارتكاب جرائم، والمقصود هنا التحريض البوليسي الذي يقوم به ضابط الشرطة من أجل اكتشاف سلوكيات إجرامية ليخلق بذلك جرائم أخرى، وهذا ما أدانته محكمة النقض المصرية حيث قضت "بأن تصرفات الضابط أثناء قيامه بالتحري والتحقيق في الجريمة يجب ألا تتجاوز الإجراءات المشروعة لكي تعتبر صحيحة ويعتبر الدليل المستمد منها صحيحا يعتد به أمام القضاء طالما أنه لم يتدخل في خلق جريمة أو التحريض عليها"، وفي قضية أخرى في الولايات المتحدة الأمريكية حيث قام ضابط من دائرة شرطة نيويورك بإنشاء موقع يسمح لمتصفحي الإنترنت بتبادل أرائهم حول الممارسات الاحتيالية التي تقع على البطاقات المصرفية، حيث كان الهدف من إنشائه ذلك الموقع هو جمع أدلة على ارتكاب الجرائم الإلكترونية الواقعة على البطاقات المصرفية وتحديد مرتكبيها، ولم يكن القصد تشجيعهم على ارتكابها، لذا اعتبر القضاء الفرنسي أن هذا النوع من المواقع لا يعد استفزازا أو تحريضا على ارتكاب الجرائم، وعلى ذلك استحدثت المحكمة العليا الأمريكية وسيلة للدفاع مستمدة من تقنية التحريض البوليسي والتي تستند إلى فكرتين: أولاهما تتمثل في منع الشرطة من اجتذاب مواطنين صالحين لارتكاب جرائم، والثانية هي احترام أخلاقيات المهنة لدى الشرطة القضائية حتى في مواجهة الجناة، إذ قال أحد القضاة في المحكمة العليا، بأن الحكومة يمكنها أن تضع طعما للقبض على المجرمين ولكن لا يمكنها خلق جريمة من أجل محاكمة مجرم. نقلا عن خضرة شنتير، الآليات القانونية لمكافحة الجريمة الإلكترونية، المرجع السابق، ص 136وما بعدها.

2ينظر المادة 65مكرر 05من ق ا ج ج.

3طبقا لنص المادة 706-73من ق ا ج الفرنسي فقد رخص المشرع الفرنسي لضباط الشرطة القضائية بالتسرب في الجرائم التالية: جرائم القتل المرتكبة من طرف عصابة منظمة، جرائم التعذيب والأعمال الوحشية المرتكبة من طرف عصابة منظمة، جنايات وجنح المتاجرة بالمخدرات، جنايات وجنح الخطف والاحتجاز المرتكبة من طرف عصابة منظمة، الجنايات والجنح المشددة في جريمة الدعارة، جرائم السرقة المرتكبة من طرف عصابة منظمة، جرائم الابتزاز، جنايات تخريب وهدم ملك من طرف عصابة منظمة، جنايات تزوير العملة، الجنايات والجنح التي تشكل أعمال إرهابية، الجنايات التي تمس بالمصالح الأساسية للأمة، جنح في مادة الأسلحة والمواد المتفجرة، جنح تبييض الأموال، جنح مساعدة الأشرار، جنايات خطف الطائرات والسفن، وكل وسيلة نقل أخرى المرتكبة من طرف عصابة منظمة، الجنايات المعاقب عليها بعشر سنوات سجن المتعلقة بانتشار أسلحة الدمار الشامل، استغلال أي منجم أو حيازة أي مادة دون رخصة استغلال أو ترخيص مصحوب باعتداء على البيئة مرتكب من طرف عصابة منظمة.

4نعيم سعيداني، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، المرجع السابق، ص 177.

كيفية صنع وبث الفيروسات وكذا عمليات القرصنة المختلفة، أو انخراطه في مجموعات ونوادي الهاكر، من أجل الحصول على أكبر قدر من المعلومات وكشف الأنشطة الإجرامية للمشتبه فيهم،[1] ومن بين القضايا التي تمت عن طريق التسرب داخل الفضاء الإلكتروني ما حققته المباحث الفيدرالية الأمريكية (FBI) حيث تمكنت من ضبط أفراد عصابة باستخدام أسلوب التسرب الرقمي أو الإلكتروني وذلك بزرع أحد ضباط الشرطة القضائية داخل المواقع الإلكترونية مما مكن من ضبط مجموعة من الأشخاص منشرين حول العالم يمتهنون عمليات قرصنة البرمجيات وتحميلها على المواقع عبر الإنترنت، محققين بذلك أرباحا وصلت إلى مليون دولار في فترة وجيزة.[2]

وخلافا للمشرع الجزائري فإن المشرع الفرنسي بالرغم من تكريسه لأسلوب التسرب الكلاسيكي الذي يسمح بسريان نصه على التسرب الذي يتم عبر شبكة الإنترنت، إلا أنه حرص على مكافحة الجرائم التي تتم بطريق الاتصالات الإلكترونية بشدة واستحدث لذلك أسلوب جديد أطلق عليه "التحقيق تحت اسم مستعار"وذلك بموجب المادة 706-87-1من ق ا ج المعدلة بموجب المادة 11من القانون 2015-993المتعلق بتكييف قانون الإجراءات الجزائية الفرنسي مع قانون الاتحاد الأوروبي، حيث أجاز بموجبها _وفي الجرائم المحددة في المادة 706-73من ق ا ج، متى ارتكبت بوسائل إلكترونية_

لضباط الشرطة القضائية استعمال هذه التقنية والدخول للعالم الرقمي بأسماء وهويات مستعارة.[3]

وتجدر الإشارة إلى أن هذه التقنية (التسرب الإلكتروني) قد سبق تطبيقها من قبل ضباط الجمارك بهدف مراقبة حركة التبادلات التجارية وغيرها داخل البيئة الرقمية والتثبت من الجرائم المرتكبة بداخلها أو عبرها.[4]

الفرع الثاني: الضوابط التي تحكم عملية التسرب في الجرائم الإلكترونية

نظرا لخطورة هذا الإجراء على الحياة الخاصة للأفراد فقد أحاطه المشرع بجملة من الضوابط والشروط الواجب مراعاتها تماشيا ومبدأ الشرعية الإجرائية، والتي تعتبر ضمانات قانونية لعدم تعسف سلطات التحري والتحقيق في اتخاذ هذا الإجراء، تتمثل فيما يلي:

أولا: الضوابط الموضوعية

1جمال براهيمي، التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص 85.

2خضرة شنتير، الآليات القانونية لمكافحة الجريمة الإلكترونية، المرجع السابق، ص 134.

3رشيدة بوكر، الحماية الجزائية للتعاملات الإلكترونية، المرجع السابق، ص 310.

4Michel Mercier, Rapport n° 491 de fait au nom de la commission des lois, déposé le 23 mars 2016, p 161.

1. لقد حصر المشرع الجزائري حالات اللجوء إلى أسلوب التسرب وهذا ما يستخلص من نص المادة 65مكرر 11من ق ا ج ج حيث أجازت اللجوء لهذا الأسلوب في حالة ما اقتضت ذلك ضرورات التحري أو التحقيق في إحدى الجرائم المبينة في نص المادة 65مكرر 5من ذات القانون، [1] والجرائم المنصوص عليها في المادتين 706-73و706-37-1من ق ا ج الفرنسي المشار إليها سابقا، [2] إلا أن المشرع الفرنسي وخلافا للمشرع الجزائري قد وسع من نطاق التحقيق تحت اسم مستعار إلى حد كبير متجاوزا بذلك ما شمله أسلوب التسرب الكلاسيكي في المادة سابقة الذكر (706-73)، وذلك بعد صدور قانون 17أوت 2015المتعلق بتكييف قانون الإجراءات الجزائية الفرنسي مع قانون الاتحاد الأوروبي، حيث حدد هذه الجرائم التي ترتكب بواسطة وسائل الاتصالات الإلكترونية في المواد 706-72و706-73من ق ا ج الفرنسي، [3] وتشمل الجرائم الماسة بنظم المعالجة الآلية للمعطيات المنصوص عليها في المادة 323-1إلى 323-4-1من قانون العقوبات الفرنسي، وجريمة تدمير أو إتلاف أو تحويل أي وثيقة أو معدات أو أدوات أو تركيبات أو أجهزة تقنية أو نظام المعالجة الآلية المنصوص عليها في المادة 411-9من قانون العقوبات الفرنسي، إضافة لجرائم الإتجار بالمخدرات، السرقة المرتكبة في إطار جماعة منظمة، تبييض الأموال في إطار جماعة منظمة، تزوير العملات، الأفعال الإرهابية، الاحتيال في إطار جماعة منظمة، الاعتداء على نظم المعالجة الآلية للمعطيات ذات الطابع الشخصي التي تنفذها الدولة المرتكبة في إطار جماعة منظمة، والمنصوص عليها في المادة 323-4-1من قانون العقوبات الفرنسي. [4]

وعلى اعتبار الجريمة الإلكترونية إحدى تلك الجرائم فإنه يجوز التسرب فيها إذا فرضت ذلك ضرورة التحري أو التحقيق فيها، وأثبتت الجهة القائمة بالتسرب عدم نجاعة الأساليب العادية للتحري وجمع الأدلة، وإلا لا يمكن اتخاذ هذا الأسلوب متى كانت أساليب التحري والأدلة كافية وإلا عد ذلك تعسفا من طرف القائم به ومن طرف السلطة التي منحت الإذن بمباشرته، فالتسرب الذي لا يلتمس من حصوله فائدة في إظهار الحقيقة يعد تسربا تحكميا. [5]

1تنص المادة 65مكرر 11من ق ا ج ج على: "عندما تقتضي ضرورات التحري أو التحقيق في إحدى الجرائم المذكورة في المادة 65مكرر 5أعلاه، يجوز لوكيل الجمهورية أ لقاضي التحقيق بعد إخطار وكيل الجمهورية، أن يأذن تحت رقابته حسب الحالة بمباشرة عملية التسرب ضمن الشروط المبينة في المواد أدناه".

2ينظر المواد 706-73و706-73- 1من ق ا ج الفرنسي المشار إليها سابقا.

3رشيدة بوكر، الحماية الجزائية للتعاملات الإلكترونية، المرجع السابق، ص 311 – 312.

4ينظر المواد 706-72و706-73من ق ا ج الفرنسي.

5خضرة شنتير، الآليات القانونية لمكافحة الجريمة الإلكترونية، المرجع السابق، ص 135.

2. تتطلب عملية التسرب أن يكون القائم بها ضابطا أو عونا للشرطة القضائية كما جاء في نص المادة 65مكرر 12من ق ا ج ج[1]، كما يجب أن يكون هذا الضابط مؤهلا للقيام بهذه العملية وله من الكفاءة والخبرة والذكاء بحيث يستطيع كسب ثقة المشتبه فيهم، وهذا ما أغفله المشرع الجزائري بخلاف المشرع الفرنسي في المادة 706-81، [2] حيث نص المشرع الفرنسي على أن يكون القائم بعملية التسرب أو كما أطلق عليه التحقيق تحت اسم مستعار، من الضباط أو الأعوان المكلفين بخدمة خاصة، إذ يخضع هؤلاء الضباط لتكوين خاص بعد أخذ الإذن من وكيل الجمهورية، وقد حدد القرار رقم 21أكتوبر 2015[3] المتعلق بالتفويض في الخدمات الخاصة للضباط الشرطة القضائية وأعوانهم هذه الخدمات والتي تعنينا هي الخدمات والوحدات التابعة للإدارة المركزية للشرطة القضائية والتي تتفرع عنها الإدارة الفرعية لمكافحة الجرائم الإلكترونية، [4] إضافة لهذا فإن المشرع الجزائري قد نص في المادة 65مكرر 14من ق ا ج ج على إمكانية تسخير أشخاص من غير ضباط وأعوان الشرطة القضائية للقيام بعمليات التسرب التقنية غير أنه لم يبين طبيعة هؤلاء الأشخاص ولا الجهة التي يسخرون من طرفها ولا مدى التزامهم بسرية هذه العمليات وهذا ما يجب تداركه باعتبار هذه العمليات تمس بالحياة الخاصة للأفراد، [5] كما أنه نتيجة أن أغلب الضباط وأعوان الشرطة معروفين لدى الأوساط الإجرامية قد ينذر هذا بفشل عملية التسرب وتعريض المتسرب للخطر خاصة في الجرائم التقليدية في حين تعتبر نسبة نجاح عملية التسرب كبيرة في الجرائم الإلكترونية التي يتم فيها التسرب داخل العالم الافتراضي وبأسماء وصفات وهمية.

كما لا يفوتنا أن ننوه بأنه وطبقا لما نص عليه المشرع الجزائري فإنه يباشر هؤلاء الضباط عملية التسرب بدائرة اختصاصهم التي يباشرون فيها وظائفهم المعتادة، إلا أنه ونظرا للطابع العابر للحدود للجريمة الإلكترونية وإمكانية ارتكابها في أي مكان فقد سمح المشرع بتمديد الاختصاص الإقليمي لهؤلاء ليشمل كافة التراب الوطني وهذا خلافا للمشرع الفرنسي الذي أجاز القيام بعملية التسرب خارج التراب

1ينظر المادة 65مكرر 12من ق ا ج ج.

2ابراهيم يامة، أساليب التحري الخاصة بالجريمة المنظمة في القانونين الجزائري والفرنسي، المرجع السابق، ص 151.

3 Arrêt du 21 Octobre 2015, publié au journal officiel du 29 octobre 2015, relatif à l'habilitation au sein de services spécialisés d'officiers ou agents de police judiciaire pouvant procéder aux enquêtes sous pseudonyme.

4رشيدة بوكر، الحماية الجزائية للتعاملات الإلكترونية، المرجع السابق، ص 311.

5يزيد بوحليط، الجرائم الإلكترونية والوقاية منها في القانون الجزائري، المرجع السابق، ص 386.

الوطني كما سمح بإمكانية مباشرتها من قبل عناصر الأمن التابعة لدول خرى على أرضه وفقا لاتفاقيات وإجراءات خاصة.[1]

3. نظرا لخطورة عملية التسرب على حياة القائم بها فقد أحاطه المشرع بجملة من الضمانات والتدابير القانونية التي تحول دون المساس به وتكفل له الحماية اللازمة، إذ جعله بمنأى عن تحمل المسؤولية الجزائية عن الجرائم التي يرتكبها أثناء عملية التسرب حسب ما ورد في المادة 65مكرر 14من ق ا ج ج[2] ونص المادة 706-82من ق ا ج ف[3]، وأوجب الالتزام بالسرية التامة وعدم الكشف عن هوية المتسرب الحقيقية وسمح له بأخذ هوية مستعارة وهو ما أوضحته المادة 65مكرر 16من ق ا ج ج بقولها: "لا يجوز إظهار الهوية الحقيقية لضباط أو أعوان الشرطة القضائية الذين يباشرون عملية التسرب تحت هوية مستعارة في أي مرحلة من مراحل الإجراءات..."، رغم أن مسألة إعطاء المتسرب هوية مستعارة يعتريها الكثير من المخاطر والصعوبات في وقتنا الحالي، خاصة مع التقدم التكنولوجي الذي نشهده إذ أصبح لكل مواطن رقما إلكترونيا خاصا به، أو وثيقة بيو مترية تحدد هويته.[4]

وحرصا من المشرع على حماية العون المتسرب فرض جزاءات جنائية على كل من يكشف هويته بالحبس من سنتين (2) إلى خمس (5) سنوات وبغرامة من 50.000دج إلى 200.000دج، وإذا ما تسبب هذا الكشف عن الهوية لأي أعمال عنف أو ضرب لهؤلاء الضباط أو لأفراد عائلتهم فتضاعف العقوبة لتصبح الحبس من خمس (5) سنوات إلى عشر (10) سنوات وبغرامة من 200.000دج إلى 500.000دج، وفي حالة ما تسبب هذا الكشف في وفاة هؤلاء الأشخاص فتكون العقوبة الحبس من عشر (10) سنوات

1بالرجوع لاتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة وفي مادتها 20بعنوان أساليب التحري الخاصة نصت على وجوب أن تقوم كل دولة طرف ضمن حدود إمكانياتها ووفقا للشروط المنصوص عليها في قانونها الداخلي إذا كانت المبادئ الأساسية لنظامها الداخلي تسمح بذلك، باتخاذ ما يلزم من تدابير وكذلك ما تراه مناسبا من استخدام أساليب تحري خاصة مثل المراقبة الإلكترونية أو غيرها من أشكال المراقبة والعمليات المستترة، من جانب سلطتها المختصة داخل إقليمها لغرض مكافحة الجريمة المنظمة مكافحة فعالة، وتشجيعا للدول الأطراف على أن تبرم عند الاقتضاء اتفاقيات وترتيبات ملائمة ثنائية أو متعددة الأطراف لاستخدام هذه الأساليب الخاصة، لمزيد من التفاصيل راجع اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة، التي اعتمدت وعرضت للتوقيع والتصديق بموجب قرار الجمعية العامة للأمم المتحدة الدورة الخامسة والعشرون (25) في 15نوفمبر 2000.

2تنص المادة 65مكرر 14من ق ا ج ج على: "يمكن ضباط وأعوان الشرطة القضائية المرخص لهم بإجراء عمليات التسرب والأشخاص الذين يسخرونهم لهذا الغرض دون أن يكونوا مسؤولين جزائيا...".

3Article n° 706-82 de code de procédure pénal :" Les officiers ou agents de police judiciaire autorisés à procéder à une opération d'infiltration peuvent, sur l'ensemble du territoire national, sans être pénalement responsables de ces acte…"

4خضرة شنتير، الآليات القانونية لمكافحة الجريمة الإلكترونية، المرجع السابق، ص 136.

إلى عشرين (20) سنة والغرامة من 500.000دج إلى 1.000.000دج طبقا لما جاء في نص المادة 65مكرر 16من ق ا ج ج والمادة 706-84من ق ا ج ف.[1]

كما لا يجوز سماع الضابط أو العون المتسرب كشاهد على العملية وهذا من باب الحماية غير المباشرة له، إذ يتم سماع الضابط المنسق الذي جرت عملية التسرب تحت مسؤوليته بدلا من الضابط أو العون المتسرب حسب ما جاء في نص المادة 65مكرر 18من ق ا ج ج[2] والمادة 706-86من ق ا ج ف[3]، كما أضافت المادة 706-61من ق ا ج ف على أنه في حالة إصرار المتهم على مواجهة العون المتسرب شخصيا فإنه يتم ذلك بالاستعانة بوسائل تقنية متطورة تساعد في إخفاء صوت المتسرب وسماعه عن بعد وهذا ما لم ينص عليه المشرع الجزائري.[4]

ثانيا: الضوابط الشكلية

1. لضمان صحة عملية التسرب نصت جل التشريعات على ضرورة حصول الضابط المتسرب على إذن من طرف الجهات القضائية المختصة، وهذا ما جاءت به المادة 65مكرر 11من ق ا ج ج والتي تقابلها المادة 706-81من ق ا ج الفرنسي، إذ يقوم وكيل الجمهورية أو قاضي التحقيق بإصدار إذن بمباشرة عملية التسرب، [5] حيث اشترط المشرع ضرورة حصول الضابط المتسرب على الإذن من وكيل الجمهورية أو من طرف قاضي التحقيق بعد إخطار وكيل الجمهورية في إطار الإنابة القضائية، على أن تباشر هذه العملية تحت رقابة وإشراف كل منهما، وهذا ما يعد ضمانا لمشروعية الدليل المستمد من هذا الإجراء.

ويشترط أن يصدر هذا الإذن بناء على تقرير يحرره ضابط الشرطة القضائية المكلف بتنسيق عملية التسرب مضمنا إياه كافة العناصر الضرورية لمعاينة الجريمة في ظروف تؤمن عدم تعرض الضابط أو العون المتسرب للخطر، [6] وحتى يكون هذا الإذن قانونيا ضمنه المشرع بجملة من الشروط القانونية، طبقا

1ينظر المادة 65مكرر 16من ق ا ج ج التي تقابلها المادة 706-84من ق ا ج ف.

2تنص المادة 65مكرر 18من ق ا ج ج على: "يجوز سماع ضابط الشرطة القضائية الذي يجري عملية التسرب تحت مسؤوليته دون سواه بوصفه شاهدا عن العملية".

3Article n° 706-86 de code de procédure pénale :" L'officier de police judiciaire sous la responsabilité duquel se déroule l'opération d'infiltration peut seul être entendu en qualité de témoin sur l'opération…"

4وهيبة رابح، الإجراءات المتبعة أمام الأقطاب الجزائية المتخصصة، المرجع السابق، ص 252.

5ينظر المادة 65مكرر 11من ق ا ج ج والتي تقابلها المادة 706-81من ق ا ج الفرنسي المشار إليهما سابقا.

6تنص المادة 65مكرر 13من ق ا ج ج على: "يحرر ضابط الشرطة القضائية المكلف بتنسيق عملية التسرب تقريرا يتضمن العناصر الضرورية لمعاينة الجرائم غير تلك التي قد تعرض للخطر أمن الضابط أو العون المتسرب وكذا الأشخاص المسخرين طبقا للمادة 65مكرر 14أدناه".

لنص المادة 65مكرر 15من ق ا ج ج، إذ يتوجب أن يكون الإذن مكتوبا ومسببا وذلك تحت طائلة البطلان،[1] فيعد التسبيب كافي للدلالة على أن الإذن مكتوب مما يؤدي إلى استبعاد الإذن الشفوي، كما أن الإذن المسبب يتيح للقاضي تقدير صحة الإذن بعملية التسرب وتقرير بطلانه في حالة مخالفته لهذه الشروط، [2] وذلك أنه يتضمن كل الحيثيات والعناصر التي أقنعت الجهات المختصة لمنح الإذن والأسباب التي دفعت الضابط المتسرب إلى اللجوء لهذا الإجراء، [3] ومن جهة ثانية يجب أن يذكر في الإذن الجريمة التي تبرر اللجوء إلى هذا الإجراء، أي إحدى الجرائم المذكورة سابقا من بينها الجريمة الإلكترونية، وكذا هوية الضابط الذي تتم العملية تحت مسؤوليته من اسم ولقب، الرتبة، الصفة، وكذا المصلحة التي ينتمي إليها، وكذا مدة عملية التسرب، وبدوره المشرع الفرنسي نص على ضرورة توافر هذه الشروط، وذلك بموجب المادة 706-83 -1ق ا ج الفرنسي المشار إليها سابقا.[4]

2. حدد المشرع الجزائري والفرنسي المدة المطلوبة لعملية التسرب بموجب المواد 65مكرر 15من ق ا ج ج و706-83ق ا ج الفرنسي، بحيث لا يمكن أن تتجاوز مدة التسرب أربعة (04) أشهر، قابلة للتجديد حسب مقتضيات التحري والتحقيق وبنفس الشروط الشكلية والموضوعية والزمنية، وفي نفس الوقت يجوز للقاضي الذي رخص بإجراء التسرب أن يأمر في أي وقت بوقفه قبل انقضاء المدة المحددة لذلك، وفي هذه الحالة أو في حالة انقضاء المهلة المحددة في رخصة التسرب وفي حالة عدم تمديدها يمكن للعون أو الضابط المتسرب مواصلة العملية للوقت الكافي لتوقيف عمليات المراقبة في ظروف تضمن أمنه.[5]

3. من المعلوم أنه بعد الانتهاء من أي إجراء يقوم ضابط الشرطة القضائية بتحرير محضر بالعملية التي قام بها ويقوم بإحالته إلى وكيل الجمهورية أو قاضي التحقيق، ومن خلال النصوص المنظمة لعملية التسرب نلاحظ أن المشرع الجزائري وكذا الفرنسي لم يشيرا إلى ما إذا كان ضابط الشرطة القضائية المسئول عن تنسيق هذه العملية يقوم بتحرير محضر حول نشاط المتسرب، ولا إلى مصير الأدلة المتحصل عليها نتيجة عملية التسرب، [6] فكل ما أشارا إليه هو إيداع الإذن أو الرخصة التي تم بها

1ينظر المادة 65مكرر 15من ق ا ج ج، والتي تقابلها المادة 706-83من ق ا ج الفرنسي.

2فوزي عمارة، اعتراض المراسلات وتسجيل الأصوات والتقاط الصور والتسرب كإجراءات تحقيق قضائي في المواد الجزائية، المرجع السابق، ص 248.

3حمزة قريشي، الوسائل الحديثة للبحث والتحري في ضوء قانون 06/22، المرجع السابق، ص78.

4ينظر المادتين 65مكرر 15من ق ا ج ج و706-83ق ا ج الفرنسي سالفتي الذكر.

5ينظر المادة 65مكرر 17من ق ا ج ج والتي تقابلها المادة 706-85من ق ا ج الفرنسي.

6كما لم يشر المشرع الجزائري إلى موقف القانون من الجرائم التي يتم اكتشافها عرضا أثناء مباشرة عملية التسرب، فقد يكتشف المتسرب جرائم أخرى غير الجريمة محل التسرب وهنا باعتبار قانون الإجراءات الجزائية لم يتعرض لهذه النقطة وإنما بالرجوع للأحكام المتعلقة باعتراض المراسلات وتسجيل الأصوات والتقاط الصور وفي المادة 65مكرر 06منه فإنه إذا ما اكتشف الضابط جرائم أخرى فإنه يتخذ بشأنها

تنفيذ العملية في ملف الإجراءات بعد الانتهاء من العملية طبقا لما جاء في الفقرة السادسة (06) من المادة 65مكرر 15من ق ا ج ج[1]، والفقرة الرابعة (04) من المادة 706-83من ق ا ج ف.[2]

المبحث الثاني: إجراءات البحث والتحري المستحدثة وفقا للقوانين الإجرائية الخاصة

قد خلصنا من الفصل السابق إلى عدم كفاية الإجراءات التقليدية لاستيعاب كافة أشكال الجريمة الإلكترونية، وهذا ما دفع المشرع الإجرائي إلى استحداث أساليب تحري جديدة تتلاءم وخصوصية هذه الجرائم، إذ لم يكتف باستخدام هذه الأساليب عند وقوع الجريمة وإنما حتى قبل وقوعها، باعتبارها إجراءات وقائية تهدف للوقاية من خطر الجريمة الإلكترونية قبل وقوعها، كأسلوب المراقبة الإلكترونية للاتصالات، وكذا تفتيش المنظومة المعلوماتية وحجز المعطيات المتحصل عليها والتي تفيد في إثبات الجريمة، وهذا كله بموجب قوانين خاصة ترجمت السياسة الإجرائية الوقائية التي اعتمدتها أغلب تشريعات الدول، وعليه سنتطرق لكل إجراء من حيث تعريفه وشروط وضوابط مباشرته، وكذا الصعوبات التي تعترض إجراءات ضبط الدليل الإلكتروني.

المطلب الأول: مراقبة الاتصالات الإلكترونية

تعتبر المراقبة (La Surveillance)من أهم مصادر التحري التي يستعان بها في بحث وتقصي مختلف الجرائم التقليدية منها والمستحدثة، وتعرف المراقبة الالكترونية (La Cyber surveillance)[3]على أنها عمل أمني أساسي له نظام معلومات إلكتروني يقوم به المراقب بواسطة الأجهزة الإلكترونية وعبر شبكة الإنترنت لتحديد غرض محدد وإفراغ النتيجة في ملف إلكتروني،[4] وقد تم استحداث هذا الإجراء كنتيجة لضعف وسائل الرقابة التقليدية في تتبع ورصد الجريمة الإلكترونية والتي

...=ما يراه مناسبا دون أن يكون ذلك سببا لبطلان هذه الإجراءات العارضة، وعلى هذا يمكن في تقديرنا الأخذ بهذا المبدأ وتطبيقه على عملية التسرب، إذا ما اكتشف العون المتسرب جرائم أخرى فإن ذلك لا يكون سببا لبطلان إجراء التحري عن الجريمة، أنظر فوزي عمارة، اعتراض المراسلات وتسجيل الأصوات والتقاط الصور والتسرب كإجراءات تحقيق قضائي في المواد الجزائية، المرجع السابق، ص 250.

1تنص المادة 65مكرر15في فقرتها الأخيرة على:"...تودع الرخصة في ملف الإجراءات بعد الانتهاء من عملية التسرب".

2Article n° 706-83 de code de procédure pénale : "L'autorisation est versée au dossier de la procédure après achèvement de l'opération d'infiltration."

3La Cyber surveillance :est la surveillance des réseaux de télécommunication. Elle implique également la vidéosurveillance, le web Cam dans les lieux public ou dans le cadre plus rétreint des entreprise. Et elle est un monde de preuve

نقلا عن نبيلة هبة هروال، الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات، المرجع السابق، ص 198.

4عبد القادر فلاح، التحقيق الجنائي للجرائم الإلكترونية وإثباتها في التشريع الجزائري، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، المجلد 04، العدد 02، 2019، ص 1699.

تتسم بطبيعتها الخاصة، إذ نجد أغلب التشريعات قد كرست أسلوب المراقبة الإلكترونية ضمن قوانينها الإجرائية العامة والخاصة، وهذا ما سنتطرق له في الفرع الأول من هذا المطلب، في حين سنعالج في الفرع الثاني مسألة مشروعية هذا الإجراء كونه يعتبر من الإجراءات الخطيرة التي تمس خصوصية الأفراد.

الفرع الأول: تعريف أسلوب المر اقبة الإلكترونية

أقرت اتفاقية بودابست نظام المراقبة إ في المادة 21منها تحت عنوان "اعتراض معطيات المحتوى"Interception de données relatives au contenuحيث ألزمت كل دولة طرف فيها ضرورة تبني جملة من الإجراءات من أجل تخويل هيئاتها وأجهزتها القضائية المختصة سلطة اتخاذ أسلوب مراقبة المعطيات المتعلقة بمحتوى الاتصالات والمنقولة عن طريق الأنظمة المعلوماتية، وتجميعها وتسجيلها عن طريق الوسائل الفنية المتوفرة[1]كما عالجت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات هي الأخرى اعتراض الاتصالات الإلكترونية ومراقبتها تحت عنوان "اعتراض معلومات المحتوى" وذلك بموجب نص المادة 29من هذه الاتفاقية.[2]

كما تبنى المشرع ج مصطلح المراقبة إ كغيره من التشريعات المقارنة الذي استمدته من نص الاتفاقية المتعلقة بمكافحة الجريمة المنظمة عبر الحدود الوطنية والتي سنتها منظمة الأمم المتحدة في إطار مكافحة الجريمة المنظمة، حيث نصت المادة 20من هذه الاتفاقية على أنه: "تقوم كل دولة طرف

1إذ تنص المادة 21من اتفاقية بودابست على ما يلي: "يجب على كل طرف أن يتبنى الإجراءات التشريعية وأية إجراءات أخرى يرى أنها ضرورية من أجل تخويل سلطاته المختصة سلطة فيما يتعلق بالجرائم الخطيرة التي يحددها القانون الداخلي، المكنات التالية:

أ. جمع أو تسجيل عن طريق تطبيق الوسائل الفنية المتواجدة على أرضه.

ب. إلزام مقدم الخدمات في نطاق قدراته الفنية المتوافرة على:

أن يجمع أو يسجل عن طريق تطبيق وسائل فنية موجودة على أرضه، أو أن يمنح السلطات المختصة عونه ومساعدته من أجل تجميع أو تسجيل، في الوقت الفعلي المعطيات المتعلقة بمحتوى اتصالات معينة على أرضه، منقولة عن طريق نظام معلوماتي...".

ينظر بوكر رشيدة، جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري والمقارن، منشورات الحلبي الحقوقية، ط1، لبنان، 2012، 367.

2إذ تنص المادة 29من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات على:"تلتزم كل دولة طرف بتبني الإجراءات التشريعية والضرورية فيما يختص بسلسلة من الجرائم المنصوص عليها في القانون الداخلي، لتمكين السلطات المختصة من:

أ. الجمع أو التسجيل من خلال الوسائل الفنية على إقليم الدولة الطرف أو،

ب. التعاون ومساعدة السلطات المختصة في جمع أو تسجيل معلومات المحتوى بشكل فوري للاتصالات المعنية في إقليمها والتي تثبت بواسطة تقنية المعلومات.

ت. إذا لم تستطع الدولة الطرف بسبب النظام القانوني الداخلي تبني الإجراءات المنصوص عليها في الفقرة (1-أ) فيمكنها تبني إجراءات أخرى بالشكل الضروري لضمان الجمع والتسجيل الفوري لمعلومات المحتوى المرافقة للاتصالات المعنية في إقليمها باستخدام الوسائل الفنية في ذلك الإقليم.

ث. تلتزم كل دولة طرف باتخاذ الإجراءات الضرورية لإلزام مزود خدمة بالاحتفاظ بسرية أي معلومة عند تنفيذ الصلاحيات المنصوص عليها في هذه المادة". من كتاب يزيد ص 434

ضمن حدود إمكانيتها وفقا للشروط المنصوص عليها في قانونها الداخلي، إذا كانت المبادئ الأساسية لنظامها القانوني الداخلي تسمح بذلك، باتخاذ ما يلزم من تدابير لإتاحة الاستخدام المناسب لأسلوب التسليم المراقب، وكذلك ما تراه مناسبا من استخدام أساليب تحري خاصة أخرى، مثل المراقبة الإلكترونية أو غيرها من أشكال المراقبة"، [1] وهذا ما أكد عليه المشرع الجزائري بموجب المادة 03ن القانون رقم 09-04المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها بنصها على: "مع مراعاة الأحكام القانونية التي تضمن سرية المراسلات والاتصالات يمكن لمقتضيات حماية النظام العام أو لمستلزمات التحريات أو التحقيقات القضائية الجارية، وفقا للقواعد المنصوص عليها في قانون الإجراءات الجزائية وفي هذا القانون، وضع ترتيبات تقنية لمراقبة الاتصالات الإلكترونية وتجميع وتسجيل محتواها في حينها والقيام بإجراءات التفتيش والحجز داخل منظومة معلوماتية".[2]

وفي هذا الإطار نجد اتفاقية بودابست ميزت بين نوعين من المعطيات المعلوماتية محل الاعتراض: المعطيات المتعلقة بالمرور والمعطيات المتعلقة بمحتوى الاتصال، فبالنسبة للنوع الأول فقد عرفتها بموجب المادة 1فقرة 4منها على أنها: "كل البيانات التي تعالج الاتصالات التي تمر عن طريق نظام معلوماتي والتي يتم إنتاجها بواسطة هذا النظام المعلوماتي بوصفه عنصرا في سلسلة الاتصال، مع تعيين المعلومات التالية: أصل الاتصال، مقصد الاتصال أو الجهة المقصودة بالاتصال، خط السير، ساعة وتاريخ الاتصال، حجم وفترة الاتصال أو نوع الخدمة، أما بالنسبة للنوع الثاني المعطيات المتعلقة بالمحتوى فلم تعرفها الاتفاقية لكن تشير إلى المحتوى الإخباري للاتصال أي مضمون الاتصال أو الرسالة وفقا لنص المادة 21من هذه الاتفاقية، ونظرا لاختلاف هاذين النوعين من المعطيات فقد أكدت اتفاقية بودابست على التمييز بينها حيث أدرجت كل إجراء على حدا تحت عنوان خاص، فخصت تجميع حركة المعطيات بعنوان "التجميع في الوقت الفعلي لمعطيات المرور" Collecte en temps real des données relative au traficالمنصوص عليها بموجب المادة 20من الاتفاقية، [3] وتجميع محتوى المعطيات فجاء تحت

1بن بادة عبد الحليم، المراقبة الإلكترونية كإجراء لاستخلاص الدليل الإلكتروني "بين الحق في الخصوصية ومشروعية الدليل الإلكتروني"، المجلة الأكاديمية للبحث القانوني، المجلد 01، العدد 03، 2019، ص 390.

2ينظر المادة 03من القانون رقم 09/04المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، المشار إليه سابقا.

3Article n° 20 " (Collecte en temps réel des données relatives au trafic) :

1. «Chaque Partie adopte les mesures législatives et natures qui se révèlent nécessaires pour habiliter ses autorités compétentes à :

a. Collecter ou enregistrer par l'application de moyens techniques existant sur son territoire ;

b. Obliger un fournisseur de service dans le cadre de ses capacités techniques existants, à

عنوان« اعتراض معطيات المحتوى» « Interception de données relatives au contenu » المنصوص عليها بموجب المادة 21من الاتفاقية، [1] وعلى ذات النهج سار المشرع الجزائري إذ بالرجوع للقانون رقم 09-04سالف الذكر نجده قد فرق هو الآخر بين اعتراض المعطيات المتعلقة بالمحتوى والتي نظمها تحت عنوان "مراقبة الاتصالات الإلكترونية "في المادة 04من ذات القانون، وبين تجميع المعطيات المتعلقة بحركة المرور تحت عنوان "حفظ المعطيات المتعلقة بحركة السير" بموجب المادة 11من ذات القانون.[2]

ولا يفوتنا أن ننوه أن إجراء مراقبة الاتصالات الإلكترونية إنما يقصد به اعتراض الاتصالات الإلكترونية أثناء بثها أي في الزمن الفعلي لنقلها بين أطراف الاتصال وليس الحصول على اتصالات إلكترونية مخزنة، ذلك أن لكل من النوعين إجراءات خاصة به، وهذا ما يستنتج من نصوص المواثيق الدولية والقانونية المذكورة أعلاه إذ نجد اتفاقية بودابست قد عبرت عن زمن الاعتراض بعبارة "في الوقت الفعلي "والاتفاقية العربية لمكافحة جرائم تقنية المعلومات عبرت عنه بعبارة "بشكل فوري"أما عن المشرع الجزائري فقد وردت تحت عبارة "في حينها"، [3] وهذا ما يؤكد على هذا الاختلاف الذي لا يزال محل جدل من قبل العديد من التشريعات المقارنة في حين حسمت البعض منها هذا الجدل أبرزها المشرع الأمريكي حيث اعتبر الاتصالات الإلكترونية المخزنة من قبيل البيانات الساكنة وبالتالي تطبق عليها الإجراءات التي تتناسب وطبيعتها الساكنة مثل التفتيش والتحفظ عليها، وهذا بموجب تعديل القسم 2703من قانون خصوصية الاتصالات الإلكترونية، [4] وقد تم تأكيد هذه القاعدة في العديد من التطبيقات مثل قضية(United states v.Smith) حيث قرر فيها القضاء بأنه لا يمكن مراقبة الاتصالات السلكية وهي في حالة تخزين إلكتروني.[5]

Collecter ou enregistrer par l'application de moyens technique existant sur son territoire, ou

Prêter aux autorités compétente son concours et son assistance pour collecter ou enregistrer, en temps réel, les données relatives au trafic associées à des communications spécifiques transmises sur son territoire au moyen d'un système informatique. »

1ينظر المادة 21من اتفاقية بودابست لمكافحة الإجرام المعلوماتي المشار إليها أعلاه.

2يزيد بوحليط، الجرائم الإلكترونية والوقاية منها في القانون الجزائري، المرجع السابق، ص 435.

3ينظر المادة 03من القانون رقم 09/04المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، المشار إليها سابقا.

4Technically, the electronic communications privacy act of 1986 amended chapter 119 of Title 18 of U.S code.

5عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي، المرجع السابق، ص 105.

أما عن تعريف أسلوب المراقبة إ فلم يتصدى المشرع الجزائري لتعريفها وإنما ترك أمر تعريفها للفقه، إذ عرفها بعض الفقهاء على أنها إجراء يتعمد فيه الإنصات والتسجيل ومحلها المحادثات الخاصة سواء أكانت مباشرة أو غير مباشرة أي سواء كانت مما يتبادله الناس في مواجهة بعضهم البعض أو عن طريق وسائل الاتصال السلكية واللاسلكية، أما البعض الآخر فيعرفها على أنها بأنها مراقبة شبكة الاتصالات أو ذلك العمل الذي يقوم به المراقب باستخدام التقنية الالكترونية لجمع البيانات والمعلومات حول المشتبه فيه سواء كان شخصا أو مكانا أو شيئا، ويتم تنفيذ المراقبة الالكترونية من خلال استهداف الاتصالات الالكترونية التي يجريها المشتبه فيه من خلال استعماله لأي وسيلة الكترونية[1] ومثال ذلك كأن يراقب نشاط أحد القراصنة المعلوماتيين أو يقوم بنسخ البريد الالكتروني ومراقبة مراسلاته عند إرساله أو استقباله للبريد[2].

كما تجدر الإشارة إلى أن المشرع الجزائري لم يتبنى إجراء المراقبة إ للاتصالات في القانون رقم 09-04كإجراء تقتضيه التحريات أو التحقيقات أو من ضمن طرق الحصول على الأدلة الرقمية فقط، بل أدرجه ضمن الإجراءات الوقائية من بعض الجرائم التي تشكل خطرا على أمن الدولة وهي كما حددتها المادة 04من هذا القانون الجرائم الإرهابية والتخريبية وكذا الجرائم الماسة بأمن الدولة منها الجرائم التي تهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني، كما يلاحظ أن المشرع ج سمح بإجراء مراقبة الاتصالات إ بمجرد وجود احتمال التورط مستقبلا في ارتكاب إحدى هذه الجرائم وقبل وقوعها حتى، غير أن احتمال وقوع جريمة إلكترونية ضعيف جدا إن لم نقل منعدم، لأنها جرائم مميزة وغير مرئية وليس لها أي مقدمات مادية بل قد تكتشف على سبيل المصادفة، ولعل هذا يعود لتخوف المشرع الجزائري من وقوع هذه الجرائم، ونحن نرى أنها خطوة إيجابية وجريئة تحسب له على اعتبار أن هذا الإجراء من بين أخطر الإجراءات مساسا بخصوصية الأفراد.[3]

وعلى غرار المشرع الجزائري تصدت بعض التشريعات المقارنة لمفهوم المراقبة إ للاتصالات منها المشرع الفرنسي حيث أجاز هذا الأخير اعتراض الاتصالات الإلكترونية والتقاط المعطيات المعلوماتية بموجب المادة 100والمادة 706-95والمادة706-102-1من القانون رقم 2016- 731الصادر في 3جوان

1حسين ربيعي، المراقبة الإلكترونية وحق الفرد في الخصوصية داخل الفضاء الرقمي، المجلة الأكاديمية للبحث القانوني، جامعة عبد الرحمان ميرة، بجاية، المجلد السابع، العدد الأول، 2016، ص 419.

2- نبيلة هبة هروال: الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات، المرجع السابق، ص 197_198.

3جمال براهيمي، التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص 92.

2016، [1] وقد أشار إلى المقصود بإجراء المراقبة إ ضمن القانون رقم 2004- 669المتعلق بالاتصالات الإلكترونية[2] المعدل للقانون رقم 91-646بموجب المادة 02منه على أنها: "إرسال واستقبال علامات أو إشارات أو كتابات أو صور أو أصوات كهرومغناطيسية"[3]في حين عرف قانون البريد والاتصالات إ الفرنسي رقم 80-567لسنة 1980الاتصالات إ بأنها: "كل انتقال أو إرسال أو استقبال لإشارات أو علامات أو كتابة أو صور أو أصوات عن طريق النظام الكهرومغناطيسي".[4]وهو نفسه التعريف الذي جاء به المشرع الجزائري في القانون رقم 09-04سالف الذكر بموجب المادة 2فقرة "و"من القانون رقم 09-04على أنها: "أي تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة إلكترونية"، كما عرفها أيضا بموجب المادة 10فقرة 1من القانون رقم 18-04المتضمن القواعد العامة للبريد والاتصالات الإلكترونية سالف الذكر، على أنها: "كل إرسال أو تراسل أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو بيانات أو معلومات مهما كانت طبيعتها، عبر الأسلاك أو الألياف البصرية أو بطريقة كهرومغناطيسية".[5]

وعلى غرار المشرع الفرنسي عرف المشرع الأمريكي المراقبة إ للاتصالات بموجب قانون خصوصية الاتصالات الفيدرالي لسنة 1968والمعدل في سنة 1986المسمى "الباب الثالث" المشار إليه أعلاه، وذلك في المادة 2510 - 4منه على أنها: "الاكتساب السمعي أو أي اكتساب لمحتويات أي اتصال سلكي أو إلكتروني أو شفوي باستخدام أي جهاز إلكتروني أو ميكانيكي أو أي جهاز آخر"، [6] كما عرف هذا القانون الاتصالات

1Loi n° 2016- 731 du 03 juin 2016 art 5, en vigueur le 05/06/2016, Code de procédure pénale.

2Loi n° 2004- 669 du 9 juillet 2004 art 2, JORF 10/07/2004,en vigueur le 10/07/2004 relative aux communications électronique et aux services de communication audiovisuelle.

3Article n° 02 du loi n° 2004-669 du 9 juillet 2004 relative aux communications électronique et aux services de communication audiovisuelle 1, JORF n° 159 du 10 juillet 2004, dispose que :Communication électronique : on entend par communication électronique les émissions, transmission ou réceptions de signes, de signaux, d'écrits, d'images ou de sons, par voie électromagnétique » .

4عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي، المرجع السابق، ص 104.

5ينظر المادة 10من القانون رقم18-04المتعلق بالبريد والاتصالات الإلكترونية سالف الذكر.

6وتعد كلمة اكتساب « Acquisition » غامضة في هذا التعريف، فعندما يقوم جهاز المراقبة الخاص بالسلطات بتسجيل محتويات اتصالات فإنه ربما يتم اكتساب الاتصال في ثلاث نقاط مختلفة:

- عندما يقوم الجهاز بتسجيل الاتصال
- عندما تحصل السلطات لاحقا على التسجيل
- عندما تقوم السلطات بتشغيل التسجيل من أجل سماعه أو رؤية محتوياته

فأي من هذه الأحداث تشكل اكتسابا؟ فتعريف المراقبة ليس واضحا ما إذا كان يقصد أن يكون الاكتساب معاصرا لبث هذه الاتصالات، وقد تبنت المحاكم الأمريكية التفسير الذي يقضي بأن كل الاتصالات السلكية والإلكترونية يتم مراقبتها فقط عندما يتم اكتسابها أي في زمن بثها،

الإلكترونية بأنها : "كل انتقال بشكل كلي أو جزئي للإشارات أو الصور أو الأصوات أو المعطيات أو المعلومات أيا كان نوعها عن طرق الكابل أو الراديو أو النظام الكهرومغناطيسي أو التصوير الكهربائي أو الصور المرئية".[1]

ومن خلال استقرائنا لهذه التعريفات يتبين أنه يوجد عدة أطراف في عملية المراقبة الإلكترونية هاته حيث يتمثل الطرف الأول في **المراقب الإلكتروني** وهو ضابط الشرطة القضائية المكلف بتتبع اتصالات المشتبه فيه عبر شبكة الإنترنت باعتماد وسائل تقنية إلكترونية، حيث يشترط أن يكون المراقب أو الضابط من الأشخاص الذين لهم دراية بوسائل الاتصال الرقمية المختلفة ويحسنون التعامل مع الحاسب الآلي وبرامجه وأنظمته المعلوماتية، كما تتطلب مهمة المراقبة من الضابط المكلف بها أن تتوافر فيه قدرات عالية ومواصفات معينة مثل طاقة الاستيعاب نظرا للكم الهائل من المعلومات والمعرفة الموجودة على شبكة الإنترنت، كما يجب أن يتمتع الضابط المراقب بقدرة القراءة التصويرية التي يقصد بها وصول معدل الشخص في القراءة للكلمات المقروءة إلى 1000كلمة في الدقيقة الواحدة إذ ينبغي عليه أن يتمتع بقراءة سريعة وفي أقل وقت ممكن وكذا الاحتفاظ بالمعلومات، بالإضافة إلى تمتعه بالذكاء الإلكتروني أي القدرة على التفكير وفهم العلاقات بين العناصر المكونة لموقف من المواقف والتكيف معه لتحقيق الهدف المراد تحقيقه من جراء عملية المراقبة إ هذه. أما الطرف الثاني **المراقب** إ (بفتح القاف) فهو المشتبه فيه على الشبكة المتمثل في بعض الأشخاص أو الحاسوب الرقمي أو بعض المواقع من الإنترنت أو البريد الإلكتروني وصفحات الويب المختلفة بما تحويها من مراسلات إلكترونية، والتي تتيح لمستخدميها الاشتراك في محادثات بين بعضهم البعض في مختلف أنحاء العالم وفي أي وقت وبسرعة وسهولة فائقة، إذ تعتبر المحادثات التي تتم عبر مواقع التواصل الاجتماعي من قبيل هذه الاتصالات إ محل المراقبة، وقد اكتسبت اسمها الاجتماعي كونها تعزز العلاقات والروابط الاجتماعية بين الأفراد، والتي تطورت في الآونة الأخيرة لتصبح وسيلة تعبيرية واحتجاجية ومن أبرز هذه المواقع، Face book, Youtube, twiter, viber, WhatsApp،[2] كما قد يكون محل المراقبة الهاتف النقال المتصل بشبكة الإنترنت وساعة

وبمعنى آخر فإن المقصود من مراقبة الاتصالات يشير إلى اكتسابها في الزمن الفعلي أثناء البث بين أطراف الاتصال فقط، فمثلا المفتش الذي يطلع لاحقا على نسخة من اتصال مخزن لا يعد مراقبة للاتصال بل تفتيشا له.

118 U.S.C.A 2510 (2012) : « Electronic communication» meansanytransfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photo electronic, or photo optical system that affects interstate or foreign commerce… ».

2عيدة بلعابد، خصوصية التحقيق في الجريمة المعلوماتية، المرجع السابق، ص 146.

اليد الذكية واللوح الرقمي وغيرها من الأجهزة الذكية شرط أن تكون متصلة بشبكة الإنترنت كون أن الاتصالات إ الناتجة عن هذه الأجهزة والبرامج هي محل المراقبة.[1]

وأما عن الطرف الثالث في عملية المراقبة إ فيتمثل في التقنية الإلكترونية المستخدمة في هذه العملية، والتي تعني مجموعة الأجهزة المتكاملة مع بعضها بغرض تشغيل مجموعة من البيانات المتعلقة بالأشخاص المشتبه فيهم وفق برنامج موضوع مسبقا لتحديدهم وضبط الأدلة الرقمية، ومن أمثلة هذه التقنيات نجد:

- **برنامج كارنيفور:**

وهو تقنية إلكترونية طورتها إدارة تكنولوجيا المعلومات التابعة لمكتب التحقيقات الفيدرالي (FBI) من أجل تعقب وفحص الرسائل الإلكترونية من خلال الخوادم التي تستخدمها الشركات المزودة لخدمات الإنترنت أو أية شبكة معلومات توفر خدمة الإنترنت، والمشتبه في خوادمها وجود معلومات عن جرائم جنائية، إذ لا يتم تنفيذ هذه العمليات إلا بعد استئذان المحكمة المختصة بوضع أجهزة تلك الشركات تحت المراقبة، ورغم انتهاك هذه الوسيلة للخصوصية المعلوماتية إلا أنها حققت نتائج جيدة في تعقب المجرمين عبر الإنترنت، [2] وأصبح يطلق عليها اسم (DCS 1000) بعد 11سبتمبر 2001وأصبحت تختص بمتابعة القضايا المتعلقة بالأمن القومي والتصدي لأي محاولة هجوم داخل الو م أ، حيث تمكن مكتب التحقيقات الفيدرالي من خلال هذه التقنية من ضبط أدلة أدان بها قائد ميليشيات كانت تخطط للدخول إلى المنشآت العسكرية لسرقة متفجرات وتفجير محطة الطاقة الموجودة جنوب شرق الو م أ باستخدامها شبكة الإنترنت في التراسل والتخطيط.[3]

- **تقنية مر اقبة مراسلات البريد الإلكتروني**

ولعل من أهم المراسلات الإلكترونية التي تكون محل مراقبة إ وتمثل مصدرا غنيا لأدلة إثبات الجرائم الإلكترونية، المراسلات التي تتم عبر البريد الإلكتروني كونه من أكثر الوسائل الحديثة استخداما للاتصال عبر الإنترنت والذي يربط الأفراد من مختلف أنحاء العالم، فهو عبارة عن نظام معلوماتي لتبادل

1بن بادة عبد الحليم، المراقبة الإلكترونية كإجراء لاستخلاص الدليل الإلكتروني "بين الحق في الخصوصية ومشروعية الدليل الإلكتروني"، المرجع السابق، ص 395.

2حسام محمد نبيل الشنراقي، الجرائم المعلوماتية دراسة تطبيقية مقارنة على جرائم الاعتداء على التوقيع الإلكتروني، المرجع السابق، ص 387.

3نبيلة هبة هروال، الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات، المرجع السابق، ص 201.

الرسائل والصور وغيرها من المواد القابلة للإدخال الرقمي أو التحميل الرقمي، ما يعتبر مستودع لحفظ المستندات والمراسلات التي تتم معالجتها رقميا في صندوق خاص وشخصي للمستخدم والتي لا يمكن الدخول أو الاطلاع عليها بسهولة كونها محمية فنيا[1]، وتنصب عملية مراقبة واعتراض مراسلات البريد الإلكتروني على ثلاثة عناصر أساسية ألا وهي:

- البريد الوارد (IN) الذي يتم من خلاله مراقبة قائمة المراسلات الإلكترونية التي وصلت للمشتبه فيه.
- البريد الصادر (OUT) وهو عكس الأول يتم من خلاله مراقبة المراسلات الصادرة أي التي أرسلها المشتبه فيه بنفسه للغير.
- الحافظ أو سلة المهملات (TRASH) فيسمح هذا الأخير من الاطلاع على المراسلات المحفوظة داخل البريد الإلكتروني الخاص بالمشتبه فيه، أو المحذوفة من طرفه.[2]

وتعتبر تقنية مراقبة البريد إ هذه من أنجع الوسائل المستخدمة في مراقبة المراسلات إ صممها العالم الأمريكي "ريتشارد اتوني"من أجل سبر محتوى البريد الإلكتروني موضوع المراقبة، وقد استخدمت هذه التقنية أجهزة الاستخبارات الأمريكية لكشف مشتبه فيه من الجنسية الروسية حاول اختراق مواقع على شبكة الإنترنت.[3]

- **تقنية تعقب المو اقع الإباحية:**

وتسمى هذه التقنية بـ"نوبد شرطة الإنترنت"وهو عبارة عن برنامج يبحث عن الصور الجنسية المخلة في الأنظمة المعلوماتية التي تعمل ببرامج تشغيل ويندوز الحديث، حيث يتعقب المراقب إ هذه الأنظمة والمواقع التي تحويها لكشف وضبط أي صور مخلة أو إباحية ومن ثم تبليغها إلى السلطات القضائية المختصة لمواصلة إجراءات التحقيق بشأنها، وتطهير الشبكة العنكبوتية من هذه المواقع.[4]

بالرغم من النجاحات الكبيرة التي حققتها هذه البرمجيات والتقنيات المتطورة في كشف الجرائم وتعقب المجرمين إلا أن بعض الفقه يرى أن هذه المراقبة البرمجية لا تزال محل نظر في القانون من حيث

1وقد عرف المشرع الجزائري البريد الإلكتروني بموجب المادة 02فقرة 2من المرسوم التنفيذي رقم 98/257المؤرخ في 25/08/1998يضبط شروط وكيفيات إقامة خدمات "أنترنات"واستغلالها على أنه: "خدمة تبادل رسائل إلكترونية بين المستعملين".

2جمال ابراهيمي، التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص 91.

3نبيلة هبة هروال، الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات، المرجع السابق، ص 203.

4المرجع نفسه، ص 203.

ضرورة الالتزام بما هو مقرر في القانون من ضمانات دستورية تحمي الحق في الخصوصية، ويرى أن إعداد برمجيات من شأنها البحث عن الجرائم ومرتكبيها أمر يحتاج إلى تطوير قد لا يتوافق مع الضمانات القانونية المعاصرة لما تشكله هذه التقنيات من انتهاك للحق في الخصوصية المعلوماتية.[1]

الفرع الثاني: مشروعية مر اقبة الاتصالات الإلكترونية

مما لا شك فيه أن مراقبة الاتصالات والمراسلات الخاصة للأفراد تعتبر من أخطر صور الاعتداء على الحق في الخصوصية، ولهذا اعتبرت جل المواثيق الدولية وكذا التشريعات الداخلية عمليات مراقبة الاتصالات الإلكترونية غير مشروعة لما تسببه من انتهاك لسرية هذه الاتصالات، ولهذا عملت على تفريد حماية تشريعية لهذا الحق، من خلال سن نصوص قانونية تعمل على توفير قدر من الحماية الجنائية لسرية المراسلات الإلكترونية هذا من جهة، ومن جهة أخرى أحاطتها بضمانات وضوابط تكفل عدم الاعتداء عليها من قبل السلطات القضائية عند مباشرتها لإجراء المراقبة الإلكترونية بصدد التحري عن بعض الجرائم الخطيرة، وهذا ما سنتطرق له بشيء من التفصيل في النقاط التالية:

أولا: عدم مشروعية هذا الإجراء

على غرار المواثيق الدولية التي دعت إلى ضرورة احترام الحياة الخاصة للفرد وعدم التدخل في شؤونه_ والتي لم تحدد وسيلة التدخل في الحياة الخاصة فيما إذا كانت عادية تقليدية أم إلكترونية _ فقد ظهرت أول اتفاقية دولية لحماية الخصوصية المعلوماتية في عام 1981عندما وضع الاتحاد الأوروبي اتفاقية حماية الأفراد من مخاطر المعالجة الآلية للبيانات الشخصية وهي تعتبر بمثابة أول صك دولي ملزم قانونا لحماية البيانات، وبعدها أصدرت منظمة التعاون الاقتصادي والتنمية دليلا إرشاديا لحماية الخصوصية ونقل البيانات الخاصة والذي بموجبه قرر مجموعة من القواعد التي تحكم عمليات المعالجة الآلية للبيانات، وفي عام 1989تبنت الأمم المتحدة دليلا يتعلق باستخدام الحوسبة في عملية تدفق البيانات الشخصية.[2]

1رشيدة بوكر، كتاب جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري والمقارن، المرجع السابق، ص 375.

2United Nations, Guidelines concerning Compteriezpersonales data files, Adopted by the General Assembly on 14 décembre 1990.

نقلا عن محمد سيد سلطان، قضايا قانونية في أمن المعلومات وحماية البيئة الإلكترونية، المرجع السابق، ص 23

كما جرمت اتفاقية بودابست لسنة 2001المتعلقة بالإجرام المعلوماتي، التجسس والتنصت على المعلومات والبيانات الشخصية[1]، إذ نصت في توصيتها رقم 15/87على تنظيم ومراقبة استخدام البيانات الشخصية في المجال الشرطي، وفي توصية أخرى رقم 04/90على حماية البيانات الشخصية المنزلة في المجال الإلكتروني المعلوماتي، [2]وأكدت في مادتها الثالثة (3) على أن الاعتراض غير القانوني للبيانات المتداولة إلكترونيا يعد جريمة معلوماتية معاقب عليها بقولها: "يقوم كل طرف من الدول الأطراف في الاتفاقية بإقرار هذه الإجراءات التشريعية وغيرها من الإجراءات الأخرى، كلما كان ذلك ضروريا لإصدار نص قانوني أو تشريعي بأنها تشكل جرائم بموجب القانون الوطني الخاص بها عند ارتكابها عن قصد وذلك من حيث اعتراض خط سير البيانات دون وجه حق ويتم ذلك بالوسائل الفنية لقطع عمليات البث والإرسال غير عمومية لبيانات الكمبيوتر إلى داخل منظومة الكمبيوتر، بما في ذلك ما ينبعث من منظومة الكمبيوتر من موجات كهرومغناطيسية تحمل معها البيانات...".[3]

إضافة لذلك أقرت الاتفاقية الأوروبية لحماية البيانات الشخصية في مجال المعلوماتية التي تبناها المجلس الأوروبي بمدينة ستراسبورغ الفرنسية، بالنتائج السلبية لاستعمال الإنترنت والشبكة المعلوماتية ونادت الدول الأطراف إلى ضرورة اتخاذ ما يجب من إجراءات للتصدي للإجرام الإلكتروني المهدد لسرية

1لقد عرفت اتفاقية بودابست لسنة 2001المتعلقة بالإجرام المعلوماتي البيانات أو المعطيات الشخصية بموجب الفقرة "ب"من المادة 1على أنها: "كل تمثيل للوقائع أو المعلومات أو المفاهيم تحت أي شكل وتكون مهيأة للمعالجة الآلية بما في ذلك برنامج معد من ذات الطبيعة ويجعل الحاسب يؤدي المهمة".

كما عرفتها المادة 4من اللائحة العامة لحماية البيانات الخاصة بالمستخدمين في دول الاتحاد الأوروبي (GDPR) بأنها معلومات لها صلة بشخص تم التعرف على هويته بشكل مباشر أو غير مباشر، على وجه الخصوص بالرجوع إلى معرف شخصي مثل الاسم ورقم الضمان الاجتماعي وبيانات الموقع والمعرف عبر الإنترنت (عنوان IPأو عنوان البريد الإلكتروني) أو لواحد أو أكثر من العوامل الخاصة بالهوية البدنية أو الفيزيولوجية أو الحيوية أو العقلية أو الاقتصادية أو الثقافية أو الاجتماعية.

وبالرجوع للقانون الفرنسي رقم 801لسنة 2004الخاص بحماية البيانات الشخصية نجده قد عرف البيانات الشخصية في المادة 2منه على أنها: "تعتبر بيانات شخصية أي معلومات تتعلق بشخص طبيعي محددة هويته أو من الممكن تحديد هويته بطريقة مباشرة أو غير مباشرة، سواء تم تحديد هويته بالرجوع إلى رقمه الشخصي أو بالرجوع إلى أي شيء يخصه"(كتابة المادة). والملاحظ أن المشرع الفرنسي قد توسع في =...مفهوم البيانات الشخصية بحيث تشمل كل معلومة تمكن من تحديد هوية الشخص مما يوسع من سبل حماية البيانات ومواجهة أي صورة من صور الاعتداء على الخصوصية المعلوماتية، خاصة مع تقدم وتطور تقنيات جمع البيانات.

أما عن القانون الجزائري فقد عرف البيانات الشخصية في الفقرة "ج"من المادة 2من القانون رقم 09-04سالف الذكر، تحت اسم "المعطيات المعلوماتية"على أنها: "أي عملية عرض للوقائع أو المعلومات أو المفاهيم في شكل جاهز للمعالجة داخل منظومة معلوماتية، بما في ذلك البرامج المناسبة التي من شأنها جعل منظومة معلوماتية تؤدي وظيفتها".

وعرفها أيضا من خلال القانون رقم 18-07في مادته الثالثة فقرة 1على أنها: "كل معلومة بغض النظر عن دعامتها متعلقة بشخص معرف أو قابل للتعرف عليه والمشار إليه أدناه، "الشخص المعني"بصفة مباشرة أو غير مباشرة لاسيما بالرجوع إلى رقم التعريف أو عنصر أو عدة عناصر خاصة بهويته البدنية أو الفيزيولوجية أو الجينية أو البيومترية أو النفسية أو الاقتصادية أو الثقافية أو الاجتماعية".

2خلايفية هدى، الإطار القانوني والداخلي لحماية الخصوصية على الإنترنت، المرجع السابق، ص 48.

3خالد ممدوح ابراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص 360.

البيانات والمعلومات، كما أصدر الاتحاد الأوروبي لائحة GDPR[1] في 14/04/2016 من طرف المفوضية الأوروبية لحماية حقوق جميع مواطني الاتحاد الأوروبي وبياناتهم الشخصية، إذ نظمت هذه اللائحة خصوصية البيانات الشخصية وأقرت حق المواطن في التحكم في بياناته وحرية توجيه معلوماته الشخصية وتخزينها أو مسحها، وفي حالة ما ثبت سرقة هذه البيانات أو اقتحامها منحت له اللائحة مدة 72ساعة لتبليغ السلطات القضائية لاتخاذ ما تراه مناسبا من إجراءات لاسترجاع وحماية هذه البيانات وتأمينها.[2]

ونتيجة للمخاطر والجرائم المستحدثة الماسة بالخصوصية المعلوماتية وعملا بتوصيات الاتفاقيات والمعاهدات الدولية عملت أغلب التشريعات المقارنة على تطوير تشريعاتها الداخلية لكي تواكب هذه التهديدات، إذ أقرت جل الدساتير المقارنة الحماية الجنائية للخصوصية المعلوماتية وكذا البيانات الشخصية فمنها من نصت بصريح العبارة على حماية الاتصالات الإلكترونية من الاعتراض والمراقبة بدون إذن من السلطات المختصة مثل المشرع المصري في المادة 57منه[3] بقولها : "للحياة الخاصة حرمة، وهي مصونة لا تمس، وللمراسلات البريدية والبرقية والإلكترونية والمحادثات الهاتفية وغيرها من وسائل الاتصال حرمة وسريتها مكفولة ولا تجوز مصادرتها أو الاطلاع عليها أو رقابتها إلا بأمر قضائي مسبب ولمدة محددة وفي الأحوال التي يبينها القانون"، ومنها من أقرت هذه الحماية ضمنيا من خلال نصوصها، من بينها الدستور الأمريكي[4] والدستور الجزائري بموجب المادة 47من التعديل الدستوري لسنة 2020والمشار إليها (في المبحث الأول عند التطرق لإجراءات اعتراض المراسلات)، حيث كفل المؤسس الدستوري حماية سرية المراسلات والاتصالات بمختلف أشكالها ما يفيد أن تكون هذه الاتصالات سلكية عادية أو إلكترونية، بحيث لا يجوز الاعتداء عليها بأي شكل، بالإضافة إلى أنه أكد على حماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.[5]

1GDPR : General Data Protection Régulation

وتعني هذه الكلمة مجموعة القوانين والقواعد التي تحمي الخصوصية المعلوماتية والبيانات الشخصية وقد جاءت هذه اللائحة محل القرار الأوروبي رقم 46/95/ EC الصادر في 24/10/1995 المتعلق بحماية البيانات الشخصية وحركتها. ينظر خلايفية هدى، الإطار القانوني والداخلي لحماية الخصوصية على الإنترنت، المرجع السابق، ص 46.

2خلايفية هدى، الإطار القانوني والداخلي لحماية الخصوصية على الإنترنت، المرجع السابق، ص 46.

3ينظر المادة 57من دستور الجمهورية المصرية المعدل بالقرار رقم 38لسنة 2019الصادر بتاريخ 23أبريل 2019.

4ينظر التعديل الرابع لدستور الولايات م أ المشار إليه سابقا.

5ينظر المادة 47من التعديل الدستوري لسنة 2020والتي تنص على: "لكل شخص الحق في حماية حياته الخاصة وشرفه. لكل شخص الحق في سرية مراسلاته واتصالاته الخاصة في أي شكل كانت، لا مساس بالحقوق المذكورة في الفقرتين الأولى والثانية إلا بأمر معلل من السلطة

ومن جهة ثانية عالجت بعض التشريعات مسألة حماية خصوصية الاتصالات الإلكترونية، إذ كانت أول معالجة تشريعية في هذا المجال في مقاطعة هيس بألمانيا في عام 1973، ثم في الو م أ عام 1974، ثم ألمانيا على المستوى الفيدرالي عام 1977، ثم في فرنسا بإصدار القانون رقم 78-17في 06جانفي 1978 المتعلق بالمعلوماتية والحريات[1] حيث تناول في الباب الأول الغرض من المعالجة الآلية للمعطيات وكذا حدد مفهوم البيانات الشخصية أما الباب الثاني فتضمن تشكيل اللجنة الوطنية للمعلوماتية والحريات والتي تعمل على حماية الحياة الخاصة والحريات الفردية والعامة، والتي يجب إخطارها قبل إجراء أي معالجة لهذه البيانات.[2]

كما تعتبر تونس من بين الدول العربية التي بادرت إلى تنظيم مجال المعالجة الآلية للمعطيات والبيانات الشخصية وذلك بإصدارها القانون رقم 63لسنة 2004المؤرخ في 27جويلية 2004، المتعلق بحماية البيانات الشخصية والذي أكد من خلاله على حق كل شخص في حماية المعطيات الشخصية المتعلقة بحياته الخاصة، وأنشأ سلطة إدارية مستقلة لحماية هذه البيانات، كما جرم من خلاله كل الأفعال الماسة بالبيانات الشخصية للفرد من التقاط وتجميع وحفظ وإفشاء دون ترخيص، [3] ومن جهة ثانية أقر مجلس الوزراء السعودي نظام مكافحة جرائم المعلوماتية والمتضمن أنواع هذه الجرائم والعقوبات المقررة لها، فوفقا لهذا النظام يعاقب على جريمة التنصت الإلكتروني بالسجن مدة لا تزيد عن سنة وغرامة لا تزيد عن خمسمائة ألف ريال أو بإحدى هاتين العقوبتين، وعلى غرار المشرع السعودي جرم المشرع الإماراتي أسلوب المراقبة والتجسس والتنصت المعلوماتي وذلك بموجب القانون رقم 5لسنة 2012المتعلق بمكافحة جرائم تقنية المعلومات[4] إذ تنص المادة 15منه على أنه: "يعاقب بالحبس وبالغرامة التي لا تقل عن مائة وخمسين ألف درهم ولا تجاوز خمسمائة ألف درهم أو بإحدى هاتين العقوبتين كل من التقط أو اعترض عمدا وبدون تصريح أي اتصال عن طريق أي شبكة معلوماتية".[5]

القضائية، حماية الأشخاص عند معالجة المعطيات ذات الطابع الشخصي حق أساسي، يعاقب القانون على كل انتهاك لهذه الحقوق". لتفاصيل أكثر أنظر المطلب الأول من المبحث الأول من هذا الفصل.

1Loi n° 78-17 du 6 juin 1978 relative à l'informatique, au fichiers et aux libertés.

2محمد سيد سلطان، قضايا قانونية في أمن المعلومات وحماية البيئة الإلكترونية، المرجع السابق، ص 24.

3بن اسماعيل سلسبيل، الحماية الجنائية للخصوصية المعلوماتية في التشريعين الجزائري والفرنسي، مجلة الاجتهاد القضائي، المجلد 12، عدد 22، أفريل2020، ص 744.

4المادة15من المرسوم بقانون رقم 5لسنة 2012بشأن مكافحة جرائم تقنية المعلومات، ج ر العدد 540ملحق السنة الثانية والأربعون، الصادرة بتاريخ 26/08/2012.

5خالد ممدوح براهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص 363.

أما عن الحماية الجنائية التي أقرها مشرعنا الوطني (الجزائري) للخصوصية المعلوماتية بما فيها الاتصالات الإلكترونية، فقد استحدث بعض النصوص القانونية وعدل أخرى مواكبة منه للتطورات التكنولوجية ومحاولة منه للتصدي الأمثل للتهديدات التي تطال الخصوصية بصفة عامة، إذ جرم كل اعتداء يقع على أنظمة المعالجة الآلية للمعطيات وأعطى لها حماية قانونية كونه اعتبر محتوياتها من الخصوصيات والحقوق الخاصة التي يمنع الاطلاع عليها، وذلك بموجب تعديل قانون العقوبات بالقانون رقم 04- 15المؤرخ في 10/11/2004باستحداث القسم السابع مكرر تحت عنوان "المساس بأنظمة المعالجة الآلية للمعطيات "من المادة 394مكرر إلى المادة 394مكرر 8، التي جرمت كل تلاعب بالمعطيات المخزنة داخل نظام معلوماتي أو تخريبها أو إفشائها، [1] والتي تقابلها المواد 1030- 1والمادة 1030- 2من

1وتتمثل هذه الجرائم حسب القانون رقم 04- 15المتضمن قانون العقوبات، في:

1. **تجريم الولوج و البقاء غير المصرح به في النظام المعلوماتي: حيث** تعتبر هذه الجريمة أحد أهم الجرائم الماسة بالخصوصية المعلوماتية في معظم التشريعات الحديثة بما فيها التشريع الجزائري نص المشرع عليها في المادة 349مكرر من القانون 04/15المعدل والمتمم لقانون العقوبات الجزائري: "يعاقب بالحبس من ثلاث (3) أشهر إلى سنة وبغرامة من 50000دج إلى 100000دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك، تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة، وإذا ترتب على الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة الحبس من ستة (6) أشهر إلى سنتين (2) والغرامة من 50000دج إلى 150000دج. "

يقصد بالولوج أو الدخول لنظام المعالجة الآلية للمعطيات الاتصال الحسي مع النظام المعلوماتي أو التحكم فيه ولو جزئيا بما يسمح بالاطلاع على المعطيات المخزنة داخله وبدون رضا المسؤول عن هذا النظام، و يتحقق هذا الفعل بإحدى الصورتين التاليتين:

أ. **الصورة الأولى:**تتحقق هذه الصورة متى تم الدخول إلى النظام المعلوماتي عن غير قصد كالخطأ والسهو مثلا أي دون توافر القصد الجنائي لدى الجاني ولكن بعد تفطنه للأمر يختار البقاء في النظام والاطلاع على محتوياته وهنا يصبح الجاني عالما بأنه غير مصرح له بالبقاء ومع ذلك تتجه إرادته إلى البقاء وهنا يتشكل القصد الجنائي .

ب. **الصورة الثانية :**تتحقق هذه الصورة إذا تم الدخول إلى النظام المعلوماتي بتصريح من صاحب الحق ولكن لمدة معينة فقط أو لجزء محدد من النظام، فيقوم الجاني بتجاوز الحدود المسموح له بها ويبقى داخل هذا النظام لمدة طويلة من تلك المحددة.

وانطلاقا من هذا فإن جريمة الولوج أو البقاء غير المشروع في النظام المعلوماتي تعتبر من الجرائم الشكلية حيث يشكل مجرد الولوج أو البقاء داخل النظام دون تصريح من صاحبه جريمة حتى ولو لم ينتج عن هذا الفعل ضرر مادي أو معنوي، يتمثل في الحصول على بيانات شخصية أو التلاعب فيها.

2. **تجريم التزوير المعلوماتي: إذ** تنص المادة 394مكرر 1من قانون العقوبات الجزائري على: "يعاقب بالحبس من ستة (6) أشهر الى ثلاث (3) سنوات وبغرامة من 500.000دج إلى 2.000.000دج كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها ".

حيث تعتبر المعطيات من الناحية الفنية وحتى القانونية لفظ يتسع ليشمل جملة من الأصناف، فقد تكون هذه المعطيات برامج خبيثة أو فيروسات يقوم الجاني بإدخالها إلى النظام المعلوماتي بهدف التجسس وجمع البيانات الخاصة أو إحداث ضرر مادي أو معنوي، كما تشير المادة السابقة على تجريم فعل التعديل في البيانات الشخصية المخزنة داخل النظام أو إزالتها دون علم صاحبها ومثال ذلك تعديل أو إزالة أو حذف في قاعدة بيانات تخص موظفين أو مرضى أو فئة أخرى، وبغض النظر عن ما تحدثه هذه الأفعال من ضرر فإنها تعتبر جريمة شكلية تامة معاقب عليه ، كما هي جرائم عمدية اشترط المشرع الجزائري في المادة 349مكرر1أن تتم عن طريق الغش بمعنى اتجاه إرادة الجاني إلى فعل الإدخال أو التعديل أو الإزالة دون رضا صاحب الحق في المعطيات أو من له السيطرة عليها.

القانون الجنائي الفيدرالي الأمريكي الخاص بإساءة استخدام الحاسبات الآلية، والذي جرم الدخول غير المصرح به إلى نظام الكمبيوتر للحصول على معلومات محددة إذ لا يعاقب هذا القانون خلافا للقانون الجزائري على مجرد الدخول للنظام أو البقاء فيه عن طريق الغش بل لابد أن يعقب هذا الدخول حصول الشخص على معلومات معينة لكي يوجب العقاب.[1]

ولم يقف المشرع الجزائري عند هذا القانون بل سن القانون رقم 06-23المعدل والمتمم لقانون العقوبات ج المشار إليه سابقا، [2] إذ جرم من خلاله كل اعتراض للاتصالات دون الحصول على إذن مسبق من السلطات المختصة وذلك بموجب المادة 303مكرر منه والتي عاقبت بالحبس والغرامة لكل من تعمد المساس بحرمة الحياة الخاصة للأشخاص بأي تقنية كانت وذلك بالتقاط صور أو تسجيل أو نقل أحاديث خاصة وسرية بدون إذن ورضا صاحبها، إلا أن اغلب الفقه يرى أن هذه المادة تخص المحادثات الخاصة التي تتم عن طريق الوسائل السلكية أو الخط التليفوني دون المحادثات التي تتم عن طريق الوسائل الإلكترونية والتي تتخذ شكل البريد الإلكتروني أو شكل المحادثة الفورية، إلا أننا نرى أن هذا الرأي غير مقبول نوعا ما لأن المشرع لم يحدد الوسيلة التي يتم بها نقل المحادثات أو تسجيلها بل جاء النص على عمومه ليشمل كل الاعتداءات الواقعة على الاتصالات سواء السلكية أو الإلكترونية وهذا ما تأكده عبارة "بأي تقنية كانت "التي استعملها كل من المشرع الجزائري والفرنسي في المادة 226-1من ق ع الفرنسي رقم 92- 684لسنة 1992[3]، والمادة 309مكرر من ق ع المصري رقم 58لسنة 1937[4]، باستخدام عبارة "جهاز من الأجهزة أيا كان نوعه "والتي تفيد أن يكون الاعتراض والمراقبة للاتصالات التي تتم عن طريق الوسائل الإلكترونية وشبكة الإنترنت، هذا من جهة ومن جهة أخرى المتمعن في الفقرة 7من المادة

---

3. **تجريم التعامل في معطيات غير مشروعة:**وردت هذه الجريمة في المادة 349مكرر2من القانون 04/15والتي نصت على: "يعاقب بالحبس من شهرين (2) إلى ثلاث (3) سنوات وبغرامة من 1.000.000دج إلى 5.000.000دج كل من يقوم عمدا وعن طريق الغش بما يأتي:

أ. تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم.

ب. حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم. "

كما نصت المادة 394مكرر3من نفس القانون على أنه تضاعف العقوبات المقررة للجرائم الماسة بالأنظمة المعلوماتية متى استهدفت الجريمة الدفاع الوطني أو الهيئات أو المؤسسات الخاضعة للقانون العام وذلك دون الإخلال بتطبيق عقوبات أشد.

1خالد ممدوح براهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص 360.

2ينظر المادة 303مكرر من القانون رقم06- 23المتضمن قانون العقوبات الجزائري المشار إليه سابقا.

3Voir l'article n° 226-1 modifié par la loi n°2020- 936 du 30 juillet 2020- art 17 en vigueur le 01 Aout 2020 ; code pénal français.

4ينظر المادة 309مكرر من القانون رقم 58لسنة 1937المؤرخ في 05أوت 1937، المتضمن قانون العقوبات المصري المشار إليه سابقا.

4من القانون رقم 09/04سالف الذكر يرى أن المشرع الجزائري خص المعطيات المتنصت عليها عن طريق عمليات مراقبة الاتصالات الإلكترونية بحماية موضوعية بأن جعل عقوبتها نفس عقوبة جنحة المساس بالحياة الخاصة للأشخاص المنصوص عليها بموجب المادة 303مكرر من قانون العقوبات المذكورة أعلاه، هذا ما يؤكد أن المادة 303مكرر من ق ع تحمي كلا النوعين من الاتصالات سواء السلكية أو الإلكترونية.

خلافا لهاته التشريعات قام المشرع الأمريكي بإدخال نصوص قانونية خاصة تسري على الاتصالات الإلكترونية بالإضافة إلى الاتصالات السلكية واللاسلكية منها ما تضمنه قانون خصوصية الاتصالات الإلكترونية الفيدرالي في القسم 119منه، مساويا في ذلك بينها وبين الاتصالات السلكية، حيث نص على عقاب كل من اعترض أو حاول اعتراض أو ساعد غيره على اعتراض اتصال سلكي أو شفوي أو إلكتروني، [1]ونحن نرى أن المشرع الأمريكي نص بصريح العبارة على حماية كل الاتصالات سواء السلكية أو الإلكترونية من الاعتراض والمراقبة بدون إذن، في حين أن التشريعات الأخرى ومن بينها التشريع الجزائري لم يكن صريحا في نصه على هذه الحماية، بل اعتمد عبارات عامة رغم أنها تفيد المطلوب ولكن حبذا لو يتدارك المشرع الوطني هذا النص بالتعديل أو إضافة مواد جديدة تحمي الاتصالات إ من كل أشكال الانتهاك المعلوماتي.

من جهة أخرى قد أضفى المشرع الجزائري أيضا حماية للمعطيات الرقمية بوجه عام منها المعطيات الشخصية وذلك بموجب القانون رقم 18-07المؤرخ في 10جوان 2018المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، [2] والذي جرم من خلاله كل أشكال الاختراق والتجميع غير القانوني للبيانات وإفشائها، وألزم المسئول عن معالجة هذه البيانات بجملة من الالتزامات المتعلقة بالتصريح والترخيص وكذا إعلام الشخص المعني قبل معالجة بياناته وكذا الالتزام بسرية هذه البيانات وفي المقابل منح الشخص المعني حقوقا معينة، وهذا كله لحماية هذه المعطيات من أي مساس أو انتهاك قد يطالها أثناء المعالجة الآلية لها.[3]

1عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي، المرجع السابق، ص 108. لمزيد من التفاصيل يراجع المطلب الأول من المبحث الأول من هذا الفصل.

2ينظر القانون رقم 18-07المؤرخ في 10جوان 2018المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي المشار إليه سابقا.

3لمزيد من التفاصيل ينظر الفصل الأول من الباب الأول.

ثانيا: الضوابط القانونية التي تحكم عملية المراقبة الالكترونية

الأصل أن سرية الاتصالات بمختلف أشكالها مضمونة ومحمية في العديد من المواثيق الدولية والدساتير والقوانين العقابية الداخلية، حيث لا يجوز المساس بها وانتهاك حرمتها كما أشرنا أعلاه، إلا أن ضرورة مكافحة الجريمة الإلكترونية حتمت استعمال بعض الوسائل والأساليب للتصدي لها والتي من شأنها انتهاك هذه الخصوصية، ونظرا لخطورة هذه الأساليب ومنها إجراء المراقبة الإلكترونية على حقوق وحريات الأفراد حرصت أغلب التشريعات على إحاطتها بجملة من الضوابط والقيود القانونية تفاديا لتعسف السلطات القضائية في استعمالها، حيث سنقتصر على أهم الضوابط الخاصة بمراقبة الاتصالات الإلكترونية فقط في حين نتفادى ذكر بعض الشروط الأخرى التي تنطبق على النوعين من الاتصالات (السلكية والإلكترونية) باعتبار أنه قد تم التطرق إليها سابقا تفاديا للتكرار، وذلك على النحو التالي:

1. الضوابط الموضوعية

وتتمثل هذه الضوابط فيما يلي:

أ. حصر الحالات التي يلجأ فيها إلى هذه الإجراءات

أجازت التشريعات المقارنة اتخاذ إجراء مراقبة الاتصالات الالكترونية لأسباب معينة وفي حالات محددة حصرا، منها المشرع الجزائري بموجب المواد 03و 04من قانون 09/04حيث أكد على الحفاظ على سرية المراسلات والاتصالات وعدم انتهاكها إلا في حالات معينة، إما لمقتضيات حماية النظام العام أو لمستلزمات التحريات والتحقيقات القضائية[1] وحدد بموجب المادة 04من ذات القانون الحالات التي تسمح باللجوء إلى المراقبة الالكترونية[2] والمتمثلة في:

- الوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة، والملاحظ هنا أن السند الشرعي الذي يبرر اللجوء إلى مراقبة الاتصالات الإلكترونية هو ضابط الوقاية من وقوع هذه الجرائم الخطيرة فقط دون وقوعها فعلا.

1-ينظر المادة 3من القانون 09/04المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها سالف الذكر.

2-ينظر المادة 4من القانون 09/04سالف الذكر.

- في حالة توافر معلومات عن احتمال الاعتداء على منظومة معلوماتية على نحو يهدد النظام العام[1] أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني، ويفهم من كلمة "احتمال"أنه يتم مراقبة الاتصالات والمنظومة المعلوماتية بمجرد احتمال الاعتداء عليها حتى ولم يترتب على ذلك ضرر أو جريمة فعلا، وهذا كون أن هذه التهديدات لو تحققت فعلا لأصبح أمر معالجة آثارها صعب للغاية، خاصة في ظل توجه العالم حول رقمنة الحكومة وإرساء دعائم الحكومة الإلكترونية ورقمنة الخدمات في مختلف القطاعات، مما ساهم بشكل رهيب في انتشار جرائم الاعتداء على المنظومة المعلوماتية التي يعتبرها القراصنة والمجرمين المعلوماتيين بنوكا ثمينة بما تحتويه من معلومات وبيانات سواء الخاصة بالأفراد أو المؤسسات وخاصة المؤسسات الحكومية التي أصبحت تستهدف كثيرا في الآونة الأخيرة.

ولعل هذه المراقبة أيضا تدخل في مجال الرقابة الوقائية السابقة على وقوع الجريمة والتي تجد أهميتها في مجال الضبط الإداري والذي سبق ونظمها المشرع الفرنسي بالقانون رقم 91- 646سالف الذكر وحدد مجالها، إذ نص على حالات اللجوء إلى هذا النوع من المراقبة الوقائية المتمثلة في حماية الأمن القومي ومصالح الاقتصاد الفرنسي وكذا مكافحة الإرهاب.[2]

- لمقتضيات التحريات والتحقيقات القضائية عندما يكون من الصعب الوصول الى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الالكترونية، والملاحظ هنا أن المشرع الجزائري لم يحدد الجرائم التي يلجأ فيها للمراقبة إ بعينها وهذا ما يفتح المجال لاستيعاب جميع الجرائم شرط أن يصعب الوصول فيها إلى أدلة تثبت وقوعها أو نسبتها لمرتكبيها، وهذا ما نص عليه المشرع الأمريكي بموجب القسم 18U.S.C sec. 2516من قانون خصوصية الاتصالات الإلكترونية سالف الذكر، الذي نص على ضرورة ن تكون المراقبة إ بصدد إحدى الجرائم المقررة في القسم 2516 (a)- (r) من ذات القانون.[3]

على خلاف المشرع الجزائري هناك بعض التشريعات المقارنة تقرر أن ضابط اتخاذ إجراء المراقبة إ هو فائدتها في إظهار الحقيقة وكشف غموض الجريمة، ويترك لقاضي التحقيق السلطة التقديرية في

1إن مصطلح "النظام العام" الذي استعمله المشرع في هذه الفقرة مصطلح واسع غير محدد المعالم لما يتضمنه النظام العام من عدة عناصر ولهذا كان على المشرع الجزائري ضبطه بتحديد عناصره المقصودة من هذه المادة منعا من حدوث إخلال بشأنه المساس بالحياة الخاصة للأفراد، ونحن نرى أن ذكر مصطلح النظام العام بهذا الشكل العمومي إنما يقصد به المشرع كل عناصر النظام العام ما دام أنه لم يحدد منها عنصر معين، كما أن هذه الجرائم قد تطال كل هذه العناصر والأسس الاجتماعية والاقتصادية والسياسية والخلقية والأمنية...الخ.

2رشيدة بوكر، الحماية الجزائية للتعاملات الإلكترونية، المرجع السابق، ص 341.

3عمر محمد بن يونس، الإجراءات الجنائية عبر الإنترنت في القانون الأمريكي، (المرشد الفيدرالي الأمريكي لتفتيش وضبط الحواسيب وصولا للدليل الإلكتروني في التحقيقات الجنائية)، ط1، موسوعة التشريعات العربية، 2005، ص 373.

تقدير مدى فائدة مراقبة الاتصالات الإلكترونية،[1] باعتبار أن السلطة القضائية هي صاحبة الاختصاص في منح الإذن حيث يمكن لها قبول أو رفض هذا الإجراء تبعا لفائدته من عدمها في الكشف عن الجريمة والمجرم الإلكتروني، وهذا ما نصت عليه كل من المواد 95و206من ق ا ج م، وكذا المادة 100من ق ا ج ف المشار إليهما سابقا.

إضافة إلى أنه قد حدد كل من المشرع المصري والفرنسي الجرائم التي تتخذ بشأنها عمليات المراقبة المتعلقة بالاتصالات بنوعيها السلكية واللاسلكية والإلكترونية وذلك في المواد 95و206من ق ا ج م، والمواد 706- 73و706- 73- 1من ق ا ج ف (والسابق بيانها في المبحث الأول الخاص بإجراءات التحري الخاصة)،

- في إطار تنفيذ المساعدة القضائية الدولية المتبادلة بين الدول: وتعرف المساعدة القضائية الدولية بأنها "إجراء قضائي تقوم به الدولة من شأنه تسهيل مهمة المحاكمة في دولة أخرى بصدد جريمة معينة[2]، ففعالية التحقيق والملاحقة القضائية في الجرائم الإلكترونية تقتضي تتبع اثر النشاط الإجرامي من خلال رصد الأجهزة والأماكن التي نفذ فيها هذا النشاط لتحديد مصدر الجريمة ومرتكبها، هذا ما يستلزم القيام بإجراءات خارج حدود الدولة الواحدة، ومن هنا تظهر أهمية تبادل المساعدة بين مختلف الدول والسلطات القضائية لها في مواجهة الإجرام بصفة عامة، الأمر الذي دعا العديد من المواثيق الدولية إلى النص على ضرورة التنسيق بين الدول بخصوص إجراءات التحقيق في هذه الجرائم، على رأسها الاتفاقية العربية لمكافحه جرائم الانترنت، وكذا الاتفاقية الأوروبية، واتفاقيه بودابست لسنة 2001،[3] كما نظمت بعض التشريعات من بينها المشرع الجزائري إجراءات المساعدة القضائية في المادة16من قانون 09/04سالف الذكر وبين إجراءات الاستجابة لطلبات المساعدة بموجب نص المادة17والمادة18من ذات القانون.[4]

وتتخذ المساعدة القضائية في المجال الجزائي صور عديدة منها: تبادل المعلومات والإجراءات بخصوص الجريمة والمجرم بين السلطات القضائية للدول، وهذا ما أكدته المادة33من الاتفاقية العربية

1عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في الإثبات الجنائي، المرجع السابق، ص 111.

2نعيم سعيداني، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، المرجع السابق، ص 89.

3يراجع هذه الاتفاقيات المشار إليها سابقا.

4 تنص المادة 17 من القانون رقم 09/04المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها : "تتم الاستجابة لطلبات المساعدة الرامية لتبادل المعلومات أو اتخاذ أي إجراءات تحفظية وفقًا للاتفاقيات الدولية ذات الصلة و الاتفاقات الدولية الثنائية و مبدأ المعاملة بالمثل".

كما تنص المادة 18من نفس القانون السابق : "يرفض تنفيذ طلبات المساعدة إذا كان من شأنها المساس بالسيادة الوطنية أو النظام العام . يمكن أن تكون الاستجابة لطلبات المساعدة مقيدة بشرط المحافظة على سرية المعلومات المبلغة أو بشرط عدم استعمالها في غير ما هو موضح في الطلب ".

لمكافحه جرائم تقنيه المعلومات[1] وكذا البنت الثالث والرابع والخامس من المادة الثامنة لاتفاقية الأمم المتحدة لمكافحه الجريمة المنظمة لسنه 2000، [2] وهو ما جسده المشرع الجزائري في المادتين 13و 14من القانون 09/04حيث نص على إنشاء هيئه وطنيه خاصة تنظم عمليه التنسيق وتبادل المعلومات بين مختلف الدول في مجال مكافحه الجرائم محل الدراسة، [3] وفي الفقرة 2من المادة 16سالفة الذكر، [4] فوفقا لهذه المادة يمكن تبادل طلبات المساعدة القضائية عن طريق وسائل الاتصال السريعة بما فيها أجهزة الفاكس والبريد الإلكتروني شرط التأكد من مدى قدرتها على توفير الحماية والأمن الكافي للمعلومات المرسلة والمستقبلة، وعلاوة على ذلك توفر هذه الوسائل السرعة في تبادل هذه الطلبات لتفادي ضياع الأدلة أو إتلافها من قبل الجناة، وتتم الاستجابة لهذه الطلبات وفقا للاتفاقيات الدولية الثنائية أو متعددة الأطراف ووفقا لمبدأ المعاملة بالمثل والتي كرسته العديد من الصكوك الدولية على رأسها اتفاقية بودابست والتي أكدت على أهمية التنسيق والتعاون في مجال مكافحة الإجرام المعلوماتي.[5]

كمالا يفوتنا أن ننوه أن الاستجابة لطلبات المساعدة القضائية ليست بالمسألة المطلقة بل تقيدها بعض الضوابط والشروط، فوفقا لنص المادة 18من القانون 09/04[6] يمكن رفض تنفيذ طلبات المساعدة إذا كان من شأنها المساس بالسيادة الوطنية أو النظام العام للدولة، كما يمكن أن تكون الاستجابة لهذه الطلبات مقيدة بشرط المحافظة على سرية المعلومات المبلغة أو بشرط عدم استعمالها في غير ما هو موضح في الطلب ومتفق عليه بين هذه الدول، ولفعالية هذه الإجراءات حثت اتفاقية بودابست في فقرتها الثالثة من المادة25، والاتفاقية العربية في فقرتها الثالثة من المادة32الدول الأطراف على تنفيذ إجراءات الإنابة بكافه الوسائل المتاحة بشكل يضمن سرعه وسلامه المعلومات المتبادلة، [7] وهو ما اعتمده المشرع الجزائري في الفقرة الثانية من المادة16من القانون 09/04سالف الذكر.

1ينظرالاتفاقية العربية لمكافحه جرائم تقنيه المعلومات المشار إليها سابقا.

2ينظراتفاقية الأمم المتحدة لمكافحه الجريمة المنظمة عبر الوطنية لسنه 2000المشار إليها سابقا.

3ليندا بن طالب، الدليل الإلكتروني ودوره في الإثبات الجنائي، المرجع السابق، ص 192.

4ينظر الفقرة 2من المادة 16من القانون رقم 09/04المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال المشار إليه سابقا.

5أدهم باسم نمر بغدادي، وسائل البحث والتحري عن الجرائم الإلكترونية، مذكرة ماجستير، كلية الدراسات العليا، جامعة النجاح الوطنية، نابلس، فلسطين، 2018، ص 84.

6ينظر المادة 18من القانون رقم 09/04المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال المشار إليه سابقا.

7بوكر رشيدة، الحماية الجزائية للتعاملات الإلكترونية، المرجع السابق، ص 410.

ب. تقييد مجال استعمال المعلومات المتحصل عليها من المر اقبة

تكون الترتيبات التقنية الموضوعة لأغراض المراقبة الالكترونية موجهة لتجميع وتسجيل المعطيات المتحصل عليها لاستعمالها في إثبات الجرائم المحددة حصرا في القوانين الجزائية، وتحديدا في المادة 04من القانون 09/04، [1]لهذا لا يجوز استعمال هذه المعلومات إلا في الحدود الضرورية التي نص عليها المشرع الجزائري وفقا لما جاءت به المادة 09من قانون 09/04حيث حددت هذه المادة حالات استعمال المعطيات المتحصل عليها من عمليات المراقبة بالحدود الضرورية للتحريات والتحقيقات القضائية، [2] وفي حالة استخدامها في غير الأغراض المقررة لها قانونا فإنه يتعرض المستخدمين المكلفين بإجراء المراقبة سواء كانوا مستخدمين تقنيين أو ضباط شرطة للمتابعة الجزائية، [3] كما يمنع قيام أي شخص أو هيئة مهما كانت طبيعتها بعمليات الاعتراض الإلكترونية للمعطيات الخاصة التي تعتبر من اختصاص الهيئة الوطنية دون سواها، [4] إلا أنه يمكن لها أن تطلب مساعدة من الوزارات أو السلطات المكلفة بشبكات الاتصالات.[5]

وتجدر الإشارة إلى أنه لم يستثنى القانون رقم 09/04في المواد 101112منه مسؤولية متعهدي ومقدمي خدمات الإنترنت في حالة عدم القيام بواجبهم في تقديم المساعدة للسلطات القضائية المكلفة بالتحري ووضع كل المعلومات والأدلة المتعلقة بتسجيل المعطيات والاتصالات الإلكترونية في حينها وكذا بوضع المعطيات التي يتعين عليهم حفظها وفقا للمادة 11من ذات القانون، تحت تصرف السلطات القضائية لكشف غموض الجريمة[6].

كما تجدر الإشارة إلى أنه يشترط أن تنفذ عملية المراقبة إ للاتصالات في سرية تامة ودون علم أو رضا المشتبه فيهم أو أصحاب الأماكن أو الأجهزة الإلكترونية المراد تتبعها، مع مراعاة عدم المساس بالسر المهني المقرر في نص المادة 45فقرة 4من ق ا ج ج، والمادة 56وما يليها من ق ا ج ف، إذ يلتزم مستخدمو الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال بالسر المهني وواجب التحفظ على

1التي تقابلها المواد 706-73و706- 73-1من ق ا ج ف، والمواد 95و206من ق ا ج م المشار إليهم سابقا.

2ينظر المادة 9من القانون رقم09/04سالف الذكر.

3ينظر المادة 26فقرة 1من المرسوم الرئاسي رقم 20-183المتضمن إعادة تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال المشار إليه سابقا

4ينظر المادة 26فقرة 2من نفس المرسوم.

5ينظر المادة 29من نفس المرسوم والتي تقابلها المادة 706- 102- 6من ق ا ج ف سالف الذكر.

6- خلايفية هدى، الإطار الدولي والداخلي لحماية الخصوصية على الإنترنت (التشريع الجزائري نموذجا)، المرجع السابق، ص 54.

المعطيات والاتصالات التي يتم جمعها، حيث يخضعون قبل تنصيبهم في مهامهم إلى أداء اليمين حسب ما ورد في المادة 27من المرسوم الرئاسي المنظم لتشكيلة هذه الهيئة.[1]

2. الضوابط الشكلية

تتمثل هذه الضوابط فيما لي:

أ. ضرورة الحصول على الإذن:

قيد القانون اللجوء إلى عملية المراقبة الإلكترونية للاتصالات بشرط الحصول على إذن قضائي مسبق لضمان تحقيق التوازن المناسب بين مصلحة العدالة والمجتمع في مكافحة الجرائم ومصلحة الفرد في حماية خصوصياته، إلا أنه هناك حالات أخرى تكون فيها هذه المراقبة مشروعة دون صدور هذا الإذن، سنتطرق إلى الحالتين في النقاط التالية:

- **حالة مراقبة الاتصالات الإلكترونية بناء على إذن:**

كما أشرنا سابقا _عند الحديث عن الضوابط القانونية الواجب مراعاتها عند إجراء اعتراض المراسلات وتسجيل الأصوات والتقاط الصور فقد اشترطت غالبية التشريعات المقارنة وجوب الحصول على إذن من السلطات المختصة لمباشرة هذه الإجراءات كونها تمس بخصوصية الأفراد وتنتهك سرية مراسلاتهم الخاصة، وإجراء المراقبة الإلكترونية للاتصالات لا يختلف كثيرا عن هذه الإجراءات، لهذا أوجبت أغلب القوانين ضرورة الحصول على إذن أو أمر قضائي مسبقا تطبيقا وتماشيا مع ما نصت عليه مختلف الدساتير المقارنة، كالدستور المصري والفرنسي والجزائري والأمريكي المشار إليهم سابقا، فبالرجوع للتشريع الأمريكي، فقد أجاز المشرع للسلطات القضائية المختصة مراقبة الاتصالات الإلكترونية شرط الحصول على أمر من أي قاضي فيدرالي أو محكمة المقاطعة أو قاضي محكمة الولاية طبقا لنص المادة 2703من قانون خصوصية الاتصالات الإلكترونية، شرط أن يستند هذا الأمر إلى أسباب معقولة تدعو للاعتقاد بأن محتوى الاتصالات له علاقة بجريمة جنائية ولهذا اشترط المشرع الأمريكي أن تضم استمارة طلب إجراء المراقبة إ للاتصالات جملة من الأسباب: كأن تبين أن إجراءات التحقيق العادية فشلت في كشف غموض الجريمة وأن هذه المراقبة سوف تكون بصدد جريمة معينة وأن لا تتجاوز هذه الأخيرة

1ينظر المادة 27من المرسوم الرئاسي رقم 20-183المتضمن إعادة تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال المشار إليه سابقا.

الاتصالات التي لا تشكل دليلا على تلك الجريمة[1]، وفي حالة قيام سلطات التحري والتحقيق بمراقبة وجمع محتويات أو اتصالات إلكترونية تشمل معلومات أكثر من تلك الواردة في الأمر بغير قصد فلا يجوز للسلطات أو للمحكمة الاعتماد على هذه المعلومات أو الأخذ بها كدليل لإثبات الجرائم، وهذا ما هو منصوص عليه بموجب المادة 3121، إضافة لهذا إذا صدر أمر بمراقبة اتصالات إلكترونية لشخص معين ومن خلال هذه العملية اكتشفت السلطات طرفا جديدا يجب مراقبته فهنا تنص المادة 3123أنه يجب على السلطات استصدار أمر جديد من المحكمة لمراقبة اتصالات هذا الشخص، [2] كما اشترط المشرع الفرنسي صدور أمر قضائي من قاضي التحقيق من أجل وضع ترتيبات تقنية لتتبع والتقاط الاتصالات الإلكترونية لغرض الوصول إلى البيانات الحاسوبية وجمعها وتسجيلها وذلك بموجب نص المادة 706-102- 1من القانون رقم 2016- 731سالف الذكر، أما عن المشرع المصري رغم عدم إفراده لنصوص خاصة تنظم مراقبة الاتصالات الإلكترونية بشكل صريح إلا أنه بالرجوع للمواد 95و206من ق ا ج م نجد أنه اشترط صدور أمر قضائي مسبب بالمراقبة سواء العادية أو الإلكترونية، حيث أجاز منح هذا الأمر من طرف قاضي التحقيق المختص دون غيره في حين لم يجز ذلك للنيابة العامة، في حين أنه نص صراحة على أنه يجب على قاضي التحقيق أن يصدر أمرا مسببا لمراقبة الاتصالات والمواقع الإلكترونية ذات الصلة بالجرائم الإرهابية وفقا للمادة 46من الباب الثاني من قانون مكافحة الإرهاب، [3]إلا أننا نرى أنه كان من الأجدر على المشرع المصري أن يفرد نصوص قانونية خاصة بالاتصالات الإلكترونية كما فعل المشرع الأمريكي والفرنسي مثلا، إذ يحدد فيها ماهية هذه الاتصالات وشروط وضوابط مراقبتها وتسجيلها وخصوصا أنه قد أصدر قانون تنظيم الاتصالات رقم 10لسنة 2003.

وعلى غرار هذه التشريعات فقد اشترط التشريع الجزائري هو الآخر هذا الإذن، فبالرجوع للمادة 04من القانون رقم 09/04سالف الذكر نجدها تجيز لضباط الشرطة القضائية مباشرة عملية المراقبة الإلكترونية للاتصالات بناء على إذن مكتوب صادر من السلطة القضائية المختصة وهنا ميز المشرع الجزائري بين حالتين: أولاهما عندما تتعلق المراقبة إ بالجرائم المذكورة في الفقرات "ب""ج""د"من المادة 04من قانون 09/04فيمنح الإذن بالمراقبة من طرف وكيل الجمهورية أثناء مرحلة التحري أو من قاضي

1ينظر المطلب الأول من المبحث الأول من هذا الفصل ص بخصوص مسألة تسبيب الإذن القضائي.

2محمود عبد الغني جاد المولى، دور الدليل الإلكتروني في الإثبات الجنائي (دراسة مقارنة)، دار الفكر الجامعي، ط 1، مصر، 2019، ص 101. هذا على خلاف المشرعين الفرنسي والجزائري إذ تقرر المادة 706-102-4من ق ا ج ف أنه إذا تم اكتشاف جرائم أخرى غير المشار غليها في الإذن أو الأمر الصادر من السلطة القضائية، فلا يترتب على ذلك بطلان إجراء المراقبة بالنسبة لهذه الجرائم العارضة أو الجديدة، وهو ما قرره المشرع الجزائري بشأن الجرائم العارضة المكتشفة في المادة 65مكرر 6فقرة 2من ق ا ج ج.

3محمود عبد الغني جاد المولى، دور الدليل الإلكتروني في الإثبات الجنائي، المرجع السابق، ص 111.

التحقيق أثناء مرحلة التحقيق الابتدائي وفقا للقواعد المنصوص عليها في قانون إ ج ج، بينما يمنح الإذن من طرف النائب العام لدى مجلس قضاء الجزائر العاصمة لضباط الشرطة القضائية المنتمين إلى الهيئة الوطنية للوقاية من الجرائم الإلكترونية المنصوص عليها في المادة 13من هذا القانون، عندما يتعلق الأمر بمراقبة الاتصالات من أجل الوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة المذكورة في الفقرة "أ"من المادة 04من ذات القانون[1].

ويقدم الإذن بناء على تقرير يبين طبيعة الترتيبات التقنية المستعملة والأغراض الموجهة إليها، حيث يشترط المشرع أن تكون هذه الترتيبات التقنية المستعملة موجهة حصريا لتجميع وتسجيل معطيات إلكترونية ذات صلة بالوقاية من هذه الأفعال، إذ تكلف بوضع هذه الترتيبات مديرية المراقبة الوقائية واليقظة الإلكترونية الموجودة على مستوى الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال[2] بناء على رخصة من السلطة القضائية المختصة وتحت مراقبتها، حيث تقوم بمراقبة الاتصالات إ للوقاية من الجرائم الموصوفة بالأفعال الإرهابية والتخريبية والاعتداء على أمن الدولة، وكذا جمع وتسجيل المعطيات الرقمية وتحديد مصدرها والقيام بتتبعها بغرض استعمالها في الإجراءات القضائية، [3] ولتنفيذ هذه العمليات تضع المديرية التجهيزات اللازمة والوسائل التقنية الضرورية على مستوى كل من المنشآت القاعدية للمتعاملين ومقدمي الخدمات، كما تلزمهم بتقديم المساعدة الضرورية لها من أجل تنفيذ مهامها.[4]

1تنص المادة 04من ق 09/04المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال على:"يمكن القيام بعمليات المراقبة المنصوص عليها في المادة 3أعلاه في الحالات الآتية:

أ. للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة.

ب. في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني.

ت. لمقتضيات التحريات والتحقيقات القضائية عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الإلكترونية.

ث. في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة.

لا يجوز إجراء عمليات المراقبة في الحالات أعلاه إلا بإذن مكتوب من السلطة القضائية المخنصة.

=...عندما يتعلق الأمر بالحالة المنصوص عليها في الفقرة "أ"من هذه المادة، يختص النائب العام لدى مجلس قضاء الجزائر بمنح ضباط الشرطة القضائية المنتمين للهيئة المنصوص عليها في المادة 13أدناه، إذنا لمدة ستة (6) أشهر قابلة للتجديد وذلك على أساس تقرير يبين طبيعة الترتيبات التقنية المستعملة والأغراض الموجهة لها...".

2ينظر الفصل الأول من الباب الأول أين تم التطرق بالتفصيل لتشكيلة هذه الهيئات وتبيان مهامها.

3ينظر المادة 15من المرسوم الرئاسي رقم 20-183المتضمن إعادة تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال المشار إليه سابقا.

4ينظر المادة 17من نفس المرسوم.

وتجدر الإشارة إلى أنه حتى يكون هذا الإذن صحيحا ومنتجا لآثاره القانونية ولا يتعرض للبطلان من طرف السلطة القضائية وجب أن يتضمن مجموعة من العناصر الأساسية وفي هذا الصدد نحيل إلى ما سبق ذكره في المطلب الأول الخاص باعتراض المراسلات السلكية واللاسلكية منعا من تكرار ما تم التطرق إليه باعتبار العناصر المتطلبة في الإذن باعتراض المراسلات التقليدية أو الإلكترونية هي نفسها، إذ تختلف فقط فيما يخص ضرورة وصف التقنيات المستعملة في عملية المراقبة الإلكترونية وكذا نظام المعالجة الآلية المراد مراقبته وصفا مفصلا وفقا لما نصت عليه المواد 706- 102- 2من ق ا ج ف، والمادة 65مكرر 7من ق ا ج ج.[1]

1. حالة مر اقبة الاتصالات الإلكترونية بدون إذن:

الأصل أن اعتراض ومراقبة الاتصالات الإلكترونية أسلوب غير مشروع إلا في حدود معينة والمتمثلة في الحصول على إذن قضائي مسبب من طرف السلطة المختصة كما أسلفنا الذكر، إلا أنه قد أجازت بعض التشريعات هذا الاعتراض بدون صدور إذن بذلك، وذلك في بعض الحالات ولمبررات معينة، تتمثل هذه الأخيرة فيما يلي:

أ. حالة المر اقبة المعتادة لمزود الخدمة

سمحت بعض التشريعات لمزود خدمة الاتصال أو الإنترنت بمراقبة الاتصالات إ الخاصة بالمشتركين في خدماته وذلك في إطار العمل اليومي لشبكاتهم من أجل حماية أنظمتهم المعلوماتية والخدمات التي يقدمونها للمشتركين من أي ضرر يمكن أن يلحق بها أو تحسبا لأي طارئ، مثل الاستيلاء عليها بالسرقة أو زرع فيروسات تخريبية، ولعل أهم هذه التشريعات التي سمحت بهذا الإجراء المشرع الأمريكي في القسم 2511 (2) (a) من قانون خصوصية الاتصالات الإلكترونية، ولكن مع احترام ضرورة التوازن بين احتياجات مزودي الخدمة في حماية حقوقهم وملكيتهم وبين حق المشترك في حماية خصوصية اتصالاته، ولهذا قيد المشرع الأمريكي هذه المراقبة بجملة من الشروط المتمثلة في:[2]

- أن يكون مزود الخدمات ضحية جريمة.
- أن يقوم بمراقبة الاتصالات الإلكترونية والتبليغ عن الجرائم التي تصل لعلمه إلى الجهات القضائية حماية لحقوقه وليس قياما بدور المساعد لهذه السلطات في التحريات والتحقيقات التي تقوم

1ينظر المطلب الأول من المبحث الأول من هذا الفصل.

2عمر محمد أبو بكر بن يونس، الإجراءات الجنائية عبر الإنترنت في القانون الأمريكي، المرجع السابق، ص 380- 386.

بها، كما يشترط أن تكون المبادرة بالتبليغ من جانب مزود الخدمة وليس بناء على طلب من سلطات التحقيق.

- ألا يشارك رجل الضبط القضائي مع مزود الخدمة في عملية المراقبة التي يقوم بها.

ب. حالة المر اقبة بناء على شكوى من المشترك

اختلفت التشريعات المقارنة حول مدى إمكانية السماح لمقدم خدمة الاتصال بمراقبة الاتصالات الإلكترونية بناء على شكوى من مشترك متضرر، من خلال مراقبة مراسلاته الواردة والصادرة من جهازه الإلكتروني محل المراقبة، إذ انقسمت في هذا إلى اتجاهين: اتجاه يرى أن مقدم الخدمات متماثل في عمله مع رجال الضبط القضائي ولهذا ليس له الحق في مراقبة اتصالات المشتكي بدون إذن، وهو الاتجاه السائد في كندا باعتبار أن قيامه بهذا الإجراء بدون إذن يخالف أحكام المادة 24- 2من ميثاق الحقوق والحريات الكندي.[1]

أما الاتجاه الثاني فيؤيد هذا النوع من المراقبة، وهو الاتجاه الذي أخذ به المشرع الأمريكي حيث يسمح القسم 2511 (2) (a)لضحايا هجومات الحواسيب والإنترنت بتفويض السلطات بمراقبة الاتصالات إ للشخص المتضرر ولكن بشروط معينة حددها القانون الأمريكي وتتمثل في:[2]

- أن يسمح المالك أو صاحب الحق لرجال الضبط القضائي بوضع الجهاز الخاص به تحت المراقبة وفقا للقسم (1) 2511 (2) (a).
- أن تتوافر دلائل كافية على أن هذه المراقبة تفيد في كشف الحقيقة.
- أن يتم ذلك في إطار تحقيق جنائي قائم وفقا للقسم (3) 2511 (2) (a).
- أن يقتصر رجال الشرطة على مراقبة الاتصالات الواردة والصادرة من وإلى الجهاز محل التحقيق أي لا تتطرق المراقبة لغير الاتصالات التي تم بثها من قبل المنتهك وفقا للقسم (4) 2511 (2) (a).

كما أن مراقبة المعلومات أو المعطيات المتعلقة بالمشترك أو العميل مثل هويته، عنوانه، سجلات الاتصال التي تبين المكالمات الصادرة والواردة، رقم الهاتف، وكذا عنوان IPالخاص بجهازه، والمعلومات الخاصة بالاتصال والتي لا تشمل مضمون الاتصال مثل عناوين البريد الإلكتروني، [3] فإنه لا يشترط

1رشيدة بوكر، الحماية الجزائية للتعاملات الإلكترونية، المرجع السابق، ص 343.

2عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في الإثبات الجنائي، المرجع السابق، ص 109.

3والتي حددتها المادة (c) 2703 .U.S.C18من قانون خصوصية الاتصالات الإلكترونية الأمريكي.

القانون صدور إذن قضائي لقيام مزود الخدمة بالكشف عنها للسلطات القضائية المختصة، بل يحتاج ذلك مذكرة استعلام تقدمها السلطات القضائية لمزود الخدمة من أجل الحصول على المعلومات المطلوبة، [1] وهذا ما أكد عليه القضاء الأمريكي في العديد من القضايا من بينها قضية Morganعام 1998، [2] كما أكد على ذلك الدستور الأمريكي في تعديله الرابع إذ قضى أن المعلومات الخاصة بالمشترك سواء الخاصة بهويته أو باتصالاته الإلكترونية التي يجريها لا تتمتع بالحماية الدستورية المقررة للمعلومات التي تضم المحتوى أو المضمون الفعلي للاتصالات، [3] وهذا ما أكده القضاء الأمريكي وقررته الدائرة العاشرة الفيدرالية في قضية Perrineعام 2008[4] بقولها: "لا يتمتع المتهم بالحق في الخصوصية وبالحماية المقررة له في التعديل الرابع من الدستور بشأن المعلومات الخاصة بهويته والموجودة لدى مزود خدمة الاتصال الإلكتروني، أما المحتوى الفعلي للاتصال فهو الذي يتمتع بحماية التعديل الرابع للدستور وذلك في ضوء أحكام القسم رقم (d) 2703 .U.S.C18من قانون خصوصية الاتصالات الإلكترونية". [5]

وهو نفس الوضع الذي قرره القانون الفرنسي بموجب المادة 34-1[6] من قانون البريد والاتصالات الإلكترونية والتي قررت أن المعلومات التي تتعلق بهوية المشترك ونوع الخدمة يمكن للسلطات القضائية

1محمود عبد الغني جاد المولى، دور الدليل الإلكتروني في الإثبات الجنائي، المرجع السابق ص 84.

2تتلخص وقائع هذه القضية في أن السيد Morgan Jessupوزوجته السيدة Barbara Smithكانوا أطراف في دعوى طلاق مرفوعة أمام محكمة Oaklandفي ولاية Michigan، وعقب ذلك قام الزوج باستخدام مواقع التواصل الاجتماعي AOLفي نشر رسالة تحت اسم مستعار على أنه هو السيدة Barbaraإذ تحتوي هذه الرسالة على أن هذه السيدة تريد تكوين صداقة مع أي شخص آخر ورقم هاتفها للاتصال بها، وبعدها بدأت هذه السيدة تتلقى مكالمات عديدة سخيفة إلى أن عرفت بموضوع الرسالة المنشورة على مواقع التواصل، فقدمت شكوى لشركة AOLلمعرفة مصدر الرسالة وبالفعل اكتشفت أنه السيد Morganفتقدمت ببلاغ ضده وطالبته بالتعويض المالي، إلا أن المتهم دفع بأن شركة الاتصال هذه خالفت قانون خصوصية الاتصالات الإلكترونية لأنها كشفت عن محتوى الاتصالات الخاصة به دون إذن قضائي، فردت الشركة بأنها لم تخالف القانون لأنها لم تفصح عن المضمون الفعلي للرسالة بل أفصحت عن هوية المرسل وخاصة أنه خالف التعاقد مع الشركة واستخدم اسم مستعار في نشر هذا النوع من الرسائل، كما أضافت أن المادة18 U.S.C 2703تشترط صدور إذن قضائي بخصوص إجبار مزودي الخدمات على تقديم المحتوى الفعلي للاتصالات متى كانت ذات صلة بالتحقيق الجنائي الجاري، وعلى ذلك أدانت المحكمة السيد Morgan.

3ينظر التعديل الدستوري الرابع للولايات م أ المشار إليه سابقا.

4تتلخص وقائع قضية بيرين Perrine في أن السيد James قام بإبلاغ الشرطة أنه أثناء محادثة له عبر غرف الدردشة مع الشخص يدعى قام هذا الأخير بعرض فيديوهات وصور فتيات قاصرات مخلة بالحياء، فقام السيد James بطلب الشرطة وطلب منه أن يعرض له المزيد من الصور والفيديوهات إلا أن هذا الأخير توقف عن الإرسال ولكن السيد جيمس قام بنسخ من المحادثة وبهذا أصدرت السلطات أمرا بالكشف عن المعلومات الخاصة بالعميل من طرف شركة ياهوو YAHOO حيث جاء تقرير الشركة أن عنوان البروتوكول لهذا الموقع تابع لشركة معينة وعليه أصدرت السلطات أمرا لهذه الشركة للكشف عن هوية صاحب هذا الحساب وتم كشفه وهو المدعو Perrine وقامت السلطات بإصدار أمر بتفتيش منزله وحاسوبه ليكتشف أنه متابع قضائيا في الكثير من القضايا من هذا النوع، نقلا عن محمود عبد الغني جاد المولى، دور الدليل الإلكتروني في الإثبات الجنائي، المرجع السابق، ص 87.

5محمود عبد الغني جاد المولى، دور الدليل الإلكتروني في الإثبات الجنائي، المرجع السابق، ص 88.

6Voir l'article n° 34 -1 du code de poste et des communications électroniques.

الاطلاع عليها دون إذن قضائي في حين لا يجوز الاطلاع على محتوى الاتصالات أو الكشف عنها إلا بإذن قضائي صادر من قاضي الحريات والحبس كما بينا سابقا.[1]

ومن زاوية أخرى يثار التساؤل حول مدى إمكانية مزود الخدمة من الكشف عن محتويات سجل الاتصالات للسلطات القضائية بدون إذن وبصورة إرادية أي برضا المزود، وهنا تباينت الآراء باختلاف النظم الإجرائية للتشريعات المقارنة، حيث فرق القانون الأمريكي بين أمرين: أولهما إذا كان مزود الخدمة يقدم خدمة متاحة للجمهور فلا يجوز له الكشف عن محتويات الاتصال إلا بناء على إذن قضائي أو في الحالات الاستثنائية المنصوص عليها في القسم(c)2702، [2] أما إذا كانت الخدمة التي يقدمها المزود غير متاحة للجمهور فيجوز له الكشف عنها للسلطات القضائية بصورة إرادية وبدون إذن قضائي وهذا ما قرره القضاء الأمريكي في قضية Andersen.[3]

أما عن القانون الفرنسي فقد قررت المادة 16من قانون الاتصالات الإلكترونية رقم 669-2004الصادر في 9يوليو 2004أنه يحق للهيئة التي تنظم الاتصالات في رفض الكشف عن الوثائق التي تحوي اتصالات المشتركين حفاظا على سريتها، في حين ألزمت المادة 58من قانون تنظيم الاتصالات المصري سالف الذكر، جهاز تنظيم الاتصالات بالحفاظ على سرية البيانات الخاصة بالعملاء حماية لخصوصيتهم ورفضت أي كشف لهذه المعلومات إلا بناء على طلب كتابي من السلطات.[4]

ت. مدة المراقبة:

يعتبر تحديد مدة المراقبة إ ضمانة لعدم تعسف السلطات المختصة في إساءة استعمال سلطتهم وانتهاك خصوصية الاتصالات إ للأفراد، ولهذا نجد أغلب التشريعات حرصت على تحديد وضبط هذه المادة، من بينها المشرع الأمريكي حيث قرر في القسم 3123من قانون خصوصية الاتصالات الإلكترونية سالف الذكر، أن المدة التي يجوز اتخاذ هذا الإجراء خلالها تقدر ب 60يوما قابلة للتجديد لمدة أخرى

1محمود عبد الغني جاد المولى، دور الدليل الإلكتروني في الإثبات الجنائي، المرجع السابق، ص 95.

2والمتمثلة في : حالة الكشف الضروري لحماية حقوق الملكية لمزود الخدمة نفسه، وحالة حصول السلطات على معلومات بدون قصد من مزود الخدمة، ثم ظهر أنها ذات علاقة بجريمة ارتكبت، وفي الحالات الضرورية الطارئة مثل تعرض شخص للموت أو الإصابات الجسدية الخطيرة إذا لم يتم الكشف عن المعلومات، وفي حالات قانون حماية الطفل والاستغلال الجنسي، وإذا كان ذلك لمستقبل الاتصال وبموافقة المرسل.

3لمعرفة تفاصيل هذه القضية ينظر محمود عبد الغني جاد المولى، دور الدليل الإلكتروني في الإثبات الجنائي، المرجع السابق، ص 98

4المرجع نفسه، ص 99.

بقرار مسبب من المحكمة، كما أورد استثناء بخصوص الحالات الطارئة والتي تكون فيها مدة المراقبة 48ساعة فقط من لحظة بدأ عملية المراقبة وتركيب أجهزة التتبع.[1]

أما عن المشرع الفرنسي فقد حدد هذه المدة بأربعة (4) أشهر قابلة للتجديد بموجب المادة 706-102- 3من ق ا ج ف سالف الذكر، في حين أن المشرع المصري لم يفرق بين مدة مراقبة الاتصالات السلكية والإلكترونية والتي حددها بموجب المادة 95والمادة 206من ق ا ج م، والمقدرة بثلاثين يوما قابلة للتجديد ممد أخرى.

أما عن المشرع الجزائري فبالرجوع لنص المادة 03من القانون رقم 09/04فإنها تشير غلى ضرورة مراعاة القواعد المنصوص عليها في ق ا ج والقانون المتعلق بالوقاية من الجرائم إ 09/04في حالة وضع ترتيبات لمراقبة الاتصالات إ وهذا ما يوحي أن المادة 65مكرر 5من ق ا ج وما تضمنته من قيد سريان مدة اعتراض المراسلات السلكية واللاسلكية المحددة بأربعة (4) أشهر قابلة للتجديد ينطبق على مراقبة الاتصالات إ، في حين أن المدة المحددة في القانون رقم 09/04بستة (6) أشهر قابلة للتجديد إنما تخص مراقبة الاتصالات إ المتعلقة بالجرائم المحددة في الفقرة "أ"من المادة 4من هذا القانون والمتمثلة في جرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة فقط بينما يتم الرجوع في بقية الحالات إلى أحكام المادة 65مكرر 5من ق ا ج ج، ومع ذلك إلا أنه كان على المشرع ج أن يضبط المدة بدقة وبصراحة في قانون 09/04لعدم تعسف السلطات في استعمالها مساسا بخصوصية الأفراد، ودفعا للغموض والعموم الذي يتنافى ومبدأ الشرعية الجنائية الإجرائية.[2]

كما تجدر الإشارة إلى أنه على ضابط الشرطة القضائية المكلف بإجراء المراقبة إ أن يحرر محضر بالعمليات التي قام بها إذ نجد أغلب التشريعات توجب هذا الإجراء كالمشرع المصري[3] والأمريكي والفرنسي[4] وكذا الجزائري[1] كما ذكرنا سابقا، حيث يشمل كل محضر تاريخ وساعة بداية العملية ونهايتها وكذا

1محمود عبد الغني جاد المولى، دور الدليل الإلكتروني في الإثبات الجنائي، المرجع السابق ، ص 102.

2جزول صالح، الخصوصية الإجرائية للجرائم الماسة بأنظمة المعالجة الآلية للمعطيات في التشريع الجزائري، إصدارات المركز الديمقراطي العربي للدراسات الإستراتيجية والسياسية والاقتصادية، الجريمة المعلوماتية وأثرها على التنمية الاقتصادية، ط 1، برلين- ألمانيا، جويلية 2020، ص 70.

3ينظر المادة 206من ق ا ج المصري.

4 l'article n° 706-102-7 du code de procédure pénale dispose que : « Le juge d'instruction ou l'officier de police judiciaire commis par lui ou requis par le procureur de la République dresse procès Verbal de chacune dès opérations de mise en place du dispositif technique Mentionne aux articles 706-1002-1 et 706–102-2 et des Opérations de Captation des données informatique ceprocès Verbal mentionner la date et l'heure auxquelles Opération a

الظروف التي تمت فيها، فيجب على ضابط الشرطة أن يقدم تقريرا مفصلا عن عمل الأجهزة الإلكترونية المستخدمة والترتيبات التقنية المتخذة في هذا الإجراء، كما يرفق بملف الدعوى محضر يتضمن وصفا أو نسخة من مضمون الاتصالات أو السجلات المضبوطة التي تم تسجيلها وتجميعها حيث يتم وضعها في وسائط تخزين معلوماتية مثل: القرص الصلب والقرص المرن أو الذاكرة الوميضية...الخ، ويتم تحريزها وختمها للحفاظ عليها من أي تلف أو تحوير من جهة، وضمان سريتها من جهة أخرى[2] وفقا لما نصت عليه المادة 25من المرسوم 20-183سالف الذكر والتي أحالت هذه المسألة إلى أحكام قانون إ ج ج.[3]

وكما أشرنا سابقا بخصوص مصير التسجيلات المتحصلة من عمليات اعتراض المراسلات السلكية واللاسلكية فإن القانون الفرنسي تطرق لهذه المسألة أيضا بخصوص السجلات والمعطيات المعلوماتية المحصلة من عملية المراقبة الإلكترونية، إذ نص على ضرورة إعدامها وإتلافها بعد الانتهاء منها بناء على طلب النيابة العامة[4] وفقا لما جاء في نص المادة 706-102-9من ق ا ج ف،[5] في حين لم يتطرق المشرع الجزائري ولا المشرع المصري مرة أخرى لمصير هذه التسجيلات الإلكترونية.

المطلب الثاني : تفتيش النظم المعلوماتية وحجز المعطيات المتواجدة بها

تهدف إجراءات التحري والتحقيق في الجريمة الإلكترونية إلى ضبط الأدلة التي تفيد في كشف الجريمة ونسبتها إلى مرتكبها، ولما كان إجراء التفتيش من أخطر هذه الإجراءات لما ينطوي عليه من مساس وانتهاك صارخ لحقوق وحريات الأفراد وخصوصياتهم، لكون محل التفتيش في هذه الجرائم يتميز بالطابع اللامادي حيث لا يعدو أن يكون إلا معلومات وبيانات إلكترونية ليسل لها مظهر محسوس في العالم المادي، هذا ما أثار عدة إشكالات حول إمكانية تفتيشها وضبطها، وعليه فما مدى قابلية هذه البيانات للتفتيش والضبط في البيئة الإلكترونية؟ وما هي أهم الضوابط التي أقرها المشرع بهذا الخصوص؟

---

commencé et celles auxquelles elle s’est terminée, les enregistrements Des données informatiques Sans places sous scelles

1ينظر المادة 65مكرر 9من ق ا ج الجزائري.

2ينظر المادة 65مكرر 10فقرة 1من ق ا ج ج والتي تقابلها المادة 706-102-7من ق ا ج المصري.

3ينظر المادة 45من ق ا ج ج المشار إليها سابقا.

4محمود عبد الغني جاد المولى، دور الدليل الإلكتروني في الإثبات الجنائي، المرجع السابق، ص 106.

5Article n° 706-102-9du code de procédure pénale dispose que : « les enregistrements des données informatiques sont détruits a la diligence du procureur de la république ou du procureur général a l’expiration du délai de prescription de l’action publique »

وهذا ما لم ينص عليه المشرع الجزائري إذ لم بين في جميع الحالات ما مصير هذه التسجيلات الإلكترونية التي تم تجميعها من خلال مراقبة الاتصالات، كما فعل بخصوص التسجيلات المحصلة من عمليات اعتراض وتسجيل المراسلات السلكية واللاسلكية المنظمة بالقانون 06-22المتضمن ق ا ج ج كما أشرنا سابقا، لمزيد من التفاصيل ينظر المطلب الأول من المبحث الأول.

الفرع الأول: التفتيش الإلكتروني

ولهذا يعتبر إجراء التفتيش في البيئة الإلكترونية من بين أهم هذه الإجراءات، إلا أنه يتميز ببعض الخصوصية والاستثناء عن نظيره التقليدي، سواء من حيث إجراءات تنفيذه أو من حيث الشروط والضمانات التي يجب على سلطة التفتيش التقيد بها أثناء مباشرته، وهذا ما سنحاول تفصيله في النقاط التالية.

أولا: تعريف التفتيش الإلكتروني

يعرف التفتيش بصفة عامة على أنه إجراء من إجراءات التحقيق يباشره موظف مختص طبقا للإجراءات المقررة قانونا، في محل يتمتع بحرمة، بهدف البحث عن أدلة مادية لجناية أو جنحة تحقق وقوعها لغرض إثباتها ونسبتها إلى المتهم [1] وقد يتطلب التحقيق تفتيش شخص المتهم أو منزله أو غيره لضبط الأشياء المتعلقة بالجريمة، كما عرفه البعض على أنه: "الاطلاع على محل منح له القانون حرمة خاصة باعتباره مستودع سر صاحبه، فلا يجوز الاطلاع عليه أو على ما بداخله إلا في الأحوال المنصوص عليها قانونا أو برضا صاحبه، وقد يكون محل التفتيش الشخص أو المسكن أو محل آخر ألحقه القانون في الحكم بالمسكن أو الشخص، والغاية من التفتيش هي البحث عن الأشياء المتصلة بالجريمة الجاري التحقيق بشأنها"، [2] إذ يفهم من هذا التعريف أن محل التفتيش لا يقتصر على محل الشخص أو مسكنه بل يتجاوز ذلك إلى محل الجريمة الإلكترونية المتمثل في البيانات والمعلومات الرقمية، وهذا ما يستنتج من خلال عبارة "محل آخر ألحقه القانون في الحكم بالمسكن أو الشخص"والذي يستوي أن يكون محلا إلكترونيا.

ومن جانب أخر قد عرف المجلس الأوروبي التفتيش الإلكتروني بأنه إجراء يسمح بجمع الأدلة المخزنة أو المسجلة بشكل إلكتروني، عن طريق استخدام وسائل إلكترونية في البحث .[3]

وعليه من خلال استقراء هذه التعريفات يمكن القول بأن التفتيش الإلكتروني هو البحث عن أدلة الجريمة في أجهزة الحاسب الآلي التي استخدمت في ارتكابها أو من خلال شبكات الاتصال مثل شبكة الإنترنت، حيث يتم تنفيذ هذه العملية بقيام سلطات التحقيق بالدخول للنظام الحاسوبي الذي ارتكبت

1عبد الفتاح بيومي حجازى، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر الإنترنت، المرجع السابق، ص 192.

2رفاه خضير جياد العارضي، الدليل الإلكتروني وأثره في مجال نظرية الإثبات الجنائي، المرجع السابق، ص 114

3صالح شنين، الحماية الجزائية للتجارة الإلكترونية، أطروحة مقدمة لنيل شهادة الدكتوراه في القانون الخاص، كلية الحقوق، جامعة أبو بكر بلقايد، تلمسان، 2012/2013، ص 234. عدلي سابق؟؟؟

فيه أو من خلاله الجريمة وذلك لبحث أو فحص البيانات الموجودة به، ولهم في ذلك القيام بعرض البيانات أو المعلومات المخزنة على القرص الصلب من خلال شاشة الحاسوب أو من خلال ضبط محتوى الاتصالات الإلكترونية.[1]

كما يختلف التفتيش القضائي عن التفتيش الوقائي والتفتيش الإداري الذي يقوم به بعض الموظفين العموميين ومن في حكمهم، وذلك لأهداف وقائية، إذ يهدف التفتيش القضائي إلى البحث عن الدليل في جرائم معينة بينما لا يطبق على التفتيش الوقائي قواعد قانون الإجراءات الجزائية ولا يقصد به البحث عن أدلة، وإنما هو إجراء بوليسي تمليه ضرورة الأمن حفاظا على سلامة الشخص محل التفتيش أو غيره، كتجريد شخص مما يحمله من أسلحة أو أدوات قد يستخدمها في الاعتداء على نفسه أو غيره، [2]أما عن التفتيش الإداري فهو ذلك الإجراء الذي يهدف إلى تحقيق إغراض إدارية تتعلق بالحفاظ على الأمن العام والنظام العام تقوم به السلطات العامة على الأماكن والمحلات العامة التي يمكن للعامة دخولها مثل مقاهي الإنترنت والمؤسسات التي تقدم خدمة الإنترنت كمزود الدخول ومزود خدمات الإنترنت طالما أن القانون يبيح لرجال السلطة العامة الدخول وإجراء تفتيش إداري في هذه الأماكن بغية الحفاظ على الأمن والنظام العموميين كأحد أهداف ومهام سلطات الضبط الإداري، [3]وفي حالة ما أسفر هذا التفتيش عن ضبط جريمة جنائية متلبس بها كان هذا الضبط صحيحا وينتج أثاره القانونية.[4]

وتجدر الإشارة أن بعض الفقه يرى أنه من الأفضل استخدام مصطلح "الولوج أو النفاذ"على عملية البحث والتفتيش في البيئة الرقمية، باعتباره المصطلح الدقيق بالنسبة للمصطلحات المعلوماتية، في حين أن مصطلح "التفتيش" بمعنى البحث والتقصي والتفحص فهو مصطلح تقليدي أكثر يتلاءم والجرائم التقليدية، إلا أننا نرى الكثير يستخدم المصطلحين معا للتنسيق بين المفاهيم التقليدية والحديثة وهذا ما نستشفه من المادة 19من الاتفاقية الأوروبية لجرائم الإنترنت.[5]

هذا من جهة ومن جهة أخرى قد أثار تفتيش النظم المعلوماتية زيادة على مسألة التناقض في المصطلحات، جدلا فقهيا حول طبيعته في مجال النظم المعلوماتية ما إذا كان إجراء خاص بمرحلة

1محمود عبد الغني جاد المولى، دور الدليل الإلكتروني في الإثبات الجنائي، المرجع السابق، ص 120

2هلالي عبد اللاه أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، (دراسة مقارنة) ط 1، دار النهضة العربية، القاهرة، مصر، 1997، ص 53.

3عمر محمدأبو بكر بن يونس، الجرائم الناشئة عن استخدام الإنترنت (الأحكام الموضوعية والجوانب الإجرائية)، المرجع السابق، ص 855.

4عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر الإنترنت، المرجع السابق، ص 193.

5نبيلة هبة هروال، الجوانب الإجرائية لجرائم الإنترنت، المرجع السابق، ص 223.

الاستدلال أم بمرحلة التحقيق الابتدائي فقط، وفي هذا انقسم الفقه إلى عدة طوائف تباينت آرائهم واختلفت حججهم في تبرير طبيعة هذا الإجراء وذلك كما يلي:

- **الاتجاه الأول:**

يأخذ أنصار هذا الاتجاه في تحديدهم لطبيعة التفتيش الإلكتروني بالهدف المرجو منه، وعليه يعتبر هذا الإجراء من إجراءات التحقيق لأنه يهدف إلى البحث عن الأدلة وضبطها وكشف حقيقة الجريمة ونسبتها إلى مرتكبها، وهو الرأي الذي أخذ به غالبية الفقه والقضاء في فرنسا ومصر،[1] وما نصت عليه مختلف النصوص القانونية، كالمادة 91من ق ا ج م،[2] والمادة 80من قانون الإجراءات الجنائية السعودي.[3]

- **الاتجاه الثاني:**

يرى أصحاب هذا الاتجاه أن التفتيش كإجراء تتحدد طبيعته حسب المرحلة التي تكون فيها الدعوى الجزائية، فإذا ما تم قبل تحريكها فيعد إجراء من إجراءات الاستدلال، أما إذا تم بعد ذلك يعتبر من إجراءات التحقيق الابتدائي، إلا أن هذا المعيار لا يمكن الاعتداد به في الجرائم الإلكترونية نظرا لطبيعتها الخاصة فقد تضطر سلطة التحقيق إلى القيام ببعض أعمال التحري والاستدلال.[4]

- **الاتجاه الثالث:**

يستند أصحاب هذا الاتجاه في تحديد طبيعة إجراء التفتيش إلى صفة القائم به، إذ يعتبر إجراء من إجراءات التحقيق إجراءات التحقيق إذا قام به أحد أعضاء التحقيق كقاضي التحقيق، في حين يكون من إجراءات الاستدلال إذا قام به أحد ضباط الشرطة القضائية،[5] إلا أننا نرى أن هذا المعيار ليس صحيحا في تحديد طبيعة التفتيش لأن القانون الإجرائي لا يعتد بصفة القائم بالإجراء ليحدد طبيعته، فبالرجوع

1هلالي عبد اللاه أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، المرجع السابق، ص 51.

2تنص في المادة 91من ق ا ج م على أن: "تفتيش المنازل عمل من أعمال التحقيق ولا يجوز الالتجاء إليه إلا بمقتضى أمر من قاضي التحقيق بناء على اتهام موجه إلى شخص يقيم في المنزل المراد تفتيشه بارتكاب جناية أو جنحة أو باشتراكه في ارتكابها، أو إذا وجدت قرائن تدل على أنه حائز لأشياء تتعلق بالجريمة"

3تنص المادة 80 فقرة 1 من ق ا ج السعودي على: " تفتيش المساكن عمل من أعمال التحقيق ولا يجوز الالتجاء إليه إلا بناء على اتهام بارتكاب جريمة موجه إلى شخص يقيم في المسكن المراد تفتيشه أو باشتراكه في ارتكابها...".

4حسين ربيعي، آليات البحث والتحقيق في الجرائم المعلوماتية، المرجع السابق، ص 111.

5 المرجع نفسه، ص 111.

لبعض القوانين الإجرائية كالقانون الجزائري والفرنسي نجد أنها تخول لضباط الشرطة القضائية استثناء القيام ببعض إجراءات التحقيق من بينها التفتيش وفي حالات محددة قانونا، كحالة التلبس بالجريمة وحالة الإنابة القضائية.

- **الاتجاه الرابع:**

حاول أنصار هذا الاتجاه التوفيق بين كل المعايير السابقة، إذ يعتبر التفتيش حسب معيارهم المختلط إجراء من إجراءات التحقيق إذا ما قامت به سلطة التحقيق وبعد تحريك الدعوى الجزائية بغية الكشف عن حقيقة الجريمة والمجرم، وهذا ما أخذت به محكمة النقض المصرية بقولها: "إن التفتيش بحسب الأصل إجراء من إجراءات التحقيق لا تأمر به إلا سلطة من سلطاته وبمناسبة جريمة_ جناية أو جنحة_ ترى أنها وقعت وصحت نسبتها إلى شخص معين وأن هناك من الدلائل ما يكفي للتعرض لحرية المتهم أو لحرمة مسكنه"[1]، وهذا ما يعني أنه يعتبر من أعمال الاستدلال متى قامت به الشرطة القضائية وقبل تحريك الدعوى الجزائية.

ولعل الرأي الراجح والأقرب للصواب هو هذا الرأي الأخير الذي وفق بين جميع المعايير باعتبار إجراء التفتيش إجراء ذو طبيعة مزدوجة فلا يمكن اعتباره من أعمال التحقيق فقط لأن مكافحة الجريمة الإلكترونية تستدعي القيام بإجراءات خاصة بالتحقيق في مرحلة الاستدلال، كما يمكن لقاضي التحقيق إنابة ضابط الشرطة القضائية للقيام ببعض أعمال التحقيق بدلا عنه.

ثانيا: ضوابط التفتيش الإلكتروني

يعد التفتيش أحد مظاهر انتهاك الحياة الخاصة للأفراد التي ساهمت المواثيق الدولية والتشريعات المقارنة في حمايتها كما سبق وذكرنا، لذلك قد حرصت أغلب القوانين الإجرائية على إحاطته بجملة من الضوابط والضمانات منعا من التعسف في تنفيذه، منها ما هو موضوعي ومنها ما هو شكلي.

1. **الضوابط الموضوعية:**

وتتمثل فيما يلي:

أ. **سبب التفتيش**

1هلالي عبد اللاه أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، المرجع السابق، ص 52.

إن سبب التفتيش في الجرائم نعني به الدافع والمبرر للقيام بالتفتيش سعيا للحصول على الدليل الجنائي، وهو الضمانة القانونية لصحة ومشروعية هذا الإجراء، إذ يتحقق هذا السبب بوقوع جريمة ما يتم بموجبها توجيه الاتهام لأشخاص معينين بارتكابها بناء على أدلة وقرائن قوية تفيد تورطهم في هذه الجريمة، وعليه لكي يكون التفتيش مشروعا في الجرائم الإلكترونية يجب تحقق ما يلي:

- **وقوع جريمة إلكترونية بالفعل، سواء كانت جناية أو جنحة**

يشترط لمباشرة التفتيش أن تقع جريمة من الجرائم الإلكترونية بصورة فعلية، وقد سبق وعرفنا الجريمة الإلكترونية على أنها عمل إرادي غير مشروع يكون فيه الحاسب الآلي أو الجهاز إ محلا أو أداة في ارتكاب الجريمة، [1] إلا أنه لا يكفي وقوع جريمة إلكترونية فقط بل يشترط أيضا أن تكون مما يعتبرها القانون جناية أو جنحة نظرا لخطورتها حيث تستبعد المخالفات كونها ليست بتلك الخطورة التي تبرر إهدار الحرية الفردية وحرمة الحياة الخاصة للأفراد بإجراء تفتيش من أجلها.[2]

وتجدر الإشارة إلى أن مسألة وقوع الجريمة من عدمها تثير إشكالا كبيرا عندما يتعلق الأمر بالتفتيش في الجرائم الإلكترونية باعتبارها جرائم مميزة وذات طبيعة خاصة كما أشرنا سابقا، كما أن تشريعات الدول قد تباينت بخصوص هذه المسألة إذ نجد مثلا المشرع المصري قد نص في المادة 91من ق ا ج على أن: "تفتيش المنازل عمل من أعمال التحقيق ولا يجوز الالتجاء إليه إلا بمقتضى أمر من قاضي التحقيق بناء على اتهام موجه إلى شخص يقيم في المنزل المراد تفتيشه بارتكاب جناية أو جنحة أو باشتراكه في ارتكابها، أو إذا وجدت قرائن تدل على أنه حائز لأشياء تتعلق بالجريمة"، [3] فمن خلال استقراء هذه المادة يتبين أن المشرع المصري يشترط أن ترتكب الجريمة بالفعل لاتخاذ إجراء التفتيش بشأنها فلا يجوز إصدار الأمر بالتفتيش لضبط جريمة مستقبلية ولو قامت التحريات والدلائل على أنها ستقع فعلا، [4] وهو ما أكده أيضا نظام الإجراءات السعودي من خلال لائحته التنفيذية في المادة 41فقرة 3منها بقولها: "لا يكون التفتيش صحيحا إلا إذا كان بعد جريمة قد وقعت فعلا أو بدلائل وأمارات كافية..."، [5] إلا أن المشرع الجزائري قد انتهج نهجا آخر إذ بالرجوع إلى نص المادتين 04و05من القانون رقم 09/04يتبين أن المشرع

1المزيد من التفاصيل ينظر المقدمة.

2رشيدة بوكر، جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري والمقارن، المرجع السابق، ص 496.

3ينظر المادة 91من ق ا ج م.

4خالد ممدوح براهيم، الإثبات الإلكتروني في المواد الجنائية والمدنية، المرجع السابق، ص 138.

5عبد الله بن عبد العزيز بن عبد الله الخثعمي، التفتيش في الجرائم المعلوماتية في النظام السعودي، رسالة مقدمة لنيل شهادة الماجستير، كلية الدراسات العليا، جامعة نايف للعلوم الأمنية، الرياض، 2011، ص55.

الجزائري قد أجاز اللجوء إلى تفتيش النظم المعلوماتية للوقاية من وقوع أي جريمة أو في حالة توفر معلومات عن احتمال الاعتداء على منظومة معلوماتية حتى ولو لم يقع هذا الاعتداء فعلا، حماية منه لأمن هذه الأنظمة والشبكات، كما يكون سبب التفتيش في هذه الجرائم إما لضرورة مقتضيات التحريات والتحقيقات القضائية عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى تفتيش هذه المنظومة المعلوماتية، وإما بسبب تنفيذ طلبات المساعدة القضائية الدولية المتبادلة،[1] وهو ما سار عليه المشرع الأمريكي إذ لم يشترط وقوع الجريمة بالفعل لكي يصدر الإذن بالتفتيش والضبط، فقد تتخذ هذه الإجراءات رغم أن الجريمة لم تقع بعد، وهو التفتيش الذي يطلق عليه اسم "Prospective Search Warrant".[2]

ومن جهة أخرى نجد أن بعض الدول لم تسن حتى الآن قوانين تصنف فيها هذه الجرائم وتحدد وصفها القانوني وكذا أركانها والعقوبات المقررة لها، مع العلم أن إجراء التفتيش لا يكون مشروعا إلا إذا بني على سبب جدي يتمثل في الوقوع الفعلي للجريمة مجتمعة الأركان.[3]

- **نسبة الجريمة لشخص أو أشخاص معينين بارتكابها أو المشاركة فيها**

لا يكفي لقيام سبب التفتيش وقوع جريمة من جرائم الإلكترونية فقط، بل يجب أن يكون ذلك الوقوع مقترنا بنسبتها إلى شخص أو أشخاص معينين إما بصفتهم فاعلين أصليين أو شركاء في تلك الجريمة، ومعنى ذلك أن تتوافر في حق الشخص المراد تفتيشه دلائل كافية تدعو إلى الاعتقاد بأنه قد ساهم في ارتكاب الجريمة الإلكترونية هذه، أو كان شريكا فيها حتى تتمكن السلطات من انتهاك خصوصية

---

1 تنص المادة 04 من القانون 04/09 على: "المادة 4 : يمكن القيام بعمليات المراقبة المنصوص عليها في المادة 3 أعلاه في الحالات الآتية :
أ ـ للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة ،
ب ـ في حالة توفر المعلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو المؤسسات الدولة أو الاقتصاد الوطني
ج ـ لمقتضيات التحريات و التحقيقات القضائية ، عندما يكون من الصعب إلى نتيجة تهم الأبحاث الجارية دون اللجوء الى الرقابة الإلكترونية،
د ـ في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة .
لا يجوز إجراء عمليات المراقبة في الحالات المذكورة إلا بإذن مكتوب من سلطة قضائية المختصة
عندما يتعلق الأمر بالحالة المنصوص عليها في الفقرة "أ " من هذه المادة ، يختص النائب العام لدى مجلس قضاء الجزائر بمنح ضباط الشرطة القضائية المنتمين للهيئة المنصوص عليها في المادة 13 أدناه ، إذنًا لمدة 6 أشهر قابلة للتجديد و ذلك على أساس تقرير يبين طبيعة الترتيبات التقنية المستعملة و الأغراض الموجهة لها".
2خضرة شنتير، الآليات القانونية لمكافحة الجرائم الإلكترونية، المرجع السابق، ص 78.
3جمال براهيمي، التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص 33.

هذا الشخص وتفتيش حاسوبه الشخصي وبرامجه الخاصة، [1] حيث إذ لم تتوافر هذه الدلائل والقرائن كان على القاضي إصدار أمر بأن لا وجه للمتابعة أو لإقامة الدعوى، [2] وهذا ما تؤكده المادة 104من ق ا ج م، [3] وهو ما قررته أيضا المادة 177من ق ا ج ف. [4]

ولما كانت الدلائل الكافية شرطا ضروريا للاتهام بالجريمة الإلكترونية وجب تعريفها، إلا أننا نرى أن القوانين الإجرائية المقارنة لم تتناولها بالتعريف وإنما اكتفت بضرورة توافرها لقيام سبب التفتيش، غير أن الفقه والقضاء تصدا لهذه المهمة[5] حيث تعددت التعريفات التي قيلت في شأنها ولعلها تدور حول مفهوم واحد ألا وهو أنها مجموعة القرائن والشبهات المستمدة من الواقع والتي تنبئ عن ارتكاب الشخص لجريمة ما، [6] أما في جريمة الإنترنت فهي مجموعة المظاهر والأمارات التي تستمد من ملابسات الجريمة وتقوم على خبرة القائم بالتفتيش[7] الذي يرجح أن يكون ذو خبرة ودراية جيدة بالتقنيات والوسائل الإلكترونية وكيفية التعامل معها لكي يستطيع نسبة الجريمة لشخص معين كأن يتم تحديد هوية الحاسوب (IP) الذي تم ارتكاب الجريمة بواسطته وكان ذلك الحاسوب يخص شخصا معينا.

- **وجود أمارات أو أدلة قوية على وجود أشياء أو أجهزة أو معدات معلوماتية لدى المتهم الإلكتروني تفيد في كشف الحقيقة**

لا يكفي لحث سلطة التحقيق إلى إصدار قرارها بالتفتيش ومباشرته وقوع جناية أو جنحة ونسبتها إلى شخص أو أشخاص معينين بارتكابها أو المشاركة فيها، بل يجب أن تتوافر أمارات أو قرائن على وجود أشياء أو أجهزة أو معدات إلكترونية لدى المتهم أو غيره تفيد في كشف الحقيقة، [8] وهذا يفيد أنه لا يمكن مباشرة التفتيش إلا إذا توافرت لدى المحقق أسباب كافية على وجود أدوات استعملت في الجريمة

1ليندا بن طالب، الدليل الإلكتروني ودوره في الإثبات الجنائي، المرجع السابق، ص 60.

2هلالي عبد اللاه أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، المرجع السابق، ص 115.

3 ينظر المادة 104 من ق ا ج المصري.

4 L'article n° 177 du code de procédure pénale dispose que : « si le juge d'instruction estime que les faits ne constituent ni crime ni délit ni contravention ou si l'auteur est reste inconnu ou sil n'existe pas de charges suffisantes contre la personne mise en examen il déclaré par une Ordonnance qu'il ny a lieu à suivre ».

5لمزيد من التفاصيل ينظر هلالي عبد اللاه أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، المرجع السابق، ص 116وما بعدها.

6رشيدة بوكر، جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري والمقارن، المرجع السابق، ص 407.

7نبيلة هبة هروال، الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات، المرجع السابق، ص 233.

8هلالي عبد اللاه أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، المرجع السابق، ص 122.

الإلكترونية أو أشياء متحصلة منها أو أية مستندات أو ملفات أو دعامات إلكترونية يحتمل أن يكون لها فائدة من كشف غموض الجريمة لدى المجرم الإلكتروني أو الشخص المراد تفتيشه.[1]

وتقدير هذه الدلائل متروك للسلطة التي تصدر الإذن بالتفتيش بشرط أن يكون تقديرها منطقيا ومتفقا مع الواقع بحيث تكشف هذه الدلائل بجدية عن وقوع الجريمة محل الإذن بالتفتيش وأن هناك متهما تنسب إليه.[2]

ب. محل التفتيش الإلكتروني

وبما أن التفتيش ما هو إلا وسيلة للإثبات المادي غايته ضبط الأدلة المادية الخاصة بالجريمة فإنه يختلف الأمر بالنسبة إلى الجرائم المعلوماتية للطبيعة الخاصة واللامادية لها عن تلك التقليدية التي لا تطرح أي إشكال من حيث محل التفتيش فيها، فالجرائم المعلوماتية تطرح عدة إشكالات ذلك أن الحاسب الآلي يحتوي على عدة مكونات مادية وأخرى معنوية ترتبط بغيرها من شبكات الاتصال المتواجدة على المستوى المحلي والدولي، ولذلك يتطلب الأمر البحث في مدى جواز وقابلية هذه المكونات الرقمية والمنطقية وكذا الشبكات البعدية للحاسب الآلي لعملية التفتيش؟

1. تفتيش المكونات المادية للحاسب الآلي

يقصد بالمكونات المادية للحاسوب بأنها "تلك الأشياء الملموسة من أجزائه وأدواته التي تعمل بشكل متكامل لأداء مهمة في معالجة البيانات آليا" وعليه يتكون الحاسب الآلي من ثلاث وحدات، تتمثل في وحدات الإدخال مثل لوحة المفاتيح وشاشات اللمس...الخ، ووحدات المعالجة مثل وحدة المعالجة المركزية ...الخ، ووحدات الإخراج كالشاشة والطابعة والأقراص المرنة والصلبة...الخ.[3]

لا يثور الخلاف حول تفتيش المكونات المادية للحاسب الآلي بحثا عن أدلة مادية تكشف عن حقيقة الجريمة الإلكترونية ومرتكبيها، إذ أنها تخضع لإجراءات التفتيش المألوفة التي ترد على الأشياء المادية طبقا للقواعد الإجرائية، إلا أن حكم تفتيش هذه المكونات يتوقف على طبيعة المكان الموجودة فيه، سواء كان عاما أو خاصا ذلك لأن لصفة المكان أهمية خاصة في مجال التفتيش، [4] فإذا كانت هذه المكونات موجودة

1رشيدة بوكر، جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري والمقارن، المرجع السابق، ص 408.

2خالد ممدوح ابراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص 214.

3يزيد بوحليط، الجرائم الإلكترونية والوقاية منها في القانون الجزائري، المرجع السابق، ص 472.

4ممدوح خالد ابراهيم، الإثبات الإلكتروني في المواد الجنائية والمدنية، المرجع السابق، ص 126.

في مكان خاص كمسكن المتهم أو أحد ملحقاته فلا يجوز تفتيشها إلا في الحالات التي يجوز فيها تفتيش مسكنه وبنفس الضمانات المقرر قانونا في أغلب التشريعات الجنائية، من بينها التشريع الفرنسي والتشريع المصري وكذا التشريع الجزائري،[1] حيث اشترطت هاته الأخيرة الحصول على رضا صريح من صاحب المسكن، ويجب كتابته وتوقيعه بخط يد صاحب الشأن، وفي حالة العكس يثبت أن صاحب الشأن لا يعرف الكتابة في المحضر مع التنويه عن رضائه، أما إذا تعذر على صاحب المسكن الحضور وقت إجراء التفتيش، فعلى ضابط الشرطة القضائية أن يعين له ممثل له، وفي حالة ما كان في حالة فرار استدعى الضابط لحضور عملية التفتيش شاهدين من غير الموظفين الخاضعين لسلطته، كما يجب أن يتم هذا التفتيش في المواعيد المقررة قانونا لذلك، ففي القانون الجزائري مثلا يشترط أن يتم التفتيش من الساعة الخامسة صباحا إلى الساعة الثامنة مساء، إلا في بعض الحالات الخاصة، حيث استثنى المشرع الجزائري تطبيق هذه الشروط على طائفة معينة من الجرائم المذكورة في الفقرة الثالثة من المادة 47من ق ا ج ج، والتي من بينها الجرائم الإلكترونية إذ يجوز فيها التفتيش في أي محل سكني أو غير سكني وفي أي ساعة من ساعات النهار أو الليل.[2]

كما يجب التمييز داخل هذا المكان بين ما إذا كانت مكونات الحاسب منعزلة عن غيرها من الحواسيب الأخرى أو أنها متصلة بحواسيب أو أجهزة متواجدة في مكان آخر كمسكن غير المتهم، ففي هذه الحالة يجب مراعاة القيود والضمانات التي يشترطها القانون لتفتيش هذه الأماكن.[3]

أما إذا ما كانت المكونات المادية للحاسوب متواجدة في أماكن عامة، سواء كانت عامة بطبيعتها كالطرق العامة مثلا، أم عامة بالتخصيص كمقاهي الإنترنت ومحلات بيع وصيانة الحواسيب والأجهزة الإلكترونية، فإن إجراءات تفتيشها تكون وفقا للأصول الخاصة بتلك الأماكن أي وفقا لإجراءات تفتيش الأشخاص وبنفس الضمانات والقيود المنصوص عليها في هذا المجال، ويستوي الأمر إذا كانت تلك المكونات في حوزة شخص مثل المبرمج أو عامل الصيانة أو موظف في شركة تنتج برامج الحاسب الآلي، إذ تطبق نفس أحكام تفتيش الأشخاص.

1ينظر المادة 45من ق ا ج ج.

2ينظر المادة 47من ق ا ج ج.

3ففي هذه الحالة يتم التفتيش بحضور صاحب المنزل الذي تكون له مصلحة مؤكدة في حضور التفتيش حتى يتمكن من الدفاع عن مصالحه الخاصة وحماية ممتلكاته، وفي حالة غيابه يتم التفتيش بحضور من ينيبه إن أمكن طبقا للمادة 92فقرة 2من ق ا ج المصري ، والمادة 45فقرة 2من ق ا ج ج. نقلا عن نبيلة هبة هروال، الجوانب الإجرائية لجرائم الإنترنت، المرجع السابق، ص 238.

ومن بين التشريعات التي تجيز تفتيش مكونات الحاسوب المادية نجد التشريع اليوناني في المادة 251من ق ا ج التي تجيز لسلطة التحقيق أن تتخذ أي إجراء أو أي شيء يكون لازما لجمع الدليل، إلى جانب التشريع اليوناني نجد المادة 487من القانون الكندي، والتي أجازت هي الأخرى تفتيش مكونات الحاسب المادية متى استدعى التحقيق ذلك، كما ينص قانون إساءة استخدام الحاسب الآلي الإنجليزي الصادر في 29جوان 1990صراحة على تفتيش مكونات الحاسب المادية،[1] وهو ما أجازته المادة 41فقرة (b) من ق ا ج الفيدرالي لضابط الشرطة القضائية تفتيش وضبط المكونات المادية للحاسب الآلي إذا كانت مجرمة أو كانت دليل أو أداة أو ثمرة لجريمة إلكترونية.[2]

2. تفتيش المكونات المعنوية للحاسب الآلي

يطلق على المكونات المعنوية للحاسوب مصطلح "البرمجيات" وهي عبارة عن برامج معينة تخزن و توضع في وسائل تخزين خاصة كي يمكن استخدامها من قبل الكمبيوتر، وهي عبارة عن شفرات خاصة لذا سميت بالكيان المنطقي، وتعرف الكيانات المنطقية للحاسب الآلي بأنها مجموعة من البرامج والقواعد المتعلقة بتشغيل وحدة معالجة البيانات[3]كما عرفها القانون الأمريكي لسنة ***1980*** بأنها: "مجموعة توجيهات أو تعليمات يمكن للحاسب استخدامها بشكل مباشر أو غير مباشر لوصول إلى نتيجة معينة".[4]

وقد ثار الجدل حول إمكانية وقابلية تفتيش هذه المكونات باعتبارها كيانات معنوية غير محسوسة، حيث انقسم الفقه المقارن إلى اتجاهين: ذهب الرأي الأول إلى جواز تفتيش البيانات الإلكترونية المعالجة آليا ويستند في ذلك إلى أن القوانين الإجرائية جاءت عامة في نصها على التفتيش، من بينها القانون اليوناني إذ فسر الفقه الجنائي عبارة "ضبط أي شيء "لتشمل المكونات المادية وغير المادية أي جميع بيانات الحاسوب، سواء كانت هذه البيانات مخزنة في حاملتها أو معالجة آليا في الذاكرة الداخلية للحاسوب،[5] وهو ما أكده القانون الكندي من خلال المادة **487**من ق إ الكندي والتي تقضي بإمكانية إصدار أمر قضائي لتفتيش وضبط أي شيء تتوافر بشأنه أسس ومبررات معقولة تدعو للاعتقاد بأن جريمة قد

1ممدوح خالد ابراهيم، الإثبات الإلكتروني في المواد الجنائية والمدنية، المرجع السابق، ص 127.

2حسام محمد نبيل الشنراقي، الجرائم المعلوماتية، المرجع السابق، ص 494.

3عفيفي كمال عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، دراسة مقارنة، منشورات الحلبي القانونية، دمشق، ط 2، 2007، ص 61.

4يزيد بوحليط، الجرائم الإلكترونية والوقاية منها في القانون الجزائري، المرجع السابق، ص 473.

5خضرة شنتير، الآليات القانونية لمكافحة الجرائم الإلكترونية، المرجع السابق، ص 74.

وقعت أو يشتبه في وقوعها، أو أن هناك نية لاستخدامه في ارتكاب جريمة أو أنه سينتج دليلا على وقوع الجريمة، وهذا ما يفسر إمكانية تفتيش المكونات المنطقية للحاسب الآلي.[1]

فيما ذهب الرأي الآخر إلى عدم جواز انطباق إجراءات التفتيش العادية على المكونات المعنوية على اعتبار أن التفتيش يهدف إلى ضبط أدلة مادية تفيد في كشف الحقيقة، ولهذا يقترح مواجهة هذا القصور بالنص على أحكام خاصة تنظم تفتيش هذه المكونات أو على الأقل تعديل قواعد التفتيش المألوفة بشكل يتلاءم مع متطلبات هذه التقنية الحديثة، خاصة مع التطورات التكنولوجية الحاصلة والتي لم تكن موجودة سابقا، فلا يمكن إعمال النصوص الخاصة بالتفتيش التقليدي على المكونات المنطقية للحاسب الآلي والنظم المعلوماتية الخاصة به لأن قياسها على الأشياء المادية يعتبر منافيا لمبدأ الشرعية الإجرائية.[2]

وفي هذا الصدد صرحت الاتفاقية الأوروبية في شأن جرائم تقنية المعلومات بحق الدول الأعضاء في تفتيش أجهزة الكمبيوتر في إطار الإجراءات الجنائية، وذلك بموجب المادة 19من القسم الرابع منها، والتي نصت صراحة على: "لكل دولة طرف من حقها أن تسن من القوانين ما هو ضروري لتمكين السلطات المختصة بالتفتيش أو الدخول إلى:

- نظام الكمبيوتر أو جزء منه أو المعلومات المخزنة به.
- الوسائط التي يتم تخزين معلومات الكمبيوتر بها ما دامت مخزنة في إقليمها".[3]

واستجابة لهذه التغييرات نظم المشرع الأمريكي إجراء التفتيش والضبط في البيئة الرقمية ضمن نصوص قانونية جديدة وذلك في القسم 2000من القانون الإجرائي الاتحادي الخاص بجرائم الحاسب، كما أصدرت إدارة العدل الأمريكية المرشد الفيدرالي لتفتيش وضبط الحواسيب لكي يكون دليلا للسلطات القضائية في تقصي الجرائم الإلكترونية، ثم تلاه المشرع الإنجليزي بنصه في قانون المتعلق بإساءة استخدام الحاسب الآلي لعام 1990على جواز تفتيش نظم الحاسوب المادية والمعنوية ، كما أجاز تفتيش نظم الحاسوب في جرائم الولوج أو التعديل غير المصرح به على أنظمة الحاسوب دون إذن طالما كان هدف

1رشيدة بوكر، جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري المقارن، المرجع السابق، ص 397.

2نعيم سعيداني، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، المرجع السابق، ص 147.

3عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في الإثبات الجنائي، المرجع السبق، ص 55- 56.

الولوج ارتكاب أفعال غير مشروعة عن قصد، أما إذا كان الولوج مجردا دون نية ارتكاب أفعال غير مشروعة فإن التفتيش ممكن ولكن بإذن قضائي.[1]

كما قام المشرع الفرنسي بتعديل نصوص التفتيش لتواكب التطورات الحديثة، إذ أضاف بموجب المادة 42من القانون رقم 2004-545المؤرخ في 21جوان 2004المتعلق بالثقة في الاقتصاد الرقمي عبارة "المعطيات المعلوماتية" مشيرا إلى المادة 94من ق ا ج لتصبح هاته الأخيرة على النحو التالي: "يباشر التفتيش في جميع الأماكن التي يمكن العثور فيها على أشياء أو معطيات معلوماتية يكون كشفها مفيدا لإظهار الحقيقة".

وهذا ما تبناه المشرع الجزائري من خلال القانون 09/04سالف الذكر في المادة الخامسة (05) منه[2] حيث أجاز للسلطات القضائية المختصة في إطار قانون الإجراءات الجزائية وفي الحالات المنصوص عليها في المادة 04من نفس القانون بالدخول إلى منظومة معلوماتية أو جزء منها وكذا المعطيات المخزنة فيها وتفتيشها وضبط الأدلة فيها.[3]

وعلى غرار هذين الاتجاهين ظهر اتجاه آخر استند في حججه إلى الواقع العملي حيث أقر بأنه لا يمكن تفتيش وضبط بيانات الحاسب الآلي إلا إذا اتخذت شكلا ماديا، وهذا ما أكده المشرع الألماني من خلال القسم 94من ق ا ج والذي يقضي أن تكون الأدلة المضبوطة ملموسة وذات طبيعة محسوسة، وهي على هذا النحو لا تشمل فقط المكونات المعنوية للحاسب بل تتعداها إلى الدعامات التي تحمل البيانات والبرمجيات والتطبيقات ذات الكيان المعنوي، ويترتب على ذلك أن البيانات منفردة عن هذه الدعامات لا تعد من الأشياء التي يمكن ضبطها إلا إذا تم طبعها وتحميلها على دعامات مادية قابلة للتفتيش والضبط،[4] كما نص القانون في رومانيا على أن التفتيش والضبط ينصب على الدعامة المادية المدون عليها البيانات الإلكترونية للحاسب الآلي، كالأشرطة المغناطيسية والأقراص بمختلف أنواعها، وليس على الكيان غير المادي، وعلى غرار هاته القوانين نجد أن القانون الأمريكي والانجليزي بالرغم من أنهم يعترفون بالطبيعة

1نعيم سعيداني ، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، المرجع السابق، ص148 .

2ينظر المادة 05من القانون رقم 09/04المشار إليه سابقا.

3يزيد بوحليط، تفتيش المنظومة المعلوماتية وحجز المعطيات في التشريع الجزائري، مجلة التواصل في الاقتصاد والإدارة والفانون، عدد 48، ديسمبر 2016. ص84.

4خالد ممدوح ابراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص 198.

المعنوية لهذه البيانات إلا أن ذلك لا يشكل مشكلة في تقديرهم على أساس أنه يمكن ضبط السجلات المعالجة أو المستندات الناتجة عنها.[1]

وتجدر الإشارة إلى أن المشكلة لا تكمن فقط في الطابع المادي والمعنوي للمكونات والبيانات الإلكترونية، بل يوجد مجموعة من الصعوبات التي تعيق عملية خضوع البيانات المخزنة آليا لقواعد التفتيش التقليدية، خاصة إذا كانت هذه البيانات أو المنظومة الإلكترونية محمية بكلمة سر أو أن تكون المعطيات المطلوبة مشفرة،[2] فهل يجوز في هذه الحالة إجبار المتهم على تزويد السلطات المختصة بالتحقيق بمفاتيح المرور وكلمات السر للدخول إلى أنظمة المعالجة الآلية؟

وهنا تباينت الآراء بصدد هذه المسألة، فاتجه الرأي الأول إلى رفض إجبار المتهم على تقديم المعلومات التي تسهل النفاذ إلى المعطيات المعلوماتية، مستندين في ذلك إلى القاعدة العامة التي تقضي بعدم إجبار المتهم على تقديم أدلة ضد نفسه وحقه في الصمت أثناء التحقيق معه وعدم الإدلاء بأقواله، وتحرص أغلب التشريعات الإجرائية على النص صراحة على حق المتهم في الصمت، ومن ذلك التشريع الأمريكي من خلال التعديل الخامس من الدستور الفيدرالي، والتشريع الفرنسي بموجب المادة 114من ق ا ج، وكذا المشرع الألماني في المادة 136من ق ا ج، والمشرع المصري الذي رغم أنه لم ينص صراحة على هذا المبدأ إلا أنه يفهم ضمنا من نص المادة 274فقرة 1من ق ا ج التي تنص على عدم استجواب المتهم إلا إذا قبل ذلك، [3] والمشرع الجزائري الذي أكد على حق المتهم في الصمت بموجب المادة 100من ق ا ج التي تقضي بأن يقوم قاضي التحقيق بتنبيه المتهم الممتثل أمامه لأول مرة بأنه حر في عدم الإدلاء بأي قرار.[4]

1هلالي عبد اللاه أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، المرجع السابق، ص 203- 204.

2عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت، المرجع السابق، ص 198.

3هلالي عبد اللاه أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، المرجع السابق، ص 205- 206.

4تنص المادة 100من ق ا ج ج على: " يتحقق قاضي التحقيق حين مثول المتهم لديه لأول مرة من هويته و يحيطه علمًا صراحة بكل واقعة من الوقائع المنسوبة إليه و ينهه بأنه حر في عدم الإدلاء بأي إقرار و ينوه عن ذلك التنبيه من المحضر فإذا أراد المتهم أن يدلي بأقوال تلقاها قاضي التحقيق منه على الفور كما ينبغي للقاضي أن يوجه المتهم بأن له الحق في اختيار محامي عنه فإن لم يختر له محاميًا عين له القاضي محامي من تلقاء نفسه إذا طلب منه ذلك و ينوه عن ذلك بمحضر كما ينبغي للقاضي علاوة على ذلك أن ينبه متهم إلى وجوب إخطاره بكل تغيير يطرأ على عنوانه و يجوز للمتهم اختيار مواطن له في دائرة اختصاص المحكمة".

وفي المقابل ذهب رأي آخر إلى القول بأنه وإن كان لا يجوز إجبار المتهم على الإدلاء بأقواله ضد نفسه إلا أنه لا ينبغي أن يكون هذا حائلا دون إجباره على تقديم معلومات يقتضيها ولوج النظام المعلوماتي متى كانت هذه المعلومات بحوزته.[1]

وعلى خلاف ذلك يجوز إجبار غير المتهم على تقديم المعلومة التي من شأنها مساعدة السلطات المختصة بالدخول للأنظمة المعلوماتية وتفتيش وضبط المعطيات بها، كإلزام مقدمي الخدمات أو مديري النظام بأن يقدموا المساعدة اللازمة للسلطات المختصة،[2] حيث تشير المذكرة التفسيرية لاتفاقية بودابست أن المعلومات التي يمكن إلزام مديري النظام بتقديمها تقتصر على المعلومات الضرورية التي تسمح بإجراء التفتيش أو الحصول الضروري على كلمة مرور معينة،[3] وقد تأثر المشرع الفرنسي بهذه الاتفاقية وفرض إجراء قسري لتسهيل عملية التفتيش وذلك بموجب المادة 57فقرة 1من ق ا ج، كما نص في المادة 230فقرة 1من نفس القانون على أنه عندما تكون المعطيات اللازمة للتحقيق مشفرة فإن لوكيل الجمهورية أو لسلطة التحقيق أو لسلطة الحكم المختصة أن يعينوا شخصا طبيعيا أو معنويا مؤهلا للقيام بفك التشفير إذا كان ذلك ضروريا، [4] وهذا ما نص عليه المشرع الجزائري في الفقرة الأخيرة من نص المادة 05من القانون رقم 09/04سالف الذكر.[5]

3. مدى خضوع المنظومة المعلوماتية (شبكات المعلومات) للتفتيش

يثير تفتيش شبكات النظام المعلوماتي صعوبات كبيرة تتعلق بالطبيعة الرقمية العالمية التي تسمح بتوزيع المعلومات عبر شبكات معلوماتية في جميع أنحاء العالم، فقد يكون الموقع الفعلي لهذه المعلومات داخل اختصاص قضائي آخر في إقليم دولة واحدة أو في إقليم دولة أو دول أخرى، [6] وهو ما يزيد الأمر تعقيدا فيثار هنا التساؤل حول مدى جواز إمداد التفتيش إلى الأنظمة المعلوماتية المتصلة بالنظام المأذون بتفتيشه والمتواجدة في دوائر اختصاص مختلفة؟ وفي هذا نكون أمام حالتين :

1رشيدة بوكر، جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري والمقارن، المرجع السابق، ص 400.

2ينظر المواد 10و11من القانون 09/04المشار إليه سابقا.

3رشيدة بوكر، الحماية الجزائية للتعاملات الإلكترونية المرجع السابق، ص 279.

4 المرجع نفسه، ص 280.

5حيث تنص الفقرة الأخيرة من المادة 05من القانون 09/04على: "... يمكن السلطات المكلفة بالتفتيش تسخير كل شخص له دراية بعلو المنظومة المعلوماتية محل البحث أو التدابير المتخذة لحماية المعطيات المعلوماتية التي تتضمنها ، قصد مساعدتها و تزويدها بكل المعلومات الضرورية لإنجاز مهمتها".

6جمال براهيمي، التحقيق الجنائي في الجرائم الالكترونية، المرجع السابق، ص 21.

أ. حالة اتصال النظام المعلوماتي للمتهم بنظام آخر موجود داخل الدولة الواحدة

لقد خولت اتفاقية بودابست بموجب مادتها 19فقرة 2سلطات التحري إمكانية توسيع إجراء التفتيش أو الولوج إلى منظومة معلوماتية أخرى أو جزء منها إذا كان ثمة أسباب تدعو للاعتقاد بأن البيانات المطلوبة مخزنة في هذا النظام المعلوماتي، أو في جزء منه، وذلك بشرط وجود هذا النظام على إقليم الدولة نفسها، ولم تتطرق الاتفاقية إلى تحديد نموذج معين للإذن بتمديد التفتيش ولا إلى كيفية تطبيقه وإنما تركت تحديد ذلك للقوانين الداخلية للدول الأطراف فيها.[1]

ومن بين التشريعات التي نصت صراحة على إمكانية وجواز امتداد الحق في التفتيش ليشمل أجهزة الحاسب الآلي أو أية منظومة معلوماتية مرتبطة بحاسب المتهم الجاري تفتيشه، نجد القانون الألماني وذلك بموجب القسم 103من ق ا ج، إذ لم ينص على وجوب صدور إذن يخص هذا التمديد، وإنما أجاز ذلك كلما دعت ضرورة التحقيق إليه، [2] وكذلك فعل المشرع البلجيكي في نص المادة 88من قانون تحقيق الجنايات على أنه: "إذا أمر قاضي التحقيق بالتفتيش في نظام معلوماتي، أو في جزء منه فإن هذا البحث يمكن أن يمتد إلى نظام معلوماتي آخر يوجد في مكان آخر غير مكان البحث الأصلي، ويتم هذا الامتداد وفقا لضابطين: أولهما إذا كان هذا التمديد ضروريا لكشف الحقيقة بشأن الجريمة محل البحث، والثاني إذا ما وجدت مخاطر تتعلق بضياع الأدلة نظرا لسهولة إتلافها والتلاعب بها.[3]

وفي نفس الإطار قام المشرع الفرنسي بتعديل قانون إ ج بموجب القانون رقم 239/2003المتعلق بالأمن الداخلي، حيث أضاف المادة 57فقرة 1من ق ا ج وذلك بموجب المادة 17فقرة 1منه[4]، والتي أجاز من خلالها لسلطات الضبط القضائي الولوج من الجهاز الرئيسي إلى المعلومات المخزنة في أنظمة وأجهزة معلوماتية أخرى وضبطها بناء على إذن بالتفتيش صادر من سلطة التحقيق.[5]

1حسام محمد نبيل الشنراقي، الجرائم المعلوماتية، المرجع السابق، ص 505.

2خالد ممدوح ابراهيم، الإثبات الإلكتروني في المواد الجنائية والمدنية، المرجع السابق، ص 132.

3 المرجع نفسه، ص 133.

4 L'article n° 17 du code n°2003/239 du sécurité dispose que « Les officies de police judiciaire ou Sous leur responsabilité les agents de police judiciaire Peuvent au cours dune perquisition effectuer dans les conditions prévues par le présent code, accéder par un système informatique implanté sur les lieux ou ce déroule la Perquisition àdès données intéressant l'enquête en cours Et stockées dans ledit système ou dans un autre système informatique; dès lors que ces données sont accessible à partir du système initial disponible pour le système initial »

5خالد حسن أحمد لطفي، الدليل الرقمي ودوره في إثبات الجريمة المعلوماتية، المرجع السابق، ص 116.

أما عن المشرع الأمريكي فقد منح لقاضي التحقيق إصدار الإذن بتفتيش ملكية داخل منطقة أو خارجها وفقا للمادة 41A من ق ا ج، وذلك متى كانت الملكية عند طلب الإذن موجودة داخل المنطقة لأنه يخشى أو يتوقع تحركها خارجها قبل تنفيذ الإذن، وقد قررت المحكمة العليا أن هذه الملكية تشمل أيضا بيانات الحاسب الآلي، وفي هذه الحالة إذا ما كانت هذه الملكية في مكان آخر من الولايات م أ فعلى رجال الضبط القضائي الحصول على أكثر من إذن لكل مكان من أماكن تواجد هذه البيانات طبقا للمادة 41 من ق ا ج الفيدرالي.[1]

ومن التشريعات العربية التي نظمت هذه المسألة نجد المشرع المصري وذلك بموجب نص المادة 6 من قانون 175/2018 المتضمن مكافحة جرائم تقنية المعلومات، والتي أجاز من خلالها لسلطات التحقيق البحث والتفتيش أو النفاذ إلى برامج الحاسب الآلي وقواعد البيانات وكذا الأجهزة والنظم المعلوماتية لغرض جمع وضبط الأدلة فيها.[2] ولم يتوانى المشرع الجزائري عن تنظيم مسألة تفتيش النظم المعلوماتية فزيادة على ما نص عليه في ق ا ج قد أضاف محل للتفتيش ألا وهو المنظومة المعلوماتية أو جزء منها وكذا المعطيات المخزنة بها[3]، حيث عالج عملية تفتيش المنظومة المعلوماتية من خلال الفصل الثالث من القانون 09/04 وذلك بموجب المادة 05 فقرة 01 منه والتي تنص على: "يجوز للسلطات القضائية وكذا ضباط الشرطة القضائية، في إطار قانون الإجراءات الجزائية وفي الحالات المنصوص عليها في المادة 94 أعلاه، الدخول بغرض التفتيش، ولو عن بعد إلى منظومة معلوماتية أو جزء منها وكذا المعطيات المخزنة فيها".

ونظرا لخطورة الجرائم المعلوماتية فقد أجاز المشرع تمديد إجراء التفتيش داخل الإقليم الوطني ذلك بموجب المادة 05 فقرة 02 من ذات القانون،[4] وعليه فقد أجاز المشرع مد التفتيش إلى منظومة معلوماتية أخرى بدون أي إشكال شريطة إعلام السلطة القضائية المختصة بذلك، وأن يكون الغرض من إجراء هذا التفتيش التوصل إلى أدلة تتعلق بالجريمة محل التفتيش والتي من شأنها أن تفيد في إظهار الحقيقة، فلا يجوز مباشرته إلا إذا كان هناك هدفا واضحا منذ البداية، فلا يجوز إذن الاطلاع غير

1 حسام محمد نبيل الشنراقي، الجرائم المعلوماتية، المرجع السابق، ص 503.

2 حسام محمد نبيل الشنراقي، الجرائم المعلوماتية، المرجع السابق، ص 116.

3 وهذا ما يستشف من أحكام المادة 5 من القانون 09/04 المشار إليه سابقا.

4 ينظر المادة 05 فقرة 2 من القانون رقم 09/04 المشار إليه سابقا.

المصرح به على ملفات البيانات المخزنة داخل الحاسب الآلي أو النظام المعلوماتي لإحدى المؤسسات مثلا أو الغير، فيعتبر إجراء التفتيش في هذه الحالة باطلا ويشكل في حد ذاته جريمة إلكترونية.[1]

ب. حالة اتصال نظام المتهم بنظام معلوماتي آخر موجود خارج إقليم الدولة

نتيجة الطابع العالمي للجريمة المعلوماتية قد يقوم الجناة بتخزين معلوماتهم وبياناتهم غير المشروعة في نظام معلوماتي خارج إقليم الدولة الواحدة عن طريق شبكة الاتصالات المفتوحة عالميا، وذلك لإعاقة وصول سلطات التحري والتحقيق إليها، ففي هذه الحالة وجب إمداد إذن التفتيش إلى خارج إقليم الدولة أي دخوله المجال الجغرافي لدولة أخرى، وهو ما يسمى "بالولوج أو التفتيش عبر الحدود" أو "التفتيش عن بعد"، [2] إلا أنه قد يتعذر هذا التفتيش بسبب تمسك الدولة بسيادتها هذا ما يثير عدة إشكالات، إضافة إلى أن هذا الامتداد يشكل اعتداء على خصوصية هذه الدول فضلا عن أنه يجعلها عرضة للاعتداء في إطار جريمة التجسس عليها والمساس بأمنها، ولهذه الأسباب ذهب جانب من الفقه خاصة الفقه الهولندي والفقه الألماني أن التفتيش الإلكتروني العابر للحدود يجب أن يتم في إطار اتفاقيات تعاون خاصة ثنائية أو دولية تجيز هذا الامتداد، وعليه فلا يجوز القيام بتفتيش المنظومة المعلوماتية لأي دولة أجنبية في ظل غياب هذه الاتفاقيات، أو على الأقل الحصول على إذن من الدولة الأجنبية احتراما لسيادتها، [3]وتطبيقا لذلك ما حدث في ألمانيا إذ عرضت على القضاء الألماني واقعة تتمثل في غش معلوماتي محلها طرفي الحاسوب أحدهما متواجد بألمانيا والآخر بسويسرا ولم يتم استرجاع البيانات المخزنة بالخارج إلا بعد التماس المساعدة المتبادلة بين الدولتين، وهذا ما يؤكد ضرورة وأهمية التعاون الدولي في مجال مكافحة الإجرام المعلوماتي.[4]

ومع ذلك فقد أجازت اتفاقية بودابست في مادتها 32إمكانية الدخول بغرض التفتيش في أجهزة أو شبكات تابعة لدولة أو دول أخرى بدون إذنها ولكن في حالتين: الأولى إذا ما تعلق هذا التفتيش بمعلومات متاحة للجمهور، والثانية إذا ما رضي صاحب أو حائز هذه البيانات بهذا التفتيش، [5]وهو نفسه ما أقرته الاتفاقية العربية لمكافحة جرائم تقنية المعلومات في مادتها 40.[6]

1حسين ربيعي، آليات البحث والتحقيق في الجرائم المعلوماتية، المرجع السابق، ص 122.

2نبيلة هبة هروال، الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات، المرجع السابق، ص 240.

3خالد ممدوح ابراهيم، الإثبات الإلكتروني في المواد الجنائية والمدنية، المرجع السابق، ص 134.

4حسين ربيعي، آليات البحث والتحقيق في الجرائم المعلوماتية، المرجع السابق، ص 123.

5خالد ممدوح ابراهيم، الإثبات الإلكتروني في المواد الجنائية والمدنية، المرجع السابق، ص 134.

6خضرة شنتير، الآليات القانونية لمكافحة الجرائم الإلكترونية، المرجع السابق، ص 95.

ومن جانب آخر دعت الاتفاقية أ م إ م كل دولة طرف أن تعتمد تدابير تشريعية وتدابير أخرى قد تكون ضرورية لتمكين السلطات المختصة من الدخول والتفتيش إلى منظومة معلوماتية أو جزء منها والبيانات المخزنة فيها، أو إلى وسائط تخزين البيانات الموجودة على إقليمها، وفقا لنص المادة 19فقرة 1منها، وهو ما جاءت به المادة 26فقرة 1من إ ع م ج ت م تحت عنوان "تفتيش المعلومات المخزنة "والتي دعت إلى:

أ. تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين سلطاتها المختصة من التفتيش أو الوصول إلى:

- تقنية معلومات أو جزء منها والمعلومات المخزنة فيها أو المخزنة عليها،
- بيئة أو وسيط تخزين معلومات تقنية معلومات والذي قد تكون معلومات مخزنة فيه أو عليه..."[1]

وفي ذات الشأن الدولي أصدر المجلس الأوروبي توصيات تجيز أن يمتد التفتيش إلى شبكات الاتصالات حتى ولو كانت خارج إقليم الدولة نفسها، ومن بين تلك التوصيات التوصية رقم 13لسنة 1995المتعلقة بالمشكلات القانونية لقانون الإجراءات الجزائية المتصلة بتقنية المعلومات والتي قضت بأنه: "لسلطة التفتيش عند تنفيذ تفتيش المعلومات وفقا لضوابط معينة أن تقوم بمد مجال تفتيش كمبيوتر معين يدخل في دائرة اختصاصها إلى غير ذلك من الأجهزة ما دامت مرتبطة بشبكة واحدة وأن تضبط المعطيات المتواجدة فيها مادام أنه من الضروري التدخل الفوري للقيام بذلك".[2]

تطبيقا لهذه التوصيات بدأت بعض التشريعات المقارنة في التصدي لهذه المشكلة وذلك بإقرار إمكانية التفتيش عن بعد في حاسوب متواجد في إقليم بلد أو دولة أجنبية، ومن بينها مشروع قانون جريمة الحاسب في هولندا، إذ ينص في مادته 125فقرة 1على إمكانية تمديد التفتيش إلى الحواسيب والنظم المعلوماتية المرتبطة بها الموجودة في دولة أخرى شريطة أن يكون هذا التدخل مؤقتا وأن تكون البيانات محل التفتيش لازمة لإظهار الحقيقة،[3] كذلك هو الشأن بالنسبة للمشرع الفرنسي، حيث أجاز بموجب المادة 57فقرة 2من ق ا ج المضافة بموجب المادة 17فقرة 2من قانون الأمن الداخلي المشار إليه سابقا

1يزيد بوحليط، الجرائم الإلكترونية والوقاية منها في القانون الجزائري، المرجع السابق، ص 474.

2رشيدة بوكر، جرائم الاعتداء على نظم المعالجة الآلية، المرجع السابق، ص 404.

3نبيلة هبة هروال، الجوانب الإجرائية لجرائم الإنترنت، المرجع السابق، ص 240.

لضابط الشرطة القضائية أن يقوم بتفتيش الأنظمة المتصلة حتى ولو تواجدت خارج الإقليم وهذا ما يبرره الفقه الفرنسي بأن العالم الافتراضي لا يعرف الحدود ولذا يجب التماشي مع طبيعة هذا العالم.

أما في الولايات م أ فالأمر متعلق بالقائم بالتفتيش، فإذا كان هذا الأخير يعلم قبل مباشرته لإجراء التفتيش عن البيانات المخزنة في الأنظمة المعلوماتية بأنها تقع في نطاق إقليم دولة أخرى، فإنه يجب أن يقدم طلب التماس مساعدة إلى سلطات الدولة الأخرى وفي حالة قبول هذا الطلب والسماح له بتمديد التفتيش يتم هذا الأخير وفق الشروط والضمانات اللازمة مع احترام سيادة تلك الدولة، أما إذا كان يجهل ذلك أو لم يكن في وسعه معرفة ذلك فإن ما يتحصل عليه من أدلة لا يمكن إهدارها وإنما يمكن قبولها في إثبات الجريمة الواقعة متى اطمأنت إليها المحكمة، وعليه فإن القانون الأمريكي يلزم رجال التحقيق بالتقيد بمبدأ الإعلان عن وجودهم والإفصاح عن ذلك أمام السلطات الأجنبية كاستئذاننا منها للدخول إلى المنظومات المتواجدة بها.[1]

قد سار المشرع الجزائري على ذات النهج وقام بإجازة تمديد التفتيش إلى منظومة معلوماتية تقع خارج الإقليم الوطني إذا ما تبين لسلطات التحقيق بأن المعطيات المبحوث عنها مخزنة في تلك المنظومة، وهذا ما نص عليه في المادة 05فقرة 04من القانون 09/04المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.[2]

وتأكيدا من المشرع الجزائري على أهمية التعاون الدولي في مجال التصدي لهذا النوع من الجرائم نص بموجب المادة 16[3]من ذات القانون على تمكين السلطات المختصة من تبادل المساعدة القضائية الدولية من أجل جمع الأدلة الإلكترونية الخاصة بهذه الجرائم والتي تفيد في التحقيق، وهو ما أشار إليه المشرع المصري من خلال المادة 4 من القانون رقم 175لسنة 2018المشار إليه سابقا، كما حثت على ذلك مواد الاتفاقية العربية لمكافحة جرائم تقنية المعلومات والتي دعت الدول الأطراف إلى تبادل المساعدات

1حسين ربيعي، آليات البحث والتحقيق في الجرائم المعلوماتية، المرجع السابق، ص 125.

2حيث تنص الفقرة 04 من المادة 05 من القانون رقم 09/04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها على: "... في الحالة المنصوص عليها في الفقرة " أ " من هذه المادة ، إذا كان هناك أسباب تدعوا للاعتقاد بأن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى و أن هذه المعطيات يمكن الدخول إليها ، انطلاقا من المنظومة الأولى ، يجوز تمديد التفتيش بسرعة الى هذه المنظومة أو جزء منها بعد إعلام السلطة القضائية المختصة مسبقًا بذلك إذا تبن مسبقًا بأن المعطيات المبحوث عنها و التي يمكن الدخول إليها انطلاقًا من المنظومة الأولى ، مخزنة في منظومة معلوماتية تقع خارج الإقليم الوطني ، فإن الحصول عليها يكون بمساعدة السلطات الأجنبية المختصة طبقا للاتفاقيات الدولية ذات الصلة وو وفقًا لمبدأ المعاملة بالمثل".

3ينظر المادة 16من القانون رقم 09/04المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال المشار إليه سابقا.

فيما بينهم من أجل تسهيل التحقيقات والإجراءات وجمع الأدلة الإلكترونية، عن طريق تبادل المعلومات المتعلقة بتطور هذه الجرائم والمجرم المعلوماتي وكذا نقل الإجراءات فيما بين الدول، وتبادل طلبات الإنابة القضائية الدولية. (وهذا ما كان محل تفصيل في المطلب الأول المتعلق بمراقبة الاتصالات الإلكترونية).[1]

ومما سبق ذكره يمكننا القول أن امتداد التفتيش إلى خارج الحدود الإقليمية للدولة ضرورة لابد منها لمكافحة الجرائم الإلكترونية كونها من الجرائم الخطيرة العابرة للحدود والتي يسهل فيها إتلاف الدليل الإلكتروني والتلاعب فيه، ولذلك وجب أن يتم هذا الإجراء وفقا للنصوص القانونية الداخلية والاتفاقيات الدولية والمبادئ المتعارف عليها بين الدول، إلا أننا نرى أن مثل هذه الإجراءات خاصة طلبات المساعدة القضائية وما تأخذه من وقت قد يؤثر على السير الحسن لإجراءات التحري والتحقيق وبالتالي يؤدي إلى الفشل في ضبط الدليل الإلكتروني، ولهذا لا تزال معم الدول تسعى جاهدة لإيجاد حلول قانونية من أجل ضمان التصدي الفعال والأمثل لهذه الجرائم.

ث. السلطة المختصة بإصدارالإذن بالتفتيش

بما أن التفتيش إجراء من إجراءات التحقيق الابتدائي التي تمس الحرية الشخصية وحرمة الحياة الخاصة للأفراد، فقد حرص المشرع الجنائي على إسنادها لجهة قضائية تكفل حماية هذه الحقوق والحريات، إلا أن هذه التشريعات لم تسر على نسق واحد فيما يخص تحديد الجهة التي يعهد إليها التحقيق الابتدائي لكي تكون صاحبة الاختصاص الأصيل بإجراء التفتيش، فقد ذهبت بعض التشريعات إلى منح هذه السلطة لقاضي التحقيق أو النيابة العامة كسلطة أصلية، واستثناء لضباط الشرطة القضائية والبعض الآخر منحها لجميع هؤلاء، [2] إذ نجد التشريع الأمريكي والانجليزي قد أخذا بهذا النظام إذ يقع على عاتق النيابة العامة القيام بأغلبية إجراءات التحقيق إلا في حالات معينة، وهذا ما سار عليه المشرع المصري إذ منح سلطة الاتهام والتحقيق معا للنيابة العامة، [3]وفقا للمادة؟؟ ، على خلاف الحال بالنسبة للقانون الفرنسي والجزائري حيث أخذ المشرعان بنظام الفصل بين سلطتي الاتهام والتحقيق، إذ

1يراجع المطلب الأول من هذا المبحث بخصوص المساعدة القضائية الدولية وأهم صورها.

2رضا هميسي، تفتيش المنظومات المعلوماتية في القانون الجزائري، مجلة العلوم القانونية والسياسية، العدد الخامس، جوان 2012، ص 171.

3عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في الإثبات الجنائي، المرجع السابق، ص 63.

عهدت سلطة الاتهام للنيابة العامة أما سلطة التحقيق فعهدت لقاضي التحقيق كاختصاص أصيل إلا أنه يمكن أن يفوض هذا الأمر لضابط الشرطة القضائية استثناء في الحالات التالية:[1]

- **حالة التلبس بالجريمة الإلكترونية**

تتسع سلطات الضبطية القضائية في حالة التلبس لدى معظم التشريعات المقارنة، [2] بحيث يصبح بإمكانها مباشرة اختصاصات سلطة التحقيق كالتفتيش بحثا عن الدليل الجنائي سواء تعلق التفتيش بشخص المتهم أو بمحل إقامته، [3]أو الأماكن المتواجد فيها الحواسيب والوسائل الإلكترونية التي يشتبه أنها محل جريمة إلكترونية، إلا أن بعض التشريعات تختلف فيما بينها حول مدى جواز تفتيش المساكن بناء على حالة التلبس وهو ما لا يجيزه المشرع الأمريكي حيث يجيز الضبط في حالة التلبس ولا يجيز التفتيش، [4] وكذا كل من المشرع المصري والجزائري حيث لم يسمحا بتفتيش المساكن في حالة التلبس وذلك إعمالا للمادة 48[5]من الدستور الجزائري لسنة 2020، والمادة 50[6]من الدستور المصري، وهذا خلافا للمشرع الفرنسي الذي أجاز ذلك بدون الحصول على إذن بذلك وفقا للمادة 56فقرة 1من ق ا ج ف.[7]

1المرجع نفسه، ص 64.

2وقد نظمت حالة التلبس في الجرائم العديد من التشريعات المقارنة، من بينها التشريع الجزائري بموجب المادة 41من ق ا ج والتي تنص على:" توصف الجناية أو الجنحة بأنها في حالة تلبس إذا كانت مرتكبة في الحال أو عقب ارتكابها كما تعتبر الجناية أو الجنحة متلبسا بها إذا كان الشخص المشتبه في ارتكابها إياها في وقت قريب جدا من وقت وقوع الجريمة العامة بالصياح أو وجدت في حيازته أشياء أو وجدت آثار أو دلائل تدعو إلى افتراض مساهمته في الجنيه او الجنحة وتبتسم بصفه التلبس كل جناية أو جنحه وقعت ولو في غير الظروف المنصوص عليها في الفقرتين السابقتين إذا كانت ارتكبت في منزل وكشف المنزل عنها عقب وقوعها و بادر في الحال باستدعاء احد ضباط الشرطة القضائية لإثباتها". والتي تقابلها المادة 30من ق ا ج المصري بقولها: "تكون الجريمة متلبسا بها حال ارتكابها أو عقب ارتكابها ببرهة يسيرة، وتعتبر الجريمة متلبسا بها إذا اتبع المجني عليه مرتكبها أو تبعته العامة مع الصياح أثر وقوعها، أو إذا وجد مرتكبها بعد وقوعها بوقت قريب حاملا آلات أو أسلحة أو أمتعة أو أوراقا أو أشياء أخرى يستدل منها على فاعل أو شريك فيها، أو إذا وجدت به في هذا الوقت آثار أو علامات تفيد ذلك"، والتي تقابلها المادة 53من ق ا ج الفرنسي التي تنص على:

« estqualifie crime ou délit flagrant le crime ou le délit qui se comment actuellement ou qui vient de se commettre il y a aussi crime ou délit flagrant lorsque dans un temps très voisin de l'action la personne soupçonnée est poursuivie pas la clameur publique ou est trouvée en possession d'objets ou présente des traces ou indices laissant penser quelle a participe crime ou au délit ».

3نبيلة هبة هروال، الجوانب الإجرائية لجرائم الإنترنت، المرجع السابق، ص 246.

4رشيدة بوكر، جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري والمقارن، المرجع السابق، ص 289.

5 تنص المادة 48 من التعديل الدستوري الجزائري على: " تضمن الدولة عدم انتهاك حرمه المسكن،

لا تفتيش إلا بمقتضى القانون وفي إطار احترامه.

لا تفتيش إلا بأمر مكتوب صادر عن السلطة القضائية المختصة".

6 تنص المادة 51 من الدستور المصري على: " الكرامة حق لكل إنسان ولا يجوز المساس بها وتلتزم الدولة باحترامها وحمايتها".

7Voir l'article n° 56 du code de procédure pénale français.

ولما كانت الجرائم الإلكترونية كغيرها من الجرائم يمكن أن تتوافر فيها شروط الجريمة المتلبس بها كان من الجائز على ضباط الشرطة القضائية إجراء تفتيش شخص المتهم أم ما يحمله من هاتف نقال أو حاسوب أو أي وسيلة إلكترونية أو تفتيش مسكنه وما يتضمنه من وسائل ومعدات إلكترونية، [1] رغم أنه لم تنص ورالعديد من التشريعات الإجرائية على إمكانية وجود حالة تلبس في الجريمة الإلكترونية مثل المشرع المصري والجزائري إلا أننا نستشف هذا من المواد 47مكرر من ق ا ج ج، والمادة 65مكرر 5من ذات القانون، [2] ومن أمثلة اكتشاف ضابط الشرطة القضائية حالة تلبس بالجريمة الإلكترونية تواجده بأحد مقاهي الإنترنت إذ به يلاحظ أحد الأشخاص يقوم بالدخول لعالم الإنترنت وتحديدا للمواقع الإباحية مثلا ويقوم بطباعة الصور بواسطة الطابعة، ففي هذه الحالة قد توفرت شروط التلبس وبالتالي للضابط أن يقوم بالقبض على الجاني وتفتيشه، [3] وكمثال آخر عن حالة التلبس بالجريمة الإلكترونية قيام الجاني بإعداد صفحات لترويج المخدرات أو الدعوة للقيام بأعمال إرهابية، وشاهده ضابط الشرطة القضائية أو أبلغ عن ذلك مزود خدمات الإنترنت، فرصدته شرطة الإنترنت وتم القبض عليه وتفتيش حاسوبه، كما حدث حين قامت شركة (AOL)لخدمات الإنترنت بالولايات م أ باكتشاف أنشطة دعارة ولقاءات جنسية مع أطفال أثناء قيامها بمراقبة أنشطة المشتركين لديها، فقامت على الفور بتقديم أسمائهم للمباحث الفيدرالية التي تمكنت من القبض عليهم بعد مراقبة أنشطتهم.[4]

ومن خلال هذه الأمثلة يتبين لنا أن حالة التلبس موجودة في الجرائم الإلكترونية وليست بعيدة الاحتمال وإن كان من الصعوبة بمكان رصد المجرم الإلكتروني في شخصه في حالة عدم تواجده مع ضابط الشرطة في فضاء مادي محسوس، بمفهوم المخالفة إن كان المجرم الإلكتروني مثلا في مقهى الإنترنت مع الضابط كما أشرنا في المثال السابق أعلاه، ففي هذه الحالة يسهل على الضابط القبض عليه واقتياده لمركز الشرطة أو حتى تفتيشه، ولكن في حالة ما إذا كان ضابط الشرطة مبحر في شبكة الإنترنت وشهد جريمة قذف أو سب إلكترونية ففي هذه الحالة لا يستطيع معرفة المجرم شخصيا وإنما يستطيع الوصول إلى بروتوكول الإنترنت خاصته أو رقم حاسوبه، ويبقى أمر معرفة هوية المجرم الإلكتروني في هذه الحالة غير مطلق، وتعتريه الكثير من العوائق والصعوبات.

1نبيلة هبة هروال، الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات، المرجع السابق، ص 248.

2وتحديدا عبارة "إذا حدث أثناء التحري في الجريمة المتلبس بها ..."من المادة 47مكرر من ق ا ج ج، وعبارة "إذا اقتضت ضرورات التحري في الجريمة المتلبس بها..."من المادة 65مكرر5من ق ا ج ج.

3نبيلة هبة هروال، الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات، المرجع السابق، ص 410.

4خضرة شنتير، الآليات القانونية لمكافحة الجرائم الإلكترونية، المرجع السابق، ص 82.

- **حالة الإنابة القضائية**

في سبيل تسهيل عمليات التحقيق وضمان عدم ضياع الأدلة الإلكترونية أجازت بعض التشريعات الجنائية لجهة التحقيق أن تندب رجال الضبط القضائي للقيام بعملية التفتيش بدلا عنها، ولا يختلف الأمر بالنسبة للجرائم الإلكترونية فالأصل أن تقوم سلطة التحقيق الأصلية بتفتيش النظم المعلوماتية والأجهزة الإلكترونية بنفسها أو لها ندب أحد رجال الضبط القضائي وفقا للقواعد المنصوص عليها قانونا، ومتى توافرت مجموعة من الشروط أبرزها وما يعنينا في دراستنا هذه، حصول ضابط الشرطة القضائية على إذن من سلطة التحقيق المختصة، وهذا ما نجده في الإنابة القضائية التي يكون محلها الجرائم التقليدية،[1] أما عن الإنابة القضائية في الجرائم الإلكترونية فنجد في المملكة المتحدة قانون إساءة استخدام الحاسب يشترط ضرورة الحصول على إذن قضائي للتفتيش بالنسبة للجرائم المدرجة في القسم الأول منه، والخاصة بالدخول غير المصرح به إلى نظام معلوماتي ما، كما يشترط أن ينبني هذا الإذن على أسباب معقولة ومنطقية تدعو للاعتقاد بأن الجريمة الإلكترونية قد وقعت أو يشتبه في وقوعها،[2] وهذا ما قضت به المادة 487من القانون الجنائي الكندي، حيث أعطت سلطة إصدار إذن لتفتيش وضبط أي شيء بما في ذلك بيانات الحاسب الآلي والأنظمة المعلوماتية طالما توافرت أسباب تثبت ارتكاب الجريمة أو يشتبه في ارتكابها، ووجود أدلة في هذه الأماكن.[3]

كما مكن قانون المنافسة الكندي أي شخص حصل على أمر قضائي بالتفتيش، من استخدام أي نظام للحاسب الآلي لتفتيش بيانات يحتويها أو متاحة لهذا النظام، أو استخراج بيانات في شكل مطبوع أو أي مخرجات أخرى، وضبطها من أجل فحصها أو نسخ صورة عنها وفقا لما جاء في نص المادة 16فقرة 1من هذا القانون.[4]

1ففي القانون الفرنسي مثلا نجد المواد 151إلى 155من ق ا ج تنظم الإنابة القضائية حيث تجيز لقاضي التحقيق تفويض ضابط الشرطة القضائية للقيام ببعض أعمال التحقيق، وهو ما يقبله في نص المواد 70و200من ق ا ج المصري والتي أعطت لعضو النيابة العامة أو لقاضي التحقيق أن يكلف مأمور الضبط القضائي ببعض أعمال التحقيق ما عدا استجواب المتهم، أما عن التشريع الجزائري فقد نظم المشرع أحكام الإنابة القضائية في الجرائم التقليدية في القسم الثامن من الباب الثالث المعنون "في جهات التحقيق"في المواد من 138إلى 142من ق ا ج ج.

2هلالي عبد اللاه أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، المرجع السابق، ص 140.

3المرجع نفسه، ص 140.

4المرجع نفسه، ص 141.

أما عن كل من المشرع الإجرائي الفرنسي والمصري والجزائري فلم يتطرقوا لمسألة الإنابة القضائية في الجرائم الإلكترونية، وبالتالي تطبق النصوص القانونية التقليدية في هذا الشأن[1]

ولصحة إذن الندب أو الإنابة القضائية لا بد من توافر بعض القواعد والشروط التي نصت عليها أغلب التشريعات الجنائية المقارنة، وهذه الشروط منها ما يتعلق بمصدر الإذن ومنها ما يتعلق بمن يصدر له الإذن ومنها ما يتعلق بالإذن نفسه، إذ يشترط أن يصدر إذن التفتيش من السلطة المختصة بالتحقيق سواء تمثلت في النيابة العامة أو قاضي التحقيق المختص إقليميا ونوعيا، ويتحدد اختصاصها هذا بمكان وقوع الجريمة أو مكان القبض على المتهم، أو محل إقامته، أما اختصاصها النوعي فيقصد به أن تكون للقاضي الذي انتدب أحد رجال الضبط سلطة مباشرة إجراء التفتيش في الجرائم الإلكترونية، أما فيما يتعلق بمن يصدر له الإذن بالتفتيش فيشترط القانون أن يكون من أحد رجال الضبط القضائي، وعليه فلا يجوز ندب أعوانهم وإلا كان هذا الندب باطلا، ويعني ذلك وجوب توافر صفة الضبطية القضائية في القائم بالتفتيش، [2] كما يشترط أن يكون هذا الضابط المنتدب مختصا إقليميا ونوعيا بالجريمة محل التفتيش، بالإضافة إلى أنه يجب أن يكون ذو خبرة ومعرفة فنية بتقنيات الحاسب الآلي وكيفية التحقيق في هذه النوعية من الجرائم، [3] وذلك حتى يستطيع أن يتعامل بشكل جيد وسليم مع مخرجات الحاسب وأنظمته المعلوماتية حفاظا على سلامة الأدلة، [4] وليس معنى هذا الاشتراط في الاختصاص ذكره في الإذن بل يذكر اسم القاضي واسم الضابط المنتدب فقط، كما لا يشترط التزام المحقق بندب ضابط معين فله أن يندب كل من يرى أنه يستطيع تنفيذ الإجراء في دائرة اختصاصه.[5]

أما عن الشروط الشكلية الواجب توافرها في الإذن بالتفتيش فتتمثل في:

1وذلك يعني الرجوع للمواد70من ق ا ج المصري، والمادة138ق ا ج الجزائري، و المادة 151و155من ق ا ج الفرنسي التي تنظم أحكام الإنابة القضائية.

2ناني لحسن، التحقيق في الجرائم المتصلة بتكنولوجيا المعلوماتية، المرجع السابق، ص 104.

3هلالي عبد اللاه أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، المرجع السابق، ص 146.

4ومثال ذلك ما حدث في الولايات م أ إذ طلبت إحدى دوائر الشرطة من إحدى الشركات التي تعرضت لقرصنة البرامج أن تتوقف عن تشغيل حاسباتها الآلية لتتمكن من وضعها تحت المراقبة بغية الكشف عن الجاني ومعرفته، بيد أن النتيجة كانت مؤسفة إذ تسببت دائرة الشرطة نظرا لنقص خبرتها في مجال التعامل مع الأنظمة والأدلة الإلكترونية، بإتلاف الملفات والبرامج الخاصة بأنظمة تلك الشركة، نقلا عن هلالي عبد اللاه أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، المرجع السابق، ص 147.

5هلالي عبد اللاه أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، المرجع السابق، ص 145

- أن يكون الإذن مكتوبا[1] ومسببا، [2] كما يجب أن يكون ومؤرخا وموقعا عليه ممن أصدره ويذكر فيه اسم من أصدره ووظيفته.[3]
- أن يكون الإذن صريحا في الدلالة على التفويض، ويتضمن صفة ووظيفة المأذون له بالتفتيش (ضابط الشرطة القضائية).[4]
- أن يحدد في الإذن نوع الجريمة وموضوع التفتيش، ومدته.[5]
- أن يحدد في الإذن محل التفتيش أي تحديد المسكن والشخص المراد تفتيشه تحديدا دقيقا، ولا شك أن هذا التحديد الدقيق للإذن بالنسبة للجرائم الإلكترونية قد يخلق إشكالات عديدة وصعوبة نوعا ما في احترام هذا الشرط أثناء الممارسة العملية في تفتيش أجهزة وأنظمة الحاسب الآلي، ويرجع ذلك للطبيعة الخاصة لهاته الجرائم والكم الهائل من البيانات والملفات التي تحتويها هذه الأجهزة، وهذا ما يثير التساؤل حول ما إذا كان يجب تحديد محل التفتيش في الإذن تحديدا دقيقا كتحديد نوع الجهاز الإلكتروني أو إحدى مكوناته (كالوحدة المركزية أو الذاكرة، أو القرص الصلب، و غيرها...)، أو ملحقاته (كالطابعة، وجهاز المسح الضوئي مثلا ...) التي يرد عليها التفتيش دون غيرها، أم أنه يكفي الحصول على الإذن بتفتيش المكان الذي تتواجد فيه هذه الأجهزة حتى يشملها جميعها؟[6]

نرى أن غالبية التشريعات المقارنة استقرت على أنه يكفي الحصول على الإذن بتفتيش مسكن المتهم حتى يكون لضباط الشرطة القضائية تفتيش كل الأجهزة الإلكترونية وملحقاتها المتواجدة بهذا المسكن، وكل الملفات والبيانات التي تحتويها هذه الأخيرة، وحجتهم في ذلك أن هاته الأجهزة تعتبر مخزنا لمئات وآلاف المعلومات والبيانات ولذلك لا يعقل مع هذه القدرة التخزينية الهائلة واللامتناهية إصدار إذن بالتفتيش حسب عدد هذه الملفات.[7]

في حين اتجهت أحكام أخرى منها أحكام القضاء الأمريكي إلى أن كل ملف في الكمبيوتر يتطلب إذنا خاصا لتفتيشه، ويرجع أساس هذا الحكم إلى اعتبار أن الكمبيوتر يحتوي على الكثير من المعلومات التي

1ينظر المواد 44من ق ا ج ج، والمادة 41فقرة 1من اللائحة التنفيذية لنظام الإجراءات ج السعودي، والمادة 91من ق ا ج م.

2ينظر المواد 41من نظام ا ج السعودي، والمادة 91فقرة 1من ق ا ج م...

3ينظر المواد 4من ق ا ج ج، والمادة 41فقرة 2من اللائحة التنفيذية لقانون ا ج السعودي.

4خالد ممدوح ابراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص 189.

5ينظر المواد 44من ق ا ج ج، والمادة 41فقرة 2من اللائحة التنفيذية لقانون ا ج السعودي.

6جمال براهيمي، التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص 38.

7لمزيد من التفاصيل ينظر عمر محمد أبو بكر بن يونس، الإجراءات الجنائية عبر الإنترنت في القانون الأمريكي، المرجع السابق، ص 56وما بعدها.

تتعلق بالحياة الخاصة لصاحب هذا الجهاز، فإذا أجزنا لضابط الشرطة القضائية فتح الملفات الأخرى وتفتيشها دون إذن خاص بها فإن هذا يعد تعد على هذه الخصوصية.[1]

أما عن موقف المشرع الجزائري اتجاه هذه المسألة فهو غير واضح وغير حاسم، ذلك أن القواعد الخاصة بالتفتيش التي جاء بها قانون ا ج ج تتعلق بالتفتيش التقليدي الذي يكون محله المساكن وملحقاتها أو المكونات المادية للأجهزة الإلكترونية،[2] وأن القواعد الخاصة بإجراء التفتيش المعلوماتي الواردة في القانون رقم 09/04لم يحدد المشرع فيها هذا الشرط، وإنما اكتفى بالإشارة إلى ضرورة قيام جهات التحقيق بإعلام السلطة القضائية المختصة مسبقا قبل تمديد التفتيش إلى منظومة معلوماتية أخرى، ومن هذه النصوص القانونية يفهم أن المشرع الجزائري يميل إلى عدم جواز تفتيش النظام المعلوماتي وما يحتويه من بيانات دون إذن خاص من السلطة المختصة.[3]

وعليه يتعين على المشرع الجزائري التدخل وسن نصوص قانونية صريحة وواضحة بخصوص هذه المسألة لتفادي هذا الغموض والإبهام الذي قد يؤدي إلى تعسف السلطات والتعدي بذلك على حرمة الحياة الخاصة للأفراد، وذلك بإتباع ما سارت عليه أغلب التشريعات المقارنة التي أجازت تفتيش مسكن المتهم وكل الأجهزة الإلكترونية بمكوناتها، وملحقاتها، والملفات المتواجدة بها، وكذا أنظمتها المعلوماتية بموجب إذن واحد صادر من السلطة المختصة.

كما تجدر الإشارة إلى أنه قد تكتشف جريمة إلكترونية أخرى غير تلك التي صدر بشأنها التفتيش كما نصت المادة 44فقرة 5من ق ا ج ج، [4] والمادة 65مكرر 5في فقرتها الثانية، وكذا المادة 50من ق ا ج م، [5] والفقرة 04من المادة 76من ق ا ج ف، [6] إذ سمحت هذه التشريعات بجواز تفتيش البيانات الخاصة بتلك الجرائم دون أن يكون ذلك سببا في بطلان إجراءات التحقيق، في حين انقسم القضاء الأمريكي إلى

1المرجع نفسه، ص 60.

2ينظر المواد من44إلى المادة 47مكرر من ق ا ج ج.

3ينظر المواد 05و06من القانون رقم 09/04المشار إليه سابقا، وينظر أيضا ليندا بن طالب، الدليل الإلكتروني ودوره في الإثبات الجنائي، المرجع السابق، ص 62.

4 تنص الفقرة 05 من المادة 44 من ق ا ج ج على: " إذا اكتشفت أثناء هذه العمليات جرائم أخرى غير تلك التي ورد ذكرها في إذن القاضي فإن ذلك لا يكون سببا لبطلان الإجراءات العارضة".

5 تنص المادة 50 من ق ا ج المصري على : " لا يجوز التفتيش الا للبحث عن أشياء الخاصةبالجريمة الجاري جمع الاستدلالات أو حصول التحقيق بشأنها ومع ذلك إذا ظهر عرضا أثناء التفتيش وجود أشياء تعد حيازاتهاالجريمة أو تفيد في كشف الحقيقة في جريمة أخرى جاز لمأمور الضبط القضائي أن يضبطها",

6Voir l'article n° 76/4 du code de procédure pénale français

اتجاهين: أقر الاتجاه الأول أنه لا يمكن لضابط الشرطة القائم بعملية التفتيش أن يقوم بتفتيش ملف ما يخص جريمة أخرى غير المأذون له بها، بل عليه أن يوقف التفتيش مؤقتا لأجل الحصول على إذن آخر للتفتيش، أما الاتجاه الثاني يرى أنه بمجرد البدء في إجراء التفتيش على جهاز الحاسوب فإن المتهم لم يعد يملك توقعا معقولا للخصوصية في المحتويات الباقية من الحاسوب خاصته، لذا قررت المحكمة أن التوسع في تفتيش كل ما يكتشف عرضا يعد أمرا مشروعا ولا ينتهك التعديل الرابع من الدستور الأمريكي، لأن الفترة التي يتوقف فيها الضابط عن التفتيش للحصول على إذن آخر قد تسمح للجاني بتدمير الأدلة والتلاعب بها، مما يسبب ضياعها نهائيا، لذا أجاز القانون لقاضي التحقيق والقائم بالتفتيش بحجز كل ما تم اكتشافه وتبليغه للنيابة العامة فورا لتقوم بما تراه مناسبا.[1]

- **حالة التفتيش الإرادي بناء على رضا المتهم**

وتتحقق هذه الحالة حينما يعرض رجل الضبط القضائي على الشخص المراد تفتيشه صراحة أن يقوم بتفتيشه أو تفتيش مسكنه ويبدي ذلك الشخص رأيه بالموافقة على التفتيش بشكل إرادي دون تعرضه للعنف أو الإكراه من قبل الضابط، حيث يلجأ إلى هذا النوع من التفتيش في حالة وجود شك لدى القائم بالتفتيش على وقوع جريمة إلكترونية، ولم تتوفر لديه الأدلة الكافية للكشف عنها أو عن مرتكبها، ويهدف هذا التفتيش إلى البحث فيما إذا كان مالك الحاسوب مثلا أو الشبكة أو المؤسسة التي تدير الخادم أو المضيف أو البيانات الكامنة في الحاسوب مرتكبا أو ضالعا في الجريمة، ومن الأمثلة على ذلك القبض على متهم في مقهى للإنترنت وقيام الضابط بتفتيش حاسوبه الذي يستخدمه، ففي هذه الحالة على الضابط أن يسأل مالك المقهى أو المدير فيما إذا كان يقبل تفتيش الحاسوب المذكور أم لا.[2]

ومن الأمثلة أيضا قيام أحد مزودي خدمة الإنترنت بترداد عبارات أمام ضابط قضائي بأن لديه اشتراك بالبريد الإلكتروني مع أحد مروجي المخدرات والمؤثرات العقلية والذي يتم من خلاله عملية الترويج، فيتدخل ذلك الأخير بسؤاله لذلك المزود على إمكانية تفتيش جهازه للتحقق، فإن وافق ذلك الأخير فإن التفتيش في هذه الحالة يكون صحيحا ولا يتطلب إذنا.[3]

1خضرة شنتير، الآليات القانونية لمكافحة الجريمة الإلكترونية، المرجع السابق، ص 85وما بعدها.

2 المرجع نفسه، ص 87.

3نبيلة هبة هروال، الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات، المرجع السابق، ص 249.

ولأن عملية التفتيش الإرادي قد تمس بخصوصية الأفراد كما هو الحال في التفتيش العادي، فكان لابد من إحاطتها بضمانات منها أن تكون صيغة الموافقة على التفتيش بشكل صريح وليس ضمني، وأن تكون مكتوبة إلا إذا كان الشخص المعني لا يعرف الكتابة فله أن يختار شخص آخر ليحل محله، ويجب في هذه الحالة ذكر كل هذا في محضر التفتيش، إلا أن بعض التشريعات نجدها تشترط صدور هذه الموافقة من الشخص المعني دون غيره وأخرى لا، مثالها المشرع الفرنسي إذ ينص في الفقرة 2من المادة 76من ق ا ج ف[1] على وجوب أن تكون هذه الموافقة صريحة ومكتوبة وصادرة من ذي الشأن ولا أحد غيره، ولم يصرح المشرع الفرنسي بإمكانية أن يحل شخص آخر محل الشخص الذي يقع عليه التفتيش، [2] في حين نجد أن المشرع الأمريكي يكتفي في حالة غياب الشخص المعني بأشخاص آخرين يحلون محله، وهذا ما نجده كثيرا في الحالات التي يشترك فيها شخصان أو أكثر في استخدام أو امتلاك ذات جهاز الحاسوب مثلا.[3]

2. الضوابط الشكلية:

وتتمثل فيما يلي:

---

1 تنص المادة 64 من ق ا ج ج على: "لا يجوز تفتيش المساكن ومعاينتها وضبط الأشياء المثبتة للتهمة إلا برضا صريح من الشخص الذي ستتخذ لديه هذه الإجراءات ويجب أن يكون هذا الرضا بتصريح مكتوب بخط يد صاحب الشأن فان كان لا يعرف الكتابةبإمكانها الاستعانة بشخص يختاره بنفسه ويذكر ذلك في المحضر مع الإشارة صراحة إلى رضاه" والتي تقابلها المادة 76 من ق ا ج الفرنسي بقولها: "

"les perquisitions visites domiciliaires et saisies de pièces a conviction ou de biens dont la confiscation est preuve a L'article 131 21 du code pénal ne peuvent effectuées sans L'assentiment Exprès de la personne Chez laquelle l'opération a lieu
cet assentiment doit faire l'objet d' une déclaration Écrite De la main de l'intéressé ou si celui ci ne sait écrire il en est fait Mention ou procès verbal ainsi Que de son Assentiment"

2هلالي عبد اللاه أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، المرجع السابق، ص 161.

3وخاصة إذا لم تكن الملفات المتواجدة بهذا الحاسوب محمية بكلمة سر خاصة بمالكها، ففي هذه الحالة يمكن لرجال الضبط القضائي الاعتماد على إرادة أحدهما طالما أن له سلطة على الحاسب محل التفتيش، وهذا ما قضى به القضاء الأمريكي في قضية United States V. Smith، والتي تتلخص وقائعها في أن المدعو Smithكان يعيش مع سيدة تدعى Uchmanوابنتها ولما أثير ضده ادعاء التحرش الجنسي بالأطفال وافقت السيدة على تفتيش الحاسوب الخاص به والموجود داخل المنزل في تجويف مرتبط بحجرة النوم الرئيسية، وبالرغم من الاستعمال القليل للحاسوب من طرف السيدة إلا أن المحكمة قررت بإمكانية إبداء هذه السيدة الموافقة على تفتيش الحاسوب الخاص بالمتهم، وذلك على أساس أنها لم تكن ممنوعة من الدخول إلى المكان المتواجد فيه الحاسوب، كما أن المتهم لم يضع كلمة سر يحمي بها حاسوبه الشخصي، كما يعد الأزواج والأبناء والشركاء المنزليون من الأشخاص الذين يمكن لهم إبداء الموافقة على تفتيش الحاسوب المشترك في حالة غياب الشخص المعني، كما يمكن للآباء الموافقة على تفتيش أغراض أبنائهم وغرفهم إذا كانوا صغارا، وهذا ما قرره القضاء الأمريكي في قضية Laving. نقلا عن نبيلة هبة هروال، الجوانب الإجرائية لجرائم الإنترنت، المرجع السابق، ص 251.

أ. الحضور الضروري لبعض الأشخاص أثناء التفتيش

إن حضور بعض الأشخاص أثناء التفتيش يعتبر ضمانة للمتهم ورقابة على سلامة الإجراء، كما يعتبر من جهة ثانية ضمانة بالنسبة للقائم بالتفتيش من اتهامه باختلاق الأدلة أو تسببه في ضياعها، إلا أنه بالرجوع للتشريعات المقارنة نجدها لم تشترط لصحة إجراء التفتيش الواقع على الأشخاص حضور شهود أو أشخاص معينين، [1] أما فيما يتعلق بتفتيش المساكن وما في حكمها نجد المشرع السعودي قد نص بموجب نظام الإجراءات الجزائية السعودي في المادة 46منه على أنه: "يتم تفتيش المسكن بحضور صاحبه أو من ينيبه أو أحد أفراد أسرته البالغين المقيمين معه، وإذا تعذر حضور أحد هؤلاء وجب أن يكون التفتيش بحضور عمدة الحي أو من في حكمه أو شاهدين ويمكن لصاحب المسكن أو من ينوب عنه من الاطلاع على إذن التفتيش ويثبت ذلك في المحضر"

أما عن قانون الإجراءات الجنائية المصري فاشترط حضور شاهدين في حالة ما إذا كان القائم بالتفتيش أحد مأموري الضبط القضائي على أن يكون هذان الشاهدان من أقارب المتهم البالغين أو من القاطنين معه بالمنزل أو من الجيران طبقا للمادة 51من ق ا ج م، أما إذا كان القائم بالتفتيش هو قاضي التحقيق أو عضو النيابة العامة فيستلزم طبقا للمادة 92منه أن يكون بحضور المتهم، وإذا لم يتيسر ذلك لغياب المتهم أو لرفضه الحضور يتم التفتيش بحضور من ينيبه كلما كان ذلك ممكنا، فإن تعذرت هذه الإنابة سواء لرفض المتهم أو لعدم إمكانية الاتصال به مقدما قبل التفتيش، كان على النيابة العامة إجرائه بدون حضور أحد.[2]

ويذهب جمهور من الفقهاء في مصر إلى اعتبار حضور المتهم هو من الشروط الجوهرية لصحة التفتيش، والذي يترتب على مخالفتها البطلان إلا أن القضاء قضى بعكس ذلك، [3] وعلى خلاف ذلك ينص القانون الجزائري في المادة 45من ق ا ج، والقانون الفرنسي في المادة 56من ق ا ج على وجوب حضور شاهدين في كلا الحالتين سواء كان القائم بالتفتيش ضابط الشرطة القضائية أو قاضي التحقيق، إذ يشترط أولا أن يتم التفتيش بحضور المتهم وفي حالة تعذره عن الحضور كان لضابط الشرطة القضائية أن يكلفه بتعيين ممثل له، وإذا امتنع أو كان هاربا استدعى ضابط الشرطة شاهدين من غير الموظفين

1عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في الإثبات الجنائي، المرجع السابق، ص 66.

2هلالي عبد اللاه أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، المرجع السابق، ص 164.

3إذ ذهبت محكمة النقض المصرية قديما إلى القول ببطلان التفتيش في حاله عدم حضور المتهم إلا أنها عدلت عن موقفها وقضت بأن عدم حضور هذا الأخير لا يترتب عليه البطلان وذلك لأن القانون لم يجعل من حضور المتهم شرطا جوهريا لصحة التفتيش، نقلا عن نبيلة هبة هروال، الجوانب الإجرائية لجرائم الإنترنت، المرجع السابق، ص 256.

الخاضعين لسلطته لحضور هذا التفتيش، غير أن المشرع الجزائري استثنى من هذا الشرط بعض الجرائم الخاصة طبقا لنص الفقرة الأخيرة من المادة 45من ق ا ج، [1] فكما هو ملاحظ قد استثنى المشرع التفتيش في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات من هذا الشرط إذ يتم التفتيش فيها دون حضور هؤلاء الأشخاص، [2] ولعل الحكمة من هذا الطابع المميز لهذه الجرائم وطبيعة الدليل الإلكتروني التي تستلزم السرية والتدخل السريع للسلطات تفاديا لطمس الدليل أو إتلافه أو التلاعب فيه، ونحن نرى أنه حسن ما فعل المشرع ج بهذا الاستثناء لأن طبيعة الجرائم التقليدية تختلف تماما عن طبيعة الجرائم الإلكترونية.

كما تجدر الإشارة إلى أن حضور هؤلاء الشهود في عملية التفتيش يتطلب أن يكونوا ملمين بتقنيات الحاسب الآلي والإنترنت والتعامل مع الأدلة الإلكترونية أو على الأقل لديهم معرفة كافية عنها، وإلا فلا جدوى من حضورهم، لأن أي تلاعب من طرف القائم بالتفتيش لن يستطيع الشاهد أن يكتشفه.[3]

ب. المدة

حرصا على تضييق نطاق الاعتداء على الحرية الشخصية وحرمة المساكن تحرص بعض التشريعات الإجرائية على تحديد وقت معين للتفتيش، في حين تترك بعض التشريعات الإجرائية أمر تحديد الوقت للقائم بالتفتيش، [4] ومن بين تلك التشريعات قانون الإجراءات الجنائية المصري والذي لم يحدد وقتا معينا يتم فيه الإجراء وإنما ترك ذلك للقائم بالتفتيش دون النظر لأي اعتبار يتعلق بالمحل المراد تفتيشه، حيث يمكن القيام به في أي ساعة من ساعات الليل أو النهار[5] وهذا ما تواترت أحكام محكمة النقض المصرية على القضاء به، [6] ونفس الشيء بالنسبة للمشرع السعودي الذي لم يحدد مدة التفتيش بل ترك أمر تحديدها للمفتش مع اشتراطه أن لا تكون هذه المدة طويلة حتى لا يبقى المتهم مهددا في حريته وحرمة مسكنه على أن تحتسب من يوم صدور الإذن، كما أضافت اللائحة التنفيذية لهذا النظام في مادتها 41فقرة 5أنه لا يجوز التفتيش بعد مضي سبعة أيام من تاريخ صدور الإذن به ما لم يصدر إذن جديد.[7]

1ينظر المادة 45من ق ا ج ج.

2ينظر المواد 45من ق ا ج ج، والمادة 56من ق ا ج الفرنسي.

3رفاه خضير جياد العرضي، الدليل الإلكتروني وأثره في مجال نظرية الإثبات الجنائي، المرجع السابق، ص 125.

4رشيدة بوكر، جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري والمقارن، المرجع السابق، ص 415.

5نبيلة هبة هروال، الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات، المرجع السابق، ص 258.

6هلالي عبد اللاه أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، المرجع السابق، ص 175.

7عبد الله بن عبد العزيز بن عبد الله الخثعمي، التفتيش في الجرائم المعلوماتية في النظام السعودي، المرجع السابق، ص 59.

وعلى العكس من ذلك نجد بعض التشريعات تحظر التفتيش في بعض الأوقات حيث وضعت قيودا زمنية لمباشرة هذا الإجراء من بينها المشرع الأمريكي إذ حدد ميقات التفتيش من الساعة السابعة صباحا إلى الساعة التاسعة مساء، [1] وقد اتبع نفس النهج كل من المشرع الفرنسي والمشرع الجزائري، فنجد المشرع الفرنسي قد حدد المدة من الساعة السادسة صباحا إلى الساعة التاسعة مساء وذلك بموجب المادة 59من ق ا ج ف، [2] في حين حددها المشرع الجزائري في المادة 47من ق ا ج ج من الساعة الخامسة صباحا إلى الساعة الثامنة مساء، [3] إلا أنه قد أوردت هذه التشريعات بعض الاستثناءات يجوز فيها الخروج عن القاعدة الأصلية، فيصح فيها إجراء التفتيش ليلا أو نهارا وتتمثل هذه الحالات فيما يلي:

- حالة رضا صاحب الشأن رضاء حرا، صريحا وعن علم بالسبب.[4]
- حالة الضرورة وتتمثل في الاستغاثة من داخل المنزل.[5]
- في الأحوال الاستثنائية المقررة قانونا كحالة الطوارئ طبقا لنص المادة 11من قانون 03أفريل لسنة 1955، وحالتي الحريق والغرق وفقا لنص المادة 76من دستور فرنسا والمادة 45من ق ا ج م، وما تنص عليه المادة 77من حق مفتش الصحة والبوليس في دخول المستشفيات للتفتيش على شؤونها.[6]
- في التحقيق في الجرائم المعاقب عليها في المواد من 342إلى 348من ق ع ج، وذلك داخل كل فندق أو منزل مفروش أو فندق عائلي أو محل لبيع المشروبات أو نادي أو منتدى أو مرقص أو أماكن المشاهدة العامة وملحقاتها، وفي أي مكان مفتوح للعموم أو يرتاده الجمهور إذا تحقق أن أشخاصا يمارسون فيه الدعارة.[7]

1رفاه خضير جياد العرضي، الدليل الإلكتروني وأثره في مجال نظرية الإثبات الجنائي، المرجع السابق، ص 125.

2 Article n° 59 du code de procédure pénale ; dispose que : « Sauf réclamation faite de l'intérieur de la maison ou exception prévues par la loi les perquisition et les visites homiliaires ne peuvent être commencées a avant 6 heures et après 21 heures

3 تنص المادة 47 فقرة 1من ق ا ج ج على: " لا يجوز البدء في تفتيش المساكن ومعاينتها قبل الساعةالخامسة صباحا ولا بعد الساعةالثامنة مساء إلا إذا طلب صاحب المنزل ذلك أو وجهت نداءات بناء أو في الأحوال الاستثنائيةالمقررة قانونيا",

4ينظر المادة 47فقرة 1من القانون 06/22المتضمن ق ا ج ج.

5ينظر المادة 47فقرة 1من القانون 06/22المتضمن ق ا ج ج.

6هلالي عبد اللاه أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، المرجع السابق، ص 177.

7ينظر المادة 47فقرة 2من ق ا ج ج، والتي كانت تقابلها المادة 59فقرة 2من ق ا ج الفرنسي وتم إلغائها من أول مارس 1994بالقانون رقم 92/336الصادر في 16ديسمبر 1992. نقلا عن هلالي عبد اللاه أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، المرجع السابق، ص 178.

- كما أضاف المشرع الجزائري قائمة من الجرائم التي يجوز فيها التفتيش في أي ساعة من ساعات النهار أو الليل بموجب الفقرة 3من المادة 47من القانون رقم 06/22المتضمن ق ا ج ج، [1] وتتمثل هذه الجرائم في جرائم المخدرات، والجريمة المنظمة، والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، وجرائم تبييض الأموال والإرهاب، وكذا الجرائم المتعلقة بالتشريع الخاص بالصرف، إذ يجوز إجراء التفتيش والمعاينة والحجز في أي محل سكني أو غير سكني في كل ساعة من ساعات النهار أو الليل وذلك بناء على إذن مسبق من وكيل الجمهورية المختص، والملاحظ أن المشرع ج بإضافته لهذه الفقرة إنما أدرك الطبيعة المميزة لهاته الجرائم وخاصة الجريمة الإلكترونية وخصوصيتها خاصة من حيث أنه يمكن ارتكابها في أي وقت وأن أدلة الإثبات فيها سهلة المحو والإتلاف، إذ يمكن للمتهم أن يقوم بمحوها أو التلاعب بها قبل وصول السلطات إليها، وبالتالي فإن تأخير إجراء التفتيش قد يعرقل من السير الحسن لمجريات التحقيق.

وتجدر الإشارة إلى أنه رغم إضافة هذه الفقرة في ق ا ج إلا أنه كان يجب على المشرع الجزائري النص على مدة تفتيش المنظومة المعلوماتية ضمن القانون 09/04الذي نظم من خلاله إجراء التفتيش في المنظومة المعلوماتية وحجز المعطيات بها، ونفس الرأي بالنسبة للمشرع المصري، إلا أن المشرع الفرنسي قد حددها من خلال الاتفاقية الأوروبية لجرائم الإنترنت بموجب المادة 19منها، والتي أقرت أن جميع البيانات يتم تفتيشها خلال المدة الزمنية المقررة للتفتيش في ق ا ج ف، أي أن يتم التفتيش من الساعة السادسة صباحا إلى الساعة التاسعة مساء، [2] إلا أنه يمكن الخروج عن هذه المدة في حالة الجرائم المتلبس بها وفقا للمادة 706- 90من ق ا ج الفرنسي، وفي إطار التحقيقات متى اقتضت الضرورة ذلك وفقا للمادة706[3]- 91من ذات القانون.[1]

---

1 تنص المادة 47من ق ا ج ج على: "غير أنه يجوز إجراء التفتيش والمعاينة والحجز في كل ساعة من ساعات النهار أو الليل قصد التحقيق في جميع الجرائم المعاقب عليها في المواد 342 إلى 348 من قانون العقوبات وذلك داخل كل فندق أو منزل مفروش أو فندق عائلي أو محل لبيع المشروبات أو نادي أو منتدى أو مرقص أو أماكن المشاهدة العامة وملحقاتها وفي أي مكان مفتوح للعموم أو يرتاده الجمهور إذا تحقق أن الأشخاص يستقبلون فيه عادة لممارسة الدعارة.

وعندما يتعلق الأمر بجرائم المخدرات أو الجريمة المنظمة عبر الحدود الوطنية أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبييض الأموال والإرهاب وكذا الجرائم المتعلقة بالتشريع الخاص بالصرف فإنه يجوز إجراء التفتيش والمعاينة و الحجز في كل محل سكني أو غير سكني في كل ساعة من ساعات النهار أو الليل وذلك بناء على إذن مسبق من وكيل الجمهورية المختص .

عندما يتعلق الأمر بالجرائم المذكورة في الفقرة الثالثة أعلاه يمكن قاضي التحقيق أن يقوم بأية عمليه تفتيش أو حجز ليلا أو نهارا وفي أي مكان على امتداد التراب الوطني أو يأمر ضباط الشرطة القضائية المختصين للقيام بذلك".

2نبيلة هبة هروال، الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات، المرجع السابق، ص 262،

3 Voir l'article n° 706-90 et 706-91 du code de procédure pénale français

ت. المحضر

لما كان التفتيش إجراء من إجراءات التحري والتحقيق فإنه يستلزم بالضرورة تحرير محضر يثبت فيه القائم بالتفتيش ما تم من إجراءات وما أسفرت عنه عملية التفتيش من أدلة[2] مادية كالحاسوب وملحقاته، أو أدلة معنوية من بيانات ومعطيات إلكترونية، ولم يتطلب القانون شكلا خاصا في محضر التفتيش سواء بالنسبة للجرائم التقليدية أو الإلكترونية، فلا يشترط لصحته سوى ما تستوجبه القواعد العامة كما أشرنا سابقا من تاريخ تحريره وتوقيع القائم بالتفتيش، كما يستلزم بالإضافة لهذه الإجراءات أن يكون القائم به متخصص في التقنيات الحديثة ومجال الحوسبة أو أن يرافق الضابط شخص خبير في هذا المجال للاستعانة به في مجال الخبرة الفنية الضرورية وفي صياغة مسودة محضر التفتيش، بحيث تتم تغطية كل الجوانب الفنية للعملية والأدلة المضبوطة وأيضا للمحافظة عليها من كل تلف أو مسح.[3]

الفرع الثاني: حجز المعطيات المعلوماتية

من المعروف أن النتيجة الطبيعية والحتمية التي تنتهي إليها إجراءات التحري والتحقيق هي ضبط الأدلة الجنائية من أجل إثبات الجريمة الواقعة ونسبتها لمرتكبها، ونظرا لكون محل الضبط يختلف في الجرائم الإلكترونية عنه في الجرائم الأخرى _إذ يرد الأول على أشياء ذات طبيعة معنوية كالبيانات المعالجة الكترونيا، أما الثاني فيرد على أشياء مادية ملموسة_ فلا يثير ضبط المكونات المادية للحاسب الآلي أية مشاكل، في حين يثور الجدل حول مدى إمكانية وقابلية ضبط وحجز البيانات والمكونات المعنوية؟[4]

وعلى إثر هذا الجدل انقسم الفقه إلى اتجاهين أساسيين:

1وهيبة رابح، الإجراءات المتبعة أمام الأقطاب الجزائية المتخصصة، المرجع السابق، ص 225.

2وهيبة رابح، الإجراءات المتبعة أمام الأقطاب الجزائية المتخصصة، المرجع السابق، ص 263.

3هلالي عبد اللاه أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، المرجع السابق، 170.

4رشيدة بوكر، جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري المقارن، المرجع السابق، ص 418.

أولا: الاتجاه الأول

يرى هذا الاتجاه أن البيانات المعالجة آليا لا تصلح أن تكون محلا للضبط والحجز لانتفاء الكيان المادي عنها وبذلك لا يمكن حجزها إلا بعد نقلها من كيانها المعنوي إلى الكيان المادي الملموس، [1] وذلك إما عن طريق تجسيدها في دعامات مادية أو تصويرها وطبعها في مخرجات الحاسوب أو في أي وعاء آخر، حيث يستند هذا الرأي إلى أن محل النصوص القانونية المنظمة لعملية الحجز هو الأدلة المادية الملموسة، [2] وهذا ما جسده الفقه الألماني وقانون الإجراءات الألماني في المادة 94منه، [3]

ثانيا: الاتجاه الثاني

يرى هذا الاتجاه إمكانية حجز هذه البيانات وحفظها على وسائط مادية، وحجتهم في ذلك أن هذه البيانات الإلكترونية ما هي إلا ذبذبات وموجات كهرومغناطيسية تقبل التسجيل والحفظ والتخزين على وسائل مادية، وبالتالي يمكن نقلها وبثها واستقبالها، وإعادة إنتاجها، ويستند هذا الرأي إلى بعض النصوص التشريعية وخاصة تلك التي أجازت التفتيش في الكيانات المعنوية للحاسب الآلي والمعطيات الإلكترونية، [4] وعليه إذا كان تفتيش المكونات المعنوية أمر ضروري ومباح فمن الضرورة إباحة ضبطها، ومن بين التشريعات التي أجازت ضبط هذه المكونات نجد التشريع الكندي في المادة 79فقرة 7من قانون الإثبات الكندي، والتي تجيز تفتيش وضبط الدفاتر والسجلات سواء كانت مكتوبة أو في شكلها الإلكتروني، كما استحدث المشرع الفرنسي قانون الأمن الداخلي رقم 239لسنة 2003المشار إليه سابقا، إذ تنص المادة 76- 1فقرة 3على أن البيانات التي يتم الحصول عليها من خلال تفتيش النظام المعلوماتي يتعين نسخها على دعامات، وتحريزها في أحراز مختومة بالشمع الأحمر، [5] وهذا تطبيقا لما جاءت به الاتفاقية الأوروبية لجرائم الإنترنت (اتفاقية بودابست) من أحكام تنظم إجراء الضبط في البيئة الإلكترونية، من خلال المادة 19من القسم الرابع منها والتي تنص على أنه: "من سلطة كل دولة طرف أن تتخذ الإجراءات التالية: أن

1Kaspersen, computer crimes and others crimes against information technology in the Netherlands in ;Ulrichsieber (ed), Information Technologycrime,kolnetc ;carlHeymannsVerlag 1994,page 343_376.

2نبيلة هبة هروال، الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات، المرجع السابق، ص 265.

3هشام محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية، المرجع السابق، ص 94.

4أشرف عبد القادر قنديل، الوسائل الإلكترونية ودورها في الإثبات، المرجع السابق، ص 112.

5 Article n° 76-1/3 du Loi n° 2003-239 du 18 mars 2003 pour la sécurité intérieure en France dispose que : « Les données auxquelles il aura été permis d'accéder dans les conditions prévues par le présent article peuvent être copiées sur tout support , les supports de stockage informatique peuvent être saisis et placés sous scellés dans les conditions prévues par le présent code ».

تضبط نظام الكمبيوتر أو جزءا منه أو المعلومات المخزنة على أي وسيط من وسائط التخزين الخاصة بالكمبيوتر، وأن تحافظ على سلامة تلك المعلومات المخزنة".[1]

كما أشار المشرع الأمريكي إلى إجراء الضبط من خلال المرشد الفيدرالي، والذي حدد من خلاله أساليب الضبط المختلفة وفقا لطبيعة كل مخالفة والقانون الصادر بشأنها، إذ أجاز مصادرة القطع الصلبة كالحاسوب مثلا.[2]وكذا في القانون البلجيكي تطرق المشرع إلى قابلية المكونات المعنوية للضبط بموجب المادة 39و39مكرر من قانون تحقيق الجنايات البلجيكي، [3]كما نجد المادة 251من ق ا ج اليوناني تعطي لسلطات التحقيق إمكانية القيام بأي شيء يكون ضروري لجمع وحماية الدليل ، كأن تعطي أمرا للخبير التقني لجمع الدليل وتحليله، كما تمنح المادة 92من ق ا ج الألماني لسلطات التحري والتحقيق بضبط الدليل رغم أنه لم ينص صراحة على ضبط المعطيات الإلكترونية وإنما اكتفى بالنص على ضبط وتسجيل أي معلومات تكون مفيدة لكشف الحقيقة.[4]

أما المشرع المصري فقد تطرق للضبط في الجريمة الإلكترونية من خلال الفقرة الأولى من المادة 06من قانون رقم 175لسنة 2018المتعلق بمكافحة جرائم تقنية المعلومات، إذ يمكن بمقتضاها لمأموري الضبط القضائي المختصين بموجب أمر مسبب من جهة التحقيق المختصة، ولمدة ثلاثين يوما قابلة للتجديد مرة واحدة، ضبط أو سحب أو جمع أو التحفظ على البيانات والأنظمة المعلوماتية وتتبعها أينما وجدت، مع الحرص على أن لا يؤثر ذلك في استمرارية أداء خدماتها، ولعل تحديد هذه المدة بثلاثين يوما بغية السرعة في إجراء الضبط والتحفظ على الأدلة الإلكترونية كونها سهلة الإتلاف والتغيير، وهذا ما أكدته المادة 27من القرار الرئاسي رقم 276لسنة 2004المتعلق بالموافقة على انضمام جمهورية مصر العربية إلى الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، الموقعة في القاهرة بتاريخ 21ديسمبر 2010، [5] كما بينت المواد 53و55والمادة 91من ق ا ج م[6] أن عملية الضبط تشمل كل ما يحتمل أن يكون قد استعمل في ارتكاب الجريمة أو نتج عن ارتكابها أو ما وقعت عليه الجريمة.

1عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في الإثبات، المرجع السابق، ص 70.

2خضرة شنتير، الآليات القانونية لمكافحة الجريمة الإلكترونية، المرجع السابق، ص 105.

3 Voir l'article n° 39 du code d'instruction criminelle.

4خضرة شنتير، الآليات القانونية لمكافحة الجريمة الإلكترونية، المرجع السابق، ص 104.

5 المرجع نفسه، ص 103.

6 ينظر المواد 53 و55 والمادة 91 من ق ا ج المصري.

ولم يتخلف المشرع الجزائري عن ركب هذه التشريعات، إذ عمل على تطوير نصوصه القانونية المتعلقة بمحل التفتيش والضبط[1] حيث تبنى إجراءات خاصة بضبط وتحريز المعطيات بما يتناسب وطبيعتها اللامادية وذلك بموجب القانون 09/04، إذ اعتمد المشرع في حجز هذه المعطيات على أسلوبين مختلفين: حيث أجازت المادة 6فقرة 1من القانون 09/04حجز المعطيات الرقمية المتحصل عليها من جراء عملية التفتيش حيث يشمل الحجز وفقا لهذه المادة الأشياء المادية والمعنوية والبيانات المعالجة الكترونيا، كما أجازت نفس المادة إمكانية حجز كل المعطيات المخزنة التي تكون مفيدة في الكشف عن الجرائم أو نسخ المعطيات محل البحث فقط وكذا المعطيات اللازمة لفهمها على دعامة تخزين الكترونية تكون قابلة للحجز والوضع في أحراز وفقا لقانون ا ج، وأضاف المشرع أنه يجب على السلطات التي تقوم بالتفتيش والحجز السهر على سلامة المعطيات في المنظومة المعلوماتية التي تجري بها العملية، كما لها أن تستعمل كافة الوسائل التقنية لإعادة تشكيل هذه المعطيات وجعلها قابلة للاستغلال لأغراض التحقيق، أما عن الأسلوب الثاني الذي اعتمده المشرع في حجز هذه المعطيات طبقا للمادة 07من ق 09/04على السلطات المختصة بالتفتيش وحجز الأدلة استعمال التقنيات اللازمة لمنع الوصول إلى المعطيات والتي تحويها المنظومة المعلوماتية والتحفظ عليها خشية منه من محو أو إتلاف هذه الأدلة، [2]إذ يندرج تحت مفهوم منع الوصول إلى المعطيات كل إجراء تتخذه السلطات المعنية لمنع الاطلاع على المعطيات ذات المحتوى المجرم، وفي هذا السياق أجاز المشرع للسلطات المختصة أن تكلف أي شخص مؤهل باستعمال الوسائل التقنية المناسبة لمنع الاطلاع على هذه المعطيات.[3]

وهذا ما أكدته اتفاقية بودابست المشار إليها أنفا حيث نصت في الفقرة الثالثة من المادة19منها على ضرورة أن يلتزم الأطراف بعمل نسخ من هذه المعطيات والاحتفاظ بها وتحريزها في دعامات مؤمنه فنيا، كما دعت إلى التحفظ العاجل على هذه المعطيات وذلك لمده 60يوما للسماح للسلطات المختصة باتخاذ إجراءات التفتيش والضبط في البيئة الرقمية، [4] وهي نفس الفترة التي حددتها الاتفاقية العربية.[5]

1ناني لحسن، التحقيق في الجرائم المتصلة بتكنولوجيا المعلوماتية بين النصوص التشريعية والخصوصية التقنية، المرجع السابق، ص 120.

2أحمد مسعود مريم، آليات مكافحة جرائم تكنولوجيا الإعلام والاتصال في ضوء قانون 09/04، المرجع السابق، ص 96.

3ينظر المادة 8من القانون 09/04المشار إليه سابقا.

4حيث تنص المادة 16من اتفاقية بودابست لمكافحة الجرائم المعلوماتية، المنبثقة عن اجتماع المجلس الأوروبي ببودابست، المجر، تحت رقم 185بتاريخ 21نوفمبر 2001."يجب على كل طرف أن يتخذ الإجراءات التشريعية وأية إجراءات أخرى، يرى أنها ضرورية من أجل السماح لسلطته المختصة أن تأمر أو أن تفرض بطريقة أخرى التحفظ على المعطيات المعلوماتية المخزنة، بما في ذلك المعطيات المتعلقة بحركة السير المخزنة بواسطة نظام معلوماتي، وبالأخص عندما يكون هناك أسباب تدعو للاعتقاد بأن هذه المعطيات على معرضة للفقد أو التعديل".

5بوكر رشيدة، الحماية الجزائية للتعاملات الإلكترونية، المرجع السابق، ص 301.

ومن الملاحظ على هذه المادة أنها لم تحدد طريقة التحفظ على المعطيات وإنما تركت ذلك لكل دولة طرف في أن تحدد نماذج معينة وملائمة للتحفظ، كتجميدها مثلا أو حمايتها من أي شيء يمكن أن يؤدي إلى إتلافها أو تجردها من صفتها، وعلى ذات النهج سارت الاتفاقية العربية، حيث ألزمت في مادتها 23الدول الأطراف بتبني الإجراءات الضرورية لتمكين السلطات المختصة من إصدار الأمر أو الحصول على الحفظ العاجل للمعلومات المخزنة وخصوصا إذا كان هناك اعتقاد بأن تلك المعلومات عرضة للفقد أو التعديل.[1]

وبالرجوع للتشريع الجزائري فإنه هو الأخر قد نص صراحة في المادة 11من القانون رقم 09/04المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها سالف الذكر، على إلزام مقدمي خدمات الإنترنت بحفظ المعطيات المتعلقة بحركة السير، وذلك عن طريق حفظ المعطيات التي تسمح بالتعرف على مستعملي الخدمة، وكذا المعطيات التي تسمح بالتعرف على المرسل إليه الاتصال وعناوين المواقع المطلع عليها، ومصدر هذا الاتصال ومكانه، وكذا تاريخ ووقت ومدة كل اتصال، [2] على أن تكون مدة حفظ هذه المعطيات المذكورة سنة واحدة ابتداء من تاريخ التسجيل طبقا للفقرة الأخيرة من المادة 11سالفة الذكر.[3]

وفضلا عن هذا قد كرس المشرع الجزائري صراحة مسألة التعاون الدولي في تنفيذ الإجراءات القضائية من بينها ضبط هذه المعطيات والتحفظ عليها في حاله ما إذا كانت مخزنه في نظم معلوماتية تقع خارج الدولة وهو ما أشار إليه في المادة17 بعبارة «اتخاذ أي إجراءات تحفظيه...".[4]

1ينظر المادة 23من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المشار إليها سابقا.

2ينظر المادة 11فقرات "أ""ب""ج""د""ه"من القانون رقم 09/04المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها المشار إليه سابقا.

3ينظر الفقرة الأخيرة من المادة 11من القانون رقم09/04المشار إليه سابقا.

4تنص المادة 11من القانون رقم 09/04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها على: " مع مراعاة طبيعة و نوعية الخدمات ، يلتزم مقدمو الخدمات بحفظ :

أ ـ المعطيات التي تسمح بالتعرف على مستعملي الخدمة ،

ب ـ المعطيات المتعلقة بالتجهيزات الطرفية المستعملة للاتصال ،

د ـ المعطيات المتعلقة بالخدمات التكميلية المطلوبة أو المستعملة و مقدميها

ه ـ المعطيات التي تسمح بالتعرف على المرسل إليه أو المرسل إليهم الاتصال و كذا عناوين المواقع المطلع عليها .

بالنسبة لنشاطات الهاتف ، يقوم المتعامل بحفظ المعطيات المذكورة في فقرة " أ " من هذه المادة و كذا تلك التي تسمح بالتعرف علة مصدر الاتصال و تحديد مكانه .

تحدد مدة حفظ المعطيات المذكورة في هذه المادة بسنة واحدة ابتداءً من تاريخ التسجيل .

كما تجدر الإشارة إلى أنه لا يشترط وجوب وجود ازدواجية التجريم بين الدول للقيام بإجراءات التحفظ وهذا ما أكدته المادة29من اتفاقيه بودابست، والمادة37من الاتفاقية العربية، فعلى الدولة المطلوب منها اتخاذ إجراء التحفظ أن تلتزم بذلك مراعيه عنصر السرعة لتفادي ضياع الأدلة، [1]

المطلب الثالث: نتائج ومعوقات البحث والتحري عن الجريمة الإلكترونية

نتيجة اختلاف البيئة التي ترتكب فيها الجريمة الإلكترونية عن الجريمة التقليدية ظهر نوع جديد من الأدلة تتميز بخصائص تتوافق مع البيئة التي نشأت ووجدت فيها، وهي الأدلة الإلكترونية أو كما تسمى بالأدلة الرقمية كونها توجد في بيئة رقمية، هذا ما جعل سلطات التحري والتحقيق تواجه مجموعة من الصعوبات والعوائق عند استخلاصها لهذا الدليل، سواء في مرحلة البحث عنه أو مرحلة تقديمه كدليل إثبات أمام القضاء، ومن خلال هذا المطلب سنحاول الوقوف على تبيان الطبيعة القانونية للدليل الإلكتروني وقيمته في مجال الإثبات الجنائي، وعرض أهم الإشكالات والصعوبات التي تواجه سلطات التحري والتحقيق في استخلاص هذا الدليل والتصدي للجريمة الإلكترونية.

الفرع الأول: الدليل الإلكتروني كنتيجة لعملية البحث والتحري عن الجريمة الإلكترونية

أدى سوء استخدام التقنيات الحديثة إلى ظهور الجريمة الإلكترونية واستفحالها، ما استتبعه بروز نوع جديد من الأدلة ألا وهي الأدلة الإلكترونية أو الرقمية نتيجة البيئة الرقمية التي تنتج فيها، فقد أصبحت الأدلة التقليدية عاجزة عن إثبات هذا النوع من الجرائم الأمر الذي دعا السلطات القضائية إلى استحداث أنماط ووسائل جديدة تقنية وعلمية من أجل استخلاص الدليل الإلكتروني وإثباته أمام القضاء، باعتباره الوسيلة التي يمارس من خلالها القاضي سلطته التقديرية في إصدار الأحكام، وعليه سنتناول في هذا الفرع ماهية الدليل الإلكتروني وكذا حجيته في إثبات هذه الجرائم.

=....دون الإخلاء بالعقوبات الإدارية المترتبة على عدم احترام الالتزامات المنصوص عليها في هذه المادة ، تقوم المسؤولية الجزائية لأشخاص الطبيعيين المعنويين عندما يؤدي ذلك إلى عرقلة حسن سير التحريات القضائية ، و يعاقب الشخص الطبيعي بالحبس من ستة أشهر 6 الى خمس 5 سنوات و بغرامة من 50.000دج إلى 500.000دج

يعاقب الشخص المعنوي بالغرامة وفقًا للقواعد المقررة في قانون العقوبات تحدد كيفيات الفقرات 1و2و3 من هذه المادة ، عند الحاجة ، عن طريق التنظيم".

1بوكر رشيدة، الحماية الجزائية للتعاملات الإلكترونية، المرجع السابق، ص 409.

أولا: الطبيعة القانونية للدليل الإلكتروني

نظرا لأهمية الدليل الإلكتروني في إثبات الجرائم وجب التعرف على مفهومه وإبراز خصائصه ومختلف الأشكال التي يكون عليها وذلك فيما يلي:

1) تعريف الدليل الإلكتروني

لم يتفق الفقه الجنائي على تعريف موحد للدليل الإلكتروني، وذلك راجع إلى التطور المستمر الذي يطرأ على البيئة التقنية التي ينشأ فيها هذا الدليل، ومع ذلك قد وردت بشأنه عدة تعريفات:

فقد عرفه البعض على أنه "ذلك الدليل المشتق من أو بواسطة النظم البرمجية المعلوماتية الحاسوبية وأجهزة ومعدات الحاسوب أو شبكات الاتصالات من خلال إجراءات قانونية وفنية لتقديمها للقضاء بعد تحليلها علميا أو ترجمتها إلى نصوص مكتوبة أو رسومات أو صور أو أشكال أو أصوات لإثبات وقوع الجريمة ولتقرير البراءة أو الإدانة فيها"، [1] وما يأخذ على هذا التعريف هو حصره للأدلة الإلكترونية في تلك التي تستخرج من أجهزة الإعلام الآلي وملحقاتها دون سواها من الوسائل التكنولوجية والرقمية الأخرى، مثل الهواتف النقالة والبطاقات الذكية والتي يمكن أن تكون مصدرا للدليل الإلكتروني.[2]

كما عرفه البعض الآخر على أنه "ذلك الدليل المأخوذ من أجهزة الكمبيوتر والذي يكون في شكل مجالات أو نبضات مغناطيسية أو كهربائية ممكن تجميعها وتحليلها باستخدام برامج وتطبيقات تكنولوجية خاصة، ليتم تقديمها في شكل دليل علمي يمكن اعتماده أمام القضاء الجزائي"، [3] أوأنه "مجموعة البيانات والمعطيات المأخوذة من العالم الافتراضي التي يمكن إعدادها وتجميعها وتخزينها إلكترونيا باستخدام برامج وتطبيقات خاصة لتظهر في شكل صور أو تسجيلات صوتية أو مرئية".[4]

كما وقد نال الدليل الإلكتروني اهتماما واسعا من قبل الهيئات الدولية وخاصة المهتمة بموضوع الأدلة الإلكترونية، فعرفته المنظمة الدولية لأدلة الحاسوب (IOCE)[5] بأنه: "المعلومات ذات القيمة

1نعيم سعيداني، آليات البحث والتحري عن الجرائم المعلوماتية في القانون الجزائري، المرجع السابق، ص 121.

2جمال براهيمي، التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص 122.

3دلال ملياني مولاي، إشكالية الإثبات في جرائم الإنترنت في التشريع الجزائري، المرجع السابق، ص 104.

4جمال براهيمي، التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص 122.

5IOCE : International Organization On Computer Evidence المنظمة الدولية لأدلة الحاسوب

المحتملة والمخزنة أو المنقولة في صورة رقمية"، [1] وهو نفس التعريف المقدم من قبل الفريق العلمي العامل على موضوع الأدلة الرقمية"، [2] كما قام التقرير الأمريكي المقدم لندوة الأنتربول العلمية حول الدليل الرقمي عام 2001بتعريفه على أنه "عبارة على بيانات يمكن إعدادها وتراسلها وتخزينها رقميا، بحيث يمكن الحاسوب من تأدية مهام معينة"، [3] وتسمية هذا الدليل بالرقمي لا يعني أنه عبارة عن أرقام فقط، وإنما يقصد به الطريقة التي تسجل بها البيانات الرقمية موضوع الدليل داخل الجهاز الإلكتروني كالحاسب الآلي مثلا، والمتمثلة في الصيغة أو النظام الرقمي (0، 1)، والتي تحول فيما بعد إلى صور وأصوات وكتابات وغيرها.

وفي إطار التعريف القانوني للدليل الإلكتروني، قام المشرع المصري بتعريفه في الفقرة 20من المادة 01من القانون رقم 175لسنة 2018بشأن مكافحة جرائم تقنية المعلومات بقوله: "الدليل الرقمي: أي معلومات إلكترونية لها قوة أو قيمة ثبوتية مخزنة أو منقولة أو مستخرجة أو مأخوذة من أجهزة الحاسب أو الشبكات المعلوماتية وما في حكمها، ويمكن تجميعها وتحليلها باستخدام أجهزة أو برامج أو تطبيقات تكنولوجية خاصة".[4]

وانطلاقا من هذه التعريفات يمكن القول بأن الدليل الإلكتروني هو عبارة عن معلومات مخزنة في نظم المعالجة الآلية وملحقاتها أو متنقلة عبرها بواسطة شبكة الاتصالات في شكل مجالات إلكترونية أو ذبذبات كهربائية أو نبضات مغناطيسية، والتي يستوي أن تكون داخل الحاسب الآلي أو أي وسيلة أو آلة إلكترونية أخرى، بحيث يتم استخلاص هذه الذبذبات وجمعها وتحليلها وترجمتها لتظهر في شكل مخرجات يقبلها العقل والمنطق ويعتمدها العلم، ليتم استخدامها في إثبات الجريمة الإلكترونية ونسبتها لمرتكبها.

2) خصائص الدليل الإلكتروني

يتميز الدليل الجنائي الإلكتروني بجملة من الخصائص العلمية والمواصفات القانونية التي تميزه عن الدليل الجنائي التقليدي، وهذا راجع للطبيعة التقنية والبيئة الافتراضية التي يتواجد فيها، وبما أن هذا

1زياد بن محمد عادل العتيبي، دراسة استطلاعية حول حجية الأدلة الرقمية في إثبات الجرائم المعلوماتية، المجلة الإلكترونية الشاملة متعددة التخصصات، العدد التاسع والعشرون، أكتوبر 2020، ص 11.

2حسين ربيعي، آليات البحث والتحقيق في الجرائم المعلوماتية، المرجع السابق، ص 262.

3نعيم سعيداني، آليات البحث والتحري عن الجرائم المعلوماتية في القانون الجزائري، المرجع السابق، ص 121,

4ينظر المادة 01فقرة 20من القانون رقم 175لسنة 2018بشأن مكافحة جرائم تقنية المعلومات المصري المشار إليه سابقا.

النوع من الجرائم يمتاز بالتطور والسرعة في الانتشار فبالضرورة أن يتميز الدليل الناتج عنها بعدة خصائص والتي لا يمكن حصرها، وعليه سوف نعرض أهمها وذلك على النحو التالي:

أ. **الدليل الالكتروني دليل علمي**

ومفاد هذه الخاصية أن الحصول على الدليل الإلكتروني يتم باستخدام الأساليب والطرق العلمية المختلفة، هذا من جهة، كما أن التعامل مع هذا النوع من الأدلة يستلزم توافر المعرفة العلمية والتقنية لدى المتعامل معه سواء كان محقق أو خبير أو قاضي مثلا، [1] فالدليل الرقمي يحتاج إلى بيئته التقنية التي تكون فيها والتي تحتوي مجموعة من البيانات والمعلومات ذات الهيئة الإلكترونية غير الملموسة لا تدرك بالحواس العادية، بل يتطلب إدراكها الاستعانة بأجهزة و معدات تقنية، وإلى استخدام نظم برمجية حاسوبية، ومن هذا المنطلق يقال أن الدليل الإلكتروني يتميز بذات الطبيعة التي يتميز بها الدليل العلمي من حيث أن الدليل العلمي يسعى للوصول إلى الحقيقة وبالتالي يستبعد تعارضه مع القواعد العلمية السليمة، فإن الدليل الالكتروني لا يجب أن يخرج عما توصل إليه العلم الرقمي و إلا فقد معناه.[2]

ب. **الدليل الالكتروني دليل تقني :**

يعتبر الدليل الإلكتروني ذو طابع تقني كونه مستوحى من البيئة التي يعيش فيها وهي البيئة الرقمية أو التقنية، المتمثلة في العالم الرقمي الافتراضي الكامن في مختلف الأجهزة الإلكترونية من وسائل اتصال كالحاسب الآلي والخوادم والشبكات بمختلف أنواعها، [3] فلا يتصور وجود الدليل الإلكتروني خارج بيئته الرقمية التقنية، هذه البيئة التي تنتج نبضات ومجالات مغناطيسية والتي تترجم من طبيعتها الرقمية إلى الطبيعة المادية التي يمكن الاستدلال بها على معلومة معينة، [4] إذ أن هذه الطبيعة الرقمية تتمثل في تعداد من الأرقام التي تكون على هيئة واحدة موحدة في الصفر والواحد، [5] وعلى الرغم من وحدة هذا الرقم الثنائي إلا أنها لا تتشابه فيما بينها، فكل نظام ثنائي يعبر عن مستند أو رسالة معينة، كما يمتاز الدليل

1زياد بن محمد عادل العتيبي، دراسة استطلاعية حول حجية الأدلة الرقمية في إثبات الجرائم المعلوماتية، المرجع السابق، ص 15.

2عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في الإثبات الجنائي، المرجع السابق، ص 34.

3ليندا بن طالب، الدليل الإلكتروني ودوره في الإثبات، المرجع السابق، ص 42.

4رفاه خضير جياد العارضي، الدليل الإلكتروني وأثره في مجال نظرية الإثبات الجنائي، المرجع السابق، ص 76.

5خالد حسن أحمد لطفي، الدليل الرقمي ودوره في إثبات الجريمة المعلوماتية، المرجع السابق، ص 140.

الالكتروني بالسعة التخزينية العالية له، حيث يمكن لمختلف الأجهزة الرقمية تخزين الآلاف من المعلومات والبيانات، كآلة الفيديو الرقمية مثلا يمكنها تخزين مئات الصور.[1]

ت. الدليل الالكتروني يصعب التخلص منه :

وتعد هذه الخاصية من أهم خصائص الدليل الإلكتروني وميزة تميزه عن غيره من الأدلة التقليدية، إذ أن هاته الأخيرة يمكن التخلص منها بكل سهولة كالأوراق مثلا والأشرطة المسجلة إذا حملت في ذاتها إقرار بارتكاب شخص لجرائم معينة، وذلك إما بتمزيقها أو حرقها أو إتلافها، كما يمكن أيضا التخلص من بصمات الأصابع مثلا بمسحها، أو حتى التخلص من الشهود بقتلهم أو تهديدهم بعدم الإدلاء بالشهادة في بعض الدول الغربية، [2] أما بالنسبة للأدلة الإلكترونية فلا يمكن التخلص منها بهذه السهولة لأنه يسهل استرجاعها بعد محوها، وإصلاحها بعد إتلافها، وإظهارها بعد إخفائها، وذلك عن طريق بعض البرامج الحاسوبية والبرمجيات والتطبيقات التي تساعد في استعادة البيانات التي تم حذفها أو إلغاءها مثل برنامج" Recoverlost Data، Rescue Box"سواء تم الإلغاء بالأمر(Delete) أو عن طريق إعادة تهيئة القرص الصلب باستخدام الأمر (Format) وسواء كانت هذه البيانات صورا أو رسومات أو كتابات أو غيرها.[3]

ث. الدليل الالكتروني القابل للنسخ:

وتعني هذه الخاصية إمكانية استخراج نسخ من الأدلة الجنائية الرقمية مطابقة للأصل ولها نفس القيمة العلمية، وهذا ما لا يتوافر في أنواع الأدلة الأخرى (التقليدية)، مما يشكل ضمانة فعالة للحفاظ على الدليل ضد الفقد والتلف أو التغيير والتزييف، [4] كما توفر هذه الميزة إمكانية تحديد ما إذا تم العبث بالدليل الإلكتروني عن طريق مقارنته بالأصل باستخدام برامج وتطبيقات معينة، [5] وهذا الأمر لاحظه المشرع البلجيكي فقام بتعديل قانون التحقيق الجنائي (Code d'instruction Criminelle) بمقتضى القانون المؤرخ في (28نوفمبر2000)حيث تم إضافة المادة (39 bis) التي تسمح بضبط الأدلة الرقمية،

1عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في الإثبات، المرجع السابق، ص 36.

2بوكر رشيدة، الحماية الجزائية للتعاملات الإلكترونية، المرجع السابق، ص 402.

3عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في الإثبات الجنائي، المرجع السابق، ص 35 -36.

4بوكر رشيدة، جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري والمقارن، المرجع السابق، ص 388.

5ليندا بن طالب، الدليل الإلكتروني ودوره في الإثبات، المرجع السابق، ص 43.

مثل نسخ المواد المخزنة في نظم المعالجة الآلية للبيانات بقصد عرضها على الجهات القضائية، [1] بالإضافة إلى ذلك يمتاز الدليل الإلكتروني بقابليته للتطور والتنوع وذلك لارتباطه بالطبيعة التقنية والعلمية المتطورة والمتجددة باستمرار والتي تتمتع بها التكنولوجيا، كما أن نشاط الجاني داخل العالم الرقمي يعتبر دليل يتم تسجيله في الكمبيوتر أو أي جهاز إلكتروني آخر ليستعمل لاحقا كدليل إثبات ضده.[2]

واستخلاصا لما سبق يمكن القول بأن تمتع الدليل الإلكتروني بهذه الخصائص جعل منه دليلا متميزا عن باقي الأدلة الأخرى من حيث التعامل معه ومن حيث حجيته في إثبات الجرائم الإلكترونية بمختلف أنواعها، وهذا ما شكل تحديا حقيقيا أمام السلطات القضائية في عملية التحري والتحقيق في هذه الجرائم، سنتطرق لهذه التحديات والمعيقات في النقاط الموالية.

3) أشكال الدليل الإلكتروني:

نظرا لطبيعة الدليل الإلكتروني والبيئة التقنية التي ينتمي إليها فإنه في تطور دائم ومستمر، هذا ما جعله يعرف عدة تقسيمات فقهية وأخرى تشريعية وقضائية، سنوضحها فيما يلي:

أ. المحاولات الفقهية لتقسيم الدليل الإلكتروني:

ظهرت عدة محاولات فقهية قسمت الدليل الإلكتروني إلى ثلاثة أقسام كما يلي:

- أدلة إلكترونية خاصة بأجهزة الحاسب الآلي وملحقاته، وتشمل جهاز الكمبيوتر وكذا الطابعة والمودم والأقراص المدمجة، وذاكرة الفلاش، والأشرطة الممغنطة...الخ.
- أدلة إلكترونية خاصة بالشبكة العالمية للمعلومات ومختلف نهاياتها الطرفية.
- أدلة إلكترونية خاصة ببروتوكولات تبادل المعلومات بين أجهزة الشبكة العالمية للمعلومات (TCP/IP).[3]

يلاحظ من هذا التقسيم أنه ميز بين شبكات الكمبيوتر والإنترنت وكذا بروتوكولات تبادل المعلومات والتي هي في الأصل واحدة، فاختلاف المصطلحات هنا لا يعني اختلاف المعنى، ولهذا تعرض هذا التقسيم إلى النقد كون أنه لا يستوعب ما قد تفرزه التكنولوجيات الحديثة من وسائل اتصال جديدة مستقبلا.[1]

1عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في الإثبات الجنائي، المرجع السابق، ص 36.

2جمال براهيمي، التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص 126.

3منيرة عبيزة، الدليل الإلكتروني والسلطة التقديرية للقاضي، مجلة العلوم القانونية والسياسية، المجلد 09، العدد 03، ديسمبر 2018، ص 564.

كما قسم بعض الفقهاء الدليل الإلكتروني حسب هيئته إلى:

- **الصور الرقمية:** وهي عبارة عن تجسيد للحقائق المرئية حول الجريمة، إذ تعتبر الصورة الرقمية أكثر تطورا من الصورة التقليدية كونها تتميز بنوع من الدقة والوضوح نتيجة استخدام أجهزة متطورة في التقاطها، [2] وهي عادة ما تقدم في شكل ورقي أو رقمي مرئي باستخدام الشاشة المرئية، أو في شكل تسجيلات فيديو أو أفلام مصورة.[3]

- **التسجيلات الصوتية:** وتشمل مختلف التسجيلات الصوتية التي يتم ضبطها وتخزينها عن طريق الوسائل الخاصة بذلك، مثل المحادثات الصوتية التي تتم عبر الهاتف أو غرف الدردشة أو عبر مواقع التواصل الاجتماعي بصفة عامة.[4]

- **النصوص المكتوبة:** وتشمل كل النصوص التي يتم كتابتها بواسطة الآلة الرقمية من طرف المستخدم، والتي يتم إدخالها من طرفه مثل الرسائل المرسلة عبر البريد الإلكتروني أو الهاتف النقال، أو الناتجة عن معالجة البيانات في وحدة المعالجة المركزية والتي نجدها في مختلف وسائل التخزين الإلكترونية كالأقراص الصلبة والمرنة مثلا، والتي يمكن إخراجها في شكل ورقي باستخدام الطابعات.[5]

ب. المحاولات التشريعية والقضائية لتقسيم الدليل الإلكتروني:

تعد الولايات المتحدة الأمريكية أحسن نموذج فيما يتعلق بالتصدي للجرائم الإلكترونية، إذ تعتبر من أولى الدول التي سنت قوانين لمكافحة هذا النوع من الإجرام، وقد قامت وزارة العدل الأمريكية سنة 2002بتقسيم الأدلة الناتجة عن هذه الجرائم إلى ثلاثة (03) أصناف كالآتي:

- السجلات التي تم إنشائها بواسطة الحاسوب وبالتالي لم يلمسها الإنسان مثل (Log files) وسجلات الهاتف والفواتير بمختلف أنواعها.[6]

- السجلات التي تم حفظ جزء منها بالإدخال والجزء الآخر تم إنشائه بواسطة الحاسوب، أي البيانات التي يتم إدخالها للحاسوب وتتم معالجتها من خلال برامج خاصة، كإجراء العمليات الحسابية مثلا، أو البيانات التي تعالج عن طريق برامج (Excel) وغيرها.[1]

1عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في الإثبات الجنائي، المرجع السابق، ص 42.

2خالد حسن أحمد لطفي، الدليل الرقمي ودوره في إثبات الجريمة المعلوماتية، المرجع السابق، ص 141.

3براهيمي جمال، التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص 129.

4المرجع نفسه، ص 129.

5المرجع نفسه، ص 128.

6عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في الإثبات الجنائي، المرجع السابق، ص 43.

وما يقال حول هذا النوع من الأدلة الإلكترونية أنها أعدت مسبقا لتكون وسيلة إثبات لبعض الوقائع والجرائم والمخالفات التي تقع عبر أجهزة الحاسوب والإنترنت، حيث يتم حفظها عمدا من أجل الاحتجاج بها لاحقا في حالة وقوع أي مخالفة، وهذا ما يقلل إمكانية فقدانها ويجعل من السهل الوصول إليها.[2]

بالإضافة لهذه الأدلة أضافت وزارة العدل والقضاء الأمريكي صنف ثالث للأدلة الإلكترونية ويشمل السجلات المحفوظة في الحاسوب أي الوثائق المكتوبة والمحفوظة مثل ملفات البريد الإلكتروني التي تحمل مختلف الرسائل المرسلة والمستقبلة وكذا المحذوفة، وملفات برامج معالجة الكلمات، وكذا رسائل غرف المحادثة عبر الإنترنت، إذ ينشئ هذا النوع من الأدلة دون إرادة الشخص عكس النوع الأول، فيترك بذلك أثرا للجاني أو ما يسمى بالبصمة الرقمية أي مختلف الآثار المعلوماتية التي يخلفها الجاني بعد استخدامه لهذه الوسائل وزيارته للمواقع الإلكترونية، وكافة الاتصالات التي قام بإجرائها، [3] إذ لم يعد هذا النوع من الأدلة للحفظ والإثبات أساسا وإنما يحفظ عن طريق بعض الوسائل الفنية المساعدة على ضبطه كبرامج التتبع والاسترداد وغيرها، وهذا ما يجعله يختلف عن النوع الأول في كونه لم يعد أصلا ليكون وسيلة إثبات وبالتالي له من الأهمية والقوة الاستدلالية أكثر من الأول، لأنه غالبا ما يتضمن معلومات ذات مصداقية وتفيد في كشف ملابسات الجريمة وهذا ما يجعله عرضة للفقدان.[4]

4) مصادر الحصول على الدليل الالكتروني :

تعددت مصادر الحصول على الدليل الالكتروني بتعدد الأجهزة الإلكترونية ومكوناتها، التي يتم فحصها واستخلاص الدليل منها، بما أن التطور العلمي والتقني لا يزال يسفر عن أنواع جديدة من الأدلة الرقمية نتطرق لأهم هذه المصادر على سبيل المثال لا الحصر، وذلك كما يلي:

أ. فحص مكونات الجهاز الإلكتروني الخاص بالمشتبه به أو المجني عليه:

كما هو معلوم أن محل أو وسيلة ارتكاب الجريمة الإلكترونية لا يقتصر على جهاز الحاسوب أو الكمبيوتر فقط وإنما قد تتم هذه الأخيرة عن طريق الهاتف أو اللوحات الإلكترونية وأجهزة التصوير الرقمية أو أي جهاز إلكتروني آخر، لهذا فإن محل التفتيش والضبط قد ينصب على المكونات المادية أو

1بهنوس آمال، الدليل الرقمي في الإجراءات الجنائية، المجلة الأكاديمية للبحث القانوني، المجلد 16، العدد 02، سنة 2017، ص 178.

2خالد حسن أحمد لطفي، الدليل الرقمي ودوره في إثبات الجريمة المعلوماتية، المرجع السابق، ص 144.

3المرجع نفسه، ص 144.

4براهيمي جمال، التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص 131.

المعنوية لهذه الأجهزة، فجهاز الكمبيوتر مثلا يتكون من قطع صلبة (Hardware) وبرمجيات (Software)، مثل الأقراص الصلبة والمرنة وغيرها، إذ يتم فحص محتويات القرص الصلب من بيانات مخزنة سواء كانت مكتوبة أو في شكل صور وأصوات، واسترجاع ما حذف منها عن طريق الاستعانة بمجموعة من البرامج والتطبيقات كما أشرنا سابقا، [1] كما يتم فحص الوحدات الفرعية الأخرى كالقرص المرن و أقراص الليزر أو أي وحدة تخزين أخرى من الممكن استعمالها مثل جهاز الفلاش (Flash memory)، [2] كما يمكن أيضا الحصول على الدليل الإلكتروني من مخرجات الطابعة ولوحة المفاتيح أو المودم وغيرها من الملحقات، أما عن فحص الهاتف النقال فيتم عن طريق فحص النظام المادي للهاتف أولا والذي يتمثل في فحص الكاميرا والشاشة والبطارية، والسماعة، وبطاقة الذاكرة، والشريحة وغيرها، كونها وسائل تمثل مصدر للدليل الذي قد يثبت أو ينفي واقعة إجرامية معينة، كما تتم هذه العملية عن طريق فحص النظام المعلوماتي للهاتف عن طريق استرداد المعلومات التي يحتويها والقيام بضبطها بالاستعانة بعدة وسائل كوسائل التشفير وإخفاء المعلومات ...الخ.[3]

كما يعتبر أيضا جهاز المجني عليه مصدرا مهما لاستخلاص الدليل الإلكتروني حيث يكشف ما قام به المشتبه فيه من جرائم، وقد يكون المجني عليه إما شخصا طبيعيا أو مؤسسة خاصة أو عامة أو هيئة حكومية و غيرها، وبالتالي فإن فحص مثل هذه الأجهزة يمكن المحقق من معرفة آثار ما تم على هذه الأجهزة من عمليات و تتبع مصدر المشتبه فيه .[4]

ومثال ذلك مقدمي خدمات الإنترنيت كشركة(Yahoo) أو جوجل (Google)أو (msn)وغيرهم، فإن مثل هذه الشركات تقوم بتسجيل البيانات الخاصة بمستخدميها هذا ما يساعد على التعرف على هوية المشتبه فيهم، وكذا البريد الالكتروني لهم، إذ عن طريق البريد الالكتروني يمكن التعرف على البيانات الشخصية لهم ومنه تحديد هويتهم وكذا تحديد مكان تواجدهم و مواقعهم.[5]

1حسام محمد نبيل الشنراقي، الجرائم المعلوماتية، دراسة تطبيقية مقارنة على جرائم الاعتداء على التوقيع الإلكتروني، المرجع السابق، ص 509.

2ممدوح خالد براهيم، الإثبات الإلكتروني في المواد الجنائية والمدنية، المرجع السابق، ص 59.

3التوجي محمد، الحماية الجنائية من الجرائم المرتكبة بواسطة الهاتف النقال، المرجع السابق، ص 199.

4 المرجع نفسه، ص 59.

5ممدوح خالد براهيم، الإثبات الإلكتروني في المواد الجنائية والمدنية، المرجع السابق، ص 58.

ب. فحص أنظمة الاتصال بالإنترنت:

يستهدف فحص أنظمة الاتصال بالإنترنت التوصل إلى معرفة الجهاز الذي قام الجاني باستخدامه في ارتكاب جريمته، وذلك عن طريق تتبع مسار الإنترنت كونه يعبر عن الحركة التراسلية للنشاط الممارس من خلال الإنترنت، فسواء تمثل هذا الجهاز في الحاسب الآلي أو الهاتف النقال أو غيره فبمجرد أن يتعرف على المسار يقوم تلقائيا باختيار البروتوكول التراسلي الذي يقوم من خلاله باستدعاء البيانات، هذا البروتوكول الذي يساعد في تتبع مسار الإنترنت عن طريق نظام الفحص الإلكتروني أو ما يسمى بـ: "علم البصمات المعاصر"، [1] إلا أنه قد اختلف الفقه بشأن هذه المسألة حيث انقسم إلى اتجاهين، يرى البعض منه بعدم إمكانية تحديد مسار الإنترنت إذ يستند هذا الرأي إلى الطبيعة المرنة للإنترنت، وأن ما يتم الوصول إليه من أدلة رقمية لا تكفي لوحدها لإثبات الجريمة الواقعة وإنما تحتاج لأدلة أخرى تؤيدها، فمثلا التوصل إلى عنوان البروتوكول الخاص بالجهاز (IP) لا يمكن الأخذ به كدليل تام ونسبته إلى مالك الجهاز أو عنوان الاسم المذكور، إذ قد يكون هذا الجهاز مسروقا أو مؤجرا أو مستعملا من طرف الغير، هذا ما يجعل إثبات هذه الجرائم من الصعوبة بمكان، في حين ذهب الرأي الثاني إلى إمكانية تتبع حركة أو مسار الإنترنت وبالتالي التوصل إلى مرتكب الجريمة، [2] وهذا ما أكدته محكمة باريس في بعض أحكامها، ومثال ذلك قضية الموقع ياهو (Yahoo). [3]

وتأسيسا على ما سبق ذكره يمكن القول أن وجود الأدلة الإلكترونية في مثل هذه الأجهزة والملحقات سواء تمثلت في أجهزة الكمبيوتر وملحقاتها أو أجهزة رقمية أخرى، فإن الحصول عليها يتطلب جملة من الوسائل والأدوات المساعدة التي تساهم في جمعها مثل برنامج معالجة الملفات مثل(X tree Pro Gold)، برنامج النسخ مثل (Lap Link)، و برنامج كشف الديسك مثل (AMA Disk , Viewdisk)، وغيرها. [4]

1التوجي محمد، الحماية الجنائية من الجرائم المرتكبة بواسطة الهاتف النقال، المرجع السابق، ص 197.

2حسام محمد نبيل الشنراقي، الجرائم المعلوماتية، دراسة تطبيقية مقارنة على جرائم الاعتداء على التوقيع الإلكتروني، المرجع السابق، ص 515.

3التوجي محمد، الحماية الجنائية من الجرائم المرتكبة بواسطة الهاتف النقال، المرجع السابق، ص 198.

4 ومن بين أشهر هذه البرامج نجد: برنامج معالجة الملفات مثل X tree Pro Goldوهو برنامج يمكن المحقق من العثور على الملفات في أي مكان على الشبكة حيث يستخدم مثلا لتقييم محتويات القرص الصلب الخاص بالمتهم أو الأقراص المرنة المضبوطة أو يستخدم لقراءة البرامج في صورتها الأصلية، كما يمكن من البحث عن كلمات معينة أو عن أسماء ملفات أو غيرها .

برنامج النسخ مثل Lap Linkوهو برنامج يسمح بنسخ البيانات من الكمبيوتر الخاص بالمتهم و نقلها من قرص إلى قرص آخر، وبهذا يفيد في الحصول على نسخة من المعلومات قبل أي محاولة لتدميرها من قبل الجاني.

برنامج كشف الديسك مثل AMA Disk، Viewdiskويمكن من خلال هذه البرنامج الحصول على محتويات القرص المرن، مهما كانت أساليب تهيئة القرص، وهذا البرنامج له نسختان نسخة عادية خاصة بالأفراد ونسخة خاصة بالشرطة.

ثانيا: حجية الدليل الإلكتروني في الإثبات الجنائي

تعد عملية تقدير الأدلة جوهر مرحلة الحكم والمرحلة الحاسمة في الدعوى الجزائية، حيث يمارس القاضي سلطته التقديرية على الأدلة محل الواقعة، وباعتبار الدليل الإلكتروني ذو طبيعة مميزة فإن مسألة الأخذ به في إثبات الوقائع الجنائية تثير العديد من الإشكالات أمام القاضي، فمجرد الحصول على الدليل وتقديمه للقضاء لا يكفي لاعتماده كدليل إدانة، وإنما ينبغي تقديره وفحصه لمعرفة قيمته في إثبات الواقعة الإجرامية، ومسألة تقييم الدليل وتحديد قابليته للإثبات تتعلق بالقاضي الذي له السلطة التقديرية في تقديره عملا بمبدأ حرية القاضي في تكوين قناعته، ولذلك اشترط القانون توافر عدة شروط في الدليل الإلكتروني حتى يمكن الأخذ به في الإثبات الجنائي، حيث تختلف هذه الشروط حسب النظام القانوني السائد في الدول هذا ما سنبينه في النقاط الموالية.

1) شروط قبول القاضي الجزائي للدليل الإلكتروني في الإثبات الجنائي:

وتتمثل هذه الشروط فيما يلي:

أ. مشروعية الدليل الإلكتروني:

تعرف المشروعية بأنها "التوافق والتقيد بأحكام القانون في إطاره ومضمونه العام"، [1] حيث تهدف المشروعية لتقرير الضمانات الأساسية للأفراد وحماية حقوقهم وحرياتهم الشخصية ضد تعسف السلطة القضائية، إذ يعد هذا المبدأ الأساس الذي يقوم عليه القانون الجنائي بشقيه الموضوعي والإجرائي، فلا ريب أن مبدأ شرعية الجرائم والعقوبات الذي يستقيم عليه بنيان القانون الجنائي الموضوعي ينعكس على قواعد الإثبات الجنائي، [2] وذلك معناه عدم قبول أي دليل جنائي إلا إذا كان

برنامج إذن التفتيش Computer Scorch Warrant Programهو برنامج يسمح بإدخال كل المعلومات الهامة المطلوبة لترقيم الأدلة و تسجيل البيانات منها ويمكن لهذا البرنامج أن يصدر إيصالات باستلام الأدلة و البحث في قوائم الأدلة المضبوطة لتحديد مكان دليل معين أو تحديد ظروف ضبط هذا الدليل.

قرص بدء تشغيل الكمبيوتر bootable Diskettهو قرص يمكن المحقق من تشغيل الكمبيوتر إذا كان نظام التشغيل فيه محميا بكلمة مرور معينة.

=...برامج اتصالات مثل LANtasticهو برنامج يستطيع ربط جهاز حاسب المحقق بجهاز حاسب المتهم لنقل ما به من معلومات وحفظها في جهاز نسخ المعلومات ومن ثم إلى القرص الصلب. لمزيد من التفاصيل حول هذه البرامج ينظر ممدوح خالد براهيم، الإثبات الإلكتروني في المواد الجنائية والمدنية، المرجع السابق، ص 58- 59.

1رفاه خضير جياد العارضي، الدليل الإلكتروني وأثره في مجال نظرية الإثبات الجنائي، المرجع السابق، ص 90.

2خالد حسن أحمد لطفي، الدليل الرقمي ودوره في إثبات الجريمة المعلوماتية، المرجع السابق، ص 191.

مشروعا في وجوده وفي طريقة الحصول عليه أو استخلاصه، وعليه سنبين مدى مقبولة الدليل الإلكتروني في الإثبات الجنائي أولا ثم مدى مشروعية أساليب الحصول عليه، في النقاط التالية:

1. **مشروعية وجود وقبول الدليل الالكتروني:**

ويقصد بمشروعية وجود الدليل الإلكتروني أن يكون الدليل معترف به في إثبات الوقائع الإجرامية، ومعنى ذلك أن يكون من ضمن الأدلة التي يجيز القانون للقاضي الاستناد إليها في حكمه، ونظرا للطبيعة المميزة للدليل الالكتروني فقد تباينت مواقف النظم القانونية المختلفة حول مسألة قبول هذا النوع من الأدلة في إثبات الجرائم بصفة عامة والجرائم الالكترونية بصفة خاصة، وعليه سوف نبين موقف هذه النظم ومدى قبولها هذا النوع من الأدلة وذلك من خلال النقاط التالية:

- **قبول الدليل الالكتروني في ظل نظام حرية الإثبات الجنائي:**

ويقصد بمبدأ حرية الإثبات الجنائي أن يكون لجميع أطراف الدعوى الحرية في اللجوء إلى كافة وسائل الإثبات للتدليل على صحة ما يدعونه، [1] فلا يرسم القانون في ظل هذا النظام _ والذي يسمى أيضا بنظام الإثبات المعنوي_ طرقا محددة للإثبات يتقيد بها القاضي الجزائي بل يتمتع القاضي بمطلق الحرية في رفض الدليل أو قبوله إذا ما اطمئن إليه فالمشرع في هذه الحالة لا يتدخل في تحديد القيمة الاقناعية للأدلة، وبالتالي يحكم القاضي وفقا لاقتناعه الشخصي وبهذا يتمتع القاضي في مثل هذا النظام بدور ايجابي في مجال الإثبات.[2]

وفي ظل هذا النظام الذي تأخذ به أغلب التشريعات أو القوانين اللاتينية نجد أنها تتناول مسألة قبول الأدلة الإلكترونية كل حسب نظامها وسياستها التشريعية الداخلية، ففي فرنسا قد أقر المشرع الفرنسي هذا المبدأ (حرية الإثبات) بموجب المادة 427من قانون الإجراءات بقولها: "ما لم يرد نص مخالف يجوز إثبات الجرائم بجميع طرق الإثبات ويحكم القاضي بناء على اقتناعه الشخصي"، وهذا النص وإن كان مخصصا لمحاكم الجنح إلا أن مبدأ حرية الإثبات يطبق أمام جميع المحاكم إلا إذا نص القانون على خلاف ذلك، [3] وتأييدا لهذا فرضت محكمة النقض الفرنسية على محاكم الموضوع تطبيق هذا المبدأ حيث تفرض حرية الإثبات بالنسبة لقضاة الموضوع إذ شددت في العديد من أحكامها على حرية القضاة في الاستعانة بأي دليل يكون لازما لتكوين عقيدتهم، كما ذهبت الدائرة الجنائية لمحكمة النقض الفرنسية

1عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في الإثبات الجنائي، المرجع السابق، ص 118.

2أشرف عبد القادر قنديل، الوسائل الإلكترونية ودورها في الاثبات، المرجع السابق، ص 121.

3عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في الإثبات الجنائي، المرجع السابق، ص 118.

لأبعد من ذلك في احترام مبدأ حرية الإثبات فهي ترى أنه طالما لا يوجد نص قانوني يستبعد صراحة نوعا معينا من الأدلة فلا يجوز للمحكمة استبعاده ولو كان غير مشروع ، وإنما تشترط أن يكون هذا الدليل قد خضع للمناقشة الحضورية في الجلسة مع احترام جميع الحقوق والحريات اللازمة.[1]

وقد أثارت مسألة قبول الأدلة المستمدة أو الناتجة عن الآلة أو الأدلة العلمية جدلا حول قبولها في مجال الإثبات الجنائي، والواقع يثبت أن القضاء الفرنسي يقبل هذه الأدلة كأشرطة التسجيل وأجهزة التصنت والأجهزة السينمائية وغيرها في حالة ما إذا استوفت شروطا معينة، كأن يتم الحصول عليها بطريقة مشروعة وأن يتم مناقشتها حضوريا من قبل أطراف الدعوى، وبالتالي يمكن القول بأن المشرع الفرنسي قد اعتمد وأقر بمسألة قبول الدليل الالكتروني في الإثبات الجنائي.[2]

أما عن المشرع الجزائري فقد أقر هذا المبدأ في المادة 212من قانون الإجراءات التي نصت على: "يجوز إثبات الجرائم بأي طريق من طرق الإثبات ما عدا الأحوال التي ينص فيها القانون على غير ذلك، وللقاضي أن يصدر حكمه تبعا لاقتناعه الشخصي"،[3] أما بخصوص قبول المشرع الجزائري للدليل الالكتروني في الإثبات فلم يكتفي بالنصوص التي تعتد بأدلة الإثبات الالكتروني في المعاملات المدنية والتجارية كالإثبات بالكتابة في الشكل الالكتروني أو التوقيع والتصديق الالكترونيين،[4] بل أقر جمله من الإجراءات الخاصة التي نظم من خلالها طرق الحصول على الدليل الالكتروني وذلك في القانون الخاص رقم 04/09 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، والذي يستفاد من نصوصه أن المشرع الجزائري يقبل صراحة الأخذ بالدليل الالكتروني في إثبات الوقائع الإجرامية وهذا بموجب المادة 04من هذا القانون والتي نظمت مسألة مراقبة الاتصالات الالكترونية، وكذا المادتين 05و06منه والتي نظمت مسألة تفتيش وحجز المعطيات المعلوماتية، ومن هذا نستنتج أن هناك اعترافا صريحا من المشرع الجزائري بحجية الأدلة الالكترونية في الإثبات الجنائي.[5]

ونفس الشيء كرسه المشرع المصري من خلال المادة 291من قانون الإجراءات حيث تنص على: "للمحكمة أن تأمر ولو من تلقاء نفسها أثناء نظر الدعوى بتقديم أي دليل تراه لازما لظهور الحقيقة"، وهذا ما أكدته محكمو النقض المصرية في العديد من أحكامها بقولها أن القانون في ما عاد ما استلزم من

1Cass ; Crim 15 Avri 1993, B n° 210, Cass ; Crim 6 Avril 1993, J.C.P, édition générale, n° 43, note Mme Rassat, p 415.

2بوكر رشيدة، الحماية الجزائية للتعاملات الإلكترونية، المرجع السابق، ص 428.

3ينظر المادة 212من ق ا ج ج.

4تنص المادة 323مكرر 1من ق 05/10 القانون المدني ج على: " يعتبر الإثبات بالكتابة في الشكل الإلكتروني كالإثبات بالكتابة على الورق بشرط إمكانية التأكد من هوية الشخص الذي أصدرها و أن تكون معدة و محفوظة في ظروف تضمن سلامتها".

5ينظر القانون رقم 09/04المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

وسائل خاصة للإثبات فتح بابه أمام القاضي الجنائي على مصراعيه ليختار من كل طرقه ما يراه موصلا إلى الكشف عن الحقيقة، وأن الأصل أن الجرائم بكافة أنواعها إلا ما استثني منها بنص خاص جاز إثباتها بكافه الطرق القانونية،[1] كما نجد أن المشرع المصري قد نص بصريح العبارة على حجية الأدلة الإلكترونية والاعتداد بها في الإثبات الجنائي، وذلك في نص المادة 14من قانون التوقيع رقم 15لسنة 2004والذي يقبل التوقيع الالكتروني في إثبات المواد المدنية والتجارية، كما نصت المادة 15من ذات القانون على المساواة في الحجية بين الكتابة والمحرر الالكتروني وكذا الصورة المنسوخة على الورق، وهذا ما يستشف منه قبول وإقرار المشرع المصري بحجية الدليل الالكتروني في إثبات المعاملات المدنية والتجارية،[2] أما بخصوص إثبات الوقائع الجنائية فقد جاءت المادة 11من القانون رقم 175لسنة2018المتعلق بمكافحة جرائم تقنية المعلومات لتأكد أن للأدلة المستمدة أو المستخرجة من الأجهزة الالكترونية والأنظمة والبرامج المعلوماتية نفس قيمه وحجية الأدلة الجنائية المادية متى ما توافرت فيها الشروط الفنية الواردة باللائحة التنفيذية لهذا القانون.[3]

وتطبيقا لما سبق ذكره فإن إعمال مبدأ حرية الإثبات يجعل من دور القاضي الجنائي دور ايجابي في كشف الحقيقة سواء في الجرائم التقليدية أو حتى المستحدثة كالجرائم الالكترونية وذلك سواء في مسألة توفير الدليل أو حتى في مسألة تقدير الدليل الجنائي بصفة عامة.

- **الدورالايجابي للقاضي الجنائي في توفير الدليل الالكتروني:**

ويقصد بالدور الايجابي للقاضي في توفير الدليل الالكتروني عدم التزامه بما يقدمه له أطراف الدعوى من أدلة، وإنما له سلطة واسعة في اتخاذ جميع الإجراءات للكشف عن الحقيقة وذلك عن طريق البحث والتنقيب عنها، وبالتالي ليس له أن يقتنع بما يقدمه إليه أطراف الدعوى والاكتفاء بتلك الأدلة وإنما عليه البحث بنفسه عما يعتقد أنه يفيد في إظهار الحقيقة،[4] فدور القاضي الجزائي هنا ليس دورا سلبيا كدور القاضي المدني والذي يقتصر على الموازنة بين الأدلة، وتطبيقا لهذا الدور الايجابي نجد أن المحاكم الفرنسية في مواد الجنح والمخالفات يمكنها أن تتخذ جميع الإجراءات التي تراها لازمه لتكوين قناعتها، فلها أن تسأل أو تستجوب المتهم كما لها أن تسمع الشهود أو تستدعي الخبراء في حالة المسائل الفنية التي تواجهها، طبقا للمادتين 442و 536من قانون الإجراءات الجزائية الفرنسي.[5]

1عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في الإثبات الجنائي، المرجع السابق، ص 119.

2أشرف عبد القادر قنديل، الوسائل الإلكترونية ودورها في الاثبات، المرجع السابق، ص 126.

3خالد ممدوح براهيم، الإثبات الإلكتروني في المواد الجنائية والمدنية، المرجع السابق، ص 54.

4أشرف عبد القادر قنديل، الوسائل الإلكترونية ودورها في الاثبات، المرجع السابق، ص 123.

5براهيمي جمال، التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص 142.

ولا يختلف الوضع في ذلك عن القانون المصري فطبقا لنص المادة 291سالفة الذكر فإنه قد أجاز القانون للمحكمة أن تتخذ أي إجراء تراه مناسبا لإظهار الحقيقة.[1]

وتطبيقا على الجرائم الالكترونية فإن القاضي الجنائي يستطيع وفي سبيل الوصول إلى الحقيقة أن يقوم ببعض الإجراءات كأن يوجه أمرا لمزود خدمة الإنترنت بتقديم بعض البيانات المعلوماتية المتعلقة بمستخدم الإنترنت كالعناوين والمواقع الالكترونية التي زارها، والوقت والتاريخ، وكذا الرسائل المتبادلة وغيرها من المعلومات المتعلقة بنشاطه داخل الشبكة، [2] كما أن للقاضي الجزائي سلطة الأمر باعتراض الاتصالات الالكترونية وسلطة الأمر بتفتيش مكونات الأجهزة الالكترونية من حواسيب وأجهزة ذكية وشبكات اتصال، متى ما قدر ضرورة هذا الإجراء، [3] كما يمكن له أن يأمر القائم بتشغيل النظام بتقديم المعلومات اللازمة لاختراق نظام معين أو الولوج إليه، أو الإفصاح عن كلمات المرور والشفرات الخاصة بتشغيل بعض البرامج، كما يعد أيضا من مظاهر الدور الايجابي للقاضي الجزائي في توفير الدليل الالكتروني الاستعانة بالخبراء في هذا المجال خاصة وأن عملية الحصول على الأدلة الالكترونية وعملية التعامل معها وفهمها يحتاج إلى خبرة ومهارة كبيرة في مجال تقنية المعلومات، ولهذا يستعين القاضي بخبير في هذه المسائل الفنية.[4]

- **الدورالايجابي للقاضي الجنائي في قبول وتقدير الدليل الالكتروني:**

وتأتي هذه المرحلة بعد مرحله توفير الدليل من قبل سلطة الادعاء أو المتهم أو القاضي كما ذكرنا سابقا وهي المرحلة التي يجد مبدأ الشرعية الإجرائية تطبيقه فيها، إذ لا يكون الدليل مقبولا في عملية الإثبات إلا إذا كان مشروعا وذلك أن القاضي لا يقدر إلا الدليل المقبول أي المشروع والذي تم البحث عنه والحصول عليه وفقا لطرق وأساليب مشروعة، فمسألة قبول وتقدير الدليل الالكتروني تتعلق بمبدأ اقتناع القاضي بهذا النوع من الأدلة، هذا المبدأ الذي يخول للقاضي حرية واسعة في البحث عن الأدلة بصفه عامة وتقديرها، فمتى ما ارتاح ضمير القاضي إلى دليل معين فيمكنه أن يستمد قناعته منه ويعول عليه في إصدار حكمه.[5]

وقد أقرت معظم التشريعات مبدأ الاقتناع القضائي إذ نجد المشرع الجزائري قد كرسه بموجب المادة 307من ق إ ج والتي تنص على: "... إن القانون لا يطلب من القضاة أن يقدموا حسابا عن الوسائل

1ينظر المادة 291من ق ا ج المصري.

2بوكر رشيدة، الحماية الجزائية للتعاملات الإلكترونية، المرجع السابق، ص 429.

3المرجع نفسه، ص 486.

4عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في الإثبات الجنائي، المرجع السابق، ص 124.

5عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في الإثبات الجنائي، المرجع السابق، ص 125.

التي بها قد وصلوا إلى تكوين اقتناعهم ولا يرسم لهم قواعد يتعين عليهم أن يخضعوا لها على الأخص تقدير تمام أو كفاية دليل ما ولكنه يأمرهم أن يسألوا أنفسهم في صمت وتدبر وأن يبحثوا بإخلاص ضمائرهم في أي تأثير قد أحدثته في إدراكهم الأدلة المسندة إلى المتهم وأوجه الدفاع عنها، ولم يضع لهم القانون سوى هذا السؤال الذي يتضمن كل نطاق واجباتهم: هل لديكم اقتناع شخصي؟"، والملاحظ أن هذه المادة مستوحاة من نص المادة 353من قانون الإجراءات الفرنسي.[1]

كما ورد هذا المبدأ في المادة 302فقرة01 من ق إ ج المصري حيث نصت على: "يحكم القاضي في الدعوى حسب العقيدة التي تكونت لديه بكامل حريته"، وتؤكد هذا المبدأ أيضا المادتين 291و300من نفس القانون.[2]

وإعمالا لهذا المبدأ يمكن القول أن الدليل الالكتروني مثله مثل الأدلة الأخرى لا يحظى بقوة حاسمة في الإثبات وإنما هو مجرد دليل لا تختلف قيمته ولا تزيد حجيته عن باقي الأدلة، وعليه يمكن للقاضي أن يؤسس اقتناعه على هذا الدليل كما له أن يستبعده وله في ذلك مطلق الحرية، إلا أن اعتبار الدليل الالكتروني من تطبيقات الدليل العلمي وما يتميز به من موضوعية وقيمة علمية يؤدي للقول أن دور القاضي في هذه الحالة يصبح ضئيل نوعا ما في تقديره لهذا الدليل، ذلك أن الدليل العلمي الالكتروني ذو قيمة قاطعة في الإثبات إلا أن هذا التصور ليس في محله، وفي هذا ذهب الفقه إلى التمييز بين أمرين أولهما القيمة العلمية القاطعة والثاني الظروف والملابسات التي وجد فيها هذا الدليل، إذ أن تقدير القاضي لا يتناول القيمة العلمية القاطعة للدليل فلا حرية له في مناقشه الحقائق العلمية الثابتة، وإنما يشمل تقديره الشخصي الملابسات والظروف التي وجد فيها هذا الدليل فبمقدوره أن يطرح الدليل الالكتروني رغم قطعيته إذا تبين له بأنه لا يتفق مع ظروف الواقعة وملابساتها، أي أن مجرد توافر الدليل العلمي لا يعني بالضرورة أن القاضي ملزم بالأخذ به والحكم بالإدانة أو البراءة وإنما يجب عليه البحث في الظروف التي وجد فيها هذا الدليل وفي الأخير يحكم وفقا لاقتناعه ويقينه الشخصي.[3]

- **قبول الدليل الالكتروني في نظام الأدلة القانونية:**

وفقا لهذا النظام فإن المشرع هو الذي يحدد حصرا الأدلة التي يجوز للقاضي اللجوء إليها في الإثبات الجنائي كما يحدد أيضا القيمة الإقناعية لكل دليل، بحيث يقتصر دور القاضي على مجرد فحص هذا الدليل للتأكد من توافر الشروط التي حددها القانون سلفا، وبهذا يعد دور القاضي في هذه الأنظمة دورا

1 Voir l'article n° 353 du code de procédure pénale français.

2بوكر رشيدة، الحماية الجزائية للتعاملات الإلكترونية، المرجع السابق، ص 461.

3عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في الإثبات الجنائي، المرجع السابق، ص 160.

سلبيا لأن القاضي يعتبر مقيد بنوع محدد من الأدلة فلا مجال للخروج عنها، ولهذا سمي هذا النظام بنظام الإثبات القانوني المقيد، [1] ومن بين الدول التي تأخذ بهذا النظام نجد الولايات المتحدة الأمريكية والمملكة المتحدة، وعليه فإن الدليل الإلكتروني في هذه النظم لا يعترف له بأية قيمة ثبوتية ما لم ينص القانون عليه صراحة مهما توافرت فيه الشروط فلا يجوز للقاضي أن يستند إليه لتكوين عقيدته واقتناعه.[2]

إن نظام الإثبات في هذه التشريعات ذات الأصل الأنجلوساكسوني يختلف عن غيره من التشريعات التي تأخذ بالنظام اللاتيني فالدليل في هذه الأنظمة تحكمه قواعد خاصة تتعلق أولها بمضمون هذا الدليل، وثانيا بكيفية تقديم هذا الدليل ومن بين هذه القواعد، قاعدة استبعاد شهادة السماع وقاعدة الدليل الأفضل أو المحرر الأصلي، فمدام الدليل الإلكتروني في أصله يمثل شهادة سماع كونه يتكون من جمل وكلمات يدخلها الشخص إلى الكمبيوتر سواء تم معالجة تلك الكلمات أو البيانات أو لا، فهذا يثير اعتراضا حول مسألة مشروعية وقبول الدليل الإلكتروني أو مخرجات الحاسوب والأجهزة الإلكترونية في الإثبات أمام القاضي الجنائي، فهل يتم رفضه واستبعاده أم قبوله في الإثبات؟[3] وهو ما سنحاول بيانه في النقاط التالية:

- **قاعدة استبعاد شهادة السماع:**

ويقصد بها الشهادة التي يدلي فيها الشاهد بما سمعه بشأن واقعة ما، وهذا النوع من الشهادة مرفوض في الأنظمة الأنجلوساكسونية من بينها التشريع الأمريكي والتشريع الانجليزي، وكذا التشريع الكندي، فلا تعتد هذه التشريعات بالشهادة السماعية في الإثبات الجنائي ويرجع السبب في ذلك إلى عدم ثقة القضاء في الشخص الذي يدلي بهذه الشهادة، وبما أن الدليل الإلكتروني يعد شهادة سماع فيعتبر دليل غير مقبول، إلا أنه في الحقيقة غير ذلك فقد وضعت هذه التشريعات قائمة من الاستثناءات على هذه القاعدة ومن بينها المعلومات والبيانات التي يتم الحصول عليها من الكمبيوتر، حيث تكون مقبولة في الإثبات ولكن بشروط معينة، [4]فلا ينطبق قبول الدليل الالكتروني على أساس استثناء قاعدة شهادة السماع على جميع أنواع سجلات ومخرجات الحاسوب، وإنما ميزت المحاكم الفيدرالية الأمريكية بين ثلاث أنواع من الأدلة الالكترونية: أولها سجلات الحاسوب المخزنة والتي تحتوي على معطيات أدخلها الشخص بنفسه ولهذا تعتبر شهادة سماعية لا تقبل بها المحاكم إلا بعد إثبات أن هذه البيانات قد تم إعدادها في

1خالد حسن أحمد لطفي، الدليل الرقمي ودوره في إثبات الجريمة المعلوماتية، المرجع السابق، ص 192.

2أشرف عبد القادر قنديل، الوسائل الإلكترونية ودورها في الإثبات، المرجع السابق، ص 119.

3عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في الإثبات الجنائي، المرجع السابق، ص 125.

4بوكر رشيدة، الحماية الجزائية للتعاملات الإلكترونية، المرجع السابق، ص 432.

ظروف تهدف إلى ضمان صحتها والثقة في مضمونها، أما عن النوع الثاني المتمثل في سجلات الحاسوب المتوالدة وفي هذه الحالة الجهاز هو الذي يقوم بتدوين البيانات التي تصلح أن تقدم إلى المحكمة فهي ليست من قبيل شهادة السماع، ولذلك تتوقف قيمتها الثبوتية على ما إذا كان الجهاز يعمل بطريقة صحيحة أم لا، أما بالنسبة للنوع الثالث الذي يجمع بين سجلات الحاسوب المخزنة والمتوالدة وإن كان منها ما يعد شهادة سماع إلا أنه في العموم لا يعد هذا النوع من السجلات شهادة سماعية وبالتالي يقبل لإثبات الوقائع الجنائية.[1]

- **قاعدة الدليل الأفضل:**

تأخذ التشريعات الأنجلوساكسونية بقاعدة الدليل الأفضل في الإثبات الجنائي والتي مفادها أن يكون إثبات محتويات الكتابة والسجل أو الصورة أصل لهذه الكتابة أو السجل أو الصورة، وهذا مفاده أنه لا يجوز تقديم الصورة لإثبات محتوى الأصل، [2]وهذا ما قرره القانون الأمريكي بموجب المادة 1002من قانون الإثبات الأمريكي والتي تقضي: "باستثناء ما هو مقرر في هذا القانون أو بقانون خاص يصدر عن الكونغرس فإن عند إثبات مضمون الكتابة والتسجيل والورقة فإنه يلزم توافر أصل الكتابة والتسجيل والصورة".[3]

وبما أن ما يتم تقديمه إلى القضاء يتمثل في مخرجات الحاسوب والتي هي عبارة عن نسخ من ملفات معينه فإن قاعدة الدليل الأفضل تقف حائلا أمام قبول الدليل الالكتروني أمام القضاء، كأن يقوم المتهم بإزالة الدليل الالكتروني عن بعد إذ يتبقى فقط نسخه منه، فهل تكفي هذه النسخة لإثبات الجريمة؟ وهذا ما أدى إلى القول بعدم قبول الدليل الالكتروني في الإثبات، [4]، غير أنه مع زيادة ظهور واستخدام المستندات الالكترونية في جميع العمليات كان سببا استدعى تغيير هذه القاعدة لكي تتلاءم مع عصر المعلومات، إذ نجد المشرع الأمريكي استحدث المادة 1001من قانون الإثبات الفيدرالي الأمريكي لتشمل بذلك الدليل الالكتروني، حيث سمحت هذه الأخيرة بالاعتراف بالمواد المكتوبة والمسجلة والالكترونية لتحظى بذات الاهتمام الذي تحظى به باقي الأدلة، [5]بالتالي قد وسع المشرع الأمريكي مدلول الكتابة

1المرجع نفسه، ص 433.

2عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في الإثبات الجنائي، المرجع السابق، ص 131.

3 Rule 1002 of Federal rules of Evidence

4بوكر رشيدة، جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري والمقارن، المرجع السابق، ص 487.

5ضريفي نادية، دراج عبد الوهاب، سلطات القاضي الجنائي في تقدير الدليل الإلكتروني المستمد من التفتيش الجنائي، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، المجلد 04، العدد 02، سنة 2019، ص 126.

والتسجيلات لتشمل كل من الكلمات أو الأرقام أو الحروف أو ما يعادلها سواء مكتوبة باليد أو منسوخة على الآلة الكاتبة أو مطبوعة أو مصورة أو اتخذت شكل نبضات مغناطيسية أو الكترونية معينة.[1]

كما أكدت الفقرة الثالثة من هذه المادة على ذلك في قولها:" إذا كانت البيانات المخزنة في حاسوب أو آلة مشابهة فإن أي مخرجات مطبوعة منها أو مخرجات يمكن قراءتها بالنظر إليها وتعكس دقة المعطيات تعد معطيات أصلية"، [2]وعليه يفهم من نص هذه المادة أن الدليل الالكتروني المستخرج من الطابعة يعد كدليل أصلي ويقبل في الإثبات دون الحاجة إلى جلب الحاسوب إلى قاعة المحكمة لتأكيد تلك الواقعة.

أما بالنسبة للمشرع الانجليزي فقد صرح بقبول صور المستندات أو جزء منها وذلك بموجب المادة 27من قانون العدالة الجنائية لسنة1988، إلا أن هذا القبول مقيد بشروط معينة نصت عليها المادة 69من قانون الشرطة والإثبات الجنائي لسنة1984والتي تشترط لصحة الدليل الالكتروني صحة برنامج التشغيل الذي يعمل به الكمبيوتر أو الجهاز، إضافة إلى حق المتهم في أن تتاح له الفرصة لإثبات أن برنامج التشغيل لا يعمل بطريقة صحيحة أو منتظمة، كما أضاف هذا القانون توجيهات أخرى تتعلق بكيفية تقدير قيمة أو وزن المعطيات أو المستندات المستخرجة عن طريق الحاسب، فقد أوصت المادة 11من الجزء الثاني من الملحق الثالث من هذا القانون مراعاة كل الظروف عند تقييم هذه البيانات المستخرجة من الحاسوب وخاصة مراعاة عنصر "المعاصرة" أي ما إذا كانت هذه المعلومات قد تم تزويد الحاسب بها في وقت معاصر لهذا الأمر أم لا.[3]

2. مشروعية الحصول على الدليل الإلكتروني:

كما ذكرنا سابقا أن للقاضي الجنائي حرية الاستعانة بكافة وسائل الإثبات اللازمة لكشف الحقيقة بما في ذلك الدليل الإلكتروني إلا أن هذه الحرية ليست مطلقة بل قيدها القانون بمجموعة من الضوابط التي يتعين على القاضي أن يمارس سلطته في نطاقها لكي لا ينحرف عن الغرض المنشود، حيث تتمثل هذه القيود في مشروعية إجراءات وطرق الحصول على هذا الدليل، ولهذا قد وضعت الاتفاقيات الدولية والدساتير والقوانين الإجرائية المختلفة نصوصا تتضمن ضوابط شرعية الإجراءات الماسة بحريات الأفراد وحقوقهم، ومن ذلك قد صادقت لجنه الوزراء التابعة للمجلس الأوروبي عام 1981على اتفاقية خاصة بحماية الأشخاص في مواجهة مخاطر المعالجة الآلية للبيانات الشخصية ومن بين أهم المحاور التي

1عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في الإثبات الجنائي، المرجع السابق، ص 132.

2 Rule 1001/3 of Federal rules Evidence ; provides that : « If data are stored in a computer or similar device, any printout or other output readable by sight shown to reflect the data accurately is an « original »

3عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في الإثبات الجنائي، المرجع السابق، ص 133_ 134.

تناولتها الاتفاقية ضرورة أن تكون البيانات المضبوطة صحيحة وكاملة ومستمدة بطرق مشروعة، كما أكدت على نفس المعنى الاتفاقية الدولية لمنع التعذيب الصادرة من الأمم المتحدة عام 1987، وكذلك المؤتمر الدولي الخامس عشر للجمعية الدولية لقانون العقوبات المنعقد في البرازيل عام 1994في مجال حركه إصلاح الإجراءات الجنائية وحماية حقوق الإنسان، [1] واقتداء بهذه المواثيق الدولية وضعت معظم الدساتير والقوانين الإجرائية الداخلية نصوصا تتضمن شرعية الإجراءات الماسة بحقوق وحريات الأفراد و اعتبرت أي دليل يتم استخلاصه بشكل مخالف لهذه النصوص غير مشروع ولا يمكن الاعتماد عليه في الإثبات، إلا أنها فرقت بين دليل البراءة ودليل الإدانة وذلك كما يلي:

- **فبالنسبة لدليل الإدانة:**

القاعدة الأساسية في القانون الانجليزي أنه متى كان الدليل منتجا في الإثبات فهو مقبول أيا كانت الطريقة التي تم الحصول عليه من خلالها حتى ولو كانت غير مشروعة، ونتيجة لحدة هذه القاعدة صدر قانون الشرطة والإثبات الجنائي سنه 1984ليعالج اختصاص الشرطة وقواعد الإثبات على نحو يحقق ضمانات إجرائية معينة، حيث تضمن هذا القانون أحكام تنظم مسألة استبعادالأدلة غير المشروعة ذلك بموجب المواد 76و78من هذا القانون، والتي نصت أن للقضاة السلطة التقديرية في استبعاد الدليل المتحصل عليه بطريقه غير مشروعة، وتطبيقا لذلك رفض القاضي في إحدى القضايا قبول تسجيلات على أساس أنها تمت بطريقة خداعية، حيث قامت الشرطة البريطانية بتركيب جهاز تنصت على خط هاتف إحدى الشاكيات بناء على موافقتها وتم تسجيل المكالمات التي تمت بينها وبين الشخص المشكوك فيه والتي تضمنت موضوعات تدينه.[2]

ومن جهة أخرى كان القضاء الأمريكي يتبنى نفس القاعدة التي يتبناها القضاء الانجليزي حيث لا يستبعد الأدلة المتحصلة بطرق غير مشروعة، إلى غاية عام 1886لاحظت المحكمة الفيدرالية العليا في قضيه عرضت عليها بأنه لا يمكن إدانة أي شخص عن طريق أدلة تم الحصول عليها بطرق غير مشروعة وذلك لحمايته من تعسف السلطات القضائية، وبالتالي عدم قبول الدليل المتحصل بالمخالفة للتعديل الدستوري الأمريكي، إلا أن هذه القاعدة يرد عليها جملة من الاستثناءات، فقد حددت المحكمة العليا ثلاث حالات لا يتم فيها استبعاد الدليل غير المشروع، أول هذه الحالات توفر حسن النية لدى رجال الشرطة عند القيام بالعمل الإجرائي، وثاني هذه الحالات عندما تكون الصلة بين العمل الإجرائي المخالف

1خالد حسن أحمد لطفي، الدليل الرقمي ودوره في إثبات الجريمة المعلوماتية، المرجع السابق، ص 198.

2ليندا بن طالب، الدليل الإلكتروني ودوره في الإثبات الجنائي، المرجع السابق، ص 144.

والدليل المتحصل منه ضعيفة وبسيطة لدرجه أنه لا يمكن إدراك هذا الخطأ أو المخالفة، وثالث هذه الحالات عندما يتم الحصول على الدليل بصورة مستقلة عن العمل الإجرائي المخالف أو غير المشروع.[1]

وتأكيدا على هذا خصص المشرع الأمريكي مبحثا مستقلا في المرشد الفيدرالي الأمريكي في المبحث الخامس منه الذي نظم تفتيش وضبط الحواسيب وصولا إلى الدليل الالكتروني والذي جاء لعلاج انتهاكات الباب الثالث من قانون المراقبة والتسجيل والتقصي أي علاج بطلان الإجراءات غير المشروعة في الحصول على هذا الدليل، إذ أوجب على رجال الضبط القضائي الالتزام بأحكام هذا الباب عند مباشرة إجراءات المراقبة الالكترونية والتفتيش والضبط وأي مخالفة لهذه الأحكام تعرض صاحبها لجزاءات جنائية وكذا إلى بطلان الدليل المتحصل عليه منها.[2]

أما عن الدول التي تبنت النظام اللاتيني أي مبدأ حرية الإثبات ومن بينها التشريع الفرنسي فنجد أن قانون إج الفرنسي رغم أنه لم يتضمن أي نصوص تتعلق بمبدأ الأمانة والنزاهة في البحث عن الحقيقة إلا أن الفقه والقضاء الفرنسي كانا بجانب هذا المبدأ وذلك في مجال البحث والتحري عن مختلف الجرائم بما فيها الجرائم الالكترونية، حيث قبل القضاء استخدام الوسائل العلمية الحديثة في البحث والتنقيب عن الجرائم ولكن شرط أن يتم الحصول على الأدلة الجنائية بطريقه مشروعة ونزيهة.[3]

أما على مستوى التشريعات العربية منها التشريع المصري فقد أقر المشرع بعدم قبول الدليل المتحصل عليه بطريقة غير مشروعة واعتبر هذا الإجراء باطلا بطلانا مطلقا، إذ حظرت المادة 302من ق إ ج الحصول على الاعتراف عن طريق استخدام الإكراه أو وسائل التعذيب، فلا يجوز إكراه المتهم مثلا على الإدلاء بكلمات المرور لنظام معلوماتي معين، كما نصت المادة 336من ق إ ج المصري على أنه:"إذا تقرر بطلان أي إجراء فإنه يتناول جميع الآثار التي تترتب عليه مباشرة إعادته متى أمكن ذلك" حيث لا يفرق المشرع في هذه الحالة بين دليل الإدانة ودليل البراءة ففي كلتا الحالتين يعتبر الدليل غير مقبول والإجراء باطل، وهذا ما أكدته محكمة النقض المصرية بقولها: "لا يكفي لسلامة الحكم أن يكون الدليل صادقا متى كان وليد إجراء غير مشروع"، وقضت أيضا بأن للقاضي أن يكون عقيدته من أي عنصر من عناصر الدعوى إلا إذا كان هذا العنصر مستمدا من إجراء باطل.[4]

1عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في الإثبات الجنائي، المرجع السابق، ص 145.

2المرجع نفسه، ص 145.

3أشرف عبد القادر قنديل، الوسائل الإلكترونية ودورها في الإثبات الجنائي، المرجع السابق، ص 133.

4رفاه خضير جياد العارضي، الدليل الإلكتروني وأثره في مجال نظرية الإثبات الجنائي، المرجع السابق، ص 94.

أما عن القانون الجزائري فلم يتضمن قانون رقم09/04 المتضمن القواعد الخاصة للوقاية من الجرائم الإلكترونية مسألة مشروعية الدليل الالكتروني حيث ترك المشرع ذلك للقواعد العامة والتي تقضي أن الأصل في الأدلة مشروعية وجودها والحصول عليها، وهذا ما قرره قانون الإجراءات الجزائية حيث تنص المادة 191من ق إ ج على: "تنظر غرفة الاتهام في صحة الإجراءات المرفوعة إليها وإذا تكشف لها سبب من أسباب البطلان قضت ببطلان الإجراء المشوب به وعند الاقتضاء ببطلان الإجراءات التالية له كلها أو بعضها..."وعليه فضلا عن بطلان الإجراء غير المشروع فإن هذا البطلان يمتد إلى الإجراءات اللاحقة له مباشرة في حالة ما إذا كان الإجراء الأول السبب الوحيد للإجراء التالي، وبالتالي إذا بطل الإجراء الأول يترتب على ذلك بطلان الإجراء اللاحق.[1]

وبالتالي لا يجوز الحصول على الدليل الالكتروني عن طريق استخدام أساليب التنويم المغناطيسي أو التحليل التخديري مثلا، أو إجبار الشاهد على الإدلاء بالسر المهني المؤتمن عليه، أو من خلال تفتيش حاسوب المتهم بدون إذن قضائي، أو إجبار مزود خدمة الإنترنت أو الاتصال الالكتروني على الكشف عن محتوى هذه الاتصالات بدون إذن من السلطة المختصة، أو إجراء عملية المراقبة الالكترونية للمشتبه فيهم بدون الحصول على إذن مسبق من السلطة المختصة.

- **بالنسبة لدليل البراءة:**

اختلفت التشريعات حول مسألة مدى اشتراط المشروعية في دليل البراءة حيث ظهرت ثلاثة اتجاهات بهذا الشأن:

يرى الاتجاه الأول أن المشروعية لازمة في كل دليل سواء كان دليل إدانة أو دليل براءة، فإثبات البراءة كالإدانة لا يكون إلا من خلال طرق مشروعة فلا يصح أن يفلت إثبات البراءة من قيد المشروعية الذي يعد شرط أساسي في أي تشريع.[2]

ويرى الاتجاه الثاني ضرورة التفرقة بين ما إذا كان دليل البراءة قد تم الحصول عليه نتيجة سلوك إجرامي أو ما إذا تم الحصول عليه نتيجة سلوك يشكل مخالفة لقاعدة إجرائية، ففي حالة ما إذا كان ناتج عن سلوك عبارة عن جريمة وجب عدم الاعتداد بهذا الدليل واستبعاده لأن القول بغير ذلك يعني إباحة بعض الجرائم وإفلاتها من العقاب، أما إذا كان الحصول على الدليل يخالف قاعدة إجرائية فقط فهنا جاز الاستناد إليه في تبرئة المتهم والحجة في ذلك أنه لا يصح أن يضار المتهم بسبب لا دخل له فيه.[3]

1ينظر المادة 191من ق ا ج ج.

2ليندا بن طالب، الدليل الإلكتروني ودوره في الإثبات الجنائي، المرجع السابق، ص 143.

3عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في الإثبات الجنائي، المرجع السابق، ص 142.

أما عن الاتجاه الثالث فيرى أن شرط المشروعية هو شرط وجوبي في دليل الإدانة دون دليل البراءة ذلك أن القاضي لا يحتاج إلى اليقين في إثبات براءة المتهم بل يكفي في ذلك الشك وهو ما يمكن الوصول إليه من خلال أي دليل ولو كان غير مشروع، وحسب هذا الرأي فأن وجوب مشروعية دليل البراءة يعرقل حق المتهم في الدفاع عن نفسه بكافة الطرق والوسائل التي يختارها.[1]

ب. وضعية الدليل الإلكتروني:

لما كان الهدف من إجراءات التحقيق هو وصول القاضي للحقيقة الواقعية، وجب أن يبني حكمه على أدلة طرحت في الجلسة وحصلت المناقشة فيها، وأن يصل بخصوصها إلى درجة اليقين التي لا تقبل الشك والاحتمال، وهذا المبدأ ينطبق على كافة الأدلة سواء كانت تقليدية أو إلكترونية، وعليه سنتطرق لهذه الشروط بالتفصيل في النقاط التالية:

1. **وجوب مناقشة الدليل الإلكتروني:**

يمثل هذا المبدأ أحد أهم المبادئ التي تقوم عليها المحاكمة العادلة والذي ينشأ عن شفوية المرافعة والحق في الدفاع، عن طريق مواجهة المتهم بالوقائع المنسوبة إليه والأدلة المعروضة فيتوجب على القاضي عرض الأدلة الالكترونية أيا كانت طبيعتها سواء المتحصل عليها من الحاسوب أو من شبكة الإنترنت سواء أكانت مطبوعة أم بيانات معروضة على الشاشة أو مخزنة على دعامة يجب مناقشتها بحضور المتهم والسماح له بإبداء رأيه بخصوصها، كما يتوجب على الخبير الحضور للجلسة وتقديم كل ما توصل إليه في تقرير الخبرة ومناقشته أمام القاضي والمتهم و المحامون والحضور،[2] فكل هذه الأدلة تكون محلا للمناقشة قبل الأخذ بها لإثبات الجريمة، وعليه فإن كل دليل يتم الحصول عليه من خلال البيئة التقنية والوسائل الالكترونية يجب أن يعرض في الجلسة وتتم مناقشته.

ولهذا قد حرصت العديد من التشريعات الجنائية على النص صراحة على هذه القاعدة منها التشريع الفرنسي حيث تنص المادة 427فقرة 02من ق ا ج على :"لا يجوز للقاضي أن يؤسس حكمه إلا على أدلة طرحت عليه أثناء المحاكمة ونوقشت أمامه في مواجهة الأطراف"، [3] كما نجد المشرع الأمريكي أكد على ضرورة أن تكون الأدلة موضوع مناقشة حضورية بين الأطراف، ورتب على مخالفة هذه القاعدة

1ليندا بن طالب، الدليل الإلكتروني ودوره في الإثبات الجنائي، المرجع السابق، ص 143.

2التوجي محمد، الحماية الجنائية من الجرائم المرتكبة بواسطة الهاتف النقال، المرجع السابق، ص 202.

3Voir l'article n° 427 de code de procédure pénale.

بطلان الإجراءات، [1] ولا يختلف الأمر عنه في التشريعات العربية إذ أقر المشرع الجزائري هذا المبدأ في المادة 212فقرة02 من ق إ جالتي تنص على "لا يسوغ للقاضي أن يبني قراره إلا على الأدلة المقدمة له في معرض المرافعات والتي حصلت المناقشة فيها حضوريا أمامه". [2]

ومما سبق يمكن القول أنه إذا كان القاضي يلتزم بأن يستمد اقتناعه من الأدلة الالكترونية التي طرحت في جلسات المحاكمة وأتيحت لأطراف الدعوة مناقشتها فمن أهم النتائج التي تترتب على هذه القاعدة: أولا عدم جواز استناد القاضي إلى علمه الشخصي أو إلى رأي غيره، ويقصد بالعلم الشخصي للقاضي معلوماته الشخصية التي يكون قد حصل عليها من خارج نطاق الدعوى المطروحة عليه والتي من الممكن أن تؤثر في تكوين قناعته عند تقديره للأدلة، فلا يجوز للقاضي أن يبني اقتناعه على هذه المعلومات الشخصية لأنها لم تكن موضع مناقشه شفوية وفي هذا إهدار لحقوق الأطراف. [3]

أما عن النتيجة الثانية فتتمثل في ضرورة التأهيل التقني والفني للقضاة لمواكبة المناقشة العلمية والتقنية للأدلة الإلكترونية، حيث يضمن هذا التأهيل نجاح مهمة القاضي في الحكم في القضية والوصول للحقيقة القضائية، وهذا ما لا يتأتى إلا عن طريق تنظيم الدورات التدريبية وتكثيفها. [4]

2. يقينية الدليل الإلكتروني:

يعرف اليقين القانوني على أنه "اقتناع مستند إلى حجج ثابتة وقطعية"، أو "عبارة عن حالة ذهنية أو عقلانية تؤكد وجود الحقيقة"، ويتم الوصول إلى اليقين عن طريق ما تستنتجه وسائل الإدراك المختلفة للقاضي من خلال ما يعرض عليه من وقائع الدعوى وما ينطبق في ذهنه من تصورات ذات درجة عالية من التوكيد. [5] وعليه عندما يصل القاضي لهذه المرحلة من اليقين فإنه يصبح مقتنعا بالحقيقة، فاليقين هو وسيلة الاقتناع فمتى ما تكامل اليقين بأن وصل القاضي إلى درجة القطع ينشأ ما يسمى بالاقتناع اليقيني وهو أساس الحقيقة القضائية التي ينشدها القاضي في حكمه.

فللقاضي الجنائي تقدير الأدلة وموازنتها وفقا لما يمليه عليه ضميره ووجدانه، دون أن يخضع في ذلك لرقابة أي جهة، إلا أنه مقيد بضرورة تأسيس حكمه وقناعته على الجزم واليقين لا على الظن والترجيح، [6] ويتم الوصول إلى درجة اليقين هذه عن طريق ما تستنتجه وسائل الإدراك لدى القاضي من خلال ما

1رفاه خضير جياد العارضي، الدليل الإلكتروني وأثره في مجال نظرية الإثبات الجنائي، المرجع السابق، ص 107.

2ينظر المادة 212فقرة 02من ق ا ج ج.

3ليندا بن طالب، الدليل الإلكتروني ودوره في الإثبات الجنائي، المرجع السابق، ص 150.

4بوكر رشيدة، جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري والمقارن، المرجع السابق، ص 516.

5المرجع نفسه، ص 517.

6المرجع نفسه، ص 518.

يعرض عليه من أدلة إلكترونية وذلك عن طريق معرفته الحسية والعلمية أو العقلية، القائمة على التحليل والاستنتاج، إلا أن هذا النوع من الأدلة يتطلب أن تكون لدى القاضي نوع أخر من المعرفة ألا وهي المعرفة المعلوماتية كون أن جهله بها قد يترتب عليه التشكيك في قيمة الدليل والحكم وفقا لذلك.[1]

كما أن شرط اليقين في أحكام الإدانة شرط عام سواء كانت الأدلة تقليدية أو مستحدثة كالدليل الالكتروني وتكمن العلة من وراء هذا القيد في أن الحكم بإدانة شخص أمر جد خطير يترتب عليه آثار جسيمة و يمكن أن ينال من حريته أو شرفه أو ماله، [2] فإذا كان الأصل في الإنسان البراءة فإنه يجب لإدانته أن يقوم الدليل القاطع على ارتكابه الجريمة سواء كانت تقليدية أو مستحدثة ونسبتها للمتهم، أما فيها يتعلق الحكم بالبراءة يكفي أن يشكك القاضي في صحة إسناد التهمة إلى المتهم حتى يقضي بالبراءة وذلك إعمالا لمبدأ تفسير الشك لمصلحة المتهم.[3] ويترتب على هذا أن كافة الأدلة الإلكترونية من أقراص ممغنطة ومخرجات ورقية وإلكترونية وغيرها، تخضع لتقدير القاضي الجنائي حيث يجب أن يستنتج منها الحقيقة بما يتفق مع اليقين ويبتعد عن الشك والاحتمال، فقد اشترط قانون البوليس والإثبات الجنائي في بريطانيا أنه لكي تتحقق يقينية الأدلة الإلكترونية يجب أن تكون هذه الأخيرة دقيقة وناتجة عن الحاسوب بصورة سليمة أي أن لا يكون هناك اعتقاد أو شك بخصوص طريقة عمل الحاسوب أو طريقة استعماله بشكل غير سليم.[4]

كما نص قانون الإثبات الجنائي الصادر سنة 1983الخاص بولاية كاليفورنيا، وكذا قانون الحاسب الآلي الصادر سنة 1984في ولاية إيوا الأمريكية على أن : "النسخ المستخرجة من البيانات التي يحتويها الحاسوب تعد من أفضل الأدلة المتاحة لإثبات هذه البيانات، وبالتالي يتحقق اليقين لهذه الأدلة".[5]

ومما سبق يمكن القول بأن معايير قبول الدليل الإلكتروني في الإثبات الجنائي تختلف من نظام لآخر إلا أن الطبيعة العلمية والتقنية للدليل لا تسمح للقاضي الجزائي بأن يشكك فيما توصل إليه العلم من حقائق، وإنما تبقى سلطته التقديرية قائمة بخصوص ظروف وملابسات الحصول على هذا الدليل، فيما إذا كانت أساليب استخلاص هذا الدليل شرعية أم لا.

1ضريفي نادية، دراج عبد الوهاب، سلطات القاضي الجنائي في تقدير الدليل الإلكتروني المستمد من التفتيش الجنائي، المرجع السابق، ص 124.

2ليندا بن طالب، الدليل الإلكتروني ودوره في الإثبات الجنائي، المرجع السابق، ص168.

3ليندا بن طالب، الدليل الإلكتروني ودوره في الإثبات الجنائي، المرجع السابق، ص 169.

4رفاه خضير جياد العارضي، الدليل الإلكتروني وأثره في مجال نظرية الإثبات الجنائي، المرجع السابق، ص 99.

5ضريفي نادية، دراج عبد الوهاب، سلطات القاضي الجنائي في تقدير الدليل الإلكتروني المستمد من التفتيش الجنائي، المرجع السابق، ص 125.

الفرع الثاني: الصعوبات التي تعترض عملية البحث والتحري عن الجريمة الإلكترونية

أدت الطبيعة التقنية والمتميزة للجرائم الإلكترونية والبيئة التي تنشأ فيها، إلى ظهور نوع من التحدي للأجهزة المختصة بالبحث والتحري في تطبيق القواعد الإجرائية التي نظمت مسألة استخلاص الدليل، مما أصبح يشكل عائقا أمامها ويضعف قيمتها في مكافحة هذا النوع من الجرائم، ولعل أهم هذه الصعوبات التي تعترض جهات التحقيق في جمعها للدليل الإلكتروني ما يلي:

أولا: صعوبات تتعلق بطبيعة الجريمة الإلكترونية والدليل الناتج عنها

فنتيجة الطبيعة الخاصة للجريمة الإلكترونية وسرعة انتشارها أصبحت تشكل تحديا أمام السياسة التشريعية الجنائية لعدم مواكبتها لهذا التطور، فضلا عن الطبيعة المميزة للدليل الناتج عنها وما تثيره إجراءات استخلاصه من إشكالات سنعرضها في النقاط التالية:

1) القصور التشريعي في مواجهة الجرائم الإلكترونية:

إن عدم تطور القوانين بنفس السرعة والوتيرة التي تتطور بها وسائل الإعلام والتكنولوجيا جعل القوانين التقليدية تقف عاجزة عن مواجهة العديد من الجرائم المستحدثة التي أفرزتها الثورة التكنولوجية، حيث أن مكافحة هذه الجرائم ما زال يتم في إطار النصوص العقابية المألوفة التي وضعت لكي تطبق على الجرائم التقليدية، وهذا ما ترتب عليه الكثير من المشكلات حول متابعة الجرائم الإلكترونية كونها تتميز بطبيعة خاصة، فالمعروف أن القوانين الوضعية السائدة في أغلب دول العالم يحكمها مبدأ الشرعية الجنائية الذي يقضي أنه لا جريمة ولا عقوبة إلا بنص قانوني، وأن نطاق التجريم بالقياس في ظل هذا المبدأ يكون ضيقا جدا، [1] وبالتالي لا يمكن العقاب على أي فعل غير مشروع يرتكب على أو بواسطة الجهاز الإلكتروني ما دام المشرع لم ينص عليه ضمن القوانين العقابية، ولهذا يتوجب على المشرع الجنائي إخضاع جميع الأفعال التي تشكل جرائم إلكترونية للتجريم والعقاب بنصوص صريحة ومباشرة لتفادي إفلات المجرمين من المساءلة الجنائية.[2]

هذا ما دفع معظم دول العالم إلى سن قوانين خاصة لتجريم هذا النوع من الجرائم وتعديل أخرى لسد هذا القصور التشريعي، الأمر الذي انعكس على الجانب الإجرائي باستحداث نصوص تشريعية إجرائية تنظم عملية التحري والتحقيق في الجرائم الإلكترونية وكذا كيفية استخلاص الأدلة الإلكترونية

1براهيمي جمال، التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص 220.

2لينا محمد الأسدي، مدى فاعلية أحكام القانون الجنائي في مكافحة الجريمة المعلوماتية، المرجع السابق، ص 238.

والتعامل معها، غير أن الملاحظ من هذه القوانين أنها لم تشمل كافة صور الأفعال غير المشروعة الناتجة عن استعمال الوسائل التكنولوجية الحديثة، وذلك بسبب عدم تطورها بنفس وتيرة تطور هذه الجرائم، كما أن بعض الدول النامية لم تسن بعد قوانين تنظم هذه الجرائم وإنما تكتفي بتطبيق النصوص التقليدية رغم ثبوت قصورها.[1]

2) صعوبات ناجمة عن طبيعة آثار الجريمة المعلوماتية:

يتميز الدليل الإلكتروني بطبيعة خاصة تميزه عن باقي الأدلة الجنائية، هذه الطبيعة التي أثارت عدة تحديات أمام جهات البحث والتحقيق بخصوص استخلاص الدليل ومتابعة الجرائم الإلكترونية، إذ تتمثل أهم هذه التحديات فيما يلي:

أ. غياب المظهر المادي للدليل الإلكتروني:

ينتج عن الجرائم التقليدية آثار مادية ملموسة عكس الجرائم الإلكترونية فهي من الجرائم الهادئة التي لا تترك بصمات أو أدلة مادية يمكن فحصها، فهي تقع في بيئة تقنية افتراضية، وعليه فإن الدليل الإلكتروني هو عبارة عن نبضات كهرومغناطيسية مكونة من سلسلة من الأرقام المخزنة في نظام حاسوبي بشكل ثنائي، مما يجعل أمر التعامل معها صعبا على سلطات التحري والتحقيق، علاوة على صعوبة ربطها بشخصية المتهم فهي لا تفصح عن هوية المستخدم، فالدليل الإلكتروني لا يفصح عن شخصية معينة، وهو ما يظهر جليا في الجرائم المرتبكة عبر الشبكة والتي يستطيع المستخدم عبرها الاتصال دون الكشف عن هويته الحقيقية، [2] إضافة إلى كون الدليل الرقمي غالبا ما يكون مشفرا عن طريق كلمات وأرقام سرية يصعب على المحقق كشفها، كما أن إمكانية تعديله والتلاعب به تشكل عائقا في نسبة هذا الدليل إلى المتهم وتحول دون الكشف عن الحقيقة.[3]

ب. سهولة محو الدليل الإلكتروني والتلاعب به:

قد جعلت الطبيعة التقنية واللامادية للدليل الإلكتروني أمر طمسه ومحوه من قبل الجاني في غاية السهولة، هذا ما يعيق إثبات الجريمة الإلكترونية إذ يقوم الجناة بإخفاء نشاطهم الإجرامي عن طريق محو أو تدمير الدليل دون ترك آثار معينة، وذلك في وقت قصير جدا لا يتعدى بضع ثواني، كما يقوم الجاني بالتلاعب في الدليل بالحذف أو التغيير بما ينفي الشكوك حوله، عن طريق إدخال بيانات مزيفة أو

1براهيمي جمال، التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص 223.

2- عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في الإثبات الجنائي، المرجع السابق، ص 252 – 251.

3ليندا بن طالب، الدليل الإلكتروني ودوره في الإثبات الجنائي، المرجع السابق، ص 175.

محرفة في النظام المعلوماتي أو تغيير مسار البيانات الصحيح بمجرد الضغط على لوحة المفاتيح ودون أي جهد منه،[1] وبالتالي يصعب على سلطات التحري والتحقيق إقامة الدليل ضده وعدم الوصول إلى الحقيقة المنشودة، كما يجدر الإشارة إلى أن محو الدليل الإلكتروني وتدميره ليس حكرا على الجاني فقط فغالبا ما يقوم المحقق أو الخبير بإتلاف الدليل عند القيام باستخلاصه أو فحصه نتيجة لنقص المعرفة الفنية له وكيفية التعامل معه، أو لسهو منه.

ثانيا: صعوبات تتعلق بجهات التحري والتحقيق في الجريمة الإلكترونية

تواجه سلطات التحقيق العديد من التحديات عند مباشرتها لإجراءات التحري والتحقيق في هذه الجرائم وجمع الدليل الناتج عنها ولعل أهم ما يعيقها في هذه المرحلة ما يلي:

1) نقص ثقافة وخبرة سلطات البحث والتحري في مجال المعلوماتية:

من بين الصعوبات التي تواجه عمليات استخلاص الدليل في الجرائم الإلكترونية، هو نقص الخبرة والمعرفة التقنية لدى سلطات البحث والتحري، وأجهزة الأمن بصفة عامة، ويرجع هذا للطبيعة الخاصة للجريمة الإلكترونية والبيئة التي تحتوي الدليل الإلكتروني وما يتميز به من خصائص كما ذكرنا سابقا، هذا ما جعل أجهزة العدالة بصفة عامة تقف عاجزة أمام هذه التحديات، إذ يتطلب الكشف عن هذه الجرائم إتباع أساليب خاصة وإستراتيجيات تتعلق باكتسابهم مهارات حول التعامل مع التقنيات المعلوماتية، وكيفيات التحري والتحقيق وجمع الأدلة من المسرح الافتراضي للجريمة، التي أصبح الجناة محترفين في التعامل معه، الأمر الذي زاد من صعوبة الكشف عن نشاطاتهم الإجرامية،[2] إضافة إلى عدم معرفتهم الواسعة باللغة العلمية الرقمية التي يتعامل بها العاملين في مجال المعلوماتية والإعلام والاتصال والتي أصبحت تشكل الطابع المميز لمحادثاتهم، كما أن شخصية المحقق سواء كان ضابط شرطة أو قاضي تؤثر هذي الأخرى على إجراءات المتابعة، كأن يتهيب من استخدام الإنترنت أو الكمبيوتر، وعدم اهتمامه بما هو مستجد في مجال المعلوماتية وأساليب التحقيق، الأمر الذي من شأنه أن يؤثر سلبا على عمليات البحث والتحريفي هذه الجرائم.[3]

كما ينتج عن نقص الخبرة لدى سلطات التحري والتحقيق تدمير وإتلاف الدليل الذي يعبر عن الحقيقة، على اعتبار أن جهلهم بأساليب ارتكاب الجريمة الإلكترونية والتعامل مع الأدلة يجعلهم كثيرا

1براهيمي جمال، التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص 198.

2رشيدة، جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري والمقارن، المرجع السابق، ص 461.

3بثينة حبيباتي، معوقات مكافحة الجريمة المعلوماتية، مجلة العلوم الإنسانية، المجلد "أ"، عدد 50، ديسمبر 2018، ص 87.

يقعون في أخطاء من هذا القبيل، والأسوأ من ذلك قد ترتكب الجريمة على مرأى ومسمع من سلطات الضبط دون الشعور بذلك، كما قد يقدمون يد العون لمرتكبي هذه الجرائم عن جهالة منهم، كحمل المشتبه فيه على استعادة معلومات من الحاسوب مثلا، بسبب عدم معرفة المحقق مما يسمح للمشتبه فيه بتدمير الدليل ومحوه تحت أنظار المحقق، أو القيام بمصادرة وحجز أجهزة الحاسوب محل الجريمة دون أدنى تعامل تقني معها وهو ما يزيد من فرضيات فقد الأدلة المادية والمعنوية.[1]

ولهذه الأسباب يرى المختصون في مكافحة الجرائم الإلكترونية أنها تشكل تحديا كبيرا لأجهزة العدالة كون أن رجال الضبط لا يزالون يعتمدون الطرق التقليدية في تتبع هذه الجرائم، وهذا ما يجب تداركه إذ نجد بعض الدول استقطبت العديد من المختصين وذوي الكفاءات العالية في مجال المعلوماتية ضمن أجهزتها الأمنية والقضائية،[2] كما بادرت أغلبها إلى إنشاء وحدات خاصة بمكافحة الجرائم الإلكترونية ، كما سبق وأن فصلنا في ذلك (في الفصل الثاني من الباب الأول)، وتعتبر الولايات المتحدة الأمريكية وفرنسا من الدول الرائدة في هذا المجال، نظرا لمعاناتها بشكل كبير من الجرائم الإلكترونية، وهو ما دفعها لإنشاء وحدات متخصصة للمكافحة والتحقيق في الإجرام المعلوماتي،[3] على غرار بعض البلدان العربية التي لا تزال متأخرة نوعا ما في مجال مكافحة هذه الجرائم مقارنة بالدول الأوروبية والأمريكية.

ومن جهة أخرى فإن التحقيق في هذه الجرائم يحتاج إلى خبراء ومختصين في هذا المجال، والذين يحتاجون وبصفة دورية ومستمرة إلى دورات تكوينية وتدريبية، لأجل تحسين معارفهم وتطويرها، وهو الأمر الذي يتطلب تكاليف باهظة،[4] إذ أن الميزانية المالية المرصودة لتدريب الضباط والمحققين لا تكفي في أغلب الأحيان فالميزانية المالية الخاصة بأجهزة الأمن والقضاء تكون ضعيفة في مجال تغطية احتياجات خبراء الحاسوب، فضلا على أنها لا تصل إلى ذات المبالغ التي تسددها المؤسسات الخاصة.[5] مما ساهم في ركود القدرات المعرفية لأجهزة العدالة وبالتالي ضعف التصدي للجرائم الإلكترونية، وتطبيقا لذلك قامت العديد من الدول بتنظيم دورات تدريبية وتعليمية لرجال الضبط القضائي والقضاة والخبراء لتدريبهم على مهارات التعامل مع مسرح الجريمة الإلكترونية والدليل الناتج عنها، وكذا أساليب التحقيق فيها، وهذا ما

1حسين ربيعي، آليات البحث والتحقيق في الجرائم المعلوماتية، المرجع السابق، ص 282. .

2براهيمي جمال، التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص 211.

3- عبد الفتاح بيومي حجازي، الدليل الجنائي في جرائم الكمبيوتر والتزوير، دراسة معمقة في جرائم الحاسب الآلي والإنترنت، دار الكتب القانونية، مصر، سنة 2004، ص 81.

4المرجع نفسه، ص 270.

5عبد الفتاح بيومي حجازي، الدليل الجنائي في جرائم الكمبيوتر والتزوير، المرجع السابق، ص 84.

لم يتأتى إلا عن طريق التعاون والتنسيق بين الدول في مجال تدريب رجال العدالة،[1] حيث يشترط في العملية التدريبية أن يكون هذا التدريب يراعي جملة من الأمور لعل أهمها أن يتوافر لدى المتدرب الصلاحية العلمية والقدرات العقلية والذهنية لتلقي التدريب، كما يجب أن يتضمن التدريب التعرف على كيفيه تشغيل الأجهزة الآلية وكذا برمجيات العمل الخاصة بها، وكيفية استخدامها في ارتكاب الجريمة الإلكترونية، وكذا كيفية استخلاص الأدلة الجنائية منها بكل حذر لتجنب عدم اتلافها، والتدرب على كيفيه تأمين هذه الأجهزة والبيانات من عمليات الاختراق والقرصنة وغيرها من المواضيع ذات الصلة والتي من ضمنها معرفه التهديدات السيبرانية وأنواع هذه الجرائم، بالإضافة إلى تلقينهم المنهج التحقيقي الذي يسير عليه المتدرب في تتبع الجريمة من خلال تعريفهم بأساليب التخطيط وتجميع المعلومات الخاصة بالمشتبه فيهم، وكذا أساليب المواجهة والاستجواب وأساليب فحص الأدلة الإلكترونية.[2]

ونظرا لأهمية التدريب في مجال مكافحة الجرائم بصفة عامة دعت أغلب الصكوك الدولية إلى ضرورة وجود تعاون بين الدول في مجال التدريب ونقل الخبرات، من بينها اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية لسنة 2000في مادتها 29، كما دعا المجلس الأوروبي في إحدى توصياته سنة 1999على ضرورة تدريب سلطات التحقيق بما يواكب تطور الجريمة الإلكترونية والتقنية الحديثة، واهتمت منظمة الأنتربول هي الأخرى بهذا المجال من خلال تنظيمها العديد من الدورات التعليمية والتدريبية لمحقق جرائم الانترنت.[3]

كما بادرت العديد من الدول الأجنبية باستحداث وإنشاء وحدات متخصصة في مجال مكافحة هذه الجرائم منها مكتب المساعدة والتدريب التابع لوزارة العدل الأمريكية الذي يعمل على مساعدة أجهزة الشرطة في البلدان خاصة النامية من أجل تعزيز قدراتها التحقيقية، ومدها بالخبرات في هذا المجال، وعلى غرار الدول الأجنبية قامت الدولة الجزائرية بتنظيم مثل هذه الدورات لتأهيل أعضاء وأجهزة التحري والتحقيق في مجال تأمين الفضاء السيبراني ومكافحة الجريمة الإلكترونية إذ تقوم مختلف الأسلاك الوطنية مثل المديرية العامة للأمن الوطني والدرك الوطني بعقد الملتقيات والدورات التدريبية في هذا المجال لزيادة الوعي بخطورة هذه الجرائم وتعليم أساسيات التعامل معها وكيفيه تتبعها وضبطها،[4] كما أبرمت العديد من الاتفاقيات الثنائية مع الدول الأوروبية مثل فرنسا والولايات م أ من أجل بعث

1ليندا بن طالب، الدليل الإلكتروني ودوره في الإثبات الجنائي، المرجع السابق، ص 222.

2حسام محمد نبيل الشنراقي، الجرائم المعلوماتية، المرجع السابق، ص 766.

3ليندا بن طالب، الدليل الإلكتروني ودوره في الإثبات الجنائي، المرجع السابق، ص 226.

4يزيد بوحليط، الجرائم الإلكترونية والوقاية منها، المرجع السابق، ص 528.

إطارات من الشرطة والدرك الوطني للتكوين في مجال التحقيق في الجرائم الإلكترونية، ومثالها تنظيم ورشة تكوينية سنة 2010حول مكافحة الجريمة المعلوماتية لفائدة ضباط الشرطة القضائية والقضاة، والتي أشرف عليها مجموعة خبراء من الاستخبارات المركزية الأمريكية وعملاء من مكتب التحقيقات الفيدرالي، وشارك فيها عدة خبراء في الجرائم الحاسوبية والملكية الفكرية وكذا قسم الجريمة المنظمة التابع لوزارة العدل الأمريكية، وقد استفاد من هذه الورشة العديد من الضباط والمتخصصين والخبراء.[1]

2) صعوبات متعلقة بتحديد المجرم الإلكتروني :

يتميز المجرم الإلكتروني عن المجرم العادي بالذكاء والمعرفة الفنية الواسعة، إذ لا يحتاج لتنفيذ جريمته لجهد وتحضير وإنما يحتاج لتخطيط محكم فضلا عن معرفته الجيدة بالتقنيات الحديثة، إذ يستخدم أساليب فنية لإخفاء نشاطه الإجرامي، فغالبا ما يضرب سياجا أمنيا على أفعاله غير المشروعة قبل ارتكابها وذلك باستخدام كلمات المرور السرية والرموز الغامضة،[2] أو دس تعليمات خفية أو ترميزها لمنع الاطلاع عليها، ولعل أن الإشكال يتفاقم في حال تخزين هذه المعلومات خارج حدود الدولة بحيث تصطدم عملية الوصول إلى الدليل الإلكتروني بمشكلة إجرائية تتعلق بمدى سريان النصوص الإجرائية من حيث المكان على هذه البيانات، (هذا ما سنتطرق له بالتفصيل لاحقا).

هذا ما يشكل تحديا أمام رجال الضبط القضائي عند معاينة وتفتيش الأجهزة الإلكترونية دون الحصول على فك لهذه الرموز والشفرات، كما يصطدم أيضا المحقق بمسألة إجبار المتهم على تقديم أدلة ضده ككلمات المرور مثلا، إذ ثار خلاف حول هذه المسألة فمنهم من يرى ضرورة ذلك ومنهم من يرى عدم جواز إجبار المتهم على فك الشفرات والكلمات السرية الخاصة به، هذا ما يستدعي من القائم بالتفتيش والمعاينة أن يسعى بنفسه للكشف عن كلمات السر، الأمر الذي يحتاج في أغلب الأحيان إلى جهد ووقت كبيرين ومعرفة واسعة بهذا الخصوص.[3]

وقد ازدادت مشكلة تحديد هوية المجرم الإلكتروني تعقيدا بسبب استحداث مجرمي المعلوماتية أسلوب التخفي عبر الشبكة من خلال استعمالهم لوسيلة مستحدثة في مجال التواصل عبر الشبكات وهي ما يعرف ب "الشبكة الخفية للنت "أو ما يصطلح عليه باللغة الإنجليزية وفي لغة المعلوماتية " The Darknet"وهي شبكة موازية لشبكة الإنترنت العادية، حيث ظهرت لأول مرة سنة 1970في الولايات المتحدة الأمريكية لأجل تأمين المعلومات العسكرية المتنقلة عبر الشبكة، ودخلت عالم المعلوماتية سنة

1بوقرين عبد الحليم، حتمية إنشاء ضبطية خاصة بالجرائم الإلكترونية، المرجع السابق، ص 185.

2براهيمي جمال، التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص 206

3المرجع نفسه، ص 207.

2002ويكفي لولوج هذه الشبكة الخفية والإبحار عبرها تحميل تطبيق معلوماتي متوفر على شبكة الإنترنت وتفعيله على جهاز الحاسوب، [1] وأشهر هذه التطبيقات تطبيق "The Onion Router"يعمل هذا الأخير على تغيير العنوان الإلكتروني للحاسوب (IP) المتصل بالشبكة الموازية الخفية عدة مرات في الساعة الواحدة فإذا كان المستعمل متصلا من فرنسا حقيقة فإنه يظهر متصلا تارة من الولايات المتحدة الأمريكية وتارة من اليابان وتارة من إنجلترا وهكذا على مدار مدة الاتصال بالشبكة، وهو ما يجعل من أمر اقتفاء أثر المجرم المعلوماتي غاية في التعقيد إن لم يكن مستحيلا، فضلا على أن نتائج تتبع العنوان التراسلي هذا ليست دائما صحيحة وموثوقة إذ ليس بالضرورة أن يكون صاحب العنوان هو نفسه مرتكب الجريمة، وخاصة في الدول العربية التي تشترك فيها العديد من الهويات في خط أو عنوان بروتوكول واحد مما يجعل الأمر صعبا ومعقدا جدا. [2]

3) **صعوبات متعلقة بالإحجام عن التبليغ:**

يعتبر تكتم المجني عليه عن التبليغ عن الجريمة الإلكترونية من أهم الأسباب التي تحول دون اكتشافها، وهذا نظرا للطبيعة الخاصة التي تتميز بها هاته الجرائم كونها جرائم مستترة وتقع في بيئة افتراضية لا تترك ورائها أي أثر خارجي، مما جعل أمر اكتشافها من قبل الضحية صعبا نوعا ما، إذ غالبا ما يكون اكتشافها بمحض الصدفة، [3] وهذا راجع لعدة أسباب منها خوف المجني أو الجهات المتضررة من الجريمة بصفة عامة على سمعتها، وخاصة الشركات والمؤسسات المالية التي تحرص على عدم انتشار خبر تعرضها للاعتداء، حفاظا على سمعتها ومصداقيتها، لما قد يوحي هذا الفعل بإهمالها وقلة خبرتها وعدم وعيها الأمني، وهو ما قد ينعكس سلبا على أرباحها وقيمة أسهمها، وكذا على ثقة المتعاملين في خدماتها، [4] وهذا ما يعبر عنه علماء الإجرام بمصطلح "الرقم الأسود "أي الجرائم غير المبلغ عنها.

وفي هذا الشأن كشفت إحدى الدراسات الإحصائية الذي قام بها المعهد الوطني للقضاء التابع لوزارة العدل الأمريكية والتي شملت 128من العاملين في مجال التحقيق الجنائي المعلوماتي والذين يمثلون 114وكالة رسمية، بأن حوالي 70% من الجرائم المعلوماتية المكتشفة لا يتم التبليغ عنها، [5] كما أكد Beter Swift) عضو اتحاد الصناعة البريطاني أن العديد من الضحايا في جرائم المعلوماتية لا يقفون عند حد

1William Gilles et Jean Harivel et Irène Bouhadana –« Darknet le coté obscur du net »- Article publier sur : Panthéon Sorbonne Magazine – Magazine D'information de L'université Paris 1 Panthéon Sorbonne – N° 06- Janvier – Février – 2014- Paris – France.

2بوكر رشيدة، جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري والمقارن، المرجع السابق، ص 475.

3المرجع نفسه، ص 471.

4حسين ربيعي، آليات البحث والتحقيق في الجرائم المعلوماتية، المرجع السابق، ص 290.

5المرجع نفسه، ص 292.

عدم الإبلاغ عن الجريمة، بل أنهم يرفضون أي تعاون مع الجهات الأمنية خشية معرفة العامة بوقوع الجريمة، ويسعون بدلا من ذلك إلى محاولة تجاوز آثارها حتى لو كانت الوسيلة هي مكافأة المجرم، ونذكر على سبيل المثال ما قام به بنك Marchant Bank Cityالإنجليزي الذي تعرض لسرقة (08) مليون جنيه أثناء تحويلها إلكترونيا إلى رصيد في سويسرا، وقد تم القبض على الفاعل أثناء محاولة سحبه المبلغ، وبدل رفع البنك دعوى ضد المتهم قام مسئول البنك بدفع مبلغ مليون جنيهللمتهممقابل شراء سكوته وعدم الإبلاغعن ما حدث[1].

ثالثا: صعوبة التعاون الدولي في مكافحة الجرائم الإلكترونية

للتعاون الدولي أهمية كبيرة في مجال مكافحة الجرائم عامة والجرائم الإلكترونية خاصة، كونها جرائم تتميز بطابعها الدولي العابر للحدود، حيث يعد التعاون القضائي الدولي أسمى مظاهر التعاون الدولي في مكافحة الجريمة، إذ يوفق بين استقلال كل دولة في ممارسة اختصاصها الجزائي على حدود إقليمها وبين ضرورة ممارسة حقها في العقاب، ولعل أهم صور التعاون القضائي الدولي، المساعدة القضائية وكذا تسليم المجرمين، ورغم هذه الأهمية إلا أنه يواجه العديد من الصعوبات والمعوقات التي تحول دون التصدي الأمثل لهذه الجرائم، ولعل من بين هذه الصعوبات الاختلافات الموجودة في التشريعات العقابية لأغلب الدول، سواء ما تعلق منها بالجوانب الموضوعية أو الإجرائية، وعليه تتمثل أهم هذه الإشكالات فيما يلي :

1) عدم وجود نموذج موحد للنشاط الإجرامي:

أدى تنوع النشاط الإجرامي وتطوره إلى ظهور أنماط مستحدثة من الجرائم، مما نتج عنه عدم وجود اتفاق عام مشترك بين الدول حول نماذجالنشاط الإجرامي المتعلق بالجرائم الإلكترونية، فما يكون مباحا في أحد الأنظمة القانونية قد يكون مجرما في نظام آخر، ويمكن إرجاع ذلك إلى عده أسباب وعوامل كاختلاف البيئات والعادات والديانات والثقافات من مجتمع لأخر، [2] أو إلى قصور التشريع ذاته في العديد من الدول وعدم مسايرته لسرعة التقدم التكنولوجي، وهذا ما يسهم في إفلات الكثير من الجناة من المسؤولية الجنائية حول الجرائم الإلكترونية، وارتكاب جرائمهم دون أي تقييد للحدود الجغرافية، هذا ما يؤكد ضرورة التعاون والتنسيق بين الدول حول توحيد النموذج الإجرامي، [3] كما ينتج عن عدم وجود

1عبد الفتاح بيومي حجازي، الدليل الجنائي في جرائم الكمبيوتر والتزوير، المرجع السابق، ص 68.

2حسام محمد نبيل الشنراقي، الجرائم المعلوماتية، جرائم الاعتداء على التوقيع الإلكتروني، المرجع السابق، ص 733.

3براهيمي جمال، التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص 224.

التجريم المزدوج صعوبة اتخاذ إجراءات تسليم المجرمين، إذ يعد هذا الشرطمن أهم الشروط الخاصة بنظام تسليم المجرمين فهو منصوص عليه في أغلب التشريعات الوطنية والصكوك الدولية المعنية، وبالرغم من أهميته إلا أنه قد يكون عقبه أمام التعاون الدولي في مجال تسليم المجرمين بالنسبة للجرائم الإلكترونية ، ذلك أنه من الصعب تحديد فيما إذا كانت النصوص التقليدية لدى الدولة المطلوب منها التسليم يمكن تطبيقها على هذه الجرائم، [1] فلا يجوز مطالبة الدولة بتسليم المجرم قصد محاكمته على سلوك مباح وفقا لقانون هذه الدولة، كما يشترط أن تكون الجرائم المراد التسليم من أجلها تحمل نفس الوصف القانوني وتشترك في الحد الأدنى من العقوبة وهذا ما لا يتحقق غالبا بسبب الاختلاف الكبير بين تشريعات الدول فيما يخص الوصف القانوني للجرائم الإلكترونية والعقوبات المقررة لها، [2] وبالتالي لا يتم التسليم، إذن فاختلاف السياسة التشريعية من دولة لأخرى يؤثر سلبا على الجانب الإجرائي و متابعة الجريمة الإلكترونية وإثباتها.[3]

ولتفادي هذا الإشكال ينبغي توحيد النظم القانونية وباعتبار هذه المسألة مستحيلة التنفيذ فإنه لا مناص من البحث عن وسيلة أخرى كتطوير النظم القانونية المختلفة وتحديثها بما يتناسب مع هذه الجرائم ويحقق توافق بينها، كالقوانين النموذجية التي تتخذ كنموذج تصدر على أساسه مختلف التشريعات قوانينها الداخلية، كالقانون النموذجي المتعلق بالتجارة الإلكترونية وكذا التوقيع الالكتروني اللذان أصدرتها الأمم المتحدة.[4]

2) تباين النظم القانونية الإجرائية:

يشكل اختلاف القوانين الإجرائية من دولة إلى أخرى عقبة أمام المواجهة الدولية للجرائم الإلكترونية لاسيما أن هذه الجرائم تتميز بالطابع الدولي والعابر للحدود، بحيث نجد إجراءات التحقيق والاستدلال والمحاكمة التي تثبت فائدتها وفعاليتها في دولة ما قد تكون عديمة الجدوى أو الفائدة في دوله أخرى، كأن يكون أحد إجراءات التحقيق مشروعا في دولة ما في حين أنه غير مشروع أو مقبول في منظور قانون الدولة الثانية، [5] وبالتالي عدم التنسيق في الإجراءات الجنائية بين الدول يؤدي إلى فشل سلطات إنفاذ القانون في مواجهة الجريمة خاصة إذا كان هذا التباين بخصوص إجراءات استخلاص الدليل الإلكتروني، ولعل أحسن مثال على ذلك التباين التشريعي القائم بين القوانين اللاتينية و الأنجلوساكسونية حول مدى

1لينا محمدالأسدي، مدى فاعلية أحكام القانون الجنائي في مكافحة الجريمة المعلوماتية، المرجع السابق، ص 256.

2براهيمي جمال، التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص 225.

3جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالأنترنت، دار النهضة العربية، القاهرة، 1998، ص 91.

4حسام محمدنبيل الشنراقي، الجرائم المعلوماتية، جرائم الاعتداء على التوقيع الإلكتروني، المرجع السابق، ص 736.

5ليندا بن طالب، الدليل الإلكتروني ودوره في الإثبات الجنائي، المرجع السابق، ص 177.

حجية الدليل الرقمي المستمد من الحاسوب الآلي في الإثبات الجنائي، ففي القوانين ذات الصبغة اللاتينية القائمة على نظام الإثبات الجنائي الحر ومنها القانون الفرنسي والجزائري والمصري، فإن القاضي الجنائي يتمتع بحرية مطلقة في تقدير الأدلة المطروحة أمامه والأخذ بما يراه مناسبا لتكوين قناعته ولو كان هذا الدليل من الأدلة الرقمية أو الإلكترونية، في حين أن النظم الأنجلوساكسونية مثل بريطانيا والولايات المتحدة الأمريكية لا تعترف للدليل الرقمي بحجية الإثبات الجنائي إلا إذا أخذ أحد الأشكال التي حددها المشرع مسبقا في وسائل الإثبات وقدر قيمتها الاقناعية وتم الحصول عليه وفقا لشروط محددة سلفا.[1]

ولتفادي هذا التباين في الأنظمة الإجرائية وجب تكثيف إبرام الاتفاقيات والمعاهدات الثنائية ومتعددة الأطراف بحيث تضع القواعد العامة التي يمكن إتباعها من طرف جميع الدول بما يحقق توافق كبير في أساليب وإجراءات التحقيق وضبط المجرمين، إذ نجد من بين أهم هذه الاتفاقيات اتفاقية بودابست لسنة 2001 وكذا اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية، واتفاقية الأمم المتحدة لمكافحة الفساد، والاتفاقية الأوروبية بشأن الإجرام المعلوماتي، وغيرها من المواثيق الدولية ذات الصلة.[2]

وعليه فإن إبرام هذه الاتفاقيات والمعاهدات الدولية يعتبر أنجع الحلول لمختلف المشاكل التي تطرحها عمليه البحث والتحري في الجرائم الإلكترونية من خلال إدراج أحكام عامة تتفق عليها جميع الدول أو أغلبها سواء من حيث الاختصاص القضائي في هذه الجرائم أو مسائل التعاون الدولي والمساعدة القضائية وكذا تسليم المجرمين في هذه الجرائم.

3) الصعوبات التي تطرحها المساعدة القضائية الدولية:

تفرض الطبيعة العالمية للجريمة الإلكترونية أحيانا تمديد إجراءات التحقيق إلى خارج الإقليم الوطني من أجل ضبط الأدلة التي تكون في إقليم دولة أخرى، وذلك عن طريق طلبات المساعدة القضائية بين الدول، ورغم أهمية هذا الإجراء وتسهيله لتبادل المعلومات والإجراءات الخاصة بمتابعة هذه الجرائم إلا أنه يواجه عدة معيقات أهمها ما يتعلق بمشكلة طلبات الإنابة القضائية الدولية التي تعد من أهم صور المساعدة القضائية الدولية، والتي بموجبها يعهد لدولة ما اتخاذ أي إجراء من إجراءات التحقيق لمصلحة الدولة الثانية مع مراعاة احترام حقوق وحريات الأفراد، حيث تهدف إلى تسهيل إجراءات التحقيق وتذليل العقبات التي تواجه السلطات القضائية خاصة في القضايا التي تأخذ بعدا دوليا، كالجرائم الإلكترونية مثلا، حيث تفرض الطبيعة العالمية لهذه الجرائم على رجال التحقيق تمديد إجراءات البحث

1براهيمي جمال، التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص 236.

2ليندا بن طالب، الدليل الإلكتروني ودوره في الإثبات الجنائي، المرجع السابق، ص 180.

والتحري إلى خارج الإقليم الوطني قصد ضبط أدلة مخزنة في حاسب متواجد في إقليم الدولة الأجنبية، ويتم ذلك بالطرق الدبلوماسية عن طريق وزارة الخارجية وسفارة الدول المعنية، [1] وبالرغم من أهميتها في التصدي للجرائم عامة، إلا أنها تتسم بالبطء والتعقيد والذي يتعارض مع طبيعة الجرائم الإلكترونية وسرعة الشبكة المعلوماتية، وهو الأمر الذي انعكس على عمليات الحصول على أدلة الإثبات في الجرائم الإلكترونية، حيث أن الدولة متلقية الطلب غالبا ما تكون متباطئة في الرد على هذا الطلب سواء بسبب نقص الخبرة لدى الموظفين أو نتيجة الصعوبات اللغوية أو الفوارق في الإجراءات التي تعقد الاستجابة السريعة، [2] إضافة لمشكلة إمكانية رفض الدولة لطلبات المساعدة القضائية واستبعاد تنفيذها خاصة في الجرائم الماسة بأمن وسيادة هذه الدولة ومصالحها الأساسية، وهذا ما سمحت به العديد من الاتفاقيات والمعاهدات الدولية مثل اتفاقية بودابست في مادتها 27فقرة 4، وهذا ما يزيد الأمر تعقيدا ويؤدي إلى تلاشي الدليل الإلكتروني وضياعه، وبالتالي عدم قدرة السلطات القضائية من الوصول إلى المجرم الإلكتروني والكشف عن الجريمة.

ومن أجل التصدي لهذه المشكلات التي أصبحت تأثر سلبا على فعالية المواجهة الدولية للجرائم الإلكترونية، تم إبرام العديد من الاتفاقيات الدولية التي ساهمت في اختصار الوقت والإجراءات عن طريق الاتصال المباشر بين سلطات التحقيق، ونجد في مقدمتها اتفاقية الأمم المتحدة لمكافحة الفساد واتفاقية شنجين الأوروبية حيث نصت جميعها على إمكانية تبادل المعلومات شفويا وعن طريق الاتصال المباشر بين سلطات الدول، [3] إلا أنها قليلة مقارنة وخطورة هذا النوع من الإجرام لذلك كان لزاما أن يكون هناك قنوات وأنظمة اتصال تسمح للجهات والسلطات القضائية المختصة بالتحقيق فيما بينها من خلال تبادل المعلومات والأدلة مع نظيراتها في الخارج، [4] وبالرغم من أن بعض الدول سارعت لإنشاء قنوات اتصال إلا أنها تبقى قليلة مقارنة بالاحتياج الذي يتطلبه التحقيق في هذه الجرائم، فلا يتحقق الهدف من المساعدة القضائية الدولية ما لم يوجد طرق وأنظمة اتصال بين الدول تتبادل من خلالها المعلومات والإجراءات الخاصة بمتابعة الجرائم بصفة عامة خاصة الجرائم المنظمة والعابرة للحدود الوطنية.

1فيروز عوض الكريم صالح ميرغني، إجراءات التحري والضبط في الجرائم الإلكترونية، المرجع السابق، ص 216.

2براهيمي جمال، التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص 238.

3وغيرها من الاتفاقيات والصكوك الدولية منها معاهدة منظمة المؤتمر الإسلامي لمكافحة الإرهاب الدولي لعام 1999، واتفاقية الرياض العربية للتعاون القضائي لعام 1983، معاهدة بودابست لمكافحة جرائم الإنترنت، وكذا توصيات المجلس الأوروبي بشأن الإجراءات الجنائية المتعلقة بتكنولوجيا المعلومات وغيرها، ينظر جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالإنترنت، المرجع السابق، ص 86.

4بثينة حبيباتي، معوقات مكافحة الجريمة المعلوماتية، مجلة العلوم الإنسانية، المرجع السابق، ص 91.

4) مشكلة الاختصاص القضائي في الجرائم المعلوماتية

تعتبر الجرائم الإلكترونية من أكثر الجرائم التي تثير مسألة الاختصاص على المستوى الداخلي والدولي، إذ لا تثير أية إشكال بالنسبة للاختصاص على المستوى الوطني أو المحلي حيث يتم الرجوع في ذلك إلى المعايير والقواعد العامة المحددة قانونا، [1] أما على المستوى الدولي فإنها تثير العديد من الإشكالات نظرا لاختلاف التشريعات والنظم القانونية للدول، و ما تتميز به[2] هذه الجرائم من طابع دولي عابر للحدود الجغرافية، فقد يحدث أن ترتكب الجريمة في إقليم دولة معينه من قبل شخص أجنبي فهنا تكون الجريمة خاضعة للاختصاص الجزائي للدولة الأولى استنادا إلى مبدأ الإقليمية، وتخضع كذلك لاختصاص الدولة الثانية على أساس مبدأ الاختصاص الشخصي، كما قد تكون هذه الجريمة من الجرائم التي تهدد أمن وسلامه دولة أخرى فتدخل في اختصاصها استنادا إلى مبدأ العينية، كما تثار فكرة تنازع الاختصاص القضائي الدولي في حالة تأسيس الاختصاص على مبدأ الإقليمية كما لو قام الجاني ببث الصور الخليعة ذات الطابع الاباحي من إقليم دولة معينة وتم الاطلاع عليها في دول أخرى، ففي هذه الحالة يثبت الاختصاص وفقا لمبدأ الإقليمية لكل دولة من الدول التي مستها الجريمة، [3] ولهذا وجب الرجوع للقواعد العامة التي تنظم انعقاد الاختصاص العالمي للمحاكم الوطنية، وهي نفسها المبادئ التي تحكم تطبيق القانون الجنائي من حيث المكان، وعليه فإلى أي مدى يمكن تطبيق هذه المبادئ على الجرائم الإلكترونية لتحديد المحكمة المختصة بنظر هاته الجرائم وكذا القانون الواجب التطبيق عليها؟

- **تطبيق مبدأ إقليمية القانون الجنائي على الجرائم الإلكترونية:**

من مظاهر سيادة الدولة على إقليمها تطبيق قانونها على كافة الجرائم التي ترتكب في إقليمها أو جزء من إقليمها بغض النظر عن جنسية مرتكبها، ويعتبر مبدأ الإقليمية مبدأ عام والحل الأول عند تطبيق القانون الجنائي من حيث المكان، ولهذا اعتمدته العديد من التشريعات من بينها المشرع الجزائري في

1قام المشرع الجزائري بإنشاء ا أقطاب المتخصصة حيث قام كخطوة أولى بموجب القانون رقم 04/14المعدل والمتمم لقانون الإجراءات الجزائية بتوسيع للاختصاص المحلي لوكيل الجمهورية وقاضي التحقيق وقضاة الحكم إلى دائرة اختصاص محاكم أخرى بخصوص جرائم معينة تتميز بالخطورة ويتطلب مكافحتها كفاءة مهنية عالية من بينها جرائم المساس بنظم المعالجة الآلية للمعطيات ليأتي بعدها المرسوم التنفيذي رقم 16– 348المعدل بالمرسوم رقم 16-267الموافق ل17أكتوبر 2016ليحدد 04محاكم وسع من اختصاصها الإقليمي ليشمل دوائر اختصاص محاكم أخرى، وهي محكمة سيدي محمد بالجزائر العاصمة، و محكمة قسنطينة، ومحكمة وهران، ومحكمة ورقلة.

وفي حالة حصول إشكال في الاختصاص فان الفصل فيه يعود لرئيس المجلس القضائي الذي تقع في دائرته اختصاص المحكمة التي تم تمديد اختصاصها ولا يكون أمره قابلا لأي طعن، و هذا التوجه نحو إنشاء محاكم خاصة في المجال الجنائي إلى جانب محاكم القانون العام يهدف إلى تقريب العدالة من المتقاضين وسرعة التقاضي وخاصة في مثل هذه الجرائم ذات البعد العالمي والسرعة الكبيرة في الانتشار.

2براهيمي جمال، التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص 187.

3ليندا بن طالب، الدليل الإلكتروني ودوره في الإثبات الجنائي، المرجع السابق، ص 184.

المادة03من قانون العقوبات بقولها: "يطبق قانون العقوبات على كافة الجرائم التي ترتكب في أراضي الجمهورية"، كما نصت المادة586من ق ا ج على أنه تعد مرتكبة في الإقليم الجزائري كل جريمة يكون عمل من الأعمال المميزة لأحد أركانها المكونة لها قد تم في الجزائر، [1] كما أخذ المشرع المصري بهذا المبدأ بموجب المادة01من قانون العقوبات المصري والتي تنص على: "تسري أحكام هذا القانون على كل من يرتكب في القطر المصري جريمة من الجرائم المنصوص عليها فيه".[2]

ويستفاد من هذه النصوص السابقة أن أحكام هذا التشريع تسري على جميع الجرائم التي تقع داخل الإقليم بغض النظر عن جنسية مرتكبها سواء كان وطنيا أو أجنبيا، كما يستفاد أن العبرة في تحديد إقليمية القاعدة الجنائية والمحكمة المختصة وبالتالي القانون الواجب التطبيق هي وقوع الجريمة كاملة أو جزء منها في إقليم تلك الدولة.

ولعل أن هذا المبدأ لا يتفق مع جرائم الانترنت نظرا للبعد العالمي لشبكة الانترنت وما تتميز به هذه الجرائم من خصائص، إذ يصعب تحديد مكان وقوع الفعل المجرم مما يؤدي إلى عدم إمكانية إخضاعها لسلطان قانون دولة معينة. [3]

وتطبيقا لهذا المبدأ فان الجرائم المعلوماتية العابرة للحدود تخضع في كثير من الأحيان لأكثر من قانون فإن وقع السلوك في نطاق بلد معين والنتيجة الإجرامية تحققت في نطاق بلد آخر فان قانون كلا البلدين يكون واجب التطبيق على الواقعة، بمعنى أنه يتم تطبيق قانون كل دولة تحقق في نطاقها أحد عناصر الركن المادي للجريمة، وهو ما يؤدي إلى تنازع إيجابي في الاختصاص بين أكثر من تشريع، ولهذا جاءت الاتفاقية الأوروبية لبودابست باعتبارها الإطار المرجعي الدولي الذي يمكن اللجوء إليه عندما يتعلق الأمر بالجرام الواقعة في العالم الافتراضي، وحددت جملة من المعايير يتم بمقتضاها تنسيق الأطراف حدود صلاحيتها، إلا أنها في الأصل لم تخرج عن المعايير التقليدية لتطرح في الأخير منطق التشاور بين الأطراف لتحديد الاختصاص القضائي الأكثر ملائمة في مجال مسألة الاختصاص.[4]

وما قيل بشأن اتفاقية بودابست يقال بشأن الاتفاقية العربية فبالرجوع للمادة30منها نجدها لم تخرج عن الضوابط التي أقرتها الاتفاقية الأوروبية فيما يخص سريان الاختصاص القضائي وإن كانت هذه الأخيرة قد حلت مشكلة تنازع الاختصاص بموجب المادة30في فقرتها الأخيرة حيث أعطت الأولوية في

1ينظر المادة 586من ق ا ج ج.

2ينظر المادة 01من ق ع المصري.

3ليندا بن طالب، الدليل الإلكتروني ودوره في الإثبات الجنائي، المرجع السابق، ص 185.

4بوكر رشيدة، الحماية الجزائية للتعاملات الإلكترونية، المرجع السابق، ص 415.

الاختصاص للدولة التي أخلت الجريمة بأمنها أو بمصالحها، ثم الدولة التي وقعت الجريمة في إقليمها، ثم الدولة التي يكون الشخص المطلوب من رعاياها، وفي حالة ما إذا اتحدت هذه الظروف فتقدم الدولة الأسبق في طلب التسليم وبالتالي يعقد لها الاختصاص.[1]

ولهذا وجب إيجاد قاعدة إجرائية أكثر مرونة تحكم مسألة الاختصاص في هذه الجرائم تتناسب وطبيعتها، إذ ذهب بعض الفقه إلى تحديد مكان واحد وهو مكان وقوع النشاط أو مكان تواجد الجهاز الخادم بالإضافة لمكان تواجد المتهم عند قيامه بتحميل المعطيات.[2]

- **تطبيق مبدأ شخصية القانون الجنائي على الجر ائم الإلكترونية:**

وهو من المبادئ الاحتياطية للاختصاص القضائي ويعني تطبيق القانون الجنائي على كل من يحمل جنسيه الدولة بغض النظر عن مكان وقوعها والمصالح التي مست بها، وإن كان تطبيق هذا المبدأ على الجرائم العادية لا يثير أي إشكال فإن تطبيقه على الجرائم الإلكترونية تعيقه بعض الصعوبات، فبالرغم من أن هذا المبدأ فعال في متابعة المجرم المعلوماتي في أي دولة ارتكب فعله الإجرامي فيها، إلا أنه يصطدم مع صعوبة تحديد الفاعل في هاته الجرائم، لأنه يعتمد بصفة أساسية على الجاني من حيث الكشف على هويته ومن ثم التعرف على جنسيته وهذه المعلومات تعد صعبة وعسيرة في الجرائم الإلكترونية أين يستعمل المشتبه فيه الأسماء المستعارة و تقنيات التشفير والكلمات السرية.[3]

- **تطبيق مبدأ عينية القانون الجنائي على الجر ائم الإلكترونية:**

أمام العجز الذي اكتنف تطبيق مبدأ إقليمية النص الجنائي على الجرائم الإلكترونية وجب البحث عن معيار آخر لتطبيق قواعد القانون الجنائي، تمثل في حماية مصالح الدولة الأساسية وسلامتها وأمنها، فطبقا لهذا المبدأ يطبق القانون الوطني على الجرائم التي ترتكب بالخارج بغض النظر عن جنسية مرتكبها شرط أن تمس هذه الجرائم بالمصالح الأساسية للدولة واستراتيجياتها، وهذا ما نص عليه كل من المشرع الفرنسي في المادة 113 -10والمصري في المادة 2من ق ع، والمشرع الجزائري من خلال المادة566من ق إ ج،[4] كما نص على تطبيق هذا المبدأ بالنسبة للجرائم الإلكترونية بموجب القانون رقم 09/04المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، وذلك في المادة15منه بقولها: "زيادة على قواعد الاختصاص المنصوص عليها في قانون الإجراءات الجزائية تختص

1يراجع المادة 30من الاتفاقية العربية لجرائم تقنية المعلومات المشار إليها سابقا.

2بوكر رشيدة، الحماية الجزائية للتعاملات الإلكترونية، المرجع السابق، ص 416.

3ملياني دلال مولاي، إشكالية الإثبات في جرائم الإنترنت في التشريع الجزائري، المرجع السابق، ص 259.

4ينظر المادة 566من ق ا ج ج.

المحاكم الجزائرية بالنظر في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال المرتكبة في الإقليم الوطني عندما يكون مرتكبها أجنبيا وتستهدف مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الاستراتيجية للاقتصاد الوطني".

والملاحظ على هذه المواد أنها قد وسعت من اختصاص المحاكم لتنظر في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال المرتكبة خارج إقليمها، كما أن المشرع الجزائري قام بإعادة صياغة المادة 566من ق ا ج فقط لتحديد المحكمة المختصة بنظر الجرائم الإلكترونية.

إلا أن تطبيق هذا المبدأ يعترضه الكثير من الإشكالات ومنها مشكلة تعارض تطبيق القانون وفقا لمبدأ العينية مع تطبيق القانون وفقا لمبدأ الإقليمية في حالة عندما تكون الجريمة المرتكبة مجرمة في قانون الدولة التي اقترفت فيها، فهنا تثار مسألة تنازع الاختصاص والقانون الواجب التطبيق بين الدولة المقترفة فيها الجريمة وفقا لمبدأ الإقليمية والدول الأخرى التي مست هذه الجريمة بمؤسساتها ومصالحها وبالتالي فقد يحاكم في هذه الحالة الشخص على فعله مرتين وهذا ما لا يسمح قانونا.[1]

- **تطبيق مبدأ عالمية القانون الجنائي على الجرائم الإلكترونية**

ويراد به تطبيق القانون الجنائي للدولة على كل جريمة يقبض على مرتكبها في إقليم تلك الدولة أي كانت جنسيته وأي كان الإقليم الذي ارتكبت فيه الجريمة، وسواء كانت المصالح التي مستها هذه الجريمة تخص تلك الدولة أو أي دولة أخرى، حيث يمتاز هذا المبدأ بأنه يقرر للقانون الجنائي نطاقا واسعا لتطبيقه، كما يتلاءم جدا مع الطبيعة العالمية للجرائم الإلكترونية إلا أنه يثير بعض الإشكالات بين الدول، كما أن أغلبها لا تأخذ بهذا المبدأ.[2]

وتأسيسا لما سبق ذكره في هذا الباب نخلص للقول أنه تطبيقا لما نادت به أغلب الاتفاقيات والمعاهدات الدولية ذات الصلة بموضوع مكافحة الجرائم الإلكترونية، سارعت أغلب الدول لتبني جملة من الإجراءات والآليات ضمن قوانينها الإجرائية، إذ عملت على تحيين نصوصها الإجرائية التقليدية لتصبح صائغة للتطبيق على هذا النوع من الإجرام، إذ أصبحت المعاينة تتم داخل المسرح الافتراضي بدل المسرح المادي، من طرف خبراء وتقنيين لهم من المعرفة والخبرة الكافية في مجال التعامل مع هذا النوع من المسارح والأدلة، وبالرغم من هذا لم تتوفق القواعد التقليدية في مواكبة تطور الجرائم الإلكترونية، الأمر الذي دعا إلى البحث عن أساليب أخرى أكثر فعالية للتصدي لهذه الجرائم، حيث قامت أغلب التشريعات

1بثينة حبيباتني، معوقات مكافحة الجريمة المعلوماتية، المرجع السابق، ص 92- 93.

2خالد حسن أحمد لطفي، القانون الواجب التطبيق على الجريمة الإلكترونية، ط1، دار الفكر الجامعي، الاسكندرية مصر، سنة 2019، ص 169.

باستحداث نصوص أخرى خاصة لتتناسب والطبيعة التقنية للجريمة والدليل الناتج عنها، مثال تطبيق مختلف صور الترصد الإلكتروني كاعتراض المراسلات وتسجيل الأصوات والتسرب وغيرها، ومن جهة ثانية تبني إجراءات مراقبة الاتصالات الإلكترونية وتفتيش المنظومات المعلوماتية وكذا حجز المعطيات المتواجدة بها والتحفظ على الدليل المتحصل عليه من هذه الإجراءات، ونتيجة أن هذه الأخيرة تعتبر خطيرة وماسة بحقوق وحريات الأفراد ضمنها المشرع شروط وضوابط قانونية تحول دون تعسف سلطات التحقيق في مباشرة هذه الإجراءات.

كما أثارت طبيعة هذه الجرائم عدة مشكلات كونها جرائم مستترة ودليلها غير مرئي وسهل التلاعب به، هذا ما شكل تحديا كبيرا أمام سلطات التحري والتحقيق من حيث تتبع هذه الجريمة والوصول إلى الدليل والتحفظ عليه، ومدى مشروعية طرق الحصول عليه ومقبوليته في الإثبات الجنائي، ناهيك عن قلة خبرة ومعرفة بعض الفئات بالتقنيات الحديثة وكيفية التعامل مع هذا الدليل، كما أثارت الطبيعة العالمية للجريمة الإلكترونية العديد من المشاكل المتمحورة حول مسألة التعاون القضائي الدولي، من حيث تبادل طلبات المساعدة القضائية بين الدول، وكذا الاختصاص القضائي والقانون الواجب التطبيق على الجرائم المرتكبة في إقليم دولة أخرى، مما حذا بالكثير من الدول إلى الانضمام إلى المعاهدات والاتفاقيات ذات الصلة لكي توحد الجهود المبذولة في سبيل التصدي الأمثل لهذه الجرائم.

خاتمة

خاتمــة

بعد ما فرغنا بحمد الله وتوفيقه من دراسة موضوعنا المتمثل في إجراءات التحقيق في الجريمة الإلكترونية والذي حصرناه فقط في مرحلة التحقيق الأولي أو مرحلة البحث والتحري عن الجريمة الإلكترونية، تعرضنا لمجموعة الإشكالات العديدة التي طرحتها المواجهة الإجرائية لهذا النوع من الجرائم، وخلصنا في الأخير لمجموعة من النتائج التي تعتبر إجابة عن هذه التساؤلات المطروحة سابقا، تتمثل أهم هذه النتائج في:

- ✓ نظرا لأن الدور الوقائي في التصدي للجرائم أهم وأسبق من متابعتها بعد وقوعها، اتجهت جهود الدول إلى الوقاية من هذه التهديدات والحيلولة دون وقوعها، عن طريق ممارستها لوظيفتي الضبط الإداري والضبط القضائي، إذ تضطلع سلطات الضبط الإداري بمهمة المحافظة على النظام العام والوقاية من مختلف أشكال التهديدات بما فيها الاعتداءات الإلكترونية، في حين تختص سلطات الضبط القضائي بردع هذه الجرائم ومتابعتها قضائيا.
- ✓ يتجسد دور سلطات الضبط الإداري التقليدية في مجال الوقاية من الجرائم الإلكترونية في إصدار المراسيم الرئاسية والتنفيذية التي تهدف إلى حماية النظام العام وصونه من مختلف أشكال التهديدات ، من بينها تلك التي تحدد وتضبط شروط وكيفيات إقامة خدمات الإنترنت واستغلالها، وتبين أنواع الشبكات ومختلف خدمات المواصلات السلكية واللاسلكية، كما تبين كيفيات سير الهيئات المختصة بمكافحة الجرائم الإلكترونية مثل الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وغيرها، إلى جانب هذه المراسيم يظهر الدور الوقائي لسلطات الضبط الإداري في مجال الوقاية من الجرائم الإلكترونية في سلطتها في إبرام والمصادقة على الاتفاقيات والمعاهدات الدولية المختلفة ذات الصلة بمكافحة هذا النوع من الإجرام، والسهر على احترام القوانين والتنظيمات وضمان حماية الأشخاص والممتلكات.
- ✓ كما يتجسد الدور الوقائي لهذه السلطات من خلال المحافظة على النظام العام والأمن العمومي والحريات العامة وتسيير أعمال الوقاية والمراقبة بما يضمن أمن الإقليم الوطني، وكذا تحديد السياسة الوطنية في مجال الأمن الداخلي للإقليم ضد الهجمات الإلكترونية التي تستهدف الأنظمة المعلوماتية خاصة عندما يتعلق الأمر بمؤسسات سيادية في الدولة.
- ✓ قامت الدولة بتسخير ضبطية إدارية مختصة في الحيلولة دون وقوع الجرائم الإلكترونية من خلال القيام بدوريات في مواقع التواصل الاجتماعي وغرف الدردشة لتتبع النشاطات غير القانونية

ومراقبة ما يحدث داخلها، ولها في ذلك جميع الصلاحيات اللازمة للوقاية من كافة صور الإجرام، كالتفتيش داخل أجهزة الكمبيوتر في مقاهي الإنترنت أو في إحدى المؤسسات للتأكد من صلاحية البرمجيات المستعملة وكشف النشاطات غير المشروعة.

- ✓ كما أن دور المؤسسات الخاصة بتنظيم البريد والمواصلات السلكية واللاسلكية يبرز بشكل كبير في مجال الوقاية من الجرائم المتعلقة بالمحتوى الرقمي نظرا لطبيعة هذه الأخيرة وعلاقتها بشبكة الاتصالات العالمية ومختلف التكنولوجيات الناتجة عنها، وذلك من خلال تحسين الخدمات والاتصالات الإلكترونية، المشاركة في تحديد عناصر الإطار القانوني والتنظيمي للحفاظ على الحقوق والحريات الأساسية في الفضاء السيبراني، واحترام أخلاقيات تكنولوجيات الإعلام والاتصال.
- ✓ أمام عجز سلطات الضبط التقليدية في ضبط الجرائم الإلكترونية استحدثت أغلب التشريعات سلطات ضبط مستقلة تمارس مهمة الضبط الإداري الإلكتروني، نجد من بينها سلطة ضبط البريد والاتصالات الإلكترونية، وبعض السلطات المختصة بالتصديق الإلكتروني، وكذا الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، والسلطة الوطنية لحماية المعطيات ذات الطابع الشخصي، والوكالات المختصة في تأمين الأنظمة المعلوماتية بما يضمن قلة الانتهاكات والاعتداءات التي تحدث في البيئة الرقمية، حيث خولها القانون جملة من الصلاحيات الواسعة تمثلت في آليات وقائية وأخرى قمعية تهدف من خلالها إلى المحافظة على النظام والأمن العموميين، وذلك بممارستها الدور التنظيمي من خلال اقتراح القوانين والتنظيمات وكذا الدور الرقابي من خلال مراقبة نشاطات إنشاء واستغلال خدمات الإنترنت المختلفة ، وحماية البيانات والمعلومات المتبادلة بين المتعاملين ، وإجراء التحريات من أجل منع وحظر النشاطات إذا ما رأت أنها لا تستوفي الشروط أو تمس بالنظام العام عن طريق أساليب متعددة كأسلوب حظر أو حجب المواقع الإلكترونية غير المشروعة وغيرها من الوسائل الوقائية.
- ✓ تعتبر مرحلة البحث والتحري من أبرز وأهم المراحل التي يستعان بها لمواجهة الجرائم بما فيها الجرائم الإلكترونية، ولهذا تم تسخير ضبطية قضائية مختصة للقيام بمباشرة إجراءاتها تعرف ب "شرطة الإنترنت"، إذ تباشر اختصاصاتها على المستويين الدولي والداخلي، وتختلف عن نظيرتها التقليدية كونها لا تعتمد على التدريبات المادية التي يتلقاها هؤلاء لقيامهم بمهمة الضبط، وإنما تعتمد على قوة تكوين البناء العلمي والتكنولوجي لأفرادها، ومعرفتهم بكيفيات التعامل مع

التقنيات الحديثة، إذ يتلقى ضباط الشرطة القضائية المختصين في التحري عن هذه الجرائم دورات تدريبية في هذا المجال تنظمها سلطات كل دولة مع تفاوت درجة الأهمية التي تليها الدولة لهذه الدورات التكوينية، إذ نجد الدول الأجنبية وخاصة الأنجلوساكسونية واللاتينية أكثر اهتمام من الدول العربية في هذا المجال.

- ✓ دعت العديد من المواثيق والصكوك الدولية وعلى رأسها اتفاقية بودابست لمكافحة جرائم تقنية المعلومات، إلى إنشاء وتأسيس سلطات مختصة تباشر عملية التحري والتحقيق في هذه الجرائم، هذا ما استجابت له العديد من الدول الأجنبية والعربية ومنها الجزائر، حيث أنشأت المصلحة المركزية لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، والتي تعمل بالتنسيق مع جهاز الشرطة القضائية والشرطة العلمية على المستوى المركزي، أما على المستوى المحلي تم استحداث عدة فرق لمكافحة الجريمة المعلوماتية وذلك على مستوى كل الولايات.
- ✓ كما خلصنا إلى أن الطبيعة الخاصة للجرائم الإلكترونية دعت المشرع الجزائي إلى إعادة تقييم بعض القواعد الإجرائية التقليدية (إجراءات البحث والتحري)، وجعلها صائغة للاستعمال في مجال الجرائم الإلكترونية، كونها لم تستجيب لخصوصية هذا النوع من الجرائم ، فضلا عن استحداث قواعد إجرائية خاصة تتلاءم والطبيعة التقنية التي تتميز بها الجريمة الإلكترونية، كالمراقبة الإلكترونية وتفتيش المنظومة المعلوماتية، والترصد الإلكتروني...الخ، وهو ما قامت به العديد من التشريعات الأجنبية والعربية، من بينها المشرع الفرنسي والأمريكي والمشرع المصري و الجزائري من خلال تعديل قانون الإجراءات الجزائية وكذا استحداث قوانين خاصة بمتابعة هذه الجرائم، من بينها القانون رقم 04/09 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها الذي نظم من خلاله المشرع الجزائري كيفية مراقبة الاتصالات الإلكترونية وتفتيش المنظومة المعلوماتية وحجز المعطيات التي تشكل جريمة، كما ألزم من خلال هذا القانون مقدمي خدمات الإنترنت ببعض الالتزامات التي من شأنها الحيلولة دون وقوع الجريمة.
- ✓ تبين من خلال الدراسة أنه رغم فعالية الإجراءات المستحدثة والخاصة في مواجهة الجريمة الإلكترونية إلا أنها تشكل خطرا كبيرا يهدد الحق في الخصوصية الذي كفلته الدساتير والقوانين، نظرا لما تتيحه هذه الإجراءات لسلطات البحث والتحري من إمكانية الاطلاع على أسرار وخصوصيات الأفراد، هذا ما جعل المشرع الجزائي يحيطها بجملة من الضوابط والشروط من

بينها حصر حالات اللجوء لهذه الإجراءات في الحالات الضرورية للتحري والتحقيق وغيرها، علاوة على ضرورة الحصول على إذن مسبق من السلطة المختصة قبل مباشرة هذه الإجراءات، لتكون كضمانات تحمي المشتبه فيه أو المتهم من تعسف سلطات التحري والتحقيق عند مباشرته لهذه الإجراءات.

- ✓ يتم التبليغ عن الجرائم الإلكترونية بنفس الطريقة التي يتم فيها التبليغ عن الجرائم العادية، وذلك إما عن طريق البلاغ المادي، أو المعنوي، أو البلاغ الرقمي الذي يتم بإرسال رسالة إلى عنوان البريد الإلكتروني للجهات المختصة بالتحري والتحقيق، وذلك عن طريق ملأ استمارة رقمية متواجدة في المواقع المخصصة لتلقي البلاغات والشكاوى، والتي استحدثتها أغلب الدول وخاصة الدول الأجنبية كونها تتعامل معها كثيرا، هذا ما حقق سرعة وفعالية في تلقي البلاغات والتنقل إلى مسرح الجريمة قبل ضياع الأدلة، في حين نجد أن الدول العربية وخاصة الجزائر رغم تفعيلها لبعض المواقع إلا أنها لا تتعامل معها كثيرا، وهذا راجع لنقص خبرة المحقق من جهة ونقص معرفة الشاكي أو المتضرر من الجريمة بالتعامل مع هذه المواقع، ومن جهة أخرى نقص ثقافة التبليغ لدى الكثيرين والتي ترجع لعدة أسباب كخوف الضحية على سمعته أو اعتباره وغيرها.
- ✓ أظهرت الدراسة أنه مهما أرست الدول من تشريعات وأجهزة وآليات لمكافحة هذا النوع من الإجرام إلا أنها لن تستطيع التصدي لها بمفردها نظرا لطابعها العالمي والدولي، هذا ما فرض فكرة التعاون الدولي بصورتيه، التعاون الأمني أو الشرطي الذي تجسد في إنشاء أجهزة متخصصة بالتحقيق في هذه الجرائم في مختلف الدول، ومن جهة أخرى التعاون القضائي الدولي والذي تجسد في إبرام الاتفاقيات والمعاهدات الدولية والإقليمية الثنائية ومتعددة الأطراف في هذا المجال، وخلق قنوات اتصال تسمح للسلطات بالاتصال بمثيلاتها من الدول الاجنبية، وكذا التنسيق معها بخصوص إجراءات متابعة الجرائم الإلكترونية. من خلال تبادل المساعدات القضائية من أجل ضمان التحقيق الفعال في هذه الجرائم.
- ✓ تتمتع الأدلة الإلكترونية والتقنية بقيمة علمية قاطعة في الدلالة على الحقائق التي تتضمنها، إلا أنها تخضع من حيث مسألة قبولها لمطلق تقدير القاضي الجزائي، الذي يتمتع بدور إيجابي في مناقشة وموازنة القيمة القانونية للدليل الإلكتروني قبل أن يطمئن إليه، شأنه في ذلك شأن باقي الأدلة، إذ يشترط توافر جملة من الشروط لقبول هذا الدليل منها شرط الصحة والمطابقة، وكذا أن يكون الدليل تم الحصول عليه بطرق مشروعة.

- ✓ كما أظهرت الدراسة أنه من المشكلات التي تواجه سلطات البحث والتحري، الطبيعة التكوينية للدليل الإلكتروني كونه ذو طبيعة رقمية غير مرئية، كما أنه قابل للتغيير والحذف، من قبل المجرم في حد ذاته أو من قبل المحقق بسبب خطأ أو تقصير منه في التعامل مع هذا الدليل، نتيجة نقص خبرته ومعرفته بالتقنيات الحديثة، هذا ما حذا بالكثير من الدول إلى تنظيم دورات تدريبية من أجل تكوين ضباط الشرطة القضائية وكذا المحققين والقضاة في مجال تكنولوجيات الإعلام والاتصال والتقنيات المتطورة بما يعود بالفائدة على أساليب البحث والتحري في هذه الجرائم.
- ✓ كما تثير الطبيعة الخاصة التي تتميز بها هذه الجرائم في حد ذاتها عدة إشكالات، كالطابع العابر للحدود الذي يثير العديد من المشاكل القانونية، من بينها سيادة الدول التي تقف حاجزا أمام سلطات التحري عندما يستوجب البحث والتفتيش عن أدلة الجريمة خارج الإقليم الوطني أو في عدة أقاليم أخرى، خاصة في ظل نقص الآليات الدولية التي تضمن التعاون القضائي والأمني بين هذه الدول في مجال مكافحة الجرائم الإلكترونية، مما أثار فكرة تنازع الاختصاص القضائي بين القاضي الوطني والقاضي الأجنبي في حالة تأسيس الاختصاص على مبدأ الإقليمية، إذ وضعت أغلب الدول معيار لفض هذا النزاع حيث يؤول الاختصاص إلى المحكمة الواقع في دائرتها مكان وقوع النشاط أو مكان الجهاز الخادم.
- ✓ رغم التفاوت بين أغلب التشريعات خاصة اللاتينية والأنجلوساكسونية حول مسألة قبول الدليل الإلكتروني، إلا أنها استقرت كلها حول وجوب التمييز بين أمرين أساسيين للحكم على القيمة الثبوتية للأدلة الإلكترونية، حيث تمثل الأمر الأول في القيمة العلمية القاطعة للدليل الإلكتروني والأمر الثاني في الظروف والملابسات التي تحيط بهذا الدليل، فالقاضي ليس له أن ينازع فيما أسفرت عليه تكنولوجيا المعلوماتية والعلوم التقنية والعلمية وإنما له أن يقدر الظروف والملابسات التي أحاطت باستخلاص الدليل ويبني بذلك قناعته عليها.

وتأسيسا على ما تم ذكره والتوصل إليه من نتائج يمكن أن نخلص للقول بأن المشرع الجزائي توفق إلى حد ما في سياسيته الإجرائية التي استحدثها لمواجهة هذا النوع من الجرائم، محاولا التماشي مع الخصوصية والطابع التقني للأدلة الإلكترونية، إلا أنه يبقى هناك بعض القصور الذي يعتري هذه السياسة من عدة جوانب، وعلى ضوء هذا حاولنا تقديم جملة من الحلول لأهم هذه الإشكالات سنعرضها في شكل توصيات أو اقتراحات وذلك على النحو التالي:

- ✓ نأمل من المشرع الجزائي وخاصة المشرع الجزائري العمل على إصدار قانون جنائي رقمي خاص بشقيه الموضوعي والإجرائي، حيث يتضمن الشق الموضوعي مختلف أشكال الجرائم الإلكترونية المنصوص عليها ضمن قوانين متفرقة، مع تجريم بعض الأفعال التي لم يتم النص عليها لحد الساعة، وإدراج الجزاءات المقررة لها، أما عن الشق الإجرائي فيضمنه كل إجراءات وأساليب التحري والتحقيق الخاصة لتتلاءم مع طبيعة هذه الجرائم، تفاديا للقصور التشريعي والثغرات القانونية التي قد يستفيد منها المجرم المعلوماتي للإفلات من المتابعة والعقاب.
- ✓ العمل على إنشاء أجهزة ووحدات أمنية متخصصة في التحقيق في هذه الجرائم، يكون لديها الخبرة والإلمام الكافي بالجوانب التقنية والفنية، عن طريق تكثيف البرامج والدورات التدريبية وعدم اقتصارها على المستوى الوطني فقط بل إتاحة المشاركة في الدورات المنعقدة في الدول الأجنبية، مما يساعد في تبادل المعلومات والخبرات والاطلاع على كل المستجدات الحاصلة في مجال تقنية المعلومات ومجال التحقيق في الجرائم المستحدثة.
- ✓ كما ندعو إلى إنشاء منظمة شرطة عربية تهتم بالتنسيق بين الدول العربية في مجال مكافحة الجرائم الإلكترونية، كمنظمة الإنتربول والأفريبول والأوروبول وغيرها.
- ✓ ضرورة تكثيف التعاون والتنسيق بين الدول من أجل تطوير وتحديث تشريعاتها الجزائية وخاصة الإجرائية التي تعنى بمكافحة الجريمة الإلكترونية، وهذا من خلال إبرام الاتفاقيات والمعاهدات الدولية الثنائية ومتعددة الأطراف في مجال التعاون الدولي في إطار مكافحة الجرائم الإلكترونية هذا من جهة، ومن جهة أخرى انضمام الدول لهاته المعاهدات والاتفاقيات مثل اتفاقية بودابست للإجرام المعلوماتي، باعتبارها من أنشط وأهم الاتفاقيات في مجال مكافحة الجرائم الإلكترونية.
- ✓ على المشرع إعادة النظر في تسيير مقاهي الإنترنت وفرض التزامات على مقدمي خدمات الإنترنت ومسيري هذه المقاهي، مع الرقابة الصارمة للأنشطة التي يقدمونها، من خلال مسك دفاتر مؤشر عليها من قبل الجهات المختصة مثلا، لتسجيل هوية الزبون ورقم جهاز الحاسوب وتاريخ ووقت استعماله، قصد الرجوع إليه لضرورات التحري والتحقيق بما يضمن عدم إفلات المجرم من المتابعة.

- ✓ على الدولة إتباع سياسة الحجب والحظر للمواقع الإباحية والإرهابية خاصة وفرض الرقابة عليها، مما يساعد في تقليل نسبة هذه النوعية من الجرائم.
- ✓ العمل بنتائج البحوث العلمية والدراسات الخاصة بهذه الجرائم وأخذها بعين الاعتبار عند وضع السياسة الجنائية من طرف المشرع الجنائي.
- ✓ العمل على نشر الوعي والثقافة الإلكترونية، عن طريق تفعيل دور الإعلام في نشر التوعية الوقائية من الجرائم الإلكترونية، وتفعيل دور المجتمع المدني من خلال تنظيم الندوات والملتقيات والأيام الدراسية للتحسيس بخطورة هذه الجرائم وتفاديها.
- ✓ تضمين المناهج الدراسية أساسيات وأخلاقيات استخدام الإنترنت، وكذا استحداث مقياس حول مواضيع الإجرام الإلكتروني وآليات مكافحته، يدرس على مستوى الجامعات العربية خاصة على مستوى كليات الحقوق والعلوم القانونية.

وبهذا تكون دراستنا اكتملت عناصرها فإن كان فيها كمال فهو لله سبحانه وتعالى، وإن اعتراها النقص وهذا شيء طبيعي فهو مني ولما لا و أنا بشر أجتهد فأخطئ وأصيب، فإن أصبت فأجري على الله وإن أخطأت فأدعوه ألا يحرمني أجر المجتهدين.

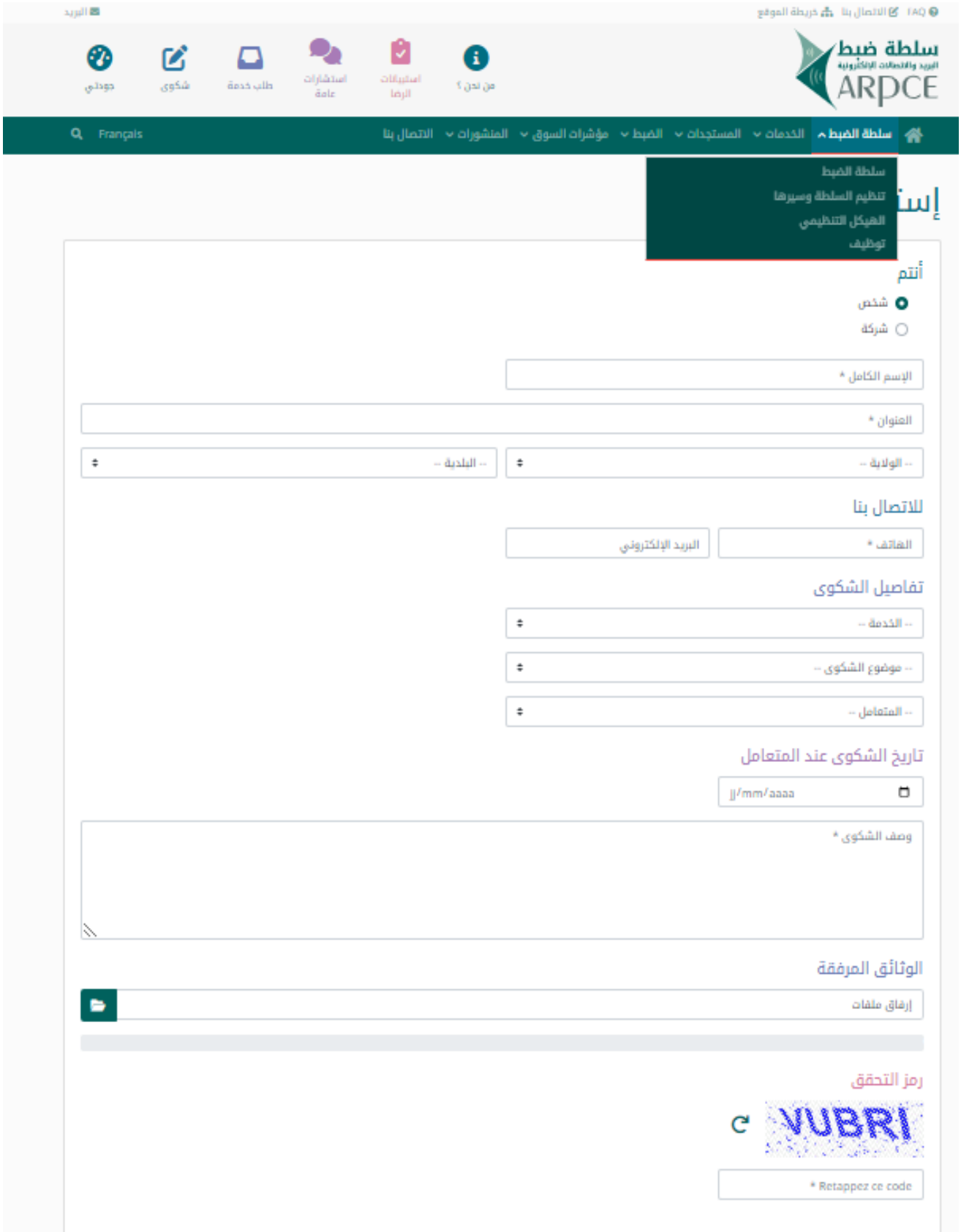
وأسأل الله أن يهدينا إلى سواء السبيل وأن يجعل هذا العمل خالصا لوجهه الكريم وأن ينفع به، وآخر دعو انا أن الحمد لله رب العالمين.

تم بحمد الله

الملاحق

ملحق رقم 01: نموذج تقديم شكوى على الموقع المخصص لمصالح الدرك الوطني

ملحق رقم 02: نموذج تقديم شكوى على موقع سلطة ضبط البريد والاتصالات الإلكترونية.



ملحق رقم 03: نموذج تقديم شكوى على مستوى موقع شرطة أبو ظبي.

ملحق رقم 04: دليل أرقام مصالح الشرطة لكل الولايات الجزائرية.

ترقيم الولاية	المصلحة	أرقام الهاتف		العنوان
		المحـــول الهـــاتفي	الفاكس	
1	أمـــن ولايـــة أدرار	049 36 10 20	049 36 10 20	حي عيسات إديـر، أدرار
		049 36 10 30	049 36 10 30	
		049 36 10 40	049 36 10 40	
2	أمـــن ولايـــة الشـلف	027 77 10 00	027 77 41 56	طريـق محمـد طويـل الشـلف
		027 77 10 62		
		027 77 16 27		
3	أمـــن ولايـــة الأغـــواط	029 15 21 24	029 15 21 11	طريـق محمـد رزوق معمـورة الأغـواط
		029 15 21 26		
		029 15 21 28		
4	أمـــن ولايـــة أم البواقـي	032 52 14 09	032 52 14 09	نهـج هـواري بومـدين أم البـواقـي
		032 52 14 33	032 52 14 33	
		032 52 14 10	032 52 14 10	
5	أمـــن ولايـــة باتنـــة	033 85 79 44	033 85 79 44	حـي المجـزرة بـاتنـة
		033 80 70 05	033 80 70 05	
		033 80 70 06	033 80 70 06	
6	أمـــن ولايـــة بجايـة	034 16 36 46	034 16 36 46	حـي حرفـي طـاوس بجايـة
		034 16 36 03	034 16 36 03	
		034 16 36 16	034 16 36 16	
7	أمـــن ولايـــة بسكـــرة	033 50 20 08	033 50 20 10	طريـــق 08 مـــارس حـــافة الـــواد بســـكرة
		033 50 20 09		
		033 50 20 10		
8	أمـــن ولايـــة بشـــار	049 24 49 02	049 24 49 02	طريـق طـالب عبـد الله بشـار
		049 24 49 03	049 24 49 03	
		049 24 49 37	049 24 49 37	
9	أمـــن ولايـــة البليـدة	025 23 79 27	025 23 79 06	طريـق بلقاسـم أوزري البليـدة
		025 23 79 28		
		025 23 79 29		
10	أمـــن ولايـــة البويـرة	026 72 77 01	026 72 77 08	طريـق 20 أوت 1955 البويـرة
		026 72 77 02		
		026 72 77 03		
11	أمـــن ولايـــة تمنراسـت	029 31 80 32	029 31 80 05	حي أمشوان تمنراسـت
		029 31 80 33		

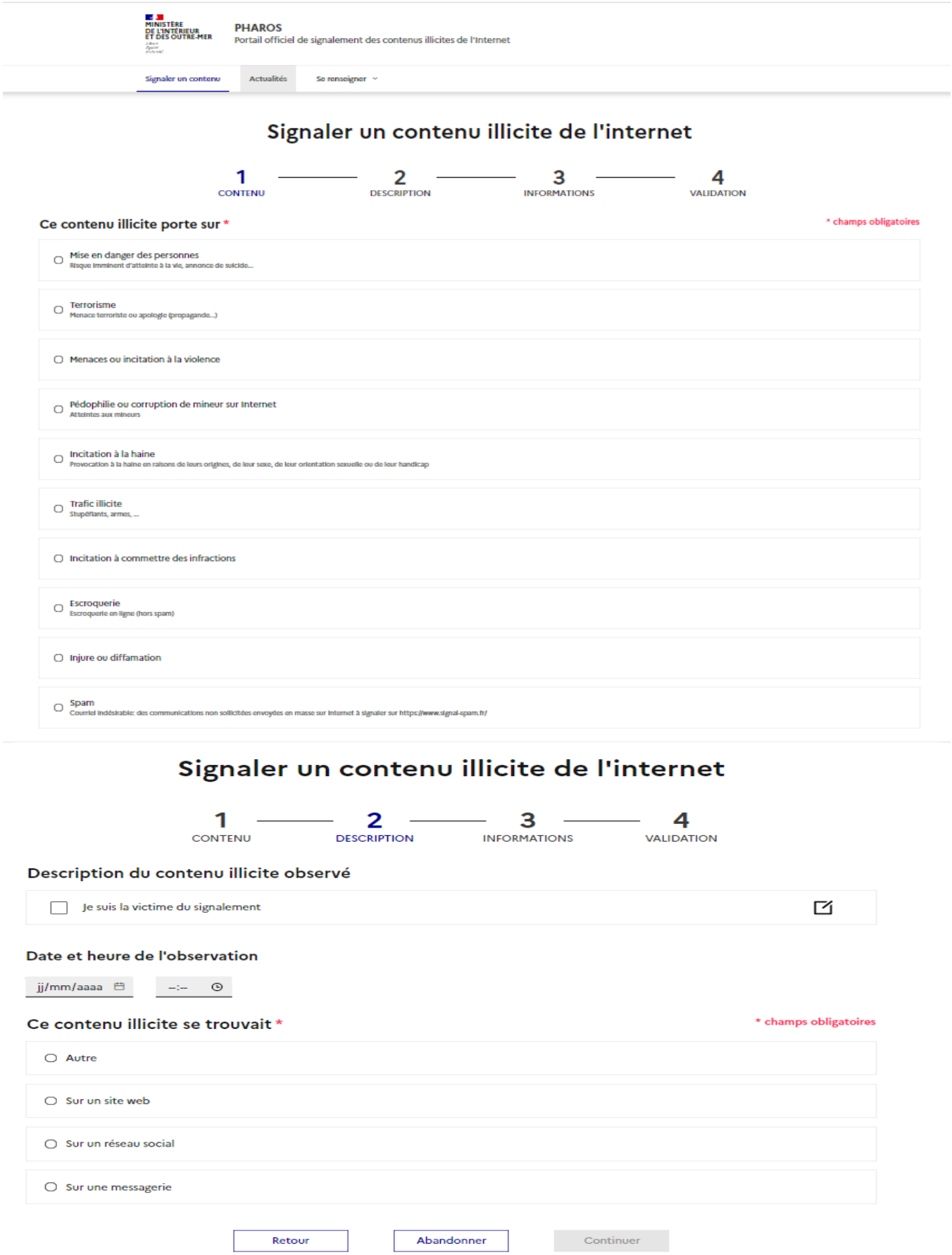
12	أمـــن ولايـــة تبســة	037 51 00 31 037 51 00 38 037 51 00 43	037 51 00 42	طريـــق الشـــرطيين الشهـــداء تبســة
13	أمـــن ولايـــة تلمســـان	043 41 79 05 043 41 79 08 043 41 79 06	043 41 79 02	طريـق بـاسـتـور تلمســـان
14	أمـــن ولايـــة تيـــارت	046 20 35 04 046 20 35 02	046 20 35 04 046 20 35 02	طريـق الســوقـر تيـــارت
15	أمـــن ولايـــة تيـــزي وزو	026 19 49 30 026 19 49 31 026 19 49 32 026 19 49 33	026 19 49 17	طريـق العـربي بن مهيـدي تيـزي وزو
16	أمـــن ولايـــة الجزائـــر	023 49 82 00 023 49 82 11	023 49 82 41	شـــارع العقيد عميـــروش الجزائـــر
17	أمـــن ولايـــة الجلفـــة	027 90 87 01 027 90 87 02 027 90 87 03	027 90 87 22	طريـــق الجـــامعة، زيـــان عاشـــور الجلفـــة
18	أمـــن ولايـــة جيجـــل	034 47 20 46 034 49 64 96 034 49 64 97	034 47 15 51	شـــارع الصومـــام جيجـــل
19	أمـــن ولايـــة سطيـــف	036 44 15 33 036 44 15 34 036 44 15 35 036 44 15 36 036 44 15 37	036 44 15 33 036 44 15 34 036 44 15 35 036 44 15 36 036 44 15 37	شـــارع الشيخ العيفـــة ســطيـــف
20	أمـــن ولايـــة سعيـــدة	048 42 89 12 048 42 89 10	048 42 89 12 048 42 89 10	طريـــق الإخـــوة فـــاطمي سعيـــدة
21	أمـــن ولايـــة سكيكـــدة	038 75 68 05 038 75 68 09 038 75 68 21 038 75 68 22	038 75 21 93	طريـــق 20 أوت 1955 سكيكـــدة
22	أمـــن ولايـــة سدي بلعبـــاس	048 71 13 09 048 71 13 10 048 71 13 11	048 71 13 09 048 71 13 10 048 71 13 11	شـــارع ميصـــالي الحـــاج سيـــدي بلعبـــاس

23	أمـــن ولايـــة عنابـــة	038 40 25 00 038 40 25 01 038 40 25 02 038 40 25 03 038 40 25 04 038 40 14 23	038 40 25 08	طريـــق شنـــافي محمـــد عنـــابة
24	أمـــن ولايـــة قالمـــة	037 26 06 30 037 26 00 34 037 26 06 45 037 26 06 46	037 26 06 30 037 26 00 34 037 26 06 45 037 26 06 46	طريـــق مجنـــدي محمـــد قـــالمة
25	أمـــن ولايـــة قسنطينـــة	031 92 64 81 031 91 75 95 031 91 17 98 031 91 18 60 031 91 18 65 031 92 75 95 031 92 79 38	031 92 64 81 031 91 75 95 031 91 17 98 031 91 18 60 031 91 18 65 031 92 75 95 031 92 79 38	طريـــق عامـــر حمـــو الكـــدية قسنطينـــة
26	أمـــن ولايـــة المديـــة	025 73 49 07 025 73 49 12 025 73 49 15	025 73 49 16	طريـــق جيـــش التحريـــر الوطنـــي بمحاذاة ثـــانوية فخـــار المديـــة
27	أمـــن ولايـــة مستغـــانم	045 35 28 37 045 35 28 36	045 35 28 37 045 35 28 36	نهـــج بـــن يحـــي بلقـــاسم مستغـــانم
28	أمـــن ولايـــة المسيـــلة	035 35 01 00 035 35 01 01 035 35 01 03	035 35 01 02	طريـــق شريـــد عبـــد الحفيـــظ المسيلة
29	أمـــن ولايـــة معســـكر	045 75 35 10 045 75 35 11	045 75 35 10 045 75 35 11	طريـــق الشهيـــد مصطفـــى الوالـــي ، منطقـــة رقم 12 معسكـــر
30	أمـــن ولايـــة ورقلـــة	029 60 00 61 029 60 00 62 029 60 00 63	029 60 00 64	منطقة النشاطات بجانب الوحدة المركزية للحماية المدنية، مقابل الإقامة الجامعية 2000 سريـــر ورقلـــة

31	أمـــن ولايـــة وهـــران	041 24 28 80 041 24 28 88 041 24 28 89 041 24 28 92	041 24 28 81	شـــارع جيـش التحـرير الوطنـي وهـران
32	أمـــن ولايـــة البيـــض	049 61 40 01 049 61 40 03	049 61 40 01 049 61 40 03	طريق بالهواري الحاج براهيم ، الحي الإداري البيض
33	أمـــن ولايـــة إليـــزي	029 41 10 71 029 41 10 72 029 41 10 73	029 41 10 72	القطاع الحضري الجديد، مقابل مقر الولاية إليزي
34	أمـــن ولايـــة برج بوعريـريـج	035 72 29 13 035 72 29 14 035 72 29 15	035 72 29 13 035 72 29 14 035 72 29 15	نهج الجمهورية برج بوعريريج
35	أمـــن ولايـــة بومـــرداس	024 94 94 12 024 94 94 13 024 94 94 14	024 94 94 15	حي 20 أوت بومرداس
36	أمـــن ولايـــة الطارف	038 30 14 01 038 30 14 03 038 30 17 80 038 30 18 67	038 30 22 47	الطريق الوطني رقم 44 الطارف
37	أمـــن ولايـــة تنـــدوف	049 37 29 02 049 37 29 03	049 37 29 02 049 37 29 03	حي موساني ، تندوف
38	أمـــن ولايـــة تسمسيـلت	046 57 55 30 046 57 55 36	046 57 55 30 046 57 55 36	شـــارع 24 فيفري تسمسيلت
39	أمـــن ولايـــة الـــوادي	032 11 29 04 032 11 29 05 032 11 29 06	032 11 29 04	حي المجاهدين الوادي
40	أمـــن ولايـــة خنشلـــة	032 72 70 33 032 72 70 35 032 72 70 41	032 72 70 33 032 72 70 35 032 72 70 41	حي شابور،17 أكتوبر خنشلة
41	أمـــن ولايـــة سوق أهـراس	037 72 22 26 037 72 22 28 037 72 22 30 037 72 28 02	037 72 22 26 037 72 22 28 037 72 22 30	حي بوثليجة العابد سوق أهراس
42	أمـــن ولايـــة تيبـــازة	024 37 19 25 024 37 19 26 024 37 19 27	024 37 19 03	بجانب حي 1700 مسكن عدل تيبازة

43	أمـــن ولايـــة ميلـة	031 47 62 26 031 47 62 27 031 47 62 28	031 47 62 08	شـــارع بن شولاق ميلة
44	أمـــن ولايـــة عين الدفلى	027 51 29 09 027 51 29 13 027 51 29 27	027 51 29 18	طريق الأمير عبد القادر عين الدفلى
45	أمـــن ولايـــة النعامـة	049 59 52 59 049 59 52 60	049 59 52 59	الطريق الوطني رقم 06 النعامة
46	أمـــن ولايـــة عين تيمـــوشنت	043 62 09 03 043 79 48 58	043 62 09 03 043 79 48 58	طريق تارقة عين تيموشنت
47	أمـــن ولايـــة غرداية	029 28 24 10 029 28 25 00 029 28 26 00	029 28 25 00	حي الحاج مسعود غرداية
48	أمـــن ولايـــة غليـزان	046 74 09 12 046 74 09 20	046 74 09 12	طريق عواد بن جبار غليزان
49	أمـــن ولايـــة تيميـون	049 30 03 66 049 30 05 16	049 30 03 66	طريق فلسطين تيمون
50	أمـــن ولايـــة برج باجـي مختـــار	049 32 67 02	049 32 67 03	طريق تمنراست، أمام مقر الولاية برج باجي مختار
51	أمـــن ولايـــة أولاد جـــلال	033 66 66 70 033 66 66 71	033 66 68 47	طريق العربي بن مهيدي أولاد جلال
52	أمـــن ولايـــة بنـــي عبـــاس	049 28 53 30 049 28 41 57	049 28 53 30 049 28 41 57	شارع فلسطين بني عباس
53	أمـــن ولايـــة إن صـــالـح	029 36 55 51	029 36 52 77	وسط مدينة عين صالح
54	أمـــن ولايـــة إن قـــزام	029 35 41 32	029 35 41 32	وسط مدينة عين قزام
55	أمـــن ولايـــة تـــوقـــرت	029 66 39 35 029 66 39 50	029 66 39 93	ساحة الحرية لبلدية توقرت، توقرت
56	أمـــن ولايـــة جـــانـــت	029 48 04 42 029 48 04 43	029 48 06 11	حي إفـــري جـــانت
57	أمـــن ولايـــة المـــغير	032 18 65 47 032 18 66 63	032 18 63 55	حي السعادة المغير
58	أمـــن ولايـــة المنيعـة	029 21 20 30 029 21 15 58	029 21 27 78	طريق العربي بن مهيدي المنيعة

ملحق رقم 05: نموذج تقديم شكوى على مستوى المنصة الرقمية الفرنسية "فاروس".



ملحق رقم 06: نموذج الإدلاء بشهادة على مستوى موقع مصالح الشرطة الجزائرية.

الملحق رقم07: إحصائيات حول تطور معدل الجرائم الإلكترونية في السنوات الأربع الأخيرة.

الجمهورية الجزائرية الديقمراطية الشعبية

المديرية العامة للأمن الوطني

أمن ولاية تيارت / المصلحة الولائية للشرطة القضائية (SWPJ)

فرقة مكافحة الجرائم المعلوماتية

احصائيات حول معدل تطور الجريمة الإلكترونية في السنوات الأخيرة (2019-2022)

نوع الجريمة	عدد القضايا سنة (2019)	عدد القضايا سنة (2020)	عدد القضايا سنة (2021)	عدد القضايا سنة (2022)
المساس بحرمة الحياة الخاصة للأشخاص	56	44	8	9
النصب والاحتيال عبر الأنترنت	3	3	9	17
التهديد والابتزاز	4	7	0	7
قرصنة حسا ت الكترونية	4	2	3	6
حيازة أسلحة من الصنف الثاني	1	2	0	0
إهانة هيئة نظامية	1	5	8	4
وضع منشورات تحريضية	8	6	4	6
عرض منشورات لأنظار الجمهور من شأنها الاضرار لمصلحة الوطنية	1	2	0	0
انتحال هوية الغير	4	3	5	8
التحريض على التجمهر	0	1	5	2
الدعوة إلى العنف من خلال خطاب الكراهية والتمييز	0	1	0	0
عرض مقاطع فيديو وتسجيلات في متناول الجمهور	0	2	0	0

الاساءة إلى شخص رئيس الجمهورية	0	1	0	0
وضع منشورات تتضمن الاشادة لأفعال الإرهابية	0	0	1	0
التحريض على الهجرة غير الشرعية	0	0	1	1
عرض أوراق نقدية مزورة للبيع	0	0	1	2
عرض أجهزة كشف المعادن للبيع	0	0	0	1
عرض شهادات طبية مزورة للبيع	0	0	0	1
عرض أجهزة بلوتوث للبيع	0	0	0	1
عرض الأجهزة الحساسة للبيع	0	0	0	1
القذف والسب	0	0	45	33
ممارسة نشاط تجاري بدون رخصة	0	0	1	0

ملحق رقم 08: إحصائيات حول قضايا الجرائم الإلكترونية المتابعة على مستوى محكمة تيارت

الجمهورية الجزائرية الديمقراطية الشعبية

وزارة العدل

مجلس قضاء تيارت

محكمة تيارت

رئيس أمانة الضبط

تيارت: 08 نوفمبر 2022

معلومات إحصائية

- بناء على طلب الأنسة: حايطي فاطيمة، طالبة دكتوراه تخصص حقوق، أستاذة مؤقتة بكلية الحقوق والعلوم السياسية بجامعة ابن خلدون بتيارت، والمتمثل في طلب إحصائيات قضائية متعلقة بالجريمة الإلكترونية المعروضة أمام محكمة تيارت خلال الفترة ما بين سنة 2019 و 30 جوان 2022، بغرض مساعدتها في إعداد أطروحة الدكتوراه الموسومة بعنوان "إجراءات التحقيق في الجرائم الإلكترونية".

نقدم نحن رئيس أمانة ضبط محكمة تيارت هذه المعلومات الإحصائية.

الجريمة	2019	2020	2021	السداسي الأول 2022
المادة 394 مكرر 1 فقرة 01 من قانون العقوبات: الدخول أو البقاء عن طريق الغش في منظومة المعالجة الآلية للمعطيات	-	-	-	02 قضايا 02 متهمين
المادة 394 مكرر 1 من قانون العقوبات: الإدخال والإزالة والتعديل بطريق الغش للمعطيات في نظام المعالجة الآلية للمعطيات	07 قضايا 10 متهمين	10 قضايا 42 متهمين	06 قضايا 07 متهمين	-
المادة 394 مكرر 5 من قانون العقوبات: المشاركة أو الإتفاق بغرض الإعداد لجريمة أو أكثر من جرائم المساس بأنظمة المعالجة الآلية للمعطيات	-	-	03 قضايا 12 متهمين	-
المساس بحرمة الحياة الخاصة	10 قضايا 10 متهمين	11 قضايا 13 متهمين	13 قضايا 15 متهمين	-
النصب	01 قضية 02 متهمين	-	-	-
التهديد بالتشهير	-	06 قضايا 07 متهمين	-	01 قضية 01 متهم
القذف	-	-	-	03 قضايا 03 متهمين

ملاحظة هامة: سلمت هذه الوثيقة بغرض استعمالها في حدود ما يسمح به القانون.

رئيس أمانة الضبط

ملحق رقم 09: الاعلان العالمي لحقوق الإنسان

الاعلان العالمي لحقوق الانسان

اعتُمد بموجب قرار الجمعية العامة ٢١٧ ألف) د-٣) المؤرخ في ١٠ كانون الأول/ديسمبر1948

في ١٠ كانون الأول/ديسمبر ١٩٤٨، اعتمدت الجمعية العامة للأمم المتحدة الإعلان العالمي لحقوق الإنسان وأصدرته، ويرد النص الكامل للإعلان في الصفحات التالية. وبعد هذا الحدث التاريخي، طلبت الجمعية العامة من البلدان الأعضاء كافة أن تدعو لنص الإعلان و"أن تعمل على نشره وتوزيعه وقراءته وشرحه، ولاسيما في المدارس والمعاهد التعليمية الأخرى، دون أي تمييز بسبب المركز السياسي للبلدان أو الأقاليم".

الديباجة

لما كان الاعتراف بالكرامة المتأصلة في جميع أعضاء الأسرة البشرية وبحقوقهم المتساوية الثابتة هو أساس الحرية والعدل والسلام في العالم.

ولما كان تناسي حقوق الإنسان وازدراؤها قد أفضيا إلى أعمال همجية آذت الضمير الإنساني، وكان غاية ما يرنو إليه عامة البشر انبثاق عالم يتمتع فيه الفرد بحرية القول والعقيدة ويتحرر من الفزع والفاقة.

ولما كان من الضروري أن يتولى القانون حماية حقوق الإنسان لكيلا يضطر المرء آخر الأمر إلى التمرد على الاستبداد والظلم.

ولما كانت شعوب الأمم المتحدة قد أكدت في الميثاق من جديد إيمانها بحقوق الإنسان الأساسية وبكرامة الفرد وقدره وبما للرجال والنساء من حقوق متساوية وحزمت أمرها على أن تدفع بالرقي الاجتماعي قدماً وأن ترفع مستوى الحياة في جو من الحرية أفسح.

ولما كانت الدول الأعضاء قد تعهدت بالتعاون مع الأمم المتحدة على ضمان اطراد مراعاة حقوق الإنسان والحريات الأساسية واحترامها.

ولما كان للإدراك العام لهذه الحقوق والحريات الأهمية الكبرى للوفاء التام بهذا التعهد.

فإن الجمعية العامة تنادي بهذا الإعلان العالمي لحقوق الإنسان على أنه المستوى المشترك الذي ينبغي أن تستهدفه كافة الشعوب والأمم حتى يسعى كل فرد وهيئة في المجتمع، واضعين على الدوام هذا الإعلان نصب أعينهم، إلى توطيد احترام هذه الحقوق والحريات عن طريق التعليم والتربية واتخاذ إجراءات مطردة، قومية وعالمية، لضمان الاعتراف بها ومراعاتها بصورة عالمية فعالة بين الدول الأعضاء ذاتها وشعوب البقاع الخاضعة لسلطانها.

المادة ١

يولد جميع الناس أحراراً متساوين في الكرامة والحقوق، وقد وهبوا عقلاً وضميراً وعليهم أن يعامل بعضهم بعضاً بروح الإخاء.

المادة ٢

لكل إنسان حق التمتع بكافة الحقوق والحريات الواردة في هذا الإعلان، دون أي تمييز، كالتمييز بسبب العنصر أو اللون أو الجنس أو اللغة أو الدين أو الرأي السياسي أو أي رأي آخر، أو الأصل الوطني أو الاجتماعي أو الثروة أو الميلاد أو أي وضع آخر، دون أية تفرقة بين الرجال والنساء. وفضلا عما تقدم فلن يكون هناك أي تمييز أساسه الوضع السياسي أو القانوني أو الدولي لبلد أو البقعة التي ينتمي إليها الفرد سواء كان هذا البلد أو تلك البقعة مستقلا أو تحت الوصاية أو غير متمتع بالحكم الذاتي أو كانت سيادته خاضعة لأي قيد من القيود.

المادة ٣

لكل فرد الحق في الحياة والحرية وسلامة شخصه.

المادة ٤

لايجوز استرقاق أو استعباد أي شخص، ويحظر الاسترقاق وتجارة الرقيق بكافة أوضاعهما.

المادة ٥

لايعرض أي إنسان للتعذيب ولا للعقوبات أو المعاملات القاسية أو الوحشية أو الحاطة بالكرامة.

المادة ٦

لكل إنسان أينما وجد الحق في أن يعترف بشخصيته القانونية.

المادة ٧

كل الناس سواسية أمام القانون ولهم الحق في التمتع بحماية متكافئة عنه دون أية تفرقة، كما أن لهم جميعا الحق في حماية متساوية ضد أي تميز يخل بهذا الإعلان وضد أي تحريض على تمييز كهذا.

المادة ٨

لكل شخص الحق في أن يلجأ إلى المحاكم الوطنية لإنصافه عن أعمال فيها اعتداء على الحقوق الأساسية التي يمنحها له القانون.

المادة ٩

لا يجوز القبض على أي إنسان أو حجزه أو نفيه تعسفاً.

المادة ١٠

لكل إنسان الحق، على قدم المساواة التامة مع الآخرين، في أن تنظر قضيته أمام محكمة مستقلة نزيهة نظراً عادلاً علنياً للفصل في حقوقه والتزاماته وأية تهمة جنائية توجه إليه.

المادة ١١

(١) كل شخص متهم بجريمة يعتبر بريئاً إلى أن تثبت إدانته قانوناً بمحاكمة علنية تؤمن له فيها الضمانات الضرورية للدفاع عنه.

(٢) لا يدان أي شخص من جراء أداة عمل أو الامتناع عن أداة عمل إلا إذا كان ذلك يعتبر جرماً وفقاً للقانون الوطني أو الدولي وقت الارتكاب، كذلك لا توقع عليه عقوبة أشد من تلك التي كان يجوز توقيعها وقت ارتكاب الجريمة.

المادة ١٢

لا يعرض أحد لتدخل تعسفي في حياته الخاصة أو أسرته أو مسكنه أو مراسلاته أو لحملات على شرفه وسمعته، ولكل شخص الحق في حماية القانون من مثل هذا التدخل أو تلك الحملات.

المادة ١٣

(١) لكل فرد حرية التنقل واختيار محل إقامته داخل حدود كل دولة.

(٢) يحق لكل فرد أن يغادر أية بلاد بما في ذلك بلده كما يحق له العودة إليه.

المادة ١٤

(١) لكل فرد الحق في أن يلجأ إلى بلاد أخرى أو يحاول الالتجاء إليها هرباً من الاضطهاد.

(٢) لا ينتفع بهذا الحق من قدم للمحاكمة في جرائم غير سياسية أو لأعمال تناقض أغراض الأمم المتحدة ومبادئها.

المادة ١٥

(١) لكل فرد حق التمتع بجنسية ما.

(٢) لا يجوز حرمان شخص من جنسيته تعسفاً أو إنكار حقه في تغييرها.

المادة ١٦

(١) للرجل والمرأة متى بلغا سن الزواج حق التزوج وتأسيس أسرة دون أي قيد بسبب الجنس أو الدين، ولهما حقوق متساوية عند الزواج وأثناء قيامه وعند انحلاله.

(٢) لا يبرم عقد الزواج إلا برضى الطرفين الراغبين في الزواج رضى كاملاً لا إكراه فيه.

(٣) الأسرة هي الوحدة الطبيعية الأساسية للمجتمع ولها حق التمتع بحماية المجتمع والدولة.

المادة ١٧

(١) لكل شخص حق التملك بمفرده أو بالاشتراك مع غيره.

(٢) لا يجوز تجريد أحد من ملكه تعسفاً.

المادة ١٨

لكل شخص الحق في حرية التفكير والضمير والدين، ويشمل هذا الحق حرية تغيير دينه أو عقيدته، وحرية الإعراب عنهما بالتعليم والممارسة وإقامة الشعائر ومراعاتها سواء أكان ذلك سراً أم مع الجماعة.

المادة ١٩

لكل شخص الحق في حرية الرأي والتعبير، ويشمل هذا الحق حرية اعتناق الآراء دون أي تدخل، واستقاء الأنباء والأفكار وتلقيها وإذاعتها بأية وسيلة كانت دون تقيد بالحدود الجغرافية.

المادة ٢٠

(١) لكل شخص الحق في حرية الاشتراك في الجمعيات والجماعات السلمية.

(٢) لا يجوز إرغام أحد على الانضمام إلى جمعية ما.

المادة ٢١

(١) لكل فرد الحق في الاشتراك في إدارة الشؤون العامة لبلاده إما مباشرة وإما بواسطة ممثلين يختارون اختياراً حراً.

(٢) لكل شخص نفس الحق الذي لغيره في تقلد الوظائف العامة في البلاد.

(٣) إن إرادة الشعب هي مصدر سلطة الحكومة، ويعبر عن هذه الإرادة بانتخابات نزيهة دورية تجري على أساس الاقتراع السري وعلى قدم المساواة بين الجميع أو حسب أي إجراء مماثل يضمن حرية التصويت.

المادة ٢٢

لكل شخص بصفته عضواً في المجتمع الحق في الضمانة الاجتماعية وفي أن تحقق بوساطة المجهود القومي والتعاون الدولي وبما يتفق ونظم كل دولة ومواردها الحقوق الاقتصادية والاجتماعية والتربوية التي لاغنى عنها لكرامته وللنمو الحر لشخصيته.

المادة ٢٣

(١) لكل شخص الحق في العمل، وله حرية اختياره بشروط عادلة مرضية كما أن له حق الحماية من البطالة.

(٢) لكل فرد دون أي تمييز الحق في أجر متساو للعمل.

(٣) لكل فرد يقوم بعمل الحق في أجر عادل مرض يكفل له ولأسرته عيشة لائقة بكرامة الإنسان تضاف إليه، عند اللزوم، وسائل أخرى للحماية الاجتماعية.

(٤) لكل شخص الحق في أن ينشئ وينضم إلى نقابات حماية لمصلحته.

المادة ٢٤

لكل شخص الحق في الراحة، وفي أوقات الفراغ، ولاسيما في تحديد معقول لساعات العمل وفي عطلات دورية بأجر.

المادة ٢٥

(١) لكل شخص الحق في مستوى من المعيشة كاف للمحافظة على الصحة والرفاهية له ولأسرته، ويتضمن ذلك التغذية والملبس والمسكن والعناية الطبية وكذلك الخدمات الاجتماعية اللازمة، وله الحق في تأمين معيشته في حالات البطالة والمرض والعجز والترمل والشيخوخة وغير ذلك من فقدان وسائل العيش نتيجة لظروف خارجة عن إرادته.

(٢) للأمومة والطفولة الحق في مساعدة ورعاية خاصتين، وينعم كل الأطفال بنفس الحماية الاجتماعية سواء أكانت ولادتهم ناتجة عن رباط شرعي أو بطريقة غير شرعية.

المادة ٢٦

(١) لكل شخص الحق في التعلم، ويجب أن يكون التعليم في مراحله الأولى والأساسية على الأقل بالمجان، وأن يكون التعليم

الأولى إلزامياً وينبغي أن يعمم التعليم الفني والمهني، وأن ييسر القبول للتعليم العالي على قدم المساواة التامة للجميع وعلى أساس الكفاءة.

(٢) يجب أن تهدف التربية إلى إنماء شخصية الإنسان إنماء كاملاً، وإلى تعزيز احترام الإنسان والحريات الأساسية وتنمية التفاهم والتسامح والصداقة بين جميع الشعوب والجماعات العنصرية أو الدينية، وإلى زيادة مجهود الأمم المتحدة لحفظ السلام.

(٣) للآباء الحق الأول في اختيار نوع تربية أولادهم.

المادة ٢٧

(١) لكل فرد الحق في أن يشترك اشتراكاً حراً في حياة المجتمع الثقافي وفي الاستمتاع بالفنون والمساهمة في التقدم العلمي والاستفادة من نتائجه.

(٢) لكل فرد الحق في حماية المصالح الأدبية والمادية المترتبة على إنتاجه العلمي أو الأدبي أو الفني.

المادة ٢٨

لكل فرد الحق في التمتع بنظام اجتماعي دولي تتحقق بمقتضاه الحقوق والحريات المنصوص عليها في هذا الإعلان تحققاً تاما.

المادة ٢٩

(١) على كل فرد واجبات نحو المجتمع الذي يتاح فيه وحده لشخصيته أن تنمو نمواً حراً كاملاً.

(٢) يخضع الفرد في ممارسة حقوقه وحرياته لتلك القيود التي يقررها القانون فقط، لضمان الاعتراف بحقوق الغير وحرياته واحترامها ولتحقيق المقتضيات العادلة للنظام العام والمصلحة العامة والأخلاق في مجتمع ديمقراطي.

(٣) لا يصح بحال من الأحوال أن تمارس هذه الحقوق ممارسة تتناقض مع أغراض الأمم المتحدة ومبادئها.

المادة ٣٠

ليس في هذا الإعلان نص يجوز تأويله على أنه يخول لدولة أو جماعة أو فرد أي حق في القيام بنشاط أو تأدية عمل يهدف إلى هدم الحقوق والحريات الواردة فيه.

ملحق رقم 10: المرسوم الرئاسي المتضمن تصديق الجزائر على اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية.

العدد 09
السّنة التّاسعة والثّلاثون

الأحد 27 ذو القعدة عام 1422 هـ
الموافق 10 فبراير سنة 2002 م

الجمهوريّة الجزائريّة
الديمقراطيّة الشّعبيّة

الجريدة الرسميّة

اتفاقات دوليّة ، قوانين ، ومراسيم
قرارات وآراء ، مقرّرات ، مناشير ، إعلانات وبلاغات

الاشتراك سنوي	الجزائر تونس المغرب ليبيا موريطانيا	بلدان خارج دول المغرب العربيّ
	سنة	سنة
النّسخة الأصليّة	1070,00 د.ج	2675,00 د.ج
النّسخة الأصليّة وترجمتها ...	2140,00 د.ج	5350,00 د.ج
		تزاد عليها نفقات الإرسال

الإدارة والتّحرير
الأمانة العامّة للحكومة
WWW.JORADP.DZ
الطّبع والاشتراك
المطبعة الرّسميّة
7 و9 و13 شارع عبد القادر بن مبارك – الجزائر
الهاتف 65.18.15 الى 17 ح.ج.ب 50 – 3200 الجزائر
Télex : 65 180 IMPOF DZ
بنك الفلاحة والتّنمية الرّيفيّة 68 KG 060.300.0007
حساب العملة الأجنبيّة للمشتركين خارج الوطن
بنك الفلاحة والتّنمية الرّيفيّة 060.320.0600.12

ثمن النّسخة الأصليّة 13,50 د.ج
ثمن النّسخة الأصليّة وترجمتها 27,00 د.ج
ثمن العدد الصّادر في السّنين السّابقة : حسب التّسعيرة.
وتسلّم الفهارس مجّانا للمشتركين.
المطلوب إرفاق لفيفة إرسال الجريدة الأخيرة سواء لتجديد الاشتراكات أو للاحتجاج أو لتغيير العنوان.
ثمن النّشر على أساس 60,00 د.ج للسّطر.

مرسوم رئاسيّ رقم 02 - 55 مؤرّخ في 22 ذي القعدة عام 1422 الموافق 5 فبراير سنة 2002، يتضمّن التّصديق، بتحفّظ، على اتفاقية الأمم المتّحدة لمكافحة الجريمة المنظمة عبر الوطنية، المعتمدة من طرف الجمعية العامّة لمنظمة الأمم المتّحدة يوم 15 نوفمبر سنة 2000.

إنّ رئيس الجمهوريّة،

- بناء على تقرير وزير الدّولة، وزير الشّؤون الخارجيّة،

- وبناء على الدّستور، لا سيّما المادّة 77-9 منه،

- وبعد الاطّلاع على اتفاقية الأمم المتّحدة لمكافحة الجريمة المنظمة عبر الوطنية، المعتمدة من طرف الجمعية العامّة لمنظمة الأمم المتّحدة يوم 15 نوفمبر سنة 2000.

يرسم ما يأتي :

المادّة الأولى : يصدّق، بتحفّظ، على اتفاقية الأمم المتّحدة لمكافحة الجريمة المنظمة عبر الوطنية، المعتمدة من طرف الجمعية العامّة لمنظمة الأمم المتّحدة يوم 15 نوفمبر سنة 2000، وتنشر في الجريدة الرّسميّة للجمهوريّة الجزائريّة الدّيمقراطيّة الشّعبيّة.

المادّة 2 : ينشر هذا المرسوم في الجريدة الرّسميّة للجمهوريّة الجزائريّة الدّيمقراطيّة الشّعبيّة.

حرّر بالجزائر في 22 ذي القعدة عام 1422 الموافق 5 فبراير سنة 2002.

عبد العزيز بوتفليقة

اتفاقية الأمم المتّحدة لمكافحة الجريمة المنظمة عبر الوطنية

المادّة الأولى

بيان الغرض

الغرض من هذه الاتفاقية تعزيز التعاون على منع الجريمة المنظمة عبر الوطنية ومكافحتها بمزيد من الفعالية.

المادّة 2

استخدام المصطلحات

لأغراض هذه الاتفاقية :

(أ) يقصد بتعبير "جماعة إجرامية منظمة" جماعة محدّدة البنية، مؤلّفة من ثلاثة أشخاص أو أكثر، موجودة لفترة من الزّمن وتقوم معا بفعل مدبّر بهدف ارتكاب واحدة أو أكثر من الجرائم الخطيرة أو الجرائم المقرّرة وفقا لهذه الاتفاقية، من أجل الحصول، بشكل مباشر أو غير مباشر، على منفعة ماليّة أو منفعة مادية أخرى،

(ب) يقصد بتعبير "جريمة خطيرة" سلوك يمثل جرما يعاقب عليه بالحرمان من الحرية لمدّة قصوى لا تقلّ عن أربع سنوات أو بعقوبة أشدّ،

(ج) يقصد بتعبير "جماعة محدّدة البنية" جماعة غير مشكّلة عشوائيا لغرض الارتكاب الفوري لجرم ما، ولا يلزم أن تكون لأعضائها أدوار محدّدة رسميا، أو أن تستمر عضويتهم فيها أو أن تكون لها بنية متطوّرة، أو

(د) يقصد بتعبير " الممتلكات" الموجودات أيا كان نوعها، سواء أكانت مادية أم غير مادية، منقولة أم غير منقولة، ملموسة أم غير ملموسة ، والمستندات أو الصكوك القانونية التي تثبت ملكية تلك الموجودات أو وجود مصلحة فيها،

(هـ) يقصد بتعبير "عائدات إجرامية" أي ممتلكات تتأتى أو يتحصّل عليها، بشكل مباشر أو غير مباشر، من ارتكاب جرم،

(و) يقصد بتعبير "التجميد" أو "الضبط" الحظر المؤقّت لنقل الممتلكات أو تبديلها أو التصرّف فيها أو تحريكها أو إخضاعها للحراسة أو السيطرة المؤقّتة بناء على أمر صادر عن محكمة أو سلطة مختصة أخرى،

(ز) يقصد بتعبير "المصادرة"، التي تشمل الحجز حيثما انطبق، التجريد النهائي من الممتلكات بموجب أمر صادر عن محكمة أو سلطة مختصّة أخرى،

(ح) يقصد بتعبير "الجرم الأصلي" أي جرم نتأت منه عائدات يمكن أن تصبح موضوع جرم حسب التعريف الوارد في المادة 6 من هذه الاتفاقية،

(ط) يقصد بتعبير "التسليم المراقب" الأسلوب الّذي يسمح لشحنات غير مشروعة أو مشبوهة بالخروج من إقليم دولة أو أكثر أو المرور عبره أو دخوله، بمعرفة سلطاته المختصة وتحت مراقبتها، بغية التحري عن جرم ما وكشف هوية الأشخاص الضالعين في ارتكابه،

(ي) يقصد بتعبير "منظمة إقليمية للتكامل الاقتصادي" منظمة شكّلتها دول ذات سيادة في منطقة ما، أعطتها الدّول الأعضاء فيها الاختصاص فيما يتعلق بالمسائل التي تنظمها هذه الاتفاقية وخوّلتها حسب الأصول ووفقا لنظامها الدّاخلي سلطة التوقيع أو التصديق عليها أو قبولها أو الموافقة عليها أو الانضمام إليها. وتنطبق الإشارات إلى "الدّول الأطراف" بمقتضى هذه الاتفاقية على هذه المنظمات في حدود نطاق اختصاصها.

المادّة 3

نطاق الانطباق

1- تنطبق هذه الاتفاقية، باستثناء ما تنصّ عليه خلافا لذلك، على منع الجرائم التالية والتحرّي عنها وملاحقة مرتكبيها :

(أ) الجرائم المقرّرة بمقتضى المواد 5 و6 و8 و23 من هذه الاتفاقية، و

(ب) الجريمة الخطيرة حسب التعريف الوارد في المادّة 2 من هذه الاتفاقية.

حيثما يكون الجرم ذا طابع عبر وطني وتضلع فيه جماعة إجرامية منظمة.

2- لأغراض الفقرة 1 من هذه المادّة، يكون الجرم ذا طابع عبر وطني إذا :

(أ) ارتُكب في أكثر من دولة واحدة، أو

(ب) ارتُكب في دولة واحدة ولكن جانبا كبيرا من الإعداد أو التخطيط له أو توجيهه أو الإشراف عليه جرى في دولة أخرى، أو

(ج) ارتكب في دولة واحدة، ولكن ضلعت في ارتكابه جماعة إجرامية منظمة تمارس أنشطة إجرامية في أكثر من دولة واحدة أو،

(د) ارتُكب في دولة واحدة، ولكن له آثارا شديدة في دولة أخرى.

المادّة 4

صون السيادة

1- يتعيّن على الدّول الأطراف أن تؤدّي التزاماتها بمقتضى هذه الاتفاقية على نحو يتفق مع مبدأي المساواة في السيادة والحرمة الإقليمية للدول، ومع مبدأ عدم التدخّل في الشؤون الدّاخلية للدول الأخرى.

2- ليس في هذه الاتفاقية ما يبيح لدولة طرف أن تقوم في إقليم دولة أخرى بممارسة الولاية القضائية وأداء الوظائف التي يناط أداؤها حصرا بسلطات تلك الدّولة الأخرى بمقتضى قانونها الداخلي.

المادّة 5

تجريم المشاركة في جماعة إجرامية منظمة

1- يتعيّن على كلّ دولة طرف أن تعتمد ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم الأفعال التالية جنائيا عندما تُرتكب عمدا :

(أ) أي من الفعلين التاليين أو كليهما، باعتبارهما جريمتين جنائيتين متميّزتين عن الجرائم التي تنطوي على الشروع في النشاط الإجرامي أو إتمامه :

"1"- الاتفاق مع شخص آخر أو أكثر على ارتكاب جريمة خطيرة لغرض له صلة مباشرة أو غير مباشرة بالحصول على منفعة ماليّة أو منفعة مادية أخرى، وينطوي، حيثما يشترط القانون الدّاخلي ذلك، على فعل يقوم به أحد المشاركين يساعد على تنفيذ الاتفاق، أو تضلع فيه جماعة إجرامية منظمة،

"2"- قيام الشخص، عن علم بهدف جماعة إجرامية منظمة ونشاطها الإجرامي العامّ أو بعزمها على ارتكاب الجرائم المعنية، بدور فاعل في :

أ) الأنشطة الإجرامية للجماعة الإجرامية المنظمة،

ب) أنشطة أخرى تضطلع بها الجماعة الإجرامية، مع علمه بأنّ مشاركته ستسهم في تحقيق الهدف الإجرامي المبيّن أعلاه،

(ب) تنظيم ارتكاب جريمة خطيرة تضلع فيها جماعة إجرامية منظمة، أو الإيعاز بارتكاب تلك الجريمة أو المساعدة أو التحريض عليه أو تيسيره أو إسداء المشورة بشأنه.

2- يمكن الاستدلال على العلم أو القصد أو الهدف أو الغرض أو الاتفاق المشار إليه في الفقرة 1 من هذه المادّة من الملابسات الوقائعية الموضوعية.

3 - يتعيّن على الدّول الأطراف التي يشترط قانونها الدّاخلي ضلوع جماعة إجرامية منظمة لتجريم الأفعال المنصوص عليها في الفقرة 1 (أ) "1" من هذه المادّة أن تكفل شمول قانونها الدّاخلي جميع الجرائم الخطيرة التي تضلع فيها جماعات إجرامية منظمة. ويتعيّن على تلك الدّول الأطراف، وكذلك على الدّول الأطراف التي يشترط قانونها الدّاخلي إتيان فعل يساعد على تنفيذ الاتفاق، لتجريم الأفعال المنصوص عليها في الفقرة 1 (أ) "1" من هذه المادّة، أن تبلغ الأمين العامّ للأمم المتحدة بذلك وقت توقيعها على هذه الاتفاقية أو وقت إيداعها صكوك التصديق عليها أو قبولها أو إقرارها أو الانضمام إليها.

المادّة 6

تجريم غسل العائدات الإجرامية

1- يتعيّن على كلّ دولة طرف أن تعتمد، وفقا للمبادئ الأساسية لقانونها الدّاخلي، ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم الأفعال التالية جنائيا في حال ارتكابها عمدا :

(أ) "1" تحويل الممتلكات أو نقلها، مع العلم بأنها عائدات إجرامية، بغرض إخفاء أو تمويه المصدر غير المشروع لتلك الممتلكات أو مساعدة أي شخص ضالع في ارتكاب الجرم الأصلي الّذي تأتت منه على الإفلات من العواقب القانونية لفعلته،

"2" إخفاء أو تمويه الطبيعة الحقيقية للممتلكات أو مصدرها أو مكانها أو كيفية التصرّف فيها أو حركتها أو ملكيتها أو الحقوق المتعلّقة بها، مع العلم بأنها عائدات إجرامية،

(ب) ورهنا بالمفاهيم الأساسية لنظامها القانوني :

"1" اكتساب الممتلكات أو حيازتها أو استخدامها مع العلم، وقت تلقيها، بأنها عائدات إجرامية،

"2" المشاركة في ارتكاب أي من الجرائم المقرّرة وفقا لهذه المادّة، أو التواطؤ أو التآمر على ارتكابها، ومحاولة ارتكابها والمساعدة والتحريض على ذلك وتسهيله وإسداء المشورة بشأنه.

2- لأغراض تنفيذ أو تطبيق الفقرة 1 من هذه المادّة :

(أ) يتعيّن على كلّ دولة طرف أن تسعى إلى تطبيق الفقرة 1 من هذه المادّة على أوسع مجموعة من الجرائم الأصلية،

(ب) يتعيّن على كلّ دولة طرف أن تدرج في عداد الجرائم الأصلية كلّ جريمة خطيرة، حسب التعريف الوارد في المادّة 2 من هذه الاتفاقية، والجرائم المقرّرة وفقا للمواد 5 و8 و23 من هذه الاتفاقية.

وفي حالة الدول الأطراف التي تحدّد تشريعاتها قائمة جرائم أصلية معيّنة، يتعيّن عليها أن تدرج في تلك القائمة، كحدّ أدنى، مجموعة شاملة من الجرائم المرتبطة بجماعات إجرامية منظمة.

(ج) لأغراض الفقرة الفرعية (ب)، يتعيّن أن تشمل الجرائم الأصلية الجرائم المرتكبة داخل وخارج الولاية القضائية للدّولة الطّرف المعنية. غير أنه لا تكون الجرائم المرتكبة خارج الولاية القضائية للدّولة الطّرف جرائم أصلية إلاّ إذا كان الفعل ذو الصلة فعلا إجراميا بمقتضى القانون الدّاخلي للدّولة التي ارتكب فيها وأن يمثل فعلا إجراميا بمقتضى القانون الدّاخلي للدّولة الطّرف التي تنفّذ أو تطبّق هذه المادّة إذا ارتكب هناك.

(د) يتعيّن على كلّ دولة طرف أن تزوّد الأمين العامّ للأمم المتحدة بنسخ من قوانينها المنفّذة لهذه المادّة ونسخ من أي تغييرات تجرى على تلك القوانين لاحقا أو بوصف لها.

(هـ) إذا كانت المبادئ الأساسية للقانون الدّاخلي للدّولة الطّرف تقتضي ذلك، يجوز النصّ على أنّ الجرائم المبيّنة في الفقرة 1 من هذه المادّة لا تنطبق على الأشخاص الذين ارتكبوا الجرم الأصلي.

(و) يجوز الاستدلال على عنصر العلم أو القصد أو الغرض، الّذي يلزم توافره في أي جرم مبيّن في الفقرة 1 من هذه المادّة، من الملابسات الوقائعية الموضوعية.

المادّة 7

تدابير مكافحة غسل الأموال

1- يتعيّن على كلّ دولة طرف :

(أ) أن تنشىء نظاما داخليا شاملا للرقابة والإشراف على المصارف والمؤسّسات الماليّة غير المصرفية وكذلك، حيثما يقتضي الأمر، سائر الهيئات المعرّضة بشكل خاصّ لغسل الأموال، ضمن نطاق اختصاصها، من أجل ردع وكشف جميع أشكال غسل الأموال، ويتعيّن أن يشدّد ذلك النظام على متطلبات تحديد هوية الزبون وحفظ السجلات والإبلاغ عن المعاملات المشبوهة.

(ب) أن تكفل، دون إخلال بأحكام المادّتين 18 و27 من هذه الاتفاقية، قدرة الأجهزة الإدارية والرقابية وأجهزة إنفاذ القوانين وسائر الأجهزة المكرّسة لمكافحة غسل الأموال (بما فيها السلطات القضائية، حيثما يقضي القانون الدّاخلي بذلك) على التعاون وتبادل المعلومات على الصعيدين الوطني والدولي ضمن نطاق الشروط التي يفرضها قانونها الداخلي، وأن تنظر، لأجل تلك الغاية، في إنشاء وحدة استخبارات ماليّة تعمل كمركز وطني لجمع وتحليل وتعميم المعلومات عما يحتمل وقوعه من غسل للأموال.

2- يتعيّن على الدول الأطراف أن تنظر في تنفيذ تدابير مجدية لكشف ورصد حركة النقد والصكوك القابلة للتداول ذات الصلة عبر حدودها، رهنا بوجود ضمانات تكفل حسن استخدام المعلومات ودون إعاقة حركة رأس المال المشروع بأي صورة من الصور. ويجوز أن تشمل تلك التدابير اشتراط قيام الأفراد والمؤسّسات التجارية بالإبلاغ عن تحويل الكميات الكبيرة من النقد ومن الصكوك القابلة للتداول ذات الصلة عبر الحدود.

3- لدى إنشاء نظام رقابي وإشرافي داخلي بمقتضى أحكام هذه المادّة، ودون مساس بأي مادّة أخرى من هذه الاتفاقية، يُهاب بالدول الأطراف أن تسترشد بالمبادرات ذات الصلة التي اتخذتها المنظمات الإقليمية والأقاليمية والمتعدّدة الأطراف لمكافحة غسل الأموال.

4- يتعيّن على الدول الأطراف أن تسعى إلى تطوير وتعزيز التعاون العالمي والإقليمي ودون الإقليمي والثنائي بين الأجهزة القضائية وأجهزة إنفاذ القانون وأجهزة الرقابة المالية من أجل مكافحة غسل الأموال.

المادّة 8

تجريم الفساد

1- يتعيّن على كلّ دولة طرف أن تعتمد ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم الأفعال التالية جنائيا عندما ترتكب عمدا :

(أ) وعد موظف عمومي بمزية غير مستحقة أو عرضها عليه أو منحه إيّاها، بشكل مباشر أو غير مباشر، سواء لصالح الموظف نفسه أو لصالح شخص آخر أو هيئة أخرى، لكي يقوم ذلك الموظف بفعل ما أو يمتنع عن القيام بفعل ما ضمن نطاق ممارسته مهامه الرّسميّة،

(ب) التماس موظف عمومي أو قبوله، بشكل مباشر أو غير مباشر، مزية غير مستحقة، سواء لصالح الموظف نفسه أو لصالح شخص آخر أو هيئة أخرى، لكي يقوم ذلك الموظف بفعل ما أو يمتنع عن القيام بفعل ما ضمن نطاق ممارسته مهامه الرّسميّة.

2- يتعيّن على كلّ دولة طرف أن تنظر في اعتماد ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم السلوك المشار إليه في الفقرة 1 من هذه المادّة الّذي يضلع فيه موظف عمومي أجنبي أو موظف مدني دولي. وبالمثل، يتعيّن على كلّ دولة طرف أن تنظر في تجريم أشكال الفساد الأخرى جنائيا.

3- يتعيّن على كلّ دولة طرف أن تعتمد أيضا ما قد يلزم من تدابير للتجريم الجنائي للمشاركة كطرف متواطئ، في جرم مقرّر بمقتضى هذه المادّة.

4- لأغراض الفقرة 1 من هذه المادّة والمادّة 9 من هذه الاتفاقية يقصد بتعبير "الموظف العمومي" أي موظف عمومي أو شخص يقدّم خدمة عمومية، حسب تعريفها في القانون الداخلي وحسبما تطبّق في القانون الجنائي للدّولة الطرف التي يقوم الشخص المعني بأداء تلك الوظيفة فيها.

المادّة 9

تدابير مكافحة الفساد

1- بالإضافة إلى التدابير المبيّنة في المادّة 8 من هذه الاتفاقية، يتعيّن على كلّ دولة طرف أن تعتمد، بالقدر الّذي يناسب نظامها القانوني ويتّسق معه، تدابير تشريعية أو إدارية أو تدابير فعّالة أخرى لتعزيز نزاهة الموظفين العموميين ومنع فسادهم وكشفه ومعاقبته.

2- يتعيّن على كلّ دولة طرف أن تتّخذ تدابير لضمان قيام سلطاتها باتخاذ إجراءات فعّالة لمنع فساد الموظفين العموميين وكشفه ومعاقبته، بما في ذلك منح تلك السلطات استقلالية كافية لردع ممارسة التأثير غير السليم على تصرفاتها.

المادّة 10

مسؤولية الهيئات الاعتبارية

1- يتعيّن على كلّ دولة طرف أن تعتمد ما قد يلزم من تدابير، بما يتفق مع مبادئها القانونية، لإرساء مسؤولية الهيئات الاعتبارية عن المشاركة في الجرائم الخطيرة التي تضلع فيها جماعة إجرامية منظمة والجرائم المقرّرة وفقا للموادّ 5 و6 و8 و23 من هذه الاتفاقية.

2- رهنا بالمبادئ القانونية للدّولة الطرف، يمكن أن تكون مسؤولية الهيئات الاعتبارية جنائية أو مدنية أو إدارية.

3- تترتب هذه المسؤولية دون مساس بالمسؤولية الجنائية للأشخاص الطبيعيّين الذين ارتكبوا الجرائم.

4- يتعيّن على كلّ دولة طرف أن تكفل، على وجه الخصوص، إخضاع الأشخاص الاعتباريين الذين تلقى عليهم المسؤولية وفقا لهذه المادّة لجزاءات جنائية أو غير جنائية فعّالة ومتناسبة ورادعة، بما في ذلك الجزاءات النقدية.

المادّة 11

الملاحقة والمقاضاة والجزاءات

1- يتعيّن على كلّ دولة طرف أن تجعل ارتكاب أي جرم مقرّر وفقا للموادّ 5 و6 و8 و23 من هذه الاتفاقية خاضعا لجزاءات تراعى فيها خطورة ذلك الجرم.

2- يتعيّن على كلّ دولة طرف أن تسعى إلى ضمان أن أية صلاحيات قانونية تقديرية يتيحها قانونها الدّاخلي فيما يتعلّق بملاحقة الأشخاص لارتكابهم جرائم مشمولة بهذه الاتفاقية تُمارس من أجل تحقيق الفعالية القصوى لتدابير إنفاذ القوانين التي تتّخذ بشأن تلك الجرائم، ومع إيلاء الاعتبار الواجب لضرورة ردع ارتكابها.

ملحق رقم 11: المرسوم الرئاسي المتضمن تصديق الجزائر على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

العدد 57 — السّنة الواحدة والخمسون

الأحد 4 ذي الحجّة عام 1435 هـ — الموافق 28 سبتمبر سنة 2014 م

الجمهورية الجزائرية
الديمقراطية الشعبية

الجريدة الرسمية

اتفاقات دولية ، قوانين ، ومراسيم
قرارات وآراء ، مقرّرات ، مناشير ، إعلانات وبلاغات

الاشتراك سنوي	الجزائر، تونس، المغرب، ليبيا، موريطانيا	بلدان خارج دول المغرب العربي
	سنة	سنة
النّسخة الأصليّة	1070,00 د.ج	2675,00 د.ج
النّسخة الأصليّة وترجمتها	2140,00 د.ج	5350,00 د.ج
		تزاد عليها نفقات الإرسال

الإدارة والتّحرير
الأمانة العامّة للحكومة

WWW.JORADP.DZ

الطّبع والاشتراك
المطبعة الرّسميّة

حي الياسمين، بئر مراد رايس، ص.ب 376 – الجزائر – محطة
الهاتف : 021.54.35.06 إلى 09
021.65.64.63
الفاكس 021.54.35.12
ح.ج.ب 50-3200 الجزائر
Télex : 65 180 IMPOF DZ
بنك الفلاحة والتّنمية الرّيفيّة 060.300.0007 68 KG
حساب العملة الأجنبيّة للمشتركين خارج الوطن
بنك الفلاحة والتّنمية الرّيفيّة 060.320.0600.12

ثمن النّسخة الأصليّة 13,50 د.ج
ثمن النّسخة الأصليّة وترجمتها 27,00 د.ج
ثمن العدد الصّادر في السّنين السّابقة : حسب التّسعيرة.
وتسلّم الفهارس مجّانا للمشتركين.
المطلوب إرفاق لفيفة إرسال البريدة الأخيرة سواء لتجديد الاشتراكات أو للاحتجاج أو لتغيير العنوان.
ثمن النّشر على أساس 60,00 د.ج للسّطر.

اتّفاقيّات واتفاقات دوليّة

مرسوم رئاسيّ رقم 14-252 مؤرّخ في 13 ذي القعدة عام 1435 الموافق 8 سبتمبر سنة 2014، يتضمّن التّصديق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، المحرّرة بالقاهرة بتاريخ 21 ديسمبر سنة 2010.

إنّ رئيس الجمهوريّة،

– بناء على تقرير وزير الشّؤون الخارجيّة،

– وبناء على الدّستور، لا سيّما المادّة 77-11 منه،

– وبعد الاطّلاع على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، المحرّرة بالقاهرة بتاريخ 21 ديسمبر سنة 2010،

يرسم ما يأتي :

المادّة الأولى : يصدّق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، المحرّرة بالقاهرة بتاريخ 21 ديسمبر سنة 2010، وتنشر في الجريدة الرّسميّة للجمهوريّة الجزائريّة الدّيمقراطيّة الشّعبيّة.

المادّة 2 : ينشر هذا المرسوم في الجريدة الرّسميّة للجمهوريّة الجزائريّة الدّيمقراطيّة الشّعبيّة.

حرّر بالجزائر في 13 ذي القعدة عام 1435 الموافق 8 سبتمبر سنة 2014.

عبد العزيز بوتفليقة

الاتفاقية العربية لمكافحة جرائم تقنية المعلومات

الديباجة

إن الدول العربية المتعاقدة،

– **رغبة** منها في تعزيز التعاون فيما بينها لمكافحة جرائم تقنية المعلومات التي تهدد أمنها ومصالحها وسلامة مجتمعاتها،

– **واقتناعا** منها بضرورة الحاجة إلى تبني سياسة جنائية مشتركة تهدف إلى حماية المجتمع العربي ضد جرائم تقنية المعلومات،

– **وأخذا** بالمبادئ الدينية والأخلاقية السامية ولا سيما أحكام الشريعة الإسلامية، وكذلك بالتراث الإنساني للأمة العربية التي تنبذ كل أشكال الجرائم، ومع مراعاة النظام العام لكل دولة،

– **والتزاما** بالمعاهدات والمواثيق العربية والدولية المتعلقة بحقوق الإنسان ذات الصلة من حيث ضمانها واحترامها وحمايتها،

قد اتفقت على ما يأتي :

الفصل الأول

أحكام عامة

المادّة الأولى

الهدف من الاتفاقية

تهدف هذه الاتفاقية إلى تعزيز التعاون وتدعيمه بين الدول العربية في مجال مكافحة جرائم تقنية المعلومات، لدرء أخطار هذه الجرائم حفاظا على أمن الدول العربية ومصالحها وسلامة مجتمعاتها وأفرادها.

المادّة 2

المصطلحات

يقصد بالمصطلحات الآتية في هذه الاتفاقية التعريف المبين إزاء كل منها :

1 – **تقنية المعلومات :** أية وسيلة مادية أو معنوية أو مجموعة وسائل مترابطة أو غير مترابطة تستعمل لتخزين المعلومات وترتيبها وتنظيمها واسترجاعها ومعالجتها وتطويرها وتبادلها وفقا للأوامر والتعليمات المخزنة بها ويشمل ذلك جميع المدخلات والمخرجات المرتبطة بها سلكيا أو لاسلكيا في نظام أو شبكة.

2 – **مزود الخدمة :** أي شخص طبيعي أو معنوي عام أو خاص يزود المشتركين بالخدمات للتواصل بواسطة تقنية المعلومات، أو يقوم بمعالجة أو تخزين المعلومات نيابة عن خدمة الاتصالات أو مستخدميها.

3 – **البيانات :** كل ما يمكن تخزينه ومعالجته وتوليده ونقله بواسطة تقنية المعلومات، كالأرقام والحروف والرموز وما إليها...

4 – **البرنامج المعلوماتي :** مجموعة من التعليمات والأوامر، قابلة للتنفيذ باستخدام تقنية المعلومات ومعدة لإنجاز مهمة ما.

5 – **النظام المعلوماتي :** مجموعة برامج وأدوات معدة لمعالجة وإدارة البيانات والمعلومات.

6 – **الشبكة المعلوماتية :** ارتباط بين أكثر من نظام معلوماتي للحصول على المعلومات وتبادلها.

7 – **الموقع** : إمكان إتاحة المعلومات على الشبكة المعلوماتية من خلال عنوان محدد .

8 – **الالتقاط** : مشاهدة البيانات أو المعلومات أو الحصول عليها .

9 – **معلومات المشترك** : أية معلومات موجودة لدى مزود الخدمة المتعلقة بمشتركي الخدمات عدا المعلومات التي يمكن بواسطتها معرفة :

أ) نوع خدمة الاتصالات المستخدمة والشروط الفنية وفترة الخدمة،

ب) هوية المشترك وعنوانه البريدي أو الجغرافي أو هاتفه ومعلومات الدفع المتوفرة بناء على اتفاق أو ترتيب الخدمة،

ج) أية معلومات أخرى عن موقع تركيب معدات الاتصال بناء على اتفاق الخدمة.

المادّة 3

مجالات تطبيق الاتفاقية

تنطبق هذه الاتفاقية ما لم ينص على خلاف ذلك، على جرائم تقنية المعلومات بهدف منعها والتحقيق فيها وملاحقة مرتكبيها، وذلك في الحالات الآتية :

1 – ارتكبت في أكثر من دولة.

2 – ارتكبت في دولة وتم الإعداد أو التخطيط لها أو توجيهها أو الإشراف عليها في دولة أو دول أخرى،

3 – ارتكبت في دولة وضلعت في ارتكابها جماعة إجرامية منظمة تمارس أنشطة في أكثر من دولة،

4 – ارتكبت في دولة وكانت لها آثار شديدة في دولة أو دول أخرى.

المادّة 4

صون السيادة

1 – تلتزم كل دولة طرف، وفقا لنظمها الأساسية أو لمبادئها الدستورية بتنفيذ التزاماتها الناشئة عن تطبيق هذه الاتفاقية على نحو يتفق مع مبدأي المساواة في السيادة الإقليمية للدول وعدم التدخل في الشؤون الداخلية للدول الأخرى.

2 – ليس في هذه الاتفاقية ما يبيح لدولة طرف أن تقوم في إقليم دولة أخرى بممارسة الولاية القضائية وأداء الوظائف التي يناط أداؤها حصرا بسلطات تلك الدولة الأخرى بمقتضى قانونها الداخلي.

الفصل الثاني

التجريم

المادّة 5

التجريم

تلتزم كل دولة طرف، بتجريم الأفعال المبينة في هذا الفصل، وذلك وفقا لتشريعاتها وأنظمتها الداخلية.

المادّة 6

جريمة الدخول غير المشروع

1 – الدخول أو البقاء وكل اتصال غير مشروع مع كل أو جزء من تقنية المعلومات أو الاستمرار به.

2 – تشدد العقوبة إذا ترتب على هذا الدخول أو البقاء أو الاتصال أو الاستمرار بهذا الاتصال :

أ) محو أو تعديل أو تشويه أو نسخ أو نقل أو تدمير للبيانات المحفوظة وللأجهزة والأنظمة الإلكترونية وشبكات الاتصال وإلحاق الضرر بالمستخدمين والمستفيدين،

ب) الحصول على معلومات حكومية سرية.

المادّة 7

جريمة الاعتراض غير المشروع

الاعتراض المتعمد بدون وجه حق لخط سير البيانات بأي من الوسائل الفنية وقطع بث أو استقبال بيانات تقنية المعلومات.

المادّة 8

الاعتداء على سلامة البيانات

1 – تدمير أو محو أو إعاقة أو تعديل أو حجب بيانات تقنية المعلومات قصدا وبدون وجه حق.

2 – للطرف أن يستلزم لتجريم الأفعال المنصوص عليها في الفقرة (1) من هذه المادة، أن تتسبب بضرر جسيم.

المادّة 9

جريمة إساءة استخدام
وسائل تقنية المعلومات

1 – إنتاج أو بيع أو شراء أو استيراد أو توزيع أو توفير :

أ) أية أدوات أو برامج مصممة أو مكيفة لغايات ارتكاب الجرائم المبينة في المادة السادسة إلى المادة الثامنة،

ب) كلمة سر نظام معلومات أو شيفرة دخول أو معلومات مشابهة يتم بواسطتها دخول نظام

معلومات ما بقصد استخدامها لأية من الجرائم المبينة في المادة السادسة إلى المادة الثامنة.

2 – حيازة أية أدوات أو برامج مذكورة في الفقرتين أعلاه، بقصد استخدامها لغايات ارتكاب أي من الجرائم المذكورة في المادة السادسة إلى المادة الثامنة.

المادّة 10

جريمة التزوير

استخدام وسائل تقنية المعلومات من أجل تغيير الحقيقة في البيانات تغييرا من شأنه إحداث ضرر، وبنية استعمالها كبيانات صحيحة.

المادّة 11

جريمة الاحتيال

التسبب بإلحاق الضرر بالمستفيدين والمستخدمين عن قصد وبدون وجه حق بنية الاحتيال لتحقيق المصالح والمنافع بطريقة غير مشروعة، للفاعل أو للغير، عن طريق :

1 – إدخال أو تعديل أو محو أو حجب للمعلومات والبيانات.

2 – التدخل في وظيفة أنظمة التشغيل وأنظمة الاتصالات أو محاولة تعطيلها أو تغييرها.

3 – تعطيل الأجهزة والبرامج والمواقع الإلكترونية.

المادّة 12

جريمة الإباحية

1 – إنتاج أو عرض أو توزيع أو توفير أو نشر أو شراء أو بيع أو استيراد مواد إباحية أو مخلة بالحياء بواسطة تقنية المعلومات.

2 – تشدد العقوبة على الجرائم المتعلقة بإباحية الأطفال والقصر.

3 – يشمل التشديد الوارد في الفقرة (2) من هذه المادة، حيازة مواد إباحية الأطفال والقصر أو مواد مخلة بالحياء للأطفال والقصر على تقنية للمعلومات أو وسيط تخزين تلك التقنيات.

المادّة 13

الجرائم الأخرى المرتبطة بالإباحية

للمقامرة والاستغلال الجنسي.

المادّة 14

جريمة الاعتداء على حرمة الحياة الخاصة

الاعتداء على حرمة الحياة الخاصة بواسطة تقنيات المعلومات.

المادّة 15

الجرائم المتعلقة بالإرهاب والمرتكبة

بواسطة تقنية المعلومات

1 – نشر أفكار ومبادئ جماعات إرهابية والدعوة لها.

2 – تمويل العمليات الإرهابية والتدريب عليها وتسهيل الاتصالات بين التنظيمات الإرهابية.

3 – نشر طرق صناعة المتفجرات والتي تستخدم خاصة في عمليات إرهابية.

4 – نشر النعرات والفتن والاعتداء على الأديان والمعتقدات.

المادّة 16

الجرائم المتعلقة بالجرائم المنظمة

والمرتكبة بواسطة تقنية المعلومات

1 – القيام بعمليات غسل أموال أو طلب المساعدة أو نشر طرق القيام بغسل الأموال.

2 – الترويج للمخدرات والمؤثرات العقلية أو الاتجار بها.

3 – الاتجار بالأشخاص.

4 – الاتجار بالأعضاء البشرية.

5 – الاتجار غير المشروع بالأسلحة.

المادّة 17

الجرائم المتعلقة بانتهاك حق المؤلف

والحقوق المجاورة

انتهاك حق المؤلف، كما هو معرف حسب قانون الدولة الطرف، وذلك إذا ارتكب الفعل عن قصد ولغير الاستعمال الشخصي، وانتهاك الحقوق المجاورة لحق المؤلف ذات الصلة كما هي معرفة حسب قانون الدولة الطرف، وذلك إذا ارتكب الفعل عن قصد ولغير الاستعمال الشخصي.

المادّة 18

الاستخدام غير المشروع

لأدوات الدفع الإلكترونية

1 – كل من زور أو اصطنع أو وضع أي أجهزة أو مواد تساعد على تزوير أو تقليد أي أداة من أدوات الدفع الإلكترونية بأي وسيلة كانت.

2 – كل من استولى على بيانات أي أداة من أدوات الدفع واستعملها أو قدمها للغير أو سهّل للغير الحصول عليها.

3– كل من استخدم الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات في الوصول بدون وجه حق إلى أرقام أو بيانات أي أداة من أدوات الدفع.

4 – كل من قبل أداة من أدوات الدفع المزورة مع العلم بذلك.

المادّة 19

الشروع والاشتراك في ارتكاب الجرائم

1 – الاشتراك في ارتكاب أية جريمة من الجرائم المنصوص عليها في هذا الفصل مع وجود نية ارتكاب الجريمة في قانون الدولة الطرف.

2 – الشروع في ارتكاب الجرائم المنصوص عليها في الفصل الثاني من هذه الاتفاقية.

3 – يجوز لأي دولة طرف الاحتفاظ بحقها في عدم تطبيق الفقرة الثانية من هذه المادة كليا أو جزئيا.

المادّة 20

المسؤولية الجنائية للأشخاص

الطبيعية والمعنوية

تلتزم كل دولة طرف، مع مراعاة قانونها الداخلي، بترتيب المسؤولية الجزائية للأشخاص الاعتبارية عن الجرائم التي يرتكبها ممثلوها باسمها أو لصالحها دون الإخلال بفرض العقوبة على الشخص الذي يرتكب الجريمة شخصيا.

المادّة 21

تشديد العقوبات على الجرائم التقليدية

المرتكبة بواسطة تقنية للمعلومات

تلتزم كل دولة طرف بتشديد العقوبات على الجرائم التقليدية في حال ارتكابها بواسطة تقنية المعلومات.

الفصل الثالث

الأحكام الإجرائية

المادّة 22

نطاق تطبيق الأحكام الإجرائية

1 – تلتزم كل دولة طرف بأن تتبنى في قانونها الداخلي التشريعات والإجراءات الضرورية لتحديد الصلاحيات والإجراءات الواردة في الفصل الثالث من هذه الاتفاقية.

2 – مع مراعاة أحكام المادة التاسعة والعشرين، على كل دولة طرف تطبيق الصلاحيات والإجراءات المذكورة في الفقرة (1) على :

أ) الجرائم المنصوص عليها في المواد السادسة إلى التاسعة عشرة من هذه الاتفاقية،

ب) أية جرائم أخرى ترتكب بواسطة تقنية للمعلومات،

ج) جمع الأدلة عن الجرائم بشكل إلكتروني.

3 – أ) يجوز لأي دولة طرف الاحتفاظ بحقها في تطبيق الإجراءات المذكورة في المادة التاسعة والعشرين فقط على الجرائم أو أصناف الجرائم المعنية في التحفظ بشرط أن لا يزيد عدد هذه الجرائم على عدد الجرائم التي تطبق عليها الإجراءات المذكورة في المادة الثلاثين، وعلى كل دولة طرف أن تأخذ بعين الاعتبار محدودية التحفظ لإتاحة التطبيق الواسع للإجراءات المذكورة في المادة التاسعة والعشرين،

ب) كما يجوز للدولة الطرف، أن تحتفظ بحقها في عدم تطبيق تلك الإجراءات كلما كانت غير قادرة بسبب محدودية التشريع على تطبيقها على الاتصالات التي تبث بواسطة تقنية معلومات لمزود خدمة، وذلك إذا كانت التقنية :

- يتم تشغيلها لصالح مجموعة مغلقة من المستخدمين،
- لا تستخدم شبكات اتصال عامة وليست مرتبطة بتقنية معلومات أخرى سواء كانت عامة أو خاصة.

وعلى كل دولة طرف أن تأخذ بعين الاعتبار محدودية التحفظ لإتاحة التطبيق الواسع للإجراءات المذكورة في المادتين التاسعة والعشرين والثلاثين.

المادّة 23

التحفظ العاجل على البيانات المخزنة

في تقنية للمعلومات

1 – تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين السلطات المختصة من إصدار الأمر أو الحصول على الحفظ العاجل للمعلومات المخزنة بما في ذلك معلومات تتبع للمستخدمين والتي خزنت على تقنية معلومات وخصوصا إذا كان هناك اعتقاد أن تلك المعلومات عرضة للفقدان أو التعديل.

2 – تلتزم كل دولة طرف بتبني الإجراءات الضرورية فيما يتعلق بالفقرة (1) بواسطة إصدار أمر إلى شخص من أجل حفظ معلومات تقنية المعلومات المخزنة والموجودة بحيازته أو سيطرته ومن أجل إلزامه بحفظ وصيانة سلامة تلك المعلومات لمدة أقصاها 90 يوما قابلة للتجديد، من أجل تمكين السلطات المختصة من البحث والتقصي.

3 – تلتزم كل دولة طرف بتبني الإجراءات الضرورية لإلزام الشخص المسؤول عن حفظ تقنية المعلومات للإبقاء على سرية الإجراءات طوال الفترة القانونية المنصوص عليها في القانون الداخلي.

المادّة 24

التحفظ العاجل والكشف الجزئي

لمعلومات تتبع للمستخدمين

تلتزم كل دولة طرف بتبني الإجراءات الضرورية فيما يخص معلومات تتبع للمستخدمين من أجل :

1 – ضمان توفر الحفظ العاجل لمعلومات تتبع للمستخدمين بغض النظر عن اشتراك واحد أو أكثر من مزودي الخدمة في بث تلك الاتصالات.

2 – ضمان الكشف العاجل للسلطات المختصة لدى الدولة الطرف أو لشخص تعينه تلك السلطات لقدار كاف من معلومات تتبع للمستخدمين لتمكين الدولة الطرف من تحديد مزودي الخدمة ومسار بث الاتصالات.

المادّة 25

أمر تسليم المعلومات

تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين السلطات المختصة من إصدار الأوامر إلى :

1 – أي شخص في إقليمها لتسليم معلومات معينة في حيازة ذلك الشخص والمخزنة على تقنية معلومات أو وسيط تخزين معلومات.

2 – أي مزود خدمة يقدم خدماته في إقليم الدولة الطرف لتسليم معلومات للمشترك المتعلقة بتلك الخدمات في حوزة مزود الخدمة أو تحت سيطرته.

المادّة 26

تفتيش المعلومات المخزنة

1 – تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين سلطاتها المختصة من التفتيش أو الوصول إلى :

أ) تقنية معلومات أو جزء منها والمعلومات المخزنة فيها أو المخزنة عليها.

ب) بيئة أو وسيط تخزين معلومات تقنية معلومات والذي قد تكون معلومات التقنية مخزنة فيه أو عليه.

2 – تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين السلطات المختصة من التفتيش أو الوصول إلى تقنية معلومات معينة أو جزء منها بما يتوافق مع الفقرة (1 – أ) إذا كان هناك اعتقاد بأن للمعلومات المطلوبة مخزنة في تقنية معلومات أخرى أو جزء منها في إقليمها وكانت هذه المعلومات قابلة للوصول قانونا أو متوفرة في التقنية الأولى فيجوز توسيع نطاق التفتيش والوصول للتقنية الأخرى.

المادّة 27

ضبط المعلومات المخزنة

1 – تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين السلطات المختصة من ضبط وتأمين معلومات تقنية المعلومات التي يتم الوصول إليها حسب الفقرة (1) من المادة السادسة والعشرين من هذه الاتفاقية.

هذه الإجراءات تشمل صلاحيات :

أ) ضبط وتأمين تقنية المعلومات أو جزء منها أو وسيط تخزين معلومات تقنية المعلومات.

ب) عمل نسخة من معلومات تقنية المعلومات والاحتفاظ بها.

ج) الحفاظ على سلامة معلومات تقنية المعلومات المخزنة.

د) إزالة أو منع الوصول إلى تلك المعلومات في تقنية المعلومات التي يتم الوصول إليها.

2 – تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين السلطات المختصة من إصدار الأوامر إلى أي شخص لديه معرفة بوظيفة تقنية المعلومات أو الإجراءات المطبقة لحماية تقنية المعلومات من أجل تقديم المعلومات الضرورية لإتمام تلك الإجراءات المذكورة في الفقرتين (2,1) من المادة السادسة والعشرين من هذه الاتفاقية.

المادّة 28

الجمع الفوري لمعلومات تتبع للمستخدمين

1 – تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين السلطات المختصة من :

أ) جمع أو تسجيل بواسطة الوسائل الفنية على إقليم تلك الدولة الطرف.

ب) إلزام مزود الخدمة ضمن اختصاصه الفني بأن :

– يجمع أو يسجل بواسطة الوسائل الفنية على إقليم الدولة الطرف، أو

– يتعاون ويساعد السلطات المختصة في جمع وتسجيل معلومات تتبع للمستخدمين بشكل فوري مع الاتصالات المعنية في إقليمها والتي تبث بواسطة تقنية المعلومات.

2 – إذا لم تستطع الدولة الطرف بسبب النظام القانوني الداخلي تبني الإجراءات المنصوص عليها في الفقرة (1 – أ) فيمكنها تبني إجراءات أخرى بالشكل الضروري لضمان

الجمع أو التسجيل الفوري للمعلومات تتبع المستخدمين للرافقة للاتصالات المعنية في إقليمها باستخدام الوسائل الفنية في ذلك الإقليم.

3 – تلتزم كل دولة طرف باتخاذ الإجراءات الضرورية لإلزام مزود الخدمة بالاحتفاظ بسرية أية معلومة عند تنفيذ الصلاحيات المنصوص عليها في هذه المادة.

المادّة 29

امتراض معلومات المحتوى

1 – تلتزم كل دولة طرف بتبني الإجراءات التشريعية والضرورية فيما يختص بسلسلة من الجرائم المنصوص عليها في القانون الداخلي، لتمكين السلطات المختصة من :

أ) الجمع أو التسجيل من خلال الوسائل الفنية على إقليم الدولة الطرف، أو

ب) التعاون ومساعدة السلطات المختصة في جمع أو تسجيل معلومات المحتوى بشكل فوري للاتصالات المعنية في إقليمها والتي تبث بواسطة تقنية معلومات.

2 – إذا لم تستطع الدولة الطرف بسبب النظام القانوني الداخلي تبني الإجراءات المنصوص عليها في الفقرة (1 – أ) فيمكنها تبني إجراءات أخرى بالشكل الضروري لضمان الجمع والتسجيل الفوري لمعلومات المحتوى للرافقة للاتصالات المعنية في إقليمها باستخدام الوسائل الفنية في ذلك الإقليم.

3 – تلتزم كل دولة طرف باتخاذ الإجراءات الضرورية لإلزام مزود خدمة بالاحتفاظ بسرية أية معلومة عند تنفيذ الصلاحيات المنصوص عليها في هذه المادة.

الفصل الرابع

التعاون القانوني والقضائي

المادّة 30

الاختصاص

1 – تلتزم كل دولة طرف بتبني الإجراءات الضرورية لمد اختصاصها على أي من الجرائم المنصوص عليها في الفصل الثاني من هذه الاتفاقية وذلك إذا ارتكبت الجريمة كليا أو جزئيا أو تحققت :

أ) في إقليم الدولة الطرف،

ب) على متن سفينة تحمل علم الدولة الطرف،

ج) على متن طائرة مسجلة تحت قوانين الدولة الطرف،

د) من قبل أحد مواطني الدولة الطرف إذا كانت الجريمة يعاقب عليها حسب القانون الداخلي في مكان ارتكابها أو إذا ارتكبت خارج منطقة الاختصاص القضائي لأية دولة،

هـ) إذا كانت الجريمة تمس أحد المصالح العليا للدولة.

2 – تلتزم كل دولة طرف بتبني الإجراءات الضرورية لمد الاختصاص الذي يغطي الجرائم المنصوص عليها في المادة 31 الفقرة (1) من هذه الاتفاقية في الحالات التي يكون فيها الجاني المزعوم حاضرا في إقليم تلك الدولة الطرف ولا يقوم بتسليمه إلى طرف آخر بناء على جنسيته بعد طلب التسليم.

3 – إذا ادعت أكثر من دولة طرف بالاختصاص القضائي لجريمة منصوص عليها في هذه الاتفاقية فيقدم طلب الدولة التي أخلت الجريمة بأمنها أو بمصالحها ثم الدولة التي وقعت الجريمة في إقليمها ثم الدولة التي يكون الشخص المطلوب من رعاياها وإذا اتحدت الظروف، فتقدم الدولة الأسبق في طلب التسليم.

المادّة 31

تسليم المجرمين

1 – أ) هذه المادة تنطبق على تبادل المجرمين بين الدول الأطراف على الجرائم المنصوص عليها في الفصل الثاني من هذه الاتفاقية بشرط أن تكون تلك الجرائم يعاقب عليها في قوانين الدول الأطراف المعنية بسلب الحرية لفترة أدناها سنة واحدة أو بعقوبة أشد.

ب) إذا انطبقت عقوبة أدنى مختلفة حسب ترتيب متفق عليه أو حسب معاهدة تسليم المجرمين فإن العقوبة الدنيا هي التي سوف تطبق.

2 – إن الجرائم المنصوص عليها في الفقرة (1) من هذه المادة تعتبر قابلة لتسليم المجرمين الذين يرتكبونها في أية معاهدة لتسليم المجرمين قائمة بين الدول الأطراف.

3 – إذا قامت دولة طرف ما بجعل تسليم المجرمين مشروطا بوجود معاهدة وقامت باستلام طلب لتسليم المجرمين من دولة طرف أخرى ليس لديها معاهدة تسليم فيمكن اعتبار هذه الاتفاقية كأساس قانوني لتسليم المجرمين فيما يتعلق بالجرائم المذكورة في الفقرة (1) من هذه المادة.

4 – الدول الأطراف التي لا تشترط وجود معاهدة لتبادل المجرمين يجب أن تعتبر الجرائم المذكورة في الفقرة (1) من هذه المادة قابلة لتسليم المجرمين بين تلك الدول.

الملحق رقم 12: المرسوم الملكي الذي ينظم تشكيلة ومهام المنظمة الدولية للشرطة السيبرانية "سايبربول".

STATUTORY ROYAL DECREE OF THE INTERNATIONAL CYBER POLICING ORGANIZATION - CYBERPOL™

™

THE
INTERNATIONAL CYBER POLICING
ORGANIZATION
NPMIA / IVoG / IVZW / AISBL

Abbreviated

CYBERPOL™

Statutory Royal Decree

NO WL22/16.595

2 July 2015

ENGLISH PUBLICATION

State Gazette Ref Page

http://www.ejustice.just.fgov.be/tsv/tsvn.htm

NPMIA / IVoG / IVZW / AISBL Organizational Number **635.897.257**

THE INTERNATIONAL CYBER POLICING ORGANIZATION, AFGEKORT : CYBERPOL INTERNATIONALE VER.IVoG; IVZW; AISBL Ref # 15128442

THE INTERNATIONAL CYBER POLICING ORGANIZATION, AFGEKORT : CYBERPOL INTERNATIONALE VER.IVoG; IVZW; AISBL Ref # 15128441

THE INTERNATIONAL CYBER POLICING ORGANIZATION, AFGEKORT : CYBERPOL INTERNATIONALE VER.IVoG; IVZW; AISBL Ref # 15128440

1

STATUTORY ROYAL DECREE OF THE INTERNATIONAL CYBER POLICING ORGANIZATION - CYBERPOL™

TRANSLATED COPY. THE ORIGIONAL CAN BE FOUND ON PAGE 15 AND 16 OF THIS DOCUMENT

KINGDOM OF BELGIUM
FEDERAL PUBLIC SERVICE JUSTICE

GENERAL DIRECTORATE OF THE LEGISLATION AND FUNDAMENTAL RIGHTS AND FREEDOMS

WL22/16.595

Philippe, King of the Belgians
To all, present and to come,

In view of the Act of 27 June on the non-profit associations, international associations not-for-profit and the foundations, articles 46 and 50, 1, respectively modified by articles282 and 284 of the program act of 2007 December 2004

Given the query of 30 April by which Madam S. Claeys, acting as notary of the International Association << **The International Cyber Policing Organization** >>, in English abbreviated <<**CYBERPOL**>>, request, for this international association in training, the legal personality;
Given the genuine act of April 3, 2015

In view of the conformity of the purpose with article 46 of the aforementioned law

On the proposal of the minister of justice

We have rules and we do rule:

Article 1. **Legal personality is granted to the international association** << **The International Cyber Policing Organization** >>, in English abbreviated <<**CYBERPOL**>> whose headquarters is established at Antwerp.

Article 2. The minister who has justice in assignments is responsible for the execution of the present decree

Bruxelles, the 2 of July 2015

Philippe (s.)
By the King:

The Minister of Justice,
(g.) K. GEENS. (s.)

For consignment complies with:
Administrative Assistant

Claudine GILSON

In the year **two thousand fifteen**
On **April third**
Before me, Ms **Saskia CLAEYS**, Associated Notary Public, at 1190 Vorst-Brussels

PREAMBLE

CYBERPOL is a private Organization already established in the United Kingdom and will be transferring all its Organizations, IP rights and skills to the in current Deed incorporated International Non-Profit Association "**The International Cyber Policing Organization**" abbreviated as "**CYBERPOL**", trademark No UK00003031007 which has priority rights and "seniority" claim rights according to international trademark laws in the section "registered under class 45" as stipulated on the Trademark act of EU by Council Directive No. 89/104/EEC (Repealed by EU Directive 2008/95/EC) or later.

The signatories of the present document have unanimously agreed to set up a non-profit organization in the form of an A.I.S.B.L. under Belgian law, in accordance with the law of 27th June 1921, the articles of association of which have been set out below.

STATUTORY ROYAL DECREE OF THE INTERNATIONAL CYBER POLICING ORGANIZATION - CYBERPOL™

GENERAL PROVISIONS

Article 1

The Organization is named **"The International Cyber Policing Organization"** abbreviated as **"CYBERPOL"**. This name must always be preceded or followed by the words "internationale vereniging zonder winstoogmerk/association internationale sans lucratif" or the abbreviation "IVZW/AISBL". **Its seat shall be in Belgium.**

The Organization is governed by Title III of the Belgian law of 27 June 1921 on the non-profit associations, the foundations and the international non-profit associations.

The registered office of the association is established in the Antwerp, Belgium judicial district. The General Assembly is authorized to transfer the registered office of the association to another location within this judicial district and to establish other offices and/or subsidiaries within or outside this judicial district.

Article 2

The Purpose is:

To ensure and promote the widest possible mutual international assistance between all **international Cyber Criminal police authorities** within the limits of the laws existing in the different countries and in the spirit of the **"Universal Declaration of Human Rights"**.

To establish and develop all institutions likely to contribute effectively to the prevention and suppression of ordinary and advanced cyber law crimes.

The activities of the Organization

- **Provide technical support for global Cyber law-enforcement** to enhance international cooperation and cyber education, understand of trends and implementing of technical tools to fight cyber crime.
- The Organization Research / **Investigates international cyber risk and monitoring facilitating international partnering** for Cyber Resilience Cooperation and cyber law-enforcement training.
- It identifies and Research / **Investigate International Cyber Crimes (ICC),** cyber-threats and global cyber-crime trends in the contemporary cyber world of today.

"CYBER WATCHDOG"

- To provides certification and targeted training services, and expert analytical support to relevant data and safe communications entities globally.
- Enable and assist promote Research and support modern international cyber-law enforcement in co-ordinate cyber risk management programs
- The International **monitoring and tracking of malevolent websites and IP's containing illegal and harmful content** capable of affecting the physical, emotional and psychological well-being of all Internet users.
- Assist International victims of Cyber Crimes and **provides administrative liaison and communications support for law-enforcement agencies** in the interest of victims of Cyber Crime.
- Educational Research on both national and international for academia, schools and institutions.
- Bring cyber risk awareness programs to public and private sector.
- **Research / Investigate and understanding of the physiological impact of cyber-crime.**
- To assists those engaged in cyber-policing on the ground understand cybercrime trends and emerging risks in order to correctly analyze information and **conduct timely operations** to ensure web safety goals are reached in all risk categories.
- Develop, write Research / Investigate and publish academic programs to Educate, assist and promote the standards for cyber security and law-enforcement across the globe.
- Research / Investigate and implement and produce courses for International security and law-enforcement co-operation, assistance and education.
- To assist victims of disasters created by cyber-crime due to the nature of critical infrastructures that was affected by cyber resilience and crimes.
- Educate and promote ***cyber awareness to all levels of life***.

The Organization is authorized to undertake all actions and to enter into all transactions (including real estate transactions) which are directly or indirectly useful or necessary for the promotion and achievement of the above-mentioned purpose.

Article 3

It shall be strictly forbidden for the Organization to undertake any intervention or activities of a political, military, religious or racial character.

MEMBERSHIPS

STATUTORY ROYAL DECREE OF THE INTERNATIONAL CYBER POLICING ORGANIZATION - CYBERPOL™

Article 4

There shall constitute three types of memberships:

1 General Assembly membership:

Consist of Government-law enforcement agencies, memberships designated by agencies for co-operation efforts and approved officials. General Assembly membership shall be subject to approval by a two-thirds majority of the General Assembly.

Members may retire by following ways:

- Dismissal by the General Secretariat or the President of its duties in exceptional cases.
- By written notice proved and accepted by the General Secretariat or the President.
- Or when services are no longer required by the General Assembly by vote of the General Assembly, Veto rights remains with the President of the Organization.
- Members who are members by member states as indicated in Appendix 1 can only retire when such legislative authority responsible has rejected the joining of the Organization by constitutional decision of that legislative authority applicable. Such rejection has to take place within six month of publication of the statute.

2 Paid memberships:

- Individual Entry Level Membership: Such as individuals engaged in public and private law-enforcement agencies or work.
- Associate Membership: Such as members of law-enforcement, cyber-crime prevention organizations.
- Agency Membership: Such as security agencies, State security agencies, intelligence agencies and other.
- Corporate Membership: Such as corporate companies, conglomerates and private firms.

Rights of such memberships shall be limited to:

Any such member could be voted to seat on any of the internal or external bodies of the Organization or participate in any activity approved by the President and or the General Secretariat.

Obligation:

All members shall uphold the name of the Organization at all times and promote the Organization in all public appearances or activities.

Members may retire by following ways:

- Dismissal by the General Secretariat or the President of its duties in exceptional cases.
- By written notice proved and accepted by the General Secretariat or the President.
- Or when services are no longer required by the General Assembly by vote of the General Assembly, Veto rights remains with the President of the Organization.

3. Non Paid memberships:

These are memberships approved by the General Secretariat in countries that are unable to pay fees and considered underprivileged or underdeveloped countries.

Rights of such memberships shall be limited to:

Any such member could be voted to seat on any of the internal or external bodies of the Organization or participate in any activity approved by the President and or the General Secretariat.

Obligation:

All members shall uphold the name of the Organization at all times and promote the Organization in all public appearances or activities.

Members may retire by following ways:

- Dismissal by the General Secretariat or the President of its duties in exceptional cases.
- By written notice proved and accepted by the General Secretariat or the President.
- Or when services are no longer required by the General Assembly by vote of the General Assembly, Veto rights remains
- with the President of the Organization.

Any country may delegate as a Member (sub 1, 2, 3) to the Organization any law-enforcement or cyber police body or officer whose functions come within the framework of activities of the Organization.

All requests for membership (sub 1, 2, 3) shall be submitted to the Secretary General. Where such membership is a governmental membership then it must be submitted by the appropriate legislative authority.

The Founder Members shall be considered lifelong Members of the General Assembly (Members sub 1) and cannot be revoked by any of the Members,

General Assembly or the Executive Committee. This membership is effective from the first day of the incorporation of the Organization and is irrevocable.

The first delegation shall be established and voted in by the Founder Members. The Founder Members may elect a President, one or more Vice-President(s) and a Secretary General. These members will be Founders of the Organization and cannot be dismissed for the duration of the Organizations lifetime.

Article 5

STRUCTURE AND ORGANIZATION

The International Cyber Policing Organization - CYBERPOL shall comprise:

The General Assembly:
That will consist of in the minimum:

- The Founders
- The President
- The Vice-President(s)
- The General Secretariat
- Delegates = Members selected by the Office of the President that could comprise of any European national and government members and/or member states internationally or organization or agency(s).

The Office of the President shall constitute the President and the Vice-President(s) of the Organization.

The Executive Committee:

That will consist of in the minimum:

- The President
- The Vice-President(s)
- The Secretary General
- Delegates = Members selected by the Office of the President that could comprise of any European national and government members and/ or member states internationally or organization or agency(s).

The General Secretariat:

That will consist of in the minimum:

The General Secretariat shall consist of the Secretary General and a technical and administrative staff entrusted with the work of the Organization. These may consist of voluntary members that are active law-enforcement members from both private and public sector.

Delegates of the General Secretariat shall be selected and be approved by the Office of the President only. These members shall be deemed not the same types of « Delegates » as described in the General Assembly and the Executive Committee but act as technical and administrative staff of the General Secretariat.

The technical and administrative staff of the General Secretariat shall be appointed by the Office of the President by recommendation of the Executive Committee (EC) of the Organization.

The National Central Bureaus:

That will consist of in the minimum:

- The President
- The Vice-President(s)
- The General Secretariat
- Delegates = Members selected by the Office of the President that could comprise of civilians and government members and or member states.

The Advisers:

That will consist of in the minimum:

- The President
- The Vice-President(s)
- The General Secretariat
- Delegates = Members selected by the Office of the President that could comprise of civilians and government members and or member states.

The Commission for the Control of Records:

That will consist of in the minimum:

- The President
- The Vice-President(s)
- The General Secretariat
- Delegates = Members selected by the Office of the President that could

THE GENERAL ASSEMBLY

Article 6

the Addressee and not that with the General Assembly.

All General Assembly decisions shall be posted within 21 days of the General Assembly on the Organizations website notice board in accordance with digital law of the EU.

Any decision taken in the absence of any Member shall be deemed final and can be contest by means of written notice to contest to the Office of the President within 7 days of such decision. The President may decide to have such decisions retaken at the cost of the opposing Member. All such cost for re-Assembly shall be covered by any apposing Member.

Article 13

Only Members delegate from Article 4, Memberships "General Assembly membership" (Members sub 1) shall have the right to vote in the General Assembly.

Article 14

The General Assembly attendance requirements shall require being a minimum of three attendees and not being less than the following attendees in order to take a decision:

- The President
- The Vice-President(s)
- The Secretary General

Decisions shall be made by a simple majority of 51% except in those cases where a two-thirds majority is required by the statute.

The President has the right to veto such decision(s) if not in the interest of the Organization. **Final approval rest with the Office of the President.**

An additional 28 members of the General Assembly (= Delegates) shall belong to different countries, due weight having been given to geographical distribution and participation. These additional 28 members shall be invited by the President to attend the General Assembly.

THE EXECUTIVE COMMITTEE

Article 15

The Executive Committee shall be composed of the President of the Organization, the Vice-President(s), the Secretary General and Delegates approved by the President. All Delegates have to be a Member of the Organization in order to be approved. The minimum number of the members of the Executive Committee shall be 3.

An additional **28 members of the Executive Committee (= Delegates) shall belong to different countries,** due weight having been given to geographical distribution and participation.

Article 16

The General Assembly shall elect, from among the Delegates, the President and one or more Vice-President(s) of the Organization.

A two-thirds majority shall be required for the election of the President; should this majority not be obtained after the second ballot, a simple majority shall suffice.

Article 17

The President shall be elected for a period of 5 years. The Vice-President(s) shall be elected for 5 years. The Secretary General shall be elected for a period of 5 years. Reelection is possible in any positions.

They may be immediately eligible for reelection either to the same posts or as Delegates on the Executive Committee.

Article 18

The President of the Organization shall:

- Preside and Chair at meetings of the Assembly and the Executive Committee and direct the discussions.
- Ensure that the activities of the Organization are in conformity with the decisions of the General Assembly and the Executive Committee.
- Present as public figure the Organization at all times. The President can also approve one or more candidate to present the Organization in public such as media/press or any other function delegated by the President and as described in the Internal Regulations.
- Have the authority to engage in projects in the interest of the Organization.
- Have veto rights in all cases.
- Assist in all programs of the Organization.
- **May have a special identification issued by the Organization.**
- The Organization can be present to third parties by anybody who is designated by the President or the General secretariat of the Organization.

Executive Committee:

Uphold as far as is achievable direct and constant contact with the Secretary General and or the President of the Organization.

Article 19

The Delegates on the Executive Committee shall be elected by the General Assembly for a period of 4 years. They shall not be immediately eligible for re-election to the same posts unless approved by the President.

Article 20

The Executive Committee shall meet at least once each year on being summoned by the President of the Organization.

The agenda, the place, the day and hour of the Executive Committee shall be communicated by public notice and / or direct communications such as emails/ letters and summonses to the members of the Executive Committee at least 45 days prior to the Executive Committee.

The decisions taken by the Executive Committee still have to pass approval of the President and the General Secretariat which on approval shall propose it for final approval by the General Assembly.

The President and the General Secretariat have the right in exceptional cases to disapprove any decisions if it's not in the interest of public and civil protection. The attendance of the Executive committee shall not be less than three members and 2/3 votes shall serve as the majority when 3 members are present in voting and 51% when 4 or more members are present in voting.

All Executive Committee decisions shall be posted within 21 days of the final approval of the General Assembly on the Organizations website notice board in accordance with digital law of the EU.

Article 21

In and during the exercise of their duties, all Members of the Executive Committee and the Organization shall conduct and identify themselves as representatives of the Organization and not as representatives of their respective organizations or countries.

Article 22

The Executive Committee shall:

- Supervise the implementation of the decisions of the General Assembly;
- Prepare the agenda for sessions of the General Assembly;
- Submit to the General Assembly any program of work or project which it considers useful;
- Direct the administration and work of the Secretary General;
- Exercise all the powers delegated to it by the General Assembly.
- **May have a special identification issued by the Organization.**

Article 23

All Executive Committee members shall remain in office until the end of the session of the General Assembly held in the year in which their term of office expires automatically. Reappointments are necessary by the General Secretariat to commence duties as Executive Committee member that shall take place in the form of Public notice on the website and or direct appointment of the General Secretariat.

Disposition of the Executive Committee shall be:

- By vote of the General Secretariat or by Dismissal of the President in extraordinary cases as set out in the Internal Regulations and will be send to the relevant Member by written notice;
- By vote of the General Assembly when services are no longer required, veto rights remains with the President of the Organization.
- Member states who are presented on the Organization in the Executive Committee shall request a formal dismissal in writing by the official department with appropriate justifications. Such request can be rejected by the President of the Organization should motivation not be substantial.

Article 24

The permanent departments of the Organization shall constitute the General Secretariat that may include the President, Vice President(s) and the Secretary General.

Article 25

The General Secretariat shall:

1. Put into application the decisions of the General Assembly and the Executive Committee once approved by the President.

2. Serve as an international center in the fight against ordinary cyber-crime.
3. Serve as a technical and information center.
4. Ensure the efficient administration of the Organization.
5. Maintain contact with national and international authorities, whereas questions relative to the search for criminals shall be dealt with through the National Central Bureaus.
6. Produce any publications which may be considered useful.
7. Organize and perform secretariat work at the sessions of the General Assembly, the Executive Committee and any other body of the Organization.
8. Draw up a draft program of work for the coming year for the consideration and approval of the General Assembly and the Executive Committee.
9. Maintain as far as possible direct and constant contact with the President of the Organization.
10. Assists where possible victims of cyber-crime.
11. **May have a special identification issued by the Organization.**

Article 26

The General Secretariat shall consist of the Secretary General and a technical and administrative staff entrusted with the work of the Organization. These may consist of voluntary members that are active law-enforcement members from both private and public sector. Delegates of the General Secretariat shall be selected and be approved by the Office of the President only. These members shall be deemed not the same types of « Delegates » as described in the General Assembly and the Executive Committee but act as technical and administrative staff of the General Secretariat.

The technical and administrative staff that is members of the General Secretariat may be nominated by any state or organization, entity or public citizen and or civil servant to sit on the General Secretariat. Such nominee shall be appointed and approved by the President of the Organization only.

Technical and administrative staff may have a special identification issued by the Organization.

The technical and administrative staff of the Organization that is not part of the General Secretariat shall be appointed by the Office of the President by recommendation of the Executive Committee of the Organization only. The term shall serve for a minimum of 5 years.

The technical and administrative staff is staff that is responsible by order of the General secretariat to exercise certain duties such as administrative, Research / Investigate, secretarial and agency responsibilities that could include cross border examination and study of any designated.

The General Secretariat may consist of the Secretary General and a technical and administrative staff. The President of the Organization may order such technical and administrative staff to have the necessary **State Clearances** or organizational to provide their activities within accordance of the **INFOSEC** rules and regulations of the Organization.

Dismissal of any General Secretariat member and Secretary General:

- Dismissal of any General Secretariat member shall by ordered and approved by the President by recommendation of the Vice-President.
- By written notice approved and accepted by the President.
- Or when services are no longer required by the General Assembly by vote of the General Assembly, Veto rights remains with the President of the Organization.

Article 27

The appointment of the Secretary General shall be proposed by the Executive Committee and approved by the President for a period of 5 years. She/he may be re-appointed for other terms but must lay down office on reaching the age of seventy- two, although she/he may be allowed to complete his term of office on reaching this age. She/he must be chosen from among persons highly competent in cyber security and police matters.

In exceptional circumstances, the Executive Committee may propose at a meeting of the General Assembly that the Secretary General will be removed from office if and when approved by the President.

Dismissal of Secretary General:

The dismissal of the Secretary General shall by order and approved by the President only. The dismissal shall apply in special circumstances only as set out in the internal rules and regulations.

By written notice proved and accepted by the President whereas a temporally or new permanent

General Secretariat has to be appointed at all times. The President may appoint anybody to act as a temporally interim Secretary General till next election if required to manage affectively the situation that might arise.

Article 28

The Secretary General shall engage and direct the staff, administer the budget, and organize and direct the permanent departments, according to the directives decided upon by the General Assembly and / or Executive Committee and /or the President.

She /he shall submit to the President and the Executive Committee and /or the General Assembly any propositions or projects concerning the work of the Organization.

She / He shall be responsible to the Executive Committee and the General Assembly. She /He shall have the right to take part in the discussions of the General Assembly, the Executive Committee and all other dependent bodies. In all the exercises of her / his duties, she /he shall represent the Organization at all times and not any particular nationality and / or organization and / or country.

Article 29

In the exercise of their duties, the ***Secretary General and the staff shall neither solicit nor accept instructions from any organization and / or institution and /or any government or authority*** outside the Organization membership.

They shall abstain from any action which might be prejudicial to their international task.

Each Member of the Organization shall undertake to respect the exclusively international character of the duties of the Secretary General and the staff, and abstain from influencing them in the discharge of their duties.

All Members of the Organization shall do their best to assist the Secretary General and the staff in the discharge of their functions.

NATIONAL CENTRAL BUREAUS

Article 30

In order to further its aims, objective and purpose, the Organization needs the constant and active co-operation of its Members, who should do all within their power which is compatible with the rules and regulations, legislations of their countries to participate diligently in its activities.

Article 31

In order to ensure the above international cooperation and assistance is met, each Member who is presenting an organization and / or a country or its authority, shall appoint a local body which will serve as the National Central Bureau for the Organization. It shall ensure liaison with:

- The various organizations and departments in the country;
- Those bodies in other countries serving as National Central Bureaus;
- The Organizations General Secretariat.

Article 32

In the case of those countries where the provisions of Article 32 are inapplicable or do not permit of effective centralized co-operation, the General Secretariat shall decide, with these membership countries, the most suitable alternative means of co-operation.

THE ADVISERS

Article 33

The Organization may consult "Advisers" on scientific matters, Research / Investigate and analyses of Research / Investigations. The role of the Advisers shall be purely advisory. Advisors must at all times when assisting promote and present the Organization and uphold its high value statute and image.

Article 34

Advisers shall be appointed for 3 years by the Executive Committee and or the President. Their appointment will become definite only after notification by the General Assembly and official approval of the President of the Organization.

All advisors shall be chosen from among those who have a world-wide reputation and qualifications in some fields of interest to the Organization. An Adviser may be removed from office by decision of the General Assembly. Advisors appointed by the President can only be removed by the Office of the President and do not account to the General Assembly unless told to do so.

THE COMMISSION FOR THE CONTROL OF RECORDS

Article 35

The Commission for the Control of Records shall provide the Organization with advice about any Member, staff and voluntary workers.

It shall be responsible for providing the Organization with advice about any project, operation, set of rules or other matter involving the processing of personal information.

The Commission for the Control of Records is an independent body which shall ensure that the processing of personal information by the Organization is in compliance with the regulations the Organization establishes in this matter.

The Commission for the Control of Records shall process requests concerning the information contained in the Organization's records.

All such records shall be accessible only to Members and staff in the Organization who is granted permission as set out in INFOSEC regulations of the Organization.

The Commission of Control of Records must undergo a security clearance and approved by the President before active. This measure is to ensure that all information of the Organization members is well contained.

The following security Clearance shall be adopted: CYBERPOL, the International Cyber Policing Organization, shall adopt 4 levels of Security Information, **COSMIC (TOP SECRET)**, **EC-SECRET**, **EC-CONFIDENTIAL** and **EC-COMMITTEE** in order to further it classification of records Research / Investigateed that could be shared with member states as noted in ***Appendix 1.***

Such Clearances shall only be approved by the General Secretariat for a max period of 3 years.

Article 36

The members of the Commission for the Control of Records shall hold the qualified expertise required for it to accomplish its functions. Its composition and its functioning shall be subject to specific rules to be laid down by the General Assembly and could be rectified at any time when approved by the President of the Organization.

BUDGET AND RESOURCES

Article 37

The Organization's financial resources shall be provided by:

1. The financial contributions from Members.
2. Gifts, bequests, subsidies, grants and other resources after these have been accepted or approved by the Office of the President.
3. IP License fees when approved by the Office of the President.
4. Public donations, seminars, educational programs, fund raising events and corporate donations.
5. Summits and forums
6. Bespoke services and Research / Investigate
7. Special assignments.
8. International Technical Assistance
9. Members state contributions.

Article 38

The General Assembly shall establish the basis of Members' subscriptions and the maximum fee that cannot exceed 250.000,00 Euro Per year. This restriction shall not apply to any government funds or grants.

The annual expenditure according to the estimate provided by the Secretary General shall be upheld. Staff including the President, Vice-President(s) and Secretary General can receive a salary provided they are active in the day to day activities of the Organization.

Article 39

The draft budget of the Organization shall be prepared by the Secretary General and submitted for approval to the Executive Committee.

It shall come into force after acceptance by the General Assembly provided that such funds are available. The expenditure budged may not exceed more than 80% of the annual funds raised in the Organization coffins. Should the General Assembly not have had the possibility of approving the budget, the Executive Committee shall take all necessary steps according to the general outlines of the preceding budget.

RELATIONS WITH OTHER ORGANIZATIONS

Article 40

STATUTORY ROYAL DECREE OF THE INTERNATIONAL CYBER POLICING ORGANIZATION - CYBERPOL[13]

The ***Organization shall establish relations and collaborate with other "organizations",*** intergovernmental or nongovernmental international organizations at any time it deems fit, having regard to the aims and purpose and activities of the Organization provided in Article 2 , The Purpose is and activities of the Organization.

The general provisions concerning the relations with international, intergovernmental or nongovernmental organizations will only be valid after their recommendation by the General Assembly with final approval from the President.

The Organization by order of the President may at any time, in connection with all matters in which it is competent, take the advice of nongovernmental international, governmental national or non-governmental national organizations.

With the approval of the General Assembly and or the President in special circumstances, the Executive Committee or, in urgent cases, the Secretary General may accept duties within the scope of its activities and competence either from other international institutions or organizations or in application of international conventions.

APPLICATION, MODIFICATION, INTERPRETATION OF THE STATUTE AND INTERNAL REGULATIONS

Article 41

The present Statute may be amended on the proposal of either any Member or the Executive Committee with approval of the following:

1. The President of the Organization,
2. All the Vice-Presidents of the Organization,
3. The General Secretariat of the Organization,
4. and 80% votes in favor of such change by all Members of the General Assembly.

Article 42

The French, English and Dutch texts of this Constitution shall be regarded as authoritative.

Article 43

Internal Regulations which regulate the functioning of the Organization further and more detailed will be drawn up by the Executive Committee for the approval of the General Assembly, acting under the ordinary conditions of majority, and of the Office of the President.

Changes to the Internal Regulations may be made by the General Assembly, acting under the ordinary conditions of majority, and approved by the Office of the President.

REPRESENTATION

Article 44

The Organization is validly represented towards third parties, before the courts and in official deeds, including those for which the intervention of a civil servant or a notary is required, by the Secretary General and a member of the Executive Committee, acting jointly, in accordance with the instructions of the Executive Committee, which will not have to justify their power against third parties.

Within the framework of the daily management, the Organization is validly represented by

1) the President and /or the Secretary General; or
2) two members of the Executive Committee acting jointly and at least one of the following, the ***President or the Secretary General,in accordance with the instructions of the Executive Committee, which will not have to justify their power against third parties.***

Moreover, ***within the framework of their mandate,*** the Organization is validly represented by special proxy holders ***authorized by the President and /or the Secretary General.***

TRADEMARK IP RIGHTS AND OWNERSHIP

Article 45

The organization is granted rights to the use of the CYBERPOL trademark No UK00003031007 "registered under class 45". All commercial that and seniority claim rights shall remain that of the IP owners.

The Organization may license, nominate any third party, agency and / or organization and / or corporation the rights to have access and / or the use the trademark under conditions to be set out by the owners of the trademark.

Such grant of uses shall be deemed a license approved for the user.

All approvals of such sub-license shall rest with the General Assembly and final approval of the President of the Organization. The President has full power to revoke any license granted at any time when it is founded that such organization the license were granted to have violated the integrity and good image of the Organization or engaged in any activity not in accordance with laws and the laws of the governing statute of that organization or country.

That the CYBERPOL AISBL is granted exclusive usage rights to use of the trademark services section only applicable to law-enforcement services and can't be revoked in the future or any point and time.

The IP rights to all commercial activity of IP's remaining trademark No UK00003031007 under classes from 1 to 44 and its seniority claim rights shall remain that of the IP trademark owners but can be shared when necessary in the interest of the Organization.

The Organization shall enter into an IP licensee agreement in order to allow the usage of the usage of the IP trademark No: UK00003031007

The use of the CYBERPOL IP NO UK00003031007: Officers of the law and official state agencies must be a member of CYBERPOL to use the official Law - enforcement Logo and must be in accordance with the regulations of uses of the Logo.

The President may grant permission to use the Logo to **officials or any civilian** when active in any operational duties when necessary.

The European Center for Information Policy and Security Ltd. (ECIPS) may file and own the rights of any trademark and or patent for commercial use under remaining classes 1 to 44 of the trademarks act due to its seniority claim rights.

Special notes:

Identification ID/INSIGNIA/ Badge using IP names and logos:

Any identification ID's/Insignia/ badge for members, staff and officers shall be approved by the Secretary General with exclusion of that of the founding members, the President and the Vice President of the Organization only.

Any unauthorized use of such Identification shall be prohibited by law as indicated in Trademark act of EU by Council Directive No. 89/104/EEC (Repealed by EU Directive 2008/95/EC) or later.

TEMPORARY MEASURES

Article 46

All bodies representing the countries mentioned in **Appendix I** shall be deemed to be Members of the Organization unless they declare through the appropriate governmental authority that they cannot accept this membership. Such a declaration should be made by means of public publication within six months of the date of the coming into force of the present statute.

DURATION

Article 47

The association can be dissolved only by majority vote of not less than 96% of the General Assembly and approval of the President of the Organization.

In such case of dissolution all funds shall be donated to the European Centre for Information Policy and Security ECIPS AISBL.

This Constitution shall come into force on 2nd July 2015

EUROPEAN UNION

****

APPENDIX 1:

LIST OF STATES TO WHICH THE PROVISIONS OF ARTICLE 48 OF THE STATUTE OF MEMBERSHIP SHALL APPLY

Argentina, Australia, Austria, Belgium, Brazil, Burma, Cambodia, Canada, Ceylon, Chile, Colombia, Costa Rica, Cuba, Denmark, Dominican Republic, Egypt, Eire, Finland, France, Federal German Republic, Greece, Guatemala, India, Indonesia, Iran, Israel, Italy, Japan, Jordan, Lebanon, Liberia, Libya, Luxembourg, Mexico, Monaco, Netherlands, Netherlands Antilles, New Zealand, Norway, Pakistan, Philippines, Portugal, Saar, Saudi Arabia, Spain, South Africa, Sudan, Surinam, Sweden, Switzerland, Syria, Thailand, Turkey, United Kingdom of Great Britain and Northern Ireland, United States of America, Uruguay, Venezuela, Yugoslavia and any other country who might join the international collaboration of the Organization.

****

Treaties that shall apply to the Decree

STATUTORY ROYAL DECREE OF THE INTERNATIONAL CYBER POLICING ORGANIZATION - CYBERPOL™

Mindful of the **Convention on Cybercrime,** also known as the **Budapest Convention on Cybercrime** or the Budapest Convention 8 November 2001. and the Additional Protocol to the Convention 1 March 2006 and,

Mindful of the United Nations (UN) Convention against Transnational Organized Crime (2000), the United Nations Security Council (UNSC) Resolution 1566 (2004) , Convention of the Prevention and Combating of Terrorism, The Protocol to the OAU Convention on the Prevention and combating of Terrorism (2004), and the AU Plan of Action on Drug Control and Crime Prevention (2007-2012), and UNLISTED,

BASIC INFORMATION

The current elected officials:

All current officials' names and identities are published in the State Gazette as from August 30th 2015. All such publications are final by decision after approval of the office of the President. All employees of CYBERPOL will undergo an International vetting process and must obtain the necessary clearances applicable.

The official appointed Notary Public of CYBERPOL

Ms Saskia Claeys

Authorized Translation(s) done by

Ms Shin-Hae Baretzky

FOR FURTHER INFORMATION WRITE TO

Info@cyberpol.org

STATUTORY ROYAL DECREE OF THE INTERNATIONAL CYBER POLICING ORGANIZATION - CYBERPOL™

CYBERPOL FLAG

قائمة المصادر والمراجع

قائمة المصادروالمراجع:

أولا: المراجع العربية:

1) الكتب:

1. أحسن بوسقيعة، التحقيق القضائي، ط 2، الديوان الوطني للأشغال التربوية، الجزائر، 2002.

2. أحمد فتحي سرور، الوسيط في شرح قانون الإجراءات الجنائية، ج1، ب ط، مطبعة القاهرة، مصر، 1979.

3. أشرف عبد القادر قنديل، الوسائل الإلكترونية ودورها في الإثبات الجنائي (دراسة مقارنة)، دار الجامعة الجديدة، مصر، 2018.

4. إيهاب خليفة، حروب مواقع التواصل الاجتماعي، ط 01، دار العربي للنشر والتوزيع، القاهرة، 2016.

5. بشيخ محمدحسين، مراقبة الإنترنت وأثرها على الحريات العامة، ط 01، المكتب العربي للمعارف، القاهرة مصر، 2019.

6. بوكر رشيدة، جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري والمقارن، ط 01، منشورات الحلبي الحقوقية، لبنان، 2012.

7. جزول صالح، الخصوصية الإجرائية للجرائم الماسة بأنظمة المعالجة الآلية للمعطيات في التشريع الجزائري، اصدارات المركز الديمقراطي العربي للدراسات الإستراتيجية والسياسية والاقتصادية، (الجريمة المعلوماتية وأثرها على التنمية الاقتصادية)، ط01، برلين- ألمانيا، جويلية 2020.

8. جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالأنترنت، دار النهضة العربية، القاهرة، 1998.

9. حدة بوخلفة، المسؤولية الجنائية لمقدمي خدمات الإنترنت، دار هومه للطباعة والنشر، الجزائر، ديسمبر 2019.

10. حسن الجوخدار، البحث الأولي أو الاستدلال في قانون أصول المحاكمات الجزائية، ط 01، دار الثقافة للنشر والتوزيع، الأردن، 2012

11. حسام محمد نبيل الشنراقي، الجرائم المعلوماتية، جرائم الاعتداء على التوقيع الإلكتروني(دراسة مقارنة)، دار الكتب القانونية، مصر- الإمارات، 2013.

12. خالد حسن أحمد لطفي، الدليل الرقمي ودوره في إثبات الجريمة المعلوماتية، ط 1، دار الفكر الجامعي، مصر، 2020.

13. خالد حسن أحمد لطفي، القانون الواجب التطبيق على الجريمة الإلكترونية، ط1، دار الفكر الجامعي، الاسكندرية مصر، سنة 2019.

14. خالد ممدوح براهيم، الإثبات الإلكتروني في المواد الجنائية والمدنية، ط 01، دار الفكر الجامعي، الاسكندرية، مصر، سنة 2020.

15. خالد ممدوح براهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، ط 1، دار الفكر الجامعي، مصر، 2018.

16. رفاه خضير جياد العارضي، الدليل الإلكتروني وأثره في مجال نظرية الإثبات الجنائي، ط1، مكتبة زين الحقوقية والأدبية، لبنان، 2019.

17. الشوا محمد سامي، القانون الإداري الجزائي، دار النهضة العربية، مصر، 1996.

18. عبد الرحمان خلفي، الإجراءات الجزائية في التشريع الجزائري والمقارن، ط 4، دار بلقيس للنشر، الجزائر، 2018/2019.

19. عبد الفتاح بيومي حجازي، الدليل الجنائي في جرائم الكمبيوتر والتزوير، (دراسة معمقة في جرائم الحاسب الآلي والإنترنت)، دار الكتب القانونية، مصر، سنة 2004.

20. عبد الفتاح محمد كيلاني، المسئولية المدنية الناشئة عن المعاملات الإلكترونية عبر الإنترنت، دار الجامعة الجديدة، مصر، 2011.

21. علي شملال، المستحدث في قانون الإجراءات الجزائية الجزائري، الكتاب الثاني (التحقيق والمحاكمة)، ط2، دار هومه، الجزائر، 2017.

22. عمار عوابدي، القانون الإداري، الجزء الأول:(النظام الإداري)، ديوان المطبوعات الجامعية، الجزائر، 2000.

23. عمار عوابدي، القانون الإداري، الجزء الثاني:(النشاط الإداري)، ط 04، ديوان المطبوعات الجامعية، الجزائر، 2007.

24. عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الإنترنت (الأحكام الموضوعية والجوانب الإجرائية)، ط 01، دار النهضة العربية، مصر، 2004.

25. عمر محمد أبو بكر بن يونس، الإجراءات الجنائية عبر الإنترنت في القانون الأمريكي، (المرشد الفيدرالي الأمريكي لتفتيش وضبط الحواسيب وصولا للدليل الإلكتروني في التحقيقات الجنائية)، ط1، موسوعة التشريعات العربية، 2005.

26. كمال عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، (دراسة مقارنة)، ط 02، منشورات الحلبي القانونية، دمشق، 2007.

27. لحسن ناني، التحقيق في الجرائم المتصلة بتكنولوجيا المعلوماتية بين النصوص التشريعية والخصوصية التقنية، النشر الجامعي الجديد، 2018

28. لينا محمد الأسدي، مدى فاعلية أحكام القانون الجنائي في مكافحة الجريمة المعلوماتية، دار الحامد للنشر والتوزيع، الأردن عمان، 2015.

29. محمد سيد سلطان، قضايا في أمن المعلومات وحماية البيئة الإلكترونية، دار ناشري للنشر الإلكتروني، الإمارات المتحدة، سنة 2012.

30. محمود عبد الغني جاد المولى، دور الدليل الإلكتروني في الإثبات الجنائي (دراسة مقارنة)، دار الفكر الجامعي، ط 1، مصر، 2019.

31. نادر عبد الكريم الغزواني، الحماية الجنائية من جرائم الإنترنت (دراسة مقارنة)، مكتبة نور للنشر، الاسكندرية مصر، 2017.

32. نبيلة هبة هروال. الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات، (دراسة مقارنة)، ط 01، دار الفكر الجامعي، الاسكندرية، مصر، سنة 2006.

33. هشام محمد فريد رستم، الجوانب الإجرائية لجرائم المعلوماتية (دراسة مقارنة)، مكتبة الآلات الحديثة، مصر، 1994.

34. هلالى عبد اللاه أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، (دراسة مقارنة)، ط 01، دار النهضة العربية، القاهرة، مصر، 1997، ص 53.

35. يزيد بوحليط، الجرائم الإلكترونية والوقاية منها في القانون الجزائري في ضوء الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، (قانون العقوبات، قانون الإجراءات الجزائية)، دار الجامعة الجديدة، مصر، 2019.

2) الرسائل الجامعية:

- <u>أطروحات الدكتوراه:</u>

36. إبراهيم يامة، لوائح الضبط الإداري ببين الحفاظ على النظام العام وضمان الحريات العامة، أطروحة مقدمة لنيل شهادة الدكتوراه في القانون العام، كلية الحقوق والعلوم السياسية، جامعة أبي بكر بلقايد، تلمسان، 2015/2014.

37. اسماعيل جابوربي، الضبط الإداري في مجال المحافظة على الأمن العام في الظروف الاستثنائية، دراسة مقارنة في النظام الإسلامي والنظام القانوني الجزائري، أطروحة مقدمة لنيل درجة الدكتوراه في علوم الشريعة والقانون، تخصص مؤسسات سياسية وإدارية، كلية الشريعة والاقتصاد، جامعة عبد القادر للعلوم الإسلامية، قسنطينة، 2018/2017.

38. بلخير محمد آيت عودية، الضبط الإداري للشبكات الاجتماعية الإلكترونية، أطروحة مقدمة لنيل شهادة دكتوراه في العلوم، تخصص قانون عام، كلية الحقوق والعلوم السياسية، جامعة باتنة 1، 2019/2018.

39. حسين ربيعي، آليات البحث والتحقيق في الجرائم المعلوماتية، آليات البحث والتحقيق في الجرائم المعلوماتية، أطروحة مقدمة لنيل شهادة الدكتوراه، تخصص قانون العقوبات والعلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة باتنة 1، 2016/2015.

40. خضرة شنتير، الآليات القانونية لمكافحة الجريمة الإلكترونية، أطروحة مقدمة لنيل شهادة الدكتوراه، تخصص القانون الجنائي، كلية الحقوق والعلوم السياسية، جامعة أحمد دراية، أدرار، 2020/2021.

41. دلال ملياني مولاي، إشكالية الإثبات في جرائم الإنترنت في التشريع الجزائري، أطروحة مقدمة لنيل شهادة الدكتوراه، تخصص قانون خاص، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد، تلمسان، 2017/2018.

42. سليماني هندون، سلطات الضبط في الإدارة الجزائرية، أطروحة مقدمة لنيل شهادة الدكتوراه في القانون العام، تخصص إدارة ومالية، كلية الحقوق، جامعة الجزائر 1، 2013/2012.

43. سهام صديق، دور سلطات الضبط الإداري في الحفاظ على النظام العام الاقتصادي(دراسة مقارنة)، أطروحة مقدمة لنيل شهادة الدكتوراه في العلوم، تخصص القانون العام، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد، تلمسان، 2019/2018.

44. صالح شنين، الحماية الجزائية للتجارة الإلكترونية، أطروحة مقدمة لنيل شهادة الدكتوراه في القانون الخاص، كلية الحقوق، جامعة أبو بكر بلقايد، تلمسان، 2012/2013.

45. عاقلي فضيلة، الحماية القانونية للحق في حرمة الحياة الخاصة، دراسة مقارنة، أطروحة مقدمة لنيل شهادة الدكتوراه، كلية الحقوق، جامعة الإخوة منثوري، قسنطينة، 2011/2012.

46. عليان بوزيان، أثر حفظ النظام العام على ممارسة الحريات العامة، دراسة مقارنة بين الشريعة الإسلامية والقانون الجزائري، أطروحة مقدمة لنيل شهادة الدكتوراه، تخصص الشريعة والقانون، كلية العلوم الإنسانية والحضارة الإسلامية، جامعة وهران، 2007/2006.

47. فيروز عوض الكريم صالح الميرغني، إجراءات التحري والضبط في الجرائم الإلكترونية، أطروحة مقدمة لنيل شهادة الدكتوراه في القانون العام، كلية الدراسات العليا والبحث العلمي، جامعة شندى، 2017.

48. ليندا بن طالب، الدليل الإلكتروني ودوره في الإثبات الجنائي، أطروحة مقدمة لنيل شهادة الدكتوراه، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، 2019.

49. وهيبة رابح، الإجراءات المتبعة أمام الأقطاب الجزائية المتخصصة، أطروحة مقدمة لنيل شهادة الدكتوراه في القانون الإجرائي، كلية الحقوق والعلوم السياسية، جامعة مستغانم، سنة 2015/2016.

- **مذكرات الماجستير:**

50. أدهم باسم نمر بغدادي، وسائل البحث والتحري عن الجرائم الإلكترونية، مذكرة مقدمة لنيل شهادة الماجستير، كلية الدراسات العليا، جامعة النجاح الوطنية، نابلس، فلسطين، 2018.

51. أمينة ركاب، أساليب التحري الخاصة في جرائم الفساد في القانون الجزائري، مذكرة مقدمة لنيل شهادة الماجستير، تخصص قانون عام معمق، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد، تلمسان، 2014-2015.

52. حمزة قريشي، الوسائل الحديثة للبحث والتحري في ضوء قانون 06/22، مذكرة مقدمة لنيل شهادة الماجستير، دراسة مقارنة، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح، ورقلة، 2011/2012.

53. عاصف جودت أحمد النجاجره، خصوصية التحقيق في الجرائم الإلكترونية، رسالة مقدمة لنيل شهادة الماجستير، جامعة القدس، فلسطين، 2019.

54. عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في الإثبات الجنائي، (دراسة مقارنة)، مذكرة مقدمة لنيل شهادة الماجستير في الحقوق، كلية الحقوق، جامعة الإسكندرية، سنة 2009.

55. عائشة نشادي، إعادة هيكلة قطاع البريد والمواصلات السلكية واللاسلكية، مذكرة مقدمة لنيل شهادة الماجستير، كلية الحقوق، جامعة الجزائر، 2005/2004.

56. عبد الله بن عبد العزيز بن عبد الله الخثعمي، التفتيش في الجرائم المعلوماتية في النظام السعودي، رسالة مقدمة لنيل شهادة الماجستير، كلية الدراسات العليا، جامعة نايف للعلوم الأمنية، الرياض، 2011.

57. عبد المالك بشارة، آلية الإنتربول في مكافحة الجريمة، مذكرة لنيل شهادة الماجستير في القانون الجنائي الدولي، كلية الحقوق والعلوم السياسية، المركز الجامعي عباس لغرور، خنشلة، 2010/2009.

58. فايز خليفة بن يعروف، المواجهة التشريعية والأمنية للجرائم المتصلة بمواقع التواصل الاجتماعي، مذكرة مقدمة لنيل شهادة الماجستير في البحث الجنائي، أكاديمية شرطة دبي، الشارقة، الإمارات، 2019.

59. فقير محمد، علاقة رئيس الجمهورية بالوزير الأول في النظامين الجزائري والمصري(دراسة مقارنة)، مذكرة لنيل شهادة الماجستير في القانون العام، تخصص إدارة ومالية، كلية الحقوق، جامعة أمحمد بوقرة، بومرداس، ب س.

60. مالك بن ذياب، حق الخصوصية في التشريع العقابي الجزائري، مذكرة مقدمة لنيل شهادة الماجستير، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، 2012/2013.

61. مريم أحمد مسعود، آليات مكافحة جرائم تكنولوجيات الإعلام والاتصال في ضوء القانون رقم 04/09، مذكرة مقدمة لنيل شهادة الماجستير في القانون الجنائي، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح، 2013.

62. مصطفى جمال حنفي زينو، دور الضبط الإداري في مجال الجرائم الإلكترونية المخلة بالأمن العام (دراسة تحليلية)، مذكرة مقدمة لنيل شهادة الماجستير في القانون العام، كلية الحقوق، جامعة الأزهر، غزة فلسطين، 2017.

63. مصطفى جمال حنفي زينو، دور الضبط الإداري في مجال الجرائم الإلكترونية المخلة بالأمن العام (دراسة تحليلية)، مذكرة مقدمة لنيل شهادة الماجستير في القانون العام، كلية الحقوق، جامعة الأزهر، غزة فلسطين، 2017.

64. مصطفى طالب نعمة الجابري، استعمال كاميرات المراقبة بين التجريم والاباحة، رسالة مقدمة لنيل شهادة الماجستير في القانون العام، معهد العلمين للدراسات العليا، قسم القانون، العراق، سنة .2020

65. نعيم سعيداني، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة مقدمة لنيل شهادة الماجستير، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر باتنة، 2013/2012.

3) المقالات العلمية:

66. أحلام بوكربوعة، آلية الاتحاد الإفريقي للتعاون الشرطي "أفريبول" ودورها في مكافحة ظاهرة الإرهاب، حوليات جامعة الجزائر 1، المجلد 34، العدد 04، سنة 2020.

67. أسامة غربي، المنظمة الدولية للشرطة الجنائية (الإنتربول) ودورها في مكافحة الجريمة المنظمة، مجلة دراسات وأبحاث، المجلد 03، العدد 03، 30 جوان 2011.

68. بثينة حبيباتني، معوقات مكافحة الجريمة المعلوماتية، مجلة العلوم الإنسانية، المجلد "أ"، العدد 50، ديسمبر 2018.

69. بن اسماعيل سلسبيل، الحماية الجنائية للخصوصية المعلوماتية في التشريعين الجزائري والفرنسي، مجلة الاجتهاد القضائي، المجلد 12، العدد 22، أفريل2020،

70. بن بادة عبد الحليم، المراقبة الإلكترونية كإجراء لاستخلاص الدليل الإلكتروني "بين الحق في الخصوصية ومشروعية الدليل الإلكتروني"، المجلة الأكاديمية للبحث القانوني، المجلد 01، العدد 03، 2019.

71. بن تركي ليلى، التعاون القضائي الدولي لمكافحة جرائم الاعتداء على التوقيع الإلكتروني (بطاقات الائتمان نموذجا)، مجلة بحوث، المجلد 10، العدد 01، 15 ديسمبر 2016.

72. بن مرزوق عنترة، البعد الإلكتروني للسياسة الأمنية الجزائرية في مكافحة الارهاب، مجلة العلوم الإنسانية والاجتماعية، العدد 38، جوان 2018.

73. بهنوس آمال، الدليل الرقمي في الإجراءات الجنائية، المجلة الأكاديمية للبحث القانوني، المجلد 16، العدد 02، سنة 2017.

74. جزول صالح، ضمانات مشروعية التنصت التلفوني واعتراض المراسلات في القانون الإجرائي الجزائري، مجلة نوميروس الأكاديمية، المجلد 01، العدد 02، يونيو 2020.

75. حزام فتيحة، الحماية المؤسساتية للأنظمة الرقمية في الفترة التشريعية الممتدة من 2009 إلى 2020، مجلة الأكاديمية للدراسات الاجتماعية والإنسانية، المجلد 13، العدد 01، 2020/10/31.

76. حزام فتيحة، حماية الأنظمة الرقمية بين الآليات التقنية وأجهزة الحماية(قراءة في أحكام المرسوم الرئاسي 20-05)، مجلة الحقوق والعلوم الإنسانية، العدد 03، أكتوبر 2020.

77. حسين ربيعي، المراقبة الإلكترونية وحق الفرد في الخصوصية داخل الفضاء الرقمي، المجلة الأكاديمية للبحث القانوني، جامعة عبد الرحمان ميرة، بجاية، المجلد 07، العدد 01، سنة2016.

78. حليم رامي، إجراءات استخلاص الدليل في الجرائم المعلوماتية، مجلة دفاتر البحوث العلمية، المجلد 09، العدد 01، سنة 2021.

79. خديجة خالدي، آلية الاتحاد الافريقي للتعاون الشرطي " أفريبول"، مجلة العلوم الاجتماعية والانسانية، المجلد 11، العدد 01، سنة 2018.

80. خرشي عثمان، الترصد الإلكتروني كآلية لمكافحة الجرائم المعلوماتية، مجلة الدراسات الحقوقية، المجلد 07، العدد 03، سبتمبر 2020.

81. رحموني محمد، منظمة الشرطة الجنائية الدولية (الإنتربول) آلية لمكافحة الجريمة المنظمة، مجلة آفاق علمية، المجلد 11، العدد 04، سنة 2019.

82. رضا هميسي، تفتيش المنظومات المعلوماتية في القانون الجزائري، مجلة العلوم القانونية والسياسية، العدد الخامس، جوان 2012.

83. رضوان قرواش، هيئات التصديق في ظل القانون رقم 04/15 المتعلق بالقواعد العامة للتوقيع والتصديق الإلكترونيين(المفهوم والالتزامات)، مجلة العلوم الاجتماعية، العدد 24، جوان 2017.

84. زياد بن محمد عادي العتيبي، دراسة استطلاعية حول حجية الأدلة الرقمية في إثبات الجرائم المعلوماتية، المجلة الإلكترونية الشاملة متعددة التخصصات، العدد 29، أكتوبر 2020.

85. سهام صديق، مظاهر استقلالية السلطات الإدارية المستقلة في الجزائر، المجلة الجزائرية للحقوق والعلوم السياسية، العدد 04، ديسمبر 2017.

86. صالح شنين، التسرب في قانون الإجراءات الجنائية الجزائري حماية للنظام العام والحريات أم حماية للنظام العام، المجلة الجزائرية للقانون المقارن، المجلد 01، العدد 02، ديسمبر 2015.

87. ضريفي نادية، دراج عبد الوهاب، سلطات القاضي الجنائي في تقدير الدليل الإلكتروني المستمد من التفتيش الجنائي، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، المجلد 04، العدد 02، سنة 2019.

88. عبد الحليم بوقرين، حتمية إنشاء ضبطية خاصة بالجرائم الإلكترونية، مجلة العلوم القانونية والسياسية، المجلد 05، العدد 01، سنة 2016.

89. عبد القادر فلاح، التحقيق الجنائي للجرائم الإلكترونية وإثباتها في التشريع الجزائري، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، المجلد 04، العدد 02، 2019.

90. عيدة بلعابد، خصوصية التحقيق في الجريمة المعلوماتية، مجلة الباحث الأكاديمي في العلوم القانونية والسياسية، العدد 06، مارس 2021.

91. منيرة عبيزة، الدليل الإلكتروني والسلطة التقديرية للقاضي، مجلة العلوم القانونية والسياسية، المجلد 09، العدد 03، ديسمبر 2018.

92. نوال لصلج، صلاحيات رئيس المجلس الشعبي البلدي والوالي في ظل القوانين الجديدة، مجلة هيرودوت للعلوم الإنسانية والاجتماعية، العدد 06، جوان 2018.

93. يامة إبراهيم، أساليب التحري الخاصة بالجريمة المنظمة في القانونيين الجزائري والفرنسي، مجلة دفاتر السياسة والقانون، المجلد 11، العدد 02، جوان 2019.

94. يزيد بوحليط، تفتيش المنظومة المعلوماتية وحجز المعطيات في التشريع الجزائري، مجلة التواصل في الاقتصاد والإدارة والفانون، العدد 48، ديسمبر 2016.

4) البحوث والمداخلات العلمية:

95. جان فرانسوا هنروت، أهمية التعاون الدولي والتجربة البلجيكية في تبادل المعلومات بين عناصر الشرطة والتعاون القضائي، بحث مقدم إلى الندوة الإقليمية حول الجرائم المتصلة بالكمبيوتر ضمن برنامج تعزيز حكم القانون في بعض الدول العربية، المملكة المغربية، في 19- 20 يونيو 2007.

96. خلايفية هدى، الإطار الدولي والداخلي لحماية الخصوصية على الإنترنت (التشريع الجزائري نموذجا) مداخلة مشارك بها في الملتقى الدولي الموسوم ب: "الخصوصية في مجتمع المعلوماتية"، في طرابلس، لبنان، 19-20جويلية 2019.

97. عزالدين عزالدين، قيادة الدرك الوطني، الإطار القانوني للوقاية من الجرائم المعلوماتية ومكافحتها، مداخلة مشارك بها في الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة، جامعة بسكرة، الجزائر، 16-17 نوفمبر 2015

98. مجمع البحوث والدراسات، الجريمة الإلكترونية في المجتمع الخليجي وكيفية مواجهتها، أكاديمية السلطان قابوس لعلوم الشرطة، جامعة نايف بن عبد العزيز للبحوث الأمنية، عمان، 2016، ص ص 37-38-40.

99. هواري عياش، بحث حول مسار التحقيقات الجنائية في مجال الجريمة المعلوماتية، المعهد الوطني للأدلة الجنائية وعلم الإجرام، كلية الحقوق، جامعة بسكرة، 2016

5) المقابلات:

100. مقابلة مع نوري ميلود، الملازم الأول للشرطة، رئيس فرقة مكافحة الجرائم المعلوماتية للمصلحة الولائية للشرطة القضائية، بمقر المصلحة، بتاريخ 26/07/2021، على الساعة 10:30.

6) النصوص القانونية:

أ. <u>الدساتير:</u>

101. المرسوم الرئاسي رقم 20-442 المؤرخ في 15 جمادى الأولى عام 1442 الموافق 30 ديسمبر 2020، يتعلق بإصدار التعديل الدستوري الجزائري، الجريدة الرسمية للجمهورية الجزائرية عدد 82 الصادرة في 30 ديسمبر 2020.

ب. <u>المواثيق الدولية:</u>

102. الإعلان العالمي لحقوق الإنسان المعتمد من طرف قرار الجمعية العامة 217 ألف (د-3) المؤرخ في 10 ديسمبر 1948

103. الدليل الأوروبي الصادر في 24 نوفمبر 1995 المعتمد من طرف الجمعية العامة للاتحاد الأوروبي بشأن حماية الأفراد فيما يتصل بمعالجة البيانات الشخصية وحرية نقلها.

104. الاتفاقية الدولية للحقوق المدنية والسياسية المعتمدة بموجب قرار الجمعية العامة للأمم المتحدة 2200 ألف (د-21) المؤرخ في 16 ديسمبر 1966، وبدأ العمل بها في 23 مارس 1976.

105. اتفاقية بودابست بشأن مكافحة الجريمة الإلكترونية المعتمدة من قبل لجنة وزراء مجلس أوروبا في دورتها التاسعة بعد المائة، بتاريخ 08 نوفمبر 2001 وتم التوقيع عليها في 23 نوفمبر 2001.

106. اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية، التي صادقت عليه الجزائر بموجب المرسوم الرئاسي رقم 02-55 المؤرخ في 2002/02/05، ج ر ج ج عدد 09، المؤرخة في 2002/11/15..

107. اتفاقية الأمم المتحدة لمكافحة الفساد، المعتمدة من قبل الجمعية العامة للأمم المتحدة بنيويورك، بتاريخ 31 أكتوبر 2003، صادقت عليها الجزائر بموجب المرسوم الرئاسي رقم 128/06 المؤرخ في 2006/04/19، ج رج ج عدد 26 بتاريخ 2006/04/25.

108. الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، المحررة بالقاهرة بتاريخ 2010/12/21، التي صادقت عليها الجزائر بموجب المرسوم الرئاسي رقم 14-252 المؤرخ في 2014/09/08، ج ر ج ج عدد 57، المؤرخة في 2014/09/28.

ج. **<u>النصوص التشريعية:</u>**

109. القانون 2000-03 المؤرخ في 2000/08/05 الذي يحدد القواعد العامة المتعلقة بالبريد وبالمواصلات السلكية واللاسلكية، ج ر ج ج عدد 48 المؤرخة في 2000/08/06.

110. القانون رقم 04- 15 المؤرخ في 27 رمضان عام 1425 الموافق 10 نوفمبر 2004، المعدل والمتمم للأمر رقم 66- 156 المؤرخ في 18 صفر عام 1386 الموافق 08 يونيو سنة 1966، المتضمن قانون العقوبات، ج ر ج ج عدد 71 الصادرة بتاريخ 10 نوفمبر 2004

111. القانون رقم 06-01المؤرخ في 20/02/2006، المتعلق بالوقاية من الفساد ومكافحته، ج ر ج ج عدد 14، الصادرة بتاريخ 08/03/2006

112. القانون رقم 06- 23المؤرخ في 29ذي القعدة عام 1427الموافق 20ديسمبر 2006، المعدل والمتمم للأمر رقم 66- 156المؤرخ في 18صفر عام 1386الموافق 08يونيو سنة 1966، المتضمن قانون العقوبات، ج ر ج ج عدد 84الصادرة بتاريخ 24ديسمبر 2006.

113. القانون رقم 22/06 المؤرخ في 20 ديسمبر 2006 المعدل والمتمم للأمر رقم 66_155 المتضمن قانون الإجراءات الجزائية، ج ر العدد 84، الصادرة بتاريخ 24 ديسمبر 2006

114. القانون رقم 04/09 المؤرخ في 14 شعبان عام 1430، الموافق 05 أوت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج ر ج ج عدد 47، الصادرة بتاريخ 16 أوت 2009.

115. قانون البلدية رقم 10/11 المؤرخ في 22 جوان 2011، ج ر ج ج عدد 37، الصادرة بتاريخ 03 يوليو 2011

116. القانون العضوي رقم 12-05 المؤرخ في 18 صفر 1433 الموافق 12 يناير 2012، يتعلق بالإعلام، ج ر ج ج عدد 02 الصادرة في 2012/01/15.

117. قانون الولاية رقم 07/12 المؤرخ في 21 فبراير 2012، ج ر ج ج عدد 12، الصادرة بتاريخ 29 فبراير 2012.

118. القانون رقم 14-04 المؤرخ في 24 فبراير 2014، المتعلق بالنشاط السمعي البصري، ج ر ج ج عدد 16 المؤرخة في 2014/03/23.

119. القانون رقم 04/15 المؤرخ في 11 ربيع الثاني عام 1436 الموافق 01 فبراير 2015، يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، ج ر ج ج عدد 06، الصادرة بتاريخ 10 فبراير 2015.

120. القانون رقم 15/03مؤرخ في 11ربيع الثاني عام 1436الموافق لأول نوفمبر 2015، يتعلق بعصرنة العدالة، ج ر ج ج عدد 06، الصادرة بتاريخ 10فبراير 2015.

121. القانون رقم 04/18 المؤرخ في 24 شعبان 1439 الموافق ل 10 مايو 2018، يحدد القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية، ج ر ج ج، العدد 27 الصادرة بتاريخ 13 ماي 2018.

122. القانون رقم 18-07 المؤرخ في 10 جوان 2018 ، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، ج ر ج ج عدد 34 الصادرة بتاريخ 10 جوان 2018.

123. القانون رقم 10/19 المؤرخ في 14 ربيع الثاني عام 1441 الموافق 11 ديسمبر 2019، المعدل والمتمم للأمر رقم 66-155 المؤرخ في 18 صفر عام 1386 الموافق 08 يونيو سنة 1966 والمتضمن قانون الإجراءات الجزائية، ج ر ج ج عدد 78، الصادرة في 18 ديسمبر 2019

124. القانون الأساسي للمنظمة الدولية للشرطة الجنائية " الأنتربول".

125. القانون الأساسي لآلية الاتحاد الإفريقي للتعاون الشرطي " الأفريبول".

د. <u>النصوص التنظيمية:</u>

<u>المراسيم الرئاسية:</u>

126. المرسوم الرئاسي رقم 01-109 المؤرخ في 09 صفر 1422 الموافق ل 03 ماي 2001 يتضمن تعيين أعضاء مجلس سلطة ضبط البريد والمواصلات، ج ر ج ج، العدد 26 الصادرة بتاريخ 09 ماي 2001.

127. المرسوم الرئاسي رقم 04-432 المؤرخ في 29 ديسمبر 2004، يتضمن إنشاء المعهد الوطني للبحث في علم التحقيق الجنائي، ج ر ج ج عدد 84، المؤرخة في 29 ديسمبر 2004.

128. المرسوم الرئاسي رقم 15-261 المؤرخ في 2015/10/08، يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج ر ج ج عدد 53، المؤرخة في 2015/10/08.

129. المرسوم الرئاسي رقم 19- 172 المؤرخ في 03 شوال عام 1440 الموافق 2019/06/06، الذي يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج ر ج ج عدد 37 الصادرة في 09 يونيو 2019.

130. المرسوم الرئاسي رقم 183/20 المؤرخ في21 ذي القعدة عام 1441 الموافق 13 يوليو سنة 2020، يتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج ر ج ج عدد 40، الصادرة في 18 يوليو 2020

131. المرسوم الرئاسي رقم 20-05 المؤرخ في 24 جمادى الأولى عام 1441 الموافق 20 جانفي 2020، يتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية، ج ر ج ج عدد 04 المؤرخة في 26 جانفي سنة 2020.

132. المرسومالرئاسي رقم 439/21 المؤرخ في 2021/11/07، يتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج ر ج ج عدد 05، المؤرخة في 2021/11/11.

المراسيم التنفيذية:

133. المرسوم التنفيذي رقم 94-247، المؤرخ في 02 ربيع الأول عام 1415 الموافق ل 10 أوت 1994، الذي يحدد صلاحيات وزير الداخلية والجماعات المحلية والتهيئة العمرانية.

134. المرسوم التنفيذي رقم 98-257 المؤرخ في 25 أوت 1998 الذي يضبط شروط وكيفيات إقامة خدمات "أنترنات" واستغلالها، ج ر ج ج عدد 63 المؤرخة في 1998/08/26، المعدل بموجب المرسوم التنفيذي رقم 2000-307 المؤرخ في 14 أكتوبر 2000، ج ر ج ج عدد 60 المؤرخة في 2000/10/15.

135. المرسوم التنفيذي رقم 11-216 المرخ في 2011/06/12، الذي يحدد صلاحيات وزير الاتصال، ج ر ج ج عدد 33، المؤرخة في 2011/06/12.

136. المرسوم التنفيذي رقم 15-320 المؤرخ في 13 ديسمبر2015 الذي يحدد نظام الاستغلال المطبق على كل نوع من أنواع الشبكات بما فيها اللاسلكية الكهربائية وعلى مختلف خدمات المواصلات السلكية واللاسلكية، ج ر ج ج عدد 68 المؤرخة في 2015/12/27.

137. المرسوم التنفيذي رقم 16-134 المؤرخ في 17 رجب 1437 الموافق 25 أفريل 2016، يحدد تنظيم المصالح التقنية والإدارية للسلطة الوطنية للتصديق الإلكتروني وسيرها ومهامها، ج ر ج ج عدد 26، الصادرة بتاريخ 28 أفريل 2016.

138. المرسوم التنفيذي رقم 16-135 المؤرخ في 17 رجب عام 1437 الموافق 25 أبريل 2016، يحدد طبيعة السلطة الحكومية للتصديق الإلكتروني وتشكيلها وتنظيمها وسيرها، ج ر ج ج عدد 26 الصادرة بتاريخ 28 أفريل 2016.

139. المرسوم التنفيذي 20-178 المؤرخ في 14 ذي القعدة 1441 الموافق 06 يوليو 2020، يحدد صلاحيات وزير البريد والمواصلات السلكية واللاسلكية، ج ر ج ج العدد 40، الصادرة بتاريخ 18 يوليو 2020.

140. المرسوم التنفيذي رقم 20-179 المؤرخ في 14 ذي القعدة الموافق 06 يوليو 2020، يتضمن تنظيم الإدارة المركزية لوزارة البريد والمواصلات السلكية واللاسلكية، ج ر ج ج العدد 40، الصادرة بتاريخ 18 يوليو 2020.

141. المرسوم التنفيذي رقم 20-332 المؤرخ في 08 ربيع الثاني عام 1442 الموافق 22 نوفمبر 2020، الذي يحدد كيفيات ممارسة نشاط الإعلام عبر الإنترنت ونشر الرد أو التصحيح عبر الموقع الإلكتروني، ج ر ج ج عدد 70 الصادرة في 25 نوفمبر 2020.

القرارات الوزارية:

142. قرار مجلس الوزراء رقم 74 لسنة 2005، بشأن الاستراتيجية الوطنية للاتصالات وتكنولوجيا المعلومات، منشور على جريدة الوقائع الفلسطينية، العدد 61، مارس 2006.

143. قرار مجلس الوزراء بشأن المصادقة على السياسات العامة لاستخدام الحاسوب وشبكة الإنترنت في المؤسسات العامة، منشور على جريدة الوقائع الفلسطينية العدد 65، بتاريخ 2006/06/14.

144. القرار رقم 51/أخ/رم/س ض ب م/ 2016 المؤرخ في 03أفريل 2016 المتضمن دفتر الشروط الذي يحدد شروط وكيفيات إقامة واستغلال خدمات توفير النفاذ إلى الإنترنت

145. قرار الجمعية العامة للأمم المتحدة رقم 73/187، حول مكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية، الدورة الرابعة والسبعون، البند 109، الصادر بتاريخ 30 جويلية 2019.

القو انين العربية الأخرى:

نصوص قانونية مصرية:

146. دستور جمهورية مصر العربية الصادر في 13 أفريل 2019.

147. القانون رقم 58لسنة 1937المؤرخ في 05أوت 1937، المتضمن قانون العقوبات المصري

148. القرار الوزاري رقم 13507 المؤرخ في 2002/07/07 نشر في الأوامر العمومية لوزارة الداخلية المصرية، العدد 07، القاهرة.

149. القانون رقم 175 لسنة 2018 بشأن مكافحة جرائم تقنية المعلومات، المؤرخ في 14 أوت 2018، ج ر ج م عدد 32 مكرر (ج).

نصوص قانونية مغربية:

150. الظهير الشريف رقم 257-04-1 الصادر في 07 يناير 2005 بتنفيذ القانون رقم 03-77 المتعلق بالاتصال السمعي البصري

151. ظهير شريف رقم 15-09-1 صادر في 22 صفر 1430 الموافق 18 فبراير 2009 بتنفيذ القانون رقم 09-08 المتعلق بحماية الأشخاص الذاتيين تجاه المعطيات ذات الطابع الشخصي، ج ر عدد 5711 بتاريخ 27 صفر 1430 الموافق 23 فبراير 2009.

نصوص قانونية سعودية:

152. قانون نظام الإعلام السعودي.

153. تنظيم هيئة الاتصالات وتقنية المعلومات، الصادر بقرار مجلس الوزراء رقم 120 بتاريخ 1440/02/21هـ

154. نظام الاتصالات وتقنية المعلومات الصادر بقرار مجلس الوزراء رقم 74 وتاريخ 1422/03/05هـ والمعدل بموجب المرسوم الملكي رقم (م/15) وتاريخ 1440/02/22هـ..

155. القانون الاتحادي رقم (5) لعام 2012 المعدل والمتمم بالقانون الاتحادي رقم (12) لعام 2016 المتعلق بمكافحة جرائم تقنية المعلومات، ج ر عدد 597 الصادرة في 2016/05/31، المعدل بالقانون الاتحادي رقم (2) لعام 2018، ج ر عدد 633 الصادرة في 2018/07/31.

156. اللائحة التنفيذية لنظام الاتصالات الصادرة بالمرسوم الملكي رقم (م/12) بتاريخ 1422/03/12هـ، الصادرة بموجب قرار وزير الاتصالات وتقنية المعلومات رقم 4 وتاريخ 1442/01/29هـ..

157. القانون الاتحادي رقم (35) لسنة 1992 المتضمن قانون الإجراءات الجزائية، الجريدة الرسمية عدد 233 مكرر الصادرة بتاريخ 1992/01/26.

نصوص قانونية تونسية:

158. القانون الأساسي عدد 63 لسنة 2004 المتعلق بحماية المعطيات الشخصية المعدل بالقانون الأساسي عدد 25 لسنة 2018.

159. القانون عدد 05 المؤرخ في 03 فيفري 2004 المتعلق بالسلامة المعلوماتية، الرائد الرسمي للجمهورية التونسية العدد 10 الصادر في 03 فيفري 2004.

160. المرسوم رقم 116 المؤرخ في 2011/11/02 المتعلق بحرية الاتصال السمعي البصري التونسي.

نصوص قانونية أردنية:

161. قانون أصول المحاكمات الجزائية رقم 09 لسنة 1961، الجريدة الرسمية الأردنية عدد 2539 الصادرة بتاريخ مارس 1961، المعدل والمتمم بالقانون رقم 16 لسنة 2001 والقانون رقم 32 لسنة 2017.

نصوص قانونية أجنبية:

162. القانون الأمريكي رقم 304- 105 الصادر في 28 أكتوبر 1998، المتضمن حقوق الطبع والنشر الرقمية للألفية.

163. القانون رقم 579/93 الصادر سنة 1974 المتعلق بالخصوصية الأمريكي

164. قانون الإجراءات الجزائية رقم 1426/57 المؤرخ في 1957/12/31، الجريدة الرسمية للجمهورية الفرنسية عدد 20، الصادرة بتاريخ 1958/01/08، والمعدل والمتمم بالقانون رقم 1109/2021 المؤرخ في 2021/08/24

165. القانون الفرنسي رقم 801لسنة 2004الخاص بحماية البيانات الشخصية.

166. التعديل الدستوري الرابع للولايات م أ.

المقالات الإلكترونية:

167. الاتحاد الدولي للاتصالات والهيئة الوطنية للأمن السيبراني في المملكة العربية السعودية يطلقان برنامجا عالميا جديدا للحفاظ على سلامة الأطفال على الأنترنت، مقال منشور في 2020/12/17 على الموقع الرسمي للاتحاد الدولي للاتصالات، متاح على الرابط التالي: https://www. itu.

int/ar/mediacentre/Pages/cm11-2020-ITU-SaudiArabia-partnership-COP-guidelines. aspx
تاريخ الاطلاع: 2021/03/07 على الساعة 18:30.

168. الاتحاد الدولي يتخذ اجراءات فاعلة لمكافحة جرائم الأنترنت، مقال منشور في 2019/05/25 على الموقع الرسمي لوزارة الاتصالات وتكنولوجيا المعلومات المصرية، ومتاح على الرابط التالي: https://mcit.gov.eg/Ar/Media_Center/Latest_News/News/1913 تاريخ الاطلاع: 2021/03/08 على الساعة 19:00.

169. أحمد عبد العزيز، شرطة أبو ظبي تشكل فرقا متخصصة لمكافحة الجرائم الإلكترونية، الإثنين 2012/02/13، مقال منشور على الرابط التالي: https://www. alittihad. ae/article/15105/2012 تاريخ الاطلاع 2021/06/13 على الساعة 21:00.

170. أساهم في سلامتي أشارك في أمن وطني، مقال منشور على الموقع الرسمي للمديرية العامة للأمن الوطني، متاح على الرابط التالي: https://www. algeriepolice. dz/ تاريخ الاطلاع 2021/12/28 على الساعة 19:45.

171. الأمن السيبراني. . . حماية وطنية لأمن الفرد والمجتمع في المملكة، مقال منشور على موقع وكالة الأنباء السعودية، في الأربعاء 2017/11/01 ، متاح على الرابط التالي: https://www. spa. gov. sa/1683272تاريخ الاطلاع: 2021/02/17 على الساعة 18:22

172. أمين صالح، مقال منشور على مجلة اليوم السابع، متاح على الرابط التالي: https://www. youm7. com/story/2019/11/5 في 2019/11/05، تاريخ الاطلاع 2021/11/08 على الساعة 13:35.

173. البحث الجنائي يلقي القبض على منشأ صفحات وهمية على الفايس بوك قام بالإساءة والتشهير بمواطنين، مقال منشور على الموقع الرسمي لمديرية الأمن العام للمملكة الأردنية الهاشمية، صفحة الأخبار، في 2017/04/03، على الرابط التالي: https://www. psd. gov. jo/index. php/ar/2015-07-07-17-14-02/76-arabi-part/2015-03-10-09-41-44/2015-04-12-05-16-34/3670-1491197263تاريخ الاطلاع: 2021/10/31 على الساعة 12:00.

174. بلحيمر: الجزائر مستهدفة بحرب إلكترونية تقودها جهات أجنبية راهنت على فشل المسار الديمقراطي، مقال منشور على الموقع الرسمي لوزارة الاتصال الجزائرية، في 2021/02/09 على الساعة 13:27، متاح على الرابط التالي: http://www. ministerecommunication. gov. dz/ar/node/9683 تاريخ الاطلاع: 2021/03/09 على الساعة 21:21.

175. التحالف بين الإنتربول والأفريبول يدخل حيز النفاذ، مقال منشور على الموقع الرسمي للمنظمة الدولية للشرطة الجنائية (الإنتربول) متاح على الرابط التالي: https://www. interpol. int/ar/1/1/2020/20 تاريخ الاطلاع 2021/11/20 على الساعة 11:00

176. جدة عبد القادر محمد، الشرطة السعودية تستعد لمواجهة ملف الجرائم الإلكترونية، مقال منشور على الرابط التالي: https://www. alarabiya. net/saudi-today/2013/12/05/تاريخ الاطلاع 2021/06/15 على الساعة 20:23.

177. حسام أبو غزالة، "فؤاد يطالب بسرعة صدور اللائحة التنفيذية لقانون جرائم المعلومات"، مقال منشور على جريدة الوطن المصرية، السبت 02 ماي 2020، متاح على الرابط التالي: https://www. elwatannews. com/news/details/4731772 تاريخ الاطلاع: 03 فيفري 2021.

178. دور الاتحاد الدولي للاتصالات في بث الاطمئنان وبناء الثقة فيما يتعلق باستخدام تكنولوجيا المعلومات والاتصالات، مقال منشور على الموقع الرسمي للاتحاد الدولي للاتصالات، متاح على الرابط التالي: https://www. itu. int/ar/mediacentre/backgrounders/Pages/role-of-ITU-in-building-confidence-and-trust-in-the-use-of-ICTs. aspx تاريخ الاطلاع: 2021/03/08 على الساعة 21:00.

179. دينا الحسيني، تعرف على دور وزارة الداخلية في مواجهة جرائم الإنترنت، الأحد 25 نوفمبر 2018 الساعة 07:00، ، مقال منشور على الرابط التالي: http://www. dotmsr. com/news/196/1268350/ تاريخ الإطلاع: 20 جانفي 2021، على الساعة 12:30.

180. زولا سومر، الرئيس تبون يأمر بتسوية وضعية الصحف الإلكترونية، مقال منشور في مجلة المساء، في 2021/02/06، على الرابط التالي: تاريخ الاطلاع 2021/03/01 على الساعة 21:20.

181. سفيان السهيلي، كيف يمكن تطوير مهام المجلس الأعلى للاتصال وتنويع تركيبته، مقال منشور في 2019/01/11، على الرابط التالي: https://www. turess. com/assabah/4782 تاريخ الاطلاع: 2021/03/25 على الساعة 20:00

182. سيف إبراهيم، "لصد الهجمات. . . هل ينشئ الخليج مركز موحد للأمن السيبراني"، مقال منشور على الرابط التالي: https://allkhaleejonline. net في2020/12/27، سا 20:58، تاريخ الاطلاع: 2021/02/10 على الساعة 18:38،

183. شرطة أبو ظبي: "أمان" طريق الحماية من الابتزاز الإلكتروني، مقال منشور بيوم 2020/12/24، على الرابط التالي: https://www. emaratalyoum. com/local-section/other/2020-12-24-1. 1435848 تاريخ الاطلاع 2021/06/13 على الساعة 20:30.

184. عادل الأبيوكي، دور وزارة الداخلية في تفعيل قانون جرائم تقنية المعلومات، مقال منشور على الجريدة اليومية الأولى في البحرين، العدد 13456 الجمعة 56 ديسمبر 2014، متاح على الرابط التالي: http://www. akhbar-alkhaleej. com/13426/article/60714. html تاريخ الاطلاع: 20 جانفي 2021 الساعة 18:00،

185. عثمان لحياني، وزير جزائري نتعرض لحرب إلكترونية خارجية تستهدف أمن البلاد، 2021/02/09، مقال منشور على الرابط التالي: https://www. alaraby. co.ukتاريخ الاطلاع: 2021/02/18 على الساعة 18:40.

186. عماد محمد، المعاينة في مجال الجرائم الإلكترونية، مقال منشور على موقع حماة الحق، على الرابط التالي: https://jordan-lawyer. com/2022/01/02/inspection-in-cybercrime/ تاريخ الاطلاع: 2022/04/23 على الساعة 16:00.

187. عمر نجيب، الحرب السيبرانية تقود العالم إلى واقع جديد. . . استهداف البنية التحتية والقطاعات العسكرية والحكومية والاقتصادية وتغيير البيئة الثقافية والفكرية، مقال منشور على صحيفة رأي اليوم، 2020/12/22 سا 09:56، على الرابط التالي: https://www. raialyoum. com/index. php/ تاريخ الاطلاع: 2021/02/13 سا 19:30.

188. غادة الشيخ، الفضاء الإلكتروني مسرح جديد للجرائم ضحاياه مراهقون، مقال منشور في جريدة الغد، متاح على الرابط التالي: https://alghad. com في 2016/04/18 على الساعة 19:12.

189. فاطمة الزهراء عبد الفتاح، آليات وضوابط مراقبة مواقع التواصل الاجتماعي، مقال منشور في الخميس 23 فيفري 2017، على الرابط التالي: https://futureuae. com/ar/Mainpage/Item تاريخ الاطلاع: 2021/02/19 على الساعة 10:30.

190. كلمة المدير العام للأمن الوطني، مقال منشور على الموقع الرسمي لمديرية الأمن الوطني الجزائري، متاح على الرابط التالي:https://www. algeriepolice. dz تاريخ الاطلاع 2021/11/20 على الساعة 18:48.

191. كوفيد 19: وزارة الاتصال تحذر من التضليل الإعلامي وخطاب التهويل، مقال منشور على الموقع الرسمي لوزارة الاتصال، في 2020/07/11 على الساعة 19:35 المتاح على الرابط التالي: http://www. ministerecommunication. gov. dz/ar/node/9257 تاريخ الاطلاع 2021/03/06 على الساعة 20:30.

لبيب فهمي، مركز أوروبي لمكافحة الجريمة الإلكترونية، مقال منشور في 2012/03/28، متاح على الرابط التالي: https://www. aljazeera. net/news/reportsandinterviews/2012/3/29/ تاريخ الاطلاع 2021/11/30 على الساعة 12:30.

192. مباركية بن عمراوي، العقيد في الدرك الوطني جمال بن رجم للإذاعة: 95 بالمائة من الجرائم الإلكترونية تم حلها بنجاح، مقال منشور على موقع الإذاعة الجزائرية، في 2018/02/14، سا 21:30، متاح على الرابط التالي: https://www. radioalgerie. dz/news/ar/article/20180214/133919. html تاريخ الاطلاع 2021/02/12 سا 11:00.

193. مدير مكتب التعاون الدولي بالمديرية العامة للأمن الوطني. . . تعزيز التعاون الشرطي الإفريقي أولويات الأفريبول، مقال منشور على الموقع التالي: https://elmaouid. dz بتاريخ 2018/03/14، تاريخ الاطلاع 2021/08/25 على الساعة 18:00.

194. مشعل الحميدان، الداخلية تتصدى لإساءات مواقع التواصل الاجتماعي إلكترونيا، مقال منشور على جريدة العرب الاقتصادية الدولية، الأربعاء 08 أغسطس 2012، متاح على الرابط التالي:

https://www. aleqt. com/2012/08/08/article_681378. html تاريخ الاطلاع: 20 جانفي 2021، على الساعة 13:36.

195. مصطفى زكي، خدمات الداخلية الإلكترونية. كيف تعاقب المتحرش عبر رسائل "فايسبوك"؟، مقال منشور على جريدة بوابة الأهرام، في 2018/11/28، على الساعة 21:23، متاح على الرابط التالي: http://gate. ahram. org. eg/News/2060253. aspx تاريخ الاطلاع: الأحد 31 جانفي 2021 على الساعة 18:15.

196. المصلحة المركزية للجريمة الإلكترونية في مواجهة مجرمي العالم الافتراضي، مقال منشور على جريدة السلام، في 2016/02/13، متاح على الرابط التالي: https://www. djazairess. com/essalam/52564 تاريخ الاطلاع: 2021/06/27 على الساعة 18:20.

197. مقال "الجعيد يدعو لمنظمة عالمية خاصة بالأمن السيبراني"، منشور على جريدة الشرق، الاثنين 2021/02/08، متاح على الرابط التالي: https://www. middle-east-online. comتاريخ الاطلاع: الأربعاء 2021/02/10 سا 17:40

198. مقال حول "المكاتب المركزية الوطنية وتدريب أجهزة الشرطة"، مقال منشور على الموقع الرسمي للمنظمة الدولية للشرطة الجنائية (الإنتربول)، متاح على الرابط التالي: https://www. interpol. int/ar/2/6/2 تاريخ الاطلاع 2021/09/24 على الساعة 13:22

199. مقال حول الدعوة لإستراتيجية وطنية ناجعة لمكافحة الجريمة الإلكترونية الجيش الوطني الشعبي بالمرصاد للتهديدات السيبرانية، مقال منشور على موقع المجلس الشعبي الوطني في 2021/02/09، على الرابط التالي: http://www. apn. dz/ar/plus-ar/actualite-speciale-ar/6429-2021-02-09-19- تاريخ الاطلاع: 2021/02/13 سا 18:30.

200. مقال حول السلامة السيبرانية والأمن الرقمي، منشور على الموقع الرسمي لحكومة دولة الإمارات، متاح على الرابط التالي: https://u. ae/ar-ae/information-and-services/justice-safety-and-the-law/cyber-safety-and-digital-security تاريخ الاطلاع 2021/03/07 على الساعة 20:00.

201. مقال حول دائرة الإشارة وأنظمة المعلومات والحرب الإلكترونية (الجزائر)، منشور على موقع ويكيبيديا على الرابط التالي: https://ar. wikipedia. org تاريخ الاطلاع: 2021/02/13 على الساعة 14:00.

202. مقال حول مهام الإدارة المركزية لوزارة الاتصال، منشور على الموقع الرسمي لوزارة الاتصال الجزائرية على الرابط التالي: http://www. ministerecommunication. gov. dz تاريخ الاطلاع 2021/01/01 على الساعة 15:00.

203. مقال حول مهام مديرية أمن مجتمع المعلومات، منشور على الموقع الرسمي لوزارة البريد والمواصلات السلكية واللاسلكية على الرابط التالي: https://www. mpt. gov. dz تاريخ الاطلاع 2021/02/20 على الساعة 18:00.

204. مقال حول وزارة الدفاع الوطني تنظم الطبعة الثانية لملتقى الأمن والدفاع السيبراني، منشور في الاثنين 25 مارس 2019، على الساعة 13:30، على الرابط التالي: https://www. aps. dz/ar/algerie/68706-2تاريخ الاطلاع :2021/02/17 على الساعة 18:00.

205. مقال منشور على الموقع الرسمي للمنظمة الدولية للشرطة الجنائية (الإنتربول)، متاح على الرابط التالي: https://www. interpol. int/ar/4/6/1 تاريخ الاطلاع 2021/09/17 على الساعة 11:30

206. مقال منشور على الموقع الرسمي للمنظمة الدولية للشرطة الجنائية (للإنتربول)، متاح على الرابط التالي: https://www. interpol. int/ar/1/1/2012/54 consulté le 18/11/2021 à 16h00 تاريخ الاطلاع: 2021/06/17 على الساعة 19:00.

207. مقال منشور في مجلة الاتحاد المصري للتأمين متاح على الرابط التالي: https://www. ifegypt. org/NewsDetails. aspx?Page_ID=1244&PageDetailID=1324 تاريخ الاطلاع 2021/11/06 على الساعة 18:00.

208. مكتب التحقيقات الفيدرالي، مقال منشور على موقع الموسوعة الحرة ويكيبيديا، متاح على الرابط التالي: https://ar. wikipedia. org/wiki/ تاريخ الاطلاع: 2021/06/06 على الساعة 14:00.

209. مناقشات رفيعة المستوى خلال حدث العالم الرقمي الافتراضي للاتحاد لعام 2020 تركز على التكنولوجيا الرقمية في مواجهة جائحة فيروس كورونا، مقال منشور في 2020/11/04، على الموقع الرسمي للاتحاد الدولي للاتصالات، المتاح على الرابط التالي: https://www. itu. int/ar/mediacentre/Pages/pr24-2020-Virtual-Digital-World-technology-COVID-19. aspx تاريخ الاطلاع: 2021/03/07 على الساعة 19:00.

210. نبيل. ق، إنشاء مركز لمكافحة الجريمة المعلوماتية في الجزائر، مقال منشور على الموقع الإخباري جزايرس، في 2008/05/17، على الرابط التالي:https://www. djazairess. com/alfadjr/71333 تاريخ الاطلاع 2021/11/20على الساعة 19:05.

211. هايدي صبري، الشرطة الرقمية. . . أحدث وسائل مكافحة الجريمة في فرنسا، مقال منشور يوم الخميس 2018/02/08، سا 07:40، على الرابط التالي: https://al-ain. com/article/digital-police-france تاريخ الاطلاع: 2021/06/11 سا 20:00.

212. هبة السيد، تنظيم الاتصالات: زيادة باقات الإنترنت المنزلي أبرز إجراءات مواجهة كورونا، مقال منشور يوم الجمعة 2020/07/10 على الساعة 03:06، متاح على الرابط التالي: https://www. youm7. com/story/2020/7/10/ تاريخ الاطلاع: 2021/03/07 على الساعة 14:30.

213. هبة السيد، وزير الاتصالات يبحث مع نظيره الفرنسي تعزيز التعاون المشترك بمجالات الذكاء الاصطناعي، مقال منشور يوم الثلاثاء 2020/10/06 على الساعة 11:41، متاح على الرابط التالي: https://www. youm7. com/story/2020/10/6/ تاريخ الاطلاع: 2021/03/08 على الساعة 19:50.

214. هند دلالي، وزارة البريد تنظم دورة تكوينية للصحفيين حول الذكاء الاصطناعي، مقال منشور في 2021/02/03 على الساعة 15:30، متاح على الرابط التالي: https://www. elikhbaria. com تاريخ الاطلاع 2021/02/24 على 19:00 سا.

215. هيئة مكافحة جرائم الابتزاز الإلكتروني مقال منشور على الموقع الرسمي لوزارة الداخلية للمملكة العربية السعودية على الرابط التالي: https://www. moi. gov. sa تاريخ الاطلاع 2021/06/15 على الساعة 18:00

ثانيا: المراجع الأجنبية:

1) Ouvrages :

A) Eric Filiol et Philippe Richard ; Cyber Criminalité-enquête sur les mafias qui envahissent leweb, Edition Dunod, paris –France, 2006, p 149-150.

B) EricFiliol et Philippe Richard ; Cyber Criminalité-enquête sur les mafias qui envahissent leweb, Edition Dunod, paris –France, 2006.

C) Jean Bradel, A. Varinard ; les grands arrêts de la procédure pénal, arrêt n° 17, Dalloz, 8 Edition, Paris, 2014

D) Kaspersen, computer crimes and others crimes against information technology in the Netherlandsin ;Ulrichsieber(ed),InformationTechnologycrime,kolnetc ;carlHeymannsVerlag 1994.

2) Thèses et Mémoires :

A) Doste Amiegee Maximilien ; La Cyber-surveillance et le secret professionnel, paradoxes ou contradictions, Mémoire D.E.A, université paris.

B) Meier Marsella Carole ; L'effectivité du processus répressif dans le traitement de la cybercriminalité enquéte sur le système juridique français, Thèse de doctorat en droit, soutenue a la faculté du droit de l'université paris 2, le 13/05/2005

C) Mignard Jean pierre ; Cybercriminalité et cyber- répression entre désorde et harmonisation mondiale, These de doctorat, université de paris panthéon- sorbonne, 2004.

3) Articles :.

A) Adeline champagnat, L'office central de lutte contre la criminalité liée aux technologies de l'information et de la communication, revue de cybercriminalité cybermenace et cyberfraude, sous la direction de Irénebouhadana et William grilles, Edition IMODEV, paris, France, 2012.

B) Adeline champagnat, L'office central de lutte contre la criminalité liée aux technologies de l'information et de la communication, revue de cybercriminalité cybermenace et cyberfraude, sous la direction de Irénebouhadana et William grilles, Edition IMODEV, paris, France, 2012.

C) Aude Géry,La stratégie française de cyberdéfense, centre de doctrine et d'enseignement du commandement, mars 2020.

D) Gérard Schoen, La douane face a la cybercriminalité, Revue de cybercriminalité cybermenave et cyberfraude, sous la direction de Irène bouhadana et William dgilles, editionImodev, paris, France, 2012.

E) J.Chevallier, de la cncl au csa, AJDA, 20-02-1989

F) J.chevallier, le nouveau statut de la liberté, AJDA, 20-02-1987.

G) J.chevallier, les instances de régulation de l'audiovisuel, regards sur l'actualité la documentation française, n° 147, janvier 1989.

H) Myriam Quémnéner, la coopération entre les organes de lutte contre la cybercriminalité, pour une stratégie de cyber sécurité français, revue de lamy droits des affaires, num° 87, France, 2013.

I) Myriam Quémnéner, la coopération entre les organes de lutte contre la cybercriminalité, pour une stratégie de cyber sécurité français, revue de lamy droits des affaires, num° 87, France, 2013.
J) Rachid Zouaimia, L'autorité de régulation de l'audiovisuel, Revue Académique de la recherche juridique, volume 17, n° 01, 2018.
K) Rachid Zouaimia, Réflexions sur le pouvoir réglementaire des autorités administratives indépendantes, Revue critique de droit et sciences politiques,volume n° 06 ; Numero 02 , 2011.

5) Documents :

A) Michel Mercier, Rapport n° 491 de fait au nom de la commission des lois, déposé le 23 mars 2016.
B) United Nations, Guidelines concerning Computerized personal data files, Adopted by the General Assembly on 14 december 1990.
C) William Gilles et Jean Harivel et IréneBouhadana –« Darknet le coté obscur du net »- Article publier sur : Panthéon Sorbonne Magazine – Magazine D'information de L'universitéParis 1 Panthéon Sorbonne – Num 06- Janvier – Février – 2014- Paris – France.

6) Textes juridiques :

A) Le constitution française du 04 octobre 1958 avec sa derniére mise à jour de 20 aout 2008

B) Ordonnance n°2020- 1733 du 16 décembre 2020 – art 11 en vigueur le 01/05/2021,code de procédure pénale français.
C) loi n°2020- 936 du 30 juillet 2020- art 17 en vigueur le 01 Aout 2020; code pénal français
D) loi n° 2004- 669 du 9 juillet 2004 art- 121 JORF 10 juillet 2004, code de procédure pénale
E) Arrêt du 21 Octobre 2015, publié au journal officiel du 29 octobre 2015, relatif à l'habilitation au sein de services spécialisés d'officiers ou agents de police judiciaire pouvant procéder aux enquêtes sous pseudonyme.
F) Loi n° 2004- 669 du 9 juillet 2004 art 2, JORF 10/07/2004,en vigueur le 10/07/2004 relative aux communications électronique et aux services de communication audiovisuelle.
G) Loi n° 78-17 du 6 juin 1978 relative à l'informatique, au fichiers et aux libertés.
H) Loi n° 2003-239 du 18 mars 2003 pour la sécurité intérieure en France
I) Royal Decree° WL 22/16.595, Dated 02 July 2015, State Gazette n° 635.897.257
J) Décision n° 96-378 DC de 23 juillet 1996, a propos de l'autorité de régulation des télécommunications, JORF du 27 juillet 1996.
K) Loi n° 2004/575 du 21juin 2004 sur la confiance dans l'économie numérique ;JO, 22 juin 2004 , p 11168.
L) Directive n° 2000/ 31/CE du parlement européen et du Conseil du 08 juin 2000 relative a certains aspecte juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur.
M) Décret n°2000-405 du 15 mai 2000, portant création d'un office central de lutte contre la criminalité liée aux technologies de l'information et de la communication.
N) Arrêt du 21 Octobre 2015, publié au journal officiel du 29 octobre 2015, relatif à l'habilitation au sein de services spécialisés d'officiers ou agents de police judiciaire pouvant procéder aux enquêtes sous pseudonyme.

7) Les articles et les documents électroniques :

A) Canadian anti-fraud centre, Disponible sur le site suivant : https://www.antifraudcentre-centreantifraude.ca/index-eng.htmconsulté le 23/10/2021 à 13h47

B) Canadian centre for cyber security, Disponible sur le site suivant : https://cyber.gc.ca/en/guidance/cybercrime-0consulté le 23/10/2021 à 13h22
C) Cyberpolstrategicframework 2016-2025, Article disponible sur le site suivant : http://cyberpol.infoconsulté le 30/11/2021, à 19 :45
D) Direction centrale de la police judiciare, Disponible sur le lien suivant : https://www.police-nationale.interieur.gouv.fr/Organisation/Direction-Centrale-de-la-Police-Judiciaireconsulté le 30/10/2021 à 18h56
E) Electronic crime cyber council, Disponible sur le site suivant : https://cacp.ca/e-crime-cyber-council-ecc-fr.htmlconsulté le 12/10/2021 à 19h45
F) Gendarmerie vers cybercriminalité, Article disponible sur le site suivant : http://cyberpolice.over-bloc.comconsulté le 18/11/2021 à 15h30
G) How interpol supports Russia to tackle international crime, Article disponible sur le site suivant :https://www.interpol.int/Who-we-are/Member-countries/Europe/RUSSIAconsulté le 16/06/2021, à 19h00
H) La chasse aux criminels sur internet, Article disponible sur le site suivant :https://www.deutschland.de/fr/topic/politique/lutter-contre-la-cybercriminalite-la-police-allemande-et-europol2021/04/18 Consulté le 16/06/2021 à 18h19
I) La police Allemagne, Article disponible sur le site suivant : https://handbookgermany.de/fr/rights-laws/police.html le 16/06/2021, à 18h30
J) Le centre de lutte contre les criminalités numériques, Disponible sur le lien suivant : https://www.gendarmerie.interieur.gouv.fr/pjgn/scrcgn/le-centre-de-lutte-contre-les-criminalites-numeriques-c3nconsulté le 18/11/2021 à 19h26
K) Ministère de l'intérieur, Cyber sécurité la stratégie du ministère de l'intérieur, 25 /01/2016, Article Disponible sur le lien suivant :https://www.interieur.gouv.fr/Archives/Archives-des-dossiers/2016-Dossiers/Securite-les-grands-plans-d-action/Cybersecurite-la-strategie-du-ministere-de-l-Interieu consulté le 20/02/2021, a 10 :00H
L) Oliver Noyan, Montée en flèche de la cybercriminalité en Allemagne,12/05/2021, Article disponible sur le site suivant :https://www.euractiv.fr/section/economie/news/dramatischer-anstieg-der-cyberkriminalitaet-in-deutschland/,Consulté le 16/06/2021, a 18h00
M) Patforme Pharos Disponible sur le lien suivant :https://www.interieur.gouv.fr/A-votre-service/Ma-securite/Conseils-pratiques/Sur-internet/Signaler-un-contenu-suspect-ou-illicite-avec-PHAROS consulté le 30/10/2021 à 13h12
N) Royal canadianmounted police, Disponible sur le site suivant : https ://www.rcmp-grc.gc.ca/ consulté le 12/10/2021 à 19h22
O) S.Nielsen, The role of the U.S military in cyberspace , Journal of information warfare , vol 15, N 02 ; 2016, p 30 ; The link : https://www.jstor.org/stable/26487529
P) SDLC : Sous direction de la lutte contre la cybercriminalité, Disponible sur le lien suivant : https://www.police-nationale.interieur.gouv.fr/Organisation/Direction-Centrale-de-la-Police-Judiciaire/Lutte-contre-la-criminalite-organisee/Sous-direction-de-lutte-contre-la-cybercriminaliteconsulté le 01/11/2021 à 13h00
Q) Service de presse national de FBI : Internet fraud center, disponible sur le lien suivant : http://www.ifccfbi.gov Consulté le 10/10/2021 à 14 :00
R) The national cybercrime coordination unit, Disponible sur le site suivant : https://www.rcmp-grc.gc.ca/en/nc3 Consulté le 12/10/2021 à 17h15
S) Voir la plateforme de signalement sur le lien suivant : www.internet.signalement.gouv.fr
T) Voir le point de contact sur le lien suivant ; www.pointdecontact.net.

فهرس المحتويات

فهرس المحتويات

فهرس المحتويات

ملخص

نتيجة الثورة المعلوماتية التي يشهدها العالم ظهر نوع مستحدث من الجرائم أطلق عليها إسم "الجرائم الإلكترونية" والتي تختلف تماما عن الجرائم التقليدية، في ذاتية أركانها وأساليب إرتكابها والبيئة الافتراضية التي تنشأ فيها، وكذا مرتكبها والذي يطلق عليه إسم "المجرم المعلوماتي"، الأمر الذي استتبعه ضرورة التصدي لهذا النوع من الإجرام، إذ قامت الدول بترشيد نصوصها الجنائية التقليدية بشقيها (الموضوعي والإجرائي) لتصبح نافذة في مواجهة هذه الجرائم.

وقد جاءت هذه الدراسة مقتصرة على الجانب الإجرائي وتحديدا على مرحلة من مراحل التحقيق الجنائي ألا و هي "مرحلة البحث والتحري عن الجريمة الإلكترونية"، حيث تطرقنا أولا إلى معرفة الوحدات المتخصصة في البحث والتحري عن هذه الجرائم وذلك على الصعيدين الدولي والداخلي، وتبيان الدور الوقائي لها في منع وقوع هاته الجرائم، من خلال سلطات الضبط التقليدي وكذا الضبط الإلكتروني، والدور الردعي الذي يتجسد من خلال الضبط القضائي المختص في متابعة هذه الجرائم، وتطرقنا في نقطة ثانية إلى إبراز خصوصية إجراءات البحث والتحري عن هذهالجرائم وما تثيرهمن تحديات أمام سلطات التحقيقوالتي تعود لطبيعة هذه الجرائم ذاتها خاصة البعد الدولي والعالمي الذي تتميز به، وأخرى تعود لطبيعة الدليل الإلكتروني الناتج عن هذه الجرائم خاصة أنه دليل غير مرئي وسهل المحو والتدمير، وأخرى ناتجة عن نقص الخبرة والمعرفة لدى سلطات التحقيق، محاولين بذلك إيجاد حلول عملية لهذه الإشكالات.

الكلمات المفتاحية:

الجريمة الإلكترونية _ إجراءات البحث والتحري _ الدليل الإلكتروني _ الضبط الإداري الإلكتروني _ آليات المكافحة الإجرائية.

Résumé :

À la suite de la révolution informatique à laquelle le monde assiste, un nouveau type de crime est apparu, appelé « cybercriminalité », qui est complètement différent des crimes traditionnels, en termes de ses éléments, ses méthodes de perpétration et de l'environnement virtuel dans d'où il découle, ainsi que son auteur, qui est appelé le « criminel de l'information ». La nécessité de lutter contre ce type de crime, car les pays ont rationalisé leurs textes pénaux traditionnels (à la fois substantiels et procéduraux) pour devenir efficaces dans la lutte contre ces crimes.

Cette étude se limitait à l'aspect procédural et plus particulièrement à l'étape de l'enquête criminelle. "La phase de recherche et d'enquête de la cybercriminalité", où nous avons d'abord abordé la connaissance des unités spécialisées dans la recherche et l'enquête de ces crimes aux niveaux internationaux et internes, Démontrant leur rôle préventif dans la prévention de ces crimes, par les pouvoirs de contrôle traditionnels et le contrôle électronique, Le rôle dissuasif qui est incarné par le contrôle judiciaire compétent dans la poursuite de ces crimes Dans un deuxième point, nous avons

souligné la spécificité des procédures de recherche et d'enquête sur ces crimes et les défis qu'ils posent aux autorités d'enquête,ce qui est dû à la nature de ces crimes eux-mêmes, en particulier la dimension internationale et mondiale qui les caractérise, Une autre est due à la nature de la preuve électronique résultant de ces crimes, d'autant plus qu'elle est invisible et facile à effacer et à détruire et le manque d'expertise et de connaissances de la part des autorités chargées de l'enquête, Il s'agit donc de trouver des solutions pratiques à ces problèmes.

Mots clés :

Cybercriminalité _ procédure de recherche et d'enquête _ la preuve électronique _ Contrôle administratif électronique _ Mécanismes de contrôle procédural.

Abstract :

As a result of the information révolution the world is witnessing, a new type of crime has emerged. "Cybercrime", which is quite different from traditional crimes, in the subjectivity of their éléments, methods of commission and the hypothetical environment in which they arise, as well as the perpetrator and so-called "Information offender", which entailed the need to address this type of crime, as States rationalized their traditional criminal texts (substantive and procedural) to become effective against such offences.

This study was limited to the procedural aspect and specifically to the stage of the criminal investigation. "The search and investigation phase of cybercrime", where we first touched upon the knowledge of specialized units in the search and investigation of such crimes at the internationals and internals levels, Demonstrating their preventive role in preventing such crimes, through traditional control powers as well as electronic control, The deterrent role that is embodied through the competent judicial control in the pursuit of these crimes In a second point, we highlighted the specificity of the procedures for the search and investigation of these crimes and the challenges they pose to the investigative authorities, which are attributable to the very nature of these crimes, especially the international and global dimension that characterizes them. Another is due to the nature of the electronic evidence resulting from these crimes, especially as it is invisible and easy to erase and destroy and the lack of expertise and knowledge on the part of the investigating authorities, thus attempting to find practical solutions to these problems.

Key words :

Cybercrime _ search and investigation procedures _ Electronic Evidence_ Electronic Administrative Control _ Procedural Control Mechanisms.