# مكافحة الجرائم الإلكترونية في القانون الجزائري

**شيخ سناء(*)**

**و شيخ محمد زكرياء(**)**

**chikhsanaa@yahoo.fr**

**المقدمة:**

إنّ انتشار التكنولوجيا الحديثة واستعمالاتها التي مسّت كل نواحي الحياة أفرز العديد من التحولات والتغيّرات بشقيها الإيجابي والسلبي. فممّا لاشكّ فيه أنّ الثورة المعلوماتية ونتيجة للتقنيات العالية التي تقوم عليها والتي تتمثل في استخدام الحواسيب وشبكة الإنترنت قد تركت آثارا إيجابية وشكلت قفزة حضارية نوعية في حياة الأفراد والدول، نظرا لما تتميّز به هذه الأنظمة المعلوماتية من سرعة ودقّة في تخزين المعلومات وتجميعها، ومن ثمّ تبادلها بين الأفراد والدول، إلاّ أنّه في المقابل فإنّ هذه التكنولوجيا أفرزت العديد من السلبيات أهمّها صعوبة تحقيق أمن المعلومات وذلك بسبب سهولة الوصول إليها والاعتداء عليها وانتهاك حريتها.

إنّ التقدم التكنولوجي وانتشار وسائل الاتصال الحديثة أدّى إلى ظهور أشكال جديدة للإجرام اصطلح على تسميتها بالجريمة الإلكترونية، ممّا دفع بالمشرع الجزائري إلى التدخل للتصدي لهذه الجريمة وتوفير حماية جزائية للأنظمة المعلوماتية، وذلك من خلال إدخال تعديلات على قانون العقوبات لجعله يتجاوب مع التطورات الإجرامية في مجال تكنولوجيا الإعلام والاتصال، واستحداث قوانين جديدة لضمان الحماية الجزائية للمعاملات الإلكترونية.

إذن، كان من الضروري أن يواكب التشريع الجزائري هذا التطور الملحوظ في الجرائم الإلكترونية، فالمواجهة التشريعية ضرورية للتعامل من خلال خلق قواعد قانونية غير تقليدية لمواجهة هذا النوع من الجرائم المستحدثة، فماذا يقصد بالجريمة الإلكترونية؟ وما هي الآليات التي وضعها المشرع الجزائري لمكافحتها؟ ولأيّ مدى وفق المشرع في مكافحة الجريمة الإلكترونية بكافة أشكالها، ومن ثمّ تحقيق حماية جزائية فعّالة للأنظمة المعلوماتية؟

هذا، ما سنحاول الإجابة عليه من خلال تعريف الجريمة الإلكترونية وتبيان خصائصها في مبحث أول، وتحديد الآليات التي وضعها المشرع الجزائري لمكافحة هذه الجريمة في مبحث ثان، ثمّ توضيح الآليات التي استحدثها المشرع في القوانين الخاصة في مبحث ثالث.

## المبحث الأول: تعريف الجريمة الإلكترونية وخصائصها

الجريمة الإلكترونية جريمة حديثة وذلك لارتباطها بتكنولوجيا متطورة هي تكنولوجيا المعلومات، ونتيجة لحداثتها، فقد كانت هناك اتجاهات مختلفة في تعريفها، كما أنّها تتميز بخصائص متفردة لا تتوفر في أي من الجرائم التقليدية، لذا كان لزاما علينا من أجل تحديد الجريمة الإلكترونية التطرق لتعريفها في مطلب أول، ثمّ تبيان خصائصها في مطلب ثان.

### المطلب الأول: تعريف الجريمة الإلكترونية

تعتبر الجريمة الإلكترونية من الظواهر الحديثة وذلك لارتباطها بتقنية حديثة هي تكنولوجيا المعلومات والاتصالات والكمبيوتر، ونظرا للتطور المستمر لتكنولوجيا المعلومات حتى الآن، يصعب وضع تعريف فقهي جامع وشامل للجريمة الإلكترونية، لذا انقسم الفقه إلى اتجاهين: الأول يضيّق من مفهوم الجريمة الإلكترونية والآخر يوسّع من مفهومها.

---

(*) أستاذة محاضرة قسم "أ" كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد، تلمسان.

(**) أستاذ محاضر قسم "أ" كلية الحقوق والعلوم السياسية، جامعة عبد الحميد بن باديس، مستغانم.

ومن التعريفات التي وضعها أنصار **الاتجاه المضيّق** أنّ الجريمة الإلكترونية هي: "كل فعل غير مشروع يكون العلم بتكنولوجيات الحاسبات الآلية بقدر كبير لازما لارتكابه من ناحية، وملاحقته والتحقيق فيه من ناحية أخرى"[١].

إنّ هذا التعريف يضيّق بدرجة كبيرة الجريمة الإلكترونية فهو يشترط توافر معرفة كبيرة بتقنيات الحاسوب ليس فقط لارتكاب الجريمة بل كذلك لملاحقتها والتحقيق فيها.

كما عرّف بعض الفقه الجريمة الإلكترونية بأنّها: "تشمل أي جريمة ضدّ المال مرتبطة بالمعالجة الآلية للمعلومات"[٢]، وبأنّها :" فعل غير مشروع موجه لنسخ أو الوصول إلى المعلومات المخزنة داخل الحاسوب أو تغييرها وحذفها أو الوصول إلى المعلومات المخزنة داخل الكمبيوتر أو تلك التي يتمّ تحويلها عن طريقه"[٣].

نلاحظ من هذه التعريفات أنّها تضيّق من مفهوم الجريمة الإلكترونية، فهي تُخرج من نطاقها العديد من الأفعال غير المشروعة التي يستخدم الحاسوب لارتكابها.

في المقابل عرّف أصحاب **الاتجاه الموسّع** الجريمة الإلكترونية بأنّها: "كل فعل أو امتناع عمدي، ينشأ عن الاستخدام غير المشروع لتقنية المعلوماتية يهدف إلى الاعتداء على الأموال المادية أو المعنوية"[٤].

ولقد ذهبت مجموعة من خبراء منظمة التعاون الاقتصادي والتنمية في عام 1983 إلى تعريف الجريمة الإلكترونية بأنّها: "كل سلوك غير مشروع أو غير أخلاقي أو غير مصرّح به يتعلّق بالمعالجة الآلية للبيانات أو بنقلها"[٥].

كما عرّفها البعض بأنّها: "كلّ سلوك إجرامي يتمّ بمساعدة الكمبيوتر"، أو هي " كل جريمة تتمّ في محيط أجهزة الكمبيوتر"، أو هي "كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلّق بالمعالجة الآلية للبيانات أو بنقلها"[٦].

أمّا مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين المنعقد في فيينا سنة 2000 فقد عرّف الجريمة الإلكترونية بأنّها: "أيّة جريمة يمكن ارتكابها بواسطة نظام حاسوب أو شبكة حاسوبية، والجريمة تلك تشمل من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في بيئة إلكترونية"[٧].

يستفاد من هذه التعريفات الموسعة أنّها حاولت الإحاطة قدر الإمكان بجميع الأشكال الإجرامية للجريمة الإلكترونية، فكل نشاط إجرامي سواء كان فعلا إيجابيا أو سلوكا سلبيا متمثلا في الامتناع، يؤدي فيه نظام الكمبيوتر دورا في ارتكاب الجريمة، أو يقع في بيئة إلكترونية يعتبر جريمة إلكترونية. فلقد أراد هذا الاتجاه الموسع عدم حصر الجريمة الإلكترونية في نطاق ضيّق حتّى لا يفلت العديد من مرتكبي صور هذه الجريمة من العقاب.

**المطلب الثاني: خصائص الجريمة الإلكترونية**

تتميز الجرائم الإلكترونية بخصائص تميّزها عن الجرائم التقليدية، ومن أهمّها ما يلي:

---

[١] – قورة نائلة، جرائم الحاسب الاقتصادية، الطبعة الأولى، دار النهضة العربية، القاهرة، 2004، ص ٢١.

[٢] – هذا تعريف للفقيه الألماني تيدمان Tiedmemann، مشار إليه في: أحمد خليفة الملط، الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية، ص ٩٤.

[٣] – مشار إليه في: نهلا عبد القادر المومني، الجرائم المعلوماتية، الطبعة الأولى، دار الثقافة للنشر والتوزيع، الأردن، 2008، ص ٤٨.

[٤] – سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، الطبعة الأولى، دار النهضة العربية، القاهرة، 1994، ص ٠٧.

[٥] – مشار إليه في نهلا عبد القادر المومني، المرجع السابق، ص ٤٩.

[٦] – خالد محمود إبراهيم، الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية، 2009، ص ٧٤.

[٧] – لقد عقد هذا المؤتمر في فيينا ما بين ١٠ و١٧ نيسان لعام ٢٠٠٠، محمود إبراهيم الغازي، الحماية الجنائية للخصوصية والتجارة الإلكترونية، مكتبة الوفاء القانونية، الإسكندرية، الطبعة الأولى، 2014، ص ١١٨.

**الفرع الأول: وقوع الجريمة الإلكترونية في بيئة المعالجة الآلية للبيانات**

تقع الجريمة الإلكترونية أثناء المعالجة الآلية للبيانات والمعطيات الخاصة بالكمبيوتر، ويمثّل هذا النظام الشرط الأساسي الذي يتعيّن توافره حتى يمكن البحث عن قيام أو عدم قيام أركان الجريمة الإلكترونية الخاصة بالتعدي على نظام معالجة البيانات، ذلك أنّه في حالة تخلّف هذا الشرط تنتفي الجريمة الإلكترونية[٨].

حيث يستلزم لقيام هذه الجريمة التعامل مع بيانات مجمّعة ومجهّزة للدخول للنظام المعلوماتي بغرض معالجتها إلكترونيا، بما يُمكّن المستخدم من إمكانية كتابتها من خلال العمليات المتبعة، والتي يتوافر فيها إمكانية تصحيحها أو تعديلها أو محوها أو تخزينها أو استرجاعها وطباعتها، وهذه العمليات وثيقة الصلة بارتكاب الجرائم، ولابدّ من فهم الجاني لها أثناء ارتكابها في حالات التزوير والتقليد[٩].

**الفرع الثاني: الجريمة الإلكترونية جريمة عابرة للحدود**

تتّسم الجريمة الإلكترونية بأنّها غالبا ذات بعد دولي، ذلك لأنّ الطابع العالمي لشبكة الإنترنت وما يرتبه من جعل معظم دول العالم في حالة اتصال دائم، يُسهّل ارتكاب الجريمة من دولة إلى دولة أخرى، فالجريمة الإلكترونية لا تعترف بالحدود بين الدول والقارات، ولذلك فهي جريمة عابرة للقارات، إذ يمكن من خلال النظام المعلوماتي ارتكاب العديد من الجرائم مثل جريمة التعدي على قواعد البيانات، وتزوير وإتلاف المستندات الإلكترونية، والاحتيال المعلوماتي والقرصنة[١٠].

هذه الطبيعة التي تتميّز بها الجريمة المعلوماتية كونها جريمة عابرة للحدود خلقت العديد من المشاكل حول تحديد الدولة صاحبة الاختصاص القضائي بهذه الجريمة، وتحديد القانون الواجب تطبيقه بالإضافة إلى إشكاليات تتعلّق بإجراءات الملاحقة القضائية.

**الفرع الثالث: صعوبة إثبات الجريمة الإلكترونية**

تتميّز الجريمة الإلكترونية بصعوبة اكتشافها، وحتى في حال اكتشاف وقوعها والإبلاغ عنها فإنّ إثباتها أمر صعب، فهي تتمّ في بيئة غير تقليدية حيث تقع خارج إطار الواقع المادي الملموس لتقوم أركانها في بيئة الحاسوب والإنترنت، ممّا يجعل الأمور تزداد تعقيدا لدى سلطات الأمن وأجهزة التحقيق والملاحقة، ففي هذه البيئة تكون البيانات والمعلومات عبارة عن نبضات إلكترونية غير مرئية تنساب عبر النظام المعلوماتي ممّا يجعل أمر طمس الدليل ومحوه كليا من قبل الفاعل أمرا في غاية السهولة[١١].

هذا، وترجع صعوبة إثبات الجريمة الإلكترونية إلى عدّة أمور منها:

– عدم ترك هذه الجريمة آثار مادية بعد ارتكابها، فلا يوجد جثث لقتلى أو آثار لدماء، وإذا اكتشفت الجريمة فلا يمكن ذلك إلاّ بمحض الصدفة[١٢].

– سرعة محو الدليل وصعوبة الوصول إليه، إذ يسهل محو الدليل من شاشة الكمبيوتر في زمن قياسي باستعمال البرامج المخصصة لذلك، إذ يتمّ عادة في لمح البصر وبمجرد لمسة خاطفة على لوحة المفاتيح بجهاز الحاسوب.

---

[٨] – خالد محمد كدفور المهيري، جرائم الكمبيوتر والإنترنت والتجارة الإلكترونية، دار الغرير للطباعة والنشر، دبي، 2005، ص ١٣٥.

[٩] – أحمد خليفة الملط، المرجع السابق، ص ١٠٥.

[١٠] – خالد ممدوح إبراهيم، المرجع السابق، ص ٧٧.

[١١] – نهلا عبد القادر المومني، المرجع السابق، ص ٥٦.

[١٢] – أحمد خليفة الملط، المرجع السابق، ص ١٠٥.

– نقص الخبرة التقنية والفنية لدى الشرطة وجهات الادعاء والقضاء، حيث تتطلب جرائم الكمبيوتر والإنترنت إلماما خاصا بتقنيات الكمبيوتر ونظم المعلومات، وهذا من أجل التحقيق فيها وملاحقة مرتكبيها قضائيا[١٣].

**الفرع الرابع: خصوصية ارتكاب الجريمة الإلكترونية**

تتميّز الجريمة الإلكترونية عن الجريمة التقليدية سواء من حيث أسلوب ارتكابها، أو من حيث مرتكبيها، فهي جريمة لا تتطلب ممارسة العنف أو الإيذاء، كما هو الحال في جريمة القتل أو الاختطاف، أو الخلع والكسر كما هو الحال في جريمة السرقة، فالجرائم الإلكترونية جرائم هادئة بطبيعتها لا تحتاج إلاّ للمسات أزرار من طرف مجرم معلوماتي يتميّز عن المجرم التقليدي بأنّه في الغالب شخص يتميّز بالذكاء وله مهارات تقنية عالية، ومعرفة بتقنيات الحاسوب والإنترنت، وفي مجال معالجة المعلومات آليا.

**الفرع الخامس: قلّة الإبلاغ عن وقوع الجريمة الإلكترونية**

لا يتمّ – غالبا – الإبلاغ عن جرائم الإنترنت إمّا لعدم اكتشاف الضحية لها أو خوفا من التشهير، إذ تُحجم الشركات والمؤسسات في مجتمعات الأعمال عن الإبلاغ عنها تجنبا للإساءة إلى السمعة وخوفا من التشهير[١٤].

**المبحث الثاني:آليات مكافحة الجريمة الالكترونية في قانون العقوبات**

أضاف المشرع الجزائري – في قانون العقوبات – مواداً لتجريم الاعتداءات الواردة على المعلومات، وذلك بموجب القانون: رقم 15/04 المتضمن تعديل قانون العقوبات، خاصة بعد التزايد اللاّمتناهي للاعتداءات على الأنظمة المعلوماتية بسبب تطور آليات الاتصال وظهور المواقع الإلكترونية والانترنت.

استحدث المشرع الجزائري بموجب القانون رقم 15/04 المؤرخ في: 10 نوفمبر 2004 المتضمن قانون العقوبات[١٥] قسما بعنوان " المساس بأنظمة المعالجة الآلية للمعطيات" حصر فيه الجرائم الماسّة بأنظمة المعالجة الآلية للمعطيات فيما يلي:

**الفرع الأول: جريمتا الدخول والبقاء غير المصرح بهما:**

نصّت المادة 394 مكرر من قانون العقوبات على ما يلي: "يعاقب بالحبس من ثلاثة أشهر إلى سنة وبغرامة من 50000دج إلى 100000دج كل من يدخل أو يبقى عن طريق الغش في كل جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك.

تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة".

يستفاد من هذه المادة أنّه يقصد بجريمة الدخول غير المصرح به الدخول غير المشروع – وهو ما عبّر عنه المشرع بالغش – إلى منظومة المعالجة الآلية للمعطيات، أي أن يكون الدخول إلى نظام المعلومات بدون وجه حق، فمناط عدم المشروعية هو انعدام سلطة الفاعل في الدخول إلى هذا النظام مع علمه بذلك.

ومن الحالات التي يكون الدخول غير مصرح به في النظام المعلوماتي، دخول الفاعل إلى النظام دون تصريح من المسؤول عن النظام أو مالكه، وقد يكون الفاعل مصرحا له بالدخول إلى جزء من النظام إلا أنه يتجاوز التصريح الممنوح له

---

[١٣] – خالد ممدوح إبراهيم، المرجع السابق، ص ٧٧.

[١٤] – سعيدي سليمة، حجاز بلال، جرائم المعلومات والشبكات في العصر الرقمي، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، 2017، ص ٦٣.

[١٥] منشور في الجريدة الرسمية، العدد 71 لسنة 2004.

ويدخل إلى كامل النظام أو إلى أجزاء أخرى يحظر عليه الدخول إليها، وهذا الفرض في الغالب يتم من طرف العاملين في المؤسسات التي يوجد بها النظام المعلوماتي.

يحصل الدخول غير المصرح به بأي وسيلة من الوسائل، فقد يتمّ باستعمال كلمة المرور الحقيقية متى كان الجاني غير مخول في استعمالها، أو عن طريق استخدام برامج أو شيفرة خاصة، أو عن طريق استخدام الرقم الكودي لشخص آخر في الدخول من خلال شخص مسموح له بالدخول سواء تمّ عن طريق شبكة الاتصال الهاتفية أو غير الانترنت[١٦].

أما جريمة البقاء غير المشروع داخل النظام المعلوماتي فيقصد بها التواجد داخل هذا النظام بالمخالفة لإرادة الشخص صاحب النظام أو من له السيطرة عليه. وتتحقق في الحالة التي يجد الشخص فيها نفسه داخل النظام عن طريق الخطأ أو الصدفة إلا أنه يقرر البقاء داخل النظام وعدم قطع الاتصال به، ويمكن تصور ذلك في الحالة التي يكون فيها الشخص في سبيله للدخول إلى نظام معلوماتي له الحق في الدخول إليه، إلا أنه يجد نفسه بسبب استخدام شيفرة خاطئة داخل نظام آخر[١٧].

نلاحظ أنّ المشرع الجزائري جرّم مجرّد الدخول أو البقاء غير المشروع داخل النظام المعلوماتي حتى ولو لم ينجم عن هذا الفعل ضرر بالنظام المعلوماتي، وشدّد العقوبة إذا ترتب على جريمة الدخول والبقاء غير المصرح بهما حذف أو تغيير لمعطيات المنظومة.

**الفرع الثاني: جريمة الاعتداء على المعطيات**

نصّت المادة 394 مكرر 1 من قانون العقوبات على ما يلي: "يعاقب بالحبس من ستة (6) أشهر إلى ثلاث (3) سنوات وبغرامة من 500000دج إلى 2000000دج كلّ من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدّل بطريق الغش المعطيات التي يتضمنها".

يتبيّن من هذه المادة أنّ المشرع الجزائري حصر صور الاعتداء على المعطيات في ثلاثة صور تتمثل في إدخال معطيات جديدة غير صحيحة إلى المعطيات الموجودة داخل النظام والتي تمت معالجتها آليا، ومحو وإزالة معطيات كانت موجودة، أو تعديل وتغيير المعطيات واستبدلها بأخرى من خلال برامج معيّنة تعمل على إتلاف المعطيات.

إذن، يعد مقترفا لجريمة الاعتداء على المعطيات كلّ من ارتكب أحد صور الاعتداء السابقة. وهي جريمة مستقلة عن جريمتي الدخول والبقاء غير المرخص بهما في نظام المعالجة، لأنه يمكن حصول الاعتداء عن بعد دون الدّخول أو البقاء في النّظام عن طريق استخدام برامج الفيروسات.

**الفرع الثالث: التعامل في معلومات غير مشروعة**

نصّت المادة 394 مكرر 2 من نفس القانون على أنّه: "يعاقب بالحبس من شهرين (2) إلى ثلاث (3) سنوات وبغرامة من 1000000دج إلى 5000000دج كل من يقوم عمدا أو عن طريق الغش بما يأتي:

1- 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 السابقة.

2- حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من أجل الجرائم المنصوص عليها في هذا القسم".

---

[١٦] – عودة يوسف سليمان، الجرائم الماسة بحرمة الحياة الخاصة التي تقع عبر وسائل تقنية المعلومات الحديثة ، ص ١٠.

[١٧] – نهلا عبد القادر المومني، المرجع السابق، ص ١٦١.

يستفاد من هذه المادة أنّ المشرع الجزائري أراد الحفاظ على ما تبقى من سريّة المعلومات بعد أن جرّم الأفعال التي يتم بواسطتها الحصول على هذه المعلومات في المادتين ٣٩٤ مكرر و٣٩٤ مكرر٢ المذكورتان أعلاه. وطبقا لنص هذه المادة فان جريمة التعامل في معلومات غير مشروعة لها صورتان، تتمثل الأولى في تجريم التعامل في المعلومات الصالحة لارتكاب جريمة عن طريق تصميمها أو البحث عن كيفية تصميمها[١٨]، أو تجميعها، أو توفيرها[١٩] أو نشرها لتمكين الغير من الاطلاع عليها[٢٠] أو الاتجار فيها، بينما تتمثل الصورة الثانية لهذه الجريمة في تجريم التعامل في معلومات متحصل عليها من جريمة عن طريق حيازتها أو إفشائها أو نشرها أو استعمالها لأي غرض.

وتضيف المادة 394 مكرر 6 بأنّه بالإضافة إلى الحبس والغرامة فإنّه "...يحكم بمصادرة الأجهزة والبرامج والوسائل المستخدمة مع إغلاق المواقع التي تكون محلاّ للجريمة من الجرائم المعاقب عليها وفقا لهذا القسم، علاوة على إغلاق المحل أو مكان الاستغلال إذا كانت الجريمة قد ارتكبت بعلم مالكها".

**المبحث الثالث: آليات مكافحة الجريمة الالكترونية في القوانين الخاصة**

نظرا لعدم كفاية نصوص قانون العقوبات لحماية الحياة الخاصة من مخاطر التكنولوجيا الحديثة، سنّ المشرع الجزائري مجموعة من القوانين لحماية الحياة الخاصة في ظل الجرائم المعلوماتية، وذلك ابتداء من سنة 2009 إلى الآن، وتتمثل هذه القوانين فيما يلي:

**المطلب الأول: آليات مكافحة الجريمة الالكترونية في قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال**

خصّ المشرع جرائم انتهاك الحياة الخاصة في البيئة الرقمية باهتمام ملحوظ فميّزها عن الجرائم التقليدية وسنّ قانونا خاصا بها هو القانون رقم 04/09 المتعلق بالقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها[٢١] الذي عرّف هذه الجرائم في المادة الثانية منه كما يلي: "الجرائم المتصلة بتكنولوجيات الإعلام والاتصال هي جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحدّدة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية".

ولقد حصر المشرع – في المادة الرابعة من هذا القانون – أربع حالات سمح فيها للسلطات المختصة باللجوء إلى مراقبة الاتصالات الإلكترونية تتمثل فيما يلي:

– الوقاية من جرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة.

– عند توافر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدّد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني.

– لمقتضيات التحري والتحقيقات القضائية عندما يصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الالكترونية.

– في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة

---

[١٨] – كتصميم برنامج يحمل فيروسا، وهو ما يطلق عليه البرامج الخبيثة.

[١٩] – وذلك عن طريق الإحالة لبرنامج يتصل ببرامج خاصة بإتلاف البيانات مثلا.

[٢٠] – وفي هذا السلوك خرق واضح للسرية المعلوماتية.

[٢١] – مؤرخ في 25 أوت 2009 منشور في الجريدة الرسمية، العدد 47 لسنة 2009.

كما ألزم المشرع مقدمي الخدمات بتقديم المساعدة للسلطات المكلفة بالتحريات القضائية لجمع وتسجيل المعطيات المتعلقة بمحتوى الاتصالات والمراسلات ووضعها تحت تصرفها، مع مراعاة سريّة هذه المعاملات، والالتزام بحفظ المعطيات التي تساعد في الكشف عن الجرائم ومرتكبيها، وكذلك التدخل الفوري لسحب المحتويات التي يطلعون عليها بمجرد العلم بمخالفتها للقوانين وتخزينها أو جعل الدخول إليها غير ممكن[٢٢].

هذا، وقد أنشأ المشرع الجزائري بموجب المادة 13 من هذا القانون هيئة وطنية للرقابة من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته، مهمّتها كشف وردع هذه الأنواع المستحدثة من الجرائم، ومساعدة السلطات القضائية في التحريات التي تجريها بشأن هذه الجرائم بما في ذلك تجميع المعلومات وإنجاز الخبرات القضائية.

**المطلب الثاني : آليات مكافحة الجريمة الإلكترونية في القانون المتعلق بالتوقيع والتصديق الإلكترونيين**

أصدر المشرع الجزائري بتاريخ 01 فبراير 2015 القانون رقم 04/15 المحدّد للقواعد المتعلقة بالتوقيع والتصديق الإلكترونيين[٢٣]، ولقد عرّف التوقيع الإلكتروني بأنّه: "بيانات في شكل إلكتروني مرفقة أو مرتبطة منطقيا ببيانات إلكترونية أخرى، تستعمل كوسيلة توثيق"، وشهادة التصديق الإلكتروني بأنّها: "وثيقة في شكل إلكتروني تثبت الصلة بين بيانات التحقق من التوقيع الإلكتروني والموقع".

إذن، يرتبط التوقيع والتصديق الإلكترونيين بمجموعة من البيانات والمعلومات ذات الطابع الشخصي التي يشكل الاعتداء عليها جريمة يعاقب مرتكبها بأحكام جزائية وردت في هذا القانون تتمثل فيما يلي:

**الفرع الأول: إفشاء البيانات الشخصية أو إساءة استعمالها**

طبقا للمادة 68 من هذا القانون يعاقب بالحبس من ثلاث أشهر إلى ثلاث سنوات وبغرامة من مليون دينار إلى خمسة ملايين دينار أو بإحدى هاتين العقوبتين فقط، كل من يقوم بحيازة أو إفشاء أو استعمال بيانات إنشاء توقيع إلكتروني موصوف خاص بالغير.

**الفرع الثاني: الإخلال بسرية البيانات**

وفقا لنص المادة 42 من هذا القانون يجب على مؤدي خدمات التصديق الإلكتروني أن يحافظوا على سرية البيانات والمعلومات المتعلقة بشهادات التصديق الإلكترونية الممنوحة، فإذا أخلوا بهذا الواجب يعاقب بالحبس من ثلاثة أشهر إلى سنتين وبغرامة من 200000دج إلى مليون دينار أو بإحدى هاتين العقوبتين[٢٤].

لقد أراد المشرع بهذا النص أن يضفي حمايته على المعلومات الشخصية التي تؤخذ من الأفراد، وأسبغ عليها صفة السرية لما لها من خصوصية معينة، وحسنا فعل عندما جرّم الإخلال بسرية هذه البيانات، فتخزين المعلومات لا يعني أنّ هذه المعلومات قد انتقلت من الخصوصية إلى العلانية، كما أنّ الرضا بالتجميع والتخزين لا يعني حرية تداول ونقل المعلومات إلى جميع الناس.

**الفرع الثالث: جمع البيانات الشخصية للمعني دون موافقته**

---

[٢٢] – يراجع نص المواد ١٠، ١١، ١٢ من القانون رقم 04/09 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

[٢٣] – منشور في الجريدة الرسمية، العدد ٠٦ لسنة ٢٠١٥.

[٢٤] – المادة 70 من القانون رقم 04/15.

نصّ القانون في المادة 43 منه على أنّه لا يمكن لمؤدي خدمات التصديق الإلكتروني أن يجمع البيانات الشخصية للمعني إلاّ بموافقته الصريحة، ومتى أخلّ بهذا الواجب يعاقب بالحبس من ستة أشهر إلى ثلاث سنوات، وبغرامة من 200000دج إلى مليون دينار أو بإحدى هاتين العقوبتين فقط.

**المطلب الثالث: آليات مكافحة الجريمة الإلكترونية في قانون القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية**

أصدر المشرع الجزائري القانون رقم 04/18 المؤرخ في 10 ماي 2018 المحدّد للقواعد العامة المتعلق بالبريد والاتصالات الإلكترونية[٢٥] والذي ألغى بموجبه القانون رقم 3/2000 المحدّد للقواعد العامة المتعلقة بالبريد والاتصالات السلكية واللاسلكية، والذي أكّد فيه على وجوب عدم مساس استعمال شبكات وخدمات الاتصال الإلكترونية بحفظ الحياة الخاصة للأفراد[٢٦]، وفي حالة مخالفة ذلك يتعرّض المخالف للأحكام الجزائية التي تضمنها هذا القانون، والمتمثلة فيما يلي:

**الفرع الأول: انتهاك سرية المراسلات الإلكترونية**

وفقا لنصّ المادة 164 من هذا القانون يعاقب بالحبس من سنة إلى خمس سنوات وبغرامة من 500000دج إلى مليون دينار كل شخص ينتهك سرية المراسلات المرسلة عن طريق البريد أو الاتصالات الإلكترونية أو يفشي مضمونها أو ينشره أو يستعمله بدون ترخيص من المرسل أو المرسل إليه أو يخبر بوجودها.

تتحقق هذه الجريمة باطلاع الشخص على الرسائل الإلكترونية أو سماع المحادثات الإلكترونية بصورة غير مشروعة، بصرف النظر عن مضمونها أو محتواها فيما إذا كان يتضمن أسرارا أم لا ،إضافة إلى إفشاء مضمونها أو نشره أو استعماله بدون ترخيص.

**الفرع الثاني: تحويل المراسلات الصادرة عن طريق البريد الإلكتروني**

تعاقب المادة 165 من القانون رقم 04/18 بالحبس من سنة إلى ثلاث سنوات وبغرامة من مليون دينار إلى خمس ملايين دينار أو بإحدى هاتين العقوبتين كل متعامل للاتصالات الإلكترونية يحوّل بأي طريقة كانت، المراسلات الصادرة أو المرسلة أو المستقبلة عن طريق الاتصالات الإلكترونية.

**المطلب الرابع: مكافحة الجريمة الإلكترونية في قانون حماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي**

في محاولة من المشرع الجزائري لمواكبة التطورات والجرائم التي تمسّ خصوصية الأفراد أصدر حديثا القانون رقم 18-07 المؤرخ في 10 يونيو 2018[٢٧] والذي هدف من خلاله إلى تحديد قواعد حماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي[٢٨] وذلك في إطار احترام الحياة الخاصة للأفراد[٢٩].

هذا، ويقصد بالمعطيات ذات الطابع الشخصي – وفقا لأحكام هذا القانون – "كل معلومة بغض النظر عن دعامتها متعلقة بشخص معرّف أو قابل للتعريف بصفة مباشرة أو غير مباشرة، لاسيّما بالرجوع إلى رقم التعريف أو عنصر أو عدّة

---

[٢٥] – منشور بالجريدة الرسمية، العدد 27 لسنة 2018.

[٢٦] – المادة 117 من القانون رقم 04/18.

[٢٧] – منشور في الجريدة الرسمية، العدد ٣٤ لسنة ٢٠١٨.

[٢٨] – طبقا لنص المادة ٠١ من هذا القانون.

[٢٩] – طبقا لنص المادة ٠٢ من هذا القانون.

عناصر خاصة بهويته البدنية أو الفيزيولوجية أو الجينية أو البيومترية أو النفسية أو الثقافية أو الاجتماعية"[٣٠]، أمّا معالجة هذه المعطيات فيقصد بها: "كل عملية منجزة بطرق أو وسائل آلية أو بدونها على معطيات ذات طابع شخصي، مثل الجمع أو التسجيل أو الحفظ أو الملاءة أو التغيير أو الاستخراج أو الاطلاع أو الاستعمال أو الإيصال عن طريق الإرسال أو النشر وكذا الإغلاق أو التشفير أو المسح أو الإتلاف"[٣١].

تجدر الإشارة إلى أنّ أي مخالفة لأحكام هذا القانون تعرّض المخالف للأحكام الجزائية المتمثلة فيما يلي:

**- خرق الحياة الخاصة عند معالجة المعطيات**

أوجب المشرع أنّ تتمّ معالجة المعطيات ذات الطابع الشخصي مهما كان مصدرها أو شكلها في إطار حماية الحياة الخاصة للأفراد[٣٢] وكلّ خرق لهذا الواجب يعاقب المخالف بالحبس من سنتين إلى 5 سنوات، وبغرامة من 200000دج إلى 500000دج[٣٣].

**- معالجة المعطيات الشخصية رغم اعتراض الشخص المعني**

اشترط المشرع – في المادة السابعة – من هذا القانون معالجة المعطيات ذات الطابع الشخصي بالموافقة الصريحة للشخص المعني، فإذا تمّت معالجة هذه المعطيات رغم اعتراضه يعاقب المخالف بالحبس من سنة إلى ثلاث سنوات وبغرامة من 100000دج إلى 300000دج[٣٤].

**- معالجة المعطيات الشخصية دون تصريح**

طبقا للمادة 12 من هذا القانون يجب إخضاع كل عملية معالجة معطيات شخصية لتصريح مسبق من السلطة المختصة، وفي حالة القيام بالمعالجة دون الحصول على هذا التصريح يعاقب المسؤول بالحبس من سنتين إلى خمس سنوات وبغرامة من 200000 دينار إلى 500000دينار.

**- الاستعمال غير الشرعي للمعطيات الشخصية**

المعلومات والبيانات الاسمية التي يتم تجميعها وتخزينها ومعالجتها في جهاز الحاسوب يتعين أن يكون لها هدف محدد وواضح ومعّين سلفا، ولا بدّ من التزام الجهة القائمة على النظام المعلوماتي بالهدف أو الغاية التي من أجلها قامت بتجميع المعلومات ومعالجتها الكترونيا، فلا يجوز وصول هذه المعلومات إلى شخص آخر أو جهة أخرى تجمع معلومات لغاية مغايرة لأنّ هذا من شأنه إلحاق الضرر بالشخص. لذا تدخل المشرع الجزائري وعاقب بالحبس من ستّة أشهر إلى سنة وبغرامة من 60000دج إلى 100000دينار، أو بإحدى هاتين العقوبتين فقط، كل من قام بإنجاز أو باستعمال معالجة معطيات غير تلك المصرح بها أو المرخص لها[٣٥].

**- جمع المعطيات الشخصية بطريقة غير شرعية**

---

[٣٠] – يراجع نص المادة ٠٣ من هذا القانون.

[٣١] – يراجع نص المادة ٠٣ من هذا القانون.

[٣٢] – المادة ٠٢ من القانون رقم ٠٧/١٨.

[٣٣] – المادة ٥٤ من القانون رقم ٠٧/١٨.

[٣٤] – المادة ٥٥ من القانون رقم 07/18.

[٣٥] – المادة ٥٨ من نفس القانون.

يعاقب بالحبس من سنة إلى ثلاث سنوات وبغرامة من 100000دينار إلى 300000 دينار كل من قام بجمع معطيات ذات طابع شخصي بطريقة تدليسية أو غير نزيهة أو غير مشروعة طبقا لنص المادة 59 من هذا القانون. فهذا الفعل فيه انتهاك للحياة الخاصة للأفراد يتمثل في جمع معلومات صحيحة عنهم لكن على نحو غير مشروع وغير قانوني.

ويستمد هذا الجمع صفته غير المشروعة إمّا من الأساليب غير المشروعة المستخدمة للحصول على هذه البيانات أو المعلومات كمراقبة الرسائل المتبادلة واعتراضها عن طريق البريد الالكتروني أو بتوصيل أسلاك خفية إلى الحاسوب الذي تختزن فيه البيانات، أو من حيث طبيعة مضمونها فتمثل صفة عدم المشروعية في أنّ البيانات غير صالحة للجمع بسبب مضمونها، كأن تتعلق بالمعتقدات الدينية والسياسية والانتماءات الحزبية والأصل العرقي للأفراد، فلا بدّ أن تكون بعيدة عن عمليات التجميع في الحواسيب، لأنّ مضمون هذه البيانات يدخل في نطاق الحياة الخاصة للأفراد[٣٦].

**- الولوج غير الشرعي للمعطيات الشخصية**

يعاقب بالحبس من 6 أشهر إلى سنتين وبغرامة من 60000 دينار إلى 200000دينار أو بإحدى العقوبتين فقط، كل من عرقل عمل السلطة الوطنية:

1- بالاعتراض على إجراء عملية التحقق في عين المكان.

2- عن طريق رفض تزويد أعضائها أو الأعوان الذين وضعوا تحت تصرفها بالمعلومات والوثائق الضرورية لتنفيذ المهمة الموكلة لهم أو إخفاء أو إزالة الوثائق أو المعلومات المذكورة.

3- عن طريق إرسال معلومات غير مطابقة لمحتوى التسجيلات وقت تقديم الطلب أو عدم تقديمها بشكل مباشر واضح[٣٧].

**- إفشاء المعطيات الشخصية**

يعاقب الشخص الذي يقوم بإفشاء معلومات محمية بموجب المادة 301 من قانون العقوبات الخاصة بإفشاء الأسرار المهمّة[٣٨].

**- الاحتفاظ بالمعطيات الشخصية أكثر من المدة القانونية**

يعاقب بغرامة من 200000دج إلى 500000دينار المسؤول عن المعالجة الذي يحتفظ بالمعطيات ذات الطابع الشخصي بعد المدّة المنصوص عليها في التشريع الساري المعمول أو تلك الواردة في التصريح أو الترخيص، وهذا وفقا لمقتضيات المادة 65 من هذا القانون.

**- نقل المعطيات الشخصية إلى دولة أجنبية**

يعاقب من سنة إلى 5 سنوات، وبغرامة من 500000 دينار إلى 1000000 دينار كل من ينقل معلومات ذات طابع شخصي نحو دولة أجنبية[٣٩].

**الخاتمة**

---

[٣٦] – نهلا عبد القادر المومني، المرجع السابق، ص ١٧٤- ١٧٥.

[٣٧] – المادة 60 من القانون رقم 07/18.

[٣٨] – المادة 62 من نفس القانون.

[٣٩] – المادة 67 من هذا القانون.

بيّنا من خلال دراستنا أنّه بالرغم من النواحي الإيجابية للأنظمة المعلوماتية إلاّ أنّه ترتّب عنها جوانب سلبية نجمت عن استغلال بعض الأفراد والجهات للتقنيات المعلوماتية لتسهيل ارتكاب العديد من الجرائم، كما أصبح النظام المعلوماتي ذاته محلاّ للاعتداء عليه وإساءة استخدامه.

وعلى اعتبار الجريمة الإلكترونية ظاهرة إجرامية مستجدّة تستهدف الاعتداء على المعلومات المخزنة أو المعالجة في نظام الحاسب الآلي أو المتبادلة عبر الشبكات، فإنّ طبيعتها المتفردة أدّت إلى صعوبة إدراجها ضمن الأوصاف التقليدية في القوانين الجنائية الوطنية والدولية إذ يتعيّن مواجهة هذه الجريمة الإلكترونية بنصوص تجريمية جديدة.

وفي هذا الشأن، كان حرص المشرع الجزائري كبيرا على مواكبة النهضة التكنولوجية والمعلوماتية التي يعيشها العصر، فأدخل تعديلات على قانون العقوبات لجعله يتجاوب مع هذه التطورات، واستحدث عدّة قوانين لضمان الحماية الجزائية للمعاملات الإلكترونية كان آخرها في 2018 عندما أصدر القانون رقم 07/18 الخاص بحماية المعاملات الإلكترونية وحماية المعلومات المعالجة ذات الطابع الشخصي وذلك في إطار احترام الحياة الخاصة للأفراد، وهذا التنوع التشريعي من شأنه أن يساهم بشكل فعّال في الوقت الراهن للتصدي للجرائم الإلكترونية في الجزائر.

ولابدّ من الاعتراف بجهود المشرع الجزائري في محاربة الجرائم الإلكترونية من خلال مواكبة أحدث الاتجاهات العلمية والنظرية ومحاكاة التقدّم التقني والتكنولوجي، إلاّ أنّها تبقى غير كافية لتحقيق أمن المعلومات، نظرا للتطور السريع للجريمة الإلكترونية من جهة، وللطابع العالمي والعابر للحدود الذي تتميّز به من جهة أخرى، لذا لابدّ من تعزيز التعاون الدولي قضائيا وإجرائيا في مجال مكافحة الجرائم الإلكترونية، والعمل على دراسة ومتابعة المستجدات العالمية.

استنادا لما سبق فإنّنا نخلص للتوصيات التالية لمواجهة الجرائم الإلكترونية:

– ضرورة التنسيق والتعاون الدولي قضائيا وإجرائيا في مجال مكافحة الجرائم الإلكترونية، ودراسة ومتابعة المستجدات على الساحة العالمية.

– تخصيص شرطة خاصة لمكافحة الجرائم الإلكترونية، وذلك من رجال الشرطة المدربين على كيفية التعامل مع أجهزة الحاسوب والإنترنت.

– تدريب رجال النيابة العامة والقضاء بشأن التعامل مع أجهزة الكمبيوتر والإنترنت من خلال دورات تدريبية متخصصة.

– تدريس مواد بكلية الحقوق بالجامعات خاصّة بالحماية القانونية للمعلوماتية وكل ما يتعلّق بالكمبيوتر والإنترنت.

**قائمة المراجع:**


– أحمد خليفة الملط، الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية.

– خالد محمود إبراهيم، الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية، 2009.

– خالد محمد كدفور المهيري، جرائم الكمبيوتر والإنترنت والتجارة الإلكترونية، دار الغرير للطباعة والنشر، دبي، 2005.

– سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، الطبعة الأولى، دار النهضة العربية، القاهرة، 1994.

– سعيدي سليمة، حجاز بلال، جرائم المعلومات والشبكات في العصر الرقمي، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، 2017.

– قورة نائلة، جرائم الحاسب الاقتصادية، الطبعة الأولى، دار النهضة العربية، القاهرة، 2004.

– عودة يوسف سليمان، الجرائم الماسة بحرمة الحياة الخاصة التي تقع عبر وسائل تقنية المعلومات الحديثة.

– محمود إبراهيم الغازي، الحماية الجنائية للخصوصية والتجارة الإلكترونية، مكتبة الوفاء القانونية، الإسكندرية، الطبعة الأولى، 2014.

– نهلا عبد القادر المومني، الجرائم المعلوماتية، الطبعة الأولى، دار الثقافة للنشر والتوزيع، الأردن، 2008.