



وزارة التعليم العالي والبحث العلمي
Ministry of Higher Education and Scientific Research
جامعة وهران 1- أحمد بن بلة
معهد علم الإجرام
University of Oran1 – Ahmed Ben Bella –
Institute of Criminology



مذكرة

لنيل شهادة ماستر

تحت عنوان

الجرائم السيبرانية ومكافحتها في الجزائر

الشعبة

..... حقوق

التخصص

..... علم الجريمة

تحت إشراف الأستاذ: حساين محمد

من إعداد الطالب: شريف محمد

لجنة المناقشة

الاسم واللقب	الصفة	المؤسسة
فيصل شرارة	رئيسا	جامعة وهران 1 أحمد بن بلة
حساين محمد	مشرفا	جامعة مستغانم
هزيل جلول	مناقشا	جامعة وهران 1 أحمد بن بلة

السنة الجامعية: 2025 / 2026

إهداء

إلى كل من آمن بأن البحث العلمي ليس ترفاً، بل مسؤولية أخلاقية وقانونية تجاه المجتمع. إلى الأسرة التي تمنح الباحث صبره

إلى من أناروا دربي بالعلم والمعرفة...

إلى الأساتذة الذين يفتحون أمام الطالب أبواب السؤال والنقد

إلى من علّمونا أن القانون درع الحضارة وحارس العدالة...

إلى كل من يؤمن بأن الفضاء الرقمي يستحق حماية حقيقية...

وإلى كل طالب قانون يؤمن أن النصوص لا تكفي وحدها، وأن العدالة تحتاج إلى معرفة دقيقة بالواقع الذي تطبق فيه.

إلى كل ضحايا الجرائم السيبرانية الذين ينتظرون من القانون الإنصاف ، أولئك من وجدوا أنفسهم أمام خطر لا يرى بالعين لكنه يترك أثراً عميقاً في الحياة الخاصة والكرامة والأمن.

إلى كل من يسعى إلى جعل الفضاء الرقمي مجالاً آمناً للحقوق والحريات والمعاملات، .

أهدي هذا العمل المتواضع.

شكر وعرفان

الحمد لله الذي وفقنا لإتمام هذا العمل، والصلاة والسلام على أشرف المرسلين.

نتقدم بجزيل الشكر والامتنان إلى الأستاذ المشرف على هذه المذكرة، على ما أولانا إياه من توجيهات علمية قيّمة وصبر جميل طوال مراحل إعداد هذا البحث.

كما نتوجه بالشكر الجزيل إلى أعضاء لجنة المناقشة الموقرين على تفضلهم بقبول مناقشة هذه المذكرة وإثرائها بملاحظاتهم القيّمة.

والشكر موصول لأساتذة معهد علم الإجرام الذين لم ييخلوا علينا بتوجيهاتهم طوال مسيرتنا الدراسية، وإلى كل من أسهم من قريب أو بعيد في إنجاز هذا العمل

كما أتوجه بالشكر إلى كل المؤسسات العلمية والقانونية التي تتيح النصوص والمراجع للباحثين، لأن إتاحة المعرفة القانونية شرط من شروط جودة البحث الأكاديمي وترقية النقاش العام حول الأمن السيبراني وحماية الحقوق الرقمية.

ملخص:

شهد المجتمع الدولي في الآونة الأخيرة طفرة تكنولوجية هائلة أحدثت تحولات جذرية على كافة الأصعدة الاقتصادية، الاجتماعية، والثقافية؛ حيث انتقلت المجتمعات من الأنماط التقليدية إلى عصر "المجتمعات الرقمية السيبرانية". وبفضل ما وفرتة التكنولوجيا الحديثة من خدمات رقمية تميزت بالسرعة الفائقة، الدقة المتناهية، وانخفاض التكلفة، تحققت قفزة نوعية في المردودية الإدارية والاقتصادية. ورغم هذه الإيجابيات المتعددة، إلا أن الثورة الرقمية حملت في طياتها تحديات أمنية وهواجس مقلقة تجسدت في ظهور نمط إجرامي مستحدث يُعرف بـ "الجرائم السيبرانية". ونظرًا للطبيعة الخاصة والخطيرة لهذه الجرائم باعتبارها ظاهرة عابرة للحدود الوطنية وتتجاوز القيود الجغرافية، لم تكن الجزائر بمعزل عن تبعاتها؛ إذ سجلت التقارير الأمنية والدراسات العلمية ارتفاعاً ملحوظاً في مؤشرات الإجرام المعلوماتي خلال السنوات الأخيرة. هذا الوضع الدقيق دفع المشرع الجزائري إلى التدخل العاجل عبر سن ترسانة قانونية وتدابير تشريعية مستحدثة تهدف إلى مكافحة هذه الظاهرة، حماية الفضاء الرقمي، وتأمين المعاملات الإلكترونية.

الكلمات المفتاحية: الجريمة السيبرانية، المجتمعات الرقمية، التكنولوجيا الحديثة، الجريمة العابرة للحدود، التشريع الجزائري.

Abstract

Recently, the international community has witnessed profound transformations across economic, social, cultural, and digital spectrums. Driven by rapid, cost-effective, and highly precise technologies, contemporary societies have fundamentally transitioned into electronic and cyber realities. Concurrently, while this digital paradigm shift offers unprecedented efficiency, it has generated sophisticated security threats, most notably cybercrime. Given the intricate, borderless nature of these offenses, Algeria has recorded a substantial surge in cybercrime indices, as substantiated by recent security and empirical reports. Consequently, the Algerian legislator has proactively intervened by promulgating a robust legal framework dedicated to suppressing cyber threats and safeguarding cyberspace.

Keywords: Cybercrime, Digital Societies, Advanced Technology, Transnational Crime, Algerian Legislation.

قائمة المختصرات

ج.ر.ج.ج: الجريدة الرسمية للجمهورية الجزائرية

ق.ع.ج: قانون العقوبات الجزائري

ق.إ.ج.ج: قانون الإجراءات الجزائية الجزائري

ق.04-09: القانون رقم 04-09 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال

STAD : منظومة المعالجة الآلية للمعطيات (Système de Traitement Automatisé de Données)

ASSI : وكالة أمن الأنظمة المعلوماتية (Agence de Sécurité des Systèmes d'Information)

DGSN : المديرية العامة للأمن الوطني (Direction Générale de la Sûreté Nationale)

CERT-DZ: الفريق الجزائري للاستجابة لحالات الطوارئ الحاسوبية

NSISS: الاستراتيجية الوطنية لأمن الأنظمة المعلوماتية (National Strategy for Information Systems Security)

ITU : الاتحاد الدولي للاتصالات (International Telecommunication Union)

UNODC : مكتب الأمم المتحدة المعني بالمخدرات والجريمة

INTERPOL : المنظمة الدولية للشرطة الجنائية

IP : بروتوكول الإنترنت (Internet Protocol)

HTTPS : بروتوكول نقل النص التشعبي الآمن

VPN : الشبكة الافتراضية الخاصة (Virtual Private Network)

AI : الذكاء الاصطناعي (Artificial Intelligence)

IoT : إنترنت الأشياء (Internet of Things)

مقدمة:

شهد العالم في العقود الأخيرة ثورة تكنولوجية معلوماتية غير مسبوقة، أحدثت تحولات جذرية في مختلف جوانب الحياة الإنسانية؛ إذ باتت شبكة الإنترنت وتقنيات الاتصال الحديثة جزءاً لا يتجزأ من النسيج الاجتماعي والاقتصادي والسياسي للمجتمعات المعاصرة. وإن كانت هذه الثورة الرقمية قد فتحت آفاقاً رحبة للتواصل والتجارة والمعرفة، فإنها بالمقابل أفرزت تحديات أمنية وقانونية بالغة الخطورة، تمثل أبرزها في ظاهرة الجرائم السيبرانية التي تتسم بالخفاء والتطور المستمر وكونها عابرة للحدود.

وتُعدّ الجريمة السيبرانية من أخطر التهديدات الأمنية التي تواجهها الدول في القرن الحادي والعشرين، لما تتميز به من خصائص تجعل مواجهتها أمراً عسيراً؛ فهي جريمة لا حدود لها تتخطى السيادة الوطنية وتُنجز في أجزاء من الثانية، ولا تتطلب من مرتكبيها التواجد الجسدي في مكان الجريمة. فضلاً عن ذلك، فإن ضحاياها يمتدون من الأفراد العاديين إلى المؤسسات الحكومية والبنى التحتية الحيوية للدول، مما يجعلها تهديداً وجودياً للأمن القومي والأمن الشخصي معاً.

لقد أصبحت هذه الجرائم إحدى أهم الهواجس التي أصبحت تؤرق المواطن في حياته الشخصية، والدول في سيادتها وأمنها، باعتبار أن التطور التكنولوجي والرقمي الهائل وما صاحبه من تأثير على كل المستويات أثر بشكل أو بآخر على أمن واستقرار الشعوب من جهة بل وأصبحت تداعيات هذه الثورة التكنولوجية تمس حرمة وخصوصية المواطن من جهة أخرى و في ظل هذا التحدي الرقمي التكنولوجي الجديد سعت الدول إلى سن حزمة من التشريعات والآليات القانونية والمؤسسية للتصدي لهذه الجريمة التي أضحت تسمى في الأدبيات الأكاديمية بالجريمة الإلكترونية أو الجريمة السيبرانية.

وعلى الصعيد الوطني، لم تكن الجزائر بمعزل عن هذه الظاهرة العالمية، بل إن التطور التكنولوجي المتسارع الذي شهده قطاع الاتصالات الجزائري خلال العقود الماضية، ولا سيما الانتشار الواسع لشبكة الإنترنت والهواتف الذكية، قد أدى إلى تنامي ملحوظ في معدلات الجرائم الإلكترونية. فقد كشفت إحصائيات المديرية العامة للأمن الوطني عن تسجيل آلاف

القضايا السيبرانية سنوياً، في تصاعد متواصل يعكس خطورة هذه الظاهرة وضرورة التصدي لها بمنظومة قانونية وأمنية فعّالة.

في السياق الجزائري، يتجلى أثر هذا التحول الرقمي في التزايد الملحوظ للجرائم السيبرانية، مما يضع المجتمع والقضاء أمام مسؤوليات جسيمة. إن التوسع في الخدمات الرقمية، مثل التجارة الإلكترونية والخدمات المصرفية عبر الإنترنت، يزيد من مساحة التعرض للخطر، ويجعل من الضروري إيجاد إطار قانوني جنائي يستجيب لهذه التحديات. إن الحاجة إلى قانون جنائي رقمي متوازن، يراعي خصوصية هذه الجرائم ويحقق التوازن بين حماية الحقوق والحريات الرقمية وتوفير الأمن السيبراني، أصبحت ملحة أكثر من أي وقت مضى.

وقد استجابت الجزائر لهذا التحدي بإصدار منظومة تشريعية متخصصة، تجلّت أساساً في القانون رقم 04-09 المؤرخ في 5 أغسطس 2009، المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها¹، والتعديلات التي أدخلت على قانون العقوبات² في هذا الشأن. كما أنشأت هيئات متخصصة للتصدي لهذه الجرائم، وانخرطت في منظومة التعاون الدولي لمواجهة خطرها العابر للحدود.

إن التحدي لا يقتصر على سن تشريعات جديدة، بل يتعداه إلى ضرورة تكييف وتحديث النصوص القانونية القائمة، مثل قانون العقوبات وقوانين مكافحة الجريمة المنظمة، لتشمل الأفعال المجرمة في الفضاء الرقمي³. كما أن تفعيل آليات التعاون الدولي، وتبادل المعلومات، وتطوير القدرات التقنية لدى الجهات المكلفة بإنفاذ القانون، يمثل ركيزة أساسية في استراتيجية مكافحة الجرائم السيبرانية. إن هذا التوجه نحو قانون جنائي رقمي متكامل يعكس إدراكاً متزايداً لضرورة حماية الفضاء الرقمي.

وبالتالي، فإن التحول الرقمي في الجزائر، رغم فوائده الجمة، قد أفرز بيئة قانونية وجنائية معقدة تستدعي مقارنة شاملة. إن تطوير قانون جنائي رقمي متوازن، قادر على مواجهة

¹ ق. 04-09: القانون رقم 04-09 المؤرخ في 5 أغسطس 2009، المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، الجريدة الرسمية عدد 47 سنة 2009

² قانون العقوبات: الأمر رقم 66-156 المؤرخ في 8 يونيو سنة 1966 المعدل والمتمم بالقانون 06-24 المؤرخ في 28/04/2024

³ وثيقة وزارة العدل: مستندات قانون العقوبات لسنة 2024. متاح على الرابط: <https://www.mjustice.gov.dz>

التحديات المستجدة، يتطلب تضافر الجهود التشريعية والتنفيذية والتقنية، مع الأخذ في الاعتبار مبادئ العدالة والفعالية، لضمان بيئة رقمية آمنة وموثوقة للمواطنين والشركات.

وبذلك يتضح أن محور "السياق العام للتحويل الرقمي" لا ينفصل عن البناء العام للدراسة، لأنه يربط بين تحديد السلوك محل التجريم، وضمانات التطبيق، ومتطلبات الوقاية المؤسسية. وتبقى القيمة التحليلية لهذا المحور في قياس قدرة القاعدة القانونية على إنتاج حماية عملية، لا في الاكتفاء بتأكيد وجود النص.

وتستمد هذه الدراسة أهميتها من الحجم المتنامي للجريمة السيبرانية في الجزائر وعلى المستوى العالمي، إذ تشير الإحصائيات إلى أن الخسائر الاقتصادية الناجمة عن الجرائم الإلكترونية على المستوى الدولي تتجاوز تريليونات الدولارات سنوياً. كما تتجلى أهميتها في الحاجة الماسة إلى تقييم مدى كفاءة المنظومة القانونية الجزائرية في التعامل مع هذه الجرائم المستحدثة، واقتراح سبل تطويرها.

أولاً: أهمية الموضوع

تكتسي دراسة الجرائم السيبرانية ومكافحتها في البيئة الجزائرية أهمية بالغة نظراً للتطور المتسارع للإدارة الرقمية في مختلف قطاعات الدولة. فمع انتقال الخدمات العمومية إلى الفضاء الرقمي، تزداد الحاجة الملحة لفهم التحديات الأمنية المرتبطة بهذه التحولات، بما في ذلك مخاطر استهداف البنية التحتية الرقمية للدولة أو تعطيل الخدمات الأساسية، مما يضع على عاتق الباحث الجزائري مهمة استكشاف الثغرات التشريعية والتنظيمية القائمة.

إن تغلغل التكنولوجيا الرقمية في عمل المؤسسات العمومية الجزائرية، من الإدارة المباشرة للمواطنين إلى تسيير المصالح الحساسة، يبرز الجانب العملي لأهمية هذا الموضوع، إذ أن أي اختراق أو هجوم على هذه المنصات قد يؤدي إلى عواقب وخيمة، ليس فقط على مستوى البيانات والمعلومات، بل أيضاً على ثقة المواطن في قدرة الدولة على حماية أصوله الرقمية. يتطلب هذا الوضع تقييماً دقيقاً لمدى فعالية الإجراءات الوقائية والتصديقية المتبعة حالياً

علاوة على ذلك، تبرز أهمية البحث في الجرائم السيبرانية من منظور حماية الأفراد في الجزائر. فالإنترنت، رغم فوائده، أصبح مسرحاً لممارسات إجرامية تستهدف الأفراد بشكل

مباشر، كجرائم الابتزاز الإلكتروني والتشهير والاعتداء على الخصوصية. إن تزايد هذه الظواهر يفرض على الباحث الجزائري ضرورة تسليط الضوء على آليات الحماية القانونية المتاحة، وتقييم كفايتها في ظل التطور المستمر لأساليب المجرمين السيبرانيين

يتطلب تحليلنا الوقوف على التحديات التي تواجه الإطار القانوني الجزائري في التصدي للجرائم السيبرانية، خاصة في ظل وجود نصوص متناثرة وغير متكاملة في بعض الأحيان، مثل قانون 04-09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها ، و تعزيز الحماية الجزائية في الخصوصية المعلوماتية في قانون العقوبات المعدل بالقانون 06-24 الصادر في 28 افريل 2024، بالإضافة إلى قانون الإجراءات الجزائية الجديد 14-25 الصادر في 03 أوت 2025 ، فهل هذه النصوص كافية لمواجهة التهديدات الجديدة؟

إن تقييم مدى فعالية الأدوات القانونية والمؤسسية المكرسة لمكافحة الجرائم السيبرانية في الجزائر، بما في ذلك دور وحدات مكافحة الجرائم المعلوماتية والشرطة التقنية، يمثل جانباً حيوياً لأهمية الموضوع. يتوجب على الباحث استكشاف مدى التنسيق بين هذه الجهات، وتقييم كفاءة الإجراءات المتبعة في جمع الأدلة الرقمية وضمان نجاح المتابعات القضائية، مع الأخذ في الاعتبار التطورات التشريعية اللاحقة .

تكتسب دراسة الجرائم السيبرانية ومكافحتها في الجزائر أهمية نظرية وعملية بالغة تتجلى في :

على الصعيد النظري: تُسهم هذه الدراسة في تأصيل المفاهيم القانونية للجريمة السيبرانية وتحديد ماهيتها وأركانها وفقاً للفقهاء الجزائري والمقارن، كما تُعنى بتحليل النصوص التشريعية الجزائرية النازمة لهذه الجرائم وبيان مدى استيعابها لمتطلبات مكافحة الجريمة الرقمية في ظل التطور التكنولوجي المتسارع.

على الصعيد العملي: تكتسب هذه الدراسة أهمية قصوى بالنظر إلى التزايد المضطرد لحوادث الجريمة السيبرانية في الجزائر، مما يجعل الحاجة ماسة إلى وضع تصورات واضحة

للممارسين القانونيين وصانعي القرار السياسي بشأن آليات التصدي الفعّال لهذه الظاهرة الإجرامية المستحدثة.

ثانياً: أسباب اختيار الموضوع

دفعتنا جملة من الأسباب الموضوعية والذاتية إلى اختيار هذا الموضوع للدراسة والبحث، يمكن إجمالها فيما يلي:

تتجلى الأسباب الذاتية لاختيار موضوع الجرائم السيبرانية ومكافحتها في الجزائر في الاهتمام الشخصي بمجال القانون الجنائي الرقمي والأمن السيبراني باعتبارهما من أبرز التخصصات القانونية الناشئة والمطلوبة في سوق العمل الجزائري والعربي ، وإدراكي المتزايد لخطورة الظاهرة وتأثيرها المتنامي على الأفراد والمجتمع والدولة، مما دفعني إلى التعمق في فهم طبيعتها القانونية والتحديات التي تفرضها على المنظومة التشريعية الجزائرية.

كما إن الرغبة في المساهمة، ولو باليسير، في سد الفجوة المعرفية وتوفير تحليل قانوني دقيق لهذا النوع المستجد من الجريمة، شكلت دافعاً أساسياً لهذا البحث.

أما الأسباب الموضوعية، فتنبثق من الواقع المتغير والمستجدات التكنولوجية المتسارعة التي جعلت من الفضاء السيبراني مسرحاً لعدد الأنشطة، الإجرامية منها وغير الإجرامية. فالتطور الرقمي غير المسبوق، والذي انعكس على كافة جوانب الحياة، أوجد بيئة خصبة لنشوء أشكال جديدة من الاعتداءات التي تتطلب استجابة قانونية ، إضافة إلى حداثة الموضوع وشح الدراسات الأكاديمية المتخصصة في الجانب الجزائري منه، فضلاً عن الحاجة الملحة لدراسة مدى كفاءة المنظومة التشريعية الجزائرية في مواكبة مستجدات الجريمة السيبرانية، ولا سيما في ظل التطور التقني المتسارع في مجال الذكاء الاصطناعي وتقنية البلوك تشين.

ثالثاً: إشكالية البحث

تتمحور إشكالية هذه الدراسة حول التساؤل الجوهرية الآتي:

"إلى أي مدى نجح المشرع الجزائري في بناء منظومة قانونية وأمنية كافية ومتكاملة لمواجهة الجرائم السيبرانية ومكافحتها بفعالية في ظل التحديات التكنولوجية المتجددة؟"
وتتفرع عن هذه الإشكالية الرئيسية جملة من التساؤلات الفرعية، أبرزها:

ما المقصود بالجريمة السيبرانية وما هي خصائصها المميّزة في ضوء الفقه والتشريع الجزائري والمقارن؟

ما هي الأحكام الموضوعية والإجرائية التي أرساها القانون 04-09 وقانون العقوبات لمواجهة الجرائم الإلكترونية؟
ما هي الهيئات المتخصصة التي أنشأها المشرع الجزائري للتصدي لهذه الجرائم، وما مدى فعاليتها؟

■ ما هي التحديات التقنية والقانونية والإجرائية التي تعترض مكافحة الجرائم السيبرانية في الجزائر؟

■ كيف يمكن تطوير المنظومة الوطنية لمكافحة الجرائم السيبرانية في ضوء التجارب الدولية الناجحة؟

يكن جوهر الإشكالية في تحديد ما إذا كانت التدابير المتخذة، سواء على المستوى التشريعي أو التنفيذي، قادرة على تحقيق الردع المنشود ضد مرتكبي الجرائم السيبرانية، دون المساس بالحقوق الأساسية للأفراد في حرية التعبير والخصوصية الرقمية، يتطلب هذا مقارنة بين الإمكانيات المتاحة للسلطات القضائية، وصلاحياتها في مجال البحث والتحقيق، وبين الضمانات التي تكفلها هذه السلطات للمشتبه بهم والمجتمع ككل.

كما تتسع الإشكالية لتشمل تقييم مدى ملاءمة العقوبات المقررة في القانون الجزائري، بموجب قانون 04-09، مع الخطورة المتزايدة للجرائم السيبرانية، ومدى قدرتها على تحقيق الردع العام والخاص. يتطلب ذلك دراسة لكيفية تعامل القضاء الجزائري مع هذه القضايا.

في نهاية المطاف، تتمحور الإشكالية حول مدى قدرة الجزائر على بناء منظومة متكاملة وفعالة لمكافحة الجرائم السيبرانية، توازن بين الحاجة الملحة للأمن السيبراني والحفاظ على الحريات الرقمية. يتطلب هذا البحث مقارنة نقدية للواقع القانوني والتطبيقي، مع اقتراح حلول ممكنة لتعزيز فعالية هذه المنظومة، وسد الثغرات المحتملة، بما يتماشى مع التطورات التكنولوجية المستمرة والتحديات الدولية المتزايدة.

أهداف الدراسة:

- تسليط الضوء على مفهوم الجريمة السيبرانية وخصائصها وأشكالها المختلفة .
- تحليل الإطار القانوني الوطني لمكافحة الجرائم السيبرانية في الجزائر .
- تقييم الجهود والاتفاقيات الدولية الموجهة لمكافحة الإجرام السيبراني .
- إبراز النقائص والتحديات التي تواجه مكافحة الجريمة السيبرانية واقتراح حلول عملية.

رابعاً: منهج البحث

اعتمدنا في هذه الدراسة على جملة من المناهج العلمية المتكاملة التي تقتضيها طبيعة الموضوع، وذلك على النحو الآتي:

- المنهج التحليلي: وذلك من خلال تحليل النصوص القانونية الجزائرية المتعلقة بالجرائم الإلكترونية، وبيان محتواها وما تضمنته من أحكام موضوعية وإجرائية.
- المنهج المقارن: باللجوء إلى المقارنة بين المنظومة التشريعية الجزائرية ونظيراتها في بعض الدول العربية والغربية كفرنسا ومصر والمملكة العربية السعودية، للوقوف على أوجه التشابه والاختلاف واستيعاب أفضل الممارسات الدولية.

خامساً: حدود الدراسة وخطتها

تحدد هذه الدراسة نطاقها الزمني والمكاني والموضوعي بوضوح، بحيث تركز على تحليل الجرائم السيبرانية وتطورها في الجزائر، مع إيلاء اهتمام خاص للفترة الممتدة إلى غاية سنة 2026. إضافة إلى استقراء التطورات التشريعية والقضائية الراهنة والمستقبلية المتوقعة في هذا المجال، والأخذ بعين الاعتبار التحديات التي تفرضها التكنولوجيا المتسارعة.

مكانياً، تنحصر الدراسة في الإطار الوطني الجزائري، مستعرضة النصوص القانونية الوطنية ذات الصلة بتجريم هذه الأفعال ومعالجتها، ، بالإضافة إلى الأطر التنظيمية الأخرى كالمراسيم مع الإشارة إلى التطورات الدولية لفهم السياق الأوسع.

موضوعياً، تتناول الدراسة ماهية الجرائم السيبرانية، وأنواعها المختلفة، وخصائصها مقارنة بالجرائم التقليدية. و تحليل مدى كفاية المنظومة القانونية الجزائرية الحالية في مواجهة هذه

المستجدات، مع التركيز على آليات الضبط والتحقيق والمتابعة القضائية وتقييم فعالية الإجراءات الوقائية والردعية المعتمدة.

ثم التطرق إلى آليات التعاون الدولي في مجال مكافحة الجرائم السيبرانية، وذلك في سياق تزايد الطابع العابر للحدود لهذه الجرائم، و بحث دور الاتفاقيات الدولية والتعاون بين الأجهزة القضائية والأمنية للدول، بما في ذلك التعاون مع المنظمات الإقليمية والدولية، كآلية ضرورية لردع المعتدين ومعاقتهم.

في الختام، تهدف هذه الدراسة إلى تقديم تحليل نقدي للجهود المبذولة في الجزائر لمكافحة الجرائم السيبرانية، وتحديد الثغرات المحتملة في الإطار القانوني والتنظيمي. كما تسعى إلى اقتراح حلول وتوصيات عملية، تأخذ في الاعتبار التطورات المستقبلية المحتملة، لضمان فعالية أكبر في حماية الفضاء السيبراني الوطني.

ولإحاطة بجوانب الموضوع وإجابة إشكاليته، ارتأينا تقسيم هذه الدراسة إلى فصلين رئيسيين، يتضمن كل منهما مبحثين، يُعنى الفصل الأول بالإطار المفاهيمي والتشريعي للجريمة السيبرانية في الجزائر، فيما يتناول الفصل الثاني آليات مكافحة هذه الجرائم وتحديات التصدي لها مع استعراض المقاربات التطويرية.

الفصل الأول: ماهية الجريمة السيبرانية

المبحث الأول: مفهوم الجريمة السيبرانية

المبحث الثاني: الجرائم السيبرانية وفق ما جاء به التشريع الجزائري

الفصل الثاني: آليات مكافحة الجريمة السيبرانية في التشريع الجزائري

المبحث الأول: الحماية الموضوعية للنظام المعلوماتي

المبحث الثاني: الحماية الإجرائية للنظام المعلوماتي

الفصل الأول

ماهية الجريمة السيبرانية

الفصل الأول ماهية الجريمة السيبرانية

يُعنى هذا الفصل بتأسيس الإطار النظري والتشريعي للجريمة السيبرانية في الجزائر، إذ لا يمكن الخوض في تفاصيل مكافحة قبل الإحاطة التامة بمفهوم الظاهرة الإجرامية ذاتها، وتحديد أبعادها القانونية والتقنية، وبيان الأحكام التشريعية الجزائية النازمة لها. ويتضمن هذا الباب بحثين متكاملين:

المبحث الأول: مفهوم الجريمة السيبرانية

يتناول هذا المبحث التأصيل المفاهيمي للجريمة السيبرانية من خلال استعراض تعريفاتها الفقهية والتشريعية، وبيان خصائصها المميزة، وتصنيف أنواعها وفقاً لمعايير مختلفة، وذلك عبر ثلاثة مطالب متتابعة.

المطلب الأول: تعريف الجريمة السيبرانية

تُعَدّ الجريمة السيبرانية من المفاهيم الحديثة نسبياً التي ارتبطت بنشأة تكنولوجيا المعلومات والاتصالات وتطورها المتسارع، ومن ثم فإنّ التحديد الدقيق لهذا المفهوم يستلزم استعراضاً تاريخياً لمراحل نشأته وتطوره، قبل التطرق إلى التعريفات الفقهية والتشريعية المختلفة. يُشكّل تعريف الجريمة السيبرانية تحدياً مفاهيمياً وقانونياً نظراً لتطورها المستمر وطبيعتها العابرة للحدود، مما يستدعي مقارنة وظيفية تميز بين الفعل الإجرامي الذي يستهدف النظام المعلوماتي ذاته، والفعل الذي يستعمل هذا النظام كوسيلة لارتكاب جريمة تقليدية أو مستحدثة. فالأولى تستهدف سلامة وكفاءة البنية التحتية الرقمية، بينما تتخذ الثانية من الوسائل السيبرانية أداة لتحقيق غايات إجرامية أخرى.

تُعرف الجريمة السيبرانية، بوظيفتها، بأنها أي فعل غير مشروع يرتكب بمساعدة وسائل المعلوماتية أو ضدها، ويترتب عليه ضرر مادي أو معنوي للفرد أو للمجتمع أو للدولة⁴. هذا

⁴ فريدة عبد الفتاح راضي، سالي عوض السفال جرائم الإلكترونية والجرائم المعلوماتية: من وجهة نظر قانونية وتقنية. المجلة الدولية للبحوث والدراسات القانونية، الإصدار 3، العدد 5 (2024).

التعريف الوظيفي يضع التركيز على الفعل الضار ووسيلته، سواء كانت الوسيلة هي محل الجريمة أو أدواتها. وبهذا تتجاوز هذه الجرائم النطاق التقليدي للجريمة، لتدخل عالم الفضاء السيبراني وتحدياته .

إن التمييز بين استهداف النظام المعلوماتي كمحل للجريمة، واستعماله كوسيلة، يفتح الباب لتحليل أعمق. فالاختراق غير المصرح به للأنظمة، أو تعطيلها، أو الحصول على معلومات محمية، يمثل استهدافاً للنظام نفسه، وهو ما تناولته بعض التشريعات في ملاحقتها الخاصة بحماية المعطيات⁵. في المقابل، فإن استخدام البريد الإلكتروني للاحتيال، أو شبكات التواصل الاجتماعي لنشر الكراهية، يجعل النظام وسيلة لارتكاب جرائم تقليدية أو مستحدثة⁶.

الفرع الأول: التطور التاريخي لظاهرة الجريمة السيبرانية:

ارتبط نشأة الجريمة السيبرانية تاريخياً بنشأة الحواسيب وشبكات الاتصال، ومرتّ بمراحل تطويرية متعاقبة يمكن إجمالها فيما يأتي:

المرحلة الأولى (1960-1980): مرحلة جرائم الحاسوب التقليدية

ظهرت في هذه المرحلة أولى صور الجريمة المعلوماتية التي اقتصرَت على الاستخدام غير المشروع للحاسوب والتلاعب بالبيانات المخزّنة، وكانت محدودة النطاق نظراً لمحدودية انتشار الحواسيب. وقد اتسمت جرائم هذه المرحلة بأنها كانت في معظمها جرائم داخلية يرتكبها موظفون من داخل المؤسسات التي يعملون فيها.

المرحلة الثانية (1980-1995): مرحلة الشبكات المحلية والانترنت الأولى

شهدت هذه المرحلة تطور الجريمة المعلوماتية بفعل انتشار الشبكات المحلية وظهور الإنترنت، وبرزت خلالها جرائم الاختراق (Hacking) لأول مرة بصورة منظمة، إذ باتت

⁵ وزارة الشؤون الخارجية والجمالية الوطنية بالخارج، توقيع الجزائر على معاهدة الأمم المتحدة لمكافحة الجريمة السيبرانية، 2024. متاح على الرابط: <https://www.mfa.gov.dz/ar/press-and-information/news-and-press-releases/mrmagrame-signed-the-united-nations-convention-on-cybercrime> ، تاريخ النشر 17-07-2026

⁶ الاتحاد الإفريقي، اتفاقية الاتحاد الإفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية، مالاو 2014. متاح على الرابط: <https://au.int>

الأنظمة المتصلة بالشبكات هدفاً للمجرمين الإلكترونيين. كما ظهر في هذه الحقبة أول فيروس حاسوبي منتشر عبر الشبكة عام 1988 المعروف (Morris worm) التي أصابت آلاف الأنظمة⁷.

المرحلة الثالثة (1995-2010): مرحلة التجارة الإلكترونية والجريمة المنظمة

مع انتشار الإنترنت تجارياً وظهرت التجارة الإلكترونية، تنوعت الجرائم الإلكترونية وأصبحت ذات طابع مالي بالدرجة الأولى، وظهرت عمليات الاحتيال الإلكتروني وسرقة بيانات بطاقات الائتمان والتصيد الاحتيالي (Phishing) وقد تحولت الجريمة الإلكترونية في هذه المرحلة من عمل فردي إلى جريمة منظمة تُدار بواسطة شبكات إجرامية عابرة للحدود.

المرحلة الرابعة (2010-الآن): مرحلة التهديدات المتطورة والجريمة السيبرانية الشاملة

تتميز هذه المرحلة بتطور كبير في أساليب الجريمة الإلكترونية وأهدافها، إذ باتت البنى التحتية الحيوية للدول ذاتها هدفاً للهجمات الإلكترونية المنسقة. وتبرز في هذه المرحلة ظواهر مثل برامج الفدية (Ransomware) والهجمات على المنشآت الحيوية، وتوظيف الذكاء الاصطناعي في تطوير الهجمات الإلكترونية.

الفرع الثاني: التعريف الفقهي والتشريعي للجريمة السيبرانية

يلاحظ عدم وجود اتفاق على مصطلح معين للدلالة على الجريمة السيبرانية، فهناك من يطلق عليها الغش المعلوماتي، أو الاختلاس المعلوماتي أو الجريمة المعلوماتية⁸. ونظراً لصعوبة إعطاء تعريف لهذه الظاهرة الإجرامية وذلك حصرها في مجال ضيق. الجرائم السيبرانية هي نشاط إجرامي يستهدف أجهزة كمبيوتر أو شبكة أو جهازاً متصلاً بالشبكة. تقع معظم الجرائم السيبرانية على أيدي لصوص أو مخترقين يودون كسب الأموال، وأحياناً يكون الهدف من وراء الجرائم السيبرانية هو إلحاق الضرر بأجهزة الكمبيوتر لأسباب

⁷ مقال الكتروني أول هجوم سيبراني في التاريخ.. كيف شلت "دودة موريس" الإنترنت عام 1988؟ مجلة www.alaraby.com/news محدث 27 يناير 2026

⁸ محمد علي العريان: "الجرائم المعلوماتية". دار الجامعة الجديدة للنشر. طبعة 2004. ص: 43.

غير الربح، وقد تكون هذه الأسباب سياسية أو شخصية. يمكن أن تقع الجرائم السيبرانية على يد أفراد أو منظمات؛ بعض هؤلاء المجرمين منظمين ويستخدمون التقنيات المتقدمة وهم ذوي مهارات فنية عالية، وبعضهم مجرد مخترقين مبتدئين. لم يستقر الفقه القانوني والتشريع المقارن على تعريف موحد للجريمة السيبرانية، وهو ما يدفعنا إلى استعراض أبرز التعريفات المطروحة في الفقه والتشريع على النحو الآتي:

أولاً: التعريفات الفقهية

تعددت التعريفات الفقهية للجريمة السيبرانية، ويمكن إجمال أبرزها في الاتجاهين الآتيين:

الاتجاه الأول - التعريف الموسع:

يذهب أصحاب هذا الاتجاه إلى توسيع نطاق الجريمة السيبرانية لتشمل كل جريمة يُستعان فيها بالحاسوب أو الشبكة المعلوماتية أداةً لارتكابها، سواء أكانت جريمة مالية أم جنسية أم ماسة بالأشخاص⁹.

يلاحظ عدم وجود اتفاق على مصطلح معين للدلالة على هذه الظاهرة المستحدثة، فهناك من يطلق عليها الغش المعلوماتي، أو الاختلاس المعلوماتي أو الجريمة المعلوماتية.

ونظراً لصعوبة إعطاء تعريف لهذه الظاهرة الإجرامية وذلك حصرها في مجال ضيق .

فهو ذلك النشاط غير القانوني الذي يتم عبر الشبكات المعلوماتية فهي لا تختلف كثيراً عن الجرائم العادية إذ أنها تتوفر أيضاً على عناصر الضحية الجاني والعمل الإجرامي تطلق على جرائم المعلوماتية عدة مصطلحات أبرزها الجرائم السيبرانية، جرائم التقنيات العالية، جرائم الحاسوب والانترنت.

الاتجاه الثاني - التعريف الضيق:

يرى أصحاب هذا الاتجاه أن الجريمة السيبرانية تقتصر على الجرائم التي يكون فيها نظام الحاسوب أو الشبكة المعلوماتية هو محل الجريمة ذاتها¹⁰، أي الجرائم الواقعة على الأنظمة المعلوماتية كالاختراق والتخريب والتلاعب بالبيانات.

⁹ مقال مهدي رضا مجلة إيليزا للبحوث والدراسات المجلد 06 /العدد: 2 - 2021 ، ص 111 تاريخ النشر 2021/12/15

ومن هذه التعاريف "الجريمة السيبرانية تشمل أي جريمة ضد المال مرتبط باستخدام المعالجة الآلية للمعلوماتية". بينما أعطى خبير أمريكي مفهوما موسعا للجريمة السيبرانية وقال: "كل فعل إجرامي متعمد أيا كانت صلته بالمعلوماتية،¹¹ ينشأ عنه خسارة تلحق بالمجني عليه وكسب يحققه الفاعل"، ويعرفها مكتب تقييم التقنية في الولايات المتحدة الأمريكية من خلال تعريف جرائم الحاسوب بأنها "الجرائم التي تلعب فيها البيانات الكمبيوترية والبرامج المعلوماتية دورا رئيسيا". وكذلك تعريف "David Thompson" بأنها: "أية جريمة يكون متطلبا اقترافها، أن تتوفر لدى فاعلها معرفة تقنية للحاسب"¹².

هناك جانب من الفقه الفرنسي، يحاول وضع تعريف لظاهرة الغش المعلوماتي حيث يرى الأستاذ "Massa" أن المقصود بها: "الاعتداءات القانونية التي ترتكب بواسطة المعلوماتية بغرض تحقيق الربح". وفي الغالب ترتكب الجريمة المعلوماتية ليس بغرض تحقيق الربح، وإنما بدافع الانتقام والسخرية من المنافسين أو غير ذلك من الدوافع.

ويعرفها الأساتذة "Lestan & Vivant" بأنها: "مجموعة من الأفعال المرتبطة بالمعلوماتية والتي يمكن أن تكون جديرة بالعقاب". ويؤكد الأستاذ "Devéze" أنه ليس المقصود مجرد إخفاء وصف قانوني، ولكن وضع مفهوم إجرامي، والذي سيكون من الممكن أن يطبق عليه أحد التعاريف المعمول بها في القانون المدني أو الجنائي أو المالي¹³.

بينما يعرف الفقيه الألماني تاديمان الجرائم السيبرانية بأنها "كل أشكال السلوك غير المشروع أو الضار بالمجتمع الذي يرتكب باستخدام الحاسب".

من خلال هذه التعريفات يتضح أنها عمومية بحيث لا يمكن السيطرة عليها، بحيث كل تعريف ينظر إلى الجرائم السيبرانية من زاوية معينة تختلف عن أخرى. لعل من هذه التعريفات الموسعة ما يقوله الفقيهان "Miche, Cerdo" من أن سوء استخدام الحاسب أو جريمة الحاسوب تشمل استخدامه كأداة لارتكاب الجريمة، بالإضافة إلى الحالات المتعلقة بالولوج غير المصرح به لحاسب المجني عليه أو بياناته، كما تمتد جريمة الحاسوب لتشمل

¹⁰المرجع السابق ص 113

¹¹ محمد سامي الشوا: "ثورة المعلومات وانعكاساتها على قانون العقوبات". دار النهضة العربية، القاهرة. 1994.

¹² الجرائم المعلوماتية في الجزائر: المواجهة والتحدي، مجلة الحقوق والعلوم السياسية - جامعة خنشلة، مجلد 12 عدد 01 سنة 2025 ص 271

¹³ محمد علي العريان: "الجرائم المعلوماتية". دار الجامعة الجديدة للنشر. طبعة 2004. ص: 44.

الاعتداءات المادية، وسواء كان هذا الاعتداء على جهاز الحاسوب ذاته أو المعدات المتصلة به، وكذلك الاستخدام غير المشروع لبطاقات الائتمان، وانتهاك ماكينات الحسابات الآلية، بما تتضمنه من شبكات تمويل الحسابات المالية بطريقة إلكترونية، وتزييف المكونات المادية والمعنوية للحاسب بل وسرقة جهاز الحاسب في حد ذاته أو مكون من مكوناته .

أما بالنسبة للفقه العربي فهناك من يرى أن تعريف الجريمة السيبرانية هي "كل فعل أو امتناع عمدي، ينشأ عن الاستخدام غير المشروع لتقنية المعلومات ويهدف إلى الاعتداء على الأموال والحقوق المعنوية".

هناك فريق آخر يرى أن الجريمة السيبرانية هي: "عمل أو امتناع يأتيه أضراراً بمكونات الحاسوب وشبكات الاتصال الخاصة به، التي يحميها قانون العقوبات ويفرض له عقاباً ."

ثانياً: التعريف في التشريع الجزائري

لم يُعرّف المشرع الجزائري صراحةً مصطلح 'الجريمة السيبرانية' أو 'الجريمة الإلكترونية'، وإنما أثر استخدام عبارة 'الجرائم المتصلة بتكنولوجيات الإعلام والاتصال' في عنوان القانون رقم 04-09 وقد ارتكز هذا القانون على مفهوم 'منظومة المعالجة الآلية للمعطيات' (STAD) بوصفها المحور الذي تدور حوله أغلب الجرائم الإلكترونية المُجرّمة.

وقد عرّفت المادة الثانية من القانون 04-09 'منظومة المعالجة الآلية للمعطيات' بأنها: 'كل منظومة تضمن بواسطة برامج معلوماتية معالجة المعطيات أو تخزينها أو نقلها'¹⁴. ويلاحظ أن هذا التعريف يتسم بالشمولية الكافية لاستيعاب مختلف صور الأنظمة المعلوماتية الحديثة.

وقد ذهب الفقه الجزائري إلى أن المشرع اتبع نهجاً توافيقاً بين الاتجاهين الضيق والموسّع، إذ أدرج في القانون 04-09 الجرائم الواقعة على الأنظمة المعلوماتية ذاتها، فيما أدرج في قانون العقوبات جرائم أخرى تُستخدم فيها التكنولوجيا وسيلةً لارتكابها.

¹⁴ قانون رقم 04-09 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها ، المؤرخ في 14 شعبان عام 1430 الموافق 05 غشت سنة 2009 الجريدة الرسمية عدد 47 لسنة 2009

ثالثاً: التعاريف الاصطلاحية :

تتسم المفاهيم القانونية المتعلقة بالجرائم المرتكبة عبر الفضاء الرقمي بوجود تداخلات قد تؤدي إلى لبس في التطبيق، مما يستدعي دقة في التمييز بين المصطلحات. ف"الجريمة المعلوماتية" غالباً ما تشير إلى الأفعال التي تستهدف الأنظمة المعلوماتية أو البيانات المخزنة فيها، سواء بالإتلاف أو الوصول غير المشروع أو التعديل ، هذا المصطلح واسع ويشمل نطاقاً من الأفعال المجرّمة تقليدياً والتي تم تكيفها لتشمل العالم الرقمي.

في المقابل، فإن "الجريمة الإلكترونية" تميل إلى التركيز على الأفعال التي تستخدم الشبكات الإلكترونية، وخاصة الإنترنت، كوسيلة لارتكاب الجرائم، بغض النظر عن الهدف المباشر¹⁵ قد تشمل هذه الأفعال الاحتيال الإلكتروني، أو نشر المحتوى المسيء، أو حتى الجرائم العابرة للحدود ، تتداخل هذه الفئة بشكل كبير مع الجريمة المعلوماتية، لكن التركيز فيها ينصب على الوسيلة المستخدمة.

أما "الجريمة السيبرانية"، فهي غالباً ما تُستخدم كمصطلح أشمل وأكثر حداثة، ليشمل كلا المفهومين السابقين، بالإضافة إلى الجرائم التي تستهدف البنية التحتية الحيوية المعتمدة على التقنية، أو تلك التي ترتبط بالأمن القومي في الفضاء السيبراني. إنها تعكس التطور المستمر للتهديدات الرقمية وتوسع نطاقها ليشمل أبعاداً استراتيجية¹⁶.

من جهة أخرى، فإن "جرائم تكنولوجيات الإعلام والاتصال" هي فئة واسعة قد تضم جميع الأفعال غير المشروعة التي ترتبط باستخدام هذه التكنولوجيات، بما في ذلك ما سبق ذكره. يمكن أن تشمل هذه الفئة أيضاً جرائم تتعلق بالخصوصية، أو انتهاك حقوق

¹⁵ مقال الفرق بين الجريمة الإلكترونية والجريمة المعلوماتية فريحات محامون ومستشارون www.frihatlaw.ps 21 يناير 2026

¹⁶ الأمن السيبراني المفهوم و الأهمية ، قاضي سعاد ، جامعة محمد بوضياف المسيلة ، سنة 2025

الفرع الثالث: الأركان القانونية للجريمة السيبرانية

تخضع الجريمة السيبرانية للأركان القانونية العامة للجريمة في الفقه الجزائري، وإن اتسمت ببعض الخصوصية في تجلّي كل ركن منها بما يلائم الطبيعة الرقمية لهذه الجرائم:

الركن الشرعي (المبدأ الدستوري: لا جريمة ولا عقوبة إلا بنص)

يستوجب مبدأ الشرعية الجنائية المكرّس في المادة 37 من الدستور الجزائري لعام 2020¹⁷ وجود نص قانوني صريح يجرّم السلوك الإلكتروني المُجرّم، وقد تجلّى هذا الركن في الجرائم السيبرانية من خلال المواد 394 مكرر وما تلاها من قانون العقوبات الجزائري¹⁸، إضافة إلى أحكام القانون رقم 04-09. غير أن التطور السريع للتكنولوجيا يطرح تحدياً جوهرياً يتعلق بإمكانية النصوص القائمة في استيعاب الجرائم المستحدثة التي لم تكن متصورة عند سن التشريع.

الركن المادي:

يتكون الركن المادي للجريمة السيبرانية من عناصر ثلاثة وهي كالتالي:

أولاً: السلوك الإجرامي

الذي يتمثل في الفعل أو الامتناع الإلكتروني المحظور قانوناً (كالدخول غير المشروع أو تخريب البيانات).

ثانياً: النتيجة الإجرامية

المتتمثلة في الأضرار المعلوماتية أو المادية التي تحدث جراء هذا السلوك.

ثالثاً: علاقة السببية

التي تربط السلوك بالنتيجة. وتكتسب النتيجة في الجرائم السيبرانية طابعاً لا مادياً في أغلب الأحيان كتدمير البيانات وانتهاك الخصوصية والتعطيل التقني للخدمات.

الركن المعنوي:

¹⁷الدستور الجزائري الصادر في 30 ديسمبر 2020 الجريدة الرسمية عدد 82 لسنة 2020
¹⁸ الأمر رقم 66-156 المؤرخ في 8 يونيو سنة 1966 المتضمن قانون العقوبات المعدل و المتمم بالقانون 24-06 الصادر في 28 أبريل 2024 ، الجريدة الرسمية عدد 30 لسنة 2024

تتشرط أغلب الجرائم السيبرانية في التشريع الجزائري توافر القصد الجنائي العام (العلم والإرادة) كشرط لقيام المسؤولية الجنائية، وتبرز هنا إشكالية الخطأ التقني غير المتعمد الذي يسفر عن أضرار جسيمة بدون قصد جنائي، كما يثير الجاني المعتقد بأن ما يقوم به مجرد اختبار أمني مشروع تساؤلات جوهرية حول إثبات القصد الجنائي أمام القضاء الجزائري.

المطلب الثاني: خصائص الجريمة السيبرانية

تتمتع الجريمة السيبرانية بجملة من الخصائص المميّزة التي تُفرّقها عن الجرائم التقليدية، وتجعل التعامل القانوني معها يستلزم نهجاً خاصاً يراعي طبيعتها التقنية و أهمها

- صعوبة معرفة مرتكب الجريمة الا باستخدام وسائل امنية ذات تقنية عالية
- الاضرار الناجمة عن الجرائم المعلوماتية غير قابل للقياس اذ انها تلحق خسائر جسيمة
- سهولة الوقوع ضحية للجريمة المعلوماتية بسبب غياب الرقابة الأمنية
- سهولة اخفاء وطمس معالم الجريمة واثارها والدلائل التي تدل على مرتكبيها
- اقل جهدا وعنفا جسديا من الجرائم التقليدية غير أن لها أثارا كبيرة
- جريمة غير مقيدة لا بزمن ولا بمكان كما تمتاز بالتباعد الجغرافي

فالجريمة السيبرانية تستمد خصائصها من خصائص الانترنت التي أضحت وسيلة مثالية لتنفيذ العديد من الجرائم والأفعال غير المشروعة والعابرة للحدود؛ إذ لم يعد هناك أيّة حدود مرئية أو مسموعة تقف أمام نقل المعلومات بسرعة، وبسهولة مذهلة، وبكميات كبيرة. و"السهولة في نقل المعلومات عبر أنظمة التقنية الحديثة جعل بالإمكان ارتكاب عن طريق حاسوب موجود في دولة معينة بينما يتحقق الفعل في دولة أخرى.¹⁹ كما يمكن ارتكابها أثناء وجود الضحية على شبكة الانترنت دون أن يلحظها أو يدري بوقوعها. فهي لا تتطلب جهدا أو عنفا مقارنةً بالجرائم التقليدية، كما تتميز بسرعة محو الدليل. ولا يُبلغ عنها في أغلب الأحيان إمّا بسبب عدم اكتشافها من قبل الضحايا أو خوفا من التشهير. وتتميّز الجرائم

¹⁹محلّاء عبد القادر المومني، "الجرائم المعلوماتية"، دار الثقافة للنشر والتوزيع، ط 1، عمان، 2008.

المعلوماتية بطبيعتها الناعمة soft crime ، فهي تعتمد على البراعة التقنية للمجرم في التعامل مع جهاز الحاسوب بعيداً عن العنف و نذكر أهم خصائصها و هي كالتالي:

أولاً: الطابع العابر للحدود (العالمية)

إن الطبيعة اللامادية للشبكة المعلوماتية والانتشار الواسع لوسائل الاتصال الحديثة منحا الجرائم السيبرانية خاصية أساسية تتمثل في عبور الحدود الجغرافية بسهولة وسرعة فائقة، إذ يمكن لمرتكبها في دولة ما أن يوجّه هجومه نحو ضحية تقع في دولة أخرى، أو يمرّ عبر خوادم في دول ثالثة لإخفاء هويته. مما يجعلها تتجاوز الاختصاصات القضائية الوطنية التقليدية.

هذا الطابع العابر للحدود يمثل تحدياً جوهرياً للقانون الجنائي، حيث يصعب تحديد مكان وقوع الجريمة أو مكان اكتشاف نتائجها بشكل قاطع، وهو ما ينعكس سلباً على إمكانية ملاحقة مرتكبها.

تثير خاصية العابرية للحدود إشكالية معقدة تتعلق بتحديد الاختصاص القضائي. ففي غياب اتفاقيات ثنائية أو متعددة الأطراف واضحة، غالباً ما تتنازع عدة دول الاختصاص ، إما بناءً على مكان وجود الضحية، أو مكان وجود الخادم المستخدم، أو مكان وقوع الضرر. هذا التنازع يمكن أن يؤدي إلى إفلات الجناة من العقاب إذا لم يتم التوصل إلى توافق بشأن الدولة المختصة بالتحقيق والمحاكمة، مما يفرض ضرورة تفعيل آليات التعاون الدولي.

يعد التعاون الدولي عنصراً حاسماً في مكافحة الجرائم السيبرانية العابرة للحدود.²⁰ وتتطلب هذه المكافحة تضافر الجهود بين الدول عبر اتفاقيات المساعدة القضائية المتبادلة، وتسليم المجرمين، وتبادل المعلومات الاستخباراتية. وغياب أو ضعف هذه الآليات قد يعيق عملية جمع الأدلة الرقمية الضرورية لإثبات الجريمة، خاصة مع التحديات التقنية المتعلقة بخصوصية البيانات وتشفيرها.

²⁰ الجهود الدولية في مواجهة الجرائم السيبرانية ، بن أودينة سندس ، جامعة غرداية، كلية الحقوق والعلوم السياسية ، 2025

في الجزائر، ورغم وجود تشريعات تهدف إلى مكافحة الجرائم السيبرانية ، إلا أن الطابع العابر للحدود لهذه الجرائم يستدعي تعزيز التعاون الدولي بشكل أكبر. إن تفعيل اتفاقيات التعاون القضائي وتوسيع نطاقها لتشمل الجرائم السيبرانية، بالإضافة إلى مواكبة التطورات التشريعية الدولية في هذا المجال، يعد أمراً ضرورياً لسد الثغرات القانونية القائمة.

إن التحديات التي يفرضها الطابع العابر للحدود على الاختصاص والتعاون الدولي تستلزم مقارنة قانونية استباقية. يتوجب على المشرع الجزائري، بالتعاون مع الأجهزة الأمنية والقضائية، العمل على تطوير آليات التعاون الدولي، وتوسيع نطاق الاتفاقيات الثنائية والمتعددة الأطراف، وتبني معايير دولية موحدة لجمع الأدلة الرقمية. هذا يتطلب أيضاً تأهيل الأطارات القضائية والأمنية للتعامل مع هذه الجرائم المستجدة.

ثانياً: الخفاء وصعوبة الكشف والإثبات

يتميز الفضاء الإلكتروني بقدر كبير من إمكانية إخفاء الهوية والتورية، إذ يلجأ مرتكبو الجرائم السيبرانية إلى أدوات متطورة لإخفاء آثارهم كشبكات VPN وتقنيات التشفير والانترنت المظلم (Dark Web)، مما يُعسّر على المحققين الرقميين تحديد هوية الجاني وجمع الأدلة الكافية للملاحقة القضائية.

ثالثاً: السرعة الفائقة في التنفيذ

تتميز الجريمة السيبرانية بأنها تُنجز في وقت قياسي قد يصل إلى أجزاء من الثانية، مما يُصعّب إمكانية التدخل للحيلولة دون وقوعها أو الحد من آثارها. وهذا ما يجعل التكيف القانوني من حيث الشروع والإتمام أمراً دقيقاً في السياق الجزائري.

رابعاً: الطابع غير المادي (اللاملموسية)

على خلاف الجرائم التقليدية التي تترك أثراً مادية ملموسة، فإن الجريمة السيبرانية تقع في الفضاء الرقمي وتستهدف في أغلب الأحيان معطيات غير مادية، مما يثير إشكاليات قانونية تتعلق بالاختصاص القضائي وقواعد الإثبات وتقدير الضرر.

تُعد خاصية اللامادية للجرائم السيبرانية من أبرز سماتها التي تميزها عن الجرائم التقليدية. فهذه الجرائم لا ترتبط بكيان مادي محسوس، بل تتجلى في فضاء رقمي غير مرئي، مما يصعب تحديد مكان وقوعها بدقة. هذا الغموض المكاني يثير تحديات كبيرة أمام تحديد الاختصاص القضائي، حيث قد تتوزع آثار الجريمة على عدة دول، مما يستدعي تفعيل آليات التعاون الدولي.

تتداخل خاصية اللامادية مع خاصية السرعة في خلق تعقيدات إضافية. فبينما تنشأ الجريمة وتنتشر آثارها في لحظات، تتطلب الإجراءات القانونية التقليدية وقتاً طويلاً، مما قد يؤدي إلى فقدان الأدلة الرقمية الهامة. فالأدلة قد تتغير أو تُحذف بسهولة، مما يستلزم تطوير أساليب تقنية وقانونية سريعة لحفظها وتأمينها.

إن تحليل خاصية السرعة يكشف عن البعد الزمني المتسارع لهذه الجرائم. فالجريمة السيبرانية قد تحدث وتتطور في أجزاء من الثانية، مما يجعل اكتشافها ومكافحتها أمراً بالغ الصعوبة. تتطلب هذه السرعة استجابة سريعة وفعالة من أجهزة إنفاذ القانون، مع ضرورة التكيف المستمر مع التقنيات الجديدة التي يستغلها المجرمون .

تؤثر هاتان الخاصيتان مجتمعتان بشكل مباشر على عملية الإثبات. فالبعد اللامادي يجعل من الصعب جمع الأدلة المادية المباشرة، بينما تفرض السرعة تحديات في تأمين الأدلة الرقمية قبل زوالها. يعتمد الإثبات بشكل كبير على الأدلة الرقمية، والتي تتطلب خبرة فنية متخصصة لجمعها وتحليلها وتقديمها أمام المحاكم.

تنترب على اللامادية والسرعة صعوبات جمة في تحديد الاختصاص القضائي، خاصة وأن الجريمة قد تمس عدة دول. إن القانون الجزائري، في ظل غياب نصوص تفصيلية تعالج هذه المعضلة بشكل كافٍ، يواجه تحديات في تطبيق قواعد الاختصاص التقليدية. ويعد قانون العقوبات 06-24 خطوة أولى، إلا أن التطبيق العملي لا يزال يتطلب المزيد من التوضيح وآليات التعاون الدولي لضمان فعالية الملاحقة القضائية.

خامساً: التطور المستمر للأساليب والأدوات

تتجدد أساليب الجريمة السيبرانية وأدواتها باستمرار بمعدل يفوق قدرة المنظومات القانونية والأمنية على مواكبتها، مما يُلقي عبئاً مضاعفاً على المشرع والأجهزة الأمنية في التكيف السريع مع المستجدات التقنية.

سادساً: انعدام الحدود الزمنية

يمكن ارتكاب الجريمة السيبرانية في أي وقت من الليل أو النهار دون قيود زمنية، بخلاف كثير من الجرائم التقليدية التي تستلزم ظروفاً زمنية معينة، كما أن آثارها قد تستمر لفترات طويلة بعد وقوع الجريمة.

المطلب الثالث : تصنيف وانواع الجريمة السيبرانية

هناك العديد من الجرائم السيبرانية و منها ما كانت جرائم تقليدية و تطورت عبر الفضاء السيبراني و تفاقمت و زاد ضررها نظرا لسهولة ارتكابها و تخفي الجاني و صعوبة تتبعه و من أشهر هذه الجرائم نذكر :

الجرائم التي تؤثر على الأطفال

- التحرش الإلكتروني: يتمثل في التواصل غير المرغوب فيه، أو الإغراء الجنسي للأطفال عبر الإنترنت، مما يهدد براءتهم وأمانهم النفسي.

- الاستغلال الجنسي للأطفال: يشمل توزيع أو تحميل محتويات استغلالية للأطفال عبر الإنترنت.
- التتمر الإلكتروني: إرسال رسائل أو نشر تعليقات تهدف إلى مضايقة أو إهانة الأطفال على وسائل التواصل الاجتماعي، مما يؤثر على ثقتهم بأنفسهم.
- خطف الهوية الرقمية: استغلال هوية الطفل الإلكترونية لتنفيذ جرائم أخرى، مما يعرض الطفل لمشاكل قانونية واجتماعية.

الجرائم التي تؤثر على الأسرة و المجتمع

- اختراق الخصوصية: التجسس أو الوصول إلى المعلومات الشخصية للأسرة، مثل الصور والمحادثات.
- الابتزاز الإلكتروني: تهديد أفراد الأسرة بنشر معلومات حساسة أو صور شخصية للحصول على المال أو خدمات معينة.
- الاحتيال المالي: سرقة بيانات بطاقات الائتمان أو الحسابات البنكية الخاصة بأفراد الأسرة.
- انتحال الشخصية: تقمص هوية أحد أفراد الأسرة لخداعهم أو استغلال اسمهم لتحقيق مكاسب غير مشروعة.

جرائم المحتوى:

- نشر محتوى غير لائق: تقديم محتوى غير ملائم للأطفال، مثل المواد الإباحية أو العنيفة، مما يؤثر على قيمهم وسلوكياتهم.
- الألعاب الإلكترونية الخطيرة: الترويج لألعاب تتضمن تحديات تهدد سلامة الطفل.
- الترويج للأيديولوجيات المتطرفة: استهداف الأطفال والأسر بنشر أفكار تحض على العنف أو الكراهية.
- ترويج لاعلانات لمؤثرين و أغاني تتنافى مع الأخلاق.

التصيد الإلكتروني (Phishing)

- إرسال رسائل بريد إلكتروني أو روابط مزيفة تهدف إلى سرقة المعلومات الشخصية أو التحكم في أجهزة الأسرة.
- التحايل في منصات الألعاب
- استغلال الأطفال في منصات الألعاب الإلكترونية لجمع بياناتهم الشخصية أو الإيقاع بهم في عمليات احتيال.
- التعرض للتطبيقات المزيفة
- تحميل تطبيقات أو ألعاب غير آمنة تحتوي على برمجيات خبيثة قد تسرق بيانات الأسرة أو تُلحق الضرر بالجهاز.

الابتزاز والتهديد الإلكتروني: تهديد الأفراد بنشر صور أو معلومات حساسة ومطالبتهم بدفع مبالغ مالية مقابل التستر عليها.

- الاحتيال المالي: عمليات النصب عبر الإنترنت، مثل الاحتيال في عمليات البيع والشراء الوهمية.
- برامج الفدية (Ransomware): برمجيات خبيثة تقوم بتشفير ملفات المؤسسة بالكامل، ويطلب الجاني دفع فدية مالية لفك التشفير واستعادة الوصول.
- هجمات حجب الخدمة (DDoS): إغراق خوادم وأنظمة الشركة بطلبات وهمية لإرباكها وتعطيل خدماتها ومنع المستخدمين الحقيقيين من الوصول إليها.
- التجسس الإلكتروني: اختراق أنظمة المنافسين أو الدول لسرقة الأسرار التجارية والخطط الاستراتيجية.
- اختراق البيانات (Data Breaches): الوصول غير المصرح به لقواعد بيانات الشركات الكبيرة لسرقة بيانات العملاء وبيعها في الأسواق السوداء.
- الجرائم التي تستهدف المجتمعات والحكومات الجرائم الإرهابية السيبرانية:
- استخدام الفضاء الرقمي لنشر الدعاية المتطرفة، أو تجنيد الأفراد، أو التخطيط لهجمات.
- الحروب السيبرانية: الهجمات المنظمة التي تدعمها دول لاستهداف البنية التحتية الحيوية لدولة أخرى (مثل شبكات الكهرباء، والمطارات، والقطاعات الصحية).
- الجرائم المتعلقة بالمحتوى غير الأخلاقي و العنيف خاصة في الانترنت العميق

- ترويج و بيع المخدرات و الأسلحة و الممنوعات.
- الاتجار بالأعضاء و الاتجار بالبشر و تنظيم رحلات الهجرة غير الشرعية.
- جرائم التشهير ونشر الكراهية وتحرض على العنصرية
- نشر معلومات مضللة أو إشاعات أو خطابات وتضرر بالأفراد والمجتمع.

المبحث الثاني : الجرائم السيبرانية وفق ما جاء به التشريع الجزائري

تتعدد الجرائم السيبرانية وتتنوع، وقد دأب الفقه والتشريع على تصنيفها وفق معايير مختلفة. ونستعرض فيما يلي أبرز أنواع هذه الجرائم وفق معيار الغرض والأثر، مع الإشارة إلى صورها الأكثر شيوعاً في الواقع الجزائري:

المطلب الأول: الجرائم الواقعة على الأنظمة الآلية والبيانات المعلوماتية

إن أنظمة المعالجة الآلية للمعطيات تحتل مكانة محورية في التجريم الجزائري للجرائم السيبرانية، باعتبارها الأداة الأساسية التي تدور حولها هذه الجرائم، سواء كانت مجرد مسرح للجريمة أو وسيلة لارتكابها أو هدفاً لها. القانون 09-04 و على الرغم من كونه قانوناً سابقاً، إلا أنه وضع اللبنة الأولى لهذا التجريم من خلال تعريفه لأنظمة المعالجة الآلية للمعطيات والتطرق إلى بعض الأفعال التي تمسها.

إن التمييز بين استهداف النظام المعلوماتي كمحل للجريمة، واستعماله كوسيلة، يفتح الباب لتحليل أعمق، فالاختراق غير المصرح به للأنظمة، أو تعطيلها، أو الحصول على معلومات محمية، يمثل استهدافاً للنظام نفسه، وهو ما تناولته بعض التشريعات في ملاحقتها الخاصة بحماية المعطيات.

أولاً: جريمة الدخول و البقاء غير المشروع إلى الأنظمة المعلوماتية

تُعدّ هذه الجريمة من أكثر الجرائم السيبرانية شيوعاً، وتتحقق بقيام شخص بالدخول إلى نظام معالجة آلية للمعطيات دون الحصول على ترخيص من صاحبه، وذلك باستخدام شتى

التقنيات كالقرصنة (Hacking) وكسر كلمات المرور واستغلال الثغرات البرمجية. وقد جرم المشرع الجزائري هذا الفعل صراحةً في المادة 394 مكرر من قانون العقوبات، محدداً له عقوبات السجن من ثلاثة أشهر إلى سنة وغرامة مالية.

يعتبر الدخول غير المشروع إلى نظام معلوماتي اعتداءً مباشراً على مبدأ السرية، حيث يهدف المتسلل إلى الوصول إلى بيانات أو معلومات لا يحق له الاطلاع عليها. هذا الاعتداء يزعزع الثقة في الأنظمة الرقمية ويقوض قدرة الأفراد والمؤسسات على حماية أسرارهم. في القانون الجزائري، يعكس النص القانوني المتعلق بهذا الجرم، ضمن قانون مكافحة الجرائم المرتكبة عن بعد عبر الأنظمة المعلوماتية، الطبيعة الخطيرة لهذا الفعل، حيث لا يقتصر الأمر على مجرد اختراق، بل يتعداه إلى انتهاك الحق في الخصوصية والأمن المعلوماتي.

أما البقاء غير المشروع، فهو يمثل تطوراً خطيراً للدخول غير المشروع، إذ لا يكفي الجاني بالولوج بل يوطد وجوده داخل النظام لغايات قد تتراوح بين التجسس المستمر، أو زرع برمجيات خبيثة، أو حتى الاستيلاء على صلاحيات. هذا التواجد غير المصرح به يهدد سلامة النظام نفسه، حيث يمكن أن يؤدي إلى تعريض البيانات للتعديل أو الإتلاف، أو تعطيل الخدمات الأساسية. إن خطر البقاء غير المشروع يكمن في قدرته على إحداث أضرار جسيمة وطويلة الأمد يصعب تداركها، مما يجعله جريمة ذات خطورة متزايدة في العصر الرقمي.

تتجلى الخطورة المزدوجة للدخول والبقاء غير المشروع في كونهما يمسّان ركيزتين أساسيتين للأمن السيبراني: السرية والسلامة. فالسرية تُكفل بعدم اطلاع غير المخولين على المعلومات، بينما تضمن السلامة استمرارية عمل الأنظمة ودقتها وعدم تعرض بياناتها للتخريب. عندما يتم اختراق هذين المبدأين، فإن الثقة في البنية التحتية الرقمية تتآكل، مما

يؤثر سلباً على المعاملات التجارية، والخدمات الحكومية، وحتى على الأنشطة الشخصية للأفراد، ويخلق بيئة رقمية غير آمنة.

في إطار النظام القانوني الجزائري، تسعى التشريعات إلى معالجة هذه الانتهاكات عبر تجريم الأفعال التي تمسّ بالدخول غير المشروع. ورغم أن النصوص قد تتطور، إلا أن الهدف يبقى قائماً في توفير حماية قانونية فعالة ضد هذه التهديدات. إن ضرورة التمييز بين الدخول غير المشروع والبقاء غير المشروع تتجلى في تحديد مدى خطورة الفعل وتحديد العقوبات المناسبة، مع الأخذ في الاعتبار الغاية التي يسعى إليها الجاني.

إن التحليل النقدي لتجريم الدخول والبقاء غير المشروع يكشف عن التحديات التي تواجه السلطات القضائية في إثبات هذه الجرائم، نظراً للطبيعة التقنية المعقدة للأنظمة المعلوماتية وصعوبة تتبع الجناة، خاصة عندما يتجاوزون الحدود الجغرافية، كما أن عدم كفاية بعض النصوص القانونية لتغطية كافة الأشكال المستجدة للجرائم السيبرانية، مثل تلك المتعلقة بالذكاء الاصطناعي أو إنترنت الأشياء، يمثل تحدياً مستمراً يتطلب مراجعة وتحديثاً دورياً للإطار القانوني لضمان فعالية مكافحة هذه الظاهرة.

ثانياً: جريمة تخريب البيانات والأنظمة المعلوماتية

تُعدّ صور المساس بالمعطيات، من حذف أو تغيير أو إتلاف أو تعطيل، أحد أبرز مظاهر الجرائم السيبرانية التي تستهدف البنية التحتية الرقمية للمجتمع. فالحذف يمثل فناً تاماً للمعطيات، مما قد يؤدي إلى ضياع أصول معلوماتية حيوية، بينما يمس التغيير بسلامة البيانات ودقتها، مما يفتح الباب أمام تضليل أو تزوير. أما الإتلاف، فيشمل أي فعل يمس بجوهر المعطيات ويجعلها غير قابلة للاستخدام، بينما يهدف التعطيل إلى منع الوصول إلى المعطيات واستغلالها.

تتجسد الآثار القانونية لهذه الأفعال في تباين خطورتها تبعاً لمدى الضرر الناتج. ففي حين قد يُنظر إلى مجرد التعطيل العابر على أنه جنحة بسيطة، يمكن أن يرتقي الحذف أو التغيير الممنهج لمعطيات ذات طبيعة حساسة، مثل تلك المتعلقة بالبنية التحتية الحيوية أو الأمن القومي، إلى مستوى الجناية ، ومن أبرز صورها الحديثة هجمات برامج الفدية (Ransomware) التي باتت تهدد المؤسسات الحكومية والخاصة على حد سواء. وقد تناول المشرع الجزائري هذه الجريمة في المادة 394 مكرر 1 من قانون العقوبات²¹ التي تشمل هذه الجريمة عن كل فعل يستهدف إتلاف أو تعديل أو حذف البيانات والمعطيات المخزنة في الأنظمة المعلوماتية، أو تعطيل عمل هذه الأنظمة أو إعاقتها.

ثالثاً: جرائم التجسس المعلوماتي وسرقة البيانات

تُعرف جرائم التجسس المعلوماتي وسرقة البيانات بأنها أنشطة غير مشروعة تستخدم تقنيات التكنولوجيا للوصول غير المصرح به إلى أنظمة المعلومات، واعتراض البيانات أو سرقتها أو إتلافها بغرض الاستيلاء على المعلومات الحساسة، أو التزج المادي، أو الإضرار بالأفراد والمؤسسات.

تتجلى هذه الجرائم في الاطلاع على البيانات السرية والمعلومات الخاصة أو سرقتها دون ترخيص، سواء أكانت بيانات شخصية أم أسراراً تجارية أم معلومات أمنية حساسة. وفي ظل التطور التقني الراهن، باتت هجمات التجسس الإلكتروني تمتد لتستهدف المنشآت الحيوية للدول ذاتها.

فيمكن تعريف جريمة التجسس المعلوماتي بأنها : (الدخول غير المصرح به أو تجاوز التصريح الممنوح، إلى نظام معلوماتي أو موقعا إلكترونياً أو شبكة معلوماتية، أو أية وسيلة تقنية أخرى، باستخدام الشبكة المعلوماتية أو الحاسب الآلي أو إحدى الوسائل التقنية لانتهاك سرية البيانات الحكومية أو الخاصة بالاطلاع عليها أو نسخها أو نشرها أو اذاعتها أو

²¹قانون رقم 06-24 مؤرخ في 19 شوال عام 1445 الموافق 28 أبريل سنة 2024 ، يهدف هذا القانون إلى تعديل وتنظيم الأمر رقم 66-156 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 والمتضمن قانون العقوبات، المعدل والمتمم.

أفشاؤها أو كشفها أو تسليمها الى الغير دولة ، شركات، فرد .. الخ) ، بمقابل أو بدون مقابل.

وعرف التجسس التقليدي في قرار لمحكمة النقض المصرية بأنه " هو تسليم سر من أسرار الدفاع إلى دولة أجنبية أو من يعمل لمصلحتها، أو الحصول عليه بغض النظر عن الوسيلة المستعملة، ويكون ذات طبيعة سرية ومتعلق بالدفاع عن البلاد، وإن لم يفش إلا بعضه أو كان خطأ أو ناقصاً²²

المطلب الثاني: الجرائم السيبرانية الواقعة على الأموال

أولاً: الاحتيال الإلكتروني والنصب عبر الإنترنت

باتت هذه الجريمة تحتل المرتبة الأولى بين الجرائم الإلكترونية في الجزائر وفق إحصائيات المديرية العامة للأمن الوطني، إذ سجّلت السلطات الجزائرية 1387 قضية نصب إلكتروني في النصف الأول من عام 2024 وحده. وتتنوع أساليبها من بيع سلع وهمية عبر الإنترنت إلى الاحتيال العاطفي (Romance Scam) وادعاء الجوائز المزيفة وانتحال صفة الجهات الرسمية. ويمثل الاحتيال الإلكتروني تحدياً قانونياً متزايداً، حيث يستغل الفضاء الرقمي لارتكاب أفعال احتيالية كانت محصورة في صورها التقليدية. يتسم هذا النوع من الجرائم بالمرونة والقدرة على تجاوز الحدود الجغرافية، مما يعقد عملية التتبع والملاحقة القضائية.

يفرض التكييف القانوني للفعل المرتكب إشكالية جوهرية، خاصة عند محاولة إدماجه ضمن الأطر القانونية القائمة التي نشأت في سياق الجرائم المادية حيث تكمن صعوبة التكييف في الفارق الجوهرية بين آلية الاحتيال التقليدية والوسائل الرقمية، فبينما يعتمد النصب التقليدي على استغلال الثقة المباشرة أو التضليل المادي، يتسم الاحتيال الإلكتروني بالاعتماد على تقنيات معقدة، مثل الهندسة الاجتماعية، أو إنشاء مواقع ويب وهمية، أو استخدام هويات

²²الطعن رقم 1519 ق جلسة 13/5/1958 محكمة النقض المصرية أشار اليه حسن الفكهاني وعبد المنعم حسني، الموسوعة الذهبية للقواعد

القانونية التي قررتها محكمة النقض المصرية منذ إنشائها ، ج 3، الدار العربية للموسوعات، القاهرة، ص 46

رقمية مزيفة. هذه التقنيات تخلق مسافة بين الضحية والجاني، وتجعل إثبات الركن المادي والمعنوي للجريمة أكثر تعقيداً في ظل غياب التفاعل المباشر.

إن القانون الجزائري، في محاولاته لمواكبة التطور التكنولوجي، حاول أن يضع إطاراً لمكافحة الجرائم السيبرانية، كمحاولة أولية للتصدي لهذه الظاهرة، حيث تناول بعض الأفعال التي يمكن أن تندرج تحت مفهوم الاحتيال الإلكتروني ومع ذلك، فإن إشكالية التطبيق تظل قائمة، لا سيما عند تفسير النصوص القانونية وتكييف الأفعال المستجدة مع النصوص القديمة، والتي لم تكن تأخذ في الحسبان خصوصيات الفضاء السيبراني.²³

إن التمييز بين الاحتيال التقليدي والإلكتروني يتطلب تحليلاً دقيقاً للعناصر المكونة للجريمة. ففي حين يتطلب الاحتيال التقليدي إثبات وقوع ضحية في الغلط بسبب وسائل احتيالية، فإن الاحتيال الإلكتروني قد يتطلب إثبات استخدام أدوات رقمية متطورة لخداع الضحية، مما يستدعي خبرات تقنية متخصصة في الإثبات. هذا الأمر يضع عبئاً إضافياً على جهات التحقيق والقضاء، ويتطلب تطوير آليات جمع الأدلة الرقمية والتثبت من صحتها²⁴.

إن تكييف الاحتيال الإلكتروني لا يقتصر على إيجاد نص قانوني مطابق، بل يتجاوز إلى فهم طبيعة الوسائل المستخدمة والنتائج المترتبة عليها. إن القوانين المنظمة وإن كانت تضع بعض الأطر، إلا أنها قد لا تغطي بشكل شامل كافة صور الاحتيال الإلكتروني المستجدة. يتطلب الأمر تطويراً مستمراً للتشريع وتدريباً مكثفاً للقضاة والشرطة القضائية لمواجهة هذه التحديات.

ثانياً: جرائم التصيد الاحتيالي (Phishing)

²³الاتحاد الإفريقي، اتفاقية الاتحاد الإفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية، مالاو 2014. متاح على الرابط: <https://au.int>
²⁴بن بوعلام نورة وبن بوعلام وردة، تعزيز الحماية الجزائية للخصوصية المعلوماتية على ضوء تعديل قانون العقوبات رقم 06-24 المؤرخ في 28 أبريل 2024، ASJP، 2025. متاح على الرابط: <https://asjp.cerist.dz/en/article/269216>

تُعدّ عمليات التصيد الاحتيالي من أكثر الجرائم المالية الإلكترونية تطوراً في الجزائر، إذ يقوم الجناة بإنشاء مواقع أو رسائل إلكترونية مزيفة تحاكي مواقع البنوك والجهات الرسمية لاستدراج الضحايا للكشف عن بياناتهم البنكية وكلمات مرورهم.

ثالثاً: غسيل الأموال الإلكتروني

أبرز التطور التقني ظاهرة غسيل الأموال عبر الوسائل الإلكترونية، ولا سيما من خلال استخدام العملات المشفرة (Cryptocurrencies) التي تتيح قدراً كبيراً من إخفاء هوية المُعاملين وإخفاء مسارات التحويل المالي. وهذه الظاهرة تُعدّ من التحديات التشريعية الكبرى في الجزائر نظراً لعدم وجود إطار قانوني متكامل لتنظيم العملات الرقمية.

رابعاً : الجرائم الماسة بالاقتصاد و الاستثمار

تُشكل الجرائم السيبرانية تهديداً مباشراً للأمن الاقتصادي، حيث تستهدف البنية التحتية المعلوماتية الحساسة، مما يؤثر سلباً على استمرارية الأعمال وثقة المستثمرين. إن تزايد هذه الجرائم، سواء كانت اختراقات لأنظمة مالية، سرقة بيانات حساسة، أو هجمات حجب الخدمة، يقوض بيئة الأعمال ويشكل عائقاً أمام جذب الاستثمارات المحلية والأجنبية. تفرض هذه التهديدات ضرورة تعزيز الإطار القانوني والتقني لمكافحتها بفعالية.

إن التأثير السلبي للجرائم السيبرانية على الاستثمار يتجلى في خلق مناخ من عدم اليقين والخوف لدى المستثمرين. فالخوف من فقدان البيانات، أو تعطيل العمليات، أو التعرض لخسائر مالية جسيمة جراء هجمات إلكترونية، يدفع المستثمرين إلى إعادة تقييم مخاطر الاستثمار في السوق الجزائري. هذا التردد قد يؤدي إلى انخفاض معدلات الاستثمار المباشر وغير المباشر، وتفضيل أسواق أخرى توفر مستوى أعلى من الأمان السيبراني .

تؤثر الجرائم السيبرانية بشكل مباشر على ثقة المتعاملين في المعاملات الرقمية. عندما يفقد الأفراد والشركات الثقة في أمن الأنظمة الإلكترونية وقدرتها على حماية بياناتهم ومعاملاتهم،

فإنهم يميلون إلى تجنب استخدامها، أو العودة إلى الوسائل التقليدية الأقل كفاءة. هذا الانحسار في الثقة يعيق التقدم نحو اقتصاد رقمي متكامل، ويضعف فعالية الأدوات القانونية والتنظيمية المصممة لتأمين المعاملات الإلكترونية، مثل تلك المنصوص عليها في قوانين مثل قانون 04-15 المتعلق بالإثبات بالتوقيع الإلكتروني²⁵.

تتطلب مكافحة الجرائم السيبرانية حمايةً استباقية للاستثمار، من خلال تطوير آليات قانونية وتقنية قادرة على ردع المجرمين وضمان إنصاف الضحايا. إن سن تشريعات فعالة، مثل قانون مكافحة الجريمة السيبرانية، وتطبيقها بحزم، بالإضافة إلى تعزيز التعاون الدولي وتبادل المعلومات، يُعد أمراً ضرورياً لرفع مستوى الأمن السيبراني. فالاستثمار في البنية التحتية الرقمية الآمنة هو استثمار في المستقبل الاقتصادي للبلاد.

المطلب الثالث: الجرائم السيبرانية الواقعة على الأشخاص والمجتمع

أولاً: الابتزاز الإلكتروني والتشهير الرقمي

تتصدر هذه الجرائم قائمة الجرائم الاجتماعية الإلكترونية في الجزائر، وتتجلى في استخدام الصور والمعطيات الشخصية وسيلةً للابتزاز أو في حملات التشهير والإساءة عبر وسائل التواصل الاجتماعي. وقد رصد الدرك الوطني الجزائري ارتفاعاً حاداً في قضايا الابتزاز الإلكتروني الموجّه للنساء عبر منصتي فيسبوك وتيك توك.

يشكل الابتزاز الرقمي أحد أبرز التحديات القانونية المعاصرة، حيث يستغل المبتزون الفضاء السيبراني لانتزاع مكاسب مادية أو غير مادية من الضحايا عبر التهديد بكشف معلومات حساسة أو مواد ذات طبيعة شخصية. يرتبط هذا الفعل ارتباطاً وثيقاً بانتهاك مبدأ الخصوصية، الذي يكفله الدستور والقوانين الوطنية. وتتجسد هذه الجريمة في صور متعددة، أبرزها التهديد بنشر صور أو محادثات خاصة، سواء كانت حقيقية أو مفبركة، بهدف إجبار الضحية على الرضوخ لمطالب المبتز، مما يمس بالكرامة الشخصية والأمن النفسي للفرد.

²⁵ القانون رقم 04-15 المؤرخ في 1 فبراير 2015 الذي يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين

تتجاوز خطورة الابتزاز الرقمي مجرد التهديد، لتصل إلى استغلال الثقة خاصة مع ظهور التزييف العميق و أدوات الذكاء الاصطناعي التي أصبحت متاحة في الفضاء السيبراني.

ثانياً: انتهاك الحياة الخاصة عبر الإنترنت و نشر الصور و المحادثات

كفل الدستور الجزائري حماية الحقوق الأساسية والحريات الفردية مع ضمان الدولة لعدم انتهاك حرمة الإنسان، وقد أولى المشرع الجزائري اهتماماً خاصاً بهذا النوع من الجرائم، وقد تم تكريس هذه المبادئ الدستورية في التطبيق بواسطة نصوص تشريعية في قانون العقوبات وقانون الإجراءات الجزائية وفي القوانين الخاصة بالبريد والاتصالات لمجابهة الجرائم الماسة بحرمة الحياة الخاصة للأفراد، وتشمل هذه الجرائم نشر الصور والتسجيلات الصوتية والمرئية دون إذن أصحابها، وإساءة استخدام البيانات الشخصية، والتجسس على الاتصالات الخاصة.

يشكل نشر الصور والمحادثات دون رضا اعتداءً صارخاً على الخصوصية والحياة الخاصة للأفراد، وهو ما كرسته التشريعات الجزائرية من خلال تجريمه. ويستند هذا التجريم إلى حماية الحق في الصورة والحق في سرية المراسلات والاتصالات. إن إثبات عدم وجود الرضا يصبح عنصراً حاسماً في تكوين الجريمة، حيث لا يكفي مجرد نشر المحتوى، بل يجب إثبات أن النشر تم ضد إرادة صاحب الحق، وأن الأخير لم يمنح موافقته الصريحة أو الضمنية على هذا النشر. يتجلى التحدي القانوني في تحديد نطاق "الرضا" في سياق المحتوى الرقمي. فالرضا يجب أن يكون حراً، واعياً، ومحددًا، لا يحتمل التأويل. ويطرح تداول الصور والمحادثات الشخصية عبر المنصات الرقمية إشكالية مدى تطابق الرضا المسبق على الاستخدامات اللاحقة، خاصة في ظل التطور التكنولوجي السريع وانتشار تطبيقات مشاركة المحتوى. إن تفسير الرضا يجب أن يراعي الطبيعة الحساسة للمعلومات الشخصية والمخاطر المرتبطة بإساءة استخدامها.

يمثل إثبات الضرر الناجم عن نشر الصور والمحادثات دون رضا ركناً أساسياً لقيام المسؤولية الجنائية والمدنية. وقد يتخذ الضرر صوراً متعددة، تتراوح بين الضرر المعنوي

المتمثل في المساس بالسمعة والشرف والاعتبار، والضرر المادي كفقْدان الوظيفة أو التعرض لابتزاز. ويتطلب الإثبات تقديم أدلة قاطعة تثبت العلاقة السببية بين فعل النشر والضرر اللاحق، مما يمنح الضحية الحق في المطالبة بالتعويض وجبر الضرر.

لقد أولت الجزائر اهتماماً متزايداً بمكافحة هذه الجرائم، حيث تضمن قانون العقوبات وقوانين أخرى، مواد تجرم المساس بالحق في الصورة وسرية المراسلات، ومع ذلك يظل التحدي قائماً في التطبيق العملي، خاصة فيما يتعلق بجمع الأدلة الرقمية وتتبع مرتكبي الجرائم العابرة للحدود، مما يستدعي تعزيز التعاون الدولي وتحديث الأدوات التشريعية والتكنولوجية لمواكبة التطورات المتسارعة في مجال الجريمة السيبرانية.

إن معالجة قضايا نشر الصور والمحادثات دون رضا تتطلب مقاربة شاملة تجمع بين التشريع الرادع، والتطبيق القضائي الفعال، والتوعية المجتمعية. وتبرز الحاجة إلى استراتيجيات قانونية تضمن تحقيق التوازن بين حماية الحقوق الفردية ومقتضيات الأمن العام، مع ضرورة مواكبة التطورات التقنية التي قد تفتح ثغرات جديدة للإساءة. إن تطوير آليات الإثبات الرقمي وتعزيز كفاءة الجهات الضبطية والقضائية في التعامل مع هذه القضايا يعتبر أمراً حيوياً لضمان فعالية المكافحة.

ثالثاً: التحرش الإلكتروني عبر الإنترنت

نُعدّ هذه الفئة من أشد الجرائم الإلكترونية خطورةً على المجتمع، وتشمل محاولات التجنيد والاستغلال الجنسي للأطفال عبر الإنترنت، والتحرش الإلكتروني بالأحداث، وتجدر الإشارة إلى أن الجزائر تحتاج إلى تطوير منظومتها التشريعية لمواكبة المعايير الدولية لحماية الأطفال في الفضاء الرقمي. و يُعد التحرش الإلكتروني اعتداءً طالما استهدف كرامة الأفراد وطمأنينتهم، حيث يتجاوز حدود الفعل التقليدي ليغزو الفضاء الرقمي، ناشراً الأذى النفسي والاجتماعي. يتجلى هذا الاعتداء في استخدام وسائل الاتصال الحديثة، كالهواتف الذكية والمنصات الاجتماعية، لإلحاق الضرر بالضحية، سواء كان ذلك بتوجيه إهانات، أو

تهديدات، أو نشر معلومات مسيئة، مما يزعزع الاستقرار النفسي للشخص ويقوض شعوره بالأمان .

إن وصف التحرش الإلكتروني كاعتداء على الكرامة يتجسد في المساس بالصورة الذاتية للفرد وقيمه الاجتماعية، حيث يهدف المعتدي غالباً إلى إذلال الضحية وإشعارها بالعجز. فالرسائل المسيئة، والتعليقات المهينة، ونشر الصور أو الفيديوها دون موافقة، كلها أفعال تقوض الاحترام الذي يستحقه كل فرد، وتترك أثراً نفسية عميقة قد تستمر لفترات طويلة، مما يؤثر على تفاعلات الضحية الاجتماعية وتقديرها لذاتها.

أما عن الطمأنينة، فإن التحرش الإلكتروني يمس بها من خلال خلق شعور دائم بالخوف والقلق لدى الضحية. فالتهديدات المستمرة، والمراقبة الرقمية، والتخويف عبر الإنترنت، كلها ممارسات تبعث على عدم الاستقرار، وتجعل الضحية تشعر بأنها تحت المجهر، ولا تمتلك ملاذاً آمناً. هذا الشعور بالتهديد المستمر يعيق الحياة اليومية ويؤثر على القدرة على ممارسة الأنشطة الاعتيادية بحرية وأمان.

وقد استجابت التشريعات الجزائية، وإن كانت بتفاوت، لهذا التحدي، إلا أن الجرائم المتعلقة بالمساس بالكرامة والطمأنينة الرقمية تحتاج إلى تفصيل أكبر. إن التحدي يكمن في تطوير آليات قانونية قادرة على مواكبة التطور السريع للوسائل الرقمية، وتوفير حماية فعالة للضحايا، مع ضمان عدم المساس بالحريات الأساسية .

إن التحرش الإلكتروني، بصفته اعتداءً مركباً على الكرامة والطمأنينة، يتطلب مقاربة قانونية شاملة تجمع بين التجريم الواضح، والعقوبات الرادعة، وآليات وقائية فعالة.

رابعاً: الإرهاب الإلكتروني والتطرف عبر الإنترنت

يُشكّل توظيف الفضاء الإلكتروني لأغراض إرهابية تهديداً بالغ الخطورة، ويتجلى ذلك في استخدام وسائل التواصل الاجتماعي لنشر الأفكار المتطرفة وتجنيد الأعضاء وتنسيق

العمليات الإرهابية، مما يستدعي تضافر الجهود الأمنية والقانونية وهو ما دفع المشرع الجزائري إلى إدراج نصوص خاصة في إطار قانون مكافحة الإرهاب.

خامسا : خطاب الكراهية

يشكل خطاب الكراهية في الفضاء الرقمي تحدياً جوهرياً للتوازن الدقيق بين ضرورة مكافحة المحتوى الضار وضمان حرية التعبير. فبينما تهدف التشريعات إلى حماية الأفراد والمجتمعات من الأذى الذي قد ينجم عن التحريض على التمييز أو العنف، فإن القيود المفروضة على الخطاب قد تؤدي، عن غير قصد، إلى تقويض المبادئ الديمقراطية التي تعتمد على تبادل الأفكار بحرية. إن تحديد الخط الفاصل بين النقد المشروع والتعبير عن الرأي وبين خطاب الكراهية المحظور يمثل معضلة قانونية وفلسفية معقدة.

تتطلب مكافحة خطاب الكراهية الرقمي مقاربة قانونية متوازنة تأخذ في الاعتبار الطبيعة المتغيرة للفضاء السيبراني وقدرته على الانتشار السريع. إن القوانين التي تجرم التحريض على الكراهية، مثل تلك المستمدة من الإطار العام لقانون العقوبات، يجب أن تكون محددة بما يكفي لتجنب الرقابة التعسفية. فالتوسع في تفسير مفاهيم مثل "التحريض" أو "التمييز" قد يفتح الباب أمام تقييد التعبير المشروع، مما يهدد جوهر الحوار الديمقراطي.

لقد جرّم المشرع الجزائري خطاب الكراهية بموجب القانون رقم 20-05 الصادر في 28 أبريل 2020²⁶ والذي يُعد الإطار القانوني الشامل للوقاية من التمييز وخطاب الكراهية ومكافحتهما. يفرض هذا القانون عقوبات صارمة، تصل في بعض الحالات إلى السجن المؤبد، حيث تعاقب المادة 34 من هذا القانون بالسجن لمدة تصل إلى عشر سنوات لكل من "ينشئ أو يدير أو يشرف على موقع إلكتروني أو حساب إلكتروني " استناداً إلى عبارة فضفاضة من قبيل " إثارة التمييز و الكراهية في المجتمع" للحد من كل أشكال التعبير أو

²⁶ القانون 05-20 الصادر في 28 أبريل سنة 2020، المتعلق بالوقاية من التمييز وخطاب الكراهية ومكافحتهما

الأفعال التي تحرض على التمييز والتعصب ومع ذلك، يبقى التحدي في التطبيق العملي والقضائي.

إن حماية حرية التعبير لا تعني السماح بالإساءة الممنهجة أو التحريض على العنف. وبالمقابل، فإن مكافحة خطاب الكراهية لا ينبغي أن تتحول إلى أداة لقمع المعارضة أو تكميم الأفواه. يتطلب هذا تحقيق توازن دقيق من خلال وضع معايير واضحة لتحديد ما يشكل خطاب كراهية محظور، مع ضمان وجود آليات قضائية فعالة لحماية الحق في التعبير، خاصة في سياق التطورات التكنولوجية المتسارعة .

الفصل الثاني

آليات مكافحة الجريمة السيبرانية

في التشريع الجزائري

الفصل الثاني: آليات مكافحة الجريمة السيبرانية في التشريع الجزائري

يُعنى هذا الفصل بدراسة المنظومة التشريعية الجزائرية المتعلقة بمكافحة الجرائم السيبرانية، من خلال تحليل أحكام القانون رقم 04-09 باعتباره الركيزة التشريعية الأساسية في هذا المجال، ثم النصوص ذات الصلة في قانون العقوبات الجزائري وسائر التشريعات المكّلة، مع إجراء مقارنة تشريعية بنظيراتها الإقليمية والدولية.

المبحث الأول: الحماية الموضوعية للنظام المعلوماتي

يُعد القانون 04-09 الصادر في الموافق 05 غشت سنة 2009 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها ، بمثابة الإطار التشريعي الأساسي الذي سعى المشرع الجزائري من خلاله إلى مواجهة التحديات المتزايدة للجرائم المستجدة في الفضاء الرقمي. وقد حاول هذا القانون، من خلال أحكامه، وضع لبنات أولية للتصدي لهذه الظاهرة، عبر تعريف بعض الأفعال المجرمة وتحديد العقوبات المناسبة لها، مع الأخذ في الاعتبار أهمية حماية البنية التحتية الرقمية ومنظومات المعلومات.

يشكل القانون 04-09 خطوة هامة نحو تفعيل آلية المكافحة، فبالرغم من محاولته تغطية نطاق واسع من الجرائم، إلا أن التقدم التقني المتسارع قد جعل بعض نصوصه تبدو قاصرة عن مواكبة التطورات المستجدة، مما يستدعي إعادة تقييم مستمرة لمدى كفايته في توفير الحماية الشاملة. من أبرز الجوانب التي يستند إليها القانون 04-09 في سعيه للمكافحة، هو تقديمه لتعريفات قانونية لبعض المفاهيم الأساسية المتعلقة بالجرائم السيبرانية، مما يساهم في توحيد الفهم وتسهيل تطبيق النصوص. كما أنه يحدد الأفعال التي تعتبر جرائم ويعاقب عليها، مثل الوصول غير المشروع إلى الأنظمة المعلوماتية أو إعاقة سيرها. هذه الأحكام تضع الأساس القانوني لمتابعة مرتكبي هذه الجرائم.

المطلب الأول: الحماية في نصوص الملكية الفكرية

توفر نصوص الملكية الفكرية حماية قانونية صارمة ضد الجرائم السيبرانية، مثل القرصنة الرقمية والتعدي على البرمجيات وقواعد البيانات. تُلزم هذه النصوص الدول بتجريم الاستخدام غير المصرح به للمصنفات المحمية وتوفير تدابير تقنية وعقوبات رادعة للحد من التعديات عبر الإنترنت²⁷

إن الجرائم السيبرانية الماسة بالملكية الفكرية والصناعية تعتبر من الجرائم الاقتصادية الحديثة وقد تطورت صور هذه الجرائم مع التطور التكنولوجي بشكل كبير ، حيث ان بعضاً من مستخدمي التقنية الحديثة استغلها في مآرب غير مشروعة طبقاً لمصالحه، فأصبحت اجهزة النسخ السريع والحاسب الآلي بشكل عام وشبكة الانترنت على وجه الخصوص ادوات لارتكاب الجريمة .وبالرغم من أن هذه الجرائم ليست بالجديدة، إلا أن اتساع رقعة ونطاق حقوق الملكية الفكرية وظهور صور جديدة منها، فضلاً عن توسع الأنشطة الاقتصادية والتجارية مع ما افرزته تلك الأنشطة من معاملات، تركز في غالبيتها على حقوق الملكية الفكرية .إن كل ذلك أدى إلى زيادة معدلات هذه الجرائم وتأثيرها بالتالي على كافة المجالات الاقتصادية والسياسية والاجتماعية .

وفي هذا الإطار أظهر استخدام الانترنت مشكلات قانونية متعددة تتصل بحقوق الملكية الفكرية ، و من أهمها فيما يتعلق بالعلامات، كيفية تنظيم تسجيل العناوين الإلكترونية واستخدامها بشكل لا يتعارض مع حقوق أصحاب العلامات ، وخاصة بعد انتشار ظاهرة القرصنة التي تعرضت لها العلامات التجارية المشهورة ، وقد أثار ذلك التساؤل عن مدى أحقية صاحب العلامة المشهورة في منع الغير من اتخاذها كعنوان إلكتروني، .كما أثار استخدام العلامات في الانترنت التساؤل بشأن كيفية تسوية المنازعات المتعلقة بتسجيل واستخدام عنوان إلكتروني بشكل قد يتعارض مع حقوق أصحاب العلامات .

فالعلامة التجارية تعد من العناصر المعنوية للمحل التجاري وللمؤسسة كونها الوسيلة الأبرز في إجتذاب العملاء، بحيث أصبحت في كثير من الحالات أكبر عناصر المحل

²⁷ الدكتور وسيم حرب ، مشروع المجانسة الإقليمية للارشادات السيبرانية ، اسكوا ، 2012/12/12

التجاري قيمة²⁸، فهي تمثل نوعاً معيناً من الجودة لجذب العملاء إلى هذه المنتجات أو الخدمات وتفضيلها على غيرها، لهذه الأسباب كانت حماية العلامة التجارية أمراً محتماً على المشرعين في سن تشريعات خاصة لحماية هذا الحق. وبغياب تلك الحماية سوف تتعرض هذه المنتجات والسلع إلى جريمة التقليد ، ، وتقتصر الحماية الجزائية على العلامة التجارية المسجلة فقط أو التي تم إيداع طلب تسجيلها لدى المعهد الوطني للملكية الصناعية دون العلامة غير المسجلة التي لا تتمتع بأية حماية في الجزائر بخلاف بعض الدول التي تمنح للعلامة غير المسجلة والمستغلة حماية²⁹. والحماية المقررة للعلامة ترد عليها في حد ذاتها بغض النظر عن القيمة الإقتصادية للسلعة أو الخدمة المرتبطة بها .

الفرع الأول: صور الاعتداءات السيبرانية على الملكية الفكرية

أولاً: التقليد

فقد أورد المشرع الجزائري عديد من الجرائم الماسة بالعلامة التجارية وأهمها جريمة التقليد والتي تأخذ صور متعددة ، كتقليد العلامة أو مشابهتها وإستعمال علامة مقلدة أو مشابهة . وعلى ضوء ذلك سن المشرع الجزائري قانون العلامات التجارية³⁰ ومن خلال المادة 22 منه "عرف التقليد على أنه " كل عمل يمس بالحقوق الإستثنائية لعلامة قام الغير خرقاً لحقوق صاحب العلامة " وإنطلاقاً من النص فإن المشرع أخذ بالمفهوم الواسع للتقليد الذي يقصد به كل فعل أو تصرف يمس بحقوق مالك العلامة التجارية المنصوص عليها في المواد 28-22 و 11 قانون العلامات التجارية والمتمثلة أساساً في :

- تزوير العلامة التجارية المسجلة وفقاً لأحكام قانون العلامات .
- تقليد علامة بطريقة تؤدي إلى تضليل الجمهور .
- كل بيع أو إقتناء بقصد البيع أو عرض للبيع بضاعة تحمل علامة تجارية .
- غصب العلامة التجارية المملوكة للغير

²⁸ حمد الله محمد حمد الله، الوجيز في حقوق الملكية الصناعية ، دار للنشر و التوزيع العمانية ، عمان ، 1999، ص 111

²⁹ التشريع في الولايات المتحدة الأمريكية

³⁰ الأمر رقم 06-03 مؤرخ في 19 جمادى الأولى عام 1424 الموافق لـ 19 يوليو سنة 2003 المتعلق بالعلامات في الجزائر

لم يبق الأمر عند هذا الحد ، بل تفتت ظاهرة جديدة ، تتمثل في السطو الإلكتروني على عناصر الملكية الصناعية ، وخاصة على العلامات التجارية بواسطة عناوين المواقع الإلكترونية ، فامتدت قرصنة العلامات التجارية إلى شبكة الاتصالات الدولية للمعلومات ، و وجدت أنماطا جديدة للعلامة التجارية لم تكن معروفة من قبل ، تتمثل في الاعتداءات الواردة على أسماء المواقع وهي مجال جديد للمضاربة .

ثانيا :السطو الإلكتروني

فالسطو الإلكتروني على العلامات التجارية بواسطة عناوين المواقع الإلكترونية يؤدي بصورة مباشرة إلى تضليل جمهور المستهلكين، الذين يتوقعون الوصول إلى العلامة التجارية التي يريدونها ، بالاعتقاد أن العلامة التجارية هي ذاتها الموقع الإلكتروني³¹. و تتمثل أغلب صور المنازعات حول العلامة التجارية وأسماء المواقع، بتسجيل أسماء متطابقة أو متشابهة مع العلامات التجارية ، و قد تعرضت العلامات المشهورة لعمليات قرصنة عن طريق تسمية عدد من المواقع بعناوين إلكترونية تطابق أو تشابه علامات مشهورة وتسجيلها بقصد منع أصحاب هذه العلامات من تسجيل عناوين إلكترونية لمواقعهم على الشبكة تطابق علاماتهم المشهورة وابتزازهم إذا رغبوا في الحصول على تلك العناوين عن طريق طلب مبالغ مالية باهظة مقابل التنازل عنها من المعتدين. وقد أطلق على هذا النوع من الاعتداء على العلامات التجارية اصطلاح³² Cybersquatting . وهو عنوان موقع على شبكة الانترنت يسمح بتحديد الموقع وتمييزه عن غيره من المواقع . وهذه المواقع قد اكتسبت أهمية كبيرة لدى مستخدمي الانترنت ولدى رجال الأعمال والشركات الراغبين في إيجاد مواقع لهم ، تحمل أسماء جذابة بقصد جذب أكبر عدد من الزائرين، ووفقاً لسياسة تسجيل أسماء النطاق والتي تعتمد على أولوية التسجيل لمن يتقدم أولاً بطلب التسجيل، قام بعض الأفراد باقتباس أسماء مشهورة سواء لأسماء تجارية معروفة أو علامات تجارية مشهورة، وهو الأمر الذي ترتب عليه إشكالات قانونية تتعلق بهذه الأسماء والنزاع على

³¹ بوشطولة بسمه ، الحماية القانونية للعلامة التجارية، مذكرة ماجستير ، كلية الحقوق ، جامعة سطيف ، 2015، ص 53.

³² حسام الدين الصغير: حماية العلامات التجارية المشهورة، بحث مقدم لحلقة الويبو الوطنية حول الملكية الفكرية للدبلوماسيين بالتعاون مع وزارة

الخارجية العمانية بالموقع : www.wipo.int

ملكيتها ، فقد تم تسجيل العلامة التجارية "Marlboro" المشهورة التي تملكها الشركة المدعية كاسم موقع www.Marlboro.com، مما دعى بهذه الشركة أن تطلب من الجهة التي تقوم بحل منازعة أسماء المواقع المتمثلة في الـويبو بالتدخل وقد قضى فريق التحكيم بضرورة تحويل اسم الموقع للشركة المشتكية و ذلك لتطابقه مع علامتها التجارية³³.

ثالثا: التسجيل المسبق للحرمان من العلامة

و من الاعتداءات كذلك تسجيل اسم موقع www.adidas.com المتطابق مع العلامة التجارية المشهورة "ADIDAS" كذلك تم تسجيل اسم موقع www.toyota.com المتطابق مع العلامة التجارية المشهورة تويوتا "TOYOTA" اليابانية كذلك تم تسجيل اسم موقع www.marriot.com المتطابق مع العلامة التجارية "Marriot" كعنوان الكتروني . كذلك تم تسجيل اسم موقع www.pepsicola.com المتطابق مع العلامة التجارية "PEPSICOLA" للمشروبات الغازية ، حيث قام مغتصب العلامة ببيع منتجات أقل جودة من المنتجات التي تبيعها الشركة، و بالطبع بالاعتماد على شهرة العلامة التجارية³⁴. كذلك تم تسجيل العلامة التجارية التي تملكها الشركة المدعية "سوني" و هي العلامة "WALKMAN" كاسم موقع ، حكمت جهة التحكيم بضرورة إعادة اسم الموقع المسجل لشركة "سوني SONY" الأصلية كصاحبة حق العلامة³⁵.

و من القضايا التي عرضت على مركز الـويبو للتحكيم والوساطة القضية التي رفعتها شركة ميكروسوفت ضد شركة "Sventh Summit" هذا الأخير قام بتسجيل اسم الموقع www.hotmail.com المتماثل مع العلامة التجارية "HOTMAIL" التي تعود لشركة "ميكروسوفت" وقد قضى المركز بنقل اسم الموقع للشركة³⁶. و قد يقوم الشخص المسجل بعرض بيع اسم الموقع المسجل على شركة منافسة للشركة التي سجل علامتها التجارية كاسم موقع ، لإجبار هذه الشركة على شراءه ، و قد يقدم على بيعه في مواقع المزاد العلني.

³³ قضية Philip Morris Vr9.net no D2003-0004 للمزيد انظر : رامي محمد علوان: المنازعات حول العلامات التجارية وأسماء مواقع الانترنت، مقال بمجلة الشريعة والقانون، جامعة الإمارات، السنة 12، العدد 22، يناير 2011، ص 29

³⁴ موسى العطيات ، الجوانب القانونية لتعاملات التجارة الالكترونية، الطبعة الاولى، دار وائل للنشر والتوزيع، الأردن، 2011 ، ص 195 .

³⁵ قضية شركة سوني رقم 0011000096109

³⁶ انظر : قرار مركز التحكيم رقم WIPO Domain Name Decision: D2016-0951

و قد يلجأ بعض المتطفلين³⁷ بتسجيل علامة تجارية مشهورة تعود لشركة كاسم موقع لعرض منتجات أو خدمات أقل جودة من المنتجات التي تبيعها أو تقدمها الشركة بالإعتماد على شهرة العلامة التجارية المشهورة المملوكة للشركة .

و امتدت قرصنة العلامات التجارية المشهورة الى اللجوء الى حيلة اخرى في تسجيل اسم موقع شبيه أو متماثل إلي حد ما لعلامة تجارية مشهورة و مملوكة للغير ، وذلك عن طريق إدخال تعديل طفيف³⁸ على إحدى حروف العلامة التجارية التي يسجلها كاسم موقع أو إضافة كلمة للعلامة التجارية العائدة للغير ويسجلها كاسم موقع³⁹ مثال ذلك تم تسجيل كاسم موقع www.abidas.com لتضليل مستهلكي علامة Adidas و غيره من الأمثلة الأخرى .

ومن الصور الأخرى للاعتداء على العلامات التجارية في مجال المعلوماتية تسجيل اسم موقع يحتوي على علامة تجارية مع إضافة عبارات تحقيرية و تشهيرية وفي هذه الصورة من الاعتداء، فيتم تسجيل العلامة التجارية العائدة لشركة كاسم موقع مع إضافة كلمه أو عبارة تسيء للشركة قبل الاسم أو بعده ، مثال boycott.cocola.com أو I hate .

الاعتداء كذلك على العلامات التجارية في مجال المعلوماتية تسجيل علامة تجارية عائدة للغير كاسم موقع عندما يتمتع صاحبها عن تجديد تسجيله للاسم، وتحدث هذه الحالة في حالة إغفال هذه الشركة تجديد تسجيل اسم موقعها ودفع رسوم التسجيل .

و كذلك على العلامات التجارية في مجال المعلوماتية تسجيل اسم موقع يحتوي على علامة تجارية عائدة لشركة منافسة في مثل هذه الحالة، تقوم شركة من بين شركتين متنافستين تعملان في مجال واحد أو تقدم كل منهما بضائع ومنتجات واحدة، بتسجيل

³⁷ الأعمال التطفلية هي صورة حديثة من صور المنافسة غير المشروعة التي تضر بالمنافسة التجارية. انظر : حلمي محمد الحجار ، الطفيلية الاقتصادية ، منشورات زين الحقوقية ، بيروت ، 2011.

³⁸ فيعتبر التقليد " l'imitation " هو الإقتصار على مجرد نقل العناصر الأساسية للعلامة أو نقل بعضها نقلاً حرفياً مع إجراء بعض الإضافات والتغييرات، فيعد ذلك تقليداً وليس تزويراً لها ، أي وضع علامة مشابهة أو قريبة الشبه في مجموعها بعلامة أخرى أصلية ، بحيث يصعب التفرقة بين كل منهما أو تمييزهما لما يوجد من لبس و خلط بينهما في ذهن المستهلك. أما " contrefaçon " التزوير هو نقل العلامة الأصلية نقلاً كاملاً ومطابقاً بدون أي تعديل لها، فتصبح طبق الأصل للعلامة الأصلية.

³⁹ رامي محمد علوان: المنازعات حول العلامات التجارية وأسماء مواقع الانترنت، مقال بمجلة الشريعة والقانون، جامعة الإمارات، السنة 12، العدد 22، يناير 2011، ص 37

العلامة التجارية العائدة للشركة الأخرى كاسم موقع حارمة إياها من تسجيل اسم موقع يحتوي على علامتها التجارية. أو تسجيل اسم موقع يحتوي على علامة تجارية عائدة لشركة غير منافسة تقترب هذه الحالة إلي حد كبير من الحالة التي سبقتها إلا أن الفارق بينهما يكمن في أن الشركتين غير متنافستين وتعملان في تجارتين مختلفتين أو تقدمان للجمهور منتجات وخدمات مختلفة، فتقوم إحدى الشركتين بتسجيل العلامة التجارية العائدة للشركة الأخرى غير المتنافسة معها كاسم موقع ، و هذه الحالة تسمى بالطفيلية الاقتصادية ، حيث ان الشركة المتطفلة تأخذ نفس التسمية قاصدة التطفل و الإستفادة من شهرة الإسم التجاري للشركة صاحبة العلامة التجارية المشهورة.

الفرع الثاني : الحماية ووسائل التصدي للجريمة السيبرانية الماسة بحقوق الملكية الفكرية

تلعب حقوق الملكية الفكرية دوراً هاماً في عملية التنمية الاقتصادية والاجتماعية لأي مجتمع، متقدم أو نام، أو أقل نمواً ، فلا يمكن لأي دولة في عصرنا الحالي أن تتصور نفسها دون إطار قانوني لحماية الملكية الفكرية والصناعية، بحيث ينعكس ذلك على حماية منتجات الفكر الإبداعية والمعرفية خاصة مع قدوم التطورات الاقتصادية والتكنولوجية الحالية التي تجتاح العالم كله ويكتسب هذا الأمر أهمية أكبر في ظل الاقتصاد العالمي الجديد الذي يتجه بسرعة نحو صيرورته اقتصاداً معرفي أ يقوم على المعرفة والمعلومات والمنتجات الفكرية التي أصبحت تشكل قيمة مادية أساسية في هذا النظام.

انطلاقاً من ذلك، تكرست الحاجة لتعميق الوعي والإدراك العام لقوانين الملكية الفكرية التي تشكل النظام القانوني الرئيسي الذي يحمي هذا الاقتصاد الجديد وقيمه .إن هذا الوعي من المفترض أن ينعكس بشكل خاص في ثقافة وأداء الإدارات العامة والخاصة، وكل من له صلة مباشرة بتوجيه وإدارة النظام الاقتصادي وفعالياته. ولعله من الملاحظ أيضاً أن للملكية الفكرية والصناعية أهمية أكبر في مجالات الاستثمار المختلفة والمرتبطة بشكل أو بآخر بتنمية الدول، حيث أن الكثير من هذه الاستثمارات تحوي شكلاً أو أكثر من أشكال حقوق الملكية الفكرية والأسرار التجارية .في ضوء ما تقدم يتبين لنا مدى ارتباط موضوع حماية

الملكية الفكرية والصناعية بعملية الاستثمار، ففي الدول حيث نظام الملكية الفكرية ضعيف نلاحظ ارتفاع في عمليات التقليد والتعدي على حقوق الملكية الفكرية والصناعية الأمر الذي يؤدي إلى انخفاض في الاستثمار في زمن أصبح فيه الاقتصاد مرتبطاً في جنباته بكل مدخلات العولمة .

أولاً : وسائل التصدي للجريمة الإلكترونية الماسة بحقوق الملكية الصناعي

يلاحظ أن هناك طريقتين لتفادي وحل المنازعات الخاصة بالعلامات التجارية وأسماء المواقع بحيث أن الطرق التقنية الوقائية تحاول أن تمنع المنازعات، بينما القانونية علاجية تهدف إلى حل المنازعات بعد وقوعها ⁴⁰.

أ- الحل التقني الوقائي:

قد أدت هذه الاعتداءات إلى انتقال سلطة منح أسماء النطاق من هيئة الانترنت للأرقام المخصصة إلى شركة الانترنت للأسماء والأرقام المخصصة و هذا من اقتراح الإدارة الوطنية للمعلومات والاتصال الأمريكية لوضع نظام موحد يمكن إعماله على المستوى الدولي لتنظيم العناوين الإلكترونية وتسوية المنازعات المتعلقة بالتداخل بينها وبين العلامات ، و ذلك في ديسمبر 1998 ، إلا أن ذلك لم يمنع من زيادة عدد الشكاوى ⁴¹ مما دفع بالمنظمة العالمية للملكية الفكرية الويبو إلى التدخل بتوصية لشركة ICANN ⁴² باعتماد آلية السياسة الموحدة لتسوية المنازعات على أسماء النطاق ، وبالإضافة إلى ذلك فقد طلبت الدول الأعضاء في الويبو إعداد دراسة حول هذا الموضوع واقتراح الحلول الملائمة لمعالجة

⁴⁰رامي محمد علوان: المنازعات حول العلامات التجارية وأسماء مواقع الانترنت، مقال بمجلة الشريعة والقانون، جامعة الإمارات، السنة 12، العدد 22، يناير 2011، ص 52

⁴¹وصلت عدد الشكاوى في ديسمبر 2008 إلى 11221 شكوى يخص المواقع المنتهية بـ .com. نسبة 02% من جملة الشكاوى وفقاً لسياسة UDRP للمزيد راجع الوثيقة Pr/2009/585 الصادرة عن منظمة الويبو، جنيف في 12 مارس 2009

⁴² اختصار لـ The internet corporation for assigned names and numbers هيئة الإنترنت للأسماء والأرقام المخصصة (الآيكان) منظمة غير ربحية تم تأسيسها دولياً لتتولى مسؤولية توزيع مجالات العناوين في بروتوكول الإنترنت وتخصيص معرفات البروتوكول وإدارة نظام سجلات المواقع العامة عالية المستوى (gTLD) وسجلات المواقع عالية المستوى لرمز الدولة (ccTLD) ، كما أنها تضطلع بمسؤولية وظائف إدارة نظام الخوادم المركزية. وقد كانت هذه الخدمات تقدم أصلاً، بموجب عقد حكومي أمريكي، من قبل سلطة تخصيص أسماء الإنترنت (IANA) وغيرها من الهيئات، أما الآن فتقوم الآيكان بالمهام التي كانت تؤديها السلطة .

وتقوم الآيكان بمراقبة توزيع المعرفات الفنية المستخدمة في عمليات الإنترنت، وتخصيص أسماء المواقع العليا ومثال ذلك .info, .com, وغيرها

المشكلات التي ظهرت في التطبيق فيما يتعلق بالتدخلين العناوين الإلكترونية والعلامات ، وقد أعدت منظمة الويبو دراسة تفصيلية حول هذا الموضوع بعد استطلاع آراء المتخصصين في العديد من الدول الأعضاء ، وأسفرت الدراسة عن مجموعة من التوصيات و اقترحت نظاما لتسوية المنازعات المتعلقة بالعناوين الإلكترونية والعلامات وتضمنت أهم التوصيات بتقرير الويبو ما يلي :

- التأكيد على ضرورة تقديم طالب عنوان إلكتروني لكافة البيانات الخاصة بالتعرف عليه والاتصال به .
- عدم تسجيل عناوين إلكترونية تماثل العلامات المشهورة أو المعروفة جدا إلا إذا كان طالب التسجيل هو صاحب العلامة، أو كان التسجيل بموافقته .
- أن يطلب من المتقدم لتسجيل العنوان الإلكتروني إتباع إجراءات التقاضي والوسائل البديلة لتسوية المنازعات المتعلقة بالعنوان الإلكتروني .
- أن يقبل طالب التسجيل السياسة الموحدة لتسوية المنازعات التي يتم اعتمادها، و هي تنظيم إجراءات فض المنازعات المتعلقة بالعناوين الإلكترونية بطريقة عملية ومبسطة .

ب : الحماية القانونية العلاجية :

1-الحماية الاجرائية: الحماية الاجرائية (الإدارية) لعناصر الملكية الصناعية من أعمال القرصنة الالكترونية تكتسي أهمية بالغة ، حيث تعتبر الإجراءات الإدارية من بين التدابير القاعدية في كثير من البلدان لكي يمنح للشخص الحق بطلب حماية إبداعه فيعتبر التسجيل الإداري الخطوة الأولى التي تُمهّد إلى طريق طلب حماية عناصر الملكية الصناعية ، و حيث ينتج عنه وثيقة إدارية تثبت وجود إبتكار معين او إبداع وبإسم صاحبه الذي يحق له الإعتراض على كل مساس بإبداعه الفكري واللجوء إلى القضاء في حالة الاعتداء غير المشروعة على الملكية الصناعية والماسة بإبداعه الفكري .

إن التشريعات الوطنية تعهد في قوانينها الداخلية إلى جهات إدارية متخصصة⁴³ بواجبات تتعلق بتسجيل حقوق الملكية الصناعية وما يقترن بذلك من صلاحيات محددة لتلك الجهات والقائمين عليها في الرقابة الكاملة لما يعرض من حقوق الملكية الصناعية يراد تسجيلها، و إضفاء الصفة القانونية عليها وما يترتب على ذلك من أحكام خاصة بحمايتها .

وعلى هذا النهج سارت معظم التشريعات في أفراد نصوص قانونية خاصة متعلقة بتسجيل حقوق الملكية الصناعية، وما يرتبط بذلك من ضوابط وأحكام ممنوحة لجهة الإدارة عند تقديم طلب التسجيل⁴⁴، وتتمثل مهام هذه الجهات المختصة في قبول إيداع وفحص وتسجيل كافة حقوق الملكية الصناعية من علامات تجارية، براءة الاختراع.. الخ .

2-الحماية القضائية: من الثابت أن التعدي على حقوق الملكية الصناعية دوماً يترتب عنه أضراراً مباشرة تمس بصاحب الحق و أضراراً غير مباشرة تمس بالسوق و بالمصلحة الاقتصادية العامة و بالإضافة إلى الأضرار بحقوق المستهلك .

■ دعوى المنافسة غير المشروعة: فقد أحاطت التشريعات المقارنة حقوق الملكية الصناعية بحماية مدنية من كل أعمال غير مشروعة، عن طريق رفع دعاوى قضائية كآلية قانونية للحد من الأعمال التنافسية غير النزيهة و من التجاوزات التي تشكل إعتداء أو عمل ضار غير مشروع على تلك الحقوق. وتعد منازعات أسماء المواقع الوطنية من المنازعات الجديدة الصعبة وذلك لأسباب متعددة منها أن شروط تسجيل أسماء المواقع وإجراءات التسجيل تختلف اختلافاً بيناً فيما بين الدول، كما أن القوانين التي يمكن

⁴³ فالقانون أوكل مهمة تسجيل حقوق الملكية الصناعية ورقابتها في كافة الجوانب الإدارية المتعلقة بالتسجيل إلى جهة متخصصة في الجزائر تسمى بالمعهد الوطني الجزائري للملكية الصناعية حسب نص المادة 11 من قانون العلامات الجزائري ، أما المشرع الأردني أعهد هذه المهمة إلى جهة خاصة تسمى "دائرة تسجيل حقوق الملكية الصناعية أما المشرع المصري أو كل الاختصاص لمصلحة التسجيل التجاري" أما المشرع الفرنسي أو كل الاختصاص إلى المعهد الوطني الفرنسي للملكية الصناعية أما المشرع المغربي أوكلها للمكتب المغربي للملكية الصناعية. للمزيد أكثر أنظر : فرحة زراوي صالح، الكامل في القانون التجاري، الجزائر ، ص 212.

⁴⁴ لهذا لم يكن المشرع الجزائري بمعزل عن تلك الحماية مكتفياً بالحماية المدنية و الجزائية ، بل فرض الحماية الادارية ، فقد أوكل هذه الحماية الى الادارة و ذلك من خلال المسجل الذي يمثل الادارة في تسجيل الحقوق أو رفضه و فرض الحماية المقررة.

الاعتماد عليها لحل منازعات أسماء المواقع تختلف كذلك من دولة الى أخرى⁴⁵، و هناك مواقف متباينة للدول فقد تبنت بعض الدول قوانين خاصة بحل المنازعات حول العلامات التجارية وأسماء المواقع ، وسنت لهذه الغاية قوانين جديدة لحماية العلامات التجارية في الفضاء الالكتروني، بينما نجد بعض الدول سكنت عن مسألة منازعات العلامات التجارية في الفضاء الالكتروني ، و من بينها المشرع الجزائري و السبب راجع لتأخر الجزائر في إستخدام تكنولوجيا المعلومات و الانترنت و الذي كان حائلاً في إصدار تشريع خاص يكفل الحماية الفعالة للأنظمة المعلوماتية و يحفظ حقوق أصحاب الملكية الصناعية من مخاطر الاستخدام السيئ لتكنولوجيا المعلومات ، لذلك أدركت الجزائر ضرورة عدم الاكتفاء بالنصوص التقليدية والثغرات القانونية ، فقد أصدرت قانون رقم 04 / 09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال و مكافحتها ، و كان ذلك رغبة منه لمواكبة التشريع الدولي بخصوص مكافحة الجريمة المعلوماتية و بالأخص الاتفاقية الدولية حول الإجرام المعلوماتي التي أبرمت في 2001 من طرف المجلس الأوروبي ، فهذا التجريم يهدف الى حماية المنظومة المعلوماتية ، لكن الملاحظ ان المشرع لم يبسط حماية خاصة للملكية الصناعية من الجريمة المعلوماتية⁴⁶.

■ **دعوى التقليد:** فقد بسطت التشريعات المقارنة حماية جنائية عن طريق رفع دعاوى التقليد ، يقوم صاحب العلامة التجارية المسجلة كاسم موقع برفع دعوى التقليد أمام

⁴⁵ Cass.com. 13 déc. 2005, JCP 2006, n 6-7, P. 289, note Christophe Caron Cahen (Murielle), Premier arrêt de la publication le 8 Mars 2006 sur le site www.legalbiznext.com cour de cassation sur les noms de domaine

⁴⁶ أكد المشرع الجزائري حماية لبرامج الحاسوب و قاعدة البيانات من خلال النص على تجريم الاعتداء على حقوق المؤلف على إعتبار الحاسوب و قاعدة البيانات من بين المصنفات الادبية المحمية طبقاً للمادة 4 من قانون رقم

03 / 05 المتضمن حقوق المؤلف و الحقوق المجاورة

محكمة ذات اختصاص على المسجل لاسم الموقع من دون وجه حق ويكون ذلك بالنسبة لأسماء المواقع الوطنية المكونة من رموز الدول المسجلة⁴⁷.

ويشترط لرفع الدعوى بصورة مستعجلة توافر شرطين هما ظهور جدية الدعوى و وضوح الأدلة لكسبها ، وفي هذه الدعوى يأمر بوقف استمرار الأفعال الدالة على التقليد ، كما يجوز له توقيع غرامة تهديدية لإجبار المقلد على وقف كافة أشكال التقليد، وقد تم نظر دعاوى كثيرة تتعلق بأسماء النطاق وتم تطبيق أحكام قانون الملكية الفكرية وقانون الإجراءات المدنية، لكي يتمتع اسم النطاق بالحماية في دعوى التقليد ضرورة تحقق الشروط التالية :

- أن يكون اسم النطاق مسجلاً سابقاً على أي علامة مميزة .
- أن يكون اسم النطاق والعلامة متطابقين في المنتجات أو الخدمات أو متماثلين .
- أن يؤدي التطابق أو التماثل بين الاسم والعلامة إلى حدوث لبس لدى الجمهور .

3 -الحماية في إطار قانون الملكية الصناعية الجزائري

نظرا لنسبية الحماية المقررة من خلال النصوص التقليدية في قانون العقوبات الجزائري كما سبق ذكره ارتأينا البحث في مدى إمكانية الحماية من خلال نصوص قانون الملكية الفكرية :هل تستفيد برامج الحاسب الآلي من الحماية الجنائية للعلامات التجارية ؟

نعلم أن كل برنامج يحمل اسما خاصا به، لذلك فقد عمد أصحاب البرامج إلى تسجيل هذا الاسم كعلامة تجارية للبرنامج، ولما كانت هذه الحماية قاصرة على الاسم دون المحتوى فقد لجأ أصحاب البرامج إلى وضع الاسم مقترنا به .

لحماية العلامات التجارية بإحكام بالشروط التي يجب توافرها في الاختراع فتتمثل فيما يلي :

شرط الابتكار، شرط الجودة ،القابلية للتطبيق الصناعي، المشروعية .

في حال توافر هذه الشروط يتحصل المخترع على براءة الاختراع وهي الوثيقة التي تمنحها الدولة للمخترع فتخول له حق استغلال اختراعه والتمتع بالحماية القانونية المقررة لهذا الغرض وذلك لمدة محدودة وبشروط معينة والجهاز المانح لهذه الشهادة هو المعهد الجزائري لحماية الملكية الصناعية .

⁴⁷ وصف المشرع الجزائري الاعمال غير المشروعة في مجال المنافسة بين الاعوان الاقتصاديين بغير النزيفة بموجب المواد من 26 الى 28 من القانون 02 /04 السالف الذكر.

4-الحماية الدولية:

نظرا للأهمية البالغة لحقوق الملكية الفكرية، عمل المشرع الدولي على حمايتها، وسنت الدول القوانين والأنظمة التي تحدد ضوابط حماية هذه الحقوق، مما يوفر لأصحابها المناخ الملائم للابتكار والإبداع فينعكس ذلك إيجابا على المجتمع .

بسبب الخسائر التي تلحق بالإقتصاد نتيجة التعدي على حقوق الملكية الفكرية والصناعية وتزايد حالات الغش وتقليد العلامات الصناعية والتجارية وقرصنة اسماء المواقع ، بل إن الدول العظمى وبما تمثله من قوة إقتصادية و وزن سياسي ، فلقد تدخل المشرع الدولي باتفاقيات تواكب التطور الحاصل في مجال المعلوماتية ، مما أوجد رغبة ملحة لبسط الحماية القانونية لحقوق الملكية الفكرية والصناعية في كل دولة تستغل فيها هذه الحقوق، وذلك كون الحماية الداخلية لم تعد فعالة في حماية حقوق الملكية الصناعية عامة و العلامات الأجنبية خاصة وذلك لسهولة إنتقال السلع والخدمات عبر القارات .

وتزايد العلاقات الدولية الاجتماعية والاقتصادية والتجارية وانتشار الفكر الانساني عبر الحدود.وتكمن أهمية توفير الحماية لحقوق الملكية الفكرية والصناعية على المستوى الدولي في ضمان حقوق المخترعين والمبدعين وأصحاب الملكية الفكرية بشكل عام في بلدان العالم أجمع، فهي تعد شرطا لازما لتشجيع الإبداع وتقدمه وتنميته تلك الاعتبارات أملت ضرورة ملحة على المجتمع الدولي لايجاد وسائل فاعلة تتمثل في اطر قانونية دولية لحماية الملكية الفكرية. فكان ان ابرمت اتفاقيات دولية كي تضع إطارا للحماية ومنها اتفاقية بيرن لحماية المصنفات الأدبية والفنية واتفاقية باريس لحماية الملكية الصناعية، واتفاقية الجوانب المتصلة بالتجارة من حقوق الملكية الفكرية" تريبيس 8 "، إضافة إلى التوجيه الأوروبي المتعلق بإنفاذ حقوق الملكية الفكرية.

المطلب الثاني: الحماية في قانون العقوبات

يشكل قانون العقوبات الجزائري، في صيغته الأصلية، إطاراً تقليدياً لمواجهة الجرائم في حين أن تعديل 06-24 يمثل خطوة هامة في تعزيز حماية الخصوصية والاعتبار في البيئة الرقمية الجزائرية، حيث سعى المشرع إلى سد ثغرات قانونية كانت تعيق المكافحة الفعالة لبعض الجرائم المستحدثة. إلا أن النطاق التطبيقي لهذا التعديل فيما يتعلق ببعض الجرائم يستدعي تحليلاً دقيقاً لمدى توافقه مع المبادئ العامة لحماية الحقوق والحريات، خاصة فيما يتعلق بتوازن العقوبات.

في سياق حماية الاعتبار، يثير تعديل 06-24 تساؤلات حول كفاية النصوص لضمان ردع كافٍ ضد جرائم القذف والسب الإلكتروني، خاصة وأن طبيعة الفضاء الرقمي تسمح بانتشار واسع وسريع للمعلومات المسيئة. ورغم أن المشرع أقر ببعض الأفعال كجرائم، إلا أن العقوبات المقررة قد تبدو في بعض الأحيان غير متناسبة مع جسامة الضرر اللاحق بالضحية، مما يفتح الباب للنقد حول فعالية الحماية.

أما فيما يتعلق بالعقوبات البديلة، فإن إدراج مفهوم المراقبة الإلكترونية كأداة لتنفيذها، عند الاقتضاء، يشكل تطوراً ملحوظاً في استراتيجية المكافحة، هذه الآلية إذا ما تم تنظيمها بشكل دقيق وتحديد شروط تطبيقها بصرامة، يمكن أن تساهم في تخفيف الاكتظاظ في المؤسسات العقابية مع تحقيق أهداف الردع والإصلاح، وهو ما يتطلب تدقيقاً في آليات التنفيذ والرقابة عليها و من ناحية أخرى، تجدر الإشارة إلى أن تطبيق تعديل 06-24 يجب أن يتم في إطار متكامل مع النصوص القانونية الأخرى ذات الصلة، مثل قانون 04-09 و قانون 07-18 المتعلق بحماية البيانات الشخصية. إن غياب التنسيق الكامل بين هذه النصوص قد يؤدي إلى تضارب أو فراغ تشريعي، مما يضعف فعالية منظومة المكافحة الشاملة ويؤثر على ضمانات الأفراد.

ختاماً، ورغم مساهمة تعديل 06-24 في تطوير الإطار القانوني لمكافحة الجرائم السيبرانية⁴⁸، فإن الحاجة إلى مزيد من التقييم النقدي والتطوير المستمر تظل قائمة. يجب أن يواكب المشرع التطورات التكنولوجية المتسارعة وأن يضمن توازناً دقيقاً بين مكافحة الجريمة وحماية الحقوق الأساسية، مع التأكيد على ضرورة تفعيل آليات المراقبة والرقابة لضمان التطبيق السليم للقانون.

الفرع الأول : مبدأ الشرعية الجزائية

إن مبدأ الشرعية الجزائية، المتجذر في كونه ضماناً أساسية لحقوق الأفراد، يفرض ضرورة وضوح النص القانوني المنظم للجرائم السيبرانية. ففي ظل الطبيعة المتطورة والسريعة لهذه الجرائم، يصبح من الضروري أن تكون الأفعال المجرمة والملاحق عليها محددة بدقة، لتجنب أي توسع غير مشروع للسلطة العقابية للدولة، والذي قد يمس بالحقوق الأساسية للأفراد في هذا الفضاء الرقمي.

يقتضي هذا الوضوح ضرورة تحديد الأفعال المادية التي تشكل الجريمة السيبرانية بعبارات لا تحتمل التأويل. فغموض النصوص قد يفتح الباب أمام تفسيرات واسعة من قبل جهات الضبط والقضاء، مما يؤدي إلى مساءلة أفراد عن أفعال لم تكن محل تجريم صريح وقت ارتكابها، الأمر الذي يتعارض مع مبدأ عدم رجعية القانون الجنائي. فالنص الواضح هو حاجز يحمي الأفراد من التعسف.

إن التحدي يكمن في صياغة قوانين مرنة بما يكفي لمواكبة التطور التقني، ولكنها في الوقت ذاته محددة بوضوح لتجنب التوسع غير المشروع. فالتشريعات الجزائية المتعلقة بالجرائم السيبرانية، كما يجب أن تضع تعريفات دقيقة للأفعال، وتحدد الأركان المادية والمعنوية لكل جريمة.

⁴⁸ قانون رقم 06-24 مؤرخ في 19 شوال عام 1445 الموافق 28 أبريل سنة 2024 ، يهدف هذا القانون إلى تعديل وتنظيم الأمر رقم 66-156 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 والمتضمن قانون العقوبات، المعدل والمتمم.

يجب أن تتجنب التشريعات استخدام عبارات فضفاضة أو عامة قد تسمح بتكليف أفعال جديدة على أنها جرائم دون وجود نص صريح. إن التوسع القضائي في تفسير النصوص التي تنظم الجرائم السيبرانية، مثل تلك المتعلقة بالوصول غير المشروع إلى الأنظمة المعلوماتية أو اعتراض البيانات، ينبغي أن يتم بحذر شديد، مع الالتزام بمبدأ الشرعية الذي يقتضي التجريم بالنص الصريح والواضح .

لذلك، فإن ضرورة وضوح النص في الجرائم السيبرانية ليست مجرد مطلب شكلي، بل هي متطلب جوهري لضمان سيادة القانون وحماية الحقوق والحريات في الفضاء الرقمي. فالتشريع الواضح والمحدد هو الأداة الفعالة لمواجهة التحديات التي تفرضها الجرائم السيبرانية، مع الحفاظ على الضمانات الأساسية للمتهمين والمجتمع ككل .

الفرع الثاني : التناسب في التجريم والعقوبة

يُعد مبدأ التناسب في التجريم والعقوبة حجر الزاوية في تحقيق العدالة الجنائية، خاصة في ظل التحديات التي تطرحها الجرائم السيبرانية. فخطورة الفعل الرقمي تتراوح بين الاعتداءات البسيطة على البيانات والأفعال التي تهدد الأمن القومي، مما يستوجب موازنة دقيقة بين جسامة الفعل المرتكب وشدة العقوبة المقررة. إن غياب هذا التناسب قد يؤدي إلى إفراط في العقاب أو تقصير فيه، كلاهما يضر بالمصلحة العامة ويثبط من عزيمة المشرع في إيجاد حلول ناجعة.

إن تفاوت الضرر الناجم عن الجرائم السيبرانية يفرض على المشرع الجزائري ضرورة تبني مقاربة تشريعية مرنة. فقد يتسبب هجوم إلكتروني في خسائر مادية محدودة لأفراد، أو قد يؤدي إلى شلل في قطاعات حيوية أو المساس بالسمعة الدولية للدولة. لذا، يتطلب تحقيق التناسب في التجريم والعقوبة تصنيفاً دقيقاً للأفعال المجرمة سيبرانياً، مع الأخذ في الاعتبار القصد الجنائي، والنتيجة الضارة، وطبيعة الأموال أو البيانات المستهدفة .

في هذا السياق، تواجه التشريعات الوطنية، بما في ذلك قانون 09-04 المتعلق بالجرائم السيبرانية، تحدياً يتمثل في مدى قدرتها على مواكبة التطور التكنولوجي السريع. فعقوبات غير متناسبة قد تفتح الباب أمام ثغرات قانونية يستغلها المجرمون، أو قد تثقل كاهل النظام القضائي بعقوبات لا تتناسب مع خطورة الفعل، خصوصاً مع تنامي جرائم مثل الاحتيال الإلكتروني أو المساس بالمعطيات الشخصية.

إن تحقيق التناسب في العقوبة يتطلب أيضاً النظر إلى الجوانب الوقائية والإصلاحية. فالهدف ليس فقط معاقبة الجاني، بل ردعه وردع غيره، وتأهيل المخطئين. ومن هذا المنطلق، يجب أن تتضمن العقوبات المقررة في القانون الجزائري، خيارات متنوعة بين الغرامات والعقوبات السالبة للحرية، مع مراعاة الظروف المشددة والمخففة، بهدف تحقيق العدالة وتجنب التطرف في تطبيق الجزاء .

من ناحية أخرى، فإن تفاوت الضرر في الجرائم السيبرانية، والذي قد يمتد من التأثير على الأفراد إلى زعزعة استقرار الدول، يستدعي تكييف العقوبات لتشمل مسؤولية الأشخاص المعنويين، كما نصت عليه بعض التشريعات الحديثة. إن تطبيق مبدأ التناسب يقتضي أن تكون العقوبة رادعة بما يكفي لتغطية أقصى صور الضرر المحتمل، مع إمكانية التخفيف في الحالات الأقل خطورة، وذلك لضمان فعالية المكافحة وتحقيق الردع العام والخاص .

الفرع الثالث : المسؤولية الجزائية للشخص الطبيعي

إن تحديد المسؤولية الجزائية للشخص الطبيعي عن الجرائم السيبرانية يركز على ضرورة إثبات ركنيها المادي والمعنوي. فالجانب المادي يتمثل في الفعل أو الامتناع عن فعل يخالف القانون، كالاختراق أو الاحتيال الإلكتروني. أما الجانب المعنوي، فيتطلب إثبات وجود القصد الجنائي أو الخطأ، وهما عنصران جوهريان لتأسيس المسؤولية، ما لم ينص القانون على غير ذلك كالمسؤولية الموضوعية في حالات استثنائية.

يتجلى القصد الجنائي في الجرائم السيبرانية كإرادة حرة لإتيان الفعل المجرم مع العلم بغير المشروعته ونتائجه المحتملة. ويتطلب تقديره في هذا السياق إثبات علم الجاني بأن فعله يمس بالأمن السيبراني أو ينتهك خصوصية الأفراد أو يضر بالبيانات. وقد يتم استنتاج هذا العلم من ظروف وملابسات ارتكاب الجريمة، ومن الأدوات المستخدمة، وطريقة التنفيذ.

أما الخطأ، فيتمثل في الإهمال أو عدم التبصر أو عدم الاحتياط، وهو ما يقع في الجرائم السيبرانية غير العمدية. فعلى سبيل المثال، قد تنشأ المسؤولية عن عدم اتخاذ التدابير الأمنية الكافية لحماية نظام معلوماتي، مما يؤدي إلى اختراقه. إن التمييز بين القصد الجنائي والخطأ له أهمية بالغة في تحديد طبيعة الجريمة وتكييفها القانوني، وبالتالي تطبيق العقوبة المناسبة.

وفي هذا الإطار، تبرز التحديات في إثبات القصد الجنائي والخطأ في البيئة السيبرانية، نظراً لطبيعتها الافتراضية وتعدد الفاعلين المحتملين وصعوبة تتبع آثار الجريمة. فالأدلة الرقمية قد تكون متغيرة أو قابلة للتعديل، مما يستدعي تطوير آليات تقنية وقانونية متقدمة للتعامل مع هذه القضايا.

لقد سعى المشرع الجزائري إلى معالجة هذه الإشكالات من خلال قانون 04-09 المتعلق بالجرائم السيبرانية، محاولاً توفير إطار قانوني لمكافحتها. ورغم التحديثات اللاحقة، تظل الحاجة ماسة إلى مزيد من التفصيل والتوضيح في مجال إثبات الركن المعنوي، لضمان تحقيق العدالة وتطبيق القانون بفعالية .

وبذلك يتضح أن محور "المسؤولية الجزائية للشخص الطبيعي" لا ينفصل عن البناء العام للدراسة، لأنه يربط بين تحديد السلوك محل التجريم، وضمانات التطبيق، ومتطلبات الوقاية المؤسسية. وتبقى القيمة التحليلية لهذا المحور في قياس قدرة القاعدة القانونية على إنتاج حماية عملية، لا في الاكتفاء بتأكيد وجود النص.

أولاً : المسؤولية داخل المؤسسات

يُعد ضعف حماية الأنظمة المعلوماتية داخل المؤسسات بيئة خصبة لارتكاب الجرائم السيبرانية، مما يطرح إشكالية قانونية معقدة تتعلق بالمسؤولية. فإذا تعرضت مؤسسة للاختراق بسبب ثغرات أمنية يعلم بها القائمون عليها أو كان بإمكانهم العلم بها، فهل تقتصر المسؤولية على الفاعل المباشر للجريمة؟ أم تمتد لتشمل المؤسسة نفسها؟ هذا التساؤل يتطلب تحليلاً دقيقاً لمفاهيم الإهمال، والتقصير، والمساهمة في الجريمة.

إن عدم اتخاذ المؤسسات الاحتياطات اللازمة لحماية أنظمتها، كعدم تحديث البرمجيات، أو عدم توفير التدريب الكافي للموظفين على الأمن السيبراني، أو حتى ضعف الرقابة على الوصول إلى البيانات الحساسة، يمكن أن يشكل أساساً للمسؤولية. فقد تُعتبر هذه الأفعال أو التقصيرات بمثابة مساهمة سلبية في وقوع الجريمة، خاصة إذا أدت بشكل مباشر إلى تمكين المجرم السيبراني من تحقيق هدفه .

في السياق الجزائري، يمكن استقراء بعض المبادئ التي قد تنطبق على هذه الإشكالية من خلال القوانين المتعلقة بالجرائم المعلوماتية، مثل القانون 04-09 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها. ورغم أن هذه النصوص تركز غالباً على الفاعل المباشر، إلا أن مبادئ المسؤولية المدنية والجنائية قد تفسح المجال لتحميل المؤسسة المسؤولية في حالات الإهمال الجسيم.

إن غياب آليات واضحة للتجريم المباشر للمسؤولية المؤسسية عن ضعف حماية الأنظمة، لا يعني بالضرورة انعدامها. فالمحاكم قد تلجأ إلى تفسير النصوص القانونية القائمة، أو إلى تطبيق المبادئ العامة للقانون، للوصول إلى حلول عادلة. وقد يظهر هذا في إطار المسؤولية المدنية للمؤسسة عن الأضرار التي لحقت بالغير نتيجة لتقصيرها الأمني

تتفاقم الإشكالية عندما تكون هناك قوانين ولوائح تنظيمية، مثل تلك التي قد تنظمها المراسيم التنظيمية كمرسوم 271-19⁴⁹، لكن المؤسسات لا تلتزم بتطبيقها، هنا يصبح ضعف الحماية نتيجة عصيان للقانون، مما يعزز من احتمالية تحميل المؤسسة مسؤولية، سواء كانت جزائية أم مدنية، عن الجرائم التي تقع نتيجة هذا التقصير المتعمد أو الناجم عن إهمال جسيم.

وبذلك يتضح أن محور "المسؤولية داخل المؤسسات" لا ينفصل عن البناء العام للدراسة، لأنه يربط بين تحديد السلوك محل التجريم، وضمانات التطبيق، ومتطلبات الوقاية المؤسسية. وتبقى القيمة التحليلية لهذا المحور في قياس قدرة القاعدة القانونية على إنتاج حماية عملية، لا في الاكتفاء بتأكيد وجود النص.

ثانياً: الضحية الرقمية

يمثل مفهوم "الضحية الرقمية" محوراً أساسياً في فهم طبيعة الجرائم السيبرانية وتحديد نطاق تأثيرها، حيث يتجاوز التحديد التقليدي للضحية ليشمل نطاقاً أوسع من الكيانات المتضررة. لا يقتصر الأمر على الأفراد الذين يتعرضون للاحتيال أو الابتزاز الإلكتروني، بل يمتد ليشمل المؤسسات الاقتصادية والشركات التي تتكبد خسائر فادحة جراء اختراق أنظمتها وسرقة بياناتها الحساسة، مما يؤثر سلباً على استمراريتها وسمعتها .

كما أن الإدارة العامة ليست بمنأى عن هذه التهديدات، فالتعرض لهجمات سيبرانية قد يشل خدمات حيوية للمواطنين، ويضر بالثقة في قدرة الدولة على حماية بياناتهم الشخصية ومعلوماتهم الحكومية. إن تزايد الاعتماد على البنية التحتية الرقمية يجعل من هذه الجهات أهدافاً مغرية للمجرمين السيبرانيين، الذين يسعون لتعطيل العمليات أو ابتزاز الحكومات.

تتجسد أهمية الضحية الرقمية أيضاً في انعكاساتها على مفهوم "الثقة الرقمية"، فكل اعتداء ناجح يضعف ركائز هذه الثقة. عندما يشعر المستخدمون بعدم الأمان في التعاملات

⁴⁹ المرسوم 271-19 الصادر في 07 أكتوبر 2019 يتضمن انشاء المرجع الوطني لتوافقية أنظمة المعلومات

الرقمية، سواء على المستوى الفردي أو المؤسسي، تتراجع المشاركة في الاقتصاد الرقمي وتتعرض مبادرات التحول الرقمي .

يبرز القانون الجزائري، خاصة في إطار (قانون 09-04)، محاولات لتحديد الأفعال المجرمة التي تمس بهذه الكيانات، وإن كان التركيز غالباً ما يكون على الفعل المادي أكثر من استقصاء عمق الضرر الذي يلحق بالضحية الرقمية بمفهومها الواسع.

إن التحليل النقدي للمفهوم يستدعي توسيع نطاق الحماية ليشمل جميع أشكال الضرر، المادي والمعنوي، التي تلحق بالأفراد والمؤسسات والإدارة، مع التركيز على إعادة بناء الثقة الرقمية كهدف استراتيجي لمكافحة الجرائم السيبرانية.

ثالثاً : العنف الرقمي ضد الأفراد

يمثل العنف الرقمي ضد الأفراد تحدياً متزايداً يتجاوز حدود المكان والزمان، حيث تستغل الأفعال الإجرامية طبيعة الفضاء السيبراني لتمارس أشكالاً مختلفة من الإيذاء. ويندرج ضمن هذه الظاهرة جرائم الابتزاز والتشهير، والتي تستهدف في جوهرها كرامة الفرد وسمعته. فالابتزاز الرقمي، على سبيل المثال، يعتمد على تهديد الضحية بنشر معلومات حساسة أو محرجة، غالباً ما تكون قد تم الحصول عليها بطرق غير مشروعة، بهدف انتزاع مال أو منفعة. أما التشهير الرقمي، فيتجسد في نشر معلومات كاذبة أو مسيئة بقصد المساس بسمعة الشخص أو شرفه، مما يلحق به أضراراً معنوية واجتماعية جسيمة.

تتعدد صور العنف الرقمي، إلا أن الابتزاز والتشهير يبرزان كأدوات قوية للتخويف والإضرار بالأفراد في البيئة الرقمية. فالضحية في حالة الابتزاز تجد نفسها في موقف ضعف شديد، حيث يتعرض خصوصيتها للتهديد المباشر، مما يفرض عليها ضغوطاً نفسية هائلة لاتخاذ

قرارات قد تكون قسرية. أما التشهير، فيؤثر على النسيج الاجتماعي للضحية، وقد يؤدي إلى عزلتها وفقدان ثقة المحيطين بها، مما يتطلب تدخلاً قانونياً حازماً لحماية حقوقها.

تتطلب مكافحة هذه الجرائم فهماً عميقاً لطبيعتها المتغيرة وتأثيراتها على الضحايا. إن الحماية القانونية تتجاوز مجرد التجريم والعقاب، لتشمل آليات وقائية واستراتيجيات فعالة لدعم الضحايا. فالتشريعات الجزائرية، تسعى إلى معالجة هذه الإشكاليات، إلا أن التحدي يكمن في مدى فعالية تطبيقها وسرعة مواكبتها للتطورات التقنية المستمرة .

يبرز دور الضحية في عملية المكافحة من خلال الإبلاغ والتعاون مع الجهات المختصة. إن تشجيع الضحايا على تقديم الشكاوى، وتوفير سبل آمنة وسرية لذلك، يعد خطوة أساسية لكشف الجناة وتقديمهم للعدالة. كما أن الوعي المجتمعي بأخطار العنف الرقمي، وتعزيز ثقافة الإبلاغ، يساهمان في بناء بيئة رقمية أكثر أماناً للجميع.

تتطلب فعالية الحماية القانونية للعنف الرقمي، وخاصة الابتزاز والتشهير، مقاربة متعددة الأوجه. يشمل ذلك تطوير النصوص القانونية لمواكبة التحديات الجديدة، وتوفير آليات دعم نفسي واجتماعي للضحايا، وتعزيز التعاون الدولي لتبادل المعلومات والخبرات في مجال مكافحة الجرائم السيبرانية . إن تحقيق التوازن بين حماية الحقوق الأساسية للأفراد ومواجهة التهديدات المتزايدة في الفضاء الرقمي هو جوهر العملية الوقائية.

المطلب الثالث: الحماية في قانون الوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال

لم يقتصر المشرع الجزائري على القانون 04-09 في تجريم السلوكيات الإلكترونية الضارة بل أدرج في قانون العقوبات مواد صريحة لتغطية الجرائم السيبرانية الموضوعية تتمثل أساساً في المواد 394 مكرر وما يليها.

أولاً : : المادة 394 مكرر - الدخول غير المشروع والبقاء فيه

تنص المادة 394 مكرر من قانون العقوبات الجزائري على ما يلي: كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة المعالجة الآلي للمعطيات أو يحاول ذلك

يعاقب بالحبس من ثلاثة أشهر إلى سنة و بغرامة من 50000 إلى 100.000 دج أو بإحدى هاتين العقوبتين. وإذا ترتب على ذلك حذف أو تغيير للمعطيات المتضمنة في المنظومة أو تدهور في عمل هذه المنظومة، فتكون العقوبة الحبس من ستة أشهر إلى ثلاث سنوات وبغرامة من 100.000 إلى 300.000 دج.

وتحليلاً لهذه المادة يتضح أن المشرع اشترط توافر ركنين أساسيين: الركن المادي المتمثل في فعل الدخول أو البقاء في نظام المعالجة الآلية للمعطيات، والركن المعنوي المتمثل في العش أي عدم مشروعية الدخول ، كما ميّز المشرع بين الصورة البسيطة والمشددة وفق ما إذا كان الدخول صاحبه إتلاف أو تعديل للبيانات

ثانيا :المادة 394 مكرر - 1 جرائم التخريب المعلوماتي

تناولت المادة 394 مكرر 1 جرائم إدخال بيانات كاذبة أو تخريب الأنظمة المعلوماتي وتتص على تجريم كل من يُدخل بيانات في نظام معالجة آلية للمعطيات مع علمه بأنها مزيفة أو مضللة، وكذلك كل من يمحو أو يُعدّل بيانات مخزنة في نظام معلوماتي بصورة غير مشروعة وتصل العقوبة في حالة استهداف أنظمة الدولة أو المؤسسات الحيوية إلى عشر سنوات سجنًا

ثالثا المادة 394 مكرر - 2 حيازة وتوزيع أدوات الاختراق

جرّمت المادة 394 مكرر 2 من قانون العقوبات حيازة البرامج والأدوات الخاصة المصممة للاختراق غير المشروع لأنظمة المعالجة الآلية للمعطيات أو تعديلها أو إتلافها أو الحصول غير المشروع على المعطيات، وكذلك توزيع هذه الأدوات أو إتاحتها للغير. وتبرز أهمية هذه المادة في مواجهة تجار أدوات الاختراق الذين يوفرون للمجرمين الإلكترونيين البرامج الخبيثة اللازمة لارتكاب جرائمهم.

رابعا :أحكام خاصة بالجرائم المشددة

أولى المشرع الجزائري اهتماماً خاصاً بالجرائم السيبرانية الموجهة نحو البنى التحتية الحيوية للدولة ومنظومات الدفاع الوطني، إذ شدّد العقوبات المقررة في هذه الحالات تشديداً

ملحوظاً. كما نصّ على ظرف التشديد في حالة الجرائم المرتكبة من قبل موظفي الدولة بحكم وظائفهم، أو الجرائم التي تتضمن عنصر التنظيم والمؤامرة المسبقة..

المطلب الثالث: الحماية في قانون الوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال

أولاً: الحماية الجنائية لحق الخصوصية في البيئة الرقمية:

يمنع القانون التعاطي مع المعلومات التي قد تؤدي إلى انتهاك السرية والخصوصية، كما يمنع استخدام البيانات الشخصية بطريقة غير شرعية، أو إفشاء غير المشروع للمعلومات والبيانات الشخصية.⁵⁰ وقد عالج المشرع الجزائري هذه الحماية من خلال المواد 394 مكرر إلى 394 مكرر 7 من قانون 15/04 منها ما تعلق بسلامة الأنظمة المعلوماتية، ومنها ما تعلق بإتاحة الأنظمة والبيانات، ومنها ما تعلق بسرية البيانات الشخصية. ومن بين الأفعال التي تعد جرائم تقنية يعاقب عليها قانون العقوبات، تجريم الدخول غير المصرح به إلى النظام المعلوماتي حيث يعد ذلك جريمة ماسة بخصوصية الأفراد، ونصت المادة 394 مكرر على أنه: "يعاقب بالحبس من ثلاثة أشهر إلى سنة وبغرامة من 50.000 دج إلى 100.000 دج كل من يدخل أو يبقى عن طريق الغش في كل أو في جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك".

وفي المادة 394 مكرر 1 جرم إدخال معطيات إلى النظام المعلوماتي أو إزالتها أو تعديلها: "يعاقب بالحبس من ستة أشهر إلى ثلاثة سنوات وبغرامة من 500.000 دج إلى 2.000.000 دج كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها". ما يفهم من النص أن فعل سواء كان عن طريق الإدخال أو التعديل أو الإزالة يتم بطريقة غير مشروعة في النظام الرقمي يعد جريمة لغض النظر عن نتائج هذه الأفعال وأثارها.

أما المادة 394 مكرر 2 فعاقب المشرع الجزائري على جريمة حيازة أو إفشاء أو نشر أو استعمال البيانات الشخصية بالحبس من شهرين إلى ثلاثة سنوات وبغرامة مالية من 1.000.000 دج إلى 5.000.000 دج كل من يقوم بالعمد أو الغش بأحد هذه الأفعال.

⁵⁰ دلخار صالح بوتاني، الحماية الجنائية الموضوعية للمعلوماتية، دار الفكر الجامعي، الإسكندرية، 2015، ص 200.

فيما يخص خصوصية وسرية الرسائل فقد نصت المادة 303 من قانون العقوبات الجزائري على أنه: "كل من يفض أو يتلف رسائل أو مراسلات موجهة إلى الغير، وذلك بسوء نية وفي غير الحالات المنصوص عليها في المادة 137، يعاقب بالحبس من شهر إلى سنة وبغرامة من 25.000 دج إلى 100.000 دج أو بإحدى هاتين العقوبتين فقط". ومن خلال هذا النص يتضح أن المشرع أدرج المراسلات الالكترونية كذلك ضمن مصطلح الرسائل والمراسلات، وبذلك تستفيد هي الأخرى من ذات الحماية المقررة. كما ننوه أن قانون البريد والمواصلات هو الآخر عرف الاتصالات في مادته 08 بأنها: "كل تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة عن طريق الأسلاك أو البصريات أو اللاسلكي الكهربائي أو أجهزة أخرى كهربائية مغناطيسية".⁵¹ ما يفهم أن المراسلات و الاتصالات الالكترونية هي الأخرى مشمولة بالحماية المقررة في المادتين 137 و 303 من قانون العقوبات.

وفي سياق متصل دائما بحماية الخصوصية الرقمية فقد نص القانون رقم 24-06 على أفعال تعد من قبيل الجرائم المعاقب عليها⁵² كتجريم التقاط وتسجيل ونقل البيانات الشخصية فبحسب المادة 303 مكرر دائما يعد مساسا بالحرية الشخصية كل التقاط أو تسجيل أو نقل للمكالمات أو الأحاديث الخاصة، أو السرية بغير إذن صاحبها أو بدون رضاه، أو كل التقاط أو تسجيل أو نقل صورة شخص في مكان خاص بغير إذن صاحبها أو رضاه.

المادة 303 مكرر 1 استهدفت كذلك تجريم الأفعال الخاصة بالاحتفاظ أو إفشاء أو استخدام البيانات على الوجه المبين سابقا.

إذا فالمشرع الجزائري وتماشيا مع التطورات التقنية التي مست جوانب الأفراد المتعددة، نظم في نصوصه العديد من الأفعال التي تعد من قبيل الجرائم الماسة بالحق في الحياة الخاصة ضمن البيئة الرقمية. ونص في قانون العقوبات المعدل والمتمم وكل القوانين ذات الصلة على العقوبات المقررة لذلك. فحين تناول قانون الإجراءات الجزائية جملة من الضمانات والإجراءات الواجب إتباعها لحماية هذا الحق.

⁵¹ القانون رقم 03/2000 المؤرخ في 05/08/2000 المتضمن القواعد العامة المتعلقة بالبريد وبالمواصلات السلكية واللاسلكية.

⁵² القانون رقم 06/24 المؤرخ في: 28/04/2024 المعدل والمتمم لقانون العقوبات الجزائري.

ثانيا: حماية الحق في الخصوصية الرقمية ضمن نصوص قانون الإجراءات الجزائية

تضمن القانون رقم 04/09 المؤرخ في 05/08/2009 المتضمن بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها جملة من الإجراءات القانونية لحماية الحق في الخصوصية الرقمية، وأورد استثناءات بخصوصها. فقد جاء في نص المادة 03 منه على أنه ولمقتضيات النظام العام، أو لمستلزمات التحريات أو التحقيقات القضائية يمكن للسلطات القضائية وضباط الشرطة القضائية بمراقبة الاتصالات الالكترونية وتفتيش المنظومة المعلوماتية. ونصت المادة 04 منه على أنه: "يمكن القيام بعمليات المراقبة المنصوص عليها في المادة 03 أعلاه في الحالات التالية:

- أ- للوقاية من الأفعال الموصوفة بالجرائم الإرهابية أو التخريبية أو الماسة بأمن الدولة.
 - ب- في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني.
 - ت- لمقتضيات التحريات والتحقيقات القضائية عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الالكترونية.....".
- ما يفهم من النصوص السابقة أن الحق في الخصوصية الرقمية مكفول للأفراد والأشخاص بموجب القوانين والتشريعات ، غير أن هذا الحق ليس مطلق لأصحابه متى تعلق الأمر بمصالح ومقتضيات الأمن العام ومجريات التحريات القضائية والمتابعة في بعض الجرائم الخطيرة.

وحتى يضمن المشرع الوطني عدم الاعتداء على هذا الحق بحجة توافر حالة من الحالات المنصوص عليها في المادة 04 ، فإنه اشترط:

- الحصول على إذن مكتوب من قبل السلطة القضائية المختصة.
- في الأفعال الموصوفة بالإرهاب والتخريب أو الجرائم الماسة بأمن الدولة ، يتولى النائب العام لدى مجلس قضاء الجزائر الاختصاص بمنح إذن المراقبة على الرسائل والمكالمات الالكترونية لضباط الشرطة القضائية لمدة 06 أشهر قابلة للتجديد وذلك على أساس تقرير يبين الترتيبات التقنية المستعملة والأغراض الموجهة لها.

- إمكانية تفتيش المنظومة المعلوماتية أو جزء منها أو منظومة تخزين المعلومات من قبل الجهات القضائية المختصة أو ضباط الشرطة القضائية، في حالة ما إذا تبين أن هذه المعطيات المبحوث عنها مخزنة في نظام معلوماتي يقع خارج الإقليم الوطني وذلك عن طريق اتفاقية التعاون الدولي المشترك في مجال مكافحة الجريمة السيبرانية أو ذات الصلة بالموضوع.
- إلزام مقدمي خدمات الانترنت وتحت طائلة العقوبات المقررة لإفشاء أسرار التحري والتحقيق بكتمان سرية العمليات التي ينجزونها بطلب من المحققين، وكذا المعلومات المتصلة بها.
- تحديد مدة الاحتفاظ بالبيانات المحجوزة بمدة سنة واحدة من تاريخ التسجيل

المبحث الثاني: الحماية الإجرائية للنظام المعلوماتي

المطلب الأول: إجراءات التحقيق في الجريمة السيبرانية

الفرع الأول : الأحكام الإجرائية في القانون 09-04

يتضمن القانون 09-04 جملة من الأحكام الإجرائية الخاصة التي تُعدّ الأبرز في هذا التشريع، إذ تُرسي قواعد خاصة تتلاءم مع الطبيعة التقنية للجريمة السيبرانية:

أولاً: المراقبة الإلكترونية للاتصالات (المواد 4-6)

أجاز القانون 09-04 في مواده 4 إلى 6 اللجوء إلى المراقبة الإلكترونية للاتصالات كوسيلة للتحقيق في الجرائم السيبرانية ، بشرط الحصول على إذن قضائي مسبق من قضاة التحقيق، ويُشترط في هذا الإذن تحديد نطاق المراقبة وموضوعها وأسبابها وأجلها وتُعدّ هذه الأحكام ضماناً قانونية جوهرية لتوازن متطلبات التحقيق الجنائي مع صون الحقوق والحريات الفردية .

ثانياً: الاستخراج الآلي للمعطيات والتفتيش الرقمي (المواد 14-16)

تتطلب معالجة الجرائم السيبرانية في الجزائر مقاربة تشريعية تعزز الإطار القانوني لجمع الأدلة الرقمية وحمايتها، ينبغي على المشرع الجزائري التوسع في تعريف الدليل الرقمي".

خصّص المشرع الجزائري في المواد 14 إلى 16 من القانون 04-09 قواعد خاصة بعمليات التفتيش الرقمي وضبط المعطيات الإلكترونية، تميّزت بعدة خصائص:

- إمكانية التفتيش عن بُعد في الأنظمة المرتبطة بنظام الهدف المُفتش
- القدرة على مصادرة أجهزة الحاسوب والدعامات الإلكترونية
- إمكانية حجز السجلات والبيانات الرقمية .

ثالثاً: الالتزام بتخزين البيانات من قِبَل مزوّد الخدمة (المادة 12)

أوجبت المادة 12 على مزوّد خدمات الاتصالات الإلكترونية الاحتفاظ ببيانات الاتصال لمدة لا تقل عن سنة واحدة ، وذلك لتمكين السلطات من الرجوع إليها عند الحاجة⁵³ في إطار التحقيقات الجنائية . وهذا الالتزام الذي يُوازي ما هو معمول به في التشريع الأوروبي والفرنسي .

الفرع الثاني : إجراءات التعامل مع الدليل الرقمي

يتطلب جمع الدليل الرقمي في الجرائم السيبرانية اتباع منهجية دقيقة تضمن سلامة الدليل وعدم المساس به، مع ضرورة التمييز بين المصادر الرقمية المتصلة وغير المتصلة بالشبكة. ينبغي على الجهات القضائية المختصة، عند ورود بلاغ أو شكوى، إصدار إنابة قضائية واضحة تحدد طبيعة الدليل المطلوب ومكان تواجده، مع تأكيد ضرورة احترام مبدأ "التسلسل الرقابي (Chain of Custody)" إن أي خلل في هذه المرحلة قد يؤدي إلى عدم قبول الدليل أمام القضاء، مما يعيق مسار العدالة.

لحفظ الدليل الرقمي، يجب على الخبراء التقنيين استخدام أدوات وتقنيات متخصصة لإنشاء نسخ طبق الأصل (Images) من وسائط التخزين الأصلية، مع التأكد من استخدام خوارزميات التجزئة (Hashing Algorithms) مثل MD5 أو SHA-256 للتحقق من سلامة النسخة ومطابقتها للأصل. يضمن هذا الإجراء منع أي تعديل غير مصرح به على

53 قانون رقم 03-2000 المتعلق بتحديد القواعد العامة المتعلقة بالبريد والمواصلات السلكية واللاسلكية.

الدليل، مما يحافظ على قيمته الإثباتية. يشدد القانون 04-09 على ضرورة التقيد بالإجراءات التقنية عند ضبط الأدلة الرقمية .

يعتبر تحليل الدليل الرقمي مرحلة حاسمة تتطلب خبرة فنية عميقة. ينبغي للخبراء المكلفين بالتحليل استخدام برمجيات متخصصة لاستعادة البيانات المحذوفة، وفحص السجلات (Logs)، وتتبع النشاطات المشبوهة.

الفرع الثالث : الأمن السيبراني

إن فرض هياكل أمن معلوماتي على المؤسسات العمومية في الجزائر، بموجب التشريعات الحالية مثل القانون 04-09 والقوانين المعدلة له، يمثل ركيزة أساسية في استراتيجية الوقاية من الجرائم السيبرانية. هذه الهياكل، التي تتضمن غالباً وحدات متخصصة ومسؤولين عن أمن المعلومات، تهدف إلى تعزيز القدرة على رصد التهديدات، وتحليل الثغرات الأمنية، وتطبيق إجراءات الحماية اللازمة. إن وجود إطار تنظيمي واضح يلزم المؤسسات بإنشاء هذه الهياكل يضمن تبني نهج استباقي بدلاً من مجرد الاستجابة للحوادث بعد وقوعها.

تتجلى الآثار الوقائية لهذه الهياكل في تطوير سياسات أمنية شاملة تتناسب مع طبيعة بيانات وعمليات كل مؤسسة. فهي تساهم في تحديد المخاطر المحتملة، وتقييم مدى تأثيرها، ووضع خطط للطوارئ والتصدي للحوادث. كما أن إلزام المؤسسات بتدريب موظفيها على أفضل الممارسات الأمنية، وتوعيتهم بمخاطر الهجمات السيبرانية، يشكل حاجزاً بشرياً هاماً ضد الاختراقات التي غالباً ما تستغل نقاط الضعف لدى الأفراد.

من ناحية أخرى، يتطلب تفعيل هذه الهياكل توفير الموارد التقنية والبشرية الكافية. قد تواجه بعض المؤسسات العمومية، خاصة ذات الميزانيات المحدودة، صعوبات في بناء قدرات أمنية متقدمة. هذا الأمر يبرز الحاجة إلى دعم حكومي موجه، ربما من خلال هيئات وطنية متخصصة في الأمن السيبراني، لتقديم الخبرة والمساعدة الفنية للمؤسسات الأقل جاهزية، مما يضمن تكافؤ الفرص في مجال الحماية.

إن التعاون بين المؤسسات العمومية نفسها، وتبادل المعلومات حول التهديدات والخبرات الأمنية، يعد عنصراً حيوياً لتعزيز الوقاية على المستوى الوطني. فالجرائم السيبرانية

غالباً ما تتجاوز حدود مؤسسة واحدة، وتتطلب استجابة جماعية ومنسقة. يمكن لهذه الهياكل أن تكون بمثابة نقاط اتصال فعالة لإنشاء شبكات تبادل معلومات آمنة، مما يتيح اكتشاف الأنماط المشتركة للهجمات والتصدي لها بشكل أكثر فعالية.

ختاماً، فإن إلزام المؤسسات العمومية بهياكل أمن معلوماتي فعالة هو خطوة ضرورية في مسار بناء بيئة سيبرانية آمنة. ومع ذلك، فإن نجاح هذه الاستراتيجية يعتمد على مدى التزام المؤسسات بتطبيقها، وتوفير الدعم اللازم لها، وتعزيز ثقافة الأمن السيبراني على جميع المستويات، بالإضافة إلى تطوير آليات للتقييم المستمر لفعالية هذه الهياكل ومدى مواكبتها للتطورات المتسارعة في عالم التهديدات السيبرانية.

أولاً : الردع الوقائي

تتجلى فعالية الوقاية من الجرائم السيبرانية مقارنة بالردع اللاحق في طبيعة هذه الجرائم المتسمة بالسرعة والانتشار. فالردع بتركيزه على العقاب بعد وقوع الجريمة، غالباً ما يكون متأخراً عن تطور أساليب المجرمين السيبرانيين الذين يبتكرون باستمرار ثغرات جديدة. أما الوقاية، من خلال تعزيز الوعي الأمني، وتطوير البنى التحتية التقنية، ووضع ضوابط صارمة للوصول إلى البيانات، فإنها تستهدف منع وقوع الجريمة من الأساس، مما يقلل من احتمالية حدوث الأضرار ويحد من انتشارها.

تفرض الطبيعة اللامركزية والمتطورة للجريمة السيبرانية تحديات كبيرة أمام فعالية الردع التقليدي. فغالباً ما يكون مصدر الجرائم خارج النطاق الجغرافي للجزائر، مما يعقد إجراءات الملاحقة القضائية والضبط القضائي في المقابل، تركز آليات الوقاية على بناء قدرات وطنية للتعامل مع التهديدات السيبرانية، مثل إنشاء مراكز الاستجابة لطوارئ الحاسوب، وتطوير بروتوكولات الأمن السيبراني، وتعزيز التعاون الدولي في مجال تبادل المعلومات الاستخباراتية

إن الاستثمار في الوقاية يعكس رؤية استباقية تتجاوز مجرد معاقبة المخالفين، لتشمل بناء ثقافة أمنية راسخة لدى الأفراد والمؤسسات. علاوة على ذلك، فإن الجرائم السيبرانية غالباً ما تحدث بشكل سريع ومتسلسل، حيث يمكن لمجموعة واحدة من الهجمات أن تؤثر على عدد كبير من الضحايا في وقت قصير. في هذه الحالة، يصبح الردع اللاحق أقل فعالية في الحد

من الأضرار، حيث تكون الخسائر قد وقعت بالفعل. بينما تهدف استراتيجيات الوقاية، مثل التطوير المستمر لأنظمة الحماية والبرمجيات الأمنية، إلى منع هذه الهجمات من النجاح في المقام الأول، مما يحافظ على سلامة البيانات والأنظمة.

تتجسد فعالية الوقاية أيضاً في قدرتها على معالجة الأسباب الجذرية للجريمة السيبرانية، بدلاً من الاكتفاء بمعالجة أعراضها. فمن خلال تعزيز الإطار القانوني والمؤسساتي، وتطوير آليات التعاون بين القطاعات المختلفة، يمكن معالجة الثغرات التقنية والإدارية التي يستغلها المجرمون. إن التنسيق بين الجهات المعنية 261-المتعلق بإنشاء لجنة وطنية للأمن السيبراني، يعزز من القدرة على رصد التهديدات والاستجابة لها بشكل استباقي.

ثانياً: وكالة أمن الأنظمة المعلوماتية

تُعدّ وكالة أمن الأنظمة المعلوماتية (ANSI) من الركائز الأساسية في منظومة الأمن السيبراني الوطنية بالجزائر⁵⁴، حيث تلعب دوراً محورياً في تنفيذ الإستراتيجية الوطنية الهادفة إلى حماية الفضاء المعلوماتي. ينبع دورها من تكليفها بوضع وتنفيذ سياسات وإجراءات موحدة لضمان أمن المعلومات والأنظمة الحيوية، بما يتماشى مع التحديات المتزايدة للتهديدات السيبرانية. يركز عملها على التنسيق مع مختلف الجهات الحكومية وغير الحكومية المعنية، بهدف بناء قدرات وطنية فعالة في هذا المجال.

تساهم الوكالة في تعزيز الإطار القانوني والتنظيمي للأمن السيبراني من خلال اقتراح تعديلات على التشريعات القائمة، وذلك بهدف مواكبة التطورات التكنولوجية والتشريعات الدولية. كما تعمل على تطوير المعايير الفنية والإرشادات اللازمة لتأمين البنى التحتية الرقمية، وتعزيز الوعي بأهمية الأمن السيبراني لدى مختلف شرائح المجتمع.

ضمن السياسة الوطنية للأمن السيبراني، تتولى وكالة أمن الأنظمة المعلوماتية مسؤولية الاستجابة للحوادث السيبرانية الكبرى، من خلال إنشاء وتطوير فرق الاستجابة للطوارئ المعلوماتية (CERTs). تعمل هذه الفرق على تحليل التهديدات، وتقديم الدعم الفني،

⁵⁴ المرسوم الرئاسي رقم 26-07 المؤرخ في 7 جانفي 2026، المتضمن إنشاء هيكل مسؤول عن أمن الأنظمة المعلوماتية وحماية المعطيات في المؤسسات والإدارات والهيئات العمومية وتحديد مهامه وتنظيمه وسيره، الجريدة الرسمية، العدد 04 لسنة 2026. متاح على الرابط:

<https://www.joradp.dz/FTP/jo-arabe/2026/A2026004.pdf>

وتنسيق الجهود بين مختلف الجهات المتضررة والمتدخلة، وذلك لتقليل الأضرار الناجمة عن الهجمات السيبرانية وضمان استمرارية الخدمات الحيوية.

تتطلب فعالية وكالة أمن الأنظمة المعلوماتية تكاملاً مؤسسانياً قوياً مع الجهات الأخرى المعنية، مثل وزارة البريد والمواصلات السلكية واللاسلكية، ووزارة الدفاع الوطني، والمديرية العامة للأمن الوطني. يعزز هذا التعاون، بتنظيم وعمل الوكالة، و الرفع من قدرتها على تبادل المعلومات، وتنسيق العمليات، وتطوير استراتيجيات مشتركة لمواجهة التحديات السيبرانية المتشعبة، بما يدعم تحقيق أهداف الأمن السيبراني الوطني.

رغم التطورات المسجلة، تظل الحاجة قائمة لتعزيز موارد وكالة أمن الأنظمة المعلوماتية، وتطوير آلياتها التشغيلية، وتوسيع نطاق صلاحياتها لتشمل مجالات أوسع مثل حماية البيانات الشخصية في ظل القوانين المنظمة مثل المرسوم 07-26، والاستثمار في البحث والتطوير لابتكار حلول تقنية متقدمة. إن تعزيز القدرات البشرية والتقنية للوكالة يعدّ أمراً ضرورياً لتمكينها من الاضطلاع بكامل مسؤولياتها في حماية الفضاء السيبراني الوطني.

المطلب الثاني: صعوبة مكافحة الجريمة السيبرانية

الفرع الأول : خصوصية الدليل الرقمي

تكتسب خصوصية الدليل الرقمي تعقيداً متزايداً نظراً لهشاشته البنيوية وقابليته العالية للتعديل، مما يضع تحديات جمة أمام جهات إنفاذ القانون في ضمان سلامة الإجراءات. فالدليل الرقمي، بطبيعته، ليس ثابتاً بل هو عبارة عن بيانات قابلة للمحو أو التغيير السهل، سواء كان ذلك بقصد التدمير أو التلاعب بالأدلة. هذه الهشاشة تفرض ضرورة تبني مقاربات تقنية وقانونية دقيقة لضمان حجية هذا الدليل أمام القضاء.

تتجسد قابلية الدليل الرقمي للتعديل في سهولة إجراء تغييرات على البيانات المخزنة، سواء عن طريق الحذف، الإضافة، أو التعديل المباشر، مما يفتح الباب أمام احتمالية تزيف الأدلة أو إتلافها. هذا الأمر يستدعي تطبيق آليات تقنية صارمة، مثل التشفير، التجزئة

(hashing)، والتوثيق الإلكتروني، للحفاظ على سلامة الدليل الرقمي من أي تدخل غير مشروع، وضمان عدم تغييره بعد جمعه.

إن أهمية السلامة التقنية في التعامل مع الدليل الرقمي لا تقتصر على مرحلة الجمع فحسب، بل تمتد لتشمل مراحل الحفظ، النقل، والتحليل. فأي خلل في هذه المراحل قد يؤدي إلى فقدان الدليل أو تشويبه، وبالتالي فقدان قيمته الإجرائية⁵⁵. يتطلب ذلك تدريب الكوادر المتخصصة وتزويدها بالأدوات التقنية اللازمة، مع ضرورة ملائمة النصوص القانونية لتعكس هذه المتطلبات⁵⁶.

في سياق مكافحة الإجرائية للجرائم السيبرانية في الجزائر، يشكل الدليل الرقمي عنصراً محورياً، لكن التعامل معه يتطلب فهماً عميقاً لخصائصه. إن قوانين مثل القانون 04-09 وقانون العقوبات 06-24، وقانون الإجراءات الجزائية 14-25، تضع إطاراً قانونياً لجمع الأدلة الرقمية، إلا أن التطبيق العملي يواجه تحديات تتعلق بضمان سلامتها.

لتحقيق العدالة في قضايا الجرائم السيبرانية، يصبح ضمان سلامة الدليل الرقمي أمراً حتمياً. فدون ذلك، تصبح الإجراءات القضائية عرضة للطعن، وقد تفشل جهود المتابعة والإدانة. لذلك، يجب على المشرع الجزائري، وكذا الأجهزة القضائية، أن يعطيا الأولوية لتطوير آليات تقنية وقانونية متكاملة تضمن حجية الدليل الرقمي وقيمه الثبوتية، بما يتوافق مع التطورات التكنولوجية الحديثة⁵⁷.

⁵⁵ المرسوم الرئاسي رقم 07-26 المؤرخ في 7 جانفي 2026، المتضمن إنشاء هيكل مسؤول عن أمن الأنظمة المعلوماتية وحماية المعطيات في المؤسسات والإدارات والهيئات العمومية وتحديد مهامه وتنظيمه وسيره، الجريدة الرسمية، العدد 04 لسنة 2026. متاح على الرابط:

<https://www.joradp.dz/FTP/jo-arabe/2026/A2026004.pdf>

⁵⁶ سلطة ضبط البريد والاتصالات الإلكترونية، صفحة نشر المرسوم الرئاسي رقم 07-26 المؤرخ في 7 جانفي 2026، وتلخص هدفه في إنشاء هيكل مسؤول عن أمن الأنظمة المعلوماتية وحماية المعطيات. متاح على الرابط: <https://www.arpce.dz/ar/pub/w6h8s2>

⁵⁷ سي مريبط شهرزاد، التصدي للجرائم الإلكترونية المنتهكة لخصوصية الأفراد في ظل قانون العقوبات رقم 06-24، ASJP، 2025. متاح على الرابط: <https://asjp.cerist.dz/en/article/282482>

الفرع الثاني : الطابع الدولي للجريمة السيبرانية

إن الطابع الدولي للجريمة السيبرانية هو سمة جوهرية تتجاوز الحدود الجغرافية للدول، حيث يمكن للمجرمين الوصول إلى الأنظمة المعلوماتية والبيانات من أي مكان في العالم، مما يتيح لهم ارتكاب جرائم ذات امتدادات عابرة للحدود. هذا الانتشار الأفقي يجعل تحديد مكان وقوع الجريمة أو مكان اكتشافها أمراً معقداً، وبالتالي يطرح تحديات مباشرة على قواعد الاختصاص القضائي التقليدية التي تستند إلى مبادئ إقليمية صارمة.

يؤدي الطابع العابر للحدود للجرائم السيبرانية إلى تعقيد مسألة الاختصاص القضائي، حيث قد تتوفر أسباب الاختصاص في عدة دول متزامنة⁵⁸. فالدولة التي تم فيها استهداف الأنظمة أو البيانات، والدولة التي صدر منها الفعل الإجرامي، والدولة التي تم فيها اكتشاف الأثر الإجرامي، قد ترى كل منها نفسها مختصة بالنظر في القضية. هذا التنازع في الاختصاص يتطلب آليات لتحديده بشكل حاسم، إما عبر الاتفاقيات الدولية أو عبر مبادئ تنازع الاختصاص المستقرة في القانون الدولي الخاص.

تتجلى الآثار المترتبة على الطابع الدولي للجرائم السيبرانية بوضوح في مجال المساعدة القضائية الدولية. فالتحقيق في هذه الجرائم يستلزم غالباً الحصول على أدلة رقمية مخزنة في خوادم أو أنظمة تقع خارج نطاق الولاية القضائية للدولة التي تجري التحقيق. هذا يستدعي تفعيل آليات التعاون الدولي، مثل اتفاقيات المساعدة القانونية المتبادلة، لطلب استخراج البيانات أو تجميدها أو حتى ضبطها، وهو ما قد يكون بطيئاً ومعقداً في ظل اختلاف التشريعات والإجراءات بين الدول .

الفرع الثالث : الذكاء الاصطناعي والجريمة السيبرانية

إن التطور المتسارع للذكاء الاصطناعي يفتح آفاقاً جديدة للجريمة السيبرانية، ويشكل تحدياً كبيراً لأنظمة المكافحة الحالية. من أبرز هذه التحديات ظاهرة "التزييف العميق "

⁵⁸ عبد الكريم قاسم، التعاون الدولي في مكافحة جرائم الإنترنت، مجلة الاجتهاد القضائي، جامعة محمد خيضر بسكرة، العدد 22، 2022.

(Deepfake)، التي تسمح بإنشاء محتوى مرئي وصوتي مزيف بمستوى عالٍ من الواقعية، مما يسهل نشر المعلومات المضللة، والابتزاز، وتشويه السمعة، بل وحتى التأثير على الاستقرار السياسي والاجتماعي. إن القدرة على توليد خطابات سياسية أو تصريحات رسمية مفبركة قد تتجاوز قدرة الأنظمة القانونية الحالية على اكتشافها وتفنيدها بسرعة .

يمثل الاحتيال الآلي، المدعوم بتقنيات الذكاء الاصطناعي، تهديداً مستقبلياً متزايداً. تعتمد هذه التقنية على استخدام خوارزميات التعلم الآلي لتحليل سلوك المستخدمين، وتصميم هجمات تصيد احتيالي⁵⁹ (Phishing) أكثر استهدافاً وإقناعاً، أو حتى أتمتة عمليات اختراق الأنظمة. إن القدرة على محاكاة سلوك بشري دقيق في تفاعلات آلية تجعل من الصعب على الأفراد والأنظمة الأمنية التمييز بين التفاعل الشرعي والهجوم الآلي، مما يزيد من احتمالية نجاح هذه العمليات الاحتيالية .

في السياق الجزائري، ورغم وجود إطار قانوني لمكافحة الجرائم السيبرانية ، إلا أن التحديات الجديدة التي يفرضها الذكاء الاصطناعي تستدعي مراجعة مستمرة وتحديثاً للتجريم والعقاب. إن طبيعة التزييف العميق والاحتيال الآلي تتطلب آليات ضبط وتقنين تتماشى مع التقنيات المستخدمة، مع التركيز على أدلة الإثبات الرقمي والمسؤولية القانونية في بيئة رقمية سريعة التغير.

إن تعقيد هذه الظواهر يستدعي مقاربة وقائية استباقية، تتجاوز مجرد التجريم اللاحق. يتطلب ذلك تعزيز الوعي المجتمعي بمخاطر هذه التقنيات، وتطوير أدوات تقنية للكشف عن المحتوى المزيف والممارسات الاحتيالية الآلية. كما أن التعاون الدولي وتبادل الخبرات في هذا المجال يصبح أمراً حتمياً لمواجهة هذه الجرائم التي لا تعرف حدوداً جغرافية، مع ضرورة تكييف التشريعات الوطنية لتتوافق مع المعايير الدولية المتطورة.

⁵⁹التصيد الاحتيالي و هة محاولة للحصول على معلومات حساسة و تفاصيل مثل أسماء المستخدمين و كلمات المرور ، هذه الكلمة مستحدثة من القاموس الإنجليزي و تعني صيد الأسماك ، المصدر من موقع ويكيبيديا

في نهاية المطاف، فإن مواجهة مخاطر التزييف العميق والاحتياز الآلي تتطلب تكاملاً بين الجهد التشريعي، والتقني، والتعليمي، والأمني. إن غياب نصوص قانونية صريحة تعالج هذه المستجدات قد يخلق ثغرات يستغلها المجرمون. لذا، فإن تقييم فعالية الإجراءات الحالية ووضع استراتيجيات مستقبلية قائمة على البحث العلمي والرصد المستمر للتطورات التقنية يصبح ضرورياً لضمان أمن الفضاء السيبراني.

الفرع الرابع : حدود الإطار الموضوعي

تنتم النصوص القانونية الموضوعية المتعلقة بالجرائم السيبرانية في الجزائر، كغيرها من التشريعات، بجمود نسبي يعيق مواكبتها للتطور التقني المتسارع. فالصياغات التقليدية لبعض الأفعال المجرمة لا تتماشى مع طبيعة الجرائم السيبرانية التي تنتم بالمرونة والقدرة على التكيف، مما يفتح ثغرات تشريعية قد يستغلها مرتكبو هذه الجرائم. هذا التباين بين واقع الجريمة الرقمية وقدرة النصوص القانونية على تأطيرها يشكل تحدياً جوهرياً في تحقيق الردع الفعال.

تتمثل أحد أبرز التحديات في مفهوم "الهوية" في الفضاء السيبراني. فالقوانين الموضوعية تعتمد غالباً على تحديد هوية الفاعل بشكل واضح، إلا أن التقنيات الحديثة تسمح بإنشاء هويات وهمية أو متخفية، مما يصعب على الضبطية القضائية تتبع الجناة وتحديد المسؤول.

المطلب الثالث: جهود الجزائر لمكافحة الجرائم السيبرانية

الفرع الأول: التشريعات المكملة للمنظومة الجزائرية

1- قانون التجارة الإلكترونية الجزائري

أصدرت الجزائر قانون التجارة الإلكترونية رقم 05-18 لعام 2018 الذي يتضمن أحكاماً تتعلق بالمعاملات الإلكترونية وصحة العقود المبرمة إلكترونياً وحماية المستهلك في

البيئة الرقمية، مما يُكْمَل المنظومة التشريعية في الجانب المتعلق بالجرائم التجارية الإلكترونية.⁶⁰

2- قانون حماية المعطيات الشخصية

صادقت الجزائر على قانون خاص بحماية المعطيات الشخصية رقم 07-18 لعام 2018، الذي يُرسي حقوقاً للأفراد تجاه استخدام بياناتهم الشخصية ويُنشئ هيئة وطنية لحماية المعطيات الشخصية، مما يوفر حماية إضافية في مواجهة الجرائم الإلكترونية الماسة بالخصوصية .

3- قانون البريد والمواصلات الإلكترونية

يتضمن قانون البريد والمواصلات الإلكترونية رقم 03-2000 الأطر القانونية للتسجيل والترخيص لمزوّدي خدمات الإنترنت والاتصالات، ويلزمهم بجملة من الالتزامات الأمنية التي تُسهم في مكافحة الجرائم السيبرانية .

4- قانون مكافحة الإرهاب

أدرج المشرع الجزائري ضمن منظومة قانون مكافحة الإرهاب نصوصاً تُجرّم التوظيف الإلكتروني للترويج للإرهاب وتمويله وتجنيد عناصره عبر الفضاء الإلكتروني
الفرع الثاني: المقارنة بين التشريع الجزائري والتشريعات الدولية
يستدعي تقييم مدى كفاءة المنظومة التشريعية الجزائرية إجراء مقارنة منهجية مع نظيراتها الإقليمية والدولية

1- مقارنة مع التشريع الفرنسي

تأثر التشريع الجزائري بوضوح بنظيره الفرنسي، لا سيما في مفهوم المعالجة الآلية للمعطيات (الذي استُعيّر من قانون جورهو الفرنسي لعام 1988. غير أن التشريع الفرنسي تطور بصورة أوسع لاستيعاب متطلبات التوجيه الأوروبي للأمن السيبراني (NIS2) والتنظيم

⁶⁰ القانون رقم 18-05 المتعلق بالتجارة الإلكترونية، الجريدة الرسمية للجمهورية الجزائرية، 2018.

العام لحماية البيانات (GDPR) ، بينما لا تزال الجزائر تعمل في إطار القانون 04-09 دون تحديثات جوهرية.

2- مقارنة مع التشريع المصري

أصدرت مصر قانون مكافحة جرائم المعلوماتية رقم 175 لعام 2018 الذي يتميز بتفصيل أكثر للجرائم الإلكترونية وعقوباتها، كما أنشأ المجلس الأعلى لتنظيم الاتصالات بصلاحيات أوسع في حجب المواقع الضارة. ويتميز التشريع الجزائري بأنه أكثر توازناً في مسألة الضمانات القضائية للمراقبة الإلكترونية مقارنةً بالنموذج المصري.

3- مقارنة مع نظام مكافحة الجرائم المعلوماتية السعودي

يتميز نظام مكافحة جرائم المعلوماتية السعودي الصادر عام 2007 بأنه نظام مستقل وشامل يتضمن تعريفات أكثر تفصيلاً وعقوبات أشد صرامة، إلا أنه يفتقر إلى الضمانات القضائية المتعلقة بالمراقبة الإلكترونية التي كفلها المشرع الجزائري. وفي المقابل، تتقدم المملكة العربية السعودية على الجزائر في مجال التنظيم والهيكل المؤسسي المتخصص في الأمن السيبراني.

4- مقارنة مع اتفاقية بودابست (اتفاقية مجلس أوروبا للجرائم الإلكترونية)

تُمثل اتفاقية بودابست لعام 2001 المرجعية الدولية⁶¹ الأبرز في مجال تشريعات الجريمة الإلكترونية، وقد بنت كثير من دول العالم تشريعاتها في ضوءها. ولم تنضم الجزائر إليها بعد، غير أن أحكام قانونها 04-09 تتقاطع معها في كثير من المسائل الجوهرية، مما يُشير إلى تأثير المشرع الجزائري بمعاييرها دون التصريح بذلك.

5- التعاون الدولي والتبادل المعلوماتي المواد (17-22)

أرست المواد 17 إلى 22 من القانون 04-09 أسس التعاون القضائي والأمني الدولي في مجال مكافحة الجرائم الإلكترونية، من خلال نظام لتبادل المعلومات والإنابات القضائية الدولية. وأنشأت هذه المواد إطاراً للتعاون مع نظيراتها من الأجهزة الأجنبية في ضوء مبدأ ازدواجية التجريم وضمانات المعاملة بالمثل.

⁶¹ اتفاقية بودابست لمجلس أوروبا بشأن الجريمة الإلكترونية، 2001.

الفرع الثالث: جهود الجزائر من خلال الاتفاقيات العربية و الدولية و العالمية

إن التحديات التي يفرضها الطابع الدولي للجريمة السيبرانية تدفع نحو تطوير أطر قانونية دولية للتعاون⁶². ويتجلى ذلك في سعي الجزائر، كما في العديد من الدول، إلى تبني الاتفاقيات الدولية ذات الصلة، وتفعيل آليات المساعدة القضائية المتبادلة من خلال اتفاقيات ثنائية أو متعددة الأطراف. فبدون تعاون فعال، يصبح من الصعب ردع هذه الجرائم وملاحقة مرتكبيها، نظراً لقدرتهم على استغلال الثغرات القانونية والتكنولوجية عبر الحدود.

في ضوء ما سبق، فإن الطابع الدولي للجريمة السيبرانية ليس مجرد وصف، بل هو واقع يفرض إعادة النظر في المفاهيم التقليدية للاختصاص القضائي وآليات التعاون القانوني. إن معالجة هذه الظاهرة تتطلب رؤية استراتيجية تتجاوز حدود الدولة، وترتكز على تضافر الجهود الدولية لضمان فعالية المكافحة، بما يضمن تحقيق العدالة وحماية المجتمعات الرقمية.

أولاً: التصديق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات

يعكس تصديق الجزائر على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، بموجب المرسوم الرئاسي رقم 14-252⁶³، التزاماً إقليمياً بمواجهة التحديات المتزايدة للجرائم السيبرانية. تأتي هذه الخطوة في سياق محاولة لتوحيد الجهود العربية في مجال مكافحة جرائم تقنية المعلومات، والتي تتجاوز الحدود الوطنية التقليدية. إن هذا التصديق يمثل نقطة انطلاق نحو تعزيز آليات التعاون القضائي والأمني بين الدول العربية، ولكنه يثير في الوقت ذاته تساؤلات حول مدى كفاية الإطار القانوني الوطني لاستيعاب أحكام الاتفاقية.

يُعدّ المرسوم 14-252 بمثابة اعتراف تشريعي بأهمية الاتفاقية العربية كأداة لتعزيز الأمن السيبراني. ومع ذلك، فإن التحليل النقدي يفرض ضرورة تقييم مدى توافق المصطلحات

⁶² عبد الكريم قاسم، التعاون الدولي في مكافحة جرائم الإنترنت، مجلة الاجتهاد القضائي، جامعة محمد خيضر بسكرة، العدد 22، 2022.

⁶³ المرسوم الرئاسي 14-252 المؤرخ في 08 سبتمبر 2014 يتضمن التصديق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات بالقاهرة بتاريخ 2010/12/21

والمفاهيم الواردة في الاتفاقية مع تلك المعتمدة في التشريعات الوطنية الجزائرية، قد تظهر فجوات أو اختلافات تفسيرية تحتاج إلى معالجة لتجنب إضعاف فعالية تطبيق الاتفاقية على أرض الواقع، وضمان عدم ترك ثغرات يستغلها مجرمو الفضاء السيبراني.

من الجداول المهمة هو تقييم كيفية تأثير أحكام الاتفاقية العربية على التحديث المستقبلي للتشريعات الوطنية. فعلى سبيل المثال، قد تتطلب مواد الاتفاقية، مثل تلك المتعلقة بتجريم أفعال معينة أو آليات التعاون، تعديلات على القانون 04-09 أو استكمالاً له بقوانين أخرى. إن عملية المواءمة التشريعية هذه تتطلب دراسة معمقة لضمان انسجام الترسانة القانونية الوطنية مع الالتزامات الدولية، دون المساس بالسيادة الوطنية الجزائرية في تنظيم هذا المجال.

إن تطبيق الاتفاقية العربية لا يقتصر على الجانب التشريعي فحسب، بل يمتد ليشمل الجانب الإجرائي والتعاوني. ويتطلب تفعيل بنودها، لا سيما تلك المتعلقة بالاستجابة السريعة وتبادل المعلومات، وجود آليات تنسيق فعالة بين مختلف الجهات المعنية في الجزائر، مثل وحدات الجرائم السيبرانية والنيابة العامة والأجهزة الأمنية. كما أن التحديات المتعلقة بالولاية القضائية في الجرائم العابرة للحدود تستدعي تفعيل آليات التعاون الدولي المنصوص عليها في الاتفاقية.

في الختام، فإن تصديق الجزائر على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات هو خطوة إيجابية نحو تعزيز الأمن السيبراني على المستوى الإقليمي. ومع ذلك، فإن فعالية هذا التصديق تتوقف على مدى قدرة الإطار القانوني الوطني على استيعاب أحكامها، وتطوير آليات التعاون العملي، وضمان التنسيق الفعال بين مختلف الجهات الفاعلة. إن التقييم المستمر لمدى التوافق والتطبيق سيحدد النجاح الحقيقي لهذا الالتزام الدولي .

ثانيا : اتفاقية مالابو

تمثل اتفاقية مالابو، رسمياً "اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية"⁶⁴، إطاراً شاملاً ومتكاملاً يهدف إلى تعزيز الأمن السيبراني وحماية البيانات عبر القارة الأفريقية. تتجاوز الاتفاقية مجرد التجريم، لتشمل جوانب وقائية وتعاونية، مع التركيز على بناء القدرات وتطوير البنى التحتية اللازمة لمواجهة التحديات المتزايدة للجرائم السيبرانية. إنها تعكس إرادة سياسية أفريقية موحدة لمعالجة هذه الظاهرة عبر الحدود.

تُعد اتفاقية مالابو خطوة هامة نحو توحيد التشريعات الوطنية الأفريقية في مجال الجرائم السيبرانية وحماية البيانات. فهي تحدد مجموعة من الجرائم السيبرانية التي يتعين على الدول الأعضاء تجريمها، وتضع مبادئ توجيهية لإنفاذ القانون والتعاون القضائي. كما تتطرق الاتفاقية إلى مفاهيم هامة مثل حماية البيانات الشخصية، وتضع أسساً لوضع سياسات وطنية فعالة في هذا المجال، مما يساهم في خلق بيئة رقمية آمنة للمواطنين والشركات.

من الناحية التحليلية، تبرز اتفاقية مالابو كنموذج للشراكة الإقليمية في مواجهة تهديدات عابرة للحدود. إلا أن فعاليتها على أرض الواقع تصطدم بتحديات كبيرة تتعلق بمدى التزام الدول الأعضاء بتطبيق أحكامها، ولا سيما في ظل تفاوت القدرات التقنية والبشرية بينها. إن مسألة تنزيل هذه الالتزامات على المستوى الوطني، وتكييف التشريعات القائمة مثل قانون 04-09 وقانون 24-06⁶⁵، يتطلب جهوداً مستمرة وإرادة سياسية قوية.

إن البعد الوقائي في اتفاقية مالابو جدير بالاهتمام، حيث تدعو إلى تعزيز الوعي المجتمعي بمخاطر الجرائم السيبرانية، وتطوير استراتيجيات لمنع وقوعها. كما تشدد على أهمية التعاون بين القطاعين العام والخاص في بناء منظومة أمن سيبراني متينة. ومع ذلك، فإن تقييم فعالية هذه الجوانب الوقائية يتطلب دراسات معمقة ومستمرة، تأخذ في الاعتبار مدى تطبيق هذه التوصيات في سياقات وطنية مختلفة.

⁶⁴ الاتحاد الإفريقي، اتفاقية الاتحاد الإفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية، مالابو 2014. متاح على الرابط:

<https://au.int>

⁶⁵ قانون العقوبات: الأمر رقم 66-156 المؤرخ في 8 يونيو سنة 1966 المعدل والمتمم بالقانون 24-06 المؤرخ في 2024/04/28

في سياق مكافحة الجرائم السيبرانية في الجزائر، يمكن اعتبار اتفاقية مالابو إطاراً مرجعياً لتعزيز الإطار القانوني الوطني. فعلى الرغم من وجود تشريعات مثل قانون 25-14⁶⁶، وقوانين أخرى تتعلق بالاتصالات .

ثالثاً : معاهدة الأمم المتحدة لمكافحة الجريمة السيبرانية

يمثل توقيع الجزائر على معاهدة الأمم المتحدة لمكافحة الجريمة السيبرانية سنة 2025⁶⁷ خطوة فارقة نحو تعزيز ترسانتها القانونية الوطنية في مواجهة التهديدات الرقمية المتزايدة. يعكس هذا التوقيع التزاماً دولياً بتوحيد الجهود لمكافحة الجرائم العابرة للحدود، والتي باتت تشكل تحدياً أمنياً واقتصادياً جسيماً. إن الانخراط في هذا الإطار الدولي يفتح آفاقاً جديدة للتعاون القضائي وتبادل المعلومات مع الدول الأطراف، مما يعزز القدرة على تتبع وإحالة مرتكبي هذه الجرائم.

إن تبني الجزائر لهذه المعاهدة، وإن كان على مستوى التوقيع المبدئي، يفرض عليها مسؤولية موازنة تشريعاتها الوطنية مع أحكامها. ويتطلب ذلك تقييماً دقيقاً للقانون 09-04 ،

بالإضافة إلى النظر في القوانين ذات الصلة مثل قانون 24-06 وقانون 18-07 المتعلق بحماية الأشخاص الطبيعيين.

⁶⁶ القانون رقم 25-14 المؤرخ في 3 غشت 2025، المتضمن قانون الإجراءات الجزائية، الجريدة الرسمية للجمهورية الجزائرية، العدد 54 لسنة 2025.

⁶⁷ اتفاقية الأمم المتحدة لمكافحة الجرائم السيبرانية، وقّعت عليها الجزائر في أكتوبر 2025.

خاتمة

شهد العالم اليوم طفرة نوعية في مجال المعاملات السيبرانية، حيث شهدت الألفية الأخيرة تطورا إلكترونيا مذهلا صاحبه تداخل وتباين التعاملات الاقتصادية والشخصية والتجارية والإدارية بما يعني تحول العالم من نمط الفضاء المغلق إلى نمط الفضاء المفتوح في كل المجالات على كل المستويات وتعتبر الجرائم المتصلة بتكنولوجيات الاعلام والاتصال إحدى أهم الهواجس التي أصبحت تؤرق المواطن في حياته الشخصية، والدول في سيادها وأمنها، باعتبار أن التطور التكنولوجي والرقمي الهائل وما صاحبه من تأثير على كل المستويات أثر بشكل أو بآخر على أمن واستقرار الشعوب من جهة بل وأصبحت تداعيات هذه الثورة التكنولوجية تمس حرمة وخصوصية المواطن من جهة أخرى. في ظل هذا التحدي الرقمي التكنولوجي الجديد سعت الدول إلى سن حزمة من التشريعات والآليات القانونية والمؤسسية للتصدي لهذه الجريمة التي أضحت تسمى في الأدبيات الأكاديمية بالجريمة المتصلة بتكنولوجيات الاعلام والاتصال. والجزائر إحدى هذه الدول التي لم تكن في منأى من تداعيات هذه الظاهرة، حيث انتشرت في الآونة الأخيرة جرائم تمس بالحياة الشخصية للمواطن وتمس أيضا بأمن واستقرار البلاد وبكل جوانب الحياة الأخرى اقتصاديا، سياسيا، ثقافيا، من هنا سعى المشرع الجزائري إلى سن العديد من التشريعات والقوانين للتصدي لهذه الجرائم وأهم هذه التشريعات القانون 09/04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها وغيره من التشريعات التي تحد من انتشار هذه الجرائم.

إن المنظومة التشريعية الجزائرية لمكافحة الجرائم السيبرانية تمتلك أسسا قانونية متينة يتقدمها القانون 04-09 بأحكامه الإجرائية المتطورة نسبيا، إضافة إلى النصوص الجنائية الموضوعية في قانون العقوبات. غير أن هذه المنظومة تستوجب تحديثا تشريعيا دوريا يواكب التطور المتسارع للجريمة السيبرانية ، ولا سيما في مسائل الذكاء الاصطناعي والعملات الرقمية وإنترنت الأشياء التي لم تتطرق إليها النصوص القائمة بصورة صريحة.

إن الجريمة السيبرانية من بين الجرائم المستحدثة و أشد خطورة على المجتمع الدولي ، لذا لابد من تضافر الجهود من اجل مكافحتها و القضاء عليها و معاقبة مرتكبيها ، و بما إن

الجزائر شاركت في المؤتمر الثالث عشر الامم المتحدة لمنع الجريمة و العدالة الجنائية و و انظمت للاتفاقية العالمية لمكافحة الجريمة السيبرانية و رغم ان هذه الجرائم غير معروفة كثيرا في المجتمع الجزائري و من يرتكبها لا يدرك مخاطرها إلا أن الجزائر وضعت قواعد قانونية لمعاقبة مرتكبي هذه الجرائم و وضعت مجموعة من الاليات و الميكانزمات من اجل تحقيق الأمن السيبراني في البلد ، خاصة و أنها تتجه نحو رقمنة جميع القطاعات مثل العدالة و التعليم و الدفاع الوطني.

أهم النتائج المتوصل إليها :

- الجرائم السيبرانية جرائم يصعب التحكم فيها و التصدي لها
- الجرائم السيبرانية تزداد خطورة في ظل التطور التكنولوجي و الالكتروني الرقمي و شبكة الانترنت و استخدام مواقع التواصل الاجتماعي
- عدم التوعية و النشر بثقافة الأمن السيبراني ومعاقبة المرتكبين لها يؤدي إلى زيادة انتشار هذه الجرائم
- أهم التوصيات المقترحة:

- إدراج مادة الأمن السيبراني في الجامعات و المدارس العسكرية و الأمنية و مدرسة القضاء، وإنشاء مدرسة خاصة بالأمن السيبراني.
- إنشاء أجهزة وطنية تابعة لوزارة الدفاع الوطني مختصة في الأمن السيبراني
- تدريب و تأهيل وحدات عسكرية و أمنية خاصة ، من اجل تأمين المنظومة المعلوماتية من الهجمات السيبرانية خاصة الهجمات الإرهابية.
- وضع نظام قانوني للجرائم المستحدثة مع إنشاء محاكم متخصصة في المعاقبة على جميع الجرائم المستحدثة

-وضع اتفاقية دولية أو اتفاقيات إقليمية لمكافحة الجريمة السيبرانية.

قائمة المراجع

أولاً: النصوص القانونية والرسمية

- دستور 2020 للجمهورية الجزائرية الديمقراطية الشعبية، الجريدة الرسمية
- اتفاقية الأمم المتحدة لمكافحة الجرائم السيبرانية، وقّعت عليها الجزائر في أكتوبر 2025.
- اتفاقية الاتحاد الأفريقي للأمن السيبراني والبيانات الشخصية (اتفاقية مالابو)، 2014.
- الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، جامعة الدول العربية. 2010
- اتفاقية بودابست لمجلس أوروبا بشأن الجريمة الإلكترونية، 2001.
- قانون الإجراءات الجزائية 25-14 الصادر في 03 أوت 2025 الجريدة الرسمية عدد 54 لسنة 2025
- قانون العقوبات ، الأمر 66-156 المعدّل والمتمم بالقانون 24-06، الصادر في 28 افريل 2024 الجريدة الرسمية عدد 30 لسنة 2024
- القانون رقم 18-05 الصادر في 10 ماي 2018 المتعلق بالتجارة الإلكترونية، الجريدة الرسمية عدد 28 لسنة 2018.
- القانون رقم 18-07 الصادر في 10 يونيو 2018 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، المعدل و المتمم بالقانون 25-11 الصادر في 24 يوليو 2025 الجريدة الرسمية عدد 48، لسنة 2025.
- قانون رقم 20-03 المتعلق بتحديد القواعد العامة المتعلقة بالبريد والمواصلات السلكية واللاسلكية.

- المرسوم الرئاسي 14-252 المؤرخ في 08 سبتمبر 2014 يتضمن التصديق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات بالقاهرة بتاريخ 2010/12/21
- القانون رقم 09-04 المؤرخ في 5 أغسطس 2009، المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية للجمهورية الجزائرية، العدد 47، 2009.
- وزارة الدفاع الوطني الجزائري، الاستراتيجية الوطنية لأمن الأنظمة المعلوماتية 2025-2029. (NSISS)

ثانياً: المؤلفات والكتب العربية

- أحمد حسام طه، الجرائم الإلكترونية: دراسة مقارنة، دار النهضة العربية، القاهرة، 2018.
- إبراهيم محمد، القانون الجنائي للأعمال الإلكترونية، دار الجامعة الجديدة، الإسكندرية، 2020.
- خالد ممدوح إبراهيم، الجريمة الإلكترونية وأساليب مكافحتها، دار الفكر الجامعي، الإسكندرية، 2017.
- سليمان عبد المنعم، أصول التجريم والعقاب في الجرائم الإلكترونية، منشورات الحلبي الحقوقية، بيروت، 2019.
- عبد الفتاح بيومي حجازي، الجريمة الإلكترونية في القانون الجزائري والمقارن، دار الفكر الجامعي، 2016.
- محمد طارق، الأمن السيبراني والجريمة الإلكترونية: منظور قانوني، دار النهضة العربية، 2021.
- نصر محمد المصري، إشكاليات الإثبات في الجرائم الإلكترونية، دار الجامعة الجديدة، 2019.
- وليد فاروق، حماية البيانات الشخصية في الفضاء الإلكتروني، دار الكتب القانونية، المحلة الكبرى، 2020.

- محمد سامي الشوا: "ثورة المعلومات وانعكاساتها على قانون العقوبات". دار النهضة العربية، القاهرة. 1994.

ثالثاً: الأطروحات الجامعية والمقالات العلمية

- الجرائم المعلوماتية في الجزائر: المواجهة والتحدي، مجلة الحقوق والعلوم السياسية - جامعة خنشلة ، مجلد 12 عدد 01 سنة 2025
- الأمن السيبراني المفهوم و الأهمية ، قاضي سعاد ، جامعة محمد بوضياف المسيلة ، سنة 2025
- الجهود الدولية في مواجهة الجرائم السيبرانية ، بن أوزينة سندس ، جامعة غرداية، كلية الحقوق والعلوم السياسية ، 2025
- فريدة عبد الفتاح راضي، سالي عوض السقاالجرائم الإلكترونية والجرائم المعلوماتية: من وجهة نظر قانونية وتقنية. المجلة الدولية للبحوث والدراسات القانونية، الإصدار 3، العدد 5 (2024).
- مقال مهدي رضا مجلة إيليزا للبحوث والدراسات المجلد 06 /العدد: 2 - 2021 ، ص تاريخ النشر 2021/12/15
- بوزيان محمد، الحماية الجنائية للمعطيات المعلوماتية في القانون الجزائري والمقارن، رسالة ماجستير، جامعة الجزائر، 2020.
- بلحيمر عبد القادر، الجرائم المعلوماتية في التشريع الجزائري - دراسة تحليلية مقارنة، أطروحة دكتوراه، كلية الحقوق، جامعة أبو بكر بلقايد تلمسان، 2019.
- حسبية بن يوسف، إشكاليات التحقيق في الجرائم الإلكترونية بين متطلبات الكشف وضمانات الحقوق، مجلة القانون والمجتمع، جامعة عبد الحميد بن باديس مستغانم، العدد 15، 2021.
- عبد الكريم قاسم، التعاون الدولي في مكافحة جرائم الإنترنت، مجلة الاجتهاد القضائي، جامعة محمد خيضر بسكرة، العدد 22، 2022.
- رشيد معزوز، دور الشرطة القضائية في مكافحة الجرائم الإلكترونية في الجزائر، مجلة الحقوق والعلوم الإنسانية، العدد 35، جامعة زيان عاشور الجلفة، 2023.

- مقال الكتروني أول هجوم سيبراني في التاريخ.. كيف شلّت "دودة موريس" الإنترنت
عام 1988؟ مجلة www.alaraby.com/news محدث 27 يناير 2026

رابعاً: المراجع الأجنبية

- Bensoussan, A., Informatique, Télécoms, Internet, Editions Francis Lefebvre, Paris, 2020.
- Clough, J., Principles of Cybercrime, Cambridge University Press, 2nd ed., 2015.
- Mitnick, K. & Simon, W., The Art of Intrusion, John Wiley & Sons, 2005.
- UNODC, Comprehensive Study on Cybercrime, United Nations Office on Drugs and Crime, Vienna, 2013.
- Interpol, Cybercrime in Africa: Threat Assessment Report, Interpol, Lyon, 2021.
- ITU, Global Cybersecurity Index 2024, International Telecommunication Union, Geneva, 2024.
- African Union, Convention on Cyber Security and Personal Data Protection (Malabo Convention), 2014.
- Council of Europe, Convention on Cybercrime (Budapest Convention), ETS No. 185, 2001.
- United Nations General Assembly, Resolution A/RES/79/243 on Cybercrime, 2024.
- Guinier, D., Sécurité et qualité des systèmes d'information, Masson, Paris, 2019.

الفهرس

7.....	مقدمة:
17.....	الفصل الأول ماهية الجريمة السيبرانية
17.....	المبحث الأول: مفهوم الجريمة السيبرانية
17.....	المطلب الأول: تعريف الجريمة السيبرانية
25.....	المطلب الثاني: خصائص الجريمة السيبرانية
29.....	المطلب الثالث : تصنيف وانواع الجريمة السيبرانية
32.....	المبحث الثاني : الجرائم السيبرانية وفق ما جاء به التشريع الجزائري
32.....	المطلب الأول: الجرائم الواقعة على الأنظمة الالية والبيانات المعلوماتية
36.....	المطلب الثاني: الجرائم السيبرانية الواقعة على الأموال
39.....	المطلب الثالث: الجرائم السيبرانية الواقعة على الأشخاص والمجتمع
46.....	الفصل الثاني: آليات مكافحة الجريمة السيبرانية في التشريع الجزائري
46.....	المبحث الأول: الحماية الموضوعية للنظام المعلوماتي
47.....	المطلب الأول: الحماية في نصوص الملكية الفكرية
59.....	المطلب الثاني: الحماية في قانون العقوبات
67.....	المطلب الثالث: الحماية في قانون الوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال....
72.....	المبحث الثاني: الحماية الإجرائية للنظام المعلوماتي
72.....	المطلب الأول: إجراءات التحقيق في الجريمة السيبرانية
77.....	المطلب الثاني: صعوبة مكافحة الجريمة السيبرانية
81.....	المطلب الثالث: جهود الجزائر لمكافحة الجرائم السيبرانية
88.....	خاتمة
90.....	قائمة المراجع