International Journal of Law Research and Studies (IJLRS)
المجلة الدولية للبحوث والدراسات القانونية
IJLRS
Vol. (5), No. (9) September 2026 الإصدار (5)، العدد (9)

المسؤولية القانونية عن الجرائم السيبرانية وأثرها في حماية بيئة الأعمال الرقمية: دراسة مقارنة

مولاي أحمد سالم
أستاذ متعاون بجامعة نواكشوط، موريتانيا
moulaye84@gmail.com

ملخص

تناول البحث موضوع المسؤولية القانونية عن الجرائم السيبرانية وآليات حماية بيئة الأعمال الرقمية، في ظل التحول المتسارع نحو الرقمنة وتزايد اعتماد الأنشطة الاقتصادية والتجارية على الوسائل والتقنيات الرقمية، ويهدف إلى بيان مفهوم الجرائم السيبرانية وخصائصها، وتحديد الأساس القانوني للمسؤولية المترتبة عنها، مع دراسة مسؤولية الأشخاص الطبيعيين والأشخاص الاعتباريين والمسيرين ومقدمي الخدمات الرقمية، إلى جانب المسؤولية المدنية والتأديبية والتنظيمية، وقد اعتمد البحث على المنهج الوصفي التحليلي والمنهج المقارن، من خلال تحليل الإطار القانوني الموريتاني والاستفادة من بعض التشريعات المقارنة، مع التركيز على مدى فعالية القواعد القانونية في حماية بيئة الأعمال الرقمية، وتوصل البحث إلى أن التشريع الموريتاني قطع خطوات مهمة في تنظيم المجال الرقمي ومكافحة الجرائم السيبرانية، إلا أن المنظومة القانونية لا تزال تواجه بعض التحديات، من أبرزها تشتت النصوص، وسرعة تطور الأنماط الإجرامية، والحاجة إلى مزيد من التنظيم لمسؤولية الأشخاص الاعتباريين ومقدمي الخدمات الرقمية، وقواعد الإبلاغ عن الحوادث وحماية البيانات التجارية، وخلص البحث إلى ضرورة تحديث التشريعات بصورة دورية، وإقرار إطار قانوني متكامل، وتعزيز مسؤولية الشركات ومقدمي الخدمات، وتطوير آليات الوقاية والأمن السيبراني والتعاون الدولي، بما يحقق حماية أكثر فعالية واستقراراً لبيئة الأعمال الرقمية.

الكلمات الافتتاحية: المسؤولية القانونية، الجرائم السيبرانية، بيئة الأعمال، الحماية، الرقمنة.

Legal Liability for Cybercrimes and Its Impact on Protecting the Digital Business Environment: A Comparative Study

"Responsabilité juridique en matière de cybercriminalité et son impact sur la protection de l'environnement numérique des entreprises: une étude comparative"

Moulaye Ahmed Salem
Associate Professor at the University of Nouakchott, Mauritania
moulaye84@gmail.com

Abstract

This research addresses the issue of legal responsibility for cybercrimes and mechanisms for protecting the digital business environment, in light of the accelerating shift towards digitalization and the increasing reliance of economic and commercial activities on digital means and technologies. It aims to clarify the concept of cybercrimes and their characteristics, and to define the legal basis for the resulting responsibility. The research examines the responsibility of natural persons, legal entities, managers, and digital service providers, in addition to civil, disciplinary, and regulatory liability. The research employs a descriptive-analytical approach and a comparative methodology, analyzing the Mauritanian legal framework

and drawing upon comparative legislation. It focuses on the effectiveness of legal rules in protecting the digital business environment. The research concludes that Mauritanian legislation has made significant strides in regulating the digital sphere and combating cybercrimes. However, the legal system still faces some challenges, most notably the fragmentation of texts, the rapid evolution of criminal patterns, the need for further regulation of the responsibility of legal entities and digital service providers, and the rules for reporting incidents and protecting commercial data. The research concludes that it is necessary to update legislation periodically, establish a comprehensive legal framework, strengthen the responsibility of companies and service providers, and develop prevention and security mechanisms. Cybersecurity and international cooperation, leading to more effective and stable protection of the digital business environment.

Keywords: Legal Responsibility, Cybercrime, Business Environment, Protection, Digitalization.

مقدمة

شهد العالم خلال العقود الأخيرة تحولاً متسارعاً نحو الرقمنة، شمل مختلف مناحي الحياة الاقتصادية والتجارية، وأدى إلى إعادة تشكيل طرق ممارسة الأنشطة المهنية وإدارة المؤسسات وإبرام المعاملات وتبادل المعلومات. فقد أصبحت التقنيات الرقمية، بما فيها شبكة الإنترنت والحوسبة السحابية والذكاء الاصطناعي وقواعد البيانات والتجارة الإلكترونية، مكونات أساسية في بيئة الأعمال الحديثة، وأسهمت في تعزيز سرعة المعاملات وخفض تكاليفها وتوسيع نطاق النشاط الاقتصادي، غير أن هذا التحول أفرز في المقابل مخاطر قانونية وأمنية جديدة، يأتي في مقدمتها انتشار الجرائم السيبرانية التي تستهدف الأنظمة المعلوماتية والبيانات والأموال والمصالح التجارية للشركات والمؤسسات، وتتميز الجرائم السيبرانية بخصوصية تجعل مواجهتها أكثر تعقيداً من الجرائم التقليدية، بالنظر إلى سرعة ارتكابها، وصعوبة اكتشاف مرتكبيها وإثباتها، وإمكانية ارتكابها عن بُعد وعبر الحدود الوطنية، فضلا عن تطور وسائل وأساليب الاعتداء بما يواكب التطور المستمر للتكنولوجيا. وقد أصبحت هذه الجرائم تمس بصورة مباشرة بيئة الأعمال الرقمية من خلال اختراق الأنظمة المعلوماتية، والاستيلاء على البيانات، والاحتيال الإلكتروني، وانتحال الهوية، وتعطيل الخدمات، والاعتداء على الأسرار والمعلومات التجارية، الأمر الذي قد يؤدي إلى خسائر مالية جسيمة، وتعطيل النشاط الاقتصادي، والإضرار بالسمعة التجارية، وتقويض الثقة في المعاملات الرقمية.

وتتجلى أهمية الموضوع في كون حماية بيئة الأعمال الرقمية لم تعد تتحقق من خلال التجريم والعقاب وحدهما، وإنما أصبحت تقتضي إقامة منظومة متكاملة للمسؤولية القانونية تشمل المسؤولية الجنائية والمدنية والتأديبية والتنظيمية، إلى جانب اعتماد آليات وقائية تقوم على الأمن السيبراني والحوكمة الرقمية وإدارة المخاطر والامتثال القانوني، كما تبرز أهمية الموضوع بالنسبة للتشريع الموريتاني بالنظر إلى تزايد الاعتماد على الوسائل الرقمية في النشاط الاقتصادي، والحاجة إلى تقييم مدى كفاية الإطار القانوني القائم في مواجهة الجرائم السيبرانية وحماية الشركات والمتعاملين في البيئة الرقمية.

وتسعى هذه الدراسة إلى تحقيق مجموعة من الأهداف، من أهمها تحديد مفهوم الجرائم السيبرانية وخصائصها في بيئة الأعمال الرقمية، وبيان طبيعة المسؤولية القانونية الناشئة عنها وأسسها، وتحديد نطاق مسؤولية الأشخاص الطبيعيين والأشخاص الاعتباريين والمسيرين ومقدمي الخدمات الرقمية، فضلاً عن دراسة آليات الحماية القانونية والوقائية لبيئة الأعمال الرقمية، كما تهدف الدراسة إلى تقييم مدى كفاية التشريع الموريتاني في مواجهة هذه الجرائم، والاستفادة من بعض التجارب التشريعية المقارنة للوصول إلى مقترحات من شأنها تعزيز الحماية القانونية والأمن القانوني للمعاملات والأنشطة الاقتصادية الرقمية.

وانطلاقاً من ذلك، تتمثل إشكالية البحث في التساؤل الآتي:

إلى أي مدى توفر قواعد المسؤولية القانونية وآليات الحماية المعتمدة في التشريع الموريتاني والتشريعات المقارنة حماية فعالة لبيئة الأعمال الرقمية في مواجهة الجرائم السيبرانية؟

وللإجابة على الإشكالية وما يتفرع عنها من تساؤلات، تم الاعتماد على المنهج الوصفي التحليلي من خلال عرض المفاهيم والقواعد القانونية المتعلقة بالجرائم السيبرانية والمسؤولية المترتبة عنها، وتحليل النصوص القانونية ذات الصلة وبيان مدى

فعاليتها في حماية بيئة الأعمال الرقمية. كما تم توظيف المنهج المقارن من خلال الاستفادة من بعض التشريعات المقارنة، بهدف إبراز أوجه التشابه والاختلاف بينها وبين التشريع الموريتاني، وتحديد الحلول التي يمكن الاستفادة منها في تطوير الإطار القانوني الوطني.

وبناء على ما سبق، سيتم تقسيم هذا البحث إلى مطلبين؛ يتناول المطلب الأول الإطار القانوني للمسؤولية عن الجرائم السيبرانية في بيئة الأعمال الرقمية، أما المطلب الثاني فيتناول صور المسؤولية القانونية وآليات حماية بيئة الأعمال الرقمية.

المطلب الأول: الإطار القانوني للجرائم السيبرانية في بيئة الأعمال الرقمي

سنتناول هذا المطلب من خلال تحديد ماهية الجرائم السيبرانية في بيئة الأعمال الرقمية (فرع أول)، ثم معرفة الأساس القانوني للمسؤولية عن الجرائم السيبرانية (فرع ثاني).

الفرع الأول: ماهية الجرائم السيبرانية في بيئة الأعمال الرقمية:

سندرس هذا الفرع من خلال معرفة مفهوم الجرائم السيبرانية وخصائصها (فقرة أولى)، ثم مع مفهوم تحديد بيئة الأعمال الرقمية وأبرز المخاطر السيبرانية التي تهددها (فقرة ثانية).

الفقرة الأولي: مفهوم الجرائم السيبرانية وخصائصها:

أولاً: مفهوم الجرائم السيبرانية:

تُعد الجرائم السيبرانية من أبرز التحديات القانونية التي أفرزها التطور التكنولوجي والاعتماد المتزايد على الوسائل الرقمية في مختلف الأنشطة الاقتصادية والتجارية. وقد أدى انتشار الإنترنت، والحوسبة السحابية، والذكاء الاصطناعي، والتجارة الإلكترونية إلى ظهور أنماط جديدة من السلوك الإجرامي تختلف في وسائلها وموضوعها عن الجرائم التقليدية، الأمر الذي دفع التشريعات الوطنية والاتفاقيات الدولية إلى تبني قواعد خاصة لمواجهتها. [1]

ولم يستقر الفقه على تعريف موحد للجريمة السيبرانية [2]، ويرجع ذلك إلى تعدد صورها وسرعة تطورها، فذهب اتجاه إلى تعريفها بأنها: "كل فعل غير مشروع يُرتكب باستخدام نظم المعلومات أو الشبكات الإلكترونية أو يكون موجهاً ضدها، ويترتب عليه الاعتداء على البيانات أو الأنظمة أو المصالح المحمية قانوناً" [3]، ومن الناحية القانونية، يمكن تعريف الجريمة السيبرانية بأنها: "كل سلوك مجرم قانوناً يرتكب عمداً باستخدام تقنية المعلومات أو الشبكات الرقمية أو يستهدفها، ويترتب عليه المساس بسرية البيانات أو سلامتها أو توافرها، أو الإضرار بالأشخاص أو الأموال أو المصالح الاقتصادية، بما في ذلك الأنشطة التجارية وبيئة الأعمال الرقمية" [4]، عرفها المشرع المغربي في المادة الثانية من القانون 20-05 المتعلق بالأمن السيبراني الصادر سنة 2020 بأنها: "مجموعة من الأفعال المخالفة للتشريع الوطني أو الاتفاقيات الدولية التي صادقت عليها المملكة المغربية، التي تستهدف شبكات ونظم المعلومات أو تستعملها كوسيلة لارتكاب جنحة أو جناية"، كما عرفها المشرع الجزائري بموجب أحكام المار 02 من القانون 09-04 على أنها: "جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات، وأي جريمة أخري ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية، أو نظام للاتصالات الإلكترونية". [5]

ثانياً: خصائص الجرائم السيبرانية:

تتميز الجرائم السيبرانية بجملة من الخصائص التي تميزها عن الجرائم التقليدية، وتفسر الحاجة إلى قواعد قانونية وإجرائية خاصة لمواجهتها، ولا سيما في مجال حماية بيئة الأعمال الرقمية.

---

[1] فريدة عبد الفتاح راضي /سالي عوض السقا، الجرائم الإلكترونية والجرائم المعلوماتية: من وجهة نظر قانونية وتقنية، المجلة الدولية للبحوث والدراسات القانونية، المجلد 03، العدد 05، 2024، ص 6.

[2] يستند تنظيم ومكافحة الجريمة السيبرانية في موريتانيا إلى القانون رقم 2016-007 المتعلق بالجريمة السيبرانية.

[3] منال هلال زهرة، تكنولوجيا الاتصال والمعلومات، ط1، دار أسامة، الأردن، 2014، ص 374.

[4] حكيمة جاب الله، انعكاسات الجريمة السيبرانية على البيئة الرقمية: دراسة في آليات واستراتيجيات مكافحتها، مجلة جلويات جامعة الجزائر 1، المجلد 35، العدد 03، السنة 2023، ص 4.

[5] فاضل عائشة، المسؤولية الجزائية في الجرائم الإلكترونية، مجلة الحقوق والحريات، المجلد 11، العدد 01 السنة 2023، ص 05.

1. **الطابع الرقمي للجريمة:**

ترتكب الجرائم السيبرانية باستخدام الحواسيب أو الشبكات أو الأنظمة المعلوماتية، أو تستهدف هذه الوسائل ذاتها، مما يجعل البيئة الرقمية مسرحًا للنشاط الإجرامي. ويترتب على ذلك أن محل الاعتداء قد يكون بيانات أو برامج أو أنظمة معلوماتية، وليس أموالًا أو أشياء مادية بالمعنى التقليدي.

هذا ويفرض الطابع الرقمي إعادة النظر في مفاهيم المال والمحرر والدليل في قانون الأعمال، إذ أصبحت البيانات التجارية وقواعد المعلومات والأصول الرقمية تمثل عناصر ذات قيمة اقتصادية تستحق الحماية القانونية.

2. **الطابع العابر للحدود:**

غالبا ما ترتكب الجريمة السيبرانية عبر شبكة الإنترنت، بما يسمح بوقوعها في أكثر من دولة في الوقت نفسه، فقد يوجد الجاني في دولة، والخادم الإلكتروني في دولة ثانية، والمجني عليه في دولة ثالثة. [1]

وعليه تثير هذه الخاصية إشكالات تنازع الاختصاص القضائي والقانون الواجب التطبيق، وتبرز أهمية التعاون القضائي الدولي وتوحيد التشريعات لمكافحة الجرائم التي تستهدف الشركات والمعاملات التجارية الدولية.

3. **صعوبة اكتشاف الجريمة وإثباتها:**

تعتمد الجرائم السيبرانية على وسائل تقنية متطورة، ويستطيع مرتكبوها إخفاء هوياتهم أو محو آثارهم الرقمية خلال وقت قصير، كما تتسم الأدلة الرقمية بسهولة التعديل أو الإتلاف.

مما يقتضي من هذه الخاصية تطوير قواعد الإثبات الإلكتروني وتعزيز قدرات جهات التحقيق في جمع وتحليل الأدلة الرقمية، بما يضمن حماية الحقوق وتحقيق الأمن القانوني في بيئة الأعمال.

4. **السرعة والاتساع في تنفيذ الجريمة:**

يمكن تنفيذ الجريمة السيبرانية خلال ثوانٍ معدودة، مع إمكانية استهداف عدد كبير من الضحايا أو الأنظمة المعلوماتية في وقت واحد، وهو ما يضاعف حجم الأضرار الاقتصادية. [2]

ففي بيئة الأعمال الرقمية قد يؤدي هجوم إلكتروني واحد إلى تعطيل نشاط شركة بأكملها أو تسريب بيانات آلاف العملاء، وهو ما يبرز ضرورة اعتماد تدابير وقائية وتشريعات رادعة.

5. **الطابع الاقتصادي والتقني:**

ترتبط معظم الجرائم السيبرانية بتحقيق منفعة مالية أو الإضرار بالمنافسين، مثل الاحتيال الإلكتروني، وسرقة الأسرار التجارية، والاعتداء على قواعد البيانات، والابتزاز الإلكتروني.

وتتجاوز آثار هذه الجرائم الإضرار بالأفراد لتطال الاقتصاد الوطني وثقة المستثمرين واستقرار الأسواق، مما يجعلها من الجرائم ذات الأهمية الخاصة في قانون الأعمال.

6. **التطور المستمر لأساليب ارتكاب الجريمة:**

تتطور وسائل ارتكاب الجرائم السيبرانية باستمرار مع تطور التكنولوجيا، إذ يستغل الجناة تقنيات حديثة مثل الذكاء الاصطناعي، والبرمجيات الخبيثة المتطورة، والهجمات على الحوسبة السحابية وإنترنت الأشياء.

ويفرض هذا التطور على المشرع اعتماد سياسة تشريعية مرنة لا تقتصر على تجريم وسائل محددة، بل تستوعب الأنماط الإجرامية المستجدة، مع تحديث النصوص القانونية بصورة دورية.

تكشف هذه الخصائص أن الجرائم السيبرانية ليست مجرد جرائم تقنية، بل تمثل تهديدًا مباشرًا لاستقرار بيئة الأعمال الرقمية،

[1] فريدة عبد الفتاح راضي /سالي عوض السقا، الجرائم الإلكترونية والجرائم المعلوماتية: من وجهة نظر قانونية وتقنية – مرجع سابق – ص 09.
[2] الجرائم السيبرانية: مفهومها وآليات مكافحاتها، مجلة الحقوق والعلوم الإنسانية، المجلد 18، العدد 01، السنة 2025، ص 04.

لما تنطوي عليه من مخاطر على سرية البيانات التجارية، واستمرارية النشاط الاقتصادي، والثقة في المعاملات الإلكترونية، ومن ثم فإن خصوصيتها تبرر إقرار نظام قانوني متكامل يجمع بين التجريم الفعال، والإجراءات الجنائية المتخصصة، وآليات الوقاية والتعاون الدولي، بما يحقق حماية فعالة للمصالح الاقتصادية في العصر الرقمي.

الفقرة الثانية: مفهوم بيئة الأعمال الرقمية وأبرز المخاطر السيبرانية التي تهددها:

سنتناول هذه الفقرة من خلال معرفة مفهوم بيئة الأعمال (أولاً) ثم تحديد أبرز المخاطر السيبرانية التي تهدد بيئة الأعمال (ثانياً)

أولاً: مفهوم بيئة الأعمال:

تعرف البيئة بأنها: مجموعة العناصر البشرية المتفاوتة المهام والاختصاصات والدرجات الوظيفة والقناعات والكفاءات العلمية، المتفاعلة فيما بينها وفق منظومة إدارية لإنجاز مهام محددة، بينما تعرف البيئة الرقمية: تعرف أيضاً "بالبيئة التكنولوجية وهي عبارة عن البعد الإنساني للتطبيقات التكنولوجية المختلفة في المؤسسات، فضلاً عن تفاعل الإنسان وقناعته ومدى تقبله للتغيرات التكنولوجية الجديدة"، فالبيئة الرقمية تعكس ذلك الانتشار والاستخدام الكبير للتكنولوجيات الحديثة في جميع المجالات وهذا يؤدي لظهور ببيئة افتراضية يتفاعل فيها الأفراد والدول إلكترونياً بعيداً عن الحواجز الجغرافية والزمنية فهي وليدة استخدام الإنسان لهذه التكنولوجيات. [1]

هذا ولا يوجد تعريف تشريعي موحد لبيئة الأعمال الرقمية، إلا أن الفقه يتجه إلى اعتبارها مجموعة الأنشطة والعلاقات التجارية والاقتصادية التي تُمارس عبر الوسائل الرقمية، بالاعتماد على نظم المعلومات، وشبكات الاتصال، والمنصات الإلكترونية، بما يتيح إنشاء المعاملات التجارية وإدارتها وتنفيذها بصورة إلكترونية، وتتميز بيئة الأعمال الرقمية بأنها تعتمد على البيانات بوصفها أصلاً اقتصادياً، وعلى سرعة تداول المعلومات، والتواصل الفوري، والربط بين مختلف الفاعلين الاقتصاديين، وهو ما يسهم في زيادة كفاءة النشاط التجاري وتوسيع نطاق الأسواق. وفي المقابل، فإن هذا الاعتماد المكثف على التكنولوجيا يجعلها أكثر عرضة للتهديدات السيبرانية التي قد تمس استمرارية النشاط الاقتصادي والثقة في المعاملات الإلكترونية.

ثانياً: أبرز المخاطر السيبرانية التي تهدد بيئة الأعمال:

تتعرض بيئة الأعمال الرقمية لعدد متزايد من المخاطر السيبرانية التي تختلف في طبيعتها وآثارها، ومن أبرزها:

1. **الهجمات على الأنظمة المعلوماتية[2]، التي تستهدف تعطيل المواقع الإلكترونية أو قواعد البيانات أو البنية التحتية الرقمية للشركات:**

تشير الهجمات السيبرانية إلى محاولات غير مشروعة تستهدف الأنظمة الرقمية بهدف الوصول إلى المعلومات الحساسة أو تعطيل الخدمات. ومع التوسع في استخدام الخدمات الرقمية، أصبحت هذه الهجمات أكثر انتشارًا وتأثيرًا.

علاوة على ذلك، أدى استخدام الحوسبة السحابية والعمل عن بعد إلى زيادة نقاط الضعف داخل المؤسسات. وبالتالي، أصبح من الضروري اعتماد استراتيجيات أمنية شاملة.

ومن أبرز أهداف هذه الهجمات:

- سرقة البيانات الحساسة.
- تعطيل الخدمات الرقمية.
- الابتزاز المالي.
- التجسس الصناعي.
- التلاعب بالمعلومات.

[1] عامر إبراهيم قدليجي، الحكومة الإلكترونية، ط1، دار المسيرة، الأردن،2015، ص 323.
[2] بحث منشور على الرابط: https://tharaaedu.com/cyber_attacks/

وبناءً على ذلك، تحتاج المؤسسات إلى فهم هذه التهديدات من أجل تطوير استراتيجيات فعالة للحماية.

ومن أبرز أنواع الهجمات السيبرانية التي تستهدف المؤسسات:

- **هجمات البرمجيات الخبيثة:**

تُعد البرمجيات الخبيثة من أكثر التهديدات انتشارًا في عالم الأمن السيبراني. فعلى سبيل المثال، قد تصل هذه البرمجيات إلى الأنظمة عبر البريد الإلكتروني أو الروابط المشبوهة.

وتشمل هذه الهجمات:

- الفيروسات.
- الديدان.
- أحصنة طروادة.
- برامج الفدية.
- برامج التجسس.

وعند إصابة النظام، تبدأ هذه البرمجيات في سرقة البيانات أو تعطيل العمليات. لذلك، من المهم اتخاذ إجراءات وقائية مثل تحديث الأنظمة واستخدام برامج الحماية. [1]

بالإضافة إلى ذلك، ينصح بتدريب الموظفين على اكتشاف الملفات المشبوهة لتقليل فرص الاختراق.

- **هجمات التصيد الاحتيالي:**

تستهدف هذه الهجمات العنصر البشري بشكل مباشر، على سبيل المثال، قد يتلقى الموظف رسالة بريد إلكتروني تبدو رسمية لكنها تحتوي على رابط خبيث.

ومن أشهر أنواع التصيد:

- التصيد التقليدي.
- التصيد الموجه.
- تصيد التنفيذيين.
- التصيد عبر الرسائل النصية.

ومن ناحية أخرى، يمكن تقليل مخاطر هذه الهجمات من خلال استخدام المصادقة الثنائية وتدريب الموظفين بشكل دوري.

- **هجمات حجب الخدمة:**

تهدف هذه الهجمات إلى تعطيل المواقع أو الخدمات الرقمية. حيث يتم إرسال عدد كبير من الطلبات إلى الخادم، مما يؤدي إلى توقف الخدمة.

نتيجة لذلك، قد تتعرض المؤسسة لخسائر مالية كبيرة. بالإضافة إلى ذلك، قد تتضرر سمعة الشركة بسبب توقف الخدمات ومن أجل الحماية، يمكن استخدام حلول الحماية السحابية وتوزيع الأحمال على الخوادم.

- **هجمات الرجل في المنتصف:**

تحدث هذه الهجمات عندما يتم اعتراض الاتصال بين المستخدم والخادم. وبالتالي، يمكن للمهاجم سرقة البيانات أو تعديلها، ومن أجل تقليل المخاطر، يجب استخدام بروتوكولات التشفير وشبكات VPN، خاصة عند العمل عن بعد.

[1] حكيمة جاب لله: انعكاسات الجريمة السيبرانية على البيئة الرقمية: دراسة في آليات واستراتيجيات مكافحتها، مجلة حوليات، جامعة الجزائر 1، المجلد 35، العدد 03، 2021، ص 13.

- **هجمات قواعد البيانات:**

تستهدف هذه الهجمات قواعد البيانات من خلال إدخال أوامر خبيثة. ونتيجة لذلك، يمكن للمهاجم الوصول إلى المعلومات الحساسة، وللحماية، يجب استخدام استعلامات آمنة واختبار الأنظمة بشكل دوري.

- **الهندسة الاجتماعية:**

تعتمد هذه الهجمات على خداع الأفراد بدلاً من اختراق الأنظمة. فعلى سبيل المثال، قد يتظاهر المهاجم بأنه موظف في قسم تقنية المعلومات، ولذلك، يعد تدريب الموظفين ورفع مستوى الوعي الأمني من أهم وسائل الحماية.

2. **سرقة البيانات التجارية، بما في ذلك الأسرار التجارية، وقواعد بيانات العملاء، والمعلومات المالية والاستراتيجية:**

في واشنطن 6 أغسطس آب (رويترز) -كشفت بيانات من جوجل وبيانات في مجال استخبارات الإنترنت اطلعت عليها رويترز أن قراصنة إلكترونيون يطلبون فدى ويستخدمون المكالمات الهاتفية لاختراق ضحاياهم استهدفوا عشرات المؤسسات المالية الأمريكية البارزة وغيرها من الشركات خلال الشهر الماضي، وتظهر البيانات أن القراصنة أنشأوا مواقع إلكترونية لسرقة كلمات مرور موظفين بشركات للاستثمار المباشر والخدمات المالية، بما في ذلك بلاكستون وبريدج ووتر أسوسيتس وأبولو جلوبال مانجمنت وباين كابيتال وكيه.كيه.آر وتي.بي.جي وسي.إم.إي جروب وكليرليك كابيتال وموديز، بالإضافة إلى شركات أخرى. [1]

3. **الاحتيال الإلكتروني[2]، من خلال انتحال الهوية أو اختراق الحسابات أو التلاعب بعمليات الدفع والتحويلات المالي.**

4. **التجسس الصناعي الإلكتروني[3]، الهادف إلى الحصول على المعلومات التجارية والتقنية لتحقيق ميزة تنافسية غير مشروعة:**

ويقصد بالتجسس الاقتصادي (يسمى كذلك التجسس الصناعي) سرقة الأسرار التجارية بهدف الحصول على معلومات حساسة لتحقيق ميزة تنافسية ومنفعة تجارية، أو تحطيم الخصم وإرباكه وإلحاق الخسائر به، ويمكن أن يحدث التجسس الاقتصادي من خلال التعاون مع شخص من داخل الشركة أو المؤسسة المراد اختراقها، أو من خلال استغلال الثغرات الأمنية التي عادة ما تكون في الأنظمة المعلوماتية المستخدمة في أعمال الشركات والمؤسسات الاقتصادية.

من أمثلة التجسس الصناعي:

- في تقرير نشر في 2 مارس /آذار 2021، يقول موقع ستراتفور -المعروف باهتمامه بموضوع التجسس وعمل الاستخبارات -إنه اعتباراً من عام 2018، خصصت الصين 72 مليار دولار لتحقيق أهداف خطة "صنع في الصين 2025"، لدعم قطاع صناعة أشباه الموصلات. وبحسب الموقع المذكور، يرتكز جزء من الخطة على توظيف المهندسين التايوانيين، مع تقديم حوافز مالية ومكافآت لمن يجلب تقنيات جديدة من شركات منافسة.
- في عام 2020، فرضت محكمة تايوانية غرامة على "الشركة المتحدة للإلكترونيات الدقيقة" (يو إم سي) (UMC) بمبلغ 36 مليون دولار، بعد أن اتهمتها شركة "ميكرون تكنولوجي (Micron Technology) "الأميركية لصناعة الرقائق بسرقة أسرار تجارية استفادت منها شركة "فوجيان جينهوا (Fujian Jinhua) "المملوكة للحكومة الصينية.[4]

[1] أنظر: https://www.reuters.com/ar/business/EPDZGUPJFBJF3EZQENCCZNRW2I-2026-08-06/
[2] د. بولحية شهيرة /د. سويح دنيا واد، الاحتيال الإلكتروني، مجلة الدراسات القانونية والاقتصادية، العدد 04، 2019، ص 5.
[3] أمثلة
[4] مقال منشور في موقع الجزيرة بتاريخ 2022/08/01، على الرابط:
https://www.aljazeera.net/encyclopedia/2022/8/1/%D8%A7%D9%84%D8%AA%D8%AC%D8%B3%D8%B3-%D8%A7%D9%84%D8%A7%D9%82%D8%AA%D8%B5%D8%A7%D8%AF%D9%8A-%D8%B3%D8%B1%D9%82%D8%A9-%D8%A7%D9%84%D8%A3%D8%B3%D8%B1%D8%A7%D8%B1
تمت الزيارة بتاريخ 2026/08/10، الساعة 19:36

5. اختراق خدمات الحوسبة السحابية وسلاسل التوريد الرقمية[1]، بما يترتب عليه انتقال آثار الهجوم إلى عدد كبير من الشركات والعملاء:

هذا ويُعد من أكبر الهجمات الإلكترونية لعام 2025: [2]

1. برامج الفدية للرعاية الصحية.
2. خرق منصة التأمين.
3. إساءة استخدام هوية SaaS.
4. التعرض للبيانات السحابية.
5. اختراق شبكة الاتصالات.
6. تعطيل الخدمة الحكومية.
7. هجوم الأنظمة المالية.

تكشف هذه المخاطر أن الجرائم السيبرانية أصبحت تمثل أحد أهم مصادر التهديد لبيئة الأعمال الرقمية، لما تلحقه من خسائر مالية، وإضرار بسمعة الشركات، وتعطيل للأنشطة الاقتصادية، وإضعاف للثقة في المعاملات الإلكترونية. لذلك لم يعد دور المشرع يقتصر على تجريم هذه الأفعال، بل أصبح مطالباً بوضع منظومة متكاملة تشمل الوقاية، وإدارة المخاطر، وحماية البيانات، وتعزيز الأمن السيبراني، بما يحقق التوازن بين تشجيع التحول الرقمي وضمان الأمن القانوني لبيئة الأعمال.

الفرع الثاني: الأساس القانوني للمسؤولية عن الجرائم السيبرانية:

سنتناول هذا الفرع من خلال الحديث عن المسؤولية الجنائية عن الجرائم السيبرانية في مجال الأعمال (فقرة أولى)، ثم التعرض للمسؤولية المدنية وغيرها من صور المسؤولية القانونية.

الفقرة الأولى: المسؤولية الجنائية عن الجرائم السيبرانية في مجال الأعمال:

سندرس هذه الفقرة من خلال تحديد مفهوم المسؤولية الجنائية عن الجرائم السيبرانية في مجال الأعمال (أولاً)، ثم التعرض لأركان المسؤولية الجنائية عن الجرائم السيبرانية في مجال الأعمال (ثانياً).

أولاً: مفهوم المسؤولية الجنائية عن الجرائم السيبرانية في مجال الأعمال:

تُعد المسؤولية الجنائية الأثر القانوني المترتب على ارتكاب فعل يجرمه القانون ويستوجب توقيع جزاء جنائي على مرتكبه، وفي مجال الجرائم السيبرانية، تقوم هذه المسؤولية متى ارتكب شخص طبيعي أو اعتباري فعلاً غير مشروع باستخدام الوسائل الرقمية أو استهدف بها الأنظمة المعلوماتية أو البيانات الإلكترونية، وكان من شأن ذلك الإضرار بالمصالح التي يحميها القانون، ولا سيما المصالح الاقتصادية والتجارية، وتكتسب المسؤولية الجنائية في بيئة الأعمال الرقمية أهمية خاصة بالنظر إلى اتساع نطاق الجرائم التي تستهدف الشركات والمؤسسات التجارية، مثل اختراق الأنظمة المعلوماتية، وسرقة الأسرار التجارية، والاحتيال الإلكتروني، والتلاعب بالمعاملات المالية، والاعتداء على قواعد البيانات، والابتزاز الإلكتروني، وهي أفعال تمس الثقة في النشاط الاقتصادي وتؤثر في استقرار السوق، وقد عرفها الأستاذ عبد القادر عودة بأنها: "تحمل الإنسان نتائج أفعاله المحرمة التي يأتيها مختاراً و هو مدرك لمعنيها ونتائجها". [3]

وتقوم المسؤولية الجنائية في هذا المجال على مبدأ شخصية المسؤولية الجنائية، بحيث لا يسأل جنائياً إلا من ثبتت نسبة الفعل الإجرامي إليه وتوافرت في حقه أركان الجريمة وشروط المساءلة، مع اتجاه العديد من التشريعات الحديثة إلى تقرير مسؤولية

[1] https://www.cloudsek.com/ar/knowledge-base/biggest-cyber-attacks
[2] المصدر الرابط التالي: https://www.cloudsek.com/ar/knowledge-base/biggest-cyber-attacks
[3] الخميس ياسمين عبد العزيز إبراهيم، المسؤولية الجنائية للحدث في الجرائم المعلوماتية، رسالة ماجستير، جامعة القصيم، كلية الشريعة والدراسات الإسلامية، السعودية، السنة الدراسية 2016 -2017، ص 12.

الشخص الاعتباري عن بعض الجرائم السيبرانية متى ارتكبت باسمه أو لحسابه بواسطة ممثليه أو أجهزته. [1]

ثانياً: أركان المسؤولية الجنائية عن الجرائم السيبرانية في مجال الأعمال:

تخضع المسؤولية الجنائية في الجرائم السيبرانية للقواعد العامة في القانون الجنائي، مع مراعاة خصوصية الوسائل الرقمية، وتقوم على مجموعة من الأركان الأساسية:

1. **الركن الشرعي:**

ويقصد به وجود نص قانوني يجرم الفعل السيبراني ويقرر له عقوبة، تطبيقا لمبدأ "لا جريمة ولا عقوبة إلا بنص." ويكتسب هذا الركن أهمية خاصة بسبب التطور المستمر للوسائل التقنية، مما يفرض تحديث التشريعات بصورة دورية لاستيعاب الأنماط الإجرامية المستحدثة.

2. **الركن المادي:**

ويتمثل في السلوك الإجرامي المرتكب باستخدام الوسائل الرقمية، سواء كان اختراقاً غير مشروع للأنظمة، أو اعتراضاً للبيانات، أو تزويراً إلكترونياً، أو احتيالاً رقمياً، أو نشر برمجيات خبيثة، مع تحقق النتيجة الإجرامية متى اشترطها القانون. [2]

3. **الركن المعنوي:**

يتمثل في القصد الجنائي، أي اتجاه إرادة الجاني إلى ارتكاب الفعل مع علمه بعدم مشروعيته. وقد يكون القصد عاماً، وقد يتطلب المشرع قصداً خاصاً في بعض الجرائم، كتحقيق منفعة مالية غير مشروعة أو الإضرار بالمنافسين أو الاستيلاء على الأسرار التجارية، هذا ولا تختلف أركان المسؤولية الجنائية في الجرائم السيبرانية من حيث البناء القانوني عن الجرائم التقليدية، غير أن خصوصية الدليل الرقمي، وإمكانية إخفاء هوية الجاني، والطبيعة العابرة للحدود لهذه الجرائم تجعل إثبات هذه الأركان أكثر تعقيداً، وهو ما يستدعي تطوير قواعد الإثبات الإلكتروني وتعزيز قدرات جهات التحقيق والخبرة الفنية.

ثالثاً: خصوصية المسؤولية الجنائية في بيئة الأعمال الرقمية:

تتميز المسؤولية الجنائية في بيئة الأعمال الرقمية بعدة خصائص تميزها عن غيرها من صور المسؤولية، من أهمها:

- اتساع دائرة الأشخاص الذين يمكن أن تثور مسؤوليتهم، لتشمل الأشخاص الطبيعيين والأشخاص الاعتباريين.
- الاعتماد على الأدلة الرقمية في إثبات الجريمة ونسبتها إلى مرتكبها.
- الارتباط الوثيق بالتعاون القضائي الدولي نتيجة للطبيعة العابرة للحدود للجرائم السيبرانية.
- تداخل أحكام القانون الجنائي مع قواعد قانون الأعمال، وقوانين حماية البيانات، والتجارة الإلكترونية، والأمن السيبراني.

تعتبر المسؤولية الجنائية حجر الأساس في مواجهة الجرائم السيبرانية التي تستهدف بيئة الأعمال، إلا أن فعاليتها لا تتوقف على تجريم الأفعال وفرض العقوبات فحسب، بل تتطلب منظومة قانونية متكاملة تشمل الوقاية، والإثبات الإلكتروني، والتعاون الدولي، وتحقيق التوازن بين حماية الاقتصاد الرقمي وتشجيع الاستثمار والابتكار. ومن هذا المنطلق، أصبحت السياسة الجنائية الحديثة تتجه إلى اعتماد مقاربة شاملة تتجاوز العقاب التقليدي، لتشمل تعزيز الامتثال الرقمي وإدارة المخاطر داخل

1 الجرائم الإلكترونية. أركانها وأسبابها ودوافع ارتكابها، بحث منشور على الرابط: https://www.rakpolice.gov.ae/MediaCenter/Details/38?uid=8e64919f1fc44c09acae4685d94b9cde

2 ما هي الجرائم في الأمن السيبراني، بحث منشور على الرابط: https://training.alkhaleej.com.sa/%D9%85%D8%A7-%D9%87%D9%8A-%D8%A7%D9%84%D8%AC%D8%B1%D8%A7%D8%A6%D9%85-%D9%81%D9%8A-%D8%A7%D9%84%D8%A3%D9%85%D9%86-%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A%D8%9F/

الشركات، بما يكفل حماية أكثر فاعلية لبيئة الأعمال الرقمية. [1]

الفقرة الثانية: المسؤولية المدنية وغيرها من صور المسؤولية القانونية:

سنتناول هذه الفقرة من خلال الحديث عن المسؤولية المدنية عن الجرائم السيبرانية في مجال الأعمال (أولاً)، ثم الحديث عن المسؤولية التأديبية والتنظيمية عن الجرائم السيبرانية (ثانياً).

أولاً: المسؤولية المدنية عن الجرائم السيبرانية في مجال الأعمال:

لا يقتصر أثر الجرائم السيبرانية على قيام المسؤولية الجنائية، بل قد يترتب عليها كذلك مسؤولية مدنية، تهدف إلى جبر الضرر الذي أصاب المضرور وإعادة التوازن إلى المراكز القانونية المتضررة، فبينما ترمي المسؤولية الجنائية إلى حماية النظام العام من خلال توقيع العقوبة على الجاني، تستهدف المسؤولية المدنية تعويض الأضرار التي تلحق بالأشخاص أو الشركات نتيجة الاعتداء على حقوقهم أو مصالحهم المشروعة[2]، وتعرف المسؤولية المدنية بأنها: "التزام المدين بتعويض الضرر الذي ترتب على إخلاله بالتزام يقع عليه." [3]

وفي بيئة الأعمال الرقمية، تتجسد المسؤولية المدنية في حالات متعددة، كاختراق الأنظمة المعلوماتية للشركات، أو سرقة البيانات التجارية، أو إفشاء الأسرار المهنية، أو تعطيل المنصات الإلكترونية، أو الاعتداء على حقوق الملكية الفكرية، أو الإخلال بالتزامات حماية البيانات. وقد تؤدي هذه الأفعال إلى خسائر مالية مباشرة، وفقدان العملاء، والإضرار بسمعة المؤسسة، وتعطيل نشاطها الاقتصادي، الأمر الذي يبرر مطالبة المسؤول بالتعويض.

وتقوم المسؤولية المدنية، بحسب الأحوال، على المسؤولية التقصيرية إذا نشأ الضرر عن فعل غير مشروع لا تربط أطرافه علاقة تعاقدية، كما قد تقوم على المسؤولية العقدية إذا كان مصدر الضرر إخلال أحد المتعاقدين بالتزاماته المتعلقة بأمن المعلومات أو سرية البيانات أو تنفيذ الخدمات الرقمية وفقاً للعقد.

ثانياً: المسؤولية التأديبية والتنظيمية عن الجرائم السيبرانية:

إلى جانب المسؤوليتين الجنائية والمدنية، قد تترتب عن الجرائم السيبرانية مسؤولية تأديبية أو تنظيمية، بحسب صفة مرتكب الفعل وطبيعة الالتزامات الملقاة على عاتقه.

أ. المسؤولية التأديبية:

تقوم المسؤولية التأديبية عندما يرتكب العامل أو الموظف أو المدير مخالفة لواجباته الوظيفية أو المهنية باستعمال الوسائل الرقمية، كالإفصاح غير المشروع عن البيانات السرية، أو إساءة استخدام الأنظمة المعلوماتية، أو مخالفة سياسات الأمن السيبراني المعتمدة داخل المؤسسة. ويترتب على ذلك توقيع جزاءات تأديبية تتدرج من الإنذار والخصم من الراتب إلى الفصل من العمل، دون أن يمنع ذلك من مساءلته مدنياً أو جنائياً إذا توافرت شروطها.

هذا وتمثل المسؤولية التأديبية وسيلة وقائية داخل المؤسسات، إذ تسهم في تعزيز ثقافة الامتثال الرقمي، وإلزام العاملين باحترام قواعد الأمن السيبراني، والحد من المخاطر الناشئة عن الأخطاء البشرية، التي تعد من أبرز أسباب الاختراقات الإلكترونية.

ب. المسؤولية التنظيمية:

تظهر المسؤولية التنظيمية في مواجهة الشركات ومقدمي الخدمات الرقمية الذين يخلون بالالتزامات القانونية المفروضة عليهم، كواجبات حماية البيانات، وتأمين الأنظمة المعلوماتية، والإبلاغ عن الحوادث السيبرانية، والامتثال للمتطلبات التنظيمية التي تفرضها السلطات المختصة. ويترتب على هذه المخالفات جزاءات إدارية وتنظيمية، مثل الغرامات، أو تعليق النشاط، أو سحب الترخيص، أو إلزام المخالف باتخاذ تدابير تصحيحية.

[1] عادل عبدالعال إبراهيم خراشي. الحماية الجنائية للحق في الخصوصية الرقمية. ط 1. القاهرة: شركة ناس للطباعة، 2015، ص 47-
[2] شيرين حميد علي الجاف. الانتهاك الجرمي لحق الخصوصية باستخدام وسائل التصوير والاتصالات المستحدثة، رسالة ماجستير، كلية القانون والعلوم السياسية. جامعة كركوك، 2019، ص 33.
[3] الصدة، عبد المنعم فرج، مصادر الالتزام. بيروت: دار النهضة العربية، 1979، من دون ذكر الطبعة، ص512.

هذا وتعكس المسؤولية التنظيمية التحول من الاكتفاء برد الفعل بعد وقوع الجريمة إلى تبني سياسة وقائية تقوم على إدارة المخاطر الرقمية وإلزام المؤسسات بتطبيق معايير الحوكمة والأمن السيبراني،[1] وقد أخذت التشريعات المقارنة بهذا الاتجاه، إدراكاً منها أن حماية بيئة الأعمال الرقمية لا تتحقق بالعقوبات الجنائية وحدها، بل تتطلب منظومة متكاملة من الالتزامات التنظيمية والرقابية.

المطلب الثاني: صور المسؤولية القانونية وآليات حماية بيئة الأعمال الرقمية

سنتناول هذا المطلب من خلال تحديد الصور المسؤولية القانونية الناشئة عن الجرائم السيبرانية (فرع أول)، ثم معرفة آليات تعزيز الحماية القانونية لبيئة الأعمال الرقمية (فرع ثاني).

الفرع الأول: صور المسؤولية القانونية الناشئة عن الجرائم السيبرانية:

سندرس هذا الفرع من خلال تحديد مسؤولية الأشخاص الطبيعيين عن الجرائم السيبرانية في بيئة الأعمال الرقمية (فقرة أولى)، ثم نحدد مسؤولية الأشخاص الاعتباريين ومقدمي الخدمات الرقمية والشركات (فقرة ثانية).

الفقرة الأولى: مسؤولية الأشخاص الطبيعيين عن الجرائم السيبرانية في بيئة الأعمال الرقمية:

لدراسة هذه الفقرة سنحدد أساس مسؤولية الأشخاص الطبيعيين (أولاً)، ثم نستعرض صورها (ثانياً).

أولاً: أساس مسؤولية الأشخاص الطبيعيين:

تقوم مسؤولية الأشخاص الطبيعيين عن الجرائم السيبرانية في بيئة الأعمال الرقمية على القواعد العامة للمساءلة القانونية، ومقتضاها أن كل شخص يرتكب فعلاً غير مشروع باستخدام الوسائل الرقمية، أو يسهم في ارتكابه، يكون مسؤولاً عن الآثار القانونية المترتبة على ذلك متى توافرت أركان المسؤولية وشروطها، حيث نصت المادة 97 من قانون الالتزامات والعقود الموريتاني على أن: "كل فعل ارتكبه الإنسان عن بينة واختيار من غير أن يسمح له به القانون، فأحدث ضرراً مادي أو معنوياً للغير، التزم مرتكبه بتعويض هذا الضرر إذا ثبت أن ذلك الفعل هو السبب المباشر في حصول الضرر"،[2] ويشمل ذلك المسير، والموظف، والمستخدم، والمتعامل الإلكتروني[3]، دون تمييز، متى ثبتت نسبة الفعل إليه.

وتتخذ هذه المسؤولية صوراً متعددة بحسب طبيعة الفعل المرتكب، فقد تكون مسؤولية جنائية إذا انطوى السلوك على جريمة معاقب عليها قانوناً، أو مسؤولية مدنية إذا ترتب عليه ضرر يستوجب التعويض، أو مسؤولية تأديبية إذا أخل الشخص بالالتزامات الوظيفية أو المهنية المفروضة عليه.

تكمن خصوصية مسؤولية الأشخاص الطبيعيين في بيئة الأعمال الرقمية في أن مصدر الخطر لم يعد يقتصر على الهجمات الخارجية، بل أصبح يشمل كذلك الأفعال الصادرة من داخل المؤسسة. ولذلك فإن المشرع لا يكتفي بتجريم الاعتداءات الإلكترونية، وإنما يسعى إلى إرساء منظومة للمساءلة تشمل كل من يخل بواجبات المحافظة على أمن المعلومات وسلامة الأنظمة الرقمية.

ثانياً: صور مسؤولية الأشخاص الطبيعيين:

أ. مسؤولية المسير:

المسير هو الشخص الذي يعهد إليه الشركاء أو المساهمون بمهمة إدارة الشركة وتحقيق غرضها الاجتماعي، سواء كان ذلك بصفة منفردة أو ضمن هيئة جماعية كمجلس الإدارة أو مجلس المديرين، ويمكن أن يكون المسير من الشركاء أو من الغير، يعين المسير إما في النظام الأساسي نفسه وبموجب عقد لاحق، ويحدد النظام الأساسي مدة التسيير التي يمكن أن تكون محددة أو غير محددة.

---

[1] شيرين حميد علي الجاف. الانتهاك الجرمي لحق الخصوصية باستخدام وسائل التصوير والاتصالات المستحدثة، رسالة ماجستير، كلية القانون والعلوم السياسية. جامعة كركوك، 2019، ص 35.

[2] المادة 97 من الأمر القانوني رقم 89-126 الصادر بتاريخ 14 سبتمبر 1989 المتضمن قانون الالتزامات والعقود الموريتاني المعدل بالقانون رقم 2001-31 الصادر بتاريخ 7 فبراير 2001.

[3] سوزان عدنان. "انتهاك حرمة الحياة الخاصة عبر الإنترنت". مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، 2013، مجلد (29). عدد (3).

ويعرف في ظل قانون الشركات بأنه ذلك الشخص الذي يمارس سلطة داخل هيكل منظم والمتمثل في الشركة وهو المخول للتصرف باسمها ولحسابها، ويمنح لذلك سلطات واسعة في الإدارة والتمثيل تحقيقا لمصلحة الشركة. [1]

وقد ميز القانوني المغربي رقم 5-96[2] بين حسب كون المسير شريكاً أو غير شريك، فالمسير الشريك يجمع بين صيفتين: صفة المدير وصفة الشريك يشارك في القرارات الجماعية ويمتلك حصصاً اجتماعية، أما المسير غير الشريك فهو شخص من الغير لا يملك أي حصة اجتماعية في الشركة، يمارس مهام التسيير فقط دون المشاركة في رأس المال، لا يملك حق التصويت في الجمعيات، لكن صلاحيته في التسيير تجاه الغير تبقي مطابقة لصلاحيات المسير الشريك.

ويُعد المسير المسؤول الأول عن إدارة الشركة وضمان سلامة أنظمتها المعلوماتية، ولذلك قد تثور مسؤوليته إذا استغل سلطاته لارتكاب جرائم سيبرانية، كالتلاعب بالبيانات المالية، أو الاستيلاء على المعلومات السرية، أو توجيه العاملين إلى ارتكاب أفعال غير مشروعة، أو إهمال اتخاذ التدابير اللازمة لحماية الأنظمة المعلوماتية متى كان هذا الإهمال مؤثراً في وقوع الجريمة وفقاً لما يقرره القانون، وقد عرف القانون الموريتاني جريمة إساءة استعمال أموال الشركة وفقاً للمادة 688 من مدونة التجارة بأنها: "تعمد المسيرين استعمال أموال أو ائتمان الشركة أو السلطة المخولة لهم، بشكل يتعارض مع المصالح الاقتصادية للشركة، بغية تحقيق أغراض شخصية أو تفضيل مؤسسة أخرى لهم فيها مصالح". [3]

هذا ولا تقتصر مسؤولية المسير على الأفعال الإيجابية، بل قد تمتد إلى حالات التقصير في تطبيق قواعد الحوكمة الرقمية وإدارة المخاطر السيبرانية، لكونه المسؤول عن وضع السياسات الكفيلة بحماية أصول الشركة الرقمية. [4]

ب. مسؤولية الموظف:

تقوم مسؤولية الموظف عندما يستغل صلاحياته الوظيفية للاعتداء على الأنظمة أو البيانات أو الأسرار التجارية، أو عندما يتجاوز حدود الترخيص الممنوح له بالدخول إلى النظام المعلوماتي، أو يقوم بنسخ البيانات أو تعديلها أو حذفها دون سند قانوني.

تشير الممارسات العملية إلى أن جزءاً مهما من الحوادث السيبرانية يرتبط بالمستخدمين الداخليين، سواء بسبب سوء النية أو الإهمال، وهو ما يفرض على المؤسسات اعتماد سياسات صارمة للتحكم في الصلاحيات والتدريب المستمر على الأمن السيبراني.

ت. مسؤولية المستخدم:

يقصد بالمستخدم كل شخص يستعمل النظام المعلوماتي أو المنصة الرقمية، سواء كان عاملاً داخل المؤسسة أو مستفيداً من خدماتها. وتقوم مسؤوليته إذا استعمل الوسائل الرقمية بصورة غير مشروعة، كاختراق الحسابات، أو نشر البرمجيات الخبيثة، أو تزوير البيانات، أو التحايل على أنظمة الدفع الإلكتروني.

ترتبط مسؤولية المستخدم بمبدأ الاستعمال المشروع للأنظمة الرقمية، فلا يكفي مجرد استعمال الوسيلة التقنية، وإنما يجب أن يكون هذا الاستعمال في الحدود التي يسمح بها القانون أو العقد أو الترخيص الممنوح له.

ث. مسؤولية المتعامل الإلكتروني:

يقصد بالمتعامل الإلكتروني كل شخص يرتبط بالشركة بعلاقة قانونية تتم عبر الوسائط الرقمية، كالمورد، أو العميل، أو الشريك التجاري، أو مقدم الخدمة، وتنشأ مسؤوليته إذا استغل العلاقة التعاقدية لارتكاب أفعال سيبرانية غير مشروعة، كالغش الإلكتروني، أو انتحال الهوية، أو تزوير المحررات الإلكترونية، أو اختراق المنصات الرقمية للحصول على مزايا غير مستحقة.

---

[1] شباتي نضيرة، هوية المسير في ظل الشركة التجارية، مجلة الندوة للدراسات القانونية، العدد الأول، 2013، ص 288.

[2] القانون المتعلق بشركة التضامن وشركة التوصية البسيطة وشركة التوصية بالأسهم وشركة الأسهم المبسطة والشركة ذات المسؤولية المحدودة وشركة المحاصة.

[3] المادة 688 من مدونة التجارة الموريتانية الصادرة 18/01/2000 بمقتضى القانون رقم: 2000/05.

[4] أحمد عبدين، مسؤولية المسير في الشركة التجارية، مذكرة لنيل شهادة ماستر أكاديمي، جامعة قاصيدي مرباح، كلية الحقوق والعلوم السياسية، السنة الجامعية 2015/2014، ص 23.

تتميز مسؤولية المتعامل الإلكتروني بأنها غالباً ما تجمع بين المسؤولية العقدية والمسؤولية التقصيرية، وقد تمتد إلى المسؤولية الجنائية إذا توافرت أركان الجريمة. ويبرز ذلك أهمية تضمين العقود الإلكترونية بنوداً تتعلق بالأمن السيبراني، وحماية البيانات، والالتزام بالإفصاح عن الحوادث الإلكترونية، بما يعزز الثقة في المعاملات الرقمية.

يتبين مما سبق أن مسؤولية الأشخاص الطبيعيين في بيئة الأعمال الرقمية تتسم بتعدد صورها وتنوع الأساس القانوني الذي تقوم عليه، تبعاً لاختلاف صفة الشخص ودوره في النشاط الاقتصادي. كما أن التطور التقني واتساع نطاق المعاملات الإلكترونية أوجبا توسيع مفهوم المسؤولية ليشمل ليس فقط مرتكب الفعل الإجرامي، وإنما أيضاً كل من يخل بالالتزامات القانونية أو المهنية التي تهدف إلى حماية الأنظمة المعلوماتية والبيانات التجارية، بما يسهم في تحقيق أمن بيئة الأعمال الرقمية واستقرارها.

الفقرة الثانية: مسؤولية الأشخاص الاعتباريين ومقدمي الخدمات الرقمية والشركات:

سندرس هذا الفقرة من خلال تحديد مسؤولية الأشخاص الاعتباريين عن الجرائم السيبرانية (أولاً)، ثم تحديد مسؤولية، ثم مقدمي الخدمات الرقمية (ثانياً)، وتحديد مسؤولية الشركات في حماية بيئة الأعمال الرقمية (ثالثاً).

أولاً: مسؤولية الأشخاص الاعتباريين عن الجرائم السيبرانية:

أصبحت مسؤولية الأشخاص الاعتباريين من المبادئ الراسخة في السياسة التشريعية الحديثة، ولا سيما في مجال الجرائم الاقتصادية والسيبرانية، إذ لم يعد النشاط الإجرامي يقتصر على الأفراد، بل قد يرتبط بالهيكل التنظيمي للشركة أو بالمصالح التي تسعى إلى تحقيقها. ومن ثم، أخذت العديد من التشريعات بمبدأ مساءلة الشخص الاعتباري متى ارتكبت الجريمة باسمه أو لحسابه بواسطة أحد أجهزته أو ممثليه أو القائمين على إدارته، دون أن يخل ذلك بمساءلة الشخص الطبيعي الذي ارتكب الفعل.

وتقوم مسؤولية الشخص الاعتباري في بيئة الأعمال الرقمية عندما يثبت أن الجريمة السيبرانية كانت نتيجة قرار صادر عن الإدارة، أو بسبب تقصير في وضع أنظمة الحماية الرقمية، أو نتيجة الإخلال بالالتزامات القانونية المتعلقة بحماية البيانات وأمن المعلومات. كما قد تنشأ المسؤولية عن الامتناع عن اتخاذ التدابير الوقائية اللازمة، إذا كان هذا الامتناع سبباً في وقوع الجريمة أو تفاقم آثارها.

وتختلف الجزاءات المقررة في مواجهة الأشخاص الاعتباريين باختلاف التشريعات، فقد تشمل الغرامات المالية، والمصادرة، وإغلاق المنشأة مؤقتاً، أو وقف بعض الأنشطة، أو الحرمان من مزاولة نشاط معين، أو نشر الحكم القضائي، وذلك بحسب جسامة الجريمة وآثارها.[1]

يمثل إقرار مسؤولية الشخص الاعتباري تحولاً مهماً في السياسة الجنائية المعاصرة، إذ لم تعد الحماية القانونية تقتصر على معاقبة الجاني الفرد، بل امتدت إلى مساءلة الكيان الاقتصادي الذي استفاد من الجريمة أو قصر في منعها. ويؤدي ذلك إلى تعزيز ثقافة الامتثال داخل الشركات، ودفعها إلى الاستثمار في نظم الأمن السيبراني والحوكمة الرقمية.

ثانياً: مسؤولية مقدمي الخدمات الرقمية:

يؤدي مقدمو الخدمات الرقمية دوراً محورياً في الاقتصاد الرقمي، سواء تعلق الأمر بمقدمي خدمات الاستضافة، أو الحوسبة السحابية، أو منصات التجارة الإلكترونية، أو خدمات الدفع الإلكتروني، أو مزودي خدمات الاتصالات والوساطة الرقمية. ويترتب على هذا الدور التزامات قانونية تتمثل في توفير بيئة رقمية آمنة، وحماية البيانات، واتخاذ التدابير الفنية والتنظيمية اللازمة للحد من المخاطر السيبرانية.

وتثور مسؤولية مقدمي الخدمات الرقمية إذا أخلوا بهذه الالتزامات، كالإهمال في تأمين الأنظمة، أو التقصير في حماية البيانات، أو عدم الاستجابة للحوادث السيبرانية، أو مخالفة الالتزامات القانونية المتعلقة بالإبلاغ عن الاختراقات، متى ترتب على ذلك ضرر للمتعاملين أو للشركات المستفيدة من خدماتهم.

ولا تقوم هذه المسؤولية بمجرد وقوع الهجوم السيبراني، وإنما تتطلب إثبات وجود إخلال بواجب قانوني أو تعاقدي كان من شأن الالتزام به الحد من وقوع الضرر أو التخفيف من آثاره.

[1] شيرين حميد علي الجاف. الانتهاك الجرمي لحق الخصوصية باستخدام وسائل التصوير والاتصالات المستحدثة، مرجع سابق، ص 40.

تتجه التشريعات الحديثة إلى عدم تحميل مقدمي الخدمات الرقمية مسؤولية مطلقة عن جميع الجرائم التي تقع عبر منصاتهم، وإنما تربط المسؤولية بمدى التزامهم بواجبات العناية واليقظة والامتثال للمتطلبات القانونية، تحقيقاً للتوازن بين حماية بيئة الأعمال الرقمية وعدم عرقلة الابتكار والاستثمار في الخدمات الرقمية.

ثالثاً: مسؤولية الشركات في حماية بيئة الأعمال الرقمية:

لا تقتصر مسؤولية الشركات على الامتناع عن ارتكاب الجرائم السيبرانية، بل تمتد إلى الالتزام بتوفير بيئة رقمية آمنة للعاملين والمتعاملين معها. ويقتضي ذلك اعتماد سياسات فعالة للأمن السيبراني، وحماية قواعد البيانات، وإدارة المخاطر الرقمية، وتدريب العاملين، ووضع خطط للاستجابة للحوادث الإلكترونية واستمرارية الأعمال.

وقد تثور مسؤولية الشركة إذا ثبت تقصيرها في الوفاء بهذه الالتزامات، وكان هذا التقصير سبباً في وقوع الهجمات السيبرانية أو في اتساع نطاق الأضرار الناتجة عنها. كما قد تتحمل المسؤولية عن الأفعال غير المشروعة التي يرتكبها العاملون لديها أثناء أداء وظائفهم أو بسببها، وفقاً للقواعد التي يقررها كل تشريع.

لم تعد مسؤولية الشركات في البيئة الرقمية مسؤولية لاحقة لوقوع الجريمة فحسب، بل أصبحت مسؤولية وقائية تقوم على إدارة المخاطر والامتثال لمتطلبات الأمن السيبراني. ويعكس هذا الاتجاه تطور مفهوم المسؤولية في قانون الأعمال، بحيث أصبح نجاح الشركة يقاس أيضاً بقدرتها على حماية أصولها الرقمية وبياناتها التجارية والمحافظة على ثقة المتعاملين معها. [1]

تكشف التطبيقات العملية للمسؤولية القانونية أن حماية بيئة الأعمال الرقمية لم تعد مسؤولية الأفراد وحدهم، وإنما أصبحت مسؤولية مشتركة تشمل الأشخاص الاعتباريين، ومقدمي الخدمات الرقمية، والشركات. ويحقق هذا التوسع في نطاق المساءلة حماية أكثر فعالية للمصالح الاقتصادية، ويعزز الثقة في المعاملات الإلكترونية، كما يسهم في ترسيخ مبادئ الحوكمة الرقمية والامتثال القانوني، بما يتلاءم مع متطلبات الاقتصاد الرقمي والتشريعات المقارنة الحديثة.

الفرع الثاني: آليات تعزيز الحماية القانونية لبيئة الأعمال الرقمية:

سنتناول هذا الفرع من خلال معرفة الآليات التشريعية والقضائية لمواجهة الجرائم السيبرانية (فقرة أولى)، ثم معرفة التدابير الوقائية والتنظيمية لتعزيز الأمن السيبراني في بيئة الأعمال (فقرة ثانية).

الفقرة الأولى: الآليات التشريعية والقضائية لمواجهة الجرائم السيبرانية:

أولاً: تطوير المنظومة التشريعية لمواجهة الجرائم السيبرانية:

يشكل الإطار التشريعي الركيزة الأساسية لحماية بيئة الأعمال الرقمية، إذ لا يمكن مواجهة الجرائم السيبرانية بفعالية في ظل نصوص قانونية تقليدية لا تستوعب طبيعة الجرائم الرقمية وأساليب ارتكابها، ولذلك اتجهت معظم التشريعات الحديثة إلى إصدار قوانين خاصة بمكافحة الجرائم السيبرانية، وتنظيم المعاملات الإلكترونية، وحماية البيانات الشخصية، إلى جانب تحديث قواعد قانون العقوبات وقانون الإجراءات الجنائية بما يتلاءم مع خصوصية الأدلة الرقمية.

كما يقتضي تعزيز الحماية القانونية مراجعة النصوص التشريعية بصورة دورية لمواكبة التطور التقني، وإقرار قواعد واضحة بشأن مسؤولية الأشخاص الطبيعيين والأشخاص الاعتباريين، وتنظيم الالتزامات القانونية لمقدمي الخدمات الرقمية، فضلاً عن وضع عقوبات تتناسب مع جسامة الأضرار الاقتصادية الناجمة عن الجرائم السيبرانية.

إن فعالية الحماية القانونية لا تقاس بوجود نصوص عقابية فحسب، وإنما بقدرتها على مواكبة التطورات التقنية وتوفير اليقين القانوني للمتعاملين في البيئة الرقمية. ومن ثم، فإن تحديث التشريعات بصورة مستمرة يعد شرطاً أساسياً لتعزيز الأمن القانوني وتشجيع الاستثمار في الاقتصاد الرقمي.

ثانياً: تعزيز فعالية الأجهزة القضائية وآليات التعاون الدولي:

تتسم الجرائم السيبرانية بطبيعة عابرة للحدود، الأمر الذي يجعل مكافحتها تتجاوز نطاق الاختصاص الوطني، ولذلك أصبح من الضروري تطوير قدرات الجهات القضائية وأجهزة إنفاذ القانون في مجال التحريات الرقمية، وجمع الأدلة الإلكترونية،

[1] أحمد عبدين، مسؤولية المسير في الشركة التجارية، مرجع سابق، ص 27.

والاستعانة بالخبرة الفنية في التحقيق والمحاكمة.

ويأخذ التعاون الدولي القضائي عدة صور من أهمها:

- المساعدة القضائية المتبادلة، حيث نصت المادة 18 من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة[1] على وجوب تقديم المساعدة القضائية بين الدول الأعضاء.
- تبادل المعلومات.
- الإنابة القضائية.
- التحقيقات المشتركة ونذكر على سبيل المثال عملية "ECC Sky" عام 2021، حيث تم إطلاق تحقيق مشترك بين الشرطة الفيدرالية البلجيكية وفرنسا وهولندا في قضية الاتجار بالمخدرات باستخدام تطبيق[2] ECC Sky.
- تسليم المجرمين. [3]

الفقرة الثانية: التدابير الوقائية والتنظيمية لتعزيز الأمن السيبراني في بيئة الأعمال:

أولاً: التدابير الوقائية داخل المؤسسات:

لم تعد الحماية القانونية لبيئة الأعمال الرقمية تقوم على الجزاء اللاحق لوقوع الجريمة فحسب، وإنما أصبحت تعتمد بصورة متزايدة على التدابير الوقائية التي تحد من احتمالية وقوع الهجمات السيبرانية. وتشمل هذه التدابير اعتماد سياسات الأمن السيبراني، وإجراء تقييم دوري للمخاطر، وتحديث أنظمة الحماية، وتشفير البيانات، وإدارة صلاحيات الوصول، وإنشاء خطط للاستجابة للحوادث الإلكترونية واستمرارية الأعمال.

كما يندرج ضمن التدابير الوقائية نشر الوعي بالأمن السيبراني بين العاملين، وتدريبهم على كيفية التعامل مع التهديدات الإلكترونية، باعتبار أن العنصر البشري يمثل أحد أهم أسباب الاختراقات السيبرانية.

تُعد الوقاية أقل تكلفة وأكثر فعالية من الاقتصار على المعالجة اللاحقة للجريمة، إذ إن بناء منظومة داخلية متكاملة لإدارة المخاطر يسهم في حماية الأصول الرقمية، ويعزز ثقة المستثمرين والعملاء، ويحد من المسؤولية القانونية التي قد تترتب على تقصير الشركة في اتخاذ التدابير اللازمة.

ثانياً: الحوكمة الرقمية والامتثال القانوني:

أصبحت الحوكمة الرقمية من أهم الوسائل الحديثة لتعزيز حماية بيئة الأعمال، إذ تقوم على وضع إطار مؤسسي يحدد المسؤوليات، ويضمن الامتثال للتشريعات المنظمة للأمن السيبراني وحماية البيانات وإدارة المخاطر الرقمية، ويقتضي ذلك تعيين مسؤولين عن الأمن السيبراني، ووضع سياسات واضحة لحماية البيانات، وإجراء مراجعات دورية لمدى الامتثال، واعتماد معايير دولية لإدارة أمن المعلومات، بما يحقق التوازن بين استغلال التقنيات الرقمية وحماية الحقوق والمصالح الاقتصادية.

وتمثل الحوكمة الرقمية تحولاً من مفهوم الحماية التقليدية إلى مفهوم الإدارة الاستباقية للمخاطر، حيث تصبح مسؤولية حماية البيئة الرقمية جزءاً من استراتيجية المؤسسة، وليس مجرد التزام قانوني يفرضه المشرع. ويؤدي هذا النهج إلى تعزيز تنافسية الشركات، والحد من المنازعات، وتحقيق الاستقرار في المعاملات التجارية الرقمية. [4]

---

[1] المادة 18 من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة "تقدم الدول الأطراف بعضها لبعض أكبر قدر من المساعدة القانونية المتبادلة في التحقيقات ..."

[2] ايمان بن عثمان/ليلي بن بغيلة، التعاون القضائي الدولي ركيزة أساسية لتحقيق العدالة الجنائية الدولية، مجلة الشهاب، المجلد 11، العدد 01، السنة 2025، ص 07

[3] سليمان عبد المنعم، الجوانب الشكلية في النظام القانوني لتسليم المجرمين، دار الجامعة الجديدة للنشر، الإسكندرية، 2007، ص 08

[4] أحمد عودة سليمان الردادي، الحوكمة الرقمية وأثرها على القطاع العام، المدلة الدولية للبحوث والدراسات القانونية، المجلد 5، العدد 5، السنة 2026، ص 5.

مما سبق يتبين أن تعزيز الحماية القانونية لبيئة الأعمال الرقمية لا يتحقق من خلال التجريم والعقاب وحدهما، وإنما يتطلب منظومة متكاملة تجمع بين التحديث التشريعي، وتطوير القضاء الرقمي، وتعزيز التعاون الدولي، وترسيخ الحوكمة الرقمية، واعتماد التدابير الوقائية داخل المؤسسات. ويعكس هذا التكامل الاتجاه الحديث في التشريعات المقارنة، الذي يقوم على المزج بين الردع القانوني والوقاية التقنية، بما يضمن حماية فعالة ومستدامة لبيئة الأعمال الرقمية في مواجهة الجرائم السيبرانية.

الفقرة الأولى: التدابير التشريعية والقضائية والوقائية في التشريعات المقارنة:

أولاً: التدابير التشريعية في التشريعات المقارنة:

اتجهت التشريعات المقارنة إلى تطوير أطر قانونية متخصصة لمواجهة الجرائم السيبرانية، إدراكاً منها لعدم كفاية النصوص الجنائية التقليدية في حماية بيئة الأعمال الرقمية، لذلك اعتمد العديد من الدول قوانين خاصة تجرم الاعتداء على الأنظمة المعلوماتية والبيانات الإلكترونية، وتنظم المعاملات الإلكترونية، وتحمي البيانات الشخصية، مع تحديث قوانين العقوبات والإجراءات الجنائية بما يتلاءم مع طبيعة الجرائم الرقمية.

وفي هذا سياق نذكر بعض التشريعات المقارنة فضلاً عن المشرع الموريتاني الذي خصصت له فقرة خاص به:

1. **أبرز القوانين المؤطرة في التشريع المغربي:** [1]

- القانون رقم 07.03: يُعد القانون الأساسي المدمج في المجموعة الجنائية، حيث يجرّم الولوج غير المشروع إلى نظم المعالجة الآلية للمعطيات، وتعطيلها، وتخريب أو تغيير بياناتها (الفصول 607-3 إلى 607-7).
- القانون رقم 09-08: يتعلق بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي، ويؤطر سرية البيانات ويراقبها عبر اللجنة الوطنية لمراقبة حماية المعطيات ذات الطابع الشخصي.
- القانون رقم 05.20: خاص بالأمن السيبراني، يضع إطاراً لحماية نظم المعلومات الخاصة بالجهات الحكومية والبنيات التحتية الحيوية، ويحدد استراتيجيات التصدي للهجمات الإلكترونية.
- القانون رقم 53.05: خاص بالتبادل الإلكتروني للمعطيات القانونية، ويضع قواعد للتعاملات الرقمية والإثبات الإلكتروني.
- قوانين مكملة: قانون مكافحة الإرهاب (رقم 03.03) فيما يخص الإرهاب السيبراني، وقانون الصحافة والنشر بالنسبة لجرائم التشهير ونشر الأخبار الزائفة عبر الوسائط الرقمية.

2. **أبرز القوانين المؤطرة في التشريع الجزائري:** [2]

- قانون العقوبات الجزائري: تم تعديله بعدة قوانين (مثل القانون 04-15 والقانون 09-04) لتجريم الدخول والبقاء غير المشروع في أنظمة المعالجة الآلية للمعطيات، والتلاعب بالبيانات أو تعطيلها.
- القانون رقم 09-04: يتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ويضع قواعد للإصغاء والمراقبة الإلكترونية وتفتيش وحجز المنظومات الرقمية.

[1] المعهد الملكي للدراسات الاستراتيجية، نظم يوم 13 مارس 2025، ندوة خصصت لعرض ومناقشة كتاب بعنوان: "الجوانب القانونية للجريمة السيبرانية والأمن السيبراني في المغرب" لمؤلفه الاستاذ رضوان مرابط. طالع الرابط:
https://www.ires.ma/ar/%D9%85%D9%86%D8%AA%D8%AF%D9%8A%D8%A7%D8%AA/%D8%AA%D9%82%D8%AF%D9%8A%D9%85-%D8%A7%D9%84%D9%83%D8%AA%D8%A8/%D8%B9%D8%B1%D8%B6-%D9%88%D9%85%D9%86%D8%A7%D9%82%D8%B4%D8%A9-%D9%83%D8%AA%D8%A7%D8%A8-%E2%80%9C%D8%A7%D9%84%D8%AC%D9%88%D8%A7%D9%86%D8%A8-%D8%A7%D9%84%D9%82%D8%A7%D9%86%D9%88%D9%86%D9%8A%D8%A9-%D9%84%D9%84%D8%AC%D8%B1%D9%8A%D9%85%D8%A9-%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A%D8%A9-%D9%88%D8%A7%D9%84%D8%A3%D9%85%D9%86-%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A-%D9%81%D9%8A-%D8%A7%D9%84%D9%85%D8%BA%D8%B1%D8%A8%E2%80%9D

[2] مهد رضا، الجرائم السيبرانية وآليات مكافحتها في التشريع الجزائري، مجلة ايليزا للبحوث والدراسات، المجلد 06، العدد 02، 2021، ص 7.

- القانون رقم 18-04: مؤرخ في 10 مايو 2018، خاص بالبريد والاتصالات الإلكترونية ويتضمن أحكاماً لتعزيز الأمن السيبراني.
- القانون رقم 18-07: مؤرخ في 10 يونيو 2018، مخصص لحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الصِفة الشخصية.

3. أبرز القوانين المؤطرة في التشريع التونسي:

تستند القوانين التونسية المتعلقة بالجريمة السيبرانية بشكل أساسي إلى المرسوم عدد 54 لسنة 2022[1] المتعلق بمكافحة الجرائم المتصلة بأنظمة المعلومات والاتصال، إلى جانب نصوص قانونية أخرى مثل مرسوم السلامة السيبرانية (عدد 17 لسنة 2023) والانضمام إلى اتفاقية بودابست في العام 2024.

كما اتجهت هذه التشريعات إلى تقرير مسؤولية الأشخاص الطبيعيين والأشخاص الاعتباريين، وفرض التزامات قانونية على الشركات ومقدمي الخدمات الرقمية في مجال حماية البيانات والأمن السيبراني، مع إقرار جزاءات جنائية ومدنية وإدارية تتناسب مع خطورة الاعتداءات الواقعة على البيئة الرقمية.

ويبرز في هذا السياق الاتجاه الذي كرسه مجلس أوروبا من خلال اتفاقية بودابست[2] بشأن الجرائم الإلكترونية، التي أرست إطاراً دولياً لتجريم أبرز صور الجرائم السيبرانية، وتيسير التعاون القضائي الدولي، وتوحيد الحد الأدنى من قواعد التجريم والإجراءات.

تكشف التشريعات المقارنة عن تحول واضح من سياسة تشريعية تقوم على رد الفعل بعد وقوع الجريمة إلى سياسة استباقية ترتكز على الوقاية وإدارة المخاطر الرقمية، وذلك من خلال إلزام المؤسسات بتطبيق معايير الأمن السيبراني والإبلاغ عن الحوادث الإلكترونية وتعزيز حماية البيانات، وهو ما يعكس اتجاهاً حديثاً في قانون الأعمال نحو ربط الامتثال القانوني بإدارة المخاطر.

ثانياً: التدابير القضائية وآليات التعاون الدولي:

لم يعد القضاء التقليدي قادراً وحده على مواجهة الجرائم السيبرانية التي تتسم بالطابع العابر للحدود، لذلك اتجهت التشريعات المقارنة إلى تطوير المنظومة القضائية من خلال إنشاء وحدات ونيابات ومحاكم متخصصة، وتدريب القضاة وأعضاء النيابة العامة وضباط الضبط القضائي على تقنيات الأدلة الرقمية، والاستعانة بالخبرة الفنية في التحقيق والمحاكمة.

كما عززت التشريعات المقارنة آليات التعاون القضائي الدولي[3]، من خلال تبادل المعلومات، والمساعدة القضائية المتبادلة، وتسليم المجرمين، وتبادل الأدلة الرقمية، بما يسهم في ملاحقة الجناة واسترداد العائدات الإجرامية وحماية المصالح الاقتصادية للدول والشركات.

تبرز أهمية التخصص القضائي في الجرائم السيبرانية بالنظر إلى تعقيد الأدلة الرقمية وتشابك الاختصاصات القضائية، إذ إن فعالية الحماية القانونية لا تتوقف على وجود نصوص التجريم، وإنما تمتد إلى قدرة القضاء على استيعاب الجوانب التقنية للجريمة وضمان سرعة الفصل في المنازعات المرتبطة بها. [4]

[1] مرسوم عدد 54 لسنة 2022 مؤرخ في 13 سبتمبر 2022 يتعلق بمكافحة الجرائم المتصلة بأنظمة المعلومات والاتصال، منشور على الرابط:
https://legislation-securite.tn/ar/latest-laws/%D9%85%D8%B1%D8%B3%D9%88%D9%85-%D8%B9%D8%AF%D8%AF-54-%D9%84%D8%B3%D9%86%D8%A9-2022-%D9%85%D8%A4%D8%B1%D8%AE-%D9%81%D9%8A-13-%D8%B3%D8%A8%D8%AA%D9%85%D8%A8%D8%B1-2022-%D9%8A%D8%AA%D8%B9%D9%84%D9%82/

[2] اتفاقية بودابست لمكافحة الجرائم الإلكترونية 2001.

[3] من أمثلته ما ذكرناه عند الحديث عن موضوع التعاون القضائي الدولي.

[4] مهد رضا، الجرائم السيبرانية وآليات مكافحتها في التشريع الجزائري، مرجع سابق، ص 11

ثالثاً: التدابير الوقائية وتعزيز الأمن السيبراني:

إلى جانب التجريم والعقاب، أولت التشريعات المقارنة اهتماماً متزايداً بالتدابير الوقائية باعتبارها الوسيلة الأكثر فاعلية لحماية بيئة الأعمال الرقمية. وتشمل هذه التدابير إلزام المؤسسات بوضع سياسات لإدارة المخاطر السيبرانية، واعتماد أنظمة متقدمة لحماية الشبكات والبيانات، وإجراء تقييمات دورية للمخاطر، ووضع خطط للاستجابة للحوادث الإلكترونية، فضلاً عن نشر ثقافة الأمن السيبراني بين العاملين.

وتمثل التدابير الوقائية تجسيداً للتحول من الحماية اللاحقة إلى الحماية الاستباقية، إذ إن تعزيز الأمن السيبراني داخل المؤسسات يقلل من احتمالية وقوع الجريمة ويحد من آثارها عند حدوثها. ومن ثم، فإن نجاح السياسة التشريعية الحديثة لا يقاس بصرامة العقوبات وحدها، بل بقدرتها على بناء منظومة متكاملة تجمع بين التشريع، والقضاء، والوقاية، بما يحقق الأمن القانوني والاستقرار في بيئة الأعمال الرقمية.

الفقرة الثانية: تقييم التشريع الموريتاني ومقترحات تطويره في ضوء التشريعات المقارنة:

سنتناول هذه الفقرة من خلال تقييم التشريع الموريتاني في مواجهة الجرائم السيبرانية في بيئة الأعمال الرقمية (أولاً)، ثم الحديث عن مقترحات تطوير التشريع الموريتاني في ضوء التشريعات المقارنة (ثانياً).

أولاً: تقييم التشريع الموريتاني في مواجهة الجرائم السيبرانية في بيئة الأعمال الرقمية:

شهد التشريع الموريتاني خلال السنوات الأخيرة اهتماماً متزايداً بتنظيم البيئة الرقمية ومواجهة الجرائم المرتكبة عبر الوسائل الإلكترونية، من خلال استحداث نصوص قانونية تعنى بتجريم الاعتداء على الأنظمة المعلوماتية، وتنظيم المعاملات الإلكترونية، وتعزيز أمن الفضاء الرقمي، وتتمثل هذه النصوص القانونية في: [1]

- قانون الجريمة السيبرانية (رقم 2016-007): يُعد التشريعي الرئيسي والأهم؛ حيث يُعرّف الجرائم المرتكبة عبر شبكات الإنترنت، ويجرم أفعالاً مثل انتحال الهوية، القرصنة، الاحتيال، وسرقة البيانات.
- قانون حماية البيانات ذات الطابع الشخصي (رقم 2017-020): صدر بتاريخ 15 نوفمبر 2017، ويهدف إلى تأمين المعطيات الشخصية للمواطنين ومنع استغلالها غير القانوني.
- القانون التوجيهي لمجتمع المعلومات (رقم 2016-006): ينظم البنية التحتية والتوجهات العامة للتحول الرقمي.
- قانون الاتصالات الإلكترونية (رقم 2013-025): يضع الضوابط الناظمة لقطاع الاتصالات والخدمات المرتبطة به.
- قانون رقم 2018 -022 / يتعلّق بالمبادلات الإلكترونية.
- قانون رقم 2024-011/ر.ج/ يتضمن تحديد هوية المشتركين في خدمات الاتصالات الإلكترونية المفتوحة للعموم واستعمال خدماتها.
- قانون مكافحة غسل الأموال وتمويل الإرهاب رقم 07-2019 الصادر بتاريخ 20 فبراير 2019.

فضلاً عن بعض الجهات المؤسسية والرقابية المتمثلة في:

- سلطة حماية البيانات ذات الطابع الشخصي: هيئة مستقلة تتولى السهر على احترام حماية المعطيات الشخصية الرقمية وفقاً للقوانين المعمول بها.
- المكتب المركزي لمكافحة الجريمة السيبرانية: وحدة أمنية متخصصة تابعة للإدارة العامة للأمن الوطني، تمتلك صلاحيات وطنية للتحقيق في الجرائم التقنية والابتزاز والاحتيال الإلكتروني.

ويعكس هذا التوجه إدراك المشرع لأهمية توفير حماية قانونية للأنشطة الاقتصادية التي أصبحت تعتمد بصورة متزايدة على الوسائط الرقمية.

[1] موقع سلطة حماية البيانات ذات الطابع الشخصي https://www.apd.mr/%D9%82%D9%88%D8%A7%D9%86%D9%8A%D9%86/

ومع ذلك، فإن تقييم المنظومة القانونية الموريتانية يكشف عن وجود عدد من التحديات التي تحد من فعاليتها في حماية بيئة الأعمال الرقمية. فمن جهة، لا تزال بعض النصوص القانونية متفرقة بين عدة قوانين، الأمر الذي قد يؤدي إلى صعوبة التطبيق وتداخل الاختصاصات. ومن جهة أخرى، فإن التطور المتسارع للجرائم السيبرانية يفوق في كثير من الأحيان سرعة التحديث التشريعي، مما يؤدي إلى ظهور صور إجرامية جديدة لا تجد تنظيماً قانونياً دقيقاً. [1]

كما يلاحظ أن التشريع الموريتاني يحتاج إلى مزيد من التفصيل في تنظيم مسؤولية الأشخاص الاعتباريين، والالتزامات القانونية المفروضة على الشركات ومقدمي الخدمات الرقمية، وقواعد الإبلاغ عن الحوادث السيبرانية، وحماية البيانات التجارية، بما يحقق مستوى أعلى من الأمن القانوني في بيئة الأعمال. [2]

ثانياً: مقترحات تطوير التشريع الموريتاني في ضوء التشريعات المقارنة:

تستوجب فعالية الحماية القانونية لبيئة الأعمال الرقمية الاستفادة من التجارب التشريعية المقارنة، ولا سيما تلك التي اعتمدت مقاربة شاملة تجمع بين التجريم، والوقاية، والامتثال، والتعاون الدولي. وفي هذا الإطار يمكن اقتراح ما يأتي:

1. تحديث التشريعات المتعلقة بالجرائم السيبرانية بصورة دورية، بما يستوعب المستجدات التقنية والأنماط الإجرامية الحديثة، كالجرائم المرتبطة بالذكاء الاصطناعي، والحوسبة السحابية، والعملات المشفرة.
2. إقرار إطار قانوني متكامل لحماية بيئة الأعمال الرقمية يربط بين قوانين الجرائم السيبرانية، والتجارة الإلكترونية، وحماية البيانات، وقانون الشركات، بما يحقق الانسجام التشريعي.
3. تعزيز تنظيم مسؤولية الأشخاص الاعتباريين ومقدمي الخدمات الرقمية، مع تحديد التزاماتهم في مجال الأمن السيبراني، والإبلاغ عن الحوادث الإلكترونية، وإدارة المخاطر الرقمية.
4. تطوير قواعد الإثبات الإلكتروني والإجراءات الجنائية الرقمية، بما يضمن سلامة الأدلة الرقمية وسرعة جمعها والمحافظة عليها، مع إنشاء وحدات قضائية وفنية متخصصة في الجرائم السيبرانية.
5. تعزيز التعاون الدولي والإقليمي في مجال مكافحة الجرائم السيبرانية، من خلال الانضمام إلى الاتفاقيات الدولية ذات الصلة، وتفعيل آليات تبادل المعلومات والمساعدة القضائية، والاستفادة من الخبرات المقارنة.
6. إلزام المؤسسات الاقتصادية بتبني برامج الامتثال والأمن السيبراني، ووضع سياسات لإدارة المخاطر، وتدريب العاملين، واعتماد معايير الحوكمة الرقمية لحماية البيانات والأصول الرقمية.

تكشف التجارب المقارنة أن نجاح السياسة التشريعية في مواجهة الجرائم السيبرانية لا يرتبط بزيادة العقوبات فحسب، وإنما يعتمد على بناء منظومة متكاملة تجمع بين التشريع الفعال، والقضاء المتخصص، والتدابير الوقائية، والامتثال المؤسسي. ومن ثم، فإن تطوير التشريع الموريتاني ينبغي أن يتجه نحو تبني رؤية شاملة تجعل الأمن السيبراني جزءاً من منظومة حماية الاستثمار وتعزيز الثقة في بيئة الأعمال الرقمية، بما ينسجم مع التحول الرقمي ومتطلبات التنمية الاقتصادية.

يتضح أن التشريع الموريتاني يمتلك أساساً قانونياً يمكن البناء عليه لحماية بيئة الأعمال الرقمية، إلا أن فعاليته تظل رهينة بتحديث النصوص القانونية، وتكاملها، وتطوير آليات تطبيقها. كما أن الاستفادة من التشريعات المقارنة من شأنها أن تسهم في بناء منظومة قانونية أكثر قدرة على مواجهة الجرائم السيبرانية، وتحقيق التوازن بين تشجيع الاستثمار الرقمي، وحماية الحقوق، وضمان الأمن القانوني للمعاملات الاقتصادية.

خاتمة

أفضى البحث في موضوع المسؤولية القانونية عن الجرائم السيبرانية وآليات حماية بيئة الأعمال الرقمية: دراسة مقارنة، إلى أن التحول المتزايد نحو البيئة الرقمية، وما صاحبه من توسع في استخدام التقنيات الحديثة في مختلف الأنشطة الاقتصادية

[1] مهد رضا، الجرائم السيبرانية وآليات مكافحتها في التشريع الجزائري، مرجع سابق، ص 13.
[2] محمد سعيد العالم، صعوبات القانون الجنائي الموريتاني في مواجهة جرائم التكنلوجيا الحديثة، المجلة الدولية للبحوث والدراسات القانونية، المجلد 05، العدد 02، السنة 2026، ص 7.

والتجارية، أدى إلى ظهور أنماط إجرامية جديدة تستهدف الأنظمة المعلوماتية والبيانات والأموال والمصالح التجارية، وهو ما فرض على التشريعات الوطنية تطوير آليات قانونية قادرة على تحقيق حماية فعالة للمتعاملين في البيئة الرقمية، وقد تبين أن مواجهة الجرائم السيبرانية لا يمكن أن تقوم على المسؤولية الجنائية والعقوبة وحدهما، وإنما تقتضي منظومة متكاملة من المسؤولية القانونية، تشمل المسؤولية الجنائية والمدنية والتأديبية والتنظيمية، إلى جانب التدابير الوقائية والحوكمة الرقمية وإدارة المخاطر. كما أظهر البحث أن خصوصية الجرائم السيبرانية، من حيث سرعتها وطابعها العابر للحدود وصعوبة اكتشافها وإثباتها، تفرض تطوير قواعد الإثبات والتعاون القضائي والدولي بما يتلاءم مع طبيعة الجريمة الرقمية.

من خلال هذه الدراسة توصلت لجملة من النتائج والتوصيات:

أولاً: النتائج

توصل البحث إلى مجموعة من النتائج، أهمها:

- أن الجرائم السيبرانية أصبحت من أبرز التهديدات التي تواجه بيئة الأعمال الرقمية، لما تسببه من أضرار مالية وتجارية ومعلوماتية، فضلاً عن تأثيرها في الثقة والاستقرار داخل المعاملات الرقمية.
- أن المسؤولية عن الجرائم السيبرانية تتعدد صورها، فلا تقتصر على المسؤولية الجنائية، بل قد تمتد إلى المسؤولية المدنية والتأديبية والتنظيمية، بحسب طبيعة الفعل والضرر والالتزام القانوني الذي تم الإخلال به.
- أن تحديد المسؤولية في البيئة الرقمية يثير صعوبات خاصة، ولا سيما فيما يتعلق بإسناد الفعل الإجرامي إلى مرتكبه، وإثبات الجرائم المرتكبة عن بعد، وتحديد المسؤوليات بين الأشخاص الطبيعيين والأشخاص الاعتباريين والمسيرين ومقدمي الخدمات الرقمية.
- أن مسؤولية الشركات والأشخاص الاعتباريين ومقدمي الخدمات الرقمية أصبحت تحتل أهمية متزايدة، بالنظر إلى الدور الذي تؤديه هذه الجهات في إدارة الأنظمة والبيانات الرقمية وتأمينها.
- أن التشريع الموريتاني أظهر اهتماماً متزايداً بتنظيم البيئة الرقمية ومكافحة الجرائم السيبرانية من خلال مجموعة من النصوص القانونية المتعلقة بالجريمة السيبرانية وحماية البيانات ومجتمع المعلومات.
- أن المنظومة القانونية الموريتانية، رغم أهميتها، لا تزال تواجه بعض أوجه القصور، من بينها تشتت النصوص القانونية، وسرعة تطور الجرائم السيبرانية مقارنة بسرعة التطور التشريعي، والحاجة إلى مزيد من التفصيل في تنظيم مسؤولية الأشخاص الاعتباريين ومقدمي الخدمات الرقمية والإبلاغ عن الحوادث السيبرانية وحماية البيانات التجارية.
- أن التدابير الوقائية والأمن السيبراني والحوكمة الرقمية تمثل مكوناً أساسياً في السياسة الحديثة لحماية بيئة الأعمال، لأنها تساعد على الحد من وقوع الاعتداءات وتقليل آثارها عند حدوثها.

ثانياً: التوصيات

بناء على النتائج السابقة، يمكن تقديم التوصيات الآتية:

- تحديث التشريع الموريتاني المتعلق بالجرائم السيبرانية بصورة دورية، بما يواكب التطور المستمر للتكنولوجيا والأنماط الإجرامية المستحدثة، ولا سيما الجرائم المرتبطة بالذكاء الاصطناعي والحوسبة السحابية وغيرها من التقنيات الحديثة.
- إقرار إطار قانوني متكامل لحماية بيئة الأعمال الرقمية، يحقق الانسجام بين النصوص المتعلقة بالجرائم السيبرانية والتجارة الإلكترونية وحماية البيانات وقانون الشركات.
- تعزيز تنظيم مسؤولية الأشخاص الاعتباريين والمسيرين ومقدمي الخدمات الرقمية، مع تحديد الالتزامات الملقاة على عاتقهم في مجال حماية الأنظمة والبيانات وإدارة المخاطر الرقمية.
- تطوير الإطار القانوني للإثبات الإلكتروني وتعزيز الوسائل الفنية والقضائية اللازمة لجمع الأدلة الرقمية وحفظها والتحقق من سلامتها وحجيتها أمام القضاء.

- تعزيز التدابير الوقائية داخل المؤسسات والشركات من خلال إلزامها بوضع سياسات للأمن السيبراني، وإجراء تقييم دوري للمخاطر، ووضع خطط للاستجابة للحوادث، وتكوين العاملين في مجال الأمن الرقمي.
- تعزيز التعاون القضائي والأمني الدولي في مجال مكافحة الجرائم السيبرانية، بالنظر إلى طبيعتها العابرة للحدود وصعوبة مواجهتها في إطار وطني منعزل.
- تعزيز ثقافة الامتثال والحوكمة الرقمية داخل الشركات، بحيث تصبح حماية البيانات والأنظمة المعلوماتية جزءاً من الإدارة اليومية للنشاط التجاري، وليس مجرد إجراء لاحق لوقوع الجريمة.

المراجع

الكتب:

- عادل عبدالعال إبراهيم خراشي. الحماية الجنائية للحق في الخصوصية الرقمية. ط 1. القاهرة: شركة ناس للطباعة، 2015.
- منال هلال زهرة، تكنولوجيا الاتصال والمعلومات، ط1 ، دار أسامة، الأردن، 2014.
- عامر إبراهيم قدليجي، الحكومة الإلكترونية، ط1 ، دار المسيرة، الأردن، 2015.
- الصدة، عبد المنعم فرج، مصادر الالتزام. بيروت: دار النهضة العربية، 1979، من دون ذكر الطبعة.
- سليمان عبد المنعم، الجوانب الشكلية في النظام القانوني لتسليم المجرمين، دار الجامعة الجديدة للنشر، الإسكندرية، 2007.

المجلات:

- فريدة عبد الفتاح راضي /سالي عوض السقا، الجرائم الإلكترونية والجرائم المعلوماتية: من وجهة نظر قانونية وتقنية، المجلة الدولية للبحوث والدراسات القانونية، المجلد 03، العدد 05، 2024.
- حكيمة جاب الله، انعكاسات الجريمة السيبرانية على البيئة الرقمية: دراسة في آليات واستراتيجيات مكافحتها، مجلة جلويات جامعة الجزائر 1، المجلد 35، العدد 03، السنة 2023.
- فاضل عائشة، المسؤولية الجزائية في الجرائم الإلكترونية، مجلة الحقوق والحريات، المجلد 11، العدد 01 السنة 2023.
- الجرائم السيبرانية: مفهومها وآليات مكافحاتها، مجلة الحقوق والعلوم الإنسانية، المجلد 18، العدد 01، السنة 2025.
- د. بولحية شهيرة /د. سويح دنيا واد، الاحتيال الإلكتروني، مجلة الدراسات القانونية والاقتصادية، العدد 04، 2019.
- سوزان عدنان. "انتهاك حرمة الحياة الخاصة عبر الإنترنت". مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، 2013، مجلد (29). عدد (3).
- شباتي نضيرة، هوية المسير في ظل الشركة التجارية، مجلة الندوة للدراسات القانونية، العدد الأول، 2013.
- إيمان بن عثمان /ليلي بن بغيلة، التعاون القضائي الدولي ركيزة أساسية لتحقيق العدالة الجنائية الدولية، مجلة الشهاب، المجلد 11، العدد 01، السنة 2025.
- أحمد عودة سليمان الردادي، الحوكمة الرقمية وأثرها على القطاع العام، المدلة الدولية للبحوث والدراسات القانونية، المجلد 5، العدد 5، السنة 2026.
- مهد رضا، الجرائم السيبرانية وآليات مكافحتها في التشريع الجزائري، مجلة ايليزا للبحوث والدراسات، المجلد 06، العدد 02، 2021.

- محمد سعيد العالم، صعوبات القانون الجنائي الموريتاني في مواجهة جرائم التكنلوجيا الحديثة، المجلة الدولية للبحوث والدراسات القانونية، المجلد 05، العدد 02، السنة 2026.

الرسائل والاطروحات:

- الخميس ياسمين عبد العزيز إبراهيم، المسؤولية الجنائية للحدث في الجرائم المعلوماتية، رسالة ماجستير، جامعة القصيم، كلية الشريعة والدراسات الإسلامية، السعودية، السنة الدراسية 2016 -2017.
- شيرين حميد علي الجاف. الانتهاك الجرمي لحق الخصوصية باستخدام وسائل التصوير والاتصالات المستحدثة، رسالة ماجستير، كلية القانون والعلوم السياسية. جامعة كركوك، 2019.
- أحمد عبدين، مسؤولية المسير في الشركة التجارية، مذكرة لنيل شهادة ماستر أكاديمي، جامعة قاصيدي مرباح، كلية الحقوق والعلوم السياسية، السنة الجامعية 2015/2014.

مراجع النت:

- بحث منشور على الرابط: https://tharaaedu.com/cyber_attacks/
- مقال منشور في موقع الجزيرة بتاريخ 2022/08/01، على الرابط:

https://www.aljazeera.net/encyclopedia/2022/8/1/%D8%A7%D9%84%D8%AA%D8%AC%D8%B3%D8%B3-%D8%A7%D9%84%D8%A7%D9%82%D8%AA%D8%B5%D8%A7%D8%AF%D9%8A-%D8%B3%D8%B1%D9%82%D8%A9-%D8%A7%D9%84%D8%A3%D8%B3%D8%B1%D8%A7%D8%B1

- المصدر الرابط التالي: https://www.cloudsek.com/ar/knowledge-base/biggest-cyber-attacks
- الجرائم الإلكترونية. أركانها وأسبابها ودوافع ارتكابها، بحث منشور على الرابط:

https://www.rakpolice.gov.ae/MediaCenter/Details/38?uid=8e64919f1fc44c09acae4685d94b9cde

- ما هي الجرائم في الأمن السيبراني، بحث منشور على الرابط:

https://training.alkhaleej.com.sa/%D9%85%D8%A7-%D9%87%D9%8A-%D8%A7%D9%84%D8%AC%D8%B1%D8%A7%D8%A6%D9%85-%D9%81%D9%8A-%D8%A7%D9%84%D8%A3%D9%85%D9%86-%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A%D8%9F/