الآليات الوقائية من جرائم تكنولوجيا الإعلام والاتصال ومكافحتها في القانون الجزائري

Mechanisms to prevent and combat ICT crimes in Algerian law

نجية عراب ثاني ♦

كلية الحقوق والعلوم السياسية-جامعة ابو بكر بلقايد تلمسان-

الجزائر

ntutorat.arabteni@yahoo.fr

تاريخ الإرسال: 2021/05/10	تاريخ القبول: 2022/05/29	تاريخ النشر:2022/06/03

الملخص:

حققت تكنولوجيا المعلومات والاتصالات فوائد عديدة تزايد الاعتماد عليها في مجالات الحياة كافة وبقدر ما أفرزته الوسائل التقنية الحديثة في الرقي والتقدم الإنساني، بقدر ما مهدت إلى بروز أنماط جديدة من الجرائم بالغة الخطورة. هذه الأنماط المستحدثة من الجرائم أدت إلى ضرورة تدخل المشرع الجزائري من اجل مكافحتها والعمل على الوقاية منها.

الكلمات المفتاحية:تدابير – جريمة – معلوماتية – مكافحة

Abstract:

Information and communication technology has achieved many benefits, within creas in greliance on it in all areas of life, to the extent that modem technical means have resulted in huma nadvancement and progress, to the extent that it has paved the way for the emeans of new types of extremely dangerous crimes. These new patterns of crimes led to the necessity of the intervention of the Algerian legislator in order to combat them and work to prevent them.

Keywords:measures - crime - information – combat.

مقدمة:

لقد أصبحت الكثير من الأنشطة اليومية تعتمد اعتمادا كبيرا على تكنولوجيا المعلومات والاتصال، فالمرافق العامة تنظم وتراقب من خلال استخدام أجهزة الكمبيوتر وشبكات الاتصال مثل النقل والإدارات

♦المؤلف المرسل

العمومية. أما في الحياة الخاصة للأفراد فان الكثير من المعاملات والأعمال التجارية تتم عن طريق أجهزة الكمبيوتر كالبيع والشراء الالكتروني والمعاملات البنكية وغيرها.

فقد شهد العالم في الفترة الأخيرة تطورا كبيرا في مجال تكنولوجيات الإعلام والاتصال، التي تقوم بشكل أكبر على الاختراعات الجديدة في مجالي الإلكترونيك والمعلوماتية، و لمسايرة هذا التطور التكنولوجي، كان لابد للدول من إيجاد الإطار القانوني المناسب، بوضع النصوص الملائمة لمختلف استعمالات تكنولوجيا الإعلام و الاتصال.

وعلى الرغم من المزايا الهائلة التي حققت وتتحقق في مجال تقنية المعلومات على جميع الأصعدة و في شتى ميادين الحياة المعاصرة، فان هذه الثورة التكنولوجية المتنامية رافقتها في المقابل جملة من الانعكاسات السلبية الخطيرة جراء سوء استخدام هذه التقنية المتطورة، تجلت في تفشي طائفة من الظواهر الإجرامية المستحدثة، ألا وهي ظاهرة الجرائم المعلوماتية.

ولما كانت الجرائم المعلوماتية ظاهرة حديثة لارتباطها بتكنولوجيا الإعلام والاتصال، كان لابد من تطوير البنية التشريعية الجنائية الوطنية بذكاء تشريعي مماثل تعكس فيه الدقة الواجبة على المستوى القانوني وسائر جوانب وأبعاد تلك التقنية الجديدة.

وعليه نطرح الإشكالية الآتية: ما مدى كفاية النصوص والآليات التي وضعها المشرع الجزائري للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها؟

للإجابة على هذه الإشكالية سوف نقسم هذه الدراسة الى نقطتين، نتناول في النقطة الأولى ماهية الجرائم المتصلة بتكنولوجيا الاعلام والاتصال وصورها ونتناول في نقطة ثانيةمدى فاعلية التشريع العقابي الجزائري في الوقاية من جرائم تكنولوجيا الإعلام والاتصال ومكافحتها.

1- مفهوم الجرائم المتصلة بتكنولوجيا الإعلام والاتصال وصورها:

إن التطور الحاصل في فتكنولوجيا الإعلام والاتصال، وظهور شبكة الانترنت بكل ما حملته من تقدم وخدمات لم يمر على العالم بسلام، لأنه بقدر ما أحدث ثار ايجابية وغير نمط حياة المجتمعات وساهم في التطور والرقي في جميع المجالات ولاسيما المعاملات الالكترونية، بقدر ما كان له اثر سلبي على حياة الناس ومصالح الدول، كل هذا تجلى في تطويع الانترنت والوسائل الالكترونية لتكون عالما من عوالم الجريمة، وهكذا ظهرت إلى الوجود الجريمة الالكترونية بشتى أنواعها.

1.1-مفهوم الجرائم المتصلة بتكنولوجيا الإعلام والاتصال:

تتميز الجرائم الالكترونية عموما بمجموعة من المفاهيم والخصائص تميزها عن غيرها من الجرائم التقليدية، وهو ما سنحاول توضيحه من خلال النقاط الآتية:

الآليات الوقائية من جرائم تكنولوجيا الإعلام والاتصال ومكافحتها في القانون الجزائري

-تعريف الجرائم المتصلة بتكنولوجيا الإعلام والاتصال:

إن الجريمة الالكترونية تتمتع بخطورة إجرامية لم يشهد لها العالم مثلا في الجرائم التقليدية، فلهذا ظهر اختلاف في تعريف هذه الجريمة، فهناك من يعرفها بأنها:" الجريمة التي تتم باستخدام جهاز الكمبيوتر من خلال الاتصال"وهناك من يعرفها على أنها:"كل عمل أو امتناع عن عمل يقوم به شخص إضرارا بمكونات الحاسب المادية أو المعنوية، وشبكات الاتصال الخاصة به باعتبارها من المصالح و القيم المتطورة التي تمتد مظلة قانون العقوبات لحمايتها". أو أنها: "استخدام الأجهزة التقنية الحديثة مثل الحاسب الآلي والهاتف النقال، أو أحد ملحقاتها أو برامجها في تنفيذ أغراض مشبوهة و أمور غير أخلاقية لا يرتضيها المجتمع"[1].

وقد تبنى المشرع الجزائري للدلالة على الجريمة الالكترونية مصطلح المساس بأنظمة المعالجة الآلية للمعطيات معتبرا أن النظام ألمعلوماتي في حد ذاته وما يحتويه من مكونات غير مادية محلا للجريمة ويمثل نظام المعالجة الآلية للمعطيات المسالة الأولية أو الشرط الأولي الذي لابد من تحققه حتى يمكن البحث في توافر أو عدم توافر أركان الجريمة من جرائم الاعتداء على هذا النظام.

كما أعطى المشرع الجزائري تعريفا للمعلوماتية من خلال المادة الثانية فقرة(ب) من القانون رقم 09-04 بأنها:" أي نظام منفصل او مجموعة من الانظمة الأنظمة المتصلة مع بعضها البعض أو مترابطة،يقوم واحد منها أو أكثر معالجة الآلية للمعطيات تنفيذا لبرنامج معين".

لقد حاول المشرع الجزائري مكافحة هذا النوع من الجرائم من خلال إصدار سلسلة من القوانين كان أولها القانون 04-15 المؤرخ في 10 نوفمبر 2004،المتضمن أحكام المساس بأنظمة المعالجة الآلية للمعطيات، و القانون رقم 06-23 المؤرخ في 20 ديسمبر 2006 المتضمن الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، من خلال تجريم كل أنواع الاعتداءات التي تستهدف أنظمة المعالجة الآلية، ثم صدور القانون رقم 09-04 المؤرخ في 05 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها، حيث جاء هذا القانون ليعزز القانونين السابقين، و ذلك من خلال وضع إطار قانوني أكثر ملائمة

مع خصوصية الجريمة المعلوماتية، كما تكمن أهميته في كونه يجمع بين القواعد الإجرائية المكملة لقانون الإجراءات الجزائية و بين القواعد الوقائية التي تسمح بالرصد المبكر للاعتداءات المحتملة و التدخل السريع لتحديد مصدرها و التعرف على مرتكبيها.

وقد نص المشرع الجزائري في المادة الثانية فقرة (أ) من القانون رقم 09-04 المؤرخ في 05 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال ومكافحتها، على أن الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال تتمثل في "جرائم المساس بأنظمة المعالجة الإلية للمعطيات المحددة في قانون

[1] زليخة زيدان، الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى،2011، ص11.

العقوبات و أي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الالكترونية".

فقد جاء القانون المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال ومكافحتها شاملا، ليطبق على كل التكنولوجيات الجديدة و القديمة و على كل تقنية تظهر مستقبلا، لهذا فهو ينطبق على شبكة الاتصالات السلكية و اللاسلكية وعلى نظم المعلوماتية، لأنه لا يمكن استغناء إحداهما على الأخرى، ذلك أن سريان المعلومات من مكان لآخر في العالم كله، والدخول إلى بنوك المعلومات و الحصول على الأبحاث العلمية من المكتبات المجودة في جميع أنحاء العالم، و عرض الكتب العلمية و شركات بيع الأدوية و مختلف السلع، و المؤتمرات التي تنعقد و تدار بواسطة الحاسب الآلي و كل من المجتمعين جالس في مكتبه ببلده و كأنهم مجتمعين بمكان واحد، كل هذه الأعمال و العمليات و غيرها تتم بواسطة شبكات الاتصالات و نظم المعلوماتية، و من ثم لا يمكن أن يكون لشبكة الاتصالات استغناء عن النظم المعلوماتية و كذلك لا يمكن ان يكون هناك استغناء لنظم المعلوماتية عن شبكة الاتصالات[1].

إن الجريمة المتصلة بتكنولوجيا الاعلام والاتصال تتمتع بخطورة إجرامية لم يشهد لها العالم مثلا في الجرائم التقليدية، فلهذا ظهر اختلاف في تعريف هذه الجريمة، فهناك من يعرفها بأنها:" الجريمة التي تتم باستخدام جهاز الكمبيوتر من خلال الاتصال"وهناك من يعرفها على أنها:"كل عمل أو امتناع عن عمل يقوم به شخص إضرارا بمكونات الحاسب المادية أو المعنوية، و شبكات الاتصال الخاصة به باعتبارها من المصالح و القيم المتطورة التي تمتد مظلة قانون العقوبات لحمايتها".أوأنها:"استخدام الأجهزة التقنية الحديثة مثل الحاسب الآلي والهاتف النقال، أو احد ملحقاتها أو برامجها في تنفيذ أغراض مشبوهة و أمور غير أخلاقية لا يرتضيها المجتمع"[2].

وقد تبنى المشرع الجزائري للدلالة على الجريمة الالكترونية مصطلح الجرائم المتصلة بتكنولوجيا الاعلام والاتصال معتبرا أن النظام ألمعلوماتي في حد ذاته وما يحتويه من مكونات غير مادية محلا للجريمة ويمثل نظام المعالجة الآلية للمعطيات المسالة الأولية أو الشرط الأولي الذي لابد من تحققه حتى يمكن البحث في توافر أو عدم توافر أركان الجريمة من جرائم الاعتداء على هذا النظام.

كما أعطى المشرع الجزائري تعريفا للمعلوماتية من خلال المادة الثانية فقرة(ب) من القانون رقم 09-04 بأنها:" أي نظام منفصل او مجموعة من الأنظمة المتصلة مع بعضها البعض أو مترابطة يقوم واحد منها أو أكثر معالجة الآلية للمعطيات تنفيذا لبرنامج معين".

لقد حاول المشرع الجزائري مكافحة هذا النوع من الجرائم من خلال إصدار سلسلة من القوانين كان أولها القانون 04-15 المؤرخ في 10 نوفمبر 2004،المتضمن أحكام المساس بأنظمة المعالجة الآلية للمعطيات، و القانون رقم 06-23 المؤرخ في 20 ديسمبر 2006 المتضمن الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، من

[1]- احمد حسام طه، الجرائم الناشئة عن استخدام الحاسب الالي، دار النهضة العربية، 2002، ص113.

[2]زليخة زيدان، الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى،2011، ص11.

خلال تجريم كل أنواع الاعتداءات التي تستهدف أنظمة المعالجة الآلية، ثم صدور القانون رقم 09-04 المؤرخ في 05 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها، حيث جاء هذا القانون ليعزز القانونين السابقين، و ذلك من خلال وضع إطار قانوني أكثر ملائمة

مع خصوصية الجريمة المعلوماتية، كما تكمن أهميته في كونه يجمع بين القواعد الإجرائية المكملة لقانون الإجراءات الجزائية وبين القواعد الوقائية التي تسمح بالرصد المبكر للاعتداءات المحتملة والتدخل السريع لتحديد مصدرها والتعرف على مرتكبيها.

وقد نص المشرع الجزائري في المادة الثانية فقرة (أ) من القانون رقم 09-04 المؤرخ في 05 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، على أن الجرائم المتصلة بتكنولوجيا الإعلام والاتصال تتمثل في "جرائم المساس بأنظمة المعالجة الإلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الالكترونية".

فقد جاء القانون المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال ومكافحتها شاملا، ليطبق على كل التكنولوجيات الجديدة و القديمة و على كل تقنية تظهر مستقبلا، لهذا فهو ينطبق على شبكة الاتصالات السلكية و اللاسلكية وعلى نظم المعلوماتية، لأنه لا يمكن استغناء إحداهما على الأخرى، ذلك أن سريان المعلومات من مكان لآخر في العالم كله، والدخول إلى بنوك المعلومات و الحصول على الأبحاث العلمية من المكتبات المجودة في جميع أنحاء العالم، و عرض الكتب العلمية و شركات بيع الأدوية و مختلف السلع، و المؤتمرات التي تنعقد و تدار بواسطة الحاسب الآلي و كل من المجتمعين جالس في مكتبه ببلده و كأنهم مجتمعين بمكان واحد، كل هذه الأعمال و العمليات و غيرها تتم بواسطة شبكات الاتصالات و نظم المعلوماتية، و من ثم لا يمكن أن يكون لشبكة الاتصالات استغناء عن النظم المعلوماتية و كذلك لا يمكن ان يكون هناك استغناء لنظم المعلوماتية عن شبكة الاتصالات[1].

-خصائص الجرائم المتصلة بتكنولوجيا الإعلام والاتصال:

تتسم الجرائم الالكترونية بجملة من الخصائص تميزها عن غيرها من الجرائم يمكن إجمالها فيما يلي:

- **جرائم عابرة للحدود:**

لقد وسعت شبكات المعلومات عملية الاتصال و تبادل المعلومات بين الدول و الأنظمة التي يفصل بينها آلاف الأميال، وقد انعكست قدرة تقنية المعلومات على اختصار المسافات و تعزيز الصلة بين مختلف أنحاء العالم على طبيعة الأعمال الإجرامية التي يعمد فيها المجرمون إلى استخدام هذه التقنيات في خرقهم للقانون، و هو ما يعني أن مسرح الجريمة المعلوماتية لم يعد محليا بل أصبح عالميا، إذ أن الفاعل لا يتواجد على مسرح

[1]- احمد حسام طه، الجرائم الناشئة عن استخدام الحاسب الالي، دار النهضة العربية، 2002، ص113.

الجريمة بل يرتكب جريمته عن بعد، و هو ما يعني عدم التواجد المادي لحصول الجريمة الالكترونية في مكان الجريمة و من ثم تتباعد المسافات بين الفعل الذي يتم من خلال جهاز كمبيوتر الفاعل و بين المعلومات محل الاعتداء، فقد يوجد الجاني في بلد ما و يستطيع الدخول إلى ذاكرة الكمبيوتر الموجود في بلد آخر، و هو بهذا السلوك قد يضر شخصا آخر موجود في بلد ثالث[1].

- **جرائم خفية ومستترة:**

لا تترك هذه الجرائم أثر لها بعد ارتكابها، مما يصعب الاحتفاظ الفني بآثارها إن وجدت، فحتى الضحية لا يلاحظها رغم أنها قد تقع أثناء وجوده على الشبكة، لان الجاني يتمتع بقدرات فنية تمكنه من تنفيذ جريمته بدقة، كالتجسس وسرقة المكالمات وإتلاف البيانات وغيرها من الجرائم[2].

وإثباتها وهذا كله يصعب من مهمة المحقق العادي في التعامل معها، حيث يستخدم فيها وسائل فنية غير عادية تعتمد التمويه في ارتكابها والتضليل في التعرف على مرتكبيها، وفي كل الأحوال تحتاج مواجهة هذه إلى خبرة فنية عالية متخصصة لإثباتها.

- **جرائم صعبة الإثبات:**

تمتاز الجرائم المعلوماتية بصعوبة الاكتشاف والإثبات وذلك نظرا لعدم ترك الجاني آثار تدل على إجرامه، فالجرائم التي تتم بواسطة إدخال الرموز والأرقام يصعب اكتشافها. فالجريمة المعلوماتية لا تترك آثار ملموسة وبذلك لا تترك شهودا يمكن الاستدلال بأقوالهم ولا أدلة مادية يمكن فحصها لأنها تقع في بيئة افتراضية يتم فيها نقل المعلومات وتناولها بواسطة نبضات الكترونية غير مرئية[3].

ويصعب في الجرائم المعلوماتية العثور على دليل مادي للجريمة وذلك راجع إلى استخدام الجاني وسائل فنية و تقنية معقدة في كثير من الأحيان، وهذا السلوك المادي في ارتكابها لا يستغرق إلا ثواني معدودة يتم فيها محو الدليل و التلاعب به[4].

- **جرائم هادئة:**

إذا كانت الجريمة التقليدية تحتاج إلى مجهود عضلي في ارتكابها كالقتل و السرقة وغيرها من الجرائم، فالجرائم الالكترونية لا تحتاج ادني مجهود عضلي بل تعتمد على الدراسة الذهنية، و التفكير العلمي المدروس القائم على معرفة تقنية الكمبيوتر وذلك يعود لكون هذا النوع من الجرائم عبارة عن معطيات و بيانات تتغير أو تعدل أو تمحى من السجلات المخزنة في ذاكرة الحاسوب، إلا أن البعض يشبهها بجرائم العنف مثل ما ذهب إليه

[1]- نائلة عادل، محمد فريدة قوره، جرائم الحاسب الآلي الاقتصادية، منشورات الحلبي الحقوقية، 2005، ص65.
[2]-هشام محمد فريد، الجوانب الإجرائية للجرائم المعلوماتية، مكتبة الآلات الحديثة، مصر،1994، ص135.
[3]-سعيد نعيم، آليات البحث والتحري المعلوماتية في القانون الجزائري، مذكرة ماجستير، جامعة الحاج لخضر باتنة،2012-2013، ص56.
[4]- هشام محمد فريد، المرجع السابق، ص211.

مكتب التحقيقات الفدرالي بالولايات المتحدة الأمريكية، نظرا لتماثل دوافع المعتدين على نظم الحاسب الآلي مع مرتكبي العنف[1].

- **صفة مرتكبها:**

مرتكب الجريمة يسمى بالمجرم المعلوماتي، وهو في الغالب شخص يتميز بالذكاء والدهاء ذو مهارات تقنية عالية وعلى دراية بالأسلوب المستخدم في مجال أنظمة الحواسب وكيفية تشغيله وكيفية تخزين المعلومات والحصول عليها.

2.1صور الجرائم المتصلة بتكنولوجيا الإعلام والاتصال:

وعليه سوف نحاول الوقوف على مختلف صور هذا النوع من الجرائم من خلال النقاط الآتية:

-الدخول أو البقاء الغير مشروع في منظومة معلوماتية:

تنص المادة 394 مكرر من القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004، على عقوبة الحبس من ثلاثة أشهر إلى سنة، وبغرامة مالية من 50.000 دج إلى 200.000 دج لكل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك.و تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة.

وإذا ترتب على الأفعال السابقة تخريب نظام اشتغال المنظومة تكون العقوبة الحبس من ستة أشهر إلى سنتين والغرامة من 50.000 دج إلى 300.000 دج. وقد أورد المشرع ظرف تشديد إذا استهدفت الجريمة الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام وهي غالبا مؤسسات تقدم خدمات عمومية.

يتضح من نص المادة أن هذا النوع من الجرائم يشمل كل الأفعال التي تنال من أنظمة الكمبيوتر، وسلامتها، وسريتها، والوثوق بها، وإمكانية استخدامها، ويشمل أيضا الدخول على النظام وإجراء تعديلات غير مشروعة عليه.

كما تشمل أيضا جرائم القرصنة »hacking« والاختراق »cracking« حيث يقوم شخص غير مرخص له بالدخول على نظام كمبيوتر معين[2].

ويرى البعض أن صور الدخول إلى النظام قد يكون بقيام الشخص بإدخال برنامج داخل الجهاز بحيث يقتصر دوره على التجسس بتسجيل نظام دخول المشتركين الأمر الذي يتيح له إمكانية الاحتفاظ بهذه المعلومات، وقد يتم الدخول باستغلال ضعف الرقابة الداخلية للدخول إلى الجهاز[1].

[1]-محمد رحموني، خصائص الجريمة الالكترونية ومجالات استخدامها، مجلة الحقيقة، العدد 41، 2018، ص64.

[2]- نورة طرشي، مكافحة الجريمة المعلوماتية، مذكرة ماجستير، جامعة الجزائر، 2011-2012، ص145.

ولتوافر القصد الجنائي في هذه الجريمة لابد أن يكون الجاني محيطا علما بكافة عناصر الجريمة و له علم بان الفعل الذي يقوم به ينصب على نظام المعالجة الآلية للمعطيات بما يتضمنه من معلومات برامج، واعتبار محل الحق الذي يحميه المشرع[2].

بمعنى أخر اتجاه إرادة الجاني إلى فعل الدخول أو فعل البقاء و أن الجاني يعلم بان ليس له الحق في الدخول إلى النظام و البقاء فيه. ولا يتوافر القصد الجنائي إذا كان الجاني يعتقد أن دخوله أو بقائه داخل النظام مسموح له أي مشروع، أو كان الجاني يجهل بوجود حضر الدخول أو البقاء[3]. فإذا اعتقد الفاعل بناءا على أسباب معقولة بأنه يقوم على سبيل المثال بإجراء بعض العمليات الحسابية عن طريق الحساب الآلي، دون أن يتجه علمه إلى انه يقوم بالدخول أو البقاء في نظام المعالجة الآلية للمعطيات، فان قصد الدخول أو البقاء لا يتوافر فيه[4].

-التصميم والبحث والاتجار للمعطيات المخزنة وإفشائها:

تنص المادة 394 مكرر2 من القانون رقم 06-23 على عقوبة الحبس من شهرين إلى ثلاث سنوات، وبغرامة مالية من 1000.000دج إلى 10.000.000 دج لكل من قام عمدا أو عن طريق الغش بما يأتي:

-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.

-حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان، المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في القسم.

يقصد المشرع هنا جريمة الاحتيال ألمعلوماتي التي يستخدم فيها الجاني كافة الوسائل التقنية للتوصل إلى البيانات المالية أو التي تتصل بحقوق مالية أو قيامه بأعمال احتيالية موجهة لنظام الكمبيوتر فيجني المنافع المادية عن طريق العبث بالبيانات أو البرامج أو حتى عمليات النظام ذاته. أو الاحتيال باستغلال مواقع الانترنت لجني مبالغ مالية عبر مشاريع وهمية لمنتجات أو خدمات أو من خلال الوصول إلى أرقام بطاقات الائتمان[5] .

إن هذا الاستخدام يكون عمديا ويتمثل في التصميم أو البحث أو التجميع أو التوفير أو النشر أو الاتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية، و يكون هذا الاستخدام عن طريق الغش فلذلك يتطلب القصد الجنائي العام إضافة إلى القصد الجنائي الخاص المتمثل في نية الغش[6].

---

[1]-عبد الله بن مسعود محمد السرياني، فاعلية الأساليب المستخدمة في إثبات جريمة التزوير الالكتروني، مطبع جامعة نايف العربية للعلوم الأمنية، الرياض،2011، ص211.

[2]- نائلة عادل، محمد فريدة قوره، المرجع السابق، ص143.

[3]- أمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، دار هومة، الجزائر، 2007، ص89.

[4]- نائلة عادل، محمد فريدة قوره، المرجع السابق، ص150.

[5]-علي عبد القادر قهوجي ، الحماية الجزائية لبرامج الحساب الآلي، دار الجامعة الجديدة، الإسكندرية، 2010، ص136.

[6]- أمال قارة، المرجع السابق، ص155.

أما في الفقرة الثانية من المادة 394 مكرر2 فقد حدد المشرع النتيجة المتوصل من خلال ارتكاب الغش في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية، وأولها الحيازة و التي يقصد بها نقل الشيء أو نزعه من حيازة المجني عليه و إدخاله في حيازة الجاني بشرط أن يكون على جهاز أو أوراق أو أي شيء مادي.أما إذا احتفظ الشخص بالمعلومة في ذهنه دون تسجيل أو تدوين فانه لا يقع تحت طائلة قانون العقوبات.

أما بالنسبة للعقوبات فتتمثل في العقوبة الأصلية والمتمثلة في الحبس و الغرامة بالنسبة للشخص الطبيعي، أما بالنسبة للشخص المعنوي فقد نصت المادة 394 مكرر4 على توقيع عقوبة الغرامة التي تعادل خمس مرات الحد الأقصى للغرامة المحددة للشخص الطبيعي عند ارتكاب إحدى الجرائم المنصوص عليها في القسم السابع مكرر، غير أن المسؤولية الجزائية للشخص المعنوي لا تستبعد المسؤولية الجزائية للأشخاص الطبيعيين بصفتهم فاعلين أو شركاء أو متدخلين في نفس الجريمة.

كما عاقب المشرع الجزائري على الشروع في الجريمة المعلوماتية بالعقوبة المقررة للجريمة ذاتها وذلك طبقا لنص المادة 394 مكرر 7 من قانون العقوبات.

أما بالنسبة للعقوبات التكميلية فتتمثل في مصادرة الأجهزة والبرامجو الوسائل المستخدمة في الجريمة و ذلك طبقا لأحكام المادة 394 مكرر 6 من قانون العقوبات.

-التزوير في المحررات الالكترونية:

من أهم الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال و التي لا تتم عن طريق نظام المعالجة الآلية للمعطيات أو عن طريق نظام اتصالات الكترونية،جريمة التزوير في المحررات الالكترونية و التي ظهرت بالتوازي مع انتشار استخدام هذه المحررات بشكل متزايد خاصة مع ظهور فكرة الحكومة الالكترونية التي تستند عليها في تقديم خدماتها للأشخاص، وأيضا تعتمد عليها البنوك و شركات التامين و المستشفيات في أداء مهامها،فضلا عن ذلك اتخذتها التشريعات الحديثة كوسيلة لإثبات كل المعاملات و الصفقات التي تقتضيها فكرة التجارة الالكترونية التي سهلت التعامل التجاري بالمحررات الالكترونية و سرعة الإنتاج وتوفير النفقات.

فالتزوير في المحررات الالكترونية هو تغيير الحقيقة عمدا بأي طريقة كانت في محرر الكتروني اعد لإثبات حق أو واقعة لها آثار قانونية، تغييرا من شانه إلحاق ضرر بالغير، وبنية استعماله فيما زور لأجله.

يتضح من خلال هذا التعريف أن فعل التزوير يقوم على عناصر مادية و عناصر معنوية و عناصر خاصة أو مفترضة، إذ تمثل العناصر المادية في تغيير الحقيقة التي تتسبب في إلحاق الضرر، ويقصد بتغيير الحقيقة و إبدالها بغيرها أو إنشاء حقيقة مخالفة أو تحريف حقيقة قائمة، وإذا ظلت الحقيقة على حالها دون تغيير، فلا تزوير حتى و لو كان الفاعل معتقدا أن ما أتى به مخالف للواقع، لان العبرة بالواقع لا بما توهمه الفاعل، وعليه فتغيير الحقيقة يخرج المحرر في صورة غير الصورة التي أنشئ من اجلها، ولا يكفي للعقاب على التزوير مجرد

تغيير الحقيقة بل لابد أن يتسبب في إحداث ضرر سواء أوقع أو كان محتمل الوقوع في وقت ارتكاب الجريمة، ويتوقع وقوع الضرر وفقا لما تنبئ به تجربة الحياة وفق تقدير الرجل العادي[1].

أما الركن المعنوي لجريمة التزوير فيتمثل في القصد العام وهو القصد ألعمدي بعنصريه العلم و الإرادة لدى الفاعل، أما القصد الجنائي الخاص، فقد استقر الفقه و القضاء أن القصد الخاص المتطلب لقيام الركن المعنوي للتزوير هو اتجاه نية المزور لحظة فعل تغيير الحقيقة إلى استعمال المحرر فيما زور من اجله، ذلك أن التزوير لا يشكل خطرا اجتماعيا يقتضي تدخل القانون الجنائي لتجريمه إلا إذا ارتكب بنية استعمال المحرر بعد تزويره.

وفيما يتعلق بالعناصر الخاصة فتتمثل في أن ينصب تغيير الحقيقة على محرر الكتروني وان يتم بأي طريقة كانت؛ والمحرر الالكتروني هو عبارة عن دعامة الكترونية للتعبير عن الفكر تتمثل في الأقراص الآلية و المرنة و الممغنطة، وأشرطة الفيديو، وشرائح العرض، والأشرطة الممغنطة.....الخ. وتحمل كتابة في شكل الكتروني وهي عبارة عن تسلل حروف أو أرقام أو أوصاف أو أية علامات أو رموز ذات معنى مفهوم ، تعالج عن طريق المكونات المادية و المعنوية لأنظمة الحوسبة و الاتصالات ثم تسجل على دعامة مغناطيسية منفصلة على النظام تحمل الطابع الافتراضي ، بحيث لا يمكن إطلاقا قراءتها أو إدراكها بالعين المجردة ،إلا من خلال عرضها على شاشة الحاسب الآلي ، ليفك رموز شفرتها. ويتم تغيير الحقيقة في هذه الكتابة الالكترونية أما أثناء معالجة و تحليل البيانات داخل الحاسب لتخرج في النهاية بشكل مزور أو ينصب مباشرة على مخرجات الحاسب أي على الكتابة الخارجة منه والمثبتة على الدعائم أو المحررات المغناطيسية، ويفهم من ذلك أن التزوير الواقع على المحررات الالكترونية، لا يقع إطلاقا على الكتابة أو المعطيات أو البيانات التي يحتويها نظام المعالجة الآلية أي المسجلة في ذاكرته وهي احد عناصره المادية والتي تشكل جزءا منه[2]. إنما يقع على مستخرجات أو منتجات النظام، أي البيانات المنفصلة عنه.

ويتم تغيير الحقيقة في المحررات الالكترونية بعدة طرق، واهم هذه الطرق أدوات كسر-كلمات السر-أو برامج فك التشفير، ووسيلة التقاط الأشعة المنبعثة من الحاسب و غيرها[3].

لقد جرمت اغلب التشريعات التزوير في المحررات الالكترونية، إلا أن خطتها في موضع النص على التجريم اختلفت، فمنها من عدلت نصوص التجريم التقليدية في قانون العقوبات وأدخلت عليها أن التزوير كما يمكن أن يقع على المحررات الورقية فانه يقع كذلك على المحررات الالكترونية، ومن أمثلتها قانون العقوبات الفرنسي-الصادر في 1992/12/61،الذي دخل حيز التنفيذ سنة1994، في مادته 1/441، إذ أتى النص عاما ليشمل التزوير بنوعيه العادي و الالكتروني، وهو ما عبر عنه بعبارة:".....في محرر مكتوب أو كل دعامة أخرى

[1]-الهام بن خليفة، الإشكالات التي تثيرها الفقرة"أ" في المادة الثانية من قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، مجلة العلوم القانونية والسياسية-العدد 10، جنفي 2015، ص 170.

[2]- علي عبد القادر قهوجي، المرجع السابق، ص139.

[3]- عبد الله بن مسعود محمد السرياني، المرجع السابق، ص96.

للتعبير عن الفكر ..."وهو ما ورد أيضا في الفصل 172 من المجلة الجنائية التونسية التي مفادها ان العقوبة تكون مستوجبة على كل من قام بصنع وثيقة مكذوبة أو تغيير متعمد للحقيقة بأي وسيلة كانت في كل سند سواء كان ماديا أو غير مادي من وثيقة معلوماتية أو الكترونية أو ميكروفيلم أو ميكروفيش ويكون موضوعه إثبات حق أو واقعة منتجة لأثار قانونية.

اما بالنسبة للمشرع الجزائري فانه يتضح من نص المادة الثانية فقرة "أ" المشار إليها سابقا، أنها لم تستوعب صورة التزوير في المحررات الالكترونية بالرغم من عمومية النص، لان العموم كان مندرج في الأنظمة المعلوماتية وأنظمة الاتصالات، في حين أن هذا النوع من التزوير يقع فحسب على مخرجات النظام المنفصلة عنه، والمحمولة على وسائط الكترونية.

وعلى الرغم من اعتراف المشرع الجزائري بالمحررات الالكترونية كوسيلة لإثبات التصرفات المدنية والتجارية، والمساواة في الحجية بالمحررات الورقية، شريطة إمكانية التأكد من هوية صاحبها وان تكون معدة ومحفوظة في ظروف تضمن سلامتها. غير انه لم يضفي عليها الحماية الجنائية من التزوير الذي يمكن أن يقع عليها، إذ بالرجوع إلى نصوص التزوير في المحررات في قانون العقوبات نلاحظ انه لا يوجد أي تعديل ادخل عليها بشأن تزوير المحررات الالكترونية، وكل ما في الأمر انه فقط أضفى عليها حماية تقنية من ضرورة التشفير بمفتاحين[1].وضرورة حصول صاحب التوقيع الالكتروني -على المحرر- على شهادة تصديق الكتروني موصوفة تسلمها له الإدارة المختصة، وهذا بموجب التوقيع و التصديق الالكتروني[2].

2-السياسة الجزائية في الوقاية من جرائم تكنولوجيا الإعلام والاتصال ومكافحتها:

لقد حاول المشرع الجزائري من خلال القانون 04/09 أن يضع الإطار القانوني الذي يتلاءم مع خصوصية الجريمة الافتراضية، ويجمع بين القواعد الإجرائية المكملة لقانون الإجراءات الجزائية وبين القواعد الوقائية التي تسمح بالرصد المبكر للاعتداءات المحتملة والتدخل السريع لتحديد مصدرها والتعرف على مرتكبيها.

وعيه سوف نحاول الوقوف على هذه القواعد الوقائية والإجرائية التي وضعها المشرع الجزائري للوقاية من هذه الجرائم ومكافحتها وذلك من خلال النقاط الآتية:

1.2- الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها:

لقد تم النص على تشكيلة وتنظيم وكيفية سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال بموجب المرسوم الرئاسي 15-261 المؤرخ في 08 أكتوبر 2015، إلا انه تم إلغاء ما جاء في

[1]- الهام بن خليفة، المرجع السابق، ص171.

[2]-القانون رقم 15-04 مؤرخ في أول فبراير سنة 2015يحدد القواعد العامة المتعلقة بالتوقيع و التصديق، الجريدة الرسمية للجمهورية الجزائرية، العدد6 .

هذا المرسوم وذلك بصدور مرسوم 19-172 المؤرخ في 06 يونيو 2019 والذي أعاد تحديد تشكيل الهيئة وتنظيمها وكيفية سيرها.

-تعريف الهيئة:

نص المرسوم الرئاسي 19-172 في مادته الأولى على انه تطبيقا لأحكام المادة 13 من القانون 04-09 المؤرخ في 05 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال و مكافحتها، يهدف هذا المرسوم إلى تحديد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها التي تدعى في صلب النص "الهيئة" ، والتي عرفتها المادة الثانية من نفس المرسوم على أنها سلطة إدارية مستقلة تتمتع بالشخصية المعنوية و الاستقلال المالي توضع تحت سلطة وزارة الدفاع الوطني، بعد ما كانت توضع لدى وزير العدل في المرسوم 15- 261 المشار إليه أعلاه.

كما تخضع الهيئة لمجموع الأحكام التشريعية والتنظيمية المطبقة في وزارة الدفاع الوطني.

-مهام الهيئة:

تمارس الهيئة المهام المنصوص عليها في المادة 14 من القانون 04-09، والمواد 11،9،12 من المرسوم الرئاسي 19-172 والمتمثلة فيما يلي:

-اقتراح عناصر الإستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

-تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

-مساعدة السلطات القضائية ومصالح الشرطة القضائية في مجال مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، وذلك من خلال جمع المعلومات والتزويد بها من خلال الخبرات القضائية.

-ضمان المراقبة الوقائية للاتصالات الالكترونية قصد الكشف عن الجرائم التي تحتاج إلى أساليب خاصة في التحري.

-جمع وتسجيل وحفظ المعطيات الرقمية وتحديد مصدرها وتتبعها بغرض استعمالها في الإجراءات القضائية

-تبادل المعلومات مع مثيلاتها الأجنبية بغرض تجميع كل المعطيات المتعلقة بتحديد مكان مرتكبي الجرائم المتصلة بتكنولوجيات الإعلام والاتصال والتعرف عليهم.

-تشكيل الهيئة وتنظيمها:

تظم الهيئة مجلس توجيه ومديرية عامة:

***مجلس التوجيه:**

يترأس مجلس التوجيه وزير الدفاع الوطني أو ممثله وهو يتشكل من ممثلي الوزارات الآتية:

-وزارة الدفاع الوطني.

-الوزارة المكلفة بالداخلية.

-وزارة العدل.

-الوزارة المكلفة بالمواصلات السلكية واللاسلكية.

وتتمثل مهام المجلس فيما يلي:

-التداول حول الإستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

-التداول حول مسائل التطوير والتعاون مع المؤسسات والهيئات الوطنية المعنية بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

-القيام دوريا بتقييم حالة التهديد في مجال الجرائم المتصلة بتكنولوجيات الإعلام والاتصال للتمكن من تحديد مضامين عمليات المراقبة الواجب القيام بهاو الأهداف المنشودة بدقة.

-اقتراح كل نشاط يتصل بالبحث وتقييم الأعمال المباشرة في مجال الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

الموافقة على برنامج عمل الهيئة وإعداد نظام داخلي والمصادقة عليه.

-إبداء الرأي في كل مسالة تتصل بمهام الهيئة وتقديم كل اقتراح يتصل بمجال الهيئة والمصادقة عليه.

-المساهمة في ضبط المعايير القانونية في مجال اختصاصه ودراسة مشروع ميزانية الهيئة والموافقة عليه[1].

يقوم مجلس التوجيه بالاجتماع في دورة عادية مرتين في السنة باقتراح من رئيسه، كما يمكنه أن يجتمع في دورة غير عادية كلما كان ذلك ضروريا، بناءا على استدعاء من رئيسه أو بطلب من أحد أعضائه أو من المدير العام للهيئة.

***المديرية العامة:**

يدير المديرية العامة مدير، حيث تتمثل صلاحيات المديرية فيما يلي:

-السهر على حسن سير الهيئة وإعداد الميزانية.

[1]- المرسوم الرئاسي رقم 19-172، المؤرخ في 26جوان 2019، يحدد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها وتنظيمها وكيفية سيرها.

-إعداد وتنفيذ برنامج عمل الهيئة.

-تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

-إعداد التقرير السنوي لنشاطات الهيئة.

وتظم المديرية العامة مديريتين:

***المديرية التقنية:**

تكلف المديرية التقنية طبقا لأحكام المادة 11 من المرسوم الرئاسي 19-172 بمهمة المراقبة الوقائية للاتصالات الالكترونية في إطار الوقاية من الجرائم الموصوفة بالأفعال الإرهابية والتخريبية والاعتداء على امن الدولة.

كما تتولى المديرية طبقا لأحكام المادة 12 من المرسوم الرئاسي 19-172 مهمة مساعدة السلطات القضائية ومصالح الشرطة بناءا على طلبها، بما في ذلك مجال الخبرات القضائية في إطار مكافحة الجريمة المتصلة بتكنولوجيات الإعلام والاتصال والجرائم التي تتطلب اللجوء إلى أساليب التحري الخاصة.

ومن مهام المديرية أيضا، جمع وتسجيل وحفظ المعطيات الرقمية وتحديد مصدرها وتتبعها بغرض استعمالها في الإجراءات القضائية.

***مديرية الإدارة والوسائل:**

تتمثل مهام مديرية الإدارة والوسائل على الخصوص في:

- تسيير الموارد البشرية والوسائل والمالية الخاصة بالهيئة.

- الإسناد التمويني والتقني للهيئة.

- صيانة العتاد والوسائل والمنشئات القاعدية.

- إعداد احتياجات الهيئة في إطار تحضير تقديرات الميزانية.

وبالإضافة الى الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال، تم استحداث المصلحة المركزية لمكافحة الجريمة المعلوماتية على مستوى المديرية العامة للأمن الوطني سنة 2011، ليتم بعدها انشاء المصلحة المركزية لمكافحة الجرائم المتصلة بتكنولوجيا الاعلام والاتصال سنة 2015.

2.2- الأساليب الإجرائية للكشف عن الجرائم المتصلة بتكنولوجيا الإعلام والاتصال:

تعتبر الضبطية القضائية صاحبة الاختصاص الأصيل في الكشف أو في التحري عن الجرائم عموما، وفي سبيل كشفها عن هذه الجرائم، أعطاها القانون سلطة التحري عن الجرائم، كما منحهم قانون الوقاية من

الفساد ومكافحته وكذا قانون الإجراءات الجزائية الجديد أساليب جديدة للتحري، أسماها "أساليب التحري الخاصة"، كما أضافت التأكيد على اعتبار جرائم المساس بأنظمة المعالجة الآلية للمعطيات من الجرائم التي قرر المشرع صراحة وبنص صريح إمكانية إتباع إجراءات التحري الخاصة في الكشف عنها ومكافحتها، نص المادة 04 من القانون 04/09 المؤرخ في 5 أوت 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، التي قررت الفقرة الثانية منها أنه: " في حالة توافر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني".

وقد سارع المشرع الجزائري بتعديل قانون الإجراءات الجزائية تماشيا مع التطور ألمعلوماتي الذي لحق بالجريمة، محاولة منه تطويقها والقضاء عليها أو على الأقل الحد من انتشارها، وذلك في إطار المكافحة الإجرائية لهذا النوع من الإجرام، حيث وضع قواعد وأحكام خاصة لسلطة التحري والمتابعة الغرض منها هو مواجهتها[1]. وقد وردت هذه الأساليب في قانون الإجراءات الجزائية المعدل والمتمم بموجب القانون 22/06 الصادر في 2006/12/20، وقانون الوقاية من الفساد ومكافحته رقم 01/06 المؤرخ في 20 فيفري 2006، وهي: أسلوب اعتراض المراسلات وتسجيل الأصوات والتقاط الصور، وكذلك أسلوب التسرب أو كما سماه قانون الوقاية من الفساد ومكافحته أسلوب الاختراق. وعليه سنوجزها كالتالي:

-مراقبة الاتصالات الإلكترونية وتجميعها:

بين القانون 04/09 الخاص بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها إجراءات مراقبة الاتصالات الإلكترونية، وتفتيش وحجز المنظومة المعلوماتية.

القاعدة أنه أضفى المشرع الجزائري الحماية القانونية للبيانات ذات الطابع الشخصي من خلال الدستور، وهذا في إطار القواعد العامة التي تعنى بالحماية القانونية للحياة الخاصة للأفراد ، وهو ما ينطوي عليه بالضرورة حماية بياناتهم الشخصية من المعالجة الآلية، بحيث اعترف المشرع الدستوري الجزائري بها في المادة 77 التي تنص على أنه: "يمارس كل واحد جميع حرياته، في إطار احترام الحقوق المعترف بها للغير في الدستور، لاسيما احترام الحق في الشرف، وستر الحياة الخاصة".

كما أيدت ذلك المادة 46 من دستور سنة 1996 التي نصت على أنه: "لا يجوز انتهاك حرمة حياة المواطن الخاصة، وحرمة شرفه، ويحميها القانون. سرية المراسلات والاتصالات الخاصة بكل أشكالها مضمونة"، إلا أنه في تعديل الدستوري لسنة 2016، حاول المشرع مواكبة التطور الذي يشهده العالم في مجال حماية البيانات

[1]- نورة، طرشي، المرجع السابق، ص155.

الشخصية، من خلال إضافة فقرتين للمادة أعلاه تنصان على أنه:" لا يجوز بأي شكل المساس بهذه الحقوق دون أمر معلل من السلطة القضائية، ويعاقب القانون انتهاك هذا الحكم".

وبهذا يكون المشرع الجزائري رغم ضمانه لسرية المراسلات والاتصالات بكل أشكالها، قد خول استثناء السلطة القضائية وفي إطار قرار معلل بأن تتبع إجراءات تمس البيانات الشخصية، بالنظر لخطورة بعض الجرائم المعلوماتية المحددة حصرا: تسجيل الاتصالات الإلكترونية في حينها.

كما بين القانون 04/09 الخاص بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها في مادته الرابعة، الحالات التي تسمح بتطبيق الإجراء الجديد المتمثل في مراقبة الاتصالات الإلكترونية، وذلك على سبيل الحصر، وهذه الحالات هي:

-للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة.

-في حالة توفر معلومات عن احتمال الاعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني.

-لمقتضيات التحريات والتحقيقات القضائية، عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء للمراقبة الإلكترونية.

يظهر من خلال استقراء نص هذه المادة، أن المشرع الجزائري يحاول الاستفادة بدوره من التطور التكنولوجي والمميزات التي يخولها، من خلال وضع المشتبهين فيهم تحت المراقبة الإلكترونية، وهي على عكس المراقبة الشخصية أقل تكلفة من حيث الوقت والمال والمخاطر الأمنية إضافة إلى فعاليتها، إلا أنه من جهة أخرى، فإن وضع الشخص تحت المراقبة الإلكترونية سواء ما تعلق باتصالاته الهاتفية أو نشاطاته عبر الانترنيت، من شأنه انتهاك حرمة البيانات ذات الطابع الشخصي له، باعتبار أنه لدواعي فرز المعلومة للتأكد من قيمتها كدليل إثبات أو نفي، يستدعي سماعها أو قراءتها بكل تأني، وهذا ما من شأنه الوصول إما لأنها معلومة ضرورية لاستكمال التحقيقات، أو أنها معلومات شخصية لا دخل لها بالقضية، كما يمكن أن يصار إلى تبرئة الشخص تماما.

وبغرض التخفيف من التأثيرات السلبية لهذه العملية على حماية الحياة الخاصة للأفراد وضع المشرع عدة ضمانات هي:

***حصر الحالات التي يمكن اللجوء فيها إلى المراقبة الإلكترونية:**

هي الحالات التي أوضحتها المادة الرابعة من القانون 04/09 على سبيل الحصر:

- للوقاية من الأفعال الموصوفة بالجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة- .

- في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني.

- لمقتضيات التحريات والتحقيقات القضائية، عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الإلكترونية.

- في إطار تنفيذ المساعدة القضائية الدولية المتبادلة.

يتضح من خلال نص المادة الرابعة أن المشرع الجزائري، حاول التضييق من الحالات التي يمكن فيها اللجوء إلى عملية المراقبة الإلكترونية وحصرها في الجرائم التي تمس الأمن الوطني، ذلك أنه عندما يتعلق الأمر مثلا بالجرائم الإرهابية والتي تطال المدنيين فإنه لا يمكن الحديث عن حقوق الإنسان، وكذا في حالات تنفيذ المساعدة القضائية، إلا أن إضافة الحالة الثالثة والتي تعني إمكانية اللجوء في كل قضية مستعصية إلى المراقبة الإلكترونية صغيرة كانت أو كبيرة، يؤدي إلى تعميم استخدام الآلية دون حد.

*** وضع آلية إقرار المراقبة الإلكترونية تحت سلطة القضاء:**

تنص المادة 2/4 من القانون 04/09، بأنه: "لا يجوز إجراء عمليات المراقبة، إلا بإذن مكتوب من السلطات القضائية المختصة".

كما أنه عندما يتعلق الأمر بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة، يختص النائب العام لدى مجلس قضاء الجزائر بمنح ضباط الشرطة القضائية، إذنا لمدة 6 أشهر قابلة للتجديد وذلك على أساس تقرير يبين طبيعة الترتيبات التقنية المستعملة والأغراض الموجهة لها.

*** تحديد تقنيات الرقابة الإلكترونية وحدود استعمال المعطيات المتحصل عليها:**

تكون الترتيبات التقنية الموضوعة للأغراض المراقبة الإلكترونية موجهة حصريا لتجميع وتسجيل معطيات ذات صلة بالحالات الواردة على سبيل الحصر أعلاه على غرار الأفعال الإرهابية أي الجرائم الأكثر خطورة.

أما عن التقنيات التكنولوجية التي يمكن أن تستعمل في إطار المراقبة الإلكترونية فهي تتمثل في:

-اعتراض المراسلات الالكترونية.

-تسجيل الأصوات.

-التقاط الصور.

-تفتيش المنظومات المعلوماتية وحجزها[1].

[1]- القانون رقم 15-04 مؤرخ في أول فبراير سنة 2015يحدد القواعد العامة المتعلقة بالتوقيع و التصديق، الجريدة الرسمية للجمهورية الجزائرية، العدد6.

وقد نصت المادة المادة 09 من القانون 04/09 المتعلقة بحدود استعمال المعطيات المتحصل عليها عن طريق الحجز بأنه لا يجوز استعمال المعلومات المتحصل عليها عن طريق عمليات المراقبة إلا في الحدود الضرورية للتحريات أو التحقيقات القضائية، ما تشير إليه هذه المادة هو أن الاستعمال المشروع للبيانات الشخصية المتحصل عليها من المراقبة الإلكترونية يتحدد بحدود ضرورات التحقيقات، وهو ما يستدعي تجريم كل استعمال لها خارج هذا الإطار.

*** سن عقوبات لجريمة إفشاء معلومات ذات طابع شخصي ناتجة عن المراقبة الإلكترونية:**

يكون الموظفين القائمين على عمليات المراقبة الإلكترونية قادرين على الاطلاع على معلومات ذات طابع مجرم وأخرى ذات طابع شخصي، وفي كلتا الحالتين يكون هؤلاء مطالبين باحترام السر المهني.

لهذا جرم المشرع كل محاولة من قبل هؤلاء الموظفين نحو استغلال عمليات المراقبة لأغراض شخصية، أو كل تجاوز لحدود المراقبة الإلكترونية نحو انتهاك حرمة الحياة الشخصية للأفراد أيا كان السبب، أو إفشاء مستندات ناتجة عن التفتيش أو إطلاع عليها شخص لا صفة له قانونا في الاطلاع عليه، وذلك بغير إذن مكتوب من المتهم أو من ذوي حقوقه أو من الموقع على هذا المستند أو من المرسل إليه ما لم تدع ضرورات التحقيق إلى غير ذلك.

- إجراءات تفتيش المنظومة المعلوماتية:

يعتبر التفتيش عن بعد في البيئة الافتراضية، مسرح جرائم تكنولوجيات الإعلام و الاتصال، من بين الإجراءات التي تبناها المشرع الجزائري في القانون 09-04، ولما كان هذا الإجراء يمس بالحياة الخاصة وضعت له عدة شروط لمباشرته.

*** تفتيش نظم المعلوماتية:**

عملية تفتيش تنصب على المكونات المادية بأوعيتها المختلفة، للبحث في أي شيء يتصل بجريمة معلوماتية ما للكشف عنها، يدخل في نطاق التفتيش التقليدي وفقا للإجراءات القانونية المعمول بها، إلا أن هناك حالات خاصة للتفتيش في هذه المكونات، هي:

الحالة الأولى: في حالة ما إذا كانت هذه المكونات موجودة في مكان خاص كمسكن المتهم أو أحد ملحقاته، فإنها تأخذ نفس الأحكام المقررة لتفتيش المسكن وبنفس الضمانات المقررة قانونا في مختلف التشريعات.

الحالة الثانية : إذا كانت مكونات الحاسوب المادية منعزلة عن غيرها من أجهزة الكمبيوتر أم أنها متصلة بجهاز أو نهاية طرفية في مكان آخر كمسكن غير مسكن المتهم، بحيث إذا كانت هناك بيانات مخزنة في أوعية هذا النظام الآخر، فإن عملية الكشف تصبح صعبة جدا، وربما مستحيلة، لذلك حتى تتم عملية تفتيش هذه الأجهزة المرتبطة بأجهزة في أماكن أخرى، يتعين مراعاة القيود والضمانات التي يوجبها المشرع لتفتيش هذه الأماكن، ففي

ألمانيا يرى الفقه[1] ، أنه يمكن أن يمتد التفتيش إلى سجلات البيانات التي تكون في موقع آخر تطبيقا لمقتضيات القسم 103 من قانون الإجراءات الجزائية الألماني، وذلك عندما يكون مكان تخزين البيانات الفعلي خارج المكان الذي يتم فيه التفتيش.

إذن لتفتيش الحاسوبات الآلية ذات نهاية طرفية في دولة أجنبية، نصت بعض التشريعات على طريقة ثانية كإجراء للتحقيق في الجريمة المعلوماتية وهذه الطريقة هي: التصنت والمراقبة الالكترونية لشبكات الحاسوب ويقصد بهذه الطريقة -التصنت- مراقبة المحادثات التلفونية وتسجيلها بالنسبة للأحاديث الخاصة بشخص أو أكثر مشتبه فيه، ويعتقد بفائدة محادثته في الكشف عن الجريمة، وذلك عن طريق إخضاعها لنوع من الرقابة بقصد التعرف على مضمونها.

وقد حذا المشرع الجزائري حذو معظم التشريعات المعاصرة، بأن قرر المادة 65 مكرر 5 وما يليها من قانون الإجراءات الجزائية التي تسمح إذا اقتضت ضرورات التحري أو التحقيق في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات باعتراض المراسلات وتسجيل الأصوات والتقاط الصور.

الحالة الثالثة :إذا وجدت مكونات الحاسوب المادية (في حالة الحاسوبات الآلية المحمولة) في الأماكن العامة بطبيعتها كالمطاعم والسيارات العامة كسيارات الأجرة ...الخ، فإن تفتيشها لا يكون إلا في الحالات التي يجوز فيها تفتيش الأشخاص، وبنفس الضمانات والقيود المنصوص عليها في هذه الحالات، وقد اتفقت بعض التشريعات، كالتشريع الجنائي الكندي في المادة 487 التي أجازت إصدار أمر قضائي لتفتيش وضبط أي شيء يؤدي للاعتقاد بأن الجريمة قد وقعت أو يشتبه في وقوعها، ونصت صراحة على إمكانية تفتيش مكونات الحاسوبات المادية للكشف عن الجريمة المعلوماتية باتخاذ أي إجراء أو القيام بأي فعل لازم لجمع الأدلة والحفاظ عليها

*تفتيش نظم الحاسوب المنطقية أو المعنوية:

يعرف الكيان المنطقي للحاسوب بأنه: "مجموعة البرامج والأساليب والقواعد وعند الاقتضاء الوثائق المتعلقة بتشغيل وحدة معالجة البيانات".

وهو يشتمل على جميع العناصر غير المادية اللازمة لتشغيل الكيان المادي كالبرامج ونظم التشغيل وقواعد البيانات ... الخ، لقد ثار الخلاف في التشريع المقارن في مسألة ضبط وتفتيش المكونات المعنوية أو المنطقية للحاسوب، فتعددت الآراء في هذا الشأن؛ فذهب رأي إلى أنه إذا كانت الغاية من التفتيش هي ضبط الأدلة المادية التي تفيد في الكشف عن الحقيقة، فإن هذا المفهوم يجب أن يمتد ليشمل البيانات الالكترونية، كالقانون الإجرائي اليوناني في نص المادة 251 التي تعطي لسلطات التحقيق إمكانية القيام بأي شيء يكون ضروريا لجمع وحماية الدليل، تفسيرا لعبارة أي شيء بأنها تشمل ضبط البيانات المخزنة أو المعالجة آليا أو الكترونيا، بما فيها

[1]- نورة طرشي، المرجع السابق، ص160.

ضبط البيانات المخزنة في حاملات البيانات المادية، أو في الذاكرة الداخلية وذلك بإعطاء المحقق أمرا للخبير بجمع البيانات التي يمكن أن تكون مقبولة كدليل للمحاكمة الجنائية، على أساس إنها كيانات يمكن قياسها بما أنها نبضات أو ذبذبات الكترونية قابلة لان تسجل وتخزن على وسائط معينة يمكن قياسها[1].

وقد حذا المشرع الجزائري في المادة 47 الفقرة الرابعة من قانون الإجراءات الجزائية الجزائري حذو التشريعات السابقة بإمكانية التفتيش والضبط على المكونات المعنوية للحاسوب، بنصه على أنه: "إذا تعلق الأمر بجريمة ماسة بأنظمة المعالجة الآلية للمعطيات يمكن لقاضي التحقيق أن يقوم بأية عملية تفتيش أو حجز ليلا أو نهارا وفي أي مكان على امتداد التراب الوطني أو يأمر ضباط الشرطة القضائية للقيام بذلك".

* القواعد الشكلية لتفتيش نظم المعلوماتية:

تتمثل هذه القواعد فيما يلي:

- **إجراء التفتيش بحضور أشخاص معينين بالقانون** :من بين هذه الأشخاص: المتهم والقائم بالتفتيش وشاهدين طبقا للمادة 45 من قانون الإجراءات الجزائية الجزائري، تنص على أن: " التفتيش يتم بحضور المتهم أو من يجوز أن يمثله وضابط الشرطة القضائية-القائم بالتفتيش-، وإذا تعذر حضور المتهم أو من يجوز أن يمثله يتم التفتيش بحضور شاهدين من غير الموظفين الخاضعين لسلطته"، غير أنه كاستثناء على هذه القواعد نص المشرع الجزائري في الفقرة الأخيرة من المادة 45 من قانون الإجراءات الجزائية الجزائري، على أنه: "لا تطبق هذه الأحكام إذا تعلق الأمر بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات".

-**إعداد محضر خاص بالتفتيش** :ويكون بتكليف القائم بالتفتيش باصطحاب كاتب يحرر محضرا خاصا بالتفتيش والضبط، تسجل فيه جميع وقائع التحقيق بالتفصيل، وذكر البيانات والأشياء والوثائق التي يتم ضبطها بكل أمانة ودقة وحرص.

-**إجراءات تنفيذ تفتيش نظم الحاسوب الآلي وميعاده** :لهذه الإجراءات خصوصية تتميز بها، وذلك لدقة التعامل مع الأجهزة والبرامج الموجودة عليها، ولكي تتم على أكمل وجه، يجب تحديد نوع النظام المراد تفتيشه، وبالتالي يجب أن يكون القائم بالتفتيش على علم بقدر كبير بعلوم الإعلام الآلي حتى يتسنى له معرفة نظم الحاسوب المراد تفتيشها، والاستعانة بخبراء النظام للاستعانة بهم في عملية إجراء التفتيش، ومعرفة إمكانية الحصول على كلمة السر والدخول للنظام المراد تفتيشه، ومعرفة مكان القيام بتحليل نظم الحاسوب الآلي.

وفي نطاق تفتيش نظم الحاسوب، نجد أن أغلب التشريعات الإجرائية لم تحدد مدة معينة لتنفيذ إجراء التفتيش ما عدا البعض منها كالتشريع الانجليزي الذي حدد مهلة الشهر الواحد من تاريخ إصدار الإذن كما أنها تختلف في الزمن الذي يجري فيه التفتيش أو تحديد المدة التي يجري فيها، غير أن الرأي الغالب في مجال تفتيش النظم المعلوماتية هو عدم تقييد المحقق بمدة زمنية معينة، بل يجب تركها للسلطة التقديرية له، لأن الوقت الذي تكثر

[1]- امينة أحمدي بوزينة، إجراءات التحري الخاصة في مجال مكافحة الجرائم المعلوماتية، مركز جيل البحث العلمي،2017، ص135

فيه الجرائم المعلوماتية هو ليلا، لسهولة الاتصال ومجانيته في ذلك الوقت في بعض الحالات، وأيضا لسهولة الدخول إلى المواقع المستهدفة بالفعل الإجرامي لقلة المستخدمين في هذا الوقت، مثلما فعل المشرع الجزائري في الفقرة الثالثة من المادة 47 من قانون الإجراءات الجزائية[1].

-- توسيع الإجراءات الخاصة بالاختصاص في الجرائم المعلوماتية:

من بين الإجراءات الخاصة المتخذة في مجال الاختصاص نذكر ما يلي:

- جواز تمديد الاختصاص المحلي والنوعي الدولي للمحاكم الجزائرية :حيث نصت المادة 329 من قانون الإجراءات الجزائية في فقرتها الأخيرة على جواز تمديد الاختصاص المحلي للمحكمة ليشمل اختصاص محاكم أخرى عن طريق التنظيم في جرائم المخدرات والجريمة المنظمة والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.

كما أنشئت الأقطاب القضائية الجزائية المتخصصة بموجب القانون 14/04 المؤرخ في 10 نوفمبر 2004 المعدل لقانون الإجراءات الجزائية من بين الجرائم التي تختص بها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات. وقد، نظم المشرع الجزائري في القانون رقم 04/09 المؤرخ في 5 أوت 2009، أحكاما جديدة خاصة بالاختصاص في مجال بالجريمة المعلوماتية تتماشى والتطور الذي لحق الجريمة، من هذه القواعد ما نصت عليه المادة الثالثة التي تضمنت الإجراءات الجديدة التي تتطلبها التحريات والتحقيقات من ترتيبات تقنية، بالإضافة إلى ذلك، قررت المادة 15 من القانون 04/09 أنه زيادة على قواعد الاختصاص المنصوص عليها في قانون الإجراءات الجزائية، تختص المحاكم الجزائرية بالنظر في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال المرتكبة خارج الإقليم الوطني عندما يكون مرتكبها أجنبيا، وتستهدف مؤسسات الدولة الجزائرية والدفاع الوطني أو المصالح الإستراتيجية للاقتصاد الوطني.

- توسيع مجال اختصاص النيابة العامة: بموجب المادة 37 من قانون الإجراءات الجزائية، تم توسيع مجال اختصاص النيابة العامة ليشمل نطاقات أخرى لم يكن مرخصا لها بها من قبل، حيث نصت هذه المادة على تمديد الاختصاص المحلي لوكيل الجمهورية إلى دائرة اختصاص محاكم أخرى عن طريق التنظيم في جرائم المخدرات والجريمة المنظمة والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، وجرائم تبييض الأموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف.

كذلك سحب نظام الملائمة من النيابة العامة في مجال متابعة بعض الجرائم، إذ يلتزم وكيل الجمهورية بتحريك الدعوى العمومية بقوة القانون، بحيث لا يتمتع بشأنها بسلطة الملائمة بين تحريك الدعوى العمومية وعدم تحريكها مثلما فعل في الجرائم المنصوص عليها في المواد 144 مكرر و144 مكرر1 و144 مكرر2 من قانون العقوبات المعدل والمتمم بالقانون رقم 09/01 المؤرخ في 26 يونيو2001 [2].

[1]- امينة أمحمدي بوزينة، المرجع السابق، ص137.

[2]- نورة طرشي، المرجع السابق، ص162.

خاتمة:

يتضح من خلال ما سبق أن جرائم تكنولوجيا الإعلام والاتصال فرضت جملة من التحديات القانونية، من اجل مكافحتها و الوقاية منها، تجسدت في المقام الأول في بعض المسائل القانونية التي تتعلق بإثبات هذه الجرائم وقبول الدليل بشأنها باعتبارها لا تترك أثرا ماديا ملموسا، كما هو الحال في الجرائم التقليدية، مما استوجب ضرورة تدخل المشرع الجزائري من اجل استحداث هيئات متخصصة للوقاية من هذه الجرائم، وضرورة إتباع إجراءات خاصة لمكافحتها. وهو ما تضمنه بالفعل القانون 09-04 والذي استحدث جملة من التدابير والإجراءات تتماشى مع خطورة هذه الجرائم. ومن أهم النتائج المتوصل إليها من خلال هده الدراسة نذكر ما يلي:

-إن استغلال تكنولوجيات الإعلام والاتصال وخاصة الانترنت أدت إلى حذف الحدود الإقليمية وتدخل المشرع عن طريق تمديد الاختصاص، ومتابعة أي شخص حتى لو كان أجنبي ارتكب سلوك إجرامي أحدث نتيجة على التراب الجزائري.

-تبني المشرع الجزائري في القانون 09-04 لطرق تحري خاصة في الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، كالمراقبة الالكترونية للاتصالات وتفتيش نظم المعلوماتية، والتي أعطى لها المشرع الشرعية القانونية بالرغم من مساسها بالحياة الخاصة للأفراد.

-تنصيب هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، والموضوعة تحت سلطة وزارة الدفاع الوطني وذلك بموجب المرسوم الرئاسي 19-172 الصدر في 06 يونيو 2019.

- تم التوسع في الاختصاص الإقليمي للسلطة القضائية في متابعة الجرائم التي تمس مؤسسات الدولة أو الدفاع الوطني أو المصالح الإستراتيجية للاقتصاد الوطني.

وعليه تم الخروج بالتوصيات الآتية:

- توفير الإمكانيات التقنية الحديثة لضمان الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال.
- وضع برامج تأهيل لعناصر الضبطية القضائية ورجال الأمن المكلفين بعمليات البحث والتحري عن الجرائم المتصلة بتكنولوجيا الإعلام والاتصال.
- تعزيز التعاون الدولي من اجل الحد من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال وذلك باعتبارها جرائم عابرة للحدود.

قائمة المراجع:

1- احمد حسام طه، الجرائم الناشئة عن استخدام الحاسب الآلي، دار النهضة العربية، 2002.

2- أمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، دار هومة، الجزائر، 2007.

3- امينة أمحمدي بوزينة، إجراءات التحري الخاصة في مجال مكافحة الجرائم المعلوماتية، مركز جيل البحث العلمي،2017.

4- زليخة زيدان، الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى،2011.

5- سعيد نعيم، آليات البحث والتحري المعلوماتية في القانون الجزائري، مذكرة ماجستير، جامعة الحاج لخضر-باتنة،2012-2013.

6- عبد الله بن مسعود محمد السرياني، فاعلية الأساليب المستخدمة في إثبات جريمة التزوير الالكتروني، مطبع جامعة نايف العربية للعلوم الأمنية، الرياض،2011.

7- علي عبد القادر قهوجي ، الحماية الجزائية لبرامج الحساب الآلي، دار الجامعة الجديدة، الإسكندرية، 2010، ص136.

8- محمد رحموني، خصائص الجريمة الالكترونية ومجالات استخدامها، مجلة الحقيقة، العدد 41، 2018.

9- نائلة عادل، محمد فريدة قوره، جرائم الحاسب الآلي الاقتصادية، منشورات الحلبي الحقوقية، 2005.

10- نورة طرشي، مكافحة الجريمة المعلوماتية، مذكرة ماجستير، جامعة الجزائر، 2011-2012.

11- الهام بن خليفة، الإشكالات التي تثيرها الفقرة"أ" في المادة الثانية من قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، مجلة العلوم القانونية والسياسية- العدد 10، جنفي 2015.

12- هشام محمد فريد، الجوانب الإجرائية للجرائم المعلوماتية، مكتبة الآلات الحديثة، مصر،1994.

13- القانون رقم 09-04 المؤرخ في 05 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها،الجريدة الرسمية للجمهورية الجزائرية، العدد47.

14- القانون رقم 15-04 مؤرخ في أول فبراير سنة 2015يحدد القواعد العامة المتعلقة بالتوقيع و التصديق، الجريدة الرسمية للجمهورية الجزائرية، العدد6 .

15- المرسوم الرئاسي رقم 19-172، المؤرخ في 26جوان 2019، يحدد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها وتنظيمها وكيفية سيرها.