

دور الأمن السيبراني في حماية الخصوصية من مخاطر الذكاء الاصطناعي The Role of Cybersecurity in Protecting Privacy from The Risks of Artificial Intelligence

بن كعبة محمد*

جامعة أبو بكر بلقايد تلمسان - الجزائر
benkabamohamed1@gmail.com

تاريخ النشر: 2025/12/30

تاريخ القبول: 2025/12/07

تاريخ الارسال: 2025/07/10

ملخص:

لقد شكل الأمن السيبراني خط الدفاع الأول في مواجهة الجرائم الرقمية، التي تزايدت وتيرتها وتنوعت أساليبها مع التطور التكنولوجي الهائل الذي يشهده العالم مؤخرا، وفي هذا الصدد يتضمن الأمن السيبراني جملة من الإجراءات والتقنيات التي تهدف إلى حماية الأنظمة والشبكات والبيانات من أي تهديدات أو هجمات إلكترونية قد تستهدفها، في مقابل تنوع الجرائم الرقمية لتشمل الاحتيال المالي، وسرقة البيانات، والتجسس الصناعي، وبرامج الفدية، وغيرها من الجرائم التي تلحق أضرارا جسيمة بالأفراد والمؤسسات والدول، وهنا يبرز دور الأمن السيبراني في ردع ومكافحة هذه الجرائم، من خلال مجموعة من الآليات والتقنيات كبرامج مكافحة الفيروسات والتشفير وأنظمة كشف التسلل، بالإضافة إلى ذلك، دون إغفال دور التعاون الدولي أيضا في مكافحة الجرائم الرقمية، لكون طبيعة هذه الجرائم تقتضي التعاون بين الدول، من أجل تنسيق الجهود لمتابعة المجرمين وتقديمهم إلى العدالة.

كلمات مفتاحية: الهجمات السيبرانية. حماية البيانات. الأمن القومي. الجرائم الإلكترونية.

Abstract:

Cybersecurity has formed the first line of defense against digital business crimes, which have increased in frequency and diversified in methods with the tremendous technological development that the world has witnessed recently. In this regard, cybersecurity includes a set of procedures and technologies that aim to protect systems, networks and data from any threats or electronic attacks. You may target it, in contrast to the diversity of digital business crimes to include financial fraud, data theft, industrial espionage, ransomware, and other crimes that cause serious harm to individuals, institutions, and countries, here the role of cybersecurity is highlighted in deterring and combating these crimes, through a set of mechanisms and technologies such as anti-virus programs. Encryption and intrusion detection systems, in addition, without forgetting the role of international cooperation in combating digital business crimes, because the nature of these crimes requires cooperation between countries, in order to coordinate efforts to pursue criminals and bring them to justice.

Keywords: Cyber-attacks. Data protection. National security. Cyber-crimes.

مقدمة

أصبح الأمن السيبراني ضرورة حتمية في عصرنا الرقمي الحالي، إذ يعد بمثابة الحصن الذي يحمي بياناتنا وأصولنا الرقمية من التهديدات المتزايدة، ومع تزايد الاعتماد على التكنولوجيا في كافة جوانب الحياة، ظهرت ما يسمى بجرائم الأعمال الرقمية كنوع من المخاطر التي تشكل تهديدا للأفراد والمؤسسات والدول على حد سواء.

فبين حق الأشخاص الطبيعيين والاعتباريين في حماية خصوصيتهم وأمن بياناتهم، وبين ضرورة استخدام المعطيات الشخصية في كافة تعاملاتهم التجارية الالكترونية، بالاعتماد على مختلف تقنيات الذكاء الاصطناعي المتاحة، كان من الضروري أن يتدخل المشرع بآليات قانونية تعمل على تحقيق التوازن بين المصالح المتقابلة، وذلك بوضع إطار قانوني يضمن حماية البيانات الشخصية لهؤلاء الأشخاص من أي جرائم رقمية قد تطالهم، ويعمل على تعزيز ثقة المستخدم في التقنيات الرقمية من جهة، ويسهل تقدم الذكاء الاصطناعي من جهة أخرى. من هذا المنطلق، عمدت مختلف التشريعات المقارنة للتدخل بغية توفير قدر من الحماية لهؤلاء الأشخاص، وبدوره، عمد المشرع الجزائري إلى ذلك، من خلال النص على قوانين تتعلق بحماية الأشخاص الطبيعيين في مجال معالجة البيانات ذات الطابع الشخصي، وكرس هذه الحماية في مواجهة التحديات التي يفرضها الذكاء الاصطناعي.

ومنه تتجلى أهمية الأمن السيبراني في مواجهة جرائم الأعمال في العصر الرقمي الذي نعيشه، كآلية لضمان الحماية للشركات والمؤسسات من جرائم الأعمال الرقمية المتزايدة، فمع التطور الهائل في التكنولوجيا والاعتماد المتزايد على الأنظمة الرقمية، أصبحت الشركات أكثر عرضة للهجمات الإلكترونية التي تستهدف سرقة البيانات الحساسة، والتلاعب بالأنظمة، وتعطيل العمليات التجارية.

وبالنظر لأهمية الموضوع، فإن الإشكالية المطروحة في هذا المقام هي: هل الأمن السيبراني قادر على مواجهة الجرائم الرقمية؟

وفي هذا الصدد، فإن موضوع الدراسة يهدف إلى توضيح أهمية الأمن السيبراني في مواجهة هذه الجرائم، مع التركيز على جهود الجزائر المبذولة في هذا المجال، خاصة بعد صدور القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات طابع شخصي، وتأثير ذلك على حماية خصوصيتهم وأمن بياناتهم الشخصية في الفضاء الرقمي.

وللإجابة عن الإشكال السابق ذكره، تم اعتماد المنهج الوصفي في ضبط مصطلحات الدراسة والمفاهيم المحددة للأمن السيبراني، أنواع التهديدات السيبرانية، أهمية حماية البيانات والبنية التحتية الرقمية وجرائم الأعمال الرقمية، أما المنهج التحليلي فتم استخدامه لتحليل مختلف النصوص القانونية واستنباط الأحكام ذات الصلة بالأمن السيبراني، وعلاقته بأنظمة الذكاء الاصطناعي، وكيفية تأثير ذلك الخصوصية المفروض حمايتها من أية انتهاكات.

وعليه فإن دراسة الموضوع تستدعي الوقوف على مسألتين رئيسيتين، الأولى تتضمن الإطار العام لمفاهيم الأمن السيبراني وجرائم الأعمال الرقمية، والمسألة الثانية تتعلق بجهود الجرائر في تعزيز الأمن السيبراني ومكافحة الجرائم الماسة بالخصوصية، لنهي دراستنا في الأخير بخاتمة تتضمن جملة النتائج التي تم التوصل إليها، مع تقديم توصيات واقتراحات مهمة.

أولاً: الإطار المفاهيمي للأمن السيبراني ومخاطر الجرائم الرقمية

إن التوجه العالمي المتزايد نحو الحكومة الإلكترونية قد أبرز بشكل جلي الأهمية القصوى للأمن السيبراني، ففي ظل التهديدات الأمنية الإلكترونية المتزايدة، والتي تستهدف الأجهزة والخلايا الأمنية، باتت حماية المنظومات المعلوماتية ضرورة ملحة.

لقد سعى المشرع الجزائري، إلى تبني الإدارة الإلكترونية كسبيل لتعزيز أمنها المعلوماتي، وفي هذا الإطار، أصبح الأمن السيبراني ركيزة أساسية ضمن المنظومة الأمنية المعاصرة، لا سيما مع التزايد الملحوظ في جرائم الأعمال الرقمية التي تستغل بشكل متنام الشبكات الإلكترونية لتحقيق أهداف إجرامية. وانطلاقاً من ذلك، تؤثر هذه الجرائم بالسلب على سلامة البنى التحتية للمعلومات الوطنية الحساسة، وخاصة تلك المتعلقة بالمعلومات الشخصية، مما يستدعي محاولة فهم الإطار المفاهيمي للأمن السيبراني وجرائم الأعمال الرقمية، كتمهيد للتقصي عن هذه القضايا بشكل أعمق.

1. تعريف الأمن السيبراني

إن الأمن السيبراني يتجسد في ضمان وجود واستمرارية مجتمع المعلومات للأمة، وضمان وحماية فضاء الإنترنت، والمعلومات الخاصة به، والأصول والبنية التحتية الحيوية، وهو ما سنتناوله بالتفصيل كالتالي:

1.1. المفهوم والخصائص

يعرف الأمن السيبراني بأنه مجموعة من الإجراءات والتقنيات التي تهدف إلى حماية الأنظمة والشبكات والبيانات من أي تهديدات أو هجمات سيبرانية، تشمل هذه التهديدات البرمجيات الخبيثة، والقرصنة، والاحتيال الإلكتروني، وغيرها، ومنه تكمن أهمية الأمن السيبراني في حماية البيانات الحساسة، والحفاظ على سرية المعلومات، وضمان استمرارية الأعمال، والحفاظ على الثقة بين الأفراد والمؤسسات¹.

كما يعرف الأمن السيبراني بأنه حالة حماية من المهاجمين أو الاستخدام غير المصرح به للبيانات الإلكترونية، أو اتخاذ التدابير اللازمة لتحقيق هذه الحماية.

لا يمكن الوصول إلى تعريف شامل للأمن السيبراني إلا من خلال تحليل مجموعة من العناصر الفاعلة والمتحركة في تحقيقه، وتشمل هذه العناصر: التكنولوجيا، الأحداث، الاستراتيجيات والعمليات والأساليب، وأخيراً العنصر البشري كمرجع أمني.

وعند التمعن في هذه العناصر، نجد أن الأمن السيبراني يجب أن يتميز بعدة خصائص أساسية، أولها أنه هو ذو طبيعة متعددة التخصصات الاجتماعية والتقنية، ثانياً، أنه يتسم بكونه شبكة خالية من الحجم، مما يعني

أن قدرات الفاعلين يمكن أن تكون متماثلة على نطاق واسع، وأخيرا، أنه يتميز بدرجة عالية من التغيير، والترابط، وسرعة التفاعل.²

أما في القانون الجزائري، فيعرف الأمن السيبراني بأنه مجموعة التدابير والسياسات والإجراءات القانونية والتقنية التي تهدف إلى حماية الفضاء السيبراني من التهديدات والمخاطر التي تستهدف الأنظمة المعلوماتية والبيانات والمعلومات الحساسة³، ويركز الأمن السيبراني في الجزائر على عدة جوانب رئيسية، منها حماية البنية التحتية الحيوية، مكافحة الجرائم السيبرانية، حماية البيانات الشخصية وتعزيز الوعي السيبراني.

وقد اعتمدت الجزائر استراتيجية وطنية للأمن السيبراني، تهدف إلى تعزيز الأمن السيبراني في البلاد، كما تم إصدار عدة قوانين وتشريعات تتعلق بالأمن السيبراني، منها قانون مكافحة الجرائم المتعلقة بتكنولوجيات الإعلام والاتصال⁴، قانون حماية الأشخاص الطبيعيين في مجال معالجة البيانات ذات الطابع الشخصي⁵.

2.1. أهمية حماية الخصوصية والبنية التحتية الرقمية

تزداد أهمية حماية البيانات والبنية التحتية الرقمية في عصرنا الحالي، مع التوسع الهائل في استخدام التكنولوجيا والاعتماد عليها في مختلف جوانب الحياة، وهو ما يفرض احترام حق الفرد في التحكم في معلوماته الشخصية على الانترنت ومنع الوصول غير المصرح إليها، خاصة اتجاه مختلف التهديدات السيبرانية التي سبق التطرق إليها، ومنه تتجلى أهمية حماية الخصوصية في حماية وتأمين عدة هذه الجوانب نذكر من بينها:

1.2.1. حماية البيانات الشخصية

تشمل البيانات الشخصية المعلومات الحساسة مثل الأسماء والعناوين وأرقام الهواتف والمعلومات المالية والصحية، ومنه فحماية هذه البيانات ضرورية لمنع إساءة استخدامها أو سرقتها.⁶

2.2.1. الخصوصية الرقمية

مع تزايد استخدام الإنترنت ووسائل التواصل الاجتماعي، أصبحت الخصوصية الرقمية أكثر عرضة للخطر، وحماية البيانات تساعد في الحفاظ على خصوصية الأفراد ومنع التجسس أو المراقبة غير المصرح بها، وتشمل البنية التحتية الحيوية أنظمة الطاقة والمياه والاتصالات والنقل، وبالتالي فإن حماية هذه الأنظمة من مختلف الهجمات الإلكترونية ضروري، للحفاظ على الأمن القومي واستقرار المجتمع.⁷

3.2.1. المعلومات الحكومية

تحتوي الأنظمة الحكومية على معلومات حساسة تتعلق بالأمن القومي والدفاع والاقتصاد، تقتضي حمايتها لمنع تسريبها أو استغلالها من قبل جهات معادية.

4.2.1. الملكية الفكرية

حماية البيانات تساعد في الحفاظ على الملكية الفكرية للشركات والمؤسسات، مثل براءات الاختراع والأسرار التجارية وحقوق النشر.

5.2.1. منع الجرائم الإلكترونية كالاختيال الإلكتروني

يشمل الاحتيال الإلكتروني سرقة الهوية والتصيد الاحتيالي والاحتيال المالي كما عرفنا سابقاً، حماية البيانات تساعد في ردع هذه الجرائم وحماية الأفراد والمؤسسات من الوقوع كضحايا لها.

6.2.1. الفيروسات والبرامج الضارة

يمكن للفيروسات والبرامج الضارة أن تتسبب في تلف البيانات وتعطيل الأنظمة وسرقة المعلومات، حماية البيانات تساعد في منع انتشار هذه البرامج وحماية الأنظمة من التلف.

وحماية هذه الأنظمة تضمن استمرارية العمل وتجنب التوقعات التي يمكن أن تتسبب في خسائر كبيرة.⁸

2. أنواع التهديدات السيبرانية

يقصد بالتهديدات السيبرانية أي فعل ضار يهدف إلى إتلاف الأنظمة الحاسوبية أو سرقة البيانات أو تعطيل العمليات الرقمية، وتتوسع هذه التهديدات بشكل كبير لتشمل الهجمات الإلكترونية الخبيثة مثل البرمجيات الضارة، وهجمات التصيد الاحتيالي، اختراقات قواعد البيانات، والتجسس السيبراني، وحتى الإرهاب السيبراني، ومن المهم فهم أنواعها المختلفة لتمكين المؤسسات وكافة المستخدمين لها من اتخاذ تدابير وقائية مناسبة للحماية من أي هجوم سيبراني⁹، لذلك سنتناول أهم الأنواع الرئيسية للتهديدات السيبرانية:

1.2. البرامج الضارة الفيروسات (Malware)

تعتبر البرامج الضارة أو الفيروسات، إحدى البرامج التي تنتشر عن طريق نسخ نفسها وإلحاقها ببرامج أخرى، مما يؤدي إلى إتلاف البيانات أو تعطيل الأنظمة، وتعد إحدى التهديدات السيبرانية الأكثر شيوعاً وخطورة، لكونها تمس مباشرة بسرية وتكامل وتوافر البيانات والأنظمة، ولقد جرم المشرع الجزائري كل الأفعال التي ترتكب باستخدام البرامج الضارة، وذلك بموجب القانون رقم 09-04، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، حيث جاء في نص المادة 37 من هذا القانون على معاقبة كل من قام بإدخال أو إتلاف أو تغيير أو إخفاء المعطيات أو أنظمة المعالجة الآلية للمعطيات، أو بمسحها أو التسبب في تعطيلها أو إلحاق ضرر بها عن قصد، أما المادة 38 من نفس القانون فتجرم صنع أو حيازة أو تزويد أو بيع أو إشهار لأي أدوات أو برامج أو معطيات معدة أو مهيأة لارتكاب جريمة من الجرائم المنصوص عليها في هذا القانون.

في مقابل ذلك، نجد قانون التوجيه 2013/40 (EU) للبرلمان الأوروبي والمجلس بتاريخ 12 أوت 2013 بشأن الهجمات على أنظمة المعلومات واستبدال قرار الإطار JHA. 222/2005، الذي جرم كل الأفعال المتعلقة بأنظمة المعلومات، بما في ذلك التدخل غير القانوني في نظام المعلومات والتدخل غير القانوني في البيانات¹⁰.

2.2. برامج التجسس (Spyware)

برامج التجسس هي عبارة عن برامج تتسلل إلى الأجهزة، لجمع معلومات عن المستخدمين دون علمهم، مثل كلمات المرور وبيانات التصفح، يتم إرسال هذه المعلومات بعد ذلك إلى جهة خارجية لأغراضها تجارية أو

إجرامية، الأمر الذي يجعلها تشكل تهديدا خطيرا للخصوصية والأمن الشخصي، يمكن أن تؤدي إلى سرقة الهوية، الاحتيال المالي، أو حتى الابتزاز، وهنا يهدف الأمن السيبراني إلى اكتشاف وإزالة برامج التجسس، وحماية بيانات المستخدمين الحساسة من الوصول غير المصرح به، من خلال استخدام برامج مكافحة التجسس، وفي هذا الصدد جاء في المادة 39 من القانون رقم 04-09 تجريم الحصول على المعطيات التي تتضمن معلومات خاصة بالأشخاص أو التي من شأنها تحديد هويتهم، عن طريق الاحتيال أو عن طريق استعمال وسائل تقنية دون موافقة المعني، وكذا اللائحة الأوروبية العامة لحماية البيانات (GDPR) واللائحة (EU) (2016/679) التي تفرض التزامات صارمة على كيفية جمع ومعالجة وتخزين البيانات الشخصية، بحيث أن أي استخدام لبرامج التجسس لجمع بيانات شخصية دون الامتثال لمبادئ اللائحة العامة لحماية البيانات يعد انتهاكا¹¹.

3.2. هجمات التصيد الاحتيالي (Phishing)

التصيد الاحتيالي هو رسائل بريد إلكتروني أو رسائل نصية أو انقر على روابط ضارة أو مكالمات هاتفية مزيفة تبدو وكأنها من مصادر موثوقة، تهدف إلى خداع المستخدمين للكشف عن معلومات حساسة، وهنا قام المشرع الجزائري بمعاقبة كل الأفعال التي تتم عن طريق هجمات التصيد الاحتيالي، بالاستناد إلى نصوص القانون رقم 04-09 سالف الذكر، وكذا مواد قانون العقوبات بالتحديد نص المادة 372 من قانون العقوبات¹²، التي جرمت كل عمليات النصب والاحتيال بشكل عام، والتي تتناسب مع الأفعال التي يقوم بها المحتالون في التصيد الاحتيالي لخداع الضحايا.

4.2. هجمات كلمات المرور

هجمات كلمات المرور هي محاولات لاكتشاف أو تخمين كلمات المرور للوصول غير المصرح به إلى الحسابات أو الأنظمة، ولأن كلمات المرور هي خط الدفاع الأول لمعظم الأنظمة الرقمية، فإن اختراقها يعني فتح الباب للوصول إلى المعلومات الحساسة أو التحكم في الحسابات، وعليه يتضمن الأمن السيبراني استخدام كلمات مرور قوية ومعقدة، المصادقة متعددة العوامل¹³ (MFA)، وسياسات تغيير كلمة المرور بانتظام، بالإضافة إلى أنظمة الكشف عن محاولات اختراق كلمات المرور.

5.2. هجمات إنترنت الأشياء (IoT Attacks) :

هجمات إنترنت الأشياء تستهدف الأجهزة المتصلة بالإنترنت، مثل الكاميرات وأجهزة الاستشعار، لتعطيلها أو استخدامها في هجمات أخرى¹⁴، ويمكن أن تؤثر هذه الهجمات على الخصوصية والسلامة والأمن المادي، يتطلب الأمن السيبراني في سياق إنترنت الأشياء تصميمًا آمنًا منذ البداية، وتحديثات برامج منتظمة، وتشفير البيانات، والمصادقة القوية¹⁵.

3. الجرائم الرقمية الماسة بحق الخصوصية

تعرف الجرائم الرقمية بأنها أنشطة غير قانونية تتم باستخدام التكنولوجيا الرقمية، وتستهدف تحقيق مكاسب مالية أو إلحاق ضرر بالآخرين، تشمل هذه الجرائم الاحتيال المالي الإلكتروني، وسرقة الملكية الفكرية، والتجسس الصناعي، والاختراق السيبراني للمؤسسات، وبالتالي سنحاول التفصيل فيها كالتالي:

13. أنواع الجرائم الرقمية

تعتبر الجرائم الرقمية ظاهرة إجرامية واسعة النطاق ومتنوعة، حيث أن هذا التنوع هو ما يجعل المواجهة القانونية والتقنية أمرا بالغ التعقيد، خصوصا وأن التطورات في مجال الذكاء الاصطناعي تساهم في إزالة القيود بين هذه الأنواع، وتمنح مرتكبيها قدرات جديدة لأتمتة الهجمات وتطويرها بشكل مستمر.

1.1.3 جرائم الاحتيال المالي الإلكتروني

تزايدت جرائم الاحتيال المالي الإلكتروني بشكل ملحوظ في السنوات الأخيرة، وذلك بالتزامن مع التطورات التكنولوجية المتسارعة والاعتماد المتزايد على الإنترنت في المعاملات المالية، وتتنوع أساليب الاحتيال الإلكتروني وتتطور باستمرار، مما يجعلها تحديا كبيرا للأفراد والمؤسسات على حد سواء، من بين أبرز أساليب الاحتيال المالي الإلكتروني، التصيد الاحتيالي، الاحتيال عبر الإنترنت، الاحتيال عبر وسائل التواصل الاجتماعي، الاحتيال عبر البرامج الضارة، الاحتيال عبر العملات الرقمية.

ولتجنب الوقوع ضحية للاحتيال المالي الإلكتروني، يجب اتخاذ الاحتياطات اللازمة، كالحذر من الرسائل الإلكترونية والرسائل النصية القصيرة المشبوهة، وكذا التحقق من مصداقية المواقع الإلكترونية والمتاجر الإلكترونية قبل إجراء أي معاملات مالية، عدم مشاركة المعلومات الشخصية أو المالية مع أي شخص غير موثوق به، والإبلاغ عن أي عمليات احتيال مشتبها بها إلى الجهات المختصة، كما يجب على الأفراد والمؤسسات أن يكونوا على دراية بأساليب الاحتيال المالي الإلكتروني، وأن يتخذوا الإجراءات اللازمة لحماية أنفسهم من هذه الجرائم.

وتولي الجزائر اهتماما متزايدا بمكافحة جرائم الاحتيال المالي الإلكتروني، في كل من قانون العقوبات في نصوص تجرم الاحتيال والنصب¹⁶، ويمكن تطبيق هذه المواد على الجرائم التي ترتكب عبر الوسائل الإلكترونية، وقانون مكافحة الجرائم المتعلقة بتكنولوجيا الإعلام والاتصال، التي تتناول الجرائم الإلكترونية في الجزائر، ويتضمن مواد تجرم الاحتيال الإلكتروني وسرقة البيانات والجرائم الأخرى التي ترتكب عبر الإنترنت.¹⁷

2.1.3 جرائم سرقة الملكية الفكرية والبيانات التجارية

تعد جرائم سرقة الملكية الفكرية والبيانات التجارية من الجرائم الخطيرة، وقد أولى القانون الجزائري اهتماما كبيرا بمكافحة هذه الجرائم، حيث تضمن مجموعة من النصوص القانونية التي تجرم هذه الأفعال وتحدد العقوبات المناسبة لها.

تشمل جرائم سرقة الملكية الفكرية مجموعة واسعة من الأفعال، مثل تقليد العلامات التجارية، ونسخ المصنفات الأدبية والفنية، وانتهاك براءات الاختراع، وسرقة الأسرار التجارية، وتعتبر هذه الأفعال جرائم يعاقب

عليها القانون الجزائري، حيث ينص قانون حماية الملكية الفكرية على عقوبات تتراوح بين الغرامات المالية والحبس، وذلك حسب طبيعة الجريمة وخطورتها¹⁸.

أما عن جرائم سرقة البيانات التجارية، فتشمل سرقة المعلومات السرية للشركات والمؤسسات، مثل قوائم العملاء، وخطط العمل، والبيانات المالية، وتعتبر هذه الجرائم من الجرائم الخطيرة التي تهدد الأمن الاقتصادي للشركات والمؤسسات، وقد جرمها القانون الجزائري في قانون العقوبات وقانون مكافحة الجرائم المعلوماتية، حيث ينص على عقوبات تتراوح بين الغرامات المالية والحبس¹⁹، وذلك حسب طبيعة الجريمة وخطورتها، وقد اتخذت الجزائر العديد من الإجراءات لمكافحة هذه الجرائم، مثل إنشاء هيئات متخصصة في حماية الملكية الفكرية والبيانات التجارية، وتفعيل دور القضاء في مكافحة هذه الجرائم، وتوعية الجمهور بأهمية حماية الملكية الفكرية والبيانات التجارية²⁰.

3.1.3. جرائم التجسس الصناعي والاختراق السيبراني للمؤسسات

يشهد العالم اليوم تزايد ملحوظ في جرائم التجسس الصناعي والاختراق السيبراني، والتي أصبحت تشكل تهديداً خطيراً للمؤسسات على اختلاف أنواعها، وفي الجزائر، لم يكن الوضع مختلفاً، حيث بدأت هذه الجرائم تظهر بشكل متزايد، مما دفع المشرع الجزائري إلى التدخل لمواجهة هذه الظاهرة من خلال سن قوانين وتشريعات تهدف إلى حماية المؤسسات من هذه المخاطر.

ويعرف التجسس الصناعي والاختراق السيبراني في القانون الجزائري، بأنه الحصول غير القانوني على معلومات سرية تخص مؤسسة ما، بهدف استخدامها لتحقيق مكاسب اقتصادية أو تجارية، أما الاختراق السيبراني، فيشمل الدخول غير المصرح به إلى أنظمة وشبكات المعلومات الخاصة بالمؤسسات، بهدف سرقة البيانات أو تعطيل الأنظمة أو إتلافها، وعليه جرم قانون العقوبات وقانون مكافحة الجرائم المتعلقة بتكنولوجيا الإعلام والاتصال²¹.

وتجدر الإشارة في الأخير، أن الجريمة السيبرانية في الجزائر تطورت وذلك تماشياً مع التطور التكنولوجي، حيث أصبحت أكثر تعقيداً وتنوعاً، ومن بين أنواع الجرائم السيبرانية المنتشرة في الجزائر كالاختيال المالي عبر الإنترنت، والتصيد الاحتيالي، وسرقة البيانات الشخصية، والابتزاز الإلكتروني، الذين سبق التفصيل فيهم²².

2.3. الاختلاف بين الجرائم الرقمية التقليدية واستغلال الذكاء الاصطناعي لأغراض غير مشروعة

لقد أدى التطور المتسارع للذكاء الاصطناعي إلى إبراز فرق جوهري ما بين القانون الجنائي والسيبراني، حيث بات من الضروري التمييز بوضوح بين الجرائم الرقمية التي تعتمد على وسائل تقليدية والجرائم التي تستغل قدرات الذكاء الاصطناعي، وهنا يكمن التمييز بين طبيعة الوسيلة الإجرامية، وإثبات النية الإجرامية.

وفي هذا الصدد، تتجلى الجرائم الرقمية التقليدية في صورة أفعال غير مشروعة، تمارس باستخدام أنظمة حاسوبية وشبكات كوسيط أو كهدف، وتعتمد في تنفيذها على وسائل وتقنيات ثابتة ومحدودة الكفاءة، كما تقوم

هذه الجرائم على ثغرات برمجية معروفة أو برمجيات خبيثة ذات نمط تنفيذي واضح، تكون العلاقة بين فعل الجاني والنتيجة الإجرامية مباشرة وواضحة، حيث يمكن تتبع جملة الأوامر الصادرة إلى النظام المستهدف بسهولة، لذلك، يعتمد الإثبات الجنائي فيها على الأدلة الرقمية التقليدية التي تثبت تدخل الفاعل المباشر أو استخدامه للأداة.

وهنا يتجلى مفهوم استغلال الذكاء الاصطناعي لأغراض غير مشروعة، كمفهوم إجرامي معقد في استخدام قدرات الذكاء الاصطناعي والتعلم الآلي لإنشاء بيئة إجرامية ذاتية التكيف أو إنتاج محتوى مزور بالغ الإقناع، فبدلاً من الاعتماد على سيناريوهات محددة مسبقاً، تصبح الوسيلة الإجرامية متكيفة وذاتية التطور لاخترق الدفاعات، وبالتالي يكمن الاختلاف الجوهرى هنا في أن الجرائم المدعومة بالذكاء الاصطناعي تكون فائقة التخصيص، كإنتاج محتوى احتيالي أو تزيف عميق، مستهدف بناءً على تحليل بيانات الضحية، مما يرفع من مستوى حقيقتها، ويجعل من الصعب اثباتها فيما بعد.

وهنا، يعد العائق الأكبر لاستغلال الذكاء الاصطناعي في الجريمة، هو إشكالية إثبات النية الإجرامية وصعوبة إثبات القصد الجنائي، لأنه في الجرائم التقليدية، الجاني هو المنفذ المباشر للجريمة، أما عند استخدام الذكاء الاصطناعي، قد يكون النظام هو من قام بتنفيذ الجريمة، مما يثير تساؤلات حول تحمل المسؤولية، إذا كانت تقع على عاتق مبرمج النظام، أو المستخدم الذي أطلق تشغيله، أو على النظام نفسه في حال اتخذ قرار إجرامي لم يكن متوقع.

وعليه، فإن التشريعات التقليدية للجرائم الرقمية، التي صيغت لمواجهة الجاني مرتكب الجريمة، والذي يستخدم أداة جامدة، قد تكون قاصرة عن استيعاب الضرر المتوقع وغير المباشر الناجم عن الأنظمة الذكية، وهو ما يعني أنه مواجهة الجرائم القائمة على الذكاء الاصطناعي تتطلب سن قوانين وتشريعات جديدة تركز على تنظيم وضبط وفرض أنظمة الذكاء الاصطناعي حماية لمتطلبات شفافية الخوارزميات وتمكين المساءلة بدلاً من الاكتفاء بتجريم الفعل النهائي.

ثانياً: تأثير الذكاء الاصطناعي على الأمن السيبراني وخصوصية البيانات

إن استخدام أنظمة الذكاء الاصطناعي في تحليل البيانات الضخمة، بما في ذلك البيانات الشخصية، يتطلب إطار قانوني صارم يضمن حماية حقوق الأفراد من جهة، ويتيح للدولة والمؤسسات استخدام هذه التقنيات لتعزيز دفاعاتها السيبرانية من جهة أخرى.

في هذا السياق، تواجه التجربة الجزائرية، خاصة القوانين المتعلقة بحماية البيانات الشخصية ومكافحة الجرائم الإلكترونية، عدة عراقيل اتجاه قدرتها على ضبط استخدامات الذكاء الاصطناعي، فمن ناحية، يمكن للذكاء الاصطناعي أن يكون أداة قوية في الكشف عن التهديدات السيبرانية المعقدة والتصدي لها بفاعلية غير مسبقة، مما يعزز الأمن القومي والرقمي، ومن ناحية أخرى، فإن إمكانية استخدامه في هجمات إلكترونية متطورة أو في معالجة البيانات دون رقابة كافية، يثير مخاوف بشأن الانتهاكات المحتملة للخصوصية

والضمانات الدستورية، وهو ما يبرز في تأثيرات الذكاء الاصطناعي على خصوصية البيانات الشخصية وأمن المعلومات الحكومية.

1. تأثير الذكاء الاصطناعي على خصوصية البيانات الشخصية

رغم الخصائص التي يمتاز بها الذكاء الاصطناعي من خلال تحليل البيانات، فإنه يثير في الوقت ذاته مخاوف عميقة بشأن حق الأفراد في الخصوصية وسلامة معلوماتهم الشخصية، مما يجعلها عرضة لمخاطر تتمحور حول الشفافية، والتمييز، وقابلية البيانات للانتهاك.

لقد أدركت التشريعات الحديثة، ومنها القانون الجزائري، ضرورة تنظيم هذه العلاقة المعقدة، وهنا يمثل القانون رقم 07-18 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة البيانات ذات الطابع الشخصي، الإطار القانوني الأساسي، حيث نص صراحة في المادة 3 منه على أن كل معالجة للبيانات ذات الطابع الشخصي يجب أن تتم بكل شفافية وشرف ونزاهة، وأن يكون لها غرض مشروع ومحدد وصريح، هذا المبدأ يمثل تهديد مباشر أمام أنظمة الذكاء الاصطناعي، خاصة فيما يتعلق بمبدأ تحديد الغرض، فخوارزميات التعلم الآلي غالباً ما تكتشف أنماط وتستنجد استنتاجات تتجاوز الهدف الأصلي الذي جمعت من أجله البيانات.

كما أن مبدأ الموافقة الصريحة والحرّة، المنصوص عليه في المادة 12 من نفس القانون، يواجه صعوبة بالغة في سياق الذكاء الاصطناعي، فكيف يمكن للمواطن أن يعطي موافقة مستنيرة على معالجة بياناته عندما تكون خوارزمية الذكاء الاصطناعي نفسها "صندوقاً أسود" غير مفهوم للمختصين أنفسهم، وتتطور قراراتها باستمرار.

وفي هذا الإطار، تعتبر صلاحية إخفاء الهوية والاسم المستعار، الذي يسمح بالحد من إمكانية التعرف على صاحب البيانات، حل قانوني وتقني هام جداً، ومع ذلك، أظهرت الأمثلة الواقعية أن الخوارزميات المتقدمة للذكاء الاصطناعي، خاصة في مجال تحليل البيانات الضخمة، يمكنها "إعادة التعرف" على الأفراد، حتى بعد تطبيق تقنيات إخفاء الهوية، بمجرد دمجها مع مجموعات بيانات أخرى، مثال ذلك ما حدث في بعض الدول حيث أمكن إعادة التعرف على الأفراد في سجلات صحية كانت تبدو مجهولة الهوية بعد مقارنتها بسجلات التصويت العامة.

إضافة إلى ذلك، يثير الذكاء الاصطناعي مسألة الحق في عدم الخضوع لقرار آلي فردي، وهو حق تتبناه التشريعات المتقدمة وله أساس في مفهوم الشفافية والمساءلة، فعندما يتخذ نظام الذكاء الاصطناعي قرار معين بشأن فرد ما، مثل رفض طلب قرض أو وظيفة، فإن القانون يفرض ضرورة توفير المنطق الأساسي وراء هذا القرار، وهو ما يتعارض مع طبيعة الخوارزميات المعقدة، وهنا العائق القانوني لا يقتصر فقط على تكييف النصوص القائمة، بل يتطلب في المستقبل إدخال تعديلات تسمح بفرض الشفافية الخوارزمية ووضع آليات للتدقيق والطعن في القرارات المتخذة بصفة آلية لضمان عدم انتهاك الخصوصية أو التسبب في تمييز غير مشروع، وبالتالي، فإن الحماية الفعالة للبيانات الشخصية في عصر الذكاء الاصطناعي تتطلب أكثر من مجرد

إطار نظري، بل تتطلب آليات تطبيق وتقنية قادرة على فرض الاحترام القانوني في بيئة تتسارع فيها الابتكارات التكنولوجية.

2. تأثير الذكاء الاصطناعي على أمن المعلومات الحكومية

إن تبني أنظمة الذكاء الاصطناعي في القطاع الحكومي يمثل سيفاً ذا حدين بالنسبة لأمن المعلومات، فمن جهة، يعد الذكاء الاصطناعي آلية قوية لتعزيز الدفاعات السيبرانية، من خلال الكشف عن التهديدات المدعومة بالذكاء الاصطناعي، على سبيل المثال، تحليل حركة مرور الشبكة الهائلة والكشف عن الأنماط الشاذة والهجمات المتقدمة بسرعة ودقة تفوق القدرة البشرية بكثير، هذا النوع من الاستخدام يتماشى مع التوجهات العامة لحماية أنظمة المعلومات الحكومية الحساسة، التي يؤكد عليها القانون رقم 07-18 سالف الذكر، ولا سيما في سياق حماية تلك المعطيات من أي اختراق غير قانوني.

وبالرغم من ذلك، تكمن المخاطر القانونية والأمنية في طبيعة الذكاء الاصطناعي نفسه، عندما يتعلق الأمر بثقة البيانات، ففي حال تعرضها للتلاعب أو الاختراق، قد يؤدي ذلك إلى نتائج خاطئة أو قرارات حكومية ضارة، مما يشكل انتهاك للمسؤولية الإدارية والقانونية عن سلامة المعلومات. وهنا يصبح تطبيق مواد القانون رقم 04-09 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، أمر بالغ الأهمية، حيث يجب تكييف أحكامه لمواجهة صور جديدة من الجرائم السيبرانية المرتكبة باستخدام أدوات الذكاء الاصطناعي.

كما قد يتعلق الأمر بمسألة اتخاذ القرار، بناء على بيانات حكومية سرية أو حساسة، فيصبح تحديد المسؤولية القانونية في حال حدوث خطأ أمني أو انتهاك للخصوصية مسألة معقدة، حيث تتطلب هذه الثغرة القانونية الجديدة تعديل في الأطر التشريعية، لا سيما في مواد المسؤولية الإدارية والمدنية المعمول بها، لضمان المساءلة والتعويض.

3. متطلبات الأمن السيبراني في ظل استراتيجيات الدفاع المدعوم بالذكاء الاصطناعي

يشهد المشهد الأمني السيبراني تحول جذري مع تزايد الاعتماد على استراتيجيات الدفاع المدعوم بالذكاء الاصطناعي، وهو ما يفرض متطلبات قانونية لضمان فعالية هذه الأنظمة وشرعيتها، خاصة بعد دمج آليات الذكاء الاصطناعي في الكشف عن التهديدات، لكنه في الوقت ذاته يثير تساؤلات حول المساءلة القانونية، الشفافية، وحماية البيانات الشخصية.

استناداً لذلك، فإن المتطلب الأول الذي تفرضه هذه الاستراتيجيات هو الشرعية والدقة في جمع ومعالجة البيانات التي تعتمد عليها خوارزميات الذكاء الاصطناعي، فالنظام القانوني يستلزم أن تكون هذه البيانات، قد جمعت بطريقة مشروعة وتخضع للحماية المنصوص عليها.

أما عن المتطلب الثاني، فهو يتعلق بمسألة المساءلة القانونية والشفافية في اتخاذ القرار، لأنه عندما يتخذ نظام الذكاء الاصطناعي قرار دفاعي، كحظر حركة مرور شبكية أو عزل نظام متضرر، يجب أن يكون هناك

إطار واضح للمساءلة يحدد الطرف المسؤول عن أي خطأ قد ينتج عن هذا القرار الآلي، وهنا تثار إشكالية تحمل المسؤولية على مطور النظام، أم على الجهة التي شغلته، لأن القانون يتطلب إمكانية مراجعة وتفسير قرارات الذكاء الاصطناعي، هذا التفسير ضروري لضمان حق الأفراد في معرفة الأساس الذي اتخذ عليه الإجراء الأمني ضدهم، وهو مبدأ دستوري أساسي، في حالة وقوع اختراق، يجب على المؤسسات أن تكون قادرة على تقديم سجلات تدقيق شفافة، توضح تسلسل الأحداث وكيف تدخل الذكاء الاصطناعي، وذلك لدعم أي تحقيق قانوني لاحق.

وأخيراً، يتطلب الأمن الذاتي لنظام الذكاء الاصطناعي، لأنه بقدر ما يستخدم الذكاء الاصطناعي للدفاع، فإنه يمكن أن يكون هدف أو نقطة ضعف بحد ذاته، حيث يمكن للمهاجمين استغلال نقاط ضعف الخوارزميات عبر ما يعرف بهجمات العدائية، لتثويته بيانات التدريب أو خداع نموذج الذكاء الاصطناعي لاتخاذ قرارات خاطئة، مثل تصنيف هجوم مشروع على أنه حركة مرور طبيعية.

ومنه، تتطلب الاستراتيجيات الدفاعية المدعومة بالذكاء الاصطناعي الالتزام بمتطلبات الأمن المتأصل، والتحقق الدوري من سلامة وموثوقية هذه النماذج، بحيث تصبح هذه الموثوقية مطلب قانوني لتشغيلها في بيئات حساسة، وهذا يستدعي تطبيق معايير فنية صارمة تشبه تلك المنصوص عليها في الإطار القانوني لتأمين الأنظمة المعلوماتية الحيوية.

ثالثاً: الإطار التشريعي والجهود الوطنية في مواجهة مخاطر الذكاء الاصطناعي على الأمن السيبراني

تبذل الجزائر جهوداً متواصلة لتعزيز الأمن السيبراني ومكافحة جرائم الأعمال الرقمية، حيث سنت قوانين تجريم الأفعال الإلكترونية الضارة وأنشأت هيئات متخصصة لمراقبة الفضاء السيبراني، كما تعمل على تطوير البنية التحتية الرقمية الآمنة وتدريب الكوادر المتخصصة في مجال الأمن السيبراني²³، هذا ويسعى المشرع إلى تعزيز التعاون الدولي في مجال مكافحة الجرائم السيبرانية من خلال توقيع اتفاقيات مع الدول والمنظمات الدولية، وهو ما سنتطرق إليه كالتالي:

1. الإطار القانوني والتنظيمي للأمن السيبراني في الجزائر

بالرجوع إلى التشريع الجزائري، نجده لم يستقر على استخدام مصطلح واحد للدلالة على جرائم الأمن السيبراني، حيث وضع نصوص تعاقب على الأفعال التي تشكل جرائم معلوماتية، وقد بدأ ذلك في سنة 2001، من خلال المواد 144 مكرر، و144 مكرر 1، و144 مكرر 2، والمادة 146 من قانون العقوبات، وفي عام 2004، أصدر المشرع نص تشريعي جديد يشمل سبعة مواد، من المادة 394 مكرر إلى المادة 394 مكرر 7، تحت عنوان "المساس بأنظمة المعالجة الآلية للمعطيات"، ليصدر في النهاية القانون رقم 09-04 المؤرخ في 05 أوت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها. وعرفها بأنها جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظم الاتصالات الإلكترونية²⁴.

وكخطوة جديدة، قام المشرع الجزائري بسن القانون 04-09 المتعلق بالوقاية من تكنولوجيات الإعلام والاتصال ومكافحتها، وإن كان تجسيد بنوده على أرض الواقع مازال ضعيفا إلى حد الساعة، نتيجة إهمال الجوانب التقنية الكفيلة بتصنيف هذه الجرائم وفي تحديد العقوبة المناسبة في حق مرتكبيها، حيث تقتصر العقوبات في غالبية الأحيان على الغرامة المالية فقط، غير أنه وضع مجموعة تدابير وقائية واجرائية للوقاية من هذه الجرائم ومكافحتها، أهمها:

- المراقبة الالكترونية.
- تفتيش وحجز المنظومة المعلوماتية.
- تمديد الاختصاص بنظر هذه الجرائم.
- تبادل المساعدة القضائية الدولية.
- استحداث الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها²⁵.

1.1. دور الهيئات والمؤسسات الحكومية في تعزيز الأمن السيبراني

تلعب الهيئات والمؤسسات الحكومية في الجزائر دور هام في تعزيز الأمن السيبراني من خلال عدة إجراءات وسياسات، تعمل هذه الهيئات على تطوير استراتيجيات وطنية للأمن السيبراني، وتحديث القوانين والتشريعات لمواكبة التحديات الرقمية المتزايدة، كما تعمل على إنشاء مراكز وطنية للأمن السيبراني لرصد التهديدات والاستجابة لها، وتنظيم حملات توعية وتدريب للموظفين والجمهور حول مخاطر الأمن السيبراني وكيفية الوقاية منها.

بالإضافة إلى ذلك، تسعى الهيئات الحكومية إلى تعزيز التعاون الدولي في مجال الأمن السيبراني وتبادل الخبرات والمعلومات مع الدول الأخرى، وتعمل على دعم البحث والتطوير في مجال الأمن السيبراني لتطوير حلول مبتكرة لمواجهة التهديدات السيبرانية، وتساهم في حماية البنية التحتية الحيوية من الهجمات السيبرانية، وتعمل على حماية البيانات الشخصية للمواطنين من الاختراقات والتسريبات، وتعمل على تشجيع القطاع الخاص على تبني أفضل الممارسات في مجال الأمن السيبراني، ومنه، يتضح بأن تلك الهيئات تعمل على مراقبة وتنظيم الفضاء السيبراني لضمان استخدامه الآمن والمسؤول²⁶.

2.1. دور المؤسسات الأمنية في تحقيق الأمن السيبراني في الجزائر

تلعب المؤسسات الأمنية الجزائرية دورا حاسما في مكافحة الجرائم السيبرانية، من خلال رصد التهديدات، وتتبع المجرمين، وتقديم الدعم الفني للجهات المعنية، وتهدف الاستراتيجية الوطنية للأمن السيبراني في الجزائر إلى حماية البنية التحتية الرقمية الحيوية، وتعزيز الوعي بالأمن السيبراني، وتطوير القدرات الوطنية في هذا المجال، كما تتضمن الاستراتيجية، مجموعة من المبادرات والبرامج الحكومية، بالإضافة إلى التعاون الدولي مع الدول والمنظمات الأخرى.

ومن أجل تحقيق الأمن السيبراني في كافة القطاعات الحساسة، تضطلع المؤسسات الأمنية بتحقيق ذلك خصوصا في ظل التطورات التكنولوجية المتسارعة والتهديدات المتزايدة، تتجلى في فرض آليات وقائية ويمكن أن تفرض في شكل إجراءات المتابعة القضائية، بالاستناد على أطر قانونية ومؤسسية، أين تقوم هذه الأخيرة وفي مقدمتها الدرك الوطني الجزائري والمديرية العامة للأمن الوطني²⁷، بمهام حيوية في مراقبة الفضاء السيبراني بشكل مستمر، بهدف رصد أي أنشطة مشبوهة وكشفها، بما في ذلك محاولات القرصنة، نشر البرمجيات الخبيثة، هجمات التصيد الاحتيالي، وغيرها من الجرائم السيبرانية التي قد تستهدف الأفراد أو المرافق الحيوية للدولة، وعند ثبوت وقوع أي حادث سيبراني، تتولى هذه الأجهزة مهمة الاستجابة السريعة، بهدف احتواء الضرر، استعادة الأنظمة المتضررة، وتحليل طبيعة الهجوم لتحديد مصدره، الأمر الذي يتطلب تكاتف بين فرق متخصصة للتعامل مع الطوارئ السيبرانية بفعالية²⁸.

إضافة إلى ذلك، تلعب المؤسسات الأمنية دور هام أمام ما يعرف بعملية التحقيق الجنائي الرقمي ومتابعة المجرمين، فعند ضبط أي جريمة إلكترونية، يتم جمع الأدلة الرقمية وتحليلها بدقة لتحديد هوية مرتكبي الجريمة وتقديمهم للعدالة، كما تساهم المؤسسات الأمنية بشكل فعال في تأمين البنية التحتية الحيوية للبلاد، بالتعاون مع القطاعات المختلفة كقطاع الطاقة، وقطاع الاتصالات الإلكترونية، وقطاع المالية، من خلال آلية التشاور وإجراء عمليات التدقيق السيبراني، كما لا يقتصر دور تلك المؤسسات على الجانب العملي فحسب، بل يمتد ليشمل الجانب التوعوي، عندما تشارك في حملات توعية موجهة لأفراد المجتمع والمؤسسات، بغية رفع مستوى الوعي بمخاطر الفضاء السيبراني وكيفية الحماية منها بأقل الأضرار.

وفي هذا الإطار، يبرز دور الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، التي جاء بها المرسوم الرئاسي رقم 19/ 172 سالف الذكر، حيث تعتبر بمثابة حجر الزاوية في التنسيق الاستراتيجي، بين جميع الفاعلين - بمن فيهم المؤسسات الأمنية - والمساهمة في بناء القدرات الوطنية في هذا المجال، أما بالنسبة للجيش الوطني الشعبي، فيلعب دور أيضا في حماية البنية التحتية الدفاعية والاستراتيجية للدولة، ولديه وحدات متخصصة في الدفاع السيبراني، تضمن أمن المعلومات والشبكات العسكرية الحيوية.

وأقل ما يقال في هذا الصدد، أن التكامل بين الأدوار العملية للدرك والشرطة، والدور الاستراتيجي للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، والدور الدفاعي للجيش، يمثل ركيزة أساسية لتحقيق الأمن السيبراني الشامل في الجزائر، ويسهم في حماية الفضاء الرقمي الوطني من مختلف التهديدات المتطورة، مما يدعم استقرار البلاد ونموها في العصر الرقمي.

2. المواجهة القانونية لاستغلال الذكاء الاصطناعي لأغراض غير مشروعة في التشريع الجزائري

- تواجه الجزائر العديد من التحديات في مجال الأمن السيبراني، مثل نقص الكفاءات المتخصصة، وتطور الجرائم السيبرانية، وصعوبة تتبع المجرمين عبر الحدود، وذلك بسبب التطور السريع للتكنولوجيا والاعتماد المتزايد على الإنترنت في مختلف جوانب الحياة، ومن أهم هذه التحديات:
- نقص الوعي: لا يزال الوعي بمخاطر الأمن السيبراني منخفضا لدى العديد من الأفراد والمؤسسات في الجزائر، مما يجعلهم عرضة للهجمات الإلكترونية.
 - ضعف البنية التحتية: تعاني البنية التحتية للأمن السيبراني في الجزائر من بعض الثغرات، مما يجعلها غير قادرة على مواجهة الهجمات الإلكترونية المتطورة.
 - قلة الكوادر المتخصصة: هناك نقص في الكوادر المتخصصة في مجال الأمن السيبراني في الجزائر، مما يعيق جهود التصدي للهجمات الإلكترونية.
 - تطور الجريمة الإلكترونية: تشهد الجريمة الإلكترونية تطور مستمر، مما يجعل من الصعب على الجهات المعنية مواكبة هذه التطورات والتصدي لها.
 - التهديدات الخارجية: تواجه الجزائر تهديدات سيبرانية خارجية من دول ومنظمات تسعى إلى استهداف مصالحها الحيوية، بالإضافة إلى هذه التحديات، تواجه الجزائر أيضا تحديات أخرى مثل:
 - صعوبة تطبيق القوانين: تواجه الجزائر صعوبة في تطبيق القوانين المتعلقة بالأمن السيبراني، وذلك بسبب نقص الإمكانيات والخبرات.
 - غياب التعاون الدولي: هناك حاجة إلى تعزيز التعاون الدولي في مجال الأمن السيبراني، وذلك لمواجهة التهديدات العابرة للحدود.²⁹

تسعى الجزائر إلى مواجهة هذه التحديات من خلال اتخاذ مجموعة من الإجراءات، مثل:

- إعداد استراتيجية وطنية للأمن السيبراني.
 - إنشاء هيئة وطنية للأمن السيبراني.
 - تطوير البنية التحتية للأمن السيبراني.
 - تأهيل الكوادر المتخصصة في مجال الأمن السيبراني.
 - تعزيز الوعي بمخاطر الأمن السيبراني.
- أما بخصوص جريمة الاستخدام غير المشروع للذكاء الاصطناعي في التجربة الجزائرية، يلاحظ عدم وجود قوانين خاصة تعالج بشكل مباشر المسؤولية الجنائية والمدنية المترتبة عنها، على الرغم من لجوء القضاة إلى قوانين أخرى يتم من خلالها تكييف هذه الجرائم، كقانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الذي جسد جرم الأفعال المرتكبة عبر الأنظمة المعلوماتية، وقام بتكييف الجرائم المرتكبة عبر الذكاء الاصطناعي مثل الاحتيال المتقدم، أو التخريب السيبراني، واعتبر نظام الذكاء الاصطناعي مجرد آلية متطورة يستخدمها الجاني لتحقيق الفعل المجرم.

في المقابل، أصدر المشرع الجزائري قانون حماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، من أجل معالجة أي انتهاك للخصوصية أو سوء استخدام للبيانات الشخصية، بما في ذلك الأضرار الناتجة عن تحليل الذكاء الاصطناعي لكميات ضخمة من البيانات، دون إغفال القواعد العامة الواردة في نصوص القانون المدني والمرتبطة بقواعد المسؤولية، وإن كانت تطرح إشكالية تتعلق بالمسؤولية المدنية الناتجة عن الأضرار التي تسببها الأنظمة الذكية، رغم محاولات الفقه القانوني في تكيف هذه المسؤولية بناء على قواعد المسؤولية عن فعل الأشياء أو المسؤولية عن المنتج المعيب، لكن هذه التكييفات تبقى محل خلاف لعدم استيعابها، لاستقلالية قرار الذكاء الاصطناعي.

الخاتمة

أقل ما يقال عن موضوع دور الأمن السيبراني في حماية الخصوصية من مخاطر الذكاء الاصطناعي، هو أن الأمن السيبراني يكتسي أهمية بالغة في حماية اقتصادنا الرقمي ومجتمعنا من التهديدات المتزايدة، خاصة وأن الجرائم السيبرانية جرائم يصعب التحكم فيها والتصدي لها نظرا لخصوصيتها باعتبارها جرائم عابرة للجغرافيا، وأيضا باعتبار أن التطور المذهل في الجانب التكنولوجي والالكتروني والرقمي صعب هو الآخر من مهمة مكافحة هذه الجريمة، وباعتبار أن الدولة كعضو في المجتمع الدولي لا تستطيع بمفرها مواجهة مثل هذه التحديات الصعبة، وعلى الرغم من تكاتف دول العالم في شكل اتحادات جهوية وإقليمية وعالمية للتصدي لهذه الجرائم السيبرانية إلا أن التحدي كان أكبر، والخسائر في ارتفاع مستمر سواء على المستوى القيمي أو الشخصي، أو مختلف الخسائر الاقتصادية والتجارية الناجمة عن الأضرار التي تمس بخاصة اقتصاديات دول العالم.

وعلى الرغم من أن المشرع الجزائري أسس منظومة تشريعية ومؤسسية للتصدي لمثل هذه الجرائم، إلا أن الظاهرة في انتشار مخيف، خاصة بسبب نقص التكوين وآليات التصدي لها، زد على ذلك تطور وسائل الإجرام بسبب تطور الآليات الالكترونية والرقمية، حيث يتضح عدم وجود استقرار على مفهوم واحد للجرائم السيبرانية، ولعل السبب في ذلك يعود الى امكانية ظهور جرائم جديدة متصلة بالعالم الافتراضي، وتدخل في نطاق هذه الجرائم.

كما استحدث المشرع الجزائري قوانين تدعم مكافحة الجرائم السيبرانية أهمها القانون رقم 18-04 المحدد للقواعد العامة المتعلقة بالبريد والاتصالات الالكترونية، والقانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، ولعل ذلك يعد قفزة نوعية في مجال مكافحة الجرائم السيبرانية.

أما عن التوصيات المقترحة في هذا الصدد، فنذكر:

- تعديل القوانين مثل قانون العقوبات والقوانين المتعلقة بالجرائم الإلكترونية، وجعلها مواكبة لآخر التطورات التكنولوجية وأنماط الجرائم السيبرانية المستحدثة.

- ضمان التطبيق الفعال للمرسوم الرئاسي رقم 172/19 الخاص بالهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، وتزويدها بالموارد البشرية والتقنية الكافية.
 - العمل على صياغة وتطبيق قانون شامل لحماية البيانات الشخصية يتماشى مع المعايير الدولية، مثل GDPR، لضمان حقوق الأفراد في التحكم ببياناتهم ومعاقبة المخالفين بصرامة.
 - إنشاء فرق استجابة للطوارئ السيبرانية (CSIRTs/CERTs) قطاعية، تتجسد في فرق متخصصة، للاستجابة للحوادث السيبرانية داخل كل قطاع حيوي، مع التنسيق المركزي مع الهيئة الوطنية.
 - تزويد المؤسسات الأمنية والقطاعات الحيوية بأحدث التقنيات والأدوات الأمنية، مثل أنظمة كشف التسلل، أنظمة إدارة المعلومات والأحداث الأمنية SIEM، منصات الاستخبارات التهديدية.
- الهوامش:**

¹ Cameron S. D. Brown, "Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice", International Journal of Cyber Criminology. Vol 9, Issue 1, January – June 2015, p57.

² Dan Craigen, Nadia Diakun-Thibault, and Randy Purse, Defining Cybersecurity. Technology Innovation Management Review, October 2014, pp 14-15.

³ Douwe Korff, CYBER SECURITY DEFINITIONS – a selection. P1, in: <https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/CPDP%202015%20-%20KORFF%20Handout.pdf>

⁴ القانون 04-09، المؤرخ في 05 أوت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج. ر. عدد 47، الصادرة بتاريخ 16 سبتمبر 2009، ص 8.

⁵ القانون رقم 07-18، المؤرخ في 10 جوان 2018، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، ج. ر. عدد 34، الصادرة بتاريخ 10 جوان 2018، ص 11.

⁶ الشوابكة محمد أمين: جرائم الحاسوب والانترنت، دار الثقافة للنشر والتوزيع، عمان، 2011، ص 23.

⁷ زيدان زبيحة: الجريمة المعلوماتية في التشريع الجزائري، دار الهدى، الجزائر، 2011، ص 89.

⁸ متولي القاضي رامي: مكافحة الجرائم المعلوماتية، دار النهضة العربية، مصر، 2011، ص 66.

⁹ عفيفي صادق أحمد طارق: الجرائم الالكترونية جرائم الهاتف المحمول، المركز القومي للإصدارات القانونية، القاهرة مصر، 2015، ص 56.

¹⁰ L'article 2 (h) de la directive n°95/46 définit le consentement comme « toute manifestation de volonté, libre, spécifique et informée par laquelle une personne concernée accepte que des données à caractère personnel la concernant fassent l'objet d'un traitement ».

¹¹ Matheus M. Hoscheidt, Elisa Felber Eichner, LEGAL AND POLITICAL MEASURES TO ADDRESS CYBERCRIME, United Nations: UFRGSMUN UFRGS Model, v.2, 2014, p 446.

¹² القانون رقم 15-04، المؤرخ في 10 نوفمبر 2004، يعدل ويتمم الأمر رقم 66-156، المتضمن قانون العقوبات، ج. ر. عدد 74، ص 12.

¹³ نبيلة هبة هروال: جرائم الانترنت دراسة مقارنة، أطروحة دكتوراة، كلية الحقوق والعلوم السياسية، جامعة أبي بكر بلقايد، تلمسان، 2013، ص 97.

¹⁴ مناصرة يوسف: جرائم المساس بأنظمة المعالجة الآلية للمعطيات، دار الخلدونية، الجزائر، 2018، ص 77.

¹⁵ قانون المرونة السيبرانية (Cyber Resilience Act - CRA) : مقترح تشريعي أوروبي في إطار المصادقة عليه كي يصبح قانون ساري المفعول، بمقتضاه تم اقتراح وضع متطلبات أمنية إلزامية لمنتجات الأجهزة والبرامج المتصلة بالإنترنت، بما في ذلك أجهزة

- إنترنت الأشياء طوال دورة حياتها، سيطلب أيضا من الشركات المصنعة ضمان أمن هذه المنتجات من التصميم وحتى ما بعد البيع، مع معالجة الثغرات الأمنية بشكل استباقي.
- ¹⁶ أنظر المادة 372 القانون رقم 04-15، المتعلق بالعقوبات، مصدر سبق ذكره.
- ¹⁷ القانون رقم 09-04، متضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، مصدر سبق ذكره.
- ¹⁸ الأمر رقم 03-07، المؤرخ في 19 جويلية 2003، يتعلق ببراءات الاختراع، ج. ر. عدد 44، الصادرة بتاريخ 23 جويلية 2003، ص 27.
- ¹⁹ أنظر في ذلك القانون رقم 18-07، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، مصدر سبق ذكره.
- ²⁰ الأمر رقم 03-06، المؤرخ في 19 جويلية 2003، يتعلق بالعلامات، ج. ر. عدد 44، الصادرة بتاريخ 23 جويلية 2003، ص 22.
- ²¹ القانون 18-04، المؤرخ في 10 ماي 2018، الذي يحدد القواعد العامة المتعلقة بالبريد والاتصالات الالكترونية، ج. ر. عدد 27، الصادرة بتاريخ 13 ماي 2018، ص 03.
- ²² بن خليفة أحمد وحفظة الأمير عبد القادر: الجريمة الالكترونية وآليات التصدي لها، مجلة الامتياز لبحوث الاقتصاد والإدارة، الأغواط، المجلد 01، العدد 01، 2017، ص 156.
- ²³ الديوان الوطني للأمن السيبراني يشرف على التنسيق الوطني في مجالات الدفاع السيبراني والتعاون الدولي، متاح على الرابط التالي: https://www.mdn.dz/site_principal، تاريخ الاطلاع (01-06-2025)، على الساعة (19:13).
- ²⁴ أنظر المادة 01 من القانون 09-04، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، مصدر سبق ذكره.
- ²⁵ أنظر المادة 01 من المرسوم الرئاسي رقم 19/172، المؤرخ في 06 جوان 2019، يحدد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها وتنظيمها وكيفية سيرها، ج. ر. عدد 37، الصادرة بتاريخ 09 جوان 2019، ص 05.
- ²⁶ الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، المحررة بالقاهرة بتاريخ 21 ديسمبر 2010، المصادق عليها من طرف الجزائر بموجب مرسوم رئاسي رقم 14-252 الموافق ل 8 سبتمبر 2014 ج. ر. عدد 57، الصادرة بتاريخ 28 سبتمبر 2014.
- ²⁷ بارة سميرة: الأمن السيبراني في الجزائر: السياسات والمؤسسات، المجلة الجزائرية للأمن الانساني، باتنة، المجلد 02، العدد 04، 2017، ص 262.
- ²⁸ كلاع شريفة: السيبراني الأمن السيبراني وتحديات الجوسسة واختراق الدخول الإلكتروني للدول عبر الفضاء السيبراني الأمن السيبراني وتحديات التجسس واختراق الدول عبر الفضاء السيبراني، مجلة الحقوق والعلوم الانسانية، الجلفة، المجلد 15، العدد 01، 2022، ص 300.
- ²⁹ الأسدي لينا: مدى فاعلية احكام القانون الجنائي في مكافحة الجريمة المعلوماتية، دار حامد للنشر والتوزيع، عمان، 2015، ص 62.