

الآليات القانونية لحماية البيانات الرقمية في بيئة التجارة الإلكترونية Legal Mechanisms to Protect Digital Data in E-Commerce Environment

محمد أمين مهري

كلية الحقوق والعلوم السياسية

مخبر الانتماء : السيادة والعولمة

ma.mehri@univ-medea.dz

عز الدين مبرك

كلية الحقوق والعلوم السياسية

مخبر الانتماء : السيادة والعولمة

mebrek.azedine@univ-medea.dz

الملخص:

نظراً للتطور السريع الذي يشهده العالم في مجال المعلوماتية، باستخدام تكنولوجيا الإعلام والاتصال (TIC)، التي اتسعت من خلالها البيئة الرقمية في شتى المجالات الاجتماعية، الاقتصادية، التجارية وغيرها، وهذا من أجل تسهيل المعاملات وتداول البيانات بين الأفراد والكيانات، ربحاً للوقت وحفاظاً على الجهد واقتصاداً للمال؛ غير أن هذه البيئة الرقمية أصبحت مهددة بالعديد من المخاطر الإلكترونية، التي تستهدف وبشكل خطير المساس بالبيانات الرقمية للأشخاص المتعاملين فيها، مما يستدعي تدخل مختلف الفاعلين في مجال أمن المعلومات لحمايتها، بتطبيق آليات قانونية وتقنية فعّالة. في هذا الصدد تعتبر البيئة الرقمية لعقود لتجارة الإلكترونية، من أكثر البيئات الرقمية عرضة للجرائم الإلكترونية، كونها تُشكل بنوكاً للمعلومات ومستودعات رقمية هامة لدى المورد الإلكتروني، تتضمن بيانات شخصية للمستهلكين الإلكترونيين، كرّس المؤسس الدستوري حمايتها تجسيدا لمبادئ الاتفاقيات الدولية المبرمة بشأن حماية حقوق الإنسان، والتي واكها المشرع الجزائري، من خلال سنّه لنصوص قانونية تهدف إلى حماية المعطيات الشخصية للأشخاص الطبيعيين، لاسيما في بيئة التجارة الإلكترونية، حيث عكف على بذل جهوده لوضع آليات قانونية فعّالة لحماية هذه البيانات وتستجيب للتطورات الحاصلة في البيئة الرقمية.

الكلمات المفتاحية: الأمن المعلوماتي، البيئة الرقمية، العقد التجاري الإلكتروني، المعطيات الرقمية، الجريمة المعلوماتية.

Abstract :

Given the world's rapid development in the field of informatics, by using the TIC, through which the digital environment has expanded in various social, economic, commercial and other fields, and this is in order to facilitate communication and exchange of information between individuals and entities, in order to save time, save effort and save money. However, this digital environment has become threatened by many electronic risks, which seriously target the digital data of the people dealing with it, which necessitates the intervention of various actors in the field of information security to protect it, by applying effective legal and technical mechanisms.

In this regard, the digital environment for decades of electronic commerce is the most vulnerable to cybercrime. As it contains important information banks of the electronic supplier, including personal data of electronic consumers, The Algerian legislator dedicated her protection to the principles of the International Convention for the Protection of Human Rights Law on the Protection of the Personal Data of Natural Persons ", where it was accompanied by Algerian legislators, in the e-commerce environment, where effective legal mechanisms for the protection of such data have been developed and are responsive to developments in the digital environment.

Keywords: Informations Security, Digital Environment, E-commercial Contract, Digital data, Cybercrime.

المؤلف المرسل: عز الدين مبرك .

مقدمة:

أدى التطور العلمي والتكنولوجي السريع، الذي يشهده العالم اليوم في شتى المجالات إلى حدوث تغيير ملحوظ في ممارسة الحياة الاجتماعية، الإقتصادية والمهنية لدى الأفراد والمؤسسات، ففي الشأن التجاري على سبيل المثال، نجد أن بيئة المعاملات التجارية قد تأثرت بهذا الزخم التكنولوجي بشكل مباشر، فأصبحت المعاملات التجارية تمارس إلكترونياً وعن بعد، باستخدام تكنولوجيات الاعلام والاتصال الحديثة، وكذلك الأمر بالنسبة لعقود التجارة الإلكترونية التي أضحت تُبرم في مجلس عقد افتراضي ودون الحضور الفعلي للأطراف.

إن الاستخدام الواسع للوسائل الاتصالات الحديثة، لاسيما في مجال التجارة الإلكترونية، أدى إلى ظهور أسواق إلكترونية مفتوحة لجمهور المستهلكين على المستويين الوطني والدولي، ينشطها الموردون الإلكترونيين من خلال ممارسة نشاطاتهم التجارية بطرق سريعة ومؤمنة، وهذا ما يعزز مبدئي السرعة والإلتزام الذين يعتمدهما القانون التجاري.

بالرجوع للفترة الصحية التي عاشها العالم خلال السنتين الأخيرتين، جراء الوضعية الوبائية التي مست معظم الدول بسبب جائحة كورونا "كوفيد19"، والتي أدت إلى غلق شبه كلي للأسواق والمساحات التجارية التقليدية، كانت سبباً مباشراً لفتح المجال أمام أسواق التجارة الإلكترونية، على المستوى الوطني والدولي، على غرار سوق أمازون (*Amazon*)، سوق علي بابا إكسبرس (*Alibaba*)، أيباي (*Ebay*)، واد كنيس (*Ouedknis*) وجوميا (*Jumia*) بالجزائر.

هذه الأسواق الإلكترونية وغيرها، انتشرت في مختلف أنحاء العالم، لتُمارس فيها مختلف النشاطات التجارية كالإشهار، التسويق، التعاقد، الفوترة، البيع، الدفع الإلكتروني، وذلك بالاعتماد على شبكة الاتصالات الإلكترونية وتقنيات الذكاء الاصطناعي، فخلقت بذلك بيئة رقمية تتضمن قواعد بيانية وبنوكاً للمعلومات، تحتوي كماً هائلاً من المعطيات الشخصية للمستهلكين الإلكترونيين، مما جعلها عرضة للعديد من الجرائم المعلوماتية كالقرصنة، الجوسسة، الإختراق، تحويل المعطيات وغيرها. لهذا بات من الضروري وضع آليات قانونية فعّالة لحماية هذه البيانات من المخاطر المحدقة بها، والتي تؤدي حتماً إلى الإضرار بالأمن الإقتصادي والتجاري للأفراد والمؤسسات. تظهر أهمية هذا الموضوع المتعلق بأمن البيانات الرقمية لعقود التجارة الإلكترونية في مدى فعّالية الآليات المكرّسة لحمايتها ضد الجرائم المرتكبة ضدها، علماً أن هذه البيئة الرقمية أدت إلى انتشار كبير للأسواق الإلكترونية عبر أنحاء العالم وأصبحت تزداد اتساعاً وتطوراً بشكل ملحوظ،

كونها أكثر تنظيماً ورواجاً للسلع والخدمات من الأسواق التقليدية، لاسيما تلك التي يقصدها المستهلكين من مختلف الدول. وفي هذا السياق يمكننا طرح الإشكالية التالية:

هل الآليات القانونية المكرّسة لحماية البيانات الرقمية في عقود التجارة الإلكترونية كافية وفعّالة؟

للإجابة على هذه الإشكالية المطروحة أمامنا بالإثراء والتحليل، إرتأينا إعتقاد المنهج الوصفي، الذي من خلاله نتطرق لدراسة الأحكام القانونية المتعلقة بالبيانات الرقمية لعقود التجارة الإلكترونية ودراسة المخاطر والتهديدات الإلكترونية الماسة بها، ثم نتطرق لدراسة مدى فعّالية الآليات القانونية المكرّسة لحماية هذه البيانات الرقمية وكذا الجهود الوطنية والدولية المبذولة لتحقيق ذلك.

في هذا الإطار إرتأينا تقسيم هذا الموضوع إلى مبحثين رئيسيين؛ سوف نتناول في المبحث الأول الإطار المفاهيمي المتعلق بالبيانات الرقمية لعقود التجارة الإلكترونية والمخاطر المهددة لها، أما في المبحث الثاني فسنتطرق فيه إلى مدى فعّالية الآليات القانونية المكرّسة لحماية هذه البيانات الرقمية من الجرائم المرتكبة ضدها.

1 – الإطار المفاهيمي للبيانات الرقمية في عقود التجارة الإلكترونية

لقد أولى المشرع الجزائري أهمية بالغة لحماية البيانات الرقمية في الفضاءات الإلكترونية، لاسيما منها بيئة التجارة الإلكترونية، وهذا تكريساً لما أفردته المؤسس الدستوري في الفقرة الأخيرة لنص المادة 46 من التعديل الدستوري سنة 2016، التي كرّسها أيضاً بموجب المادة 47 من التعديل الدستوري الأخير سنة 2020¹، وهذا نظراً لأهمية هذه البيانات التي تتضمنها البيئة الرقمية لعقود التجارة الإلكترونية، والتي تندرج ضمن الحقوق الأساسية للأشخاص، المكفولة بموجب القانون.

1 – 1 مفهوم البيانات الرقمية لعقود التجارة الإلكترونية

تناول المؤسس الدستوري حماية البيانات الشخصية للأشخاص الطبيعيين في الفقرة الأخيرة لنص المادة 46 من التعديل الدستوري سنة 2016 كما يلي: "... حماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي حق أساسي يضمنه القانون ويعاقب على انتهاكه"²، كما تناول أيضاً تعريف البيانات الرقمية بموجب أحكام القانون رقم 07-18 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي³، بالإضافة إلى تعريف أطراف العقد التجاري الإلكتروني بموجب القانون رقم 05-18 المتعلق بالتجارة الإلكترونية⁴.

1-1-1 تعريف البيانات الرقمية ذات الطابع الشخصي

تطرق المشرع الجزائري لمفهوم المعطيات ذات الطابع الشخصي بموجب التعريف الوارد في نص المادة 03 من القانون رقم 07-18، المتعلق بحماية الأشخاص الطبيعية في مجال معالجة المعطيات ذات الطابع الشخصي، ذلك بأنها: "كل معلومة بغض النظر عن دعائها، متعلقة بشخص معرّف أو قابل للتعرف عليه والمشار إليه أدناه، "الشخص المعني" بصفة مباشرة أو غير مباشرة، لاسيما بالرجوع إلى رقم التعريف أو عنصر أو عدة عناصر خاصة بهويته البدنية أو الفيزيولوجية أو الجينية أو البيومترية أو النفسية أو الاقتصادية أو الثقافية أو الاجتماعية"⁵.

أما العملية المتعلقة بمعالجة هذه المعطيات ذات الطابع الشخصي فعرفها كما يلي: "كل عملية أو مجموعة عمليات منجزة بطرق أو بوسائل آلية أو بدونها على معطيات ذات طابع شخصي، مثل الجمع أو التسجيل أو التنظيم، أو الحفظ أو الملائمة بشكل آخر من أشكال الإتاحة أو التقريب أو الربط البيني والإغلاق أو التشفير أو المسح أو الإتلاف".

الملاحظ في هذين التعريفين أنهما وردا على سبيل التعميم، بدليل عبارتي "كل معلومة" و "كل عملية"، التي تفيد بأن كل منها وردت على سبيل المثال لا الحصر، وهو الأمر الذي من شأنه إزالة كافة الإشكالات المتعلقة بطبيعة المعطيات الشخصية التي تكون محلاً للحماية، سواءاً كان هذا الشخص طبيعى أو معنوي، وسواءاً كانت معطياته الشخصية اسمية أو عائلية أو مهنية أو مالية. من خلال هذا التعريف القانوني للبيانات الرقمية ذات الطابع الشخصي، بما فيها المتداولة في بيئة التجارة الإلكترونية، يتضح لنا مدى أهمية هذه البيانات الرقمية التي أقرّ المشرع حمايتها، باعتبارها من الحقوق الأساسية التي يضمن القانون حمايتها ويعاقب على المساس بها أو انتهاكها.

1-1-2 تعريف العقد التجاري الإلكتروني وتحديد أطرافه

تناول المشرع الجزائري مفهوم العقد التجاري الإلكتروني بموجب التعريف الوارد في نص المادة 06 من القانون رقم 05-18، المتعلق بالتجارة الإلكترونية كما يلي: "العقد بمفهوم القانون رقم 02-04، الذي يحدد القواعد المطبقة على الممارسات التجارية، ويتم إبرامه عن بُعد دون الحضور الفعلي والمتزامن لأطرافه، باللجوء لتقنيات الإتصال الإلكتروني"⁶.

أما أطراف العقد الإلكتروني المتمثلة في المستهلك والمورد الإلكترونيين، فعرفهما المشرع الجزائري بموجب نفس المادة كما يلي:

أولاً: تعريف المستهلك الإلكتروني: "كل شخص طبيعى أو معنوي يقتني بعوض أو بصفة مجانية سلعة أو خدمه عن طريق الاتصالات الإلكترونية من المورد الإلكتروني بغرض الاستخدام النهائي"⁷.

ثانياً: تعريف المورد الإلكتروني: " كل شخص طبيعي أو معنوي يقوم بتسويق أو إقتراح توفير السلع والخدمات عن طريق الإتصالات الإلكترونية"⁸.

بتحديد المشرع للمفاهيم المتعلقة بالبيانات الرقمية ذات الطابع الشخصي وكذا تعريفه للعقد التجاري الإلكتروني وتحديد أطرافه المتمثلة في كل من المستهلك والمورد الإلكترونيين، يكون بذلك قد ضبط المصطلحات القانونية المتعلقة بالبيئة الرقمية لعقود التجارة الإلكترونية، حتى يتسنى له تحديد الجرائم الإلكترونية الماسة بها ومكافحتها، عن طريق الآليات القانونية المقررة لحماية البيانات في البيئة الرقمية.

1 - 2 المخاطر الإلكترونية الماسة بالبيانات الرقمية لعقود التجارة الإلكترونية

تتعدد المخاطر الإلكترونية الماسة بالبيانات الرقمية لعقود التجارة الإلكترونية، بحسب طبيعتها وطُرق ارتكابها وصفة مرتكبها، فمنها ما يتعلق بإخلال المورد الإلكتروني بالتزاماته التعاقدية تجاه المستهلك الإلكتروني ومنها ما يتعلق بالجرائم الإلكترونية المرتكبة من طرف الغير في بيئة التجارة الإلكترونية.

1 - 2 - 1 المخاطر الناتجة عن إخلال المورد الإلكتروني بالتزاماته التعاقدية تجاه المستهلك

سنّ المشرع الجزائري جُملة من الالتزامات القانونية على المورد الإلكتروني، تناولها بموجب القانون رقم 05-18 المتعلق بالتجارة الإلكترونية، وذلك قصد حماية البيانات الشخصية للمستهلكين الإلكترونيين، التي تتضمنها قواعد البيانات لديه، والناتجة على إثر المعاملات الإلكترونية التي تتم بينهما في البيئة الرقمية التجارية، حيث تُوزع هذه الالتزامات عبر مختلف مرحلتين للتعاقد الإلكتروني.

أولاً: مرحلة ما قبل إبرام العقد:

يجب على المورد الإلكتروني أن يلتزم بتقديم عروضه التجارية إلكترونياً للمستهلك، دون غش أو تضليل أو تدليس، بحيث يجب أن يكون هذا الإعلان المخصص للعروض المقدمة من طرفه بطريقة مرئية، مقروءة ومفهومة ومتضمنة لمختلف المعلومات المتعلقة بخصائص ومميزات السلع أو الخدمات المعروضة وكذا أسعارها، إلى جانب تقديم المورد الإلكتروني لجميع بياناته المهنية⁹.

كما يجب أن توثق هذه المعاملة التجارية بمختلف تفاصيلها في عقد تجاري إلكتروني، يصادق عليه المستهلك الإلكتروني وفقاً لمبدأ سلطان الإرادة، وهذا من أجل حمايته من الإشهارات الإلكترونية المضللة وتفاديه لجميع المناورات التدليسية التي قد تنجم عن تصرفات المورد الإلكتروني، طبقاً لما ورد في نص المادة 10 من القانون رقم 05-18.

ثانياً: مرحلة إبرام العقد الإلكتروني وتنفيذه:

بعد تحقق رضا المستهلك الإلكتروني وقبوله للعرض التجاري المقدم من طرف المورد الإلكتروني، يخضع هذا الأخير للالتزامات التي تضمنتها المادة 11 من نفس القانون، والتي تتعلق بشروط إبرام العقد الإلكتروني، الذي يشترط فيه أن يتضمن كافة البيانات الشخصية والمهنية المتعلقة بالعمليّة التجارية، وكذا وجوب احترامه لحق المستهلك في العدول عن اقتناء السلعة أو الخدمة المعروضة عليه، طبقاً لما ورد في نص المادة 22 من نفس القانون.

كما يلتزم المورد الإلكتروني أيضاً بتأمين البيانات الشخصية للمستهلكين الإلكترونيين طبقاً للمادة 26 من نفس القانون، الوارد نصها كما يلي:

" ينبغي للمورد الإلكتروني الذي يقوم بجمع المعطيات ذات الطابع الشخصي ويشكل ملفات الزبائن والزبائن المحتملين ألا يجمع إلا البيانات الضرورية لإبرام المعاملات التجارية".

كما يجب عليه أيضاً أن يحصل على موافقة المستهلكين الإلكترونيين قبل أن يجمع بياناتهم الشخصية وأن يضمن لهم أمن نظم المعلومات وسرية البيانات المتداولة في بيئة المعاملات التجارية ذات الطابع الإلكتروني، وبذلك يكون المورد قد التزم بالأحكام القانونية المعمول بها في هذا المجال¹⁰.

بناءً على ما سبق، نستنتج أن المشرع بفرضه لهذه الالتزامات القانونية على المورد الإلكتروني، يستهدف حماية البيانات الشخصية للمستهلك الإلكتروني، باعتباره طرف ضعيف في العلاقة العقدية، وكذا ضمان نزاهة وشفافية الممارسات التجارية ذات الطابع الإلكتروني.

1 - 2 - الجرائم الإلكترونية الماسة بالبيانات الرقمية في بيئة التجارة الإلكترونية

اهتم المؤسس الدستوري بحماية البيانات الشخصية، نظراً لخطورة الجرائم الإلكترونية المرتكبة ضدها، ومدى إضرارها بالأفراد والمؤسسات، حيث اعتبرها من الحقوق الأساسية المكفولة بموجب القانون، والتي يعاقب على انتهاكها طبقاً لنص المادة 47 من التعديل الدستوري لسنة 2020.

بالرجوع للمشرع الجزائري، وبعد الفراغ الذي عرفته منظومته القانونية في مجال حماية المعطيات ذات الطابع الشخصي، وعلى غرار باقي التشريعات المقارنة عكف على إعداد نصوص قانونية كفيلة بحماية البيانات ذات الطابع الشخصي من الجرائم الماسة بها ومكافحتها، فسنّ القانون رقم 07-18، الذي يكفل حماية البيانات الشخصية للأشخاص الطبيعيين من المخاطر الإلكترونية الماسة بها، والتي نذكر منها ما يلي¹¹:

- الجوسسة الإلكترونية،

- الترصّد الإلكتروني،
 - الاختراق والقرصنة للمعطيات،
 - تحويل المعطيات الشخصية وانتحال الصفة،
 - جمع البيانات دون إذن أو ترخيص مسبق،
 - الدخول غير المشروع للنظم المعلوماتية والمعالجة غير المشروعة للبيانات الشخصية،
- ناهيك عن صعوبة أو ربما استحالة إرجاع الحال لما كان عليه قبل وقوع الخطر.

هذه الجرائم الإلكترونية الواردة على سبيل المثال، كانت سببا مباشراً لاهتمام المشرع الجزائري بصياغة نصوص قانونية، يستهدف من ورائها تحقيق الأمن السيبراني للبيئة الرقمية، لاسيما منها ذات الطابع التجاري، وحمايتها من المخاطر التي يمكن أن تتعرض لها، بالإضافة إلى خلق آليات ووسائل قانونية وتقنية تستجيب لمتطلبات البيئة الرقمية والتطورات الحاصلة في بيئة التجارة الإلكترونية.

2 - فعالية الحماية القانونية للبيانات الرقمية في عقود التجارة الإلكترونية

يقتضي الأمن المعلوماتي للبيئة الرقمية بذل جهود لخلق آليات قانونية، تكون كفيلة بتحقيق حماية مدنية وجزائية فعالة لبيئة التجارة الإلكترونية، وكذا إنشاء أجهزة وهيئات ذات بعد وطني ودولي، مختصة في أمن وحماية البيانات الرقمية من الجرائم المعلوماتية المرتكبة ضدها.

2 - 1 إجراءات الحماية المدنية والجزائية للبيانات الرقمية في عقود التجارة الإلكترونية

بالرجوع لأحكام الشريعة العامة المتعلقة بحماية حقوق المستهلك، لاسيما منها الواردة في عقود التجارة الإلكترونية، نجد بأن المشرع الجزائري قد وضع جملة من الاجراءات القانونية ذات الطابع المدني والجزائي، يستهدف من خلالها إرساء قواعد المسؤولية المدنية والجزائية على المورد الإلكتروني، باعتباره مسؤولاً عن الأضرار الناجمة عن إخلاله بالتزاماته المهنية، التي أدت إلى الإضرار بالبيانات الشخصية للمستهلك الإلكتروني.

2 - 1 - 1 إجراءات الحماية المدنية للبيانات الرقمية في عقود التجارة الإلكترونية

إلى جانب الأحكام العامة المتعلقة بحماية حقوق المستهلك أثناء التعاقد، كرّس المشرع حماية بياناته الشخصية في عقود التجارة الإلكترونية بموجب القانون رقم 05-18، كونه يُعتبر طرف ضعيف في بيئة التجارة الإلكترونية، بالتالي مكنه القانون من الدفاع عن حقوقه الشخصية عن طريق رفع دعوى أمام القضاء المدني للمطالبة بإبطال العقد الإلكتروني والتعويض عن الضرر الذي لحق به جراء المساس بمعطياته الشخصية في البيئة الرقمية.

أولاً: حق المستهلك المتضرر في المطالبة بإبطال العقد الإلكتروني:

تكريساً لحماية حقوق المستهلك في بيئة التجارة الإلكترونية، مكنّ المشرع هذا الأخير من الدفاع عن حقوقه الشخصية أمام القاضي المدني، عن طريق رفع دعوى إبطال العقد الإلكتروني، طبقاً لما ورد في نص المادة 14 من القانون رقم 05-18، لاسيما في حالة عدم احترام المورد الإلكتروني لأحكام المادة 10، التي تنص على وجوب توثيق المعاملة الإلكترونية من قبل المورد الإلكتروني، بموجب عقد إلكتروني مصادق عليه من طرف المستهلك الإلكتروني، بالإضافة إلى ما ورد في أحكام المادة 13 التي تنص على ضمان أمن وسريّة هذه المعاملة الإلكترونية من قبل المورد الإلكتروني¹².

ثانياً: حق المستهلك المتضرر في المطالبة بالتعويض جراء المساس بمعطياته الشخصية:

بالرجوع لأحكام المادة 26 من القانون رقم 05-18، فإنه يحق للمستهلك الإلكتروني المتضرر، المطالبة بالتعويض عن الأضرار التي لحقت به جراء المساس بمعطياته الشخصية التي تضمنها العقد التجاري الإلكتروني¹³، وذلك بسبب إخلال المورد الإلكتروني بالتزاماته التعاقدية ذات الطابع الإلكتروني، التي أفردتها المشرع على النحو التالي:

- إلزام المورد الإلكتروني بإعلام المستهلك الإلكتروني بتجميع بياناته الشخصية الضرورية وحمايتها،
- الحصول على موافقة المستهلك الإلكتروني المتعاقد معه قبل جمع بياناته الشخصية ومعالجتها،
- إنشاء المورد الإلكتروني لملفات إلكترونية (بنك معلومات) للزبائن وحمايتها من المخاطر الماسة بها،
- الإلتزام بضمان أمن وسريّة البيانات الرقمية المتعلقة بالعقود الإلكترونية المبرمة مع المستهلكين.

2 - 1 - 2 إجراءات الحماية الجزائية للبيانات الرقمية في عقود التجارة الإلكترونية

تقتضي أهمية البيانات الرقمية في بيئة التجارة الإلكترونية ضرورة وضع قواعد إجرائية ذات طابع جزائي، كفيلة بردع الجرائم الماسة بها، سواءً كانت صادرة من طرف المورد الإلكتروني باعتباره طرف قوي في البيئة الرقمية لعقود التجارة الإلكترونية أو كانت صادرة من طرف الغير. بناءً على هذا الأساس، أقرّ المشرع الجزائري عقوبات جزائية، أصلية وتكميلية ضد كل مورد إلكتروني أخلّ بالتزاماته المهنية المنصوص عنها في قانون التجارة الإلكترونية، وألحق ضرراً بالمستهلك الإلكتروني جراء المساس بمعطياته الشخصية، حيث تمثلت هذه العقوبات فيما يلي:

أولاً: العقوبات الأصلية المقررة ضد الجرائم المرتكبة في البيئة الرقمية للتجارة الإلكترونية:

إلى جانب العقوبات المنصوص عليها في القسم السابع مكرر من قانون العقوبات الجزائري، أقرّ المشرع عقوبات أصلية تضمنتها القوانين المتعلقة بالتجارة الإلكترونية وحماية المعطيات ذات الطابع الشخصي، حيث يعتبر كل مساس بالبيانات الشخصية للمستهلك الإلكتروني سواءً كان ذلك بخرق قواعد البيانات المحفوظة لدى المورد الإلكتروني أو بالتجسس عنها أو قرصنتها أو تقليدها أو إتلافها، فإن ذلك يؤدي إلى قيام المسؤولية الجزائية على مرتكب الجريمة، طبقاً للأحكام القانونية والتنظيمية المعمول بها في هذا المجال، والتي تنص على ضمان أمن نظم المعلومات وسرية البيانات.

على هذا الأساس وطبقاً لأحكام القانون رقم 07-18، فإن المشرع قسّم الجرائم الماسة بالبيئة الرقمية إلى قسمين، يشمل القسم الأول جرائم متعلقة بجمع ومعالجة المعطيات الشخصية بطرق غير مشروعة، أما القسم الثاني فيشمل جرائم تتعلق بسوء الاستعمال أو الاستغلال غير المشروع للمعطيات الشخصية.

1- الجرائم المتعلقة بجمع ومعالجة المعطيات ذات الطابع الشخصي بطرق غير مشروعة

بالرجوع لأحكام المادتين 57، 59 من القانون رقم 17-18، فإن الجرائم المتعلقة بجمع ومعالجة المعطيات ذات الطابع الشخصي بطرق غير مشروعة تتمثل في:

- معالجة معطيات شخصية دون الموافقة الصريحة للشخص المعني بها،
- جمع معطيات شخصية بطريقة تدليسية أو غير نزيهة أو غير مشروعة.

وطبقاً لأحكام هاتين المادتين، فإن العقوبة المقررة للجريمة المنصوص عنها في المادة 57 من نفس القانون، فتتمثل في الحبس من سنتين (02) إلى خمسة (05) سنوات وبغرامة مالية من 200,000 إلى 500,000 دج، أما بالنسبة للعقوبة المقررة للجريمة المنصوص عنها في المادة 59، فتتمثل في الحبس من سنة واحدة (01) إلى ثلاثة (03) سنوات وبغرامة مالية من 100,000 إلى 300,000 دج.

2- الجرائم المتعلقة بسوء الإستعمال أو الاستغلال غير المشروع للمعطيات الشخصية

بالرجوع لأحكام المواد 58، 60، 62 و67، فإن هذه الجرائم الإلكترونية تتمثل في:

- القيام بإنجاز أو استعمال المعطيات لأغراض أخرى غير تلك المصرح بها،
- السماح لأشخاص غير مؤهلين بالولوج للمعطيات ذات الطابع الشخصي،
- إفشاء معطيات محمية وذات طابع شخصي،

- نقل معطيات ذات طابع شخصي نحو دولة أجنبية دون ترخيص من السلطة الوطنية المكلفة بحماية المعطيات ذات الطابع الشخصي¹⁴.
وطبقاً لما ورد في أحكام المواد المذكورة أعلاه، فإن العقوبات المقررة على هذه الجرائم، تتمثل في:
- بالنسبة لجريمة القيام بإنجاز أو استعمال المعطيات لأغراض أخرى غير تلك المصرح بها فإن العقوبة المقررة لها تتمثل في الحبس من ستة (6) أشهر إلى واحد (1) سنة والغرامة من 60.000 إلى 100.000 دج.
- بالنسبة لجريمة السماح لأشخاص غير مؤهلين بالولوج للمعطيات ذات الطابع الشخصي، فإن العقوبة المقررة لها تتمثل في الحبس من سنتين (2) إلى خمسة (5) سنوات والغرامة من 200.000 إلى 500.000 دج.
- بالنسبة لجريمة إفشاء معطيات محمية وذات طابع شخصي، فإن الشخص المعني بها يعاقب بالعقوبات المنصوص عنها في المادة 301 من قانون العقوبات.
- بالنسبة لجريمة نقل معطيات ذات طابع شخصي نحو دولة أجنبية دون ترخيص من السلطة الوطنية المكلفة بحماية المعطيات ذات الطابع الشخصي، فإن العقوبة المقررة لها تتمثل في الحبس من سنة (1) إلى خمسة (5) سنوات والغرامة من 500.000 إلى 1000.000 دج.

ثانياً: عقوبات تكميلية مقررة على الجرائم المعلوماتية الماسة بالبيانات الرقمية

بالرجوع لنص المادة 46 من القانون رقم 07-18، فإن المشرع قد خول للسلطة الوطنية المكلفة بحماية المعطيات ذات الطابع الشخصي، اتخاذ كافة الإجراءات العاقبية ذات الطابع الإداري، ضد كل شخص مسؤول عن هذه المعطيات، ما لم يلتزم بضمان حمايتها أو تسبب في خرقها أو قرصنتها أو إستعمالها غير المشروع، وبذلك يكون معرض لعقوبات تكميلية، تتمثل في: الإنذار، الإعذار، السحب المؤقت للتصريح، السحب النهائي للترخيص وتعليق ممارسة النشاط التجاري.

هذه العقوبات التكميلية تُعد قرارات إدارية تأديبية، قابلة للطعن أمام مجلس الدولة وفقاً لأحكام التشريع الساري المفعول¹⁵.

2 - 2 الجهود المبذولة لتكريس حماية البيانات الرقمية في عقود التجارة الإلكترونية

بالرغم من وجود ترسانة من النصوص القانونية الخاصة بحماية البيانات الشخصية في البيئة الرقمية، إلا أنها تبقى غير كافية وبدون فعالية بسبب صعوبة تطبيقها في البيئة الرقمية المتطورة، لاسيما في ظل التنامي السريع والمستمر للجرائم المعلوماتية، مما استدعى تظافر جهود

الدول للتصدي لها عن طريق إبرام إتفاقيات دولية لحماية هذه البيانات في البيئة الرقمية، وكذا إنشاء أجهزة وهيئات دولية ووطنية كفيلة بالتصدي لهذه الجرائم المعلوماتية ومكافحتها.

2 - 2 - 1 الإتفاقيات الدولية المبرمة بشأن حماية البيانات الشخصية في البيئة الرقمية

نظراً للانتشار المتنامي للجرائم الإلكترونية وارتفاع معدلات خطورتها، التي تجاوزت حدود السيطرة، بات من الضروري على الدول بناء جسور التعاون فيما بينها لخلق آليات كفيلة بحماية البيانات الشخصية في الفضاء السيبراني؛ وفي هذا الصدد عُقدت عدة إتفاقيات دولية لمكافحة الجرائم المنظمة، ومن بينها الجريمة المعلوماتية المرتكبة في البيئة الرقمية، ومن بين هذه الإتفاقيات نذكر:

(1) مؤتمر فيينا حول التعاون الأمني الدولي لمكافحة الجريمة المنظمة: انعقد بفيينا في أبريل سنة 1923، وكان من أهم مخرجاته، إنشاء ما سميَّ حينها «اللجنة الدولية للشرطة الجنائية»، التي انحصرت مهامها في التنسيق بين الأجهزة الأمنية للدول الأوروبية، لكن ما لبثت أن توقفت عن ممارسة نشاطاتها بسبب اندلاع الحرب العالمية الثانية سنة 1939، ليُعاد إحيائها من جديد، خلال المؤتمر الدولي الذي انعقد في فيينا بالنمسا ما بين السادس والتاسع من شهر يونيو سنة 1946، حيث اتفق المشاركون في هذا المؤتمر وكانوا يمثلون سبع عشرة دولة، على تأسيس المنظمة الدولية للشرطة الجنائية (INTERPOL) بديلاً عن اللجنة الدولية للشرطة الجنائية سالفة الذكر، ويتمثل دورها في تبادل أعضاء منظمة (الأنتربول)، المعلومات عن المجرمين، المبحوث عنهم دولياً، ويتعاونون فيما بينهم لمكافحة الجرائم المنظمة والعابرة للحدود، مثل جرائم التهريب وعمليات المتاجرة غير المشروعة للأسلحة والجريمة المعلوماتية والدعارة والإرهاب وغيرها¹⁶.

مؤتمر المجلس الأوروبي: انعقد في لكسمبورغ سنة 1991، والذي أنشأت بموجبه شرطة الاتحاد الأوروبي (EUROPOL)، لمكافحة الجرائم المنظمة، ومنها الجرائم المعلوماتية المرتكبة ضد المعطيات الشخصية، وملاحقة مرتكبيها ومعاقبتهم.

(2) اتفاقية التعاون لدول الخليج: المنعقدة سنة 1994 والتي تهدف إلى مكافحة الجرائم المنظمة العابرة للحدود، بما في ذلك الجريمة المعلوماتية الماسة بالبيانات الشخصية في البيئة الرقمية ومتابعة مرتكبيها وتسليمهم لمعاقبتهم.

3) مؤتمر مجلس الوزراء العرب : انعقد في القاهرة سنة 1995 والذي تم على إثره إبرام الاتفاقية العربية لمكافحة جرائم تقنيات المعلومات، وإنشاء لجنة مكافحة الجرائم المُستجدة، وهي لجنة مكونة من خبراء ومختصين في مجال القانون وتكنولوجيا المعلوماتية، حيث تُعد هذه الأخيرة تقاريرها السنوية حول الجرائم المستحدثة والمنظمة والعابرة للحدود في الدول العربية.

4) إتفاقية بودابست (المجر): تم إنعقادها في عاصمة المجر خلال الفترة 08-23 نوفمبر 2001، دخلت حيز النفاذ في جويلية 2004، حيث تُعد من أهم الإتفاقيات الدولية لمكافحة الجرائم الإلكترونية وخاصة جرائم الإنترنت، كونها تضمنت بالتحديد أنواع الجرائم الإلكترونية الماسة بالبيانات الشخصية كالإختراق الإلكتروني، الإرهاب الإلكتروني، تزوير بطاقات الإئتمان، الدعارة الإلكترونية، القرصنة والترصّد الإلكتروني وغيرها من الجرائم المعلوماتية الماسة بالفضاءات الرقمية¹⁷.

5) الاتفاقية العربية لمكافحة جرائم تقنيات المعلومات: تم ابرامها في مؤتمر مجلس الوزراء العرب المنعقد بالقاهرة بتاريخ 21 ديسمبر سنة 2010، تم من خلاله التطرق إلى السُبل الفعّالة لمكافحة الجريمة المعلوماتية، ومتابعة مرتكبيها.

صادقت الجزائر على هذه الاتفاقية بموجب مرسوم رئاسي رقم 14-252، مؤرخ في 08 سبتمبر 2014، المتضمن لتصديق رئيس الجمهورية على هذه الاتفاقية¹⁸.

6) اتفاقية الاتحاد الإفريقي في مجال الأمن السيبراني وحماية البيانات الشخصية: تم ابرامها في شهر جوان سنة 2014، خلال مؤتمر رؤساء الاتحاد الإفريقي، أين غطت نطاق واسع جدًا من المعاملات والأنشطة الرقمية إلى جانب مكافحة جرائم القرصنة، الإرهاب الإلكتروني، الدعارة الإلكترونية، خطابات الكراهية وغيرها، بالإضافة إلى إنشاء جهاز الأفريبول (AFRIPOL) بالجزائر في 13 ديسمبر 2015 والذي يتشكل من قوات الأمن الوطني لـ 41 دولة إفريقية، حيث يُعد أكبر منظمة أمنية للشرطة في القارة الإفريقية، يكلف بمكافحة الجريمة المنظمة والعابرة للحدود.

2 - 2 - 2 الأجهزة والهيئات المتخصصة في حماية البيانات الشخصية في البيئة الرقمية
تنفيذاً لأحكام الإتفاقيات الدولية والإقليمية بشأن مكافحة الجرائم المنظمة والعابرة للحدود، بما في ذلك الجرائم الإلكترونية الماسة بالمعطيات الشخصية المتعلقة ببيئة التجارة الإلكترونية، التي تقتضي تظافر جهود الجميع لإنشاء أجهزة وهيئات كفيلة بحمايتها من المخاطر والتهديدات الماسة بها.

أولاً: الهيئات الدولية المكلفة بحماية البيانات الشخصية في البيئة الرقمية

تكريساً لجهود التعاون الدولي في مجال حماية البيانات الرقمية ذات الطابع الشخصي، وتنفيذاً لمبادئ الاتفاقيات الدولية المبرمة في ذات الشأن، تم إنشاء العديد من الأجهزة والهيئات الأمنية والإدارية، الاستشارية والرقابية ذات الطابع الوقائي والردعي على المستويين الدولي والوطني، نذكر منها ما يلي:

1) مركز التبليغ عن الشكاوي الخاصة بجرائم الإنترنت *Internet_Crime_Complaint_Center*

يعد مركز التبليغ عن شكاوي الأشخاص المتضررين من الجرائم السيبرانية (IC3)، هيئة إدارية ذات طابع رقابي، أنشأت بالولايات المتحدة الأمريكية سنة 1998، نتيجة الإرتفاع الكبير في نسبة الجرائم المعلوماتية التي مست مختلف المجالات الاقتصادية، الاجتماعية، التجارية وغيرها، مع عدم وجود أية جهة يمكن المتضررين اللجوء إليها لتقديم شكاويهم آنذاك.

يتشكل المركز من أعضاء المكتب الفيدرالي للتحقيقات (FBI)، كما يستند في ممارسة مهامه على المكتب الأمريكي للتفتيش البريدي « *Postal Inspection Service* » المكلف بالتحقيق والتحري في الجرائم الماسة بالمعطيات الشخصية للزبائن لدى البريد والاتصالات الإلكترونية¹⁹.

2) الوكالة الوطنية لأمن نظم المعلومات: *National Information Systems Security Agency*

هي هيئة وطنية مختصة في أمن المعلومات ومراقبتها، كما تختص أيضاً في تصميم الشبكات الإلكترونية الخاصة والمحصنة من الاختراقات "VPN"، "VLAN" و "VSAT"، تم إنشائها بالولايات المتحدة الأمريكية سنة 2009، وألحقت بالأمانة العامة للدفاع والأمن القومي "SGDSN"، حيث تعتبر سلطة وطنية مكلفة بمساعدة رئيس الوزراء فيما يتعلق بالأمن القومي ومكافحة الجرائم المعلوماتية العابرة للحدود، كما تعمل على تلبية حاجيات السلطات العامة في الدولة، المتعلقة بمكافحة جرائم المعلوماتية.

3) وحدة مبادرات جرائم الإنترنت: *Internet_Crime_Initiatives_Unit*

هي هيئة وطنية مختصة في أمن المعلومات ومكافحة الجرائم الإلكترونية عبر الإنترنت، تابعة لمركز الشكاوي الخاصة بجرائم الإنترنت "IC3"؛ أنشأت في بنسلفانيا بالولايات المتحدة الأمريكية سنة 2010، وتقوم بالتعاون مع الشرطة الجنائية الدولية (الأنتربول) للبحث والتحري عن الجرائم الإلكترونية المرتكبة ضد الأفراد والمؤسسات على المستوى الدولي²⁰.

بالإضافة إلى ذلك، تم خلق العديد من الأجهزة الدولية والإقليمية، المكلفة بأمن المعلومات ومكافحة الجرائم المنظمة، نذكر منها الشرطة الجنائية الدولية (*INTERPOL*)، مكتب الشرطة الإفريقية (*AFRIPOL*) وشرطة الاتحاد الأوروبي (*EUROPOL*)، حيث أصبحت كلها تلعب دورًا هامًا في مكافحة الجرائم المنظمة، ولاسيما منها الجرائم الإلكترونية الماسة بالبيانات الشخصية²¹.

ثانياً: الأجهزة والهيئات الوطنية المكلفة بحماية البيانات الرقمية في التشريع الجزائري

أولى المشرع الجزائري أهمية بالغة لحماية المعطيات ذات الطابع الشخصي، بما في ذلك البيانات الرقمية لعقود التجارة الإلكترونية، من خلال إنشائه لأجهزة متخصصة في حماية الفضاءات الرقمية، تضم تشكيلة بشرية مكونة في أعلى المستويات، تشمل محققين وخبراء من نوع خاص، تجتمع فيهم صفة الضبطية القضائية بالإضافة إلى اكتسابهم للخبرة الواسعة في مجال النظم المعلوماتية وأمن البيانات الرقمية²².

تجلت هذه الأهمية في إنشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها بموجب القانون رقم 04-09، التي تعمل إلى جانب السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي التي تم إنشائها بموجب القانون رقم 07-18، بالإضافة إلى جهاز الشرطة القضائية، الذي يعمل إلى جانب الوحدات التابعة لأسلاك الأمن الوطني، الدرك الوطني، دائرة الاستعلام العسكري، وكذا رجال القضاء.

1- الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها

أنشئت هذه الهيئة الوطنية بموجب المادة 13 من القانون رقم 04-09، المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، باعتبارها سلطة إدارية مستقلة توضع لدى الوزير المكلف بالعدل، وتمارس مهامها تحت رقابة السلطة القضائية ممثلة في كل من وكيل الجمهورية، قاضي التحقيق، غرفة الاتهام وقضاة الحكم²³.

أحال المشرع تنظيم الهيئة وتحديد تشكيلتها وكيفية سيرها، للتنظيم الصادر بموجب المرسوم الرئاسي رقم 15-261،²⁴ ووفقاً لأحكام قانون الإجراءات الجزائية تضم الهيئة مديريات ومراكز وملحقات جهوية أمنية وتقنية، مُشكّلة من قضاة وضباط وأعوان أمن من الشرطة القضائية، تابعين لمصالح الاستعلام العسكرية والدرك والأمن الوطني، وتعمل الهيئة على تجميع وتسجيل وحفظ المعطيات الشخصية للأفراد وتحديد مصدرها ومسارها، من أجل استعمالها في الإجراءات القضائية المتبعة للكشف عن الجرائم المعلوماتية المنصوص عليها في قانون العقوبات²⁵.

2- السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي

تضمن نص المادة 22 من القانون رقم 07-18، إنشاء السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي، التي تعتبر سلطة إدارية مختصة، تتمتع بالشخصية المعنوية والاستقلال المالي، تخضع لرئيس الجمهورية، تتشكل من 16 عضو طبقاً لنص المادة 23.

طبقاً لنص المادة 25، تتمثل المهام الأساسية للهيئة فيما يلي:

- منح التراخيص وتلقي التصريحات المتعلقة بمعالجة المعطيات ذات الطابع الشخصي،
- تقديم إستشارات للأشخاص والكيانات التي تلجأ لمعالجة البيانات ذات الطابع الشخصي،
- الترخيص بنقل المعطيات الشخصية نحو الخارج، وفق شروط منصوص عليها في القانون،
- تلقي الإحتجاجات والطعون والشكاوي بخصوص معالجة المعطيات وإعلام أصحابها،
- نشر التراخيص الممنوحة في السجل الوطني لحماية المعطيات ذات الطابع الشخصي،
- تطوير علاقات التعاون مع الأجهزة والهيئات الأجنبية المماثلة مع مراعاة المعاملة بالمثل،
- إصدار عقوبات إدارية تأديبية وفقاً لأحكام هذا القانون،
- وضع معايير في مجال حماية المعطيات ذات الطابع الشخصي،
- وضع قواعد السلوك والأخلاقيات التي تخضع لها معالجة المعطيات ذات الطابع الشخصي،
- المحافظة على الطابع السري لمعالجة البيانات الشخصية، لاسيما في عقود التجارة الإلكترونية،
- تقديم أي إقتراح من شأنه تحسين الإطار التشريعي والتنظيمي لمعالجة المعطيات الشخصية²⁶.

3- الوحدات التابعة لسلوك الأمن الوطني:

تتواجد على مستوى جهاز الأمن الوطني ثلاثة وحدات رئيسية مكلفة بالبحث والتحقيق

في الجرائم المعلوماتية وهي كالتالي:

- المخبر المركزي للشرطة العلمية بالجزائر العاصمة،
- المخبر الجهوي للشرطة العلمية بقسنطينة،
- المخبر الجهوي للشرطة العلمية بوهران.

وفي سبيل تدعيم مصالح الشرطة القضائية، قامت المديرية العامة للأمن الوطني سنة 2010 بخلق ما يقارب 23 خلية استعلام لمكافحة الجريمة المعلوماتية²⁷ على مستوى ولايات الوسط، الشرق، الغرب والجنوب، لتقوم فيما بعد بتعميم هذه الخلايا على جميع أنحاء الوطن ابتداءً من 2016.

الوحدات التابعة للقيادة العامة للدرك الوطني

من بين أهم الوحدات التابعة للدرك الوطني، تلك المكلفة بالبحث والتحقيق في الجرائم المعلوماتية على المستوى المركزي، نذكر المعهد الوطني للأدلة الجنائية وعلم الإجرام، الكائن مقره بمدينة بوشاوي بالعاصمة، الذي تم إنشائه بموجب المرسوم الرئاسي رقم 04-83.²⁸ يعتبر المعهد هيئة وطنية ذات طابع إداري، يتمتع بالشخصية المعنوية والاستقلال المالي، يوضع تحت وصاية وزير الدفاع الوطني، مكلف بالبحث والتحري عن الأدلة الجنائية التي تسمح بإدانة مرتكبي الجريمة، بناءً على طلب من القضاة والمحققين أو السلطات المؤهلة لذلك.

إلى جانب ذلك، توجد عدة أجهزة أخرى تابعة للدرك الوطني، نذكر منها:

- مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية للدرك الوطني،
- مديرية الأمن العمومي والاستغلال،
- المصلحة المركزية للتحريات الجنائية.

بالإضافة إلى فصائل الأبحاث، التابعة للدرك الوطني والمكلفة بالتحقيق في الجرائم المعلوماتية.²⁹

4- الأجهزة القضائية المكلفة بحماية البيانات الرقمية في بيئة التجارة الإلكترونية

عكف المشرع الجزائري منذ بداية المسار الإصلاح للعدالة، الذي شرعت فيه الجزائر بداية من سنة 2000، من خلال استحداث أقطاب جزائية ذات اختصاص إقليمي موسع، تم بموجب القانون رقم 04-14، المعدل والمتمم للأمر رقم 66-155، المتضمن لقانون الإجراءات الجزائية، أجاز خلاله المشرع الجزائري توسيع اختصاص بعض المحاكم ووكلاء الجمهورية وقضاة التحقيق في جرائم محددة على سبيل الحصر، توصف بأنها على درجة عالية من التعقيد³⁰:

- جرائم المخدرات،
- الجرائم المنظمة عبر الحدود الوطنية،
- الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات،
- جريمة تبييض الأموال والإرهاب،
- الجرائم المتعلقة بالتشريع الخاص بالصرف.

في هذا الصدد وبموجب المرسوم التنفيذي رقم 06-384، تم تمديد الاختصاص لأربعة محاكم موزعة عبر التراب الوطني كما يلي³¹:

- محكمة سيدي أمحمد بالعاصمة: يمتد الاختصاص الإقليمي لها وللمجالس القضائية التالية: الجزائر، شلف، الأغواط، البليدة، تيزي وزو، الجلفة، المدية، المسيلة، بومرداس، تيبازة وعين الدفلى

- محكمة قسنطينة: يمتد الاختصاص الإقليمي لها وللمجالس القضائية التالية: قسنطينة، أم البواقي، باتنة، بجاية، تبسة، جيجل، سطيف، سكيكدة، عنابة، قالمة، برج بوعرييج، الطارف، الوادي، خنشلة، سوق اهراس وميلة.

- محكمة ورقلة: يمتد الاختصاص الإقليمي لها وللمجالس القضائية التالية: ورقلة، أدرار، تمنراست، إيليزي، بسكرة، الوادي وغرداية.

- محكمة وهران: يمتد الاختصاص الإقليمي لها وللمجالس القضائية التالية: وهران، بشار، تلمسان، تيارت، تندوف، سعيدة، سيدي بلعباس، مستغانم، معسكر، البيض، تيسمسيلت، النعامة، عين تموشنت وغليزان.

الخاتمة:

على ضوء ما سبق ذكره في ورقتنا البحثية هذه، يمكننا القول بأن التطورات الحاصلة في بيئة التجارة الإلكترونية، ترتب عنها ارتفاعاً كبيراً في حجم البيانات الرقمية للمستهلكين الإلكترونيين، لاسيما في العقدين الأخيرين بسبب الإقبال الواسع على الأسواق الإلكترونية، وهذا الحجم الكبير للبيانات الرقمية المتداولة في بيئة التجارة الإلكترونية، جعلها عرضة لاعتداءات إلكترونية متعددة وخطيرة، تقتضي توافر آليات قانونية فعّالة لحمايتها من الجرائم السيبرانية المرتكبة ضدها، وهذا ما عكف المشرع الجزائري على تجسيده من خلال التعديل المرن للنصوص القانونية، ومواكبته للتطورات الحاصلة في بيئة التجارة الإلكترونية.

هذا التكريس التشريعي لحماية البيانات في بيئة التجارة الإلكترونية، تضمن عدة آليات وقائية وردعية وإنشاء أجهزة مختصة في حماية المعطيات الشخصية، لمواكبةً للتطورات التكنولوجية الحاصلة في البيئة الرقمية على المستويين الوطني والدولي، إلا أن هذه الآليات القانونية تبقى غير كافية وناقصة الفعّالية، طبقاً لإحصائيات الجريمة الإلكترونية الواردة عن أجهزة الاستعلام الأمني وكذا القضايا ذات الصلة المرفوعة أمام القضاء، التي تشهد ارتفاعاً رهيباً في السنوات الأخيرة؛ بالتالي فإن المواجهة تبقى صعبة في ظل انعدام التطبيق الصارم لهذه الحماية، بالإضافة إلى النقص الملحوظ في الإمكانيات البشرية والمادية المخصصة لذلك، إلى

جانب قلة الخبرة التقنية على مستوى أجهزة القضاء، وعدم انسجام النصوص القانونية مع الوسائل التقنية المتاحة للأمن المعلوماتي.

في هذا السياق نقترح بعض التوصيات التي يمكن أن تُسهم في تفعيل آليات الحماية القانونية للبيانات الرقمية في بيئة التجارة الإلكترونية من خلال:

أولاً: التكيف الدقيق والمرن للنصوص القانونية المتعلقة بحماية البيانات الرقمية في شتى المجالات ومسايرتها للتطورات التكنولوجية الحاصلة فيها، حتى تكون كفيلة بتحقيق الأمن المعلوماتي للبيئة الرقمية، بما في ذلك بيئة التجارة الإلكترونية.

ثانياً: تعزيز الحماية القانونية للبيانات الرقمية بتحقيق تنمية بشرية ومادية في مجال المعلوماتية، من خلال تحسين جودة التعليم والتكوين في المجال التكنولوجي والذكاء الاصطناعي؛ فهذا لن يتأتى إلا باعتماد الدولة على طاقاتها البشرية المكونة في أعلى المستويات العلمية والتكنولوجية، كما تعمل على تطوير منظومتها المعلوماتية بصناعة أجهزتها الإلكترونية محلياً وتطوير تقنياتها داخلياً بدل اللجوء إلى استيرادها من الخارج.

ثالثاً: تكريس مبادئ التعاون الدولي في مجال التجارة الإلكترونية، من أجل حماية البيانات الرقمية من مخاطر الجريمة الإلكترونية التي تمتد آثارها إلى خارج حدود الدولة، حيث تقتضي تضافر جميع الجهود الأمنية والقانونية والتقنية على المستويين الوطني والدولي.

رابعاً: تكثيف جهود التعاون العربي في مجال مكافحة الجرائم المعلوماتية، من خلال إبرام اتفاقيات إقليمية مشتركة لإنشاء أجهزة أمنية كفيلة بحماية البيئة الرقمية من مخاطر الجريمة الإلكترونية، على غرار إنشاء جهاز الشرطة العربية (ARAPOLE)، بالإضافة على إنشاء معاهد متخصصة في التكوين والتطوير لأمن المعلومات وبناء منظومات دفاعية للبيئة الرقمية، خاصة منها بيئة التجارة الإلكترونية.

خامساً: موازاة مع عصرنة قطاع العدالة، نقترح استحداث قسم خاص بالمنازعات الإلكترونية بتشكيلة جماعية مكونة من قضاة مختصين في مجال تكنولوجيا المعلومات، من خلال تكوينهم في ذات المجال، لتمكينهم من متابعة القضايا المتعلقة بالجرائم المعلوماتية بأنفسهم، دون اللجوء إلى جهات أخرى لمسيرة حيثيات الوقائع المتعلقة بالقضايا المرفوعة أمامهم.

¹ - التعديل الدستوري 2020، صادر بموجب مرسوم رئاسي رقم 20-251، مؤرخ في 15 سبتمبر 2020، الجريدة الرسمية عدد 54، مؤرخ في 16 سبتمبر 2020، المادة 47.

- ² - التعديل الدستوري 2016، بموجب القانون رقم 16-01 صادر في 06 مارس 2016، الجريدة الرسمية عدد 14، مؤرخ في 14 مارس 2016، المادة 46.
- ³ - قانون رقم 18-07، صادر في 10 جوان 2018، يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، الجريدة الرسمية عدد 34، مؤرخ في 10 يونيو 2018.
- ⁴ - قانون رقم 18-05، صادر في 10 مايو 2018، يتعلق بالتجارة الإلكترونية، الجريدة الرسمية عدد 27، مؤرخ في 27 شعبان 1439 هـ الموافق لـ 13 مايو 2018.
- ⁵ - أنظر الفقرة الأولى والثالثة من نص المادة 03 من القانون رقم 18-07، مصدر سابق.
- ⁶ - أنظر نص المادة 06 من القانون رقم 18-05، مصدر سابق.
- ⁷ - أنظر الفقرة الثانية والثالثة من نص المادة 06 من القانون رقم 18-05، مصدر سابق.
- ⁸ - أنظر الفقرة الرابعة من نص المادة 06، نفس المصدر سابق.
- ⁹ - أنظر نص المادة 11، نفس المصدر السابق.
- ¹⁰ - أنظر نص المادتين 22 و 26 من القانون رقم 18-05، مصدر سابق.
- ¹¹ - دليلة ليطوش، الحماية القانونية للحق في الخصوصية الرقمية للمستهلك الإلكتروني، مقال، مجلة العلوم الإنسانية، المجلد رقم ب، عدد 52، كلية الحقوق، جامعة الإخوة منتوري، قسنطينة، 2019، ص 177.
- ¹² - أنظر فحوى المواد 10، 13، 14 من القانون رقم 18-05، مصدر سابق.
- ¹³ - أنظر نص المادة 26 من نفس القانون رقم 18-05، مصدر سابق.
- ¹⁴ - أنظر فحوى المواد 58، 60، 62 و 67 من القانون رقم 18-07، مصدر سابق.
- ¹⁵ - تومي يحي، الحماية القانونية للمعطيات ذات الطابع الشخصي على ضوء القانون 18-07، مجلة الأستاذ الباحث للدراسات القانونية والسياسية المجلد 4، العدد 02، دراسة تحليلية، كلية الحقوق والعلوم السياسية، جامعة يحي فارس، المدية، 2019، ص 21.
- ¹⁶ - Gaston Raymond, Informatique et liberté personnelle, Encyclopédie juridique, tome 3, édition Dalloz, Paris, 2013, P428.
- ¹⁷ - درار نسيم، الأمن المعلوماتي و سبل مواجهة مخاطره في التعامل الإلكتروني، دراسة مقارنة، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد، تلمسان، 2016، ص 285.
- ¹⁸ - أنظر المرسوم الرئاسي رقم 14-252، يتضمن التصديق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، المحررة بالقاهرة بتاريخ 21 ديسمبر 2010، الجريدة الرسمية عدد 57 مؤرخ في 28 سبتمبر 2014.
- ¹⁹ - IC3 the "Internet Crime Complaint Center" is to provide the public with a reliable and convenient reporting mechanism to submit information to the Federal Bureau of Investigation concerning suspected Internet-facilitated criminal activity and to develop effective alliances with law enforcement and industry partners. Information is analyzed and disseminated for investigative and intelligence purposes to law enforcement and for public awareness, <http://www.ic3.gov/default.aspx>
- ²⁰ - Olivier Simon, Internet et le droit, Aspects juridiques des données numériques, édition Eyrolles, Paris, 2011, P317.
- ²¹ - Olivier Simon, Op.cit, P319.
- ²² - ربيعي حسين، آليات البحث والتحقيق في الجرائم المعلوماتية، أطروحة دكتوراه، جامعة باتنة، 2016، ص 171.
- ²³ - القانون رقم 09-04، صادر في 05 غشت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، الجريدة الرسمية عدد 47، مؤرخ في 16 غشت 2009، المادة 13.

24- أنظر نص المادة 02، المرسوم الرئاسي رقم 15-261، صادر في 08 أكتوبر 2015، الجريدة الرسمية عدد 53، مؤرخ في 08 أكتوبر 2015.

- تومي يحي، الحماية القانونية للمعطيات ذات الطابع الشخصي على ضوء القانون 18-07، مرجع سابق، ص 20. 25

26 - أنظر فحوى المواد 22، 23، 25 من القانون 18-07، مصدر سابق.

27 - عبد الرحمان حملاوي، دور المديرية العامة للأمن الوطني في مكافحة الجريمة الالكترونية، ورقة بحثية لأعمال الملتقى الوطني حول الوقاية والمكافحة، يومي 16-17 نوفمبر 2015، كلية الحقوق، جامعة بسكرة، ص 09-10.

28 - أنظر المرسوم الرئاسي رقم 04-183، صادر في 26 جوان 2004، يتضمن إحداث المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني، وتحديد قانونه الأساسي، الجريدة الرسمية، عدد 41 مؤرخ في 27 جوان 2004.

29 - عز الدين عز الدين، الإطار القانوني للوقاية من الجرائم المعلوماتية ومكافحتها، ورقة بحثية مقدمة لأعمال الملتقى الوطني حول الوقاية والمكافحة، المنعقد يومي 16 و 17 نوفمبر 2015، كلية الحقوق، جامعة بسكرة، الجزائر.

30- أنظر المواد 37، 40، 329 من قانون الإجراءات الجزائية المعدل والمتمم بموجب القانون رقم 06-22، الصادر في 20 ديسمبر 2006، المعدل والمتمم للأمر رقم 66-155، الصادر في 08 يونيو 1966، الجريدة الرسمية عدد 84، مؤرخ في 24 ديسمبر 2006.

31 - المرسوم التنفيذي رقم 06-348 صادر في 05 أكتوبر 2006، يتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق، الجريدة الرسمية، عدد 63، مؤرخ في 08 أكتوبر 2006.

قائمة المصادر والمراجع :

أولاً: المصادر القانونية:

(1) الدساتير

- التعديل الدستوري سنة 2020، صادر بموجب المرسوم الرئاسي رقم 20-251، مؤرخ في 15 سبتمبر 2020، الجريدة الرسمية عدد 54، مؤرخ في 16 سبتمبر 2020.
- التعديل الدستوري سنة 2016، صادر بموجب القانون رقم 16-01 مؤرخ في 06 مارس 2016، الجريدة الرسمية عدد 14، مؤرخ في 14 مارس 2016.

(2) النصوص التشريعية

- قانون الإجراءات الجزائية المعدل والمتمم بموجب القانون رقم 06-22، صادر في 20 ديسمبر 2006، يعدل ويتمم الأمر رقم 66-155، مؤرخ في 08 يونيو 1966، الجريدة الرسمية عدد 84، مؤرخ في 24 ديسمبر 2006.
- القانون رقم 09-04، صادر في 05 غشت 2009، يتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، الجريدة الرسمية عدد 47، مؤرخ في 16 غشت 2009.
- قانون العقوبات الجزائري المعدل والمتمم بموجب الأمر رقم 16-02، صادر في 19 جوان 2016، يعدل ويتمم الأمر 66-156، الجريدة الرسمية عدد 37، مؤرخ في 22 جوان 2016.

- قانون رقم 05-18، صادر في 10 مايو 2018، يتعلق بالتجارة الإلكترونية، الجريدة الرسمية عدد 27، مؤرخ في 13 مايو 2018.

- قانون رقم 07-18، صادر في 10 جوان 2018، يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، الجريدة الرسمية عدد 34، مؤرخ في 10 يونيو 2018.

(3) النصوص التنظيمية:

- مرسوم رئاسي رقم 04-183، صادر في 26 جوان 2004، يتضمن إحداث المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني، الجريدة الرسمية، عدد 41 مؤرخ في 27 جوان 2004.

- مرسوم رئاسي رقم 14-252، صادر في 08 سبتمبر 2014، يتضمن التصديق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المحررة بالقاهرة بتاريخ 21 ديسمبر 2010، الجريدة الرسمية عدد 57، مؤرخ في 28 سبتمبر 2014.

- مرسوم رئاسي رقم 15-261، صادر في 08 أكتوبر 2015، يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، الجريدة الرسمية عدد 53، مؤرخ في 08 أكتوبر 2015.

- مرسوم تنفيذي رقم 06-348 صادر في 05 أكتوبر 2006، يتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق، الجريدة الرسمية، عدد 63، مؤرخ في 08 أكتوبر 2006.

ثانياً: مراجع باللغة العربية

(1) كتب قانونية

- منتصر سعيد، المنظمة الدولية للشرطة الجنائية (الانتربول)، دار الفكر الجامعي، الإسكندرية، 2008.

(2) أطروحات ورسائل جامعية:

- درار نسيم، الأمن المعلوماتي وسبل مواجهة مخاطره في التعامل الإلكتروني، دراسة مقارنة، أطروحة دكتوراه، كلية الحقوق، جامعة أبوبكر بلقايد، تلمسان، 2016.

- ربيعي حسين، آليات البحث والتحقيق في الجرائم المعلوماتية، أطروحة دكتوراه، كلية الحقوق، جامعة باتنة، 2016.

(3) مقالات في مجلات علمية:

- مكتب الأمم المتحدة، تقارير مؤتمرات الأمم المتحدة لمنع الجريمة والعدالة الجنائية 1955-2015، مجلة مكتب الأمم المتحدة، الدوحة، قطر، 2015.

- تومي يحي، الحماية القانونية للمعطيات ذات الطابع الشخصي على ضوء القانون 07-18، مقال، مجلة الأستاذ الباحث للدراسات القانونية والسياسية المجلد 4، العدد 02، دراسة تحليلية، كلية الحقوق والعلوم السياسية، جامعة يحي فارس، المدية، 2019.

- دليلة ليطوش، الحماية القانونية للحق في الخصوصية الرقمية للمستهلك الإلكتروني، مقال، مجلة العلوم الإنسانية، المجلد رقم ب، عدد 52، كلية الحقوق، جامعة الإخوة منتوري، قسنطينة، 2019.

(4) مداخلات في ملتقيات وطنية

- عبد الرحمان حملاوي، دور المديرية العامة للأمن الوطني في مكافحة الجريمة الالكترونية، ورقة بحثية لأعمال الملتقى الوطني حول الوقاية والمكافحة، يومي 16-17 نوفمبر 2015، كلية الحقوق، جامعة بسكرة.

- عزالدين عز الدين، الإطار القانوني للوقاية من الجرائم المعلوماتية ومكافحتها، ورقة بحثية مقدمة لأعمال الملتقى الوطني حول الوقاية والمكافحة، يومي 16-17 نوفمبر 2015، كلية الحقوق، جامعة بسكرة.

ثالثاً: مراجع باللغة الأجنبية

- Gaston Raymond, Informatique et liberté personnelle, Encyclopédie juridique, tome3, édition Dalloz, Paris, 2013.

- Olivier Simon, Internet et le droit, Aspects juridiques des données numériques, édition Eyrolles, Paris, 2011.

رابعاً: منشورات إلكترونية على مواقع الإنترنت:

- الموقع الإلكتروني لمركز الشكاوي الخاصة بجرائم الإنترنت، تم الاطلاع عليه بتاريخ 17 ديسمبر 2021،

الساعة: 21:30، بواسطة الرابط الإلكتروني: <http://www.ic3.gov/default.aspx>

- الموقع الإلكتروني للموسوعة العربية، تم الاطلاع عليه بتاريخ 03-01-2022، الساعة: 21:30، بواسطة

الرابط الإلكتروني: <http://arab-ency.com.sy/law/details/25946>