

الحماية القانونية لبيانات المتعاملين في البيئة الرقمية

The legal protection of costumer's data in the digital environment



رحيل سمير *¹، سوفالو أمال²

¹ جامعة الجزائر 1، الجزائر

s.rahil@univ-alger.dz

² جامعة الجزائر 1، الجزائر

a.soufalou@univ-alger.dz

تاريخ الإرسال: 2024/09/14 تاريخ القبول: 2024/10/20 تاريخ النشر: 2024/12/01

ملخص:

توسع استعمال الإنترنت نتيجة التطور الهائل الذي عرفه مجال النظم المعلوماتية، فظهرت البيئة الرقمية كمجتمع افتراضي موازي للمجتمع الحقيقي الذي نعيشه، أين أصبح الإنسان يمارس مختلف معاملاته اليومية بسرعة و سهولة. لكن في خضم هذا التطور وانتشار استعمال البيانات الشخصية في العالم الافتراضي، زادت المخاطر التي تهدد أمنها وسلامتها، لاسيما أن التعامل بهذه البيانات يتم عبر شبكات الاتصال المفتوحة التي تحيطها الكثير من المخاطر وتطالبها العديد من الاعتداءات، هو الأمر الذي جعل المشرع الجزائري يسعى لتعديل قوانينه و مواكبة التطورات الحاصلة، كما قام باستحداث قوانين خاصة بهدف توفير حماية أكثر لبيانات متعاملي العالم الافتراضي، وتعزيز الثقة والأمان بينهم، كان أهمها القانون 04-15 و القانون 04-18.

الكلمات المفتاحية: الحماية القانونية؛ البيانات الشخصية؛ البيئة الرقمية؛ المعاملات الإلكترونية

Abstract:

The use of the Internet expanded as a result of the tremendous development witnessed in the field of information systems. The digital environment appeared as a virtual society parallel to the real society in which we live, where humans began to carry out their various daily transactions quickly and easily. But in the midst of this development and the spread of personal data in the virtual world, the danger to people's private lives and the rest of their rights and property is increasing, especially since dealing with this data takes place via open networks that are surrounded by many risks and subject to many attacks, which is what made the Algerian legislator seek to amend its laws to keep pace with the current developments. It also created special laws that would provide more protection for the data of users of the virtual world, the most important of which were Law 15-04 and Law 18-04.

Keywords: legal protection; personal data; digital environment; Electronic transactions.

مقدمة:

لا يزال التطور التكنولوجي يلقي بظلاله على كافة مجالات حياة الإنسان كنتيجة لما شهده العالم في السنوات الأخيرة من تطور هائل للنظم المعلوماتية، كانت بدايته الثورة المعلوماتية ثم تطور وسائل الاتصالات الإلكترونية للذات أنتجا عملاق الإنترنت، حيث نشأ داخل هذه الشبكة العالمية مجتمع افتراضي موازي للمجتمع الحقيقي الذي نعيشه، أين أصبح الشخص يمارس مختلف نشاطاته اليومية بكل سرعة و سهولة من مكانه، دون عناء التنقل.

في خضم هذا التطور الذي عرفه مجال النظم المعلوماتية انتشر التعامل بالبيانات الشخصية بمختلف أنواعها، التي تمثل هوية الشخص و تعتبر كذلك وسيلة أساسية تمكنه من إقامة العلاقات و المعاملات في البيئة الرقمية. مقابل ذلك أصبحت هذه الوسائل خطرا بالغاً يهدد الحياة الخاصة للفرد وحقه في سرية معلوماته الشخصية، لاسيما أن التعامل بهذه البيانات يتم عبر الشبكات المفتوحة التي تعترضها الكثير من الانتهاكات والاعتراضات.

من هنا تبرز أهمية الدراسة، حيث بات من الضروري توفير الحماية اللازمة لمعاملتي العالم الافتراضي من الأعمال الإجرامية، التي عرفت هي كذلك بدورها طفرة نوعية بالموازاة مع تطور الوسائل التكنولوجية المستخدمة في ذلك، هو الأمر الذي يثير مسألة التوفيق بين ضرورة الاستفادة من هذه الوسائل التقنية، وبين وجوب إيجاد الوسائل القانونية اللازمة لتفادي الأضرار المترتبة عن استخدامها، فبالقدر الذي سهلت فيه الوسائل التكنولوجية تنظيم البيانات الشخصية و التعامل؛ بقدر ما سهلت إمكانية الحصول عليها و تجميعها من طرف الغير بهدف الاستغلال غير المشروع لها، مما يثير مسألة الثقة عند التعامل بهذه الوسائل و الأمن المعلوماتي إلى جانب ذلك.

هذه الإشكالات أصبحت هاجسا يؤرق المشرعين عند تنظيم مجال المعاملات الإلكترونية، و على غرار هؤلاء سعى المشرع الجزائري إلى مراجعة منظومته القانونية، من خلال تعديل القوانين العامة و استحداث أخرى خاصة حتى تكون قوانينه أكثر ملاءمة لتطور المعاملات و العلاقات بين أشخاص المجتمع الحديث، أدرج ضمنها مختلف الآليات و الإجراءات القانونية لحماية بيانات الأشخاص، كان من بينها القانون 04-15 المحدد للقواعد العامة المتعلقة بالتوقيع و التصديق الإلكترونيين،¹ و القانون 04-18 المحدد للقواعد العامة المتعلقة بالبريد و الاتصالات الإلكترونية.²

¹ القانون رقم 04-15 المؤرخ في 01 فيفري 2015، المحدد للقواعد العامة المتعلقة بالتوقيع و التصديق

الإلكترونيين، ج ر، ع 06، الصادر في 10 فيفري 2015.

² القانون رقم 04-18 المؤرخ في 10 ماي 2018، المحدد للقواعد العامة المتعلقة بالبريد و الاتصالات

الإلكترونية، ج ر، ع 27، الصادر في 13 ماي 2018.

وعليه نطرح الإشكالية التالية: ما هي الحماية القانونية التي وفرها المشرع الجزائري للبيانات الشخصية في إطار التعامل الإلكتروني؟ وما مدى فعالية النصوص المستحدثة لذلك؟

للإجابة على هذه الإشكالية اعتمدنا على المنهج الوصفي، كونه يساعد في التعرف على المفاهيم الجديدة للموضوع و إظهار مختلف الجوانب المحيطة به، كما اعتمدنا كذلك على المنهج التحليلي من أجل تحليل النصوص القانونية و المادة العلمية المتعلقة بالموضوع، بهدف الإحاطة بالجوانب القانونية المتعلقة بالبيانات الشخصية للمتعاملين في البيئة الرقمية، و معرفة مدى نجاعة النصوص القانونية في توفير الحماية القانونية اللازمة لها.

حيث تمّ تقسيم الموضوع إلى مبحثين:

تطرقنا في المبحث الأول إلى: حماية البيانات الشخصية المرتبطة بالتوقيع والتصديق الإلكترونيين في القانون رقم 04-15

أما المبحث الثاني فخصصناه لدراسة: حماية البيانات الشخصية من جرائم الإتصالات الإلكترونية في إطار القانون 04-18

المبحث الأول

حماية البيانات الشخصية المرتبطة بالتوقيع والتصديق الإلكترونيين في القانون رقم 04-15

مع الانتشار الواسع لاستخدام وسائل الاتصال الحديثة والتطورات الحاصلة في مجال التعامل بين الأشخاص و إقامة التصرفات عن بعد، دأب المشرع الجزائري على مراجعة القواعد القانونية حتى تكون أكثر ملاءمة و تماشيا مع مقتضيات التجارة الإلكترونية و التعاقد الإلكتروني

حيث أقر الكتابة و التوقيع الإلكترونيين من بين الوسائل المستخدمة في ذلك، فأعترف بهما عند تعديله للقانون المدني سنة 2005،¹ تبعه بجملة من النصوص القانونية التي تنظم و تحدد أحكام التعامل بها؛ فأصدر القانون رقم 04-15، الذي عرّف من خلاله التوقيع الإلكتروني في المادة (02) على أنه: " بيانات في شكل إلكتروني، مرفقة أو مرتبطة منطقيا ببيانات إلكترونية أخرى، تستعمل كوسيلة توثيق".²

¹ إعترف المشرع الجزائري بالكتابة و التوقيع الإلكترونيين عند تعديل القانون المدني سنة 2005، ضمن المادتين (323مكرر1) و (327)، و ذلك بموجب القانون رقم 10-05 المؤرخ في 20 جوان 2005، المعدل و المتمم للأمر رقم 58-75 المتضمن القانون المدني الجزائري.

² جاء هذا التعريف في الفقرة الثانية من المادة الثانية، التي أورد المشرع ضمنها مجموعة من التعريفات، لتحديد مفهوم هذه المصطلحات الجديدة في الميدان القانوني، نظرا للطبيعة التقنية التي تميزها، كما أنه تباينت التعريفات التي تطلق عليها، سواء من طرف المشرعين أو الفقهاء.

ومن منظور حماية البيانات الشخصية، يمكن تعريف هذا التوقيع على أنه مجموعة البيانات الإلكترونية الشخصية التي تحدد هوية الشخص و تمكنه من إقامة علاقات و معاملات في البيئة الرقمية، حيث ينفرد الموقع بهذه البيانات و يتميز بها عن غيره من الأشخاص.

و لإضفاء الموثوقية على هذه البيانات و سلامة التعامل بها، جعل المشرع شهادة التصديق الإلكتروني كأساس لإنشاء هذا التوقيع و في نفس الوقت وسيلة للتحقق من صحته و سلامته.

حيث عرّفت المادة الثانية شهادة التصديق الإلكتروني بأنها: "وثيقة في شكل إلكتروني تثبت الصلة بين بيانات التحقق من التوقيع الإلكتروني و الموقع".

و من هنا يتضح أن بيانات هذه الشهادة تبقى شخصية مادامت متعلقة ببيانات التوقيع و بيانات الشخص الموقع،¹ بالرغم من حيازتها لدى جهات التوثيق (جهات التصديق الإلكتروني).

نظرا لأهمية هذه البيانات و الدور الذي تلعبه في مجال المعاملات الإلكترونية، أحاطها المشرع الجزائري بالعناية اللازمة لمنع التعدي عليها و الاستعمال غير المشروع.

لتوضيح ذلك سنتطرق في (المطلب الأول) إلى تدابير حماية بيانات التوقيع و التصديق الإلكترونيين، ثم نتعرض في (المطلب الثاني) إلى الجزاءات المقررة للأفعال الماسة بهذه البيانات.

المطلب الأول: تدابير حماية بيانات التوقيع و شهادة التصديق الإلكترونيين

تتجلى مظاهر حماية البيانات الشخصية في قانون 04-15 من خلال جملة الشروط الصارمة و الضوابط التقنية التي فرضها المشرع، بخصوص عملية إنشاء التوقيع الإلكتروني و كذا إجراءات إصدار شهادة التصديق الإلكتروني؛ كتدابير وقائية و حماية قبلية للبيانات المتعلقة بها.

حيث جاء في المادة (08) من القانون المذكور أعلاه، أنه لا يعتد بالتوقيع الإلكتروني في مجال المعاملات الإلكترونية، إلا بالتوقيع الإلكتروني الموصوف.²

و هذا التوقيع حسب نص المادة (07) هو التوقيع الذي يجب أن تتوفر فيه مجموعة المتطلبات تتعلق بموثوقيته و أمن بياناته، نذكر أهمها:

¹ ثروت عبد الحميد، التوقيع الإلكتروني- ماهيته، مخاطره، و كيفيات مواجهتها، دار الجامعة الجديدة، مصر، 2007، ص 61.

² لقد ميز المشرع بين نوعين من التوقيع، الأول توقيع إلكتروني بسيط (عادي)، والثاني هو التوقيع الإلكتروني الموصوف، و الفرق بينهما أن الأول يتم إنشاءه بتقنيات و إجراءات بسيطة، حيث لا تتوفر على نسبة عالية من الحماية و الأمان، أما التوقيع الإلكتروني الموصوف فهو التوقيع الذي يتم إنشاؤه بشهادة تصديق إلكتروني موصوفة، و وفق آلية مؤمنة و موثوقة...يحوز هذا الأخير على نسبة عالية من الأمان و المصادقية عند التعامل به.

أن ينشأ على أساس شهادة تصديق إلكتروني موصوفة، أن تكون بياناته مرتبطة ببيانات الشخص الموقع وحده دون سواه، كما يجب أن يكون هذا التوقيع مصمما بواسطة آلية مؤمنة خاصة بإنشاء التوقيع الإلكتروني، تجدر الإشارة إلى أن هذه الشروط قد انفرد بها المشرع الجزائري عن غيره من التشريعات، التي لم تشر إلى شهادة التصديق الإلكتروني الموصوفة ضمن تعريف التوقيع الإلكتروني المؤمن.¹

الفرع الأول: آليات إنشاء التوقيع كوسيلة حماية لبياناته

من أجل موثوقية هذا التوقيع وسلامة بياناته، حدد المشرع في الفصل الثاني آليات إنشائه، بحيث يجب أن ينشأ التوقيع الإلكتروني الموصوف وفق آلية مؤمنة حسب الشروط و المتطلبات المنصوص عليها في المادة(11)، كما يجب أن ينشأ وفقاً لآلية تمكّن التحقق منه بصفة موثوقة طبقاً للشروط المنصوص عليها في المادة(13).

عند الاطلاع على مجموعة الشروط السابق ذكرها، يتضح جليا حرص المشرع على ضرورة وقاية البيانات المتعلقة بإنشاء التوقيع الإلكتروني، في مواجهة أيّ اختراق أو تعدي عليها. كما حرص كذلك على عدم وقوع استعماله من طرف الغير، بالتأكيد على أنه عند إنشاء التوقيع يجب أن يكون معرّفاً بشخصية الموقع وأن يكون مميزاً له عن غيره، بالإضافة لاشتراط إنشائه وفق آليات تقنية تضمن تأمين بياناته وإمكانية التحقق من صحة وسلامة التوقيع، وذلك لما رآه المشرع من أهمية بالغة في حماية حقوق المتعاملين مع صاحب التوقيع. وهو ما نص عليه قانون اليونسترال النموذجي بشأن التجارة الإلكترونية لسنة 1996، في مادته السابعة: "...إذا ما إشتراط القانون وجود توقيع شخص في رسالة بيانات، يجب أن تستخدم فيها طريقة لتعيين ذلك الشخص".²

ولتعزيز الحماية أكثر للبيانات المستخدمة في إنشاء التوقيع الإلكتروني وإستعماله، أكدّ المشرع في المادة(14) على أنه لا يمكن منح الإعتماد لمقدمي الخدمات الإلكترونية من طرف الهيئة الرسمية المكلفة بذلك، إلا بعد التأكد من مطابقة الآليات المستخدمة في إنشاء التوقيع مع المتطلبات والشروط المذكورة سابقا.

¹ حزام فتيحة، الإثبات الإلكتروني في المسائل المدنية و التجارية، أطروحة دكتوراه في العلوم القانونية،

جامعة الجزائر 1 بن يوسف بن خدة، سنة 2015-2016، ص32.

² أبو الهجاء محمد إبراهيم، عقود التجارة الإلكترونية، دار الثقافة للنشر، الأردن 2011. ص 126.

الفرع الثاني: شهادة التصديق الإلكتروني ضماناً لحماية حقوق المتعاملين وبياناتهم الشخصية

أما بخصوص شهادة التصديق الإلكتروني، فالغرض منها هو توثيق البيانات الإلكترونية بتأكيد إنتسابها لمُصدرها مع التحقق من سلامتها؛ بمعنى أن جهات التصديق الإلكتروني¹ تلعب دور الموثق كطرف ثالث محايد، كوسيط بين المتعاملين يقوم بتوثيق المعاملات ويسمح بالتأكد من الهوية الإلكترونية مع صحة البيانات عن طريق شهادة التصديق التي يصدرها.

و نظرا للدور الكبير لهذه الشهادة وأهميتها في توثيق المعاملات الإلكترونية، أقرّ المشرع مجموعة من الشروط القانونية والضوابط التقنية لإصدارها، من طرف جهات معتمدة ومرخص لها من الدولة، تحت إشراف هيئات عليا في البلاد، نظمها المشرع الجزائري في القانون 04-15 على شكل سلطات ضمن الفصل الثاني بعنوان: "سلطات التصديق الإلكتروني".

و تتمثل هذه السلطات في: السلطة الوطنية للتصديق الإلكتروني²، تنشأ لدى الوزير الأول³، والسلطة الحكومية للتصديق الإلكتروني، تنشأ لدى الوزير المكلف بالبريد وتكنولوجيا الإعلام والاتصال⁴. كما عينت السلطة المكلفة بضبط البريد والمواصلات السلكية واللاسلكية، كسلطة إقتصادية للتصديق الإلكتروني⁵، حيث تقوم هذه الأخيرة بدور مؤدي خدمات التصديق إلى غاية تعيين الجهة المختصة بذلك.

¹ اختلفت التسميات التي أطلقها الفقه والقانون على هذه الجهات، بين تسمية التوثيق الإلكتروني، الطرف الثالث الموثق، الغير الموثق، مقدم خدمة التصديق الإلكتروني... أما المشرع الجزائري فأطلق عليها تسمية مؤدي خدمة التصديق الإلكتروني.

² تولى تنظيمها وسير عملها المرسوم التنفيذي رقم 134-16 المؤرخ في 25 أفريل 2016، المحدد لتنظيم المصالح التقنية والإدارية للسلطة الوطنية للتصديق الإلكتروني وسيرها ومهامها، ج ر، ع 26، الصادر في 28 أفريل 2016.

³ تولى تنظيمها المرسوم التنفيذي رقم 134-16 المؤرخ في 25 أفريل 2016، المحدد لتنظيم المصالح التقنية والإدارية للسلطة الوطنية للتصديق الإلكتروني وسيرها ومهامها، ج ر، ع 26، الصادر في 28 أفريل 2016.

⁴ نظم أحكامها المرسوم التنفيذي رقم 135-16 المؤرخ في 25 أفريل 2016، المحدد لطبيعة السلطة الحكومية للتصديق الإلكتروني وتشكيلها وتنظيمها وسيرها، ج ر، ع 26، الصادر في 28 أفريل 2016.

⁵ تمّ تعيين هذه السلطة وتحديد مهامها بموجب المادتين (29) و (30) من القانون 04-15، كما أن هذه السلطة تقوم بدور مؤدي خدمات التصديق الإلكتروني وكذا منح الإعتمادات لمقدمي خدمات التوقيع والتصديق الإلكترونيين، خلال مرحلة انتقالية حددت بخمس سنوات إلى حين صدور النصوص التنظيمية التي تحدد الجهات المعنية بذلك، وهذا طبقا للمادتين (78) و (79) من نفس القانون، لكن من الناحية العملية لم يتم تعيين أي جهة تقوم بذلك، وهو الأمر الذي جعل معظم النصوص المنظمة للتوقيع الإلكتروني دون تفعيل.

إلى جانب الخدمات التي تؤديها هذه السلطات في مجال الخدمات الإلكترونية و السهر على تنظيمها و تطويرها، هي مكلفة كذلك بالعديد من المهام و الصلاحيات في مجال حماية البيانات الإلكترونية، نذكر أهمها في النقاط التالية:

- إعداد دفتر الشروط المحدد لكيفيات تأدية خدمات التصديق الإلكتروني.

- إعداد وتنفيذ تدابير الأمن المادي و سياسة الأمن المعلوماتي

- إعداد وتنفيذ تدابير الأمن التنظيمية و التقنية

- ضمان اليقظة فيما يخص أمن الأنظمة و الشبكة المعلوماتية

- منح التراخيص لمؤدي خدمات التصديق و التوقيع الإلكترونيين، مع متابعة و مراقبة نشاطهم

- حفظ البيانات المتعلقة بمنح شهادات التصديق

- الإحتفاظ بشهادات التصديق الإلكتروني المنتهية صلاحيتها¹

كما تتجلى مظاهر حماية البيانات الإلكترونية للأشخاص في القانون رقم 04-15 من خلال الإجراءات الصارمة التي فرضها المشرع من أجل منح الترخيص لمؤدي خدمات التصديق الإلكتروني، بالإضافة إلى الواجبات و المسؤولية المشددة عليه، حيث خصص لذلك الفصل الثالث من الباب الثاني بعنوان: "النظام القانوني لتأدية خدمات التصديق الإلكتروني".

و على من يرغب القيام بنشاط مؤدي خدمات التصديق الإلكتروني أن يقدم طلب الترخيص، و أن يستوفي جملة من الشروط المذكورة في المادة(34)، نذكر أهمها:

- أن يكون خاضعا للقانون الجزائري إذا كان شخص معنوي أو الجنسية الجزائرية بالنسبة للشخص

الطبيعي

- أن يتمتع بمؤهلات و خبرة ثابتة في ميدان تكنولوجيا الإعلام و الإتصال

- ألا يكون قد سبق الحكم عليه في جناية أو جنحة تتنافى مع نشاط تأدية خدمات التصديق

و عند حصوله على الترخيص لمباشرة نشاطه تترتب عليه عدة إلتزامات، يهدف من خلالها المشرع تحقيق

سلامة و حماية بيانات الأشخاص المتعاملين معه، منها ما جاء في المادة(42)، حيث يجب عليه الحفاظ على

سرية البيانات و المعلومات المتعلقة بشهادة التصديق الإلكتروني الممنوحة.

¹ لمزيد من التفصيل و الإطلاع على المهام الأخرى، راجع مواد المرسومين التنفيذييين المذكورين أعلاه.

كما نصت المادة (43) على أنه لا يمكنه جمع البيانات الشخصية إلا بعد موافقة صريحة من المعني، و لا يمكنه أن يجمع إلا البيانات الشخصية الضرورية لمنح شهادة التصديق الإلكتروني، مع ضمان عدم إستعمال هذه البيانات لأغراض أخرى.

أما بخصوص المسؤولية المدنية المترتبة على مؤدي خدمة التصديق الإلكتروني فقد نصّت المادة (53) صراحة على أنه يكون مسؤولا عن الضرر الذي يلحق بأية هيئة أو أي شخص اعتمدوا على شهادة تصديق مسلمة من طرفه، وذلك إذا ثبت عدم صحة المعلومات الواردة في الشهادة التي قدمها، أو في حالة منحه شهادة تصديق دون التأكد من مطابقة بيانات هوية صاحب التوقيع مع بيانات التحقق المحددة في شهادة التصديق الإلكتروني.

عند الإطلاع على جملة الشروط المفروضة على منح الترخيص لمؤدي خدمات التصديق، يتضح حرص المشرع الجزائري على توفير الضمانات اللازمة لتحقيق الأمن و الثقة بين المتعاملين الرقميين، و إضفاء حماية أوفر لحقوقهم بضمن عدم قوع أي شكل من أشكال الإحتيال أو تلاعب بالبيانات الشخصية من طرف مؤدي خدمة التصديق الإلكتروني أو من الغير.

كما نستنتج من خلال التطرق للإجراءات المتبعة في عملية التصديق الإلكتروني أن وضع صلاحيات منح الترخيص في يد السلطة الإقتصادية للتصديق الإلكتروني كجهة حكومية، سيضمن رقابة الدولة على مقدمي خدمات التصديق الإلكتروني، وإستمرارية لتطبيق الشروط والضوابط التي يقرها القانون، وبالتالي تحقيق الأمان والإستقرار في نظام التعامل الإلكتروني.

المطلب الثاني: الحماية الجزائية للبيانات الشخصية في القانون رقم 04-15

أقر المشرع نوعين من العقوبات على مخالفتي أحكام هذا القانون، تضمنها الباب الرابع بعنوان: "العقوبات"، و تقسم إلى نوعين: عقوبات مالية وإدارية، والأخرى جزائية

الفرع الأول: العقوبات المالية والإدارية

نظرا لأهمية التنظيم الذي تكتسيه عملية التصديق الإلكتروني، لاسيما أنها متعلقة بأمن الأشخاص و مرتبطة مع النظام العام، حرص المشرع على تطبيق التدابير و شروط ممارسة هذه المهام، مقابل ذلك أقر عقوبات مالية وإدارية لمخالفتي أحكام القانون المنظم لها.

ورد في نص المادة (64) من ذات القانون أنه في حالة عدم إحترام مؤدي خدمات التصديق الإلكتروني لأحكام دفتر الشروط و سياسة التصديق الإلكتروني، تطبق عليه السلطة الإقتصادية عقوبة مالية يتراوح مبلغها ما بين (200) ألف دج و (500) دج، كما يمكن أن تصل العقوبة إلى سحب الترخيص الممنوح له و إلغاء شهادته.

كما جاء في نص المادة (65) أنه في حالة إنتهاك مؤدي خدمات التصديق الإلكتروني لمقتضيات الدفاع الوطني والأمن العمومي، تقوم السلطة بالسحب الفوري للترخيص منه، مع إتخاذ التدابير التحفظية اللازمة بشأن تجهيزاته.

الفرع الثاني: العقوبات الجزائية

لتدعيم الحماية القانونية للبيانات الشخصية المرتبطة بخدمات التوقيع و التصديق الإلكترونيين، حرص المشرع الجزائي على أن تكتسي هذه البيانات طابع السرية والأمان، عند تنظيمه لنشاطات مقدمي خدمات التوقيع و التصديق، حيث حصر المشرع في هذا القانون الأفعال المجرمة و المعاقب عليها من المادة (66) إلى المادة (75)، و أقر عقوبات لمرتكبها بالحبس من (3) ثلاث أشهر إلى (3) ثلاث سنوات، مع غرامات مالية تتراوح ما بين (20) ألف دج إلى (5) خمس ملايين دج.

تتمثل هذه الجرائم في الأفعال التالية:

- حيازة أو إفشاء أو إستعمال بيانات إنشاء توقيع إلكتروني تخص الغير.
 - عدم الحفاظ على سرية البيانات و المعلومات المتعلقة بالتوقيع و شهادة التصديق الإلكترونيين
 - جمع البيانات الشخصية للغير دون موافقة صريحة منهم
 - إستعمال بيانات التوقيع و شهادة التصديق الإلكتروني لأغراض أخرى
 - الكشف عن معلومات سرية من قبل المكلف بعمليات التدقيق، كان قد علمها أثناء تأدية مهامه
 - تأدية خدمات التصديق الإلكتروني دون ترخيص، أو بعد سحب الترخيص.
- كما أقرت المادة (75) عقوبة الشخص المعنوي إذا ارتكبت لحسابه إحدى الجرائم المذكورة سابقا، حيث تضاعف الغرامة المالية إلى (5) خمس مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي.
- تجدر الإشارة إلى أن تجريم المشرع لتلك الأفعال ورد على سبيل الحصر وليس على سبيل المثال، حيث خصص لكل فعل مادة تجرمه، و بذلك يعاب على المشرع أنه ضيق من دائرة التجريم ولم يترك المجال لهذه النصوص أن تستوعب أشكالا أخرى من أعمال الإعتداءات التي تمس بالبيانات الشخصية، لاسيما و أن هذه الأفعال في تطور مستمر مع كل تطور تكنولوجي.

المبحث الثاني

حماية البيانات الشخصية من جرائم الاتصالات الإلكترونية في القانون 04-18

مع تعدد وسائل الاتصالات التكنولوجية و توسع استعمالها في شتى مجالات عمل الإنسان، نظرا لما تتيحه هذه الوسائل من سهولة في التعامل و القيام بمختلف التصرفات مع أشخاص متواجدين في أماكن

بعيدة من العالم، كما أنه علاوة على السرعة التي تحققها في نقل البيانات و تدفقها بكميات كبير، يمكن لهذه الوسائل معالجتها و التحكم فيها بدقة و سرعة فائقة. لكن رغم كل المزايا التي جاء بها هذا التطور التقني إلا أنه قد تعددت معه المخاطر التي تهدد سلامة و أمن البيانات الشخصية،¹ لاسيما أن التعامل بها يتم عبر الشبكات المفتوحة مما يسمح بإعتراضها عند تبادلها، مع إمكانية الوصول إلى أماكن تخزينها و الاستيلاء عليها من طرف مرتكبي الجرائم المعلوماتية، باستعمال وسائل و تقنيات أكثر تطورا و حداثة.

يهدف وضع حد لهذه الجرائم و على إثر تعديل قانون العقوبات، قام المشرع الجزائري باستحداث القانون رقم 04-09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال،² هذا الأخير عرف بدوره عدة نقائص على المستوى العملي، نظرا لصدوره المتأخر مقابل التطور التقني المتسارع الذي أظهر مخاطر جديدة و وسع من مفهومها، هذا الأمر الذي تطلب صدور القانون رقم 04-18 لتدارك النقائص التي شابت القانون السابق، حيث توسع المشرع في توضيح المفاهيم الجديدة المتعلقة بالأمن السيبراني من خلال تعريف المصطلحات التقنية التي أوردها في المادة (10)،³ حتى يكون تطبيق نصوصه أكثر فعالية و مواكبة للمستجدات الحاصلة في ميدان تكنولوجيا الاتصالات، على عكس قانون العقوبات الذي تضمن بصفة عامة الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات و كذا حماية الحياة الخاصة للأفراد، بالإضافة لذلك أراد المشرع من خلال القانون 04-18 تحقيق الأهداف المرجوة من وضع منظومة قانونية جديدة تكون أكثر ضمانا لأمن و سلامة البيانات الشخصية المتبادلة عبر شبكات الاتصالات الإلكترونية، حيث تعددت مظاهر هذه الحماية بين إتخاذ تدابير وقائية أو تقرير عقوبات لمرتكبي الجرائم الإلكترونية باستخدام شبكات الإتصال الإتصالات.

تأسيسا على ما سبق، سنتطرق في (المطلب الأول) إلى الحماية المؤسسية للبيانات الشخصية في القانون 04-18، ثم العقوبات المقرر لحماية البيانات الشخصية في هذا القانون (المطلب الثاني).

¹ أمير فرج يوسف، الجرائم المعلوماتية على شبكة الإنترنت، كلية الحقوق جامعة الفيوم، مراجع قانونية، مصر، 2008، ص 217.

² القانون رقم 04-09 المؤرخ في 05 أوت 2009، المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الإتصال و مكافحتها، ج ر، ع 47، الصادر في 16 أوت 2009.

³ أخذ المشرع بالمفهوم الواسع للأمن السيبراني من خلال التعريف الوارد في الفقرة 3 من المادة (10)، حيث جعله يشمل كل الأدوات و السياسات و مفاهيم الأمن و الآليات الأمنية ... و الضمانات و التكنولوجيا التي يمكن إستخدامها في حماية الإتصالات الإلكترونية ضد أي حدث من شأنه المساس بتوفر و سلامة و سرية البيانات المخزنة أو المعالجة أو المرسلة.

المطلب الأول: الحماية المؤسسية للبيانات الشخصية في قانون 04-18

من مظاهر الحماية القبلية للبيانات الشخصية التي جاء بها هذا القانون هو إنشاء هيئات إدارية تسهر على متابعة ومراقبة مستغلي ومتعاملي شبكات الاتصالات، حيث تضمنت نصوصه جملة من الآليات الوقائية والضوابط القانونية التي ألزم المشرع اتخاذها والعمل بها عند إنشاء واستغلال شبكات الاتصالات الإلكترونية، تحت إشراف ومراقبة سلطة ضبط البريد والاتصالات الإلكترونية، و الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، نتعرض لهذه المهام بشكل من التفصيل في الفرعين التاليين:

الفرع الأول: سلطة ضبط البريد والاتصالات الإلكترونية

أنشأت سلطة الضبط بموجب المادة (11) من هذا القانون التي ورد فيها أنه: "تنشأ سلطة ضبط... تتمتع بالشخصية المعنوية والاستقلال المالي، تدعى بسلطة الضبط..."¹

من بين المهام المسندة إليها في مجال حماية البيانات الإلكترونية نذكر أهمها:

- السهر على متابعة نشاطات متعاملي البريد والاتصالات الإلكترونية، و مراقبة مدى احترامهم للأحكام القانونية والتنظيمية المتعلقة خصوصا بالأمن السيبراني
- السهر على حقوق المشتركين في خدمات الاتصالات الإلكترونية
- وضع إجراءات تحدد كيفية معالجة شكاوى المشتركين
- نشر كل معلومة مفيدة لحماية حقوق المشتركين، و القيام بحملات تحسيسية و توعوية لفائدتهم
- منح التراخيص لإنشاء واستغلال شبكات الاتصالات الإلكترونية، وتراخيص الشبكات الخاصة
- بالإضافة لهذه المهام، و بموجب المادتين (29) و (30) من القانون 04-15 تم تعيين هذه السلطة كسلطة اقتصادية للتصديق الإلكتروني، مكلفة بمتابعة و مراقبة مؤدي خدمات التصديق الإلكتروني الذين يقدمون خدمات التوقيع و التصديق الإلكترونيين لصالح الجمهور.
- باستقراء النصوص السابقة و عند الاطلاع على مختلف المهام الموكلة لهذه السلطة يتضح جليا الطابع الوقائي الذي أضفاه المشرع على أمن شبكات الاتصال، و الحماية القبلية التي يسعى إلى توفيرها للبيانات الشخصية، حيث أوجب أن يخضع نظام إنشاء و استغلال شبكات الاتصالات الإلكترونية وتقديم خدمات الاتصالات الإلكترونية إلى مجموعة من القواعد و الشروط تضمنتها المادة (97)، نذكر أهمها:
- ضمان أمن و سلامة الشبكات الإلكترونية
- إحترام شروط خصوصية البيانات والمعلومات التي يتم إيصالها بواسطة شبكات الاتصالات الإلكترونية

¹ تم إنشاء سلطة الضبط في مجال الاتصالات لأول مرة في الجزائر بموجب القانون رقم 03-2000 تحت تسمية سلطة ضبط البريد والاتصالات السلكية و اللاسلكية.

- احترام شروط حماية الحياة الخاصة للمشاركين والبيانات ذات الطابع الشخصي

- إلزامية احترام الملكية الفكرية وحقوق المؤلف والحقوق المجاورة

كما أكدت المادة (117) على أنه يجب ألا يمس استعمال شبكات وخدمات الاتصالات الإلكترونية بكرامة وحفظ الحياة الخاصة للآخرين.

عند القراءة المتأنية لهذا النص، نلاحظ أن المشرع قد استعمل المفهوم الواسع والأسلوب العام في مخاطبة كل مستعملي ومستغلي الشبكات، علاوة على مقدمي خدمات الاتصالات الإلكترونية، والمقصود بذلك منع كل استعمال غير مشروع للشبكات، سواء كان بغرض الاستفادة من خدمات الشبكات من طرف المشتركين أو بغرض تقديم الخدمات من طرف المتعاملين.

كما نلاحظ تكرار مصطلح "الحياة الخاصة بالآخرين" في كثير من المواد، ما يدل على حرص المشرع و تأكيده على حماية هذا الحق، حيث أراد يشمل حماية الحقوق الأخرى التي تدخل في دائرته من خلال ذكرها، كالحق في سرية المراسلات، حقوق الملكية الفكرية، الحق في سرية البيانات الشخصية... وغيرها وفي إطار متابعة ومراقبة عمل المتعاملين، فقد اشترط حصولهم على رخصة تمنحها سلطة الضبط حتى يتمكنوا من ممارسة نشاطهم وفقا لدفتر شروط خاص بكل نشاط (المادة 123).

مع إلزام المتعاملين و مستخدمهم في المادة (160) بإحترام سرية المراسلات الإلكترونية، وكذا إحترام الحياة الخاصة و المعلومات الإسمية للمشاركين.

لم يكتفي المشرع بمنع المتعاملين من التعرض للبيانات الخاصة بالأشخاص، بل ألزمهم إضافة لذلك بإتخاذ التدابير التي من شأنها أن تضمن سرية المكالمات و المعلومات الشخصية للمشاركين التي يحوزوها المتعاملين، وألا يسمحوا بالإطلاع عليها إلا بإذن مسبق من السلطة القضائية (المادة 119).

وكتدبير إحترازي جاء في المادة (118) أنه في حالة الإستعمال غير المشروع لشبكات و خدمات الإتصالات الإلكترونية، يتم إعلام المتعامل من طرف سلطة الضبط من أجل التدخل الفوري لمنع النفاذ إلى الشبكات، و وقف الإعتداء مباشرة.

الفرع الثاني: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الإتصال و مكافحتها

و لتدعيم مهام و سير عمل هذه السلطة، تمّ إنشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الإتصال و مكافحتها، وذلك بموجب المرسوم الرئاسي رقم 19-172،¹ هي مؤسسة عمومية

¹ المرسوم الرئاسي رقم 19-172 المؤرخ في 06 يونيو 2019، المحدد لتشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الإتصال و مكافحتها وتنظيمها و كفاءات سيرها، ج ر، ع 37، الصادر في 09 يونيو 2019.

ذات طابع إداري تتمتع بالشخصية المعنوية والإستقلال المالي، توضع تحت سلطة وزارة الدفاع الوطني.¹ هيكلها الأساسية هي: مجلس التوجيه والمديرية العامة.

حيث يتشكل مجلس التوجيه من عدة وزراء يرأسه وزير الدفاع الوطني، ومن بين المهام الموكلة لهذا المجلس في مجال حماية البيانات الرقمية والوقاية من جرائم الإتصالات، نذكر أهمها:

- إعداد إستراتيجية وطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال
- التداول حول مسائل التطوير والتعاون مع المؤسسات والهيئات الوطنية المعنية بالجرائم المتصلة بتكنولوجيا الإعلام والإتصال

- التقييم الدوري لحالة التهديد في مجال الجرائم الإلكترونية
- المساهمة في ضبط المعايير القانونية في مجال إختصاص الهيئة²
كما تساعد هذه الهيئة مديرية عامة، تتولى عدة مهام في مجال الأمن المعلوماتي، نذكر أهمها:
- تنشيط وتنسيق ومراقبة عمليات الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال
- تبادل المعلومات مع الهيئات الأجنبية بغرض تجميع كل المعطيات، بتحديد مكان مرتكبي الجرائم الإلكترونية والتعرف عليهم³

تضم المديرية العامة عدة مديريات، أهمها المديرية التقنية المكلفة بمهمة المراقبة الوقائية للإتصالات الإلكترونية، وفي هذا الإطار حددت مهامها أساسا في:

- مساعدة السلطات القضائية ومصالح الشرطة القضائية في إطار مكافحة الجريمة المتصلة بتكنولوجيا الإعلام والإتصال

- جمع وتسجيل وحفظ المعطيات الرقمية وتحديد مصدرها وتتبعها بغرض إستعمالها في الإجراءات القضائية.⁴

¹ المادة (02) من نفس المرسوم، تجدر الإشارة إلى أن هذه الهيئة كانت تحت سلطة وزير العدل في ظل المرسوم الرئاسي رقم 15-261، قبل إلغاء أحكامه بموجب المادة 24 من المرسوم الرئاسي رقم 19-172. لمزيد من التفصيل إطلع على: المرسوم الرئاسي رقم 15-261 المؤرخ في 08 أكتوبر 2015، المحدد لتشكيلة و تنظيم و كفاءات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها، ج ر، ع 53، الصادر في 08 أكتوبر 2015.

² المادة (06) من المرسوم الرئاسي رقم 19-172.

³ المادة (09) من نفس المرسوم.

⁴ المادتين (11) و (12) من نفس المرسوم.

جدير بالذكر أنه بالإضافة لإنشاء هذه الهيئات، في سبيل تشكيل أجهزة وطنية تسهر على تحقيق الأمن السيبراني داخل الجزائر وخارجها، قد تم إنشاء منظومة وطنية لأمن الأنظمة المعلوماتية بموجب المرسوم الرئاسي رقم 05-20¹ حيث تعتبر هذه المنظومة أداة الدولة في مجال أمن الأنظمة المعلوماتية، وتشكل الإطار التنظيمي لإعداد إستراتيجية وطنية لأمن الأنظمة المعلوماتية²، تم إنشاء هذه المنظومة ووضعها لدى وزارة الدفاع الوطني، مكونة من مجلس وطني لأمن الأنظمة المعلوماتية مكلف بإعداد الإستراتيجية الوطنية لأمن الأنظمة المعلوماتية، وتعمل تحت إشراف هذا المجلس وكالة أمن الأنظمة المعلوماتية، مكلفة بتنسيق تنفيذ الاستراتيجية الوطنية لأمن الأنظمة المعلوماتية، كما يساعد المجلس في ممارسة مهامه عدة هيكل من وزارة الدفاع مختصة في هذا المجال³. يتشكل هذا المجلس من عدة وزراء، ويمكن أن يستعين بأي شخص أو مؤسسة من شأنها تنوير أعماله.

المطلب الثاني: الحماية الجزائية للبيانات الشخصية في القانون رقم 04-18

قبل التطرق للحماية الجزائية التي خصها المشرع للبيانات الشخصية في مجال الإتصالات الإلكترونية، تجدر الإشارة إلى أنه عند تعديل قانون العقوبات سنة 2004 بموجب القانون رقم 04-15⁴، قد أدرج المشرع ضمن الفصل الثالث منه القسم السابع مكرر بعنوان: "المساس بأنظمة المعالجة الآلية للمعطيات"⁵، وقد حاول بذلك التصدي لظاهرة الإجرام المعلوماتي من خلال تجريم الأفعال الماسة بنظم المعالجة الآلية للمعطيات، بإعطائها إما وصف الإعتداء على نظم المعالجة الآلية، أو وصف الإعتداء على معطيات أنظمة المعالجة الآلية، كما أعطاها كذلك وصف الإعتداء على سير نظام المعالجة الآلية للمعطيات⁶.

عند إستقراء نصوص هذه المواد يتضح أن المشرع لم يتطرق صراحة إلى الجرائم التي تمس بالبيانات الشخصية ولا شبكات الإتصال التي تنقلها، وإنما جرم كل أنواع الإعتداءات التي تستهدف الأنظمة المعلوماتية والمعطيات التي تحتويها دون تحديد نوعية المعطيات التي تمسها هذه الجرائم، كما أنه لم يحدد المقصود بأنظمة المعالجة الآلية للمعطيات ولم يتطرق إلى الوسائل التي تربطها ببعضها

¹ المرسوم الرئاسي رقم 05-20 المؤرخ في 20 جانفي 2020، يتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية، ج ر، ع 04، الصادر في 26 جانفي 2020.

² المادة (2) من نفس المرسوم.

³ المادة (3) من نفس المرسوم.

⁴ الأمر رقم 66-156 المؤرخ في 08 جوان 1966 المتضمن قانون العقوبات الجزائري، المعدل والمتمّم بالقانون رقم 04-15 المؤرخ في 10 نوفمبر 2004، ج ر، ع 71 سنة 2004.

⁵ تضمن هذا القسم (08) ثمانية مواد من المادة 394 مكرر إلى المادة 394 مكرر 7.

⁶ عيمور راضية عيمور راضية، الجريمة الإلكترونية وآليات مكافحتها في التشريع الجزائري، المجلة الأكاديمية للبحوث القانونية والسياسية، المجلد السادس، العدد الأول، سنة 2022، ص 99.

وهو ما يطرح التساؤل حول إعتبار شبكات الإتصال الإلكترونية ضمن هذه الأنظمة أم لا؟ وهل هي مشمولة بالحماية المقررة في هذا القسم؟

بالإضافة للإشكالات العملية التي تعترض تطبيق هذه النصوص، لاسيما صعوبة إثبات الركن المادي للجريمة في حالة التعدي على البيانات عند انتقالها عبر شبكات الاتصال، لكن مع حرص المشرع على إعداد منظومة قانونية تغطي حماية أكثر للبيانات الشخصية، وجعل النصوص أكثر دقة وملاءمة مع خصوصيات هذه الجرائم، قرر من خلال القانون 04-18 مجموعة من العقوبات لعدم احترام الأحكام القانونية في مجال الإتصالات الإلكترونية، سواء طرف مستغلي أنظمة البريد، او منشئي ومستغلي شبكات الإتصالات الإلكترونية، أو مستغلي أنظمة الإتصالات الإلكترونية، حيث تعددت هذه العقوبات بين إدارية ومالية وعقوبة الحبس، حسب كل حالة.

تحددت هذه الجرائم في الأفعال التي تمس بالبيانات الشخصية عن طريق التعرض للمراسلات والبيانات التي تتضمنها، حيث حاول المشرع التصدي لها من خلال إعطاء وصف لكل فعل مجرم مع تقرير الجزاء المقابل له في الباب الرابع تحت عنوان: "الأحكام الجزائية"

حيث جاء في نص المادة (164) أنه: "يعاقب بالحبس من سنة إلى خمس سنوات، و بغرامة مالية من (500) ألف دج إلى (1) مليون دج، كل شخص ينتهك سرية المراسلات المرسلّة عن طريق البريد أو الإتصالات الإلكترونية أو يفشي مضمونها أو ينشره أو يستعمله دون ترخيص من المرسل أو المرسل إليه أو يخبر بوجودها" كما ورد في المادة (165) أنه: "يعاقب بالحبس من سنة إلى (3) ثلاث سنوات و بغرامة مالية من (1) مليون دج إلى (5) خمس ملايين دج، أو بإحدى العقوبات كل متعامل للبريد يفتح أو يحول أو يخرب البريد، أو يساعد في ارتكاب هذه الأفعال.

وتسري نفس العقوبات على كل متعامل للاتصالات الإلكترونية يحول بأية طريقة كانت المراسلات الصادرة أو المرسلّة أو المستقبلّة عن طريق الاتصالات الإلكترونية، أو يأمر أو يساعد في ارتكاب هذه الأفعال". وبالنسبة للشخص المعنوي فأقرله المشرع المسؤولية الجزائية في إطار الجرائم الواردة في هذا القانون، حسب ما ورد في نص المادة 187، على أن يتم تقدير العقوبة الخاص به إلى نص المادة 18 مكرر من قانون العقوبات.

وتشدد العقوبات على مرتكبي الجرائم السابق ذكرها في حالة العود، طبقا للمادة (188) من ذات القانون. على عكس القانون رقم 04-15 الذي تطرقنا إليه سابقا، يتضح من أحكام هذا الباب المخصص للعقوبات أن المشرع قد استعمل المفاهيم الواسعة في تجريم أفعال الاعتداءات على المراسلات الإلكترونية، وتعمّد صياغة

المصطلحات الشاملة حتى تستطيع هذه النصوص استيعاب أشكال أخرى من الأفعال الإجرامية قد تظهر مع التطور التكنولوجي لاحقا.

كما نلاحظ من خلال هذه النصوص أن إستراتيجية المشرع الجزائري في التصدي لظاهرة الإجرام المعلوماتي في مجال الاتصالات، قد ارتكزت على جملة من القواعد الموضوعية حدد من خلالها الأفعال الماسة بالبيانات الشخصية وما يقابلها من جزاء، سواء تمثلت هذه الأفعال في ممارسة أحد نشاطات استغلال الشبكات الإلكترونية أو إنشائها أو استغلال أنظمة الاتصالات بطرق مخالفة للقانون.

خاتمة:

تبين من خلال هذه الدراسة أن المشرع الجزائري قد عرف تأخرا في تعديل قوانينه ولم يواكب التطورات الحاصلة في مجال النظم المعلوماتية إلا في السنوات الأخيرة، أين عرف تحسنا ملحوظا من خلال جملة التعديلات التي قام بها، حيث إهتدى إلى تعديل قانون العقوبات بتوسيع مفهوم حماية الخصوصية إلى الحماية من الجرائم الإلكترونية، وكذا حماية المعطيات الرقمية ضمن حماية أنظمة المعالجة الآلية للمعطيات، تبع تلك التعديلات باستحداث جملة من القوانين الخاصة، كانت أكثر تجاوبا مع الطبيعة الرقمية لأفعال التعدي على بيانات المتعاملين في البيئة الرقمية، كان أهمها القانون 04-15 الذي خصص منه جزءا مهما لحماية بيانات التوقيع الإلكتروني مع بيانات شهادة التصديق الإلكترونية، لمنع أي تعد عليها أو استعمال غير مشروع لها، وذلك من أجل الحفاظ على مصداقية التوقيع الإلكتروني و تحقيق الهدف من إنشائه، حتى لا يكون عرضة لأعمال الإحتيال أو التلاعب بالهويات المزيفة داخل الفضاء الرقمي، ولكي تكون هذه الحماية كافية تبعها المشرع بتنظيم نشاطات مستغلي و مستعملي شبكات الاتصالات الإلكترونية من خلال القانون 04-18 الذي حدد في جزء منه جزاءات لمخالفي أحكامه، بالنص على معاقبة كل من ارتكب فعل من شأنه المساس بالمراسلات الإلكترونية أو البيانات التي تتضمنها، بغية تحقيق الأمن القانوني و تعزيز الثقة لدى المتعاملين الإلكترونيين،

ومنه توصلنا إلى النتائج التالية:

- أن تزايد حاجة الأفراد لاستخدام شبكات الاتصال الإلكترونية قد أفرز مخاطر جديدة في تطور مستمر وتهديد متزايد لأمن وسلامة البيانات الشخصية.

- استدرك المشرع الجزائري النقص الذي كان يعترى قواعد الحماية التقليدية لممتلكات الأفراد و حقهم في الخصوصية، وقد واكب التطورات التكنولوجية بتكريس حق الخصوصية في قوانين خاصة تضمن حماية بياناتهم الشخصية و سرية مراسلاتهم.

- طوع المشرع مفهوم حماية الحياة الخاصة من الجريمة الإلكترونية، ووسع من دائرة التجريم التي تدخل ضمنها كل الأفعال الماسة بخصوصية الأشخاص وبياناتهم الخاصة، مهما كانت الوسائل المستعملة في ذلك.

- أدرك المشرع الجزائري أهمية البيانات المتعلقة بالتوقيع و التصديق الإلكترونيين التي تعتبر أساس التعامل في البيئة الرقمية، فقرر جملة من التدابير الوقائية والأحكام الجزائية لحمايتها بصدر القانون رقم 04-15، إلا أنه عند تجريم الأفعال الماسة بهذه البيانات يعاب عليه أنه حصرها و حددها في بعض الأشكال فقط، ولم يترك المجال مفتوحا أمام الأفعال الجديدة التي يمكن أن تظهرها التطورات لاحقا.

- لا يمكن أن تتحقق الثقة بين المتعاملين في البيئة الرقمية إلا بتوفر الأمن القانوني، الذي يرتبط بدوره بمدى فعالية النصوص القانونية المنظمة لهذا المجال.

- تفتن المشرع الجزائري للنقائص التي شابت القانون رقم 04-09، و جاء بالقانون رقم 04-18 الذي كان أكثر تفصيلا ووضوحا في التصدي لجرائم الاتصالات الإلكترونية.

- يتضح من نصوص القانون 04-18 الطابع الوقائي، ورغبة المشرع توفير الحماية القبلية للبيانات الرقمية في مجال الاتصالات الإلكترونية من خلال الحماية المؤسسية، ويتجلى ذلك في اتخاذ آليات و تدابير إدارية للتصدي لهذا النوع من الجرائم تحت إشراف و رقابة هيئات عليا في الدولة، خصوصا أنه عبر عنها بمفهوم الاستراتيجية الأمنية.

- أحسن ما فعل المشرع في القانون رقم 04-18، عند تجريمه للأفعال الماسة بالمراسلات الإلكترونية، أنه استعمل الأسلوب العام عند صياغة المواد و توسيع نطاق الأفعال المجرمة، و بالتالي توسع مجال تطبيق النصوص على الأفعال التي يمكن أن تظهر لاحقا.

- أحسن فعلا المشرع عندما فتح النطاق الجغرافي لمكافحة الجرائم المعلوماتية والوقاية منها، وذلك من خلال توسيع مهام الهيئة الوطنية إلى خارج الوطن بتبادل المعلومات مع مثيلاتها الأجنبية، نظرا لطبيعة الجريمة الإلكترونية التي لا تعترف بالحدود الجغرافية؛ لكن تطبيق ذلك يتطلب القيام بالعديد من اتفاقيات التعاون الأمني، على المستوى الإقليمي والدولي.

من خلال هذه النتائج يمكن اقتراح بعض التوصيات نذكرها فيما يلي:

- ضرورة إعداد نصوص قانونية لتنظيم المراقبة الإلكترونية.

- اشتراط توفر تقنيات و تدابير الأمن المعلوماتي في المواقع والمنصات الرقمية، من خلال إلزام أصحابها باتخاذ التدابير الضرورية لذلك.

- التعجيل بتفعيل العمل بالتوقيع والتصديق الإلكترونيين، من أجل وضع حد للتعامل بالهويات المزيفة، وبالتالي إمكانية تتبع آثار الاختراقات والاستعمال غير المشروع لبيانات الغير.
- إعادة النظر في صياغة النصوص المجرمة لأفعال التعدي على بيانات التوقيع والتصديق الإلكترونيين، أو تقرير الإحالة الصريحة إلى المادة (394) وما يليها من قانون العقوبات، كونها أكثر استجابة لمتطلبات حماية البيانات الشخصية.
- توسيع التكوين في الأمن المعلوماتي لكافة فئات المجتمع.
- ضرورة القيام بدورات تحسيسية، للتوعية من مخاطر الجرائم الإلكترونية.
- تفادي التعامل بالمعلومات الشخصية وتقديمها، في المواقع الإلكترونية إلا بعد التأكد من موثوقيتها وأنها تتوفر على مستوى عالي من الأمن الرقمي.

قائمة المصادر والمراجع:

أولا) النصوص القانونية:

- القوانين:

- 1) الأمر رقم 66-156 المؤرخ في 08 جوان 1966 المتضمن قانون العقوبات الجزائري، ج ر، ع 49، المعدل والمتمم بالقانون رقم 04-15 المؤرخ في 10 نوفمبر 2004، ج ر، ع 71 سنة 2004.
- 2) الأمر رقم 75-58 المؤرخ في 26 سبتمبر 1975، المتضمن القانون المدني الجزائري، ج ر، ع 78، المعدل والمتمم بالقانون 05-10 المؤرخ في 20 جوان 2005، ج ر، ع 44، سنة 2005.
- 3) القانون رقم 09-04 المؤرخ في 05 أوت 2018، المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها، ج ر، ع 47، الصادر في 16 أوت 2018.
- 4) القانون رقم 15-04 المؤرخ في 01 فيفري 2015، المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، ج ر، ع 06، الصادر في 10 فيفري 2015.
- 5) القانون رقم 18-04 المؤرخ في 10 ماي 2018، المحدد للقواعد العامة المتعلقة بالبريد والإتصالات الإلكترونية، ج ر، ع 27، الصادر في 13 ماي 2018.

- المراسيم:

- 1) المرسوم الرئاسي رقم 15-261 المؤرخ في 08 أكتوبر 2015، المحدد لتشكيلة وتنظيم وكيفية سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها، ج ر، ع 53، الصادر في 08 أكتوبر 2015.
- 2) المرسوم الرئاسي رقم 19-172 المؤرخ في 06 يونيو 2019، المحدد لتشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها وتنظيمها وكيفية سيرها، ج ر، ع 37، الصادر في 09 يونيو 2019.

الحماية القانونية لبيانات المتعاملين في البيئة الرقمية

3) المرسوم الرئاسي رقم 05-20 المؤرخ في 20 جانفي 2020، يتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية، ج ر، ع 04، الصادر في 26 جانفي 2020.

4) المرسوم التنفيذي رقم 16-134 المؤرخ في 25 أفريل 2016، المحدد لتنظيم المصالح التقنية والإدارية للسلطة الوطنية للتصديق الإلكتروني وسيرها ومهامها، ج ر، ع 26، الصادر في 28 أفريل 2016.

5) المرسوم التنفيذي رقم 16-135 المؤرخ في 25 أفريل 2016، المحدد لطبيعة السلطة الحكومية للتصديق الإلكتروني وتشكيلها وتنظيمها وسيرها، ج ر، ع 26، الصادر في 28 أفريل 2016.

- الكتب:

1) أمير فرج يوسف، الجرائم المعلوماتية على شبكة الإنترنت، كلية الحقوق جامعة الفيوم، مراجع قانونية، مصر، 2008.

2) أبو الهجاء محمد إبراهيم، عقود التجارة الإلكترونية، دار الثقافة للنشر، الأردن، 2011.

3) ثروت عبد الحميد، التوقيع الإلكتروني- ماهيته، مخاطره، وكيفية مواجهتها، دار الجامعة الجديدة، مصر، 2007.

4) خالد ممدوح إبراهيم، الجرائم المعلوماتية، الطبعة الأولى، دار الفكر الجامعي، مصر، 2009.

- الرسائل والمذكرات:

1) حزام فتيحة، الإثبات الإلكتروني في السائل المدنية و التجارية، أطروحة دكتوراه في العلوم القانونية، جامعة الجزائر 1 بن يوسف بن خدة، سنة 2015-2016.

2) باهية فاطمة، آثار قواعد الإثبات الإلكتروني على المراكز القانونية للخصوم (دراسة مقارنة)، أطروحة مقدمة لنيل شهادة الدكتوراه في العلوم القانونية، كلية الحقوق، جامعة الجيلالي اليااس سيدي بلعباس، 2017-2018.

- المقالات:

1) عيمور راضية، الجريمة الإلكترونية وآليات مكافحتها في التشريع الجزائري، المجلة الأكاديمية للبحوث القانونية و السياسية، المجلد السادس، العدد الأول، سنة 2022.