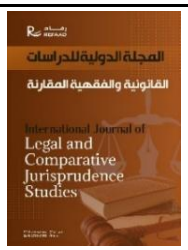
International Journal of Legal and Comparative Jurisprudence Studies (LCJS)
المجلة الدولية للدراسات القانونية والفقهية المقارنة
Journal Homepage: https://www.refaad.com/Journal/Index/9
E-ISSN 2708-6607 | P-ISSN 2708-6593
Vol. 6, Issue 3, 2025, pp. 240 - 250
www.refaad.com



The Role of Artificial Intelligence in Proving Cybercrimes: A Comparative Study of Emirati and Moroccan Law

دور الذكاء الاصطناعي في إثبات الجرائم السيبرانية "دراسة مقارنة بين القانون الإماراتي والمغربي"

Mohammed Abdulla bin Saifan Al Shamsi[1*]
[1] Police college Abu Dhabi, UAE.
* Corresponding Author: Mohammed Al Shamsi (shootar49@gmail.com)

محمد عبدالله بن سفيان الشامسي[1*]
[1] كلية الشرطة- أبو ظبي- الإمارات العربية المتحدة.
*الباحث المراسل: محمد الشامسي (shootar49@gmail.com)

Received استلام البحث	Revised مراجعة البحث	Accepted قبول البحث
2025/10/1	2025/12/17	2025/12/28

DOI: https://doi.org/10.31559/LCJS2025.6.3.6

Abstract:

Objectives: This research aims to examine the challenges posed by cybercrimes to traditional criminal evidence systems, in light of the rapid development of information technologies and the complexity of methods used to commit such crimes. It also seeks to highlight the role of artificial intelligence in supporting detection, analysis, and evidentiary mechanisms, and to assess the adequacy of the legal framework governing its use through a comparative analysis between Emirati and Moroccan legislation.

Methods: The study adopts a descriptive-analytical approach to analyze the legal and technical frameworks of cybercrimes and their evidentiary methods, alongside a comparative approach to identify similarities and differences between the legal regulations in the United Arab Emirates and Morocco, particularly with regard to the probative value of digital evidence and the use of modern technologies.

Results: The research concludes that traditional criminal evidence tools suffer from significant limitations in dealing with digital evidence, making the use of artificial intelligence a practical necessity to enhance the effectiveness of criminal investigations. It further demonstrates that Emirati legislation has adopted a more flexible and proactive approach to regulating modern technologies, whereas Moroccan legislation still requires legislative development to keep pace with technological advancements.

Conclusions: The study underscores the need to establish a clear legislative framework regulating the use of artificial intelligence in criminal evidence, to strengthen the training of judges and judicial police officers, and to enhance judicial oversight mechanisms, in a manner that ensures a balance between combating cybercrimes and protecting fundamental rights and freedoms.

Keywords: *Cybercrime; Artificial Intelligence; Criminal Evidence; Digital Evidence; Comparative Legislation.*

الملخص:

الأهداف: تهدف هذه الدراسة إلى دراسة التحديات التي تطرحها الجرائم السيبرانية أمام نظم الإثبات الجنائي التقليدية، في ظل التطور المتسارع لتقنيات المعلومات وتعقيد أساليب ارتكاب هذا النوع من الجرائم. كما يسعى إلى إبراز دور الذكاء الاصطناعي في دعم آليات الكشف والتحليل والإثبات، وبيان مدى ملاءمة الإطار القانوني المنظم لاستخدامه، من خلال مقارنة بين التشريع الإماراتي والتشريع المغربي.

المنهجية: اعتمدت الدراسة على المنهج الوصفي التحليلي من أجل تحليل الإطارين القانوني والتقني للجرائم السيبرانية ووسائل إثباتها، إلى جانب المنهج المقارن للكشف عن أوجه التشابه والاختلاف بين التنظيم القانوني في كل من الإمارات العربية المتحدة والمغرب، خاصة فيما يتعلق بحجية الأدلة الرقمية وتوظيف التقنيات الحديثة.

النتائج: توصلت الدراسة إلى أن وسائل الإثبات الجنائي التقليدية تعاني من قصور واضح في التعامل مع الأدلة الرقمية، مما يجعل الاستعانة بالذكاء الاصطناعي ضرورة عملية لتعزيز فعالية البحث الجنائي. كما أظهر أن التشريع الإماراتي اتجه نحو تنظيم أكثر مرونة واستباقية لاستخدام التقنيات الحديثة، في حين لا يزال التشريع المغربي في حاجة إلى تطوير وتحديث تشريعي يواكب هذه التحولات.

الخلاصة: خلصت الدراسة إلى ضرورة وضع إطار تشريعي واضح ينظم استخدام الذكاء الاصطناعي في الإثبات الجنائي، مع تعزيز تكوين القضاة وأجهزة الضبط القضائي، وتكريس رقابة قضائية فعالة تضمن التوازن بين مكافحة الجرائم السيبرانية وحماية الحقوق والحريات الأساسية.

الكلمات المفتاحية: *الجرائم السيبرانية؛ الذكاء الاصطناعي؛ الإثبات الجنائي؛ الأدلة الرقمية؛ التشريع المقارن.*

الاستشهاد

Citation

الشامسي، محمد. (2025). دور الذكاء الاصطناعي في إثبات الجرائم السيبرانية "دراسة مقارنة بين القانون الإماراتي والمغربي". *المجلة الدولية للدراسات القانونية والفقهية المقارنة*، 6 (3)، 240- 250.

Al Shamsi, M. S. (2025). The Role of Artificial Intelligence in Proving Cybercrimes: A Comparative Study of Emirati and Moroccan Law. *International Journal of Legal and Comparative Jurisprudence Studies*, 6(3), 240-250. https://doi.org/10.31559/LCJS2025.6.3.6 [In Arabic]

المقدمة:

أصبح العالم اليوم يعيش على وقع الثورة الرقمية وما صاحبها من تطورات تكنولوجية متسارعة غيرت ملامح الحياة الإنسانية في مختلف المجالات، وإذا كان هذا التطور قد أتاح فرصًا -غير مسبوقة- في تسهيل التواصل وتبادل المعلومات وتعزيز المعرفة، فإنه في المقابل قد أفرز أشكالًا جديدة من المخاطر، وفي مقدمتها الجرائم السيبرانية التي تجاوزت الحدود الجغرافية للدول، واضحت تهدد الأمن العام والحقوق الفردية -على حد سواء- وهنا يبرز الدور المحوري للقانون باعتباره الأداة الأساسية التي تمتلكها الدولة لتنظيم الحياة الاجتماعية ومواجهة الانحرافات الإجرامية بمختلف صورها.

والتطور الذي أصاب أوجه الحياة المختلفة من ثقافية أو اقتصادية أو اجتماعية أو سياسية لم يؤد إلى تحقيق الاستقرار في المجتمع؛ وبالتالي، التخلص من شبح الجريمة وآثارها السلبية المدمرة (جعفر، 2013، ص 6).

بحيث إن الجريمة لم تعد مرتبطة بالمعايير التقليدية التي عرفتها التشريعات الجنائية في القرنين التاسع عشر والعشرين، بل أصبحت أكثر تعقيدًا وتجردًا من الطابع المادي الذي كان يميزها. فظهرت الجريمة الإلكترونية، التي تتخذ من البيانات والأنظمة المعلوماتية مسرحًا لها، وأضحى مرتكبوها مجهولين أو بعيدين عن مكان ارتكابها، الأمر الذي جعل وسائل الإثبات التقليدية عاجزة عن ملاحقة هذا النمط الجديد من الإجرام، وفرض على المشرّع البحث عن آليات حديثة تتماشى مع طبيعة هذه الجرائم.

ومن أبرز التحولات التي شهدها مجال العدالة الجنائية في هذا السياق، الاعتماد على الأدلة الرقمية كوسيلة لإثبات الجرائم المعلوماتية. فهذه الأدلة، وإن كانت غير مادية، أصبحت ذات حجية قوية إذا ما استجمعت وفق معايير تقنية وقانونية دقيقة. غير أن طبيعتها الخاصة تثير تحديات عملية وقانونية، من حيث ضمان سلامتها، وحمايتها من التلاعب، وإثبات صحتها أمام القضاء. وهو ما يضع جهات البحث والتحري أمام مسؤوليات جسيمة تتجاوز ما ألفته في الجرائم التقليدية.

إلى جانب ذلك، لم يقتصر تأثير الثورة التكنولوجية على بروز الجرائم المعلوماتية فحسب، بل تعداها إلى ظهور تقنيات أكثر تقدمًا مثل الذكاء الاصطناعي، الذي لم يعد مجرد فكرة نظرية، بل تحول إلى واقع ملموس توظف تطبيقاته في مجالات متعددة: من الطب والتعليم إلى الاقتصاد والقضاء. وقد أظهر الذكاء الاصطناعي إمكانيات كبيرة في مكافحة الجريمة والتنبؤ بها، غير أنه في المقابل أتاح إمكانيات جديدة لارتكاب جرائم معقدة يصعب اكتشافها أو إسناد المسؤولية الجنائية عنها إلى أشخاص محددين، وهو ما يعرف بجرائم الذكاء الاصطناعي.

وتكمن خطورة هذه الجرائم في كونها قد ترتكب بواسطة أنظمة قادرة على اتخاذ قرارات مستقلة، مما يثير إشكاليات قانونية حول المسؤولية الجنائية، ومدى إمكانية إخضاع هذه الأنظمة أو مبرمجيها للقواعد التقليدية للتجريم والعقاب. كما يفرض تحديات جديدة على السياسة الجنائية التي يتعين عليها إيجاد حلول فعّالة تراعي خصوصية هذه الجرائم المستحدثة، دون أن تخل بالحقوق والحريات الأساسية للأفراد.

ومن هذا المنطلق، يكتسي موضوع البحث حول استخدام الذكاء الاصطناعي في إثبات الجرائم السيبرانية أهمية علمية وعملية بالغة. فعلى المستوى العلمي، يسهم في إثراء النقاش القانوني المتعلق بعلاقة التكنولوجيا بالقانون الجنائي، ومدى قدرة السياسة الجنائية على التكيف مع المستجدات التقنية. أما على المستوى العملي، فإنه يلامس حاجة ملحة لدى الأجهزة الأمنية والقضائية إلى وسائل جديدة قادرة على التصدي لهذه الجرائم بكفاءة وفعالية.

وعليه، فإن الإشكالية المحورية التي تطرحها هذه الدراسة يمكن صياغتها على الشكل التالي: **إلى أي حد يمكن الاستعانة بتقنيات الذكاء الاصطناعي في إثبات الجرائم السيبرانية بما يضمن تحقيق الأمن السيبراني من جهة، وحماية الحقوق والحريات من جهة أخرى؟**

ويتفرع عن هذه الإشكالية مجموعة من التساؤلات الفرعية، من قبيل:

- ما هي خصوصية الجريمة السيبرانية وأبعادها القانونية؟
- كيف يمكن توظيف الذكاء الاصطناعي في مجال الإثبات الجنائي؟

أهداف الدراسة:

تهدف هذه الدراسة إلى توضيح مفهوم الذكاء الاصطناعي ودوره في المجال الجنائي، مع إبراز خصوصية الجرائم السيبرانية والصعوبات التي تطرحها على مستوى الإثبات. كما يسعى إلى تحليل الإطار القانوني المنظم لإثبات هذه الجرائم في كل من التشريع الإماراتي والمغربي، وتقييم حجية الأدلة المستمدة من تقنيات الذكاء الاصطناعي. ويرمي البحث كذلك إلى إجراء مقارنة قانونية بين التشريعين لاستخلاص أوجه القوة والقصور، واقتراح توصيات تشريعية وقانونية تواكب التطور التكنولوجي وتدعم فعالية العدالة الجنائية.

منهجية الدراسة:

تعتمد هذه الدراسة على الجمع بين المنهج الوصفي التحليلي والمنهج المقارن، باعتبارهما الأنسب لدراسة دور الذكاء الاصطناعي في إثبات الجرائم السيبرانية. إذ يوظف المنهج الوصفي التحليلي لوصف وتحليل الإطارين القانوني والتقني للذكاء الاصطناعي، وبيان طبيعة الجرائم السيبرانية وصعوبات إثباتها، مع تحليل النصوص القانونية والفقهية والقضائية ذات الصلة في كل من التشريع المغربي والإماراتي، ودراسة حجية الأدلة المستمدة من التقنيات الذكية ومدى مشروعيتها. كما يعتمد المنهج المقارن لإبراز أوجه التشابه والاختلاف بين النظامين القانونيين في تنظيم وسائل إثبات الجرائم السيبرانية، وتقييم مدى فعالية كل تشريع في مواكبة التطور التكنولوجي، واستخلاص سبل تطوير القواعد القانونية ذات الصلة.

خطة الدراسة:

المبحث الأول: طبيعة الجرائم السيبرانية وتصنيفاتها

المطلب الأول: ماهية الجرائم السيبرانية وخصائصها.

الفقرة الأولى: مفهوم الجريمة السيبرانية.

الفقرة الثانية: خصائص الجريمة السيبرانية.

المطلب الثاني: أنواع الجرائم السيبرانية.

الفقرة الأولى: الجرائم التي تقع على الإنترنت.

الفقرة الثانية: الجرائم التي تقع بواسطة الإنترنت.

المبحث الثاني: إثبات الجرائم السيبرانية بوسائل الذكاء الاصطناعي

المطلب الأول: آليات البحث والتحقيق في الجرائم السيبرانية.

الفقرة الأولى: إجراءات البحث والتحقيق في الجرائم السيبرانية.

الفقرة الثانية: الأجهزة المختصة بالبحث والتحقيق في الجرائم المعلوماتية.

المطلب الثاني: صعوبات إثبات الجرائم السيبرانية عن طريق الذكاء الاصطناعي.

الفقرة الأولى: مدى حجية الدليل الإلكتروني المولد بالذكاء الاصطناعي.

الفقرة الثانية: التحديات القانونية والأخلاقية لإثبات الجرائم السيبرانية.

المبحث الأول: طبيعة الجرائم السيبرانية وتصنيفاتها

إن الجريمة السيبرانية هي نتاج للثورة الرقمية التي انعكست سلبًا على المجتمع الذي يرغب العيش في الاطمئنان والأمان، بحيث أصبحت شريكًا عن بعد لتصل إلى عقر داره دون اختراق للأبواب والنوافذ ودون استعمال للعنف الذي كنا نراه في الجرائم التقليدية. وهذا ما يجعلنا في البداية نقف على ماهية هذه الجرائم السيبرانية وخصائصها (المطلب الأول)، ثم ننتقل بعد ذلك، إلى الحديث عن تصنيفاتها في (المطلب الثاني). بهدف إعطاء فكرة حول طبيعة هذه الجرائم قبل الحديث عن دور الذكاء الاصطناعي في إثبات الجرائم السيبرانية في التشريعين المغربي والإماراتي.

المطلب الأول: ماهية الجرائم السيبرانية وخصائصها

كما هو معلوم، أن مفهوم الجريمة السيبرانية عرف تطورًا في العقود الأخيرة، بالشكل الذي جعل الفقه والقضاء يحددان عناصرها بين الحين والآخر، وهذا ما يجعل نقف على المفهوم في (الفقرة الأولى)، ثم ننتقل بعد ذلك للحديث عن خصائص الجريمة السيبرانية (الفقرة الثانية).

الفقرة الأولى: مفهوم الجريمة السيبرانية

إن مصطلح الجرائم السيبرانية هو إحدى المصطلحات الحديثة والمستخدمة عن جرائم الإنترنت الذي تعددت مصطلحاته وذلك لنشأة وتطور ظاهرة الإجرام المرتبط والمتصل بتقنية المعلومات. بحيث اختلفت المصطلحات التي أطلقت على هذه الأفعال غير المشروعة التي تقع في نطاق المعلوماتية حتى أنه يقال إن لكل باحث مشهود له في مجال المعلوماتية تعريفه الخاص الذي ينطلق منه لدراسة هذه الأفعال غير المشروعة.

وتتعدد التعريفات التي أخذ بها الفقه في تعريفه للجرائم المعلوماتية بحسب النظرة التي يرى بها كل اتجاه تلك الجرائم، فمنهم من اعتد في تعريفها بوسيلة ارتكابها ومنهم من أخذ بموضوع الجريمة ذاتها، ومنهم من رأى أن يعتد فيها بالجانبين باعتبار وسيلتها وموضوعها، ومن الفقه من رأى بأنها تتميز عن غيرها من الجرائم بسمة خاصة تتعلق بنوع الأشخاص الذين يرتكبونها وما يتسمون به من سمات خاصة وأتناول تلك الاتجاهات المختلفة في تعريف الجريمة المعلوماتية (فكري، 2014، ص 83).

وفي الحقيقة لو تأملنا نجد بأن مصطلح الجرائم السيبرانية (cyber crime) هو مصطلح أجنبي، لكنه هو المتداول والمستخدم من قبل التشريعات والفقه المقارن؛ وإن الجرائم السيبرانية تعد من الجرائم التي تباينت تسمياتها عبر المراحل الزمنية لتطورها، فكانت بداية من مصطلح إساءة استخدام الكمبيوتر، مرورًا باصطلاح احتيال الكمبيوتر، والجريمة المعلوماتية، فاصطلاحات جرائم الكمبيوتر، والجريمة المرتبطة بالكمبيوتر، وجرائم التقنية العالية، إلى جرائم الهاكرز، فجرائم الإنترنت، إلى آخر المصطلحات الجرائم السيبرانية.

تتباين الاتجاهات الفقهية في تحديد ماهية الجريمة السيبرانية، إذ انطلق بعض الباحثين من وسيلة ارتكابها معتبرين أن استعمال الحاسوب أو الأجهزة التقنية هو ما يميزها، غير أن هذا الرأي محل انتقاد لكون تعريف الجريمة يجب أن يستند إلى الفعل المجرم في ذاته لا إلى الوسيلة المستخدمة، فمجرد توظيف الحاسوب في ارتكاب فعل غير مشروع لا يكفي لاعتباره جريمة إلكترونية.

وفي مقابل ذلك، ذهب اتجاه آخر إلى ربط تعريف الجريمة الإلكترونية بالطابع الشخصي للجاني وما يمتلكه من خبرة تقنية، غير أن هذا التوجه بدوره غير دقيق، لأن الجريمة قد ترتكب من خلال تعاون عدة أشخاص بينهم المخطط والمحرض والمنفذ والمساهم، وقد لا تتوافر الخبرة الفنية لدى جميعهم.

وبناءً على ما تقدم، يقوم التعريف القانوني للجريمة السيبرانية على عناصر ثلاثة هي السلوك المجرم ووصفه القانوني، وجود نص يجرم ذلك السلوك ويحدد عقوبته، ثم محل الاعتداء المتمثل في المعطيات أو النظم المعلوماتية. ومن ثم يمكن القول إن الجريمة السيبرانية هي سلوك غير مشروع

صادر عن إرادة إجرامية ومعاقب عليه قانونًا يتعلق محله بالمعطيات أو النظم المعلوماتية، سواء أكان فعلًا إيجابيًا أم امتناعًا عن فعل. كما أن هذه الجريمة تتميز بخصائص تجعلها مختلفة عن الجرائم التقليدية، فهي في الغالب تمس مصالح معنوية وليست مادية، ولا تعترف بحدود مكانية أو جغرافية، إضافة إلى ما تتسم به من تباعد زمني ومكاني بين الجاني والمجني عليه.

الفقرة الثانية: خصائص الجريمة السيبرانية

تتميز الجرائم المعلوماتية بخصوصيات تجعلها مختلفة عن الجرائم التقليدية، فهي مرتبطة بشكل مباشر بعالم التكنولوجيا والحاسوب سواء باعتباره وسيلة أو هدفًا للجريمة، وقد انعكست هذه الخصوصية على شخصية المجرم المعلوماتي الذي يختلف عن المجرم التقليدي في طرق التنفيذ والمهارات المستخدمة.

ومن أبرز ما يميز هذه الجرائم أنها ذات طابع دولي عابر للحدود، إذ إن تطور وسائل الاتصال والإنترنت جعل العالم أشبه بقرية صغيرة، بحيث يمكن للجاني أن يكون في بلد والضحية في بلد آخر، بينما يظهر أثر الجريمة في دولة ثالثة، وهو ما يثير صعوبات قانونية تتعلق بتحديد الاختصاص القضائي والقانون الواجب التطبيق، الأمر الذي يستلزم تعاونًا دوليًا من خلال الاتفاقيات والمعاهدات لمواجهتها.

كما أن هذه الجرائم تتميز بصعوبة اكتشافها وإثباتها لكونها ترتكب في بيئة افتراضية لا تترك آثاراً مادية تقليدية، وغالبًا ما تُمحى أدلتها في لحظات معدودة، إضافة إلى لجوء مرتكبيها إلى وسائل تقنية متقدمة تحجب هوياتهم، وهو ما يعقد عمل أجهزة العدالة خاصة مع ضعف الخبرة التقنية لدى كثير من المحققين والقضاة. ويزيد الأمر تعقيدًا إحجام الضحايا عن الإبلاغ عنها، إما لعدم اكتشافهم لها في وقت مبكر، أو خوفًا من التشهير وفقدان السمعة والثقة لدى العملاء، خصوصًا في قطاع الأعمال والمؤسسات المالية، الأمر الذي يدفعهم أحيانًا إلى معالجة الموضوع داخليًا بعيدًا عن السلطات (الأموي، 2021، ص 32).

وانطلاقًا من ذلك تبرز الحاجة الملحة إلى تطوير التشريعات الوطنية بما يضمن سرية التبليغ والتحقيق والمحاكمة، وتوفير حماية قانونية للمبلغين، مع العمل على تأهيل الأطر الأمنية والقضائية وتأمين تعاون دولي فعال يواكب هذا النمط الجديد والمعقد من الجرائم.

المطلب الثاني: أنواع الجرائم السيبرانية

إن بيان أصناف الجرائم المعلوماتية ليس بالأمر البسيط، نظرًا لاختلافها من مجتمع لأخر من حيث تطوره ومدى استخدامه للحاسب الآلي، ودرجة اعتماده عليه في مختلف جوانب الحياة وكذلك تباين واختلاف الفقهاء وعدم تبنيهم المعايير واحدة ثابتة ولضوابط مشتركة، وفي هذا الصدد ذهب بعضهم إلى وضع عدة أسس من أجل تصنيف الجرائم المعلوماتية وتقسيماتها، فمنهم من يصنفها على أساس الرجوع إلى وسيلة ارتكاب الجريمة أو حسب دافع المجرم وآخرين على أساس محل الجريمة (الأموي، 2021، ص40).

ومن ضمن تلك التقسيمات التقسيم الذي اعتمدته الاتفاقية الأوروبية "بودابست" (للتوسع أكثر؛ راجع اتفاقية بودابست والبرتوكول الملحق بها بشأن مكافحة الجريمة الإلكترونية المعتمدة سنة 2001).

- الجرائم التي تستهدف سلامة وسرية عناصر المعطيات والنظم: تضم الدخول غير القانوني، الاعتراض غير القانوني، تدمير المعطيات، اعتراض النظم، إساءة استخدام الأجهزة).
- الجرائم المرتبطة بالكمبيوتر: تضم التزوير والاحتيال المرتبطين بالكمبيوتر).
- الجرائم المرتبطة بالمحتوى: وهي الجرائم المتعلقة بالأفعال الإباحية وغير الأخلاقية).
- الجرائم المرتبطة بالأشخاص والأموال: وتضم السرقة والاحتيال والتزوير والاطلاع على البيانات الشخصية، المعلومات المضللة والزائفة، أنشطة الاعتداء على الخصوصية، القرصنة، بث البيانات من مصادر مجهولة الإرهاب الالكتروني... وغيرها من الجرائم.

ويصنف الفقهاء وبعض الباحثين جرائم الحاسوب والإنترنت ضمن فئات عديدة، ولكن على العموم، يمكن تقسيمها إلى مجموعتين أساسيتين، الأولى جرائم تقع على الإنترنت (الفقرة الأولى)، والثانية جرائم تقع بواسطة الإنترنت (الفقرة الثانية).

الفقرة الأولى: الجرائم التي تقع على الإنترنت

في بعض الحالات، لا تمثل الشبكة المعلوماتية سوى عنصر سلبي في ارتكاب الجريمة، إذ تكون مجرد فضاء للاعتداء وارتكاب الجريمة؛ ففي مثل هذه الوضعيات، يتركز اهتمام الجاني على البيانات والمعلومات المخزنة أو المتبادلة عبر الإنترنت، سواء كانت ذات طبيعة خاصة أو عامة، محاولًا اختراق الأنظمة الأمنية -إن وجدت- للاعتداء على الأموال أو المصالح المرتبطة بها.

وقد أفرزت البيئة الرقمية شكلًا جديدًا من القيم الاقتصادية أُطلق عليه "الأموال المعلوماتية"، وهي ناتجة عن الاستخدامات المتعددة للبرامج والأنظمة المعلوماتية في الميادين الاجتماعية والاقتصادية. ومع بروز هذه القيمة، ظهرت جرائم مستحدثة سميت "الجرائم المعلوماتية"، ويمكن النظر إليها من جانبين:

أولهما: عندما تستخدم الوسائل المعلوماتية كأداة لارتكاب جرائم تقليدية، كالسرقة أو النصب أو خيانة الأمانة.

ثانيهما: عندما تكون المعلومات نفسها هي موضوع الاعتداء، سواء بالاستيلاء عليها أو إساءة توظيفها أو استغلالها للإضرار بالغير.

وتندرج ضمن هذه الفئة عدة صور من الجرائم، من أبرزها:

أولًا: جريمة الاختراق

يقصد بالاختراق في المجال المعلوماتي كل سلوك ينطوي على اقتحام الأنظمة أو الشبكات المعلوماتية الخاصة بالأفراد أو المؤسسات، سواء كانت عامة أو خاصة، باستعمال وسائل تقنية متعددة، من قبيل برامج كسر كلمات المرور أو الأكواد السرية أو غيرها من الوسائط المماثلة، وذلك بهدف الاطلاع غير المشروع على البيانات أو التلاعب بها أو إتلافها أو الاستيلاء عليها. ويعتبر هذا الفعل من بين أبرز صور الجرائم السيبرانية التي تهدد أمن المعلومات واستقرار المعاملات الإلكترونية.

وقد أولى المشرع العربي أهمية خاصة لهذا السلوك، حيث نص القانون النموذجي العربي لمكافحة الجريمة المعلوماتية في مادته الثالثة على تجريم كل من يلج، عن طريق التحايل أو بغير وجه حق، إلى نظم المعالجة الآلية للبيانات، مع تقرير عقوبة أشد متى ترتب عن هذا الفعل مساس بسلامة البيانات أو محوها أو تعديلها أو تعطيل النظام المستهدف.

وانسجامًا مع هذا التوجه، تبنى المشرع المغربي مقتضيات زجرية في القانون رقم 07.03 القاضي بتتميم مجموعة القانون الجنائي فيما يخص المس بنظم المعالجة الآلية للمعطيات، حيث اعتبر أن مجرد الولوج الاحتيالي إلى نظام للمعالجة الآلية يشكل جريمة قائمة بذاتها، وشدد العقوبة متى نتج عن هذا الولوج إتلاف أو حذف أو تغيير للمعطيات أو اضطراب في سير النظام. كما نص على مسؤولية الفاعل حتى في حالة ما إذا تم الدخول بطريق المصادفة ثم استمر في البقاء داخله دون مبرر قانوني.

أما المشرع الإماراتي، فقد تضمن المرسوم بقانون اتحادي رقم 34 بشأن مكافحة الشائعات والجرائم الإلكترونية نصوصًا واضحة في هذا السياق (نص المشرع الاماراتي في المادة 2 من المرسوم أعلاه على تجريم وعقاب الاختراق الالكتروني بغرامة وعقوبة سالبة للحرية.)

إذ جرم الدخول غير المشروع إلى موقع إلكتروني أو نظام معلوماتي أو شبكة معلوماتية، ولو تم الدخول بالصدفة أو عن غير قصد، ورتب عقوبات أشد متى كان الهدف من هذا الدخول الحصول على بيانات أو معلومات سرية أو استخدامها أو إفشاؤها أو إلحاق الضرر بها، بل شدد العقوبة أكثر إذا تعلق الأمر بأنظمة حكومية أو بيانات ذات طبيعة استراتيجية تمس الأمن القومي أو الاقتصاد الوطني.

وعليه، فإن جريمة الاختراق في التشريعات المقارنة، العربية عامة، والمغربية والإماراتية على وجه الخصوص، لا تتوقف فقط عند فعل الدخول غير المشروع، وإنما تمتد لتشمل البقاء داخل النظام المعلوماتي أو محاولة تعطيله أو المساس بمعطياته، مما يعكس الوعي التشريعي المتزايد بخطورة هذا السلوك على المصالح الفردية والجماعية وعلى الأمن المعلوماتي للدولة.

ثانيًا: المو اقع المعادية

ظهرت على شبكة الإنترنيت العديد من المواقع التي تستهدف تقويض النظام العام أو الإضرار بالمصالح العليا للدول، ومن أبرز صورها:

- المواقع السياسية المعادية: وهي التي تنشأ بهدف الطعن في شرعية الأنظمة السياسية القائمة وبث الشائعات والأخبار الكاذبة لإحداث الانقسام الداخلي.
- المواقع الدينية المعادية: حيث تنشئ بعض الجهات مواقع تتظاهر بالانتماء إلى الدين الإسلامي، لكنها في الواقع تنشر محتويات إباحية أو تنصيرية أو أفكاراً مناهضة للشريعة.
- المواقع المعادية للأشخاص أو الجهات: تستهدف الرموز الفكرية أو السياسية أو الدينية من خلال حملات التشهير أو نشر الأخبار الزائفة بغرض الإضرار بسمعتها أو بمصالحها المالية.

ثالثًا: جر ائم القرصنة المعلوماتية

تعد القرصنة المعلوماتية من أبرز صور الاعتداءات الإلكترونية، إذ تشمل مختلف الأفعال غير المشروعة التي تستهدف اختراق نظم المعالجة الآلية للمعطيات والعبث بها، سواء عبر الاستيلاء على الحسابات الشخصية والملفات الخاصة، أو قرصنة البرامج والأنظمة المعلوماتية.

ويعتبر المثال الشهير لقضية موقع ويكيليكس سنة 2010، حينما جرى نشر مئات الآلاف من الوثائق الرسمية الأمريكية (للتوسع أكثر راجع الموقع: https://www.bbc.com/arabic/worldnews/2010/12/101227_yearender_2010_wikileaks)، تجسيدًا لمخاطر هذا النوع من الجرائم التي قد تهدد الأمن القومي للدول.

وقد تصدى القانون المغربي لهذه الممارسات من خلال القانون رقم 07.03 المتمم لمجموعة القانون الجنائي، حيث نص على تجريم كل دخول أو بقاء غير مشروع في نظام للمعالجة الآلية للمعطيات، وتشديد العقوبة إذا اقترن الفعل بتعطيل النظام أو إتلاف المعطيات.

وبالمثل، فقد عالج المشرع الإماراتي هذه الظاهرة بمقتضى المرسوم بقانون اتحادي رقم 34 لسنة 2021 بشأن مكافحة الشائعات والجرائم الإلكترونية، إذ نص على عقوبات صارمة تطال كل من يقوم بالاعتداء على أنظمة المعلومات أو الاستيلاء على بياناتها.

ر ابعًا: جر ائم التجسس الإلكتروني

يمثل التجسس أحد أقدم الوسائل المستعملة في النزاعات السياسية والعسكرية، غير أن التحول الرقمي أفرز ما يعرف بـ"التجسس الإلكتروني"، الذي يمكن من اختراق الأنظمة والشبكات والوصول إلى معلومات سرية ذات طابع عسكري أو اقتصادي أو استراتيجي. وهو ما يشكل اعتداءً خطيرًا على خصوصية البيانات وحصانة الدول والمؤسسات.

وانسجاما مع ذلك، فإن التجسس عبر الوسائط الالكترونية يعتمد على استخدام التقنيات الالكترونية في الحصول على المعلومات، ولقد عرفه الفقه بأنه قيام الغير باستخدام البرامج التي تتيح له الاطلاع على البيانات والمعلومات الخاصة بالشركات والمؤسسات التجارية العاملة على شبكة الإنترنت (نعمان، ص294).

وقد أولى المشرع المغربي أهمية خاصة لهذه الجريمة، حيث نص في القانون رقم 05.20 المتعلق بالأمن السيبراني على ضرورة حماية نظم المعلومات ذات الطابع الحساس المرتبطة بالأمن القومي، مع تقرير مسؤولية جنائية على كل من يتعمد اختراقها أو استغلالها.

أما في التشريع الإماراتي، فإن المرسوم بقانون اتحادي رقم 34 لسنة 2021 اعتبر أي عمل يستهدف الحصول على بيانات أو معلومات تخص الدولة أو مؤسساتها الحيوية أو إفشاءها جريمة تجسس إلكتروني، ورتب عليها عقوبات قد تصل إلى السجن المؤبد إذا تعلق الأمر بمصالح الأمن القومي.

خامسًا: الإرهاب الإلكتروني

شهد الإرهاب تحوّلًا نوعيًا بفعل الثورة الرقمية، حيث لم يعد يعتمد فقط على الوسائل التقليدية، وإنما اتخذ بعدًا إلكترونيًا بالغ الخطورة. فالجماعات الإرهابية اليوم قادرة على استغلال الحواسيب والشبكات لتعطيل البنى التحتية الحيوية، مثل أنظمة الكهرباء والمياه والمواصلات والمراقبة الجوية والبحرية، بل وحتى النظم البنكية والمالية، مما يجعل الإرهاب الإلكتروني أحد أخطر التحديات الأمنية التي تواجهها الدول الحديثة.

وقد استحضر المشرع المغربي هذا الخطر في إطار القانون الجنائي، خاصة من خلال القانون رقم 03.07 المتعلق بالجرائم المعلوماتية، إلى جانب المقتضيات الخاصة بمكافحة الإرهاب التي يمكن أن تنطبق على الاعتداءات الإلكترونية المهددة للأمن والاستقرار.

أما في الإمارات العربية المتحدة، فقد جاء المرسوم بقانون اتحادي رقم 34 لسنة 2021 ليضع إطارًا متكاملًا لتجريم الأفعال الإرهابية الإلكترونية، سواء تعلق الأمر بإنشاء مواقع للترويج لأفكار متطرفة أو شن هجمات تستهدف البنى التحتية المعلوماتية، مع إقرار عقوبات مشددة تصل إلى الإعدام أو السجن المؤبد إذا ارتبطت الأفعال بتهديد سلامة الدولة وأمنها القومي.

الفقرة الثانية: الجرائم التي تقع بواسطة الإنترنت

تعد شبكة الإنترنت في بعض الحالات أداة إيجابية لارتكاب الجريمة، حيث تمكن المجرم المعلوماتي من تحقيق أهدافه بسهولة، ويلاحظ أن معظم هذه الجرائم تقع على الأشخاص بدرجات متفاوتة.

أولًا: الجرائم الجنسية والممارسات غير الأخلاقية

تستغل شبكة الإنترنت بصورة غير مشروعة لنشر الدعارة والإغواء وترويج المواد الفاحشة، مما يؤدي إلى استهداف الفئات الهشة واستغلال عوامل الضعف والانحراف لديهم. وتشمل هذه الأفعال التحريض على أنشطة جنسية محرّمة، وإفساد القاصرين أو استغلالهم عبر الوسائط الإلكترونية، إضافة إلى تسهيل نشر أو استضافة المواد الإباحية والإخلال بالحياء العام. وفي جوهرها، تلتقي جميع هذه الصور في نقطة واحدة تتمثل في توظيف الإنترنت والحاسب الآلي لتسويق الدعارة أو نشر الفاحشة، واستغلال المستخدمين -سواء كانوا قاصرين أو راشدين- في ممارسات جنسية غير مشروعة.

ثانيًا: الجرائم المالية

1. **جرائم بطاقات الائتمان والتحولات الإلكترونية غير المشروعة:**

لقد أدى انتشار التعامل بالبطاقات الائتمانية عبر الإنترنت إلى بروز عمليات اختراق واسعة النطاق، حيث يتمكن الجناة من الحصول على أرقام البطاقات واستغلالها في التحويلات المالية غير القانونية. وتتم هذه الجرائم بأشكال مختلفة، من بينها:

- الاحتيال من طرف العميل بحسن نية عبر مشاريع وهمية أو بطرق احتيالية للحصول على المال.
- إساءة استعمال العميل للبطاقات الائتمانية عن سوء نية، كاستخدام بطاقة منتهية الصلاحية أو ملغاة.
- استعمال الغير للبطاقات المسروقة أو المزورة، أو الاستيلاء على بياناتها وسحب الأموال بطرق تقنية دقيقة.

2. **القمار وغسل الأموال عبر الإنترنت:**

غالبًا ما ترتبط أنشطة غسل الأموال بمواقع القمار الافتراضية التي تنشأ في أماكن خارج الرقابة القانونية، وهو ما مكن العصابات من توظيف الإنترنت لتسريع وتوسيع عمليات غسل الأموال بعيدًا عن أعين السلطات.

3. **تزوير البيانات:**

يعتبر تزوير البيانات من أكثر الجرائم المعلوماتية شيوعًا، حيث يتم التلاعب بالبيانات المخزنة أو تعديلها بغرض تحقيق مكاسب غير مشروعة. وقد شددت العديد من التشريعات، مثل القانون النموذجي العربي واتفاقية بودابست، على تجريم هذه الأفعال حمايةً للثقة العامة في المعاملات الإلكترونية والوثائق الرسمية.

ثالثًا: الجرائم المنظمة

الجرائم المنظمة ليست وليدة العصر الرقمي، غير أن توظيف التكنولوجيا منحها أبعاداً أكثر خطورة واتساعًا. فقد لجأت عصابات المافيا وغيرها من التنظيمات الإجرامية إلى إنشاء مواقع إلكترونية تستخدم في غسل الأموال أو الاتجار بالأعضاء البشرية، معتمدة على هياكل تنظيمية محكمة تدر عليها أرباحًا هائلة.

رابعًا: تجارة المخدرات عبر الإنترنت

أصبحت شبكة الإنترنت أداة رئيسية في ترويج المخدرات، سواء عبر التخزين أو التواصل بين التجار والمستهلكين، مما حولها إلى بيئة خصبة للمعاملات غير المشروعة (الغماري، 2024).

خامساً: الاعتداء على التجارة الإلكترونية

مع تنامي التجارة الإلكترونية، برزت عمليات التجسس والسطو المعلوماتي، سواء من قبل شركات منافسة أو أطراف دولية، وهو ما يشكل تهديدًا خطيرًا للأمن القومي والاقتصادي. وقد بلغت هذه الاعتداءات مستوى خطيرًا من خلال عمليات السطو على أموال البنوك عن بُعد، مستخدمة تقنيات متقدمة تمكن المجرمين من الاستيلاء على مبالغ ضخمة قبل كشف الاختراق.

المبحث الثاني: إثبات الجرائم السيبرانية بوسائل الذكاء الاصطناعي

تشكل مسألة الإثبات حجز الزاوية في البحث والتحري عن الجرائم بشكل عام؛ سواء على المستوى الموضوعي أو على المستوى الإجرائي؛ وهذا ما دفع بالتشريعات إلى تعديل وسائل الإثبات؛ بالشكل الذي تواكب التطور الذي يعرف عالم الإجرام، وخصوص الرقمي.

وفي هذا السياق، سوف نعالج في الشق الأول من هذا المبحث آليات البحث والتحقيق في الجرائم السيبرانية (المطلب الأول)، ثم ننتقل بعد ذلك، في الشق الثاني إلى الحديث عن صعوبات إثبات الجرائم السيبرانية عن طريق الذكاء الاصطناعي (المطلب الثاني).

المطلب الأول: آليات البحث والتحقيق في الجرائم السيبرانية

بقدر ما حققته تكنولوجيا المعلومات في المجال الرقمي من آثار إيجابية، إلا أنها في الوقت نفسه مهدت إلى ظهور أنواع جديدة من الجرائم بالغة الخطورة، شكلت اعتداءات على الأفراد والمؤسسات الخاصة والعامة، وسببت خسائر كبيرة الاقتصاد الدولة ألا وهي الجرائم المعلوماتية بشتى أنواعها كما سبق ذكره في الفصل الأول، لذلك أدى الاستخدام غير المشروع للتقنية المعلوماتية إلى ظهور علم جديد في البحث الجنائي وهو علم البحث الجنائي الرقمي الذي يهتم بالدليل الرقمي بالنظر للآثار التي يتركها المجرم المعلوماتي أثناء ارتكابه الجريمة معلوماتية.

الفقرة الأولى: إجراءات البحث والتحقيق في الجرائم السيبرانية

يعد البحث والتحقيق من أبرز الإجراءات القانونية التي تتخذ بعد وقوع الجريمة، لما لها من دور محوري في التثبت من حقيقة وقوعها، وتحديد مسؤولية مرتكبها، وضمان إقامة الإسناد المادي للجريمة وفق قواعد الإثبات المختلفة. ومن خلال هذه الإجراءات يستجلّى الواقع المادي للجريمة، بهدف الوصول إلى إصدار حكم قضائي عادل سواء بالإدانة أو البراءة، بعد جمع وتحليل الأدلة المتوفرة.

أولًا: البحث والتحقيق في القانون المغربي

تنقسم عملية البحث والتحقيق في القانون المغربي إلى مرحلتين أساسيتين:

1. **مرحلة البحث والتحري:** تتولى فيها الشرطة القضائية جمع الاستدلالات الأولية حول الجريمة، ويكون هدفها الكشف عن ملابسات الواقعة وتجميع المعلومات الأولية.
2. **مرحلة التحقيق الابتدائي:** تدخل هذه المرحلة ضمن اختصاص السلطة القضائية، وتنقسم بدورها إلى:

- **تحقيق إعدادي:** يناط به رجال الشرطة القضائية بموجب إنابة صادرة عن قاضي التحقيق، أو مباشرة من قبل النيابة العامة، حسب مقتضيات القانون (العلمي، 2017.).
- **تحقيق نهائي:** يتم خلال مرحلة المحاكمة أمام المحكمة، ويهدف إلى تقديم الأدلة أمام القاضي لاتخاذ القرار القضائي.

ويلاحظ أن التشريع المغربي، من خلال قانون المسطرة الجنائية الجديد، يسعى إلى تنظيم إجراءات البحث والتحقيق بما يتلاءم مع خصوصية الجرائم المعلوماتية وطرق إثباتها الرقمية.

ثانيًا: البحث والتحقيق في القانون الإماراتي

في القانون الإماراتي، تنظم إجراءات البحث والتحقيق ضمن إطار يضمن التوازن بين حماية الحقوق الفردية وفاعلية مكافحة الجريمة، إذ توكل مهام البحث والتحري إلى الشرطة الاتحادية والنيابة العامة، مع تمكين السلطات القضائية من الإشراف المباشر على مراحل التحقيق، وخصوصًا في الجرائم ذات الطابع السيبراني، حيث تستعمل وسائل تقنية متقدمة لتحديد مرتكبي الجرائم وجمع الأدلة الرقمية بشكل قانوني.

ثالثًا: التحديات الخاصة بالتحقيق في البيئة الرقمية

إذا كان التحقيق التقليدي يعتمد على ذكاء المحقق وفطنته وسرعة بديهته، فإن التحقيق في البيئة الرقمية يتطلب تطوير أساليب متقدمة، واستعمال تقنيات متخصصة لمواكبة التطور المستمر في أساليب ارتكاب الجرائم السيبرانية. وفي هذا السياق، ظهر دور الذكاء الاصطناعي كأداة فعالة في:

- **تحليل البيانات الضخمة :(Big Data Analytics)** معالجة كميات هائلة من البيانات الرقمية واستخلاص مؤشرات جنائية محتملة؛ بحيث تشير البيانات الضخمة إلى الكم الهائل من المعلومات المتدفقة والمتنوعة، التي تتسم بالسرعة والتعقيد، بحيث يصعب معالجتها بالوسائل التقليدية، وفي المجال السيبراني، يتضمن ذلك دراسة سجلات الدخول؛ كحركات المرور الشبكي Network Traffic الرسائل المشبوهة، وحسابات المستخدمين،

بهدف اكتشاف سلوك غير طبيعي قد يدل على هجوم أو سلوك إجرامي (https://www.heraldopenaccess.us/openaccess/digital-forensics-confronting-modern-cyber-crimes-technological-advancements-and-future-challenges https://www.verizon.com/business/resources/T163/reports/2025-dbir-data-breach-investigations-report.pdf https://www.mirlabs.net/jias/index.html).

- **التعلم الآلي :(Machine Learning)** تمكين الأنظمة الذكية من التعلم الذاتي لتحسين اكتشاف الأنشطة المشبوهة.
- **التعرف على الأنماط :(Pattern Recognition)** مقارنة الأنشطة الرقمية بسلوكيات مسجلة سابقًا لتعقب مرتكبي الجرائم.
- **المراقبة التنبؤية:** هناك ما يعرف بالتنبؤ بالجريمة؛ أي توقع حدوثها في المستقبل أو الوقوف على سلوك مستقبلي ينطوي على خطورة إجرامية لدى بعض الأفراد يدفعهم لارتكاب الجريمة في المستقبل. وقد أدى استخدام التكنولوجيا في إطار عمل الشرطة والبحث الجنائي إلى ظهور ما يسمى بالشرطة التنبؤية Predivtive Policing والتي تهدف في المقام الأول إلى التنبؤ بأماكن ارتكاب الجريمة ووقوعها في المستقبل القريب، وذلك من خلال تحليل البيانات المخزنة لدى أجهزة البحث، وهو ما تم استخدامه في الولايات المتحدة منذ بداية القرن الحالي (علي، ص 1009).
- **تحليل البصمات الرقمية :(Digital Forensics AI)** كما هو معلوم، أن الجريمة الرقمية تترك وراءها آثارًا مختلفة عن الجرائم التقليدية، فقد برز مفهوم البصمات الرقمية التي تعد بمثابة الأدلة الالكترونية القابلة للتحليل والتتبع. وهي بمثابة الأثار الالكترونية التي يتركها المستخدم أثناء تفاعله مع الأنظمة والشبكات والأجهزة؛ كسجلات الدخول، عناوين بروتوكول الإنترنت، بيانات الأجهزة المستخدمة (Ikwu & Ciommoni, 2023).

رابعًا: القواعد الإجرائية الحديثة للبحث والتحقيق

مع تطور التكنولوجيا، أصبح من الضروري تكييف إجراءات البحث والتحقيق مع طبيعة الأدلة الرقمية، بما يحقق التوازن بين فعالية التحقيق وحماية الحقوق الفردية. ومن أبرز هذه الإجراءات:

- **تقنية تحديد الموقع:** تمكن من تحديد أماكن تواجد المشتبه فيهم وقت ارتكاب الجريمة، سواء في الزمن الفعلي أو عبر تتبع تحركاتهم السابقة، وذلك باستخدام عنوان بروتوكول الإنترنت (IP Address) الذي يميّز الجهاز وصاحبه. ويواجه هذا الإجراء أحيانًا تحديات مثل تعدد الأجهزة المرتبطة بنفس العنوان أو رفض الشركات الأجنبية التعاون مع السلطات.
- **الاختراق المعلوماتي :**يعد شكلًا متقدمًا من التفتيش، يتيح الوصول إلى الأنظمة الرقمية للوصول إلى المعلومات الضرورية للتحقيق، سواء عن طريق مراقبة افتراضية أو المساهمة الوهمية ضمن جهة إجرامية بهدف استدراج مرتكبي الجرائم. وقد تناولت مواد مشروع القانون المغربي (82-11 إلى 82-16 و713-1 إلى 713-44) هذه الآلية.
- **المراقبة الإلكترونية:** تشمل جمع البيانات عن الأشخاص أو الأماكن أو الأنشطة المشبوهة باستخدام الوسائل التقنية، مثل مراقبة البريد الإلكتروني أو أنظمة الحواسيب المخترقة.

إن دمج الذكاء الاصطناعي في هذه الإجراءات يتيح تعزيز فعالية البحث والتحقيق، وضمان جمع أدلة دقيقة وقابلة للاعتماد أمام القضاء، سواء في المغرب أو الإمارات.

الفقرة الثانية: الأجهزة المختصة بالبحث والتحقيق في الجرائم المعلوماتية

مع تطور التكنولوجيا وتوسع استخدام المعلوماتية في مختلف القطاعات، برزت الجرائم المعلوماتية كأحد أخطر أشكال الجريمة الحديثة، نظرًا لقدرتها على التأثير المباشر على الأمن الاقتصادي، الاجتماعي والسياسي للدول. وبناءً على ذلك، شرعت الدول في تأسيس أجهزة متخصصة للبحث والتحقيق في هذه الجرائم، مزودة بالكفاءات الفنية، والتدريب المتخصص، والوسائل البشرية والمادية الضرورية للتعامل مع الأدلة الرقمية المعقدة، وضمان جمعها بطريقة قانونية لإثبات التهم أمام القضاء. وفيما يلي تفصيل لهذه الأجهزة في كل من القانون المغربي والإماراتي.

أولًا: الأجهزة المختصة بالبحث والتحري في القانون المغربي

- **المكتب المركزي للأبحاث القضائية BCIJ:**

يعد المكتب المركزي للأبحاث القضائية إحدى الركائز الأساسية في مكافحة الجرائم الكبرى بالمغرب، بما فيها الجرائم المعلوماتية ذات الصلة بالإرهاب أو الأمن القومي، ويخضع المكتب للمديرية العامة لمراقبة التراب الوطني، ويختص بمعالجة الملفات الكبرى مثل مكافحة الخلايا الإرهابية، الجرائم العابرة للحدود، الاتجار بالمخدرات، والاختطاف؛ بحيث يندرج التعامل مع الجرائم المعلوماتية ضمن نطاق جرائم الإرهاب وفق المواد من 218-1 إلى 218-9 من مجموعة القانون الجنائي المغربي، مما يخضع التحقيق فيها لاختصاص للمكتب المركزي للأبحاث القضائية.

وفي هذا السياق، ساهم المكتب في تفكيك شبكة قرصنة إلكترونية استهدفت البنوك المغربية سنة 2020، بعد تحليل الأدلة الرقمية ومتابعة المتهمين عبر الأساليب التقنية الحديثة.

- **المديرية العامة لأمن نظم المعلومات DGSSI:**

تأسست هذه المديرية لتنفيذ السياسة الوطنية في مجال أمن المعلومات، وتهدف إلى حماية البنية التحتية الرقمية الوطنية، وتعزيز قدرة الدولة على رصد ومكافحة الجرائم المعلوماتية.

- **مصلحة المعلوميات التابعة للدرك الملكي:**

تعمل هذه المصلحة على متابعة الجرائم المعلوماتية في نطاق مهام الدرك الملكي، مع التركيز على الجرائم المرتبطة بالشبكات الوطنية والمواقع الحكومية. وتتمثل المهام الأساسية في الكشف عن المخترقين، وتحديد الأساليب التقنية المستخدمة، وتقديم الدعم الفني للتحقيقات القضائية.

كما ساهمت مصلحة المعلوميات في كشف شبكة احتيال إلكتروني استهدفت المواطنين عبر رسائل احتيالية في عام 2022، بالتنسيق مع النيابة العامة المغربية.

اللجنة الوطنية لمراقبة حماية المعطيات ذات الطابع الشخصي:

تأسست اللجنة بموجب القانون رقم 09.08 لحماية المعطيات الشخصية، وتتمثل مهامها في ضمان أن معالجة البيانات الشخصية تتم وفقًا للقانون، واحترام الحقوق الأساسية للأفراد؛ بحيث تتميز بمجموعة من الصلاحيات كمراقبة عمليات معالجة البيانات والتحقق من توافقها مع القانون، وكذلك إصدار العقوبات الإدارية، المالية، أو الجنائية عند وجود مخالفات، وكذلك الوصول إلى جميع عناصر المعالجة لضمان الرقابة الفعالة.

وفي هذا الإطار، قامت اللجنة في 2021 بإيقاف معالجة بيانات شخصية غير قانونية من قبل شركة تقنية أجنبية تعمل في المغرب، وفرض غرامة مالية وفق القانون.

ثانيًا: الأجهزة المختصة في القانون الإماراتي

تتوزع المسؤوليات بين عدة هيئات لضمان حماية الفضاء الإلكتروني والتحقيق في الجرائم المعلوماتية:

- **الإدارة العامة للتحريات الجنائية الإلكترونية:**

تختص هذه الإدارة بالكشف والتحقيق في الجرائم المعلوماتية، وجمع الأدلة الرقمية اللازمة للملاحقات القضائية. وتخضع مهامها للقانون الاتحادي رقم 5 لسنة 2012 بشأن مكافحة جرائم تقنية المعلومات، الذي يحدد العقوبات والآليات القانونية لمكافحة الجرائم الإلكترونية، بحيث تمكنت الإدارة من ضبط مجموعة قرصنة استهدفت البنوك والمؤسسات المالية عبر الإمارات سنة 2019، بالتنسيق مع البنوك والهيئات القضائية.

- **النيابة العامة الإلكترونية:**

تعمل على متابعة الجرائم المعلوماتية قضائيًا، والتأكد من التزام الأجهزة بجمع الأدلة وفق المعايير القانونية؛ وذلك برفع القضايا أمام القضاء، ومراقبة التحقيقات، وضمان مدى صحة وشرعية الأدلة الرقمية للاستخدام في المحاكم، وذلك في إطار تعاون النيابة العامة مع الشرطة الإلكترونية وفق القانون الاتحادي رقم 2012/5، بما يشمل حماية البيانات الشخصية وضمان سلامة التحقيقات الرقمية.

- **الهيئة الوطنية للأمن السيبراني:**

تشرف الهيئة على الاستراتيجية الوطنية للأمن السيبراني، وحماية البنية التحتية الرقمية، ومراقبة التهديدات الإلكترونية. ويمكن تحديد المهام المنوطة بالهيئة في كل من: وضع السياسات الوطنية للأمن السيبراني، التنسيق مع الأجهزة القضائية والشرطية، وإعداد خطط الحماية الوطنية. وأطلقت الهيئة في 2020 برنامجًا للتدريب على التحقيقات الرقمية للأطر الأمنية والقضائية، بهدف تعزيز قدرات الدولة في مواجهة الجرائم المعلوماتية.

وبناء على ما سبق، يمكن ملاحظة أن كلا من المغرب والإمارات اعتمد على مبدأ تخصص الأجهزة للتعامل مع الجرائم المعلوماتية، نظرا لطبيعتها التقنية وحساسيتها، مع تباين في توزيع الاختصاصات:

في **المغرب**، توجد مديريات متخصصة ضمن الأمن الوطني والدرك الملكي، إضافة إلى لجان لحماية البيانات الشخصية، مع التركيز على التنسيق الداخلي بين الأجهزة.

في **الإمارات**، توزعت المهام بين النيابة العامة، وزارة الداخلية، والهيئة الوطنية للأمن السيبراني، مع تركيز أكبر على التنسيق بين الأجهزة لضمان حماية شاملة للفضاء الإلكتروني.

ويجدر بالذكر أن، كلا النظامين القانونيين يولي أهمية قصوى لتدريب الأطر والمتخصصين في تحليل الأدلة الرقمية، وضمان الالتزام بالقوانين الوطنية والدولية في التحقيق في الجرائم المعلوماتية، بما يعزز مبدأ المسؤولية القانونية وحماية الحقوق الفردية.

المطلب الثاني: صعوبات إثبات الجرائم السيبرانية عن طريق الذكاء الاصطناعي

يعرف الإثبات على المستوى العملي مجموعة من الصعوبات والتحديات القانونية والأخلاقية، والتي قد تحد من نجاعته وتجعل من المتخصصين والممارسين للشأن القانوني والقضائي في صعوبة من أمرهم عند البحث والتحقيق والحكم في الجرائم السيبرانية.

وانسجامًا مع ذلك، لابد من الوقوف على حجية الدليل الإلكتروني الناتج عن الذكاء الاصطناعي في (الفقرة الأولى)، ثم ننتقل بعد ذلك، إلى الحديث عن التحديات القانونية والأخلاقية

الفقرة الأولى: مدى حجية الدليل الإلكتروني المولد بالذكاء الاصطناعي

إن موقع الذكاء الاصطناعي داخل المنظومات الأمنية والقضائية يختلف من دولة إلى أخرى تبعًا لمدى تطور بنياتها التكنولوجية وإطارها التشريعي. ففي الحالة المغربية، ورغم أن المشرع لم يحسم بعد في تنظيم الاستعمال المباشر لتقنيات الذكاء الاصطناعي ضمن وسائل الإثبات الجنائي، إلا أن الممارسة العملية تبين اعتمادًا متزايدًا لبعض الأجهزة الأمنية، وخاصة الشرطة القضائية ومختبرات الدرك الملكي، على برمجيات ذكية في تحليل الأدلة الإلكترونية وفك شفراتها التقنية (أحادوش، 2011_2012، ص 87).

كما بدأت الهيئة الوطنية لحماية المعطيات الشخصية في إدماج الانعكاسات المحتملة لهذه التقنيات ضمن عملها الرقابي، لاسيما ما يتعلق بصون الحقوق الفردية والخصوصية الرقمية. ومع ذلك، يبقى نطاق توظيف هذه الوسائل محدودًا، إذ لا يتجاوز في الغالب مرحلة البحث والتحقيق، دون أن يترتب عنه اعتراف صريح بحجيتها كوسيلة إثبات مستقلة أمام القضاء.

أما في التجربة الإماراتية، فقد تبنى المشرع نهجاً أكثر تقدمًا ووضوحًا، إذ لم يكتف بإرساء ترسانة قانونية متينة لمواجهة الجرائم السيبرانية، وإنما عمل على وضع خطة وطنية شاملة لإدماج الذكاء الاصطناعي في مختلف القطاعات، بما فيها الأمن والقضاء؛ ومن أبرز تجليات ذلك إطلاق مبادرات نوعية مثل "المحاكم الذكية" و"النيابة العامة الذكية"، فضلًا عن اعتماد وزارة الداخلية والنيابة العامة على أنظمة متطورة لتحليل البيانات الرقمية وتحويلها إلى تقارير فنية وقانونية تساهم في تكوين القناعة القضائية.

ومن خلال المقارنة بين التجربتين، يبدو أن المغرب مدعو إلى الانخراط في إصلاحات عميقة تستهدف:

- مراجعة القانون الجنائي وتحيينه بما يستوعب صور الجرائم المعلوماتية المستجدة، مع إقرار حجية صريحة للأدلة الرقمية الناتجة عن تطبيقات الذكاء الاصطناعي.
- إحداث بنية مؤسساتية متخصصة في الذكاء الاصطناعي الجنائي، على غرار النموذج الإماراتي، تتسم بالاستقلالية وترتبط مباشرة بالسلطة القضائية.
- تعزيز آليات التعاون الثنائي بين المغرب والإمارات في مجال الذكاء الاصطناعي الجنائي، بما يتيح تبادل الخبرات والممارسات الفضلى.
- صياغة قواعد قانونية ضابطة تضمن التوازن بين تحقيق الأمن الفعّال وصون الحقوق والحريات، حتى لا تتحول هذه الأدوات إلى وسائل للمراقبة المطلقة أو المساس بالخصوصية الفردية.

الفقرة الثانية: التحديات القانونية والأخلاقية لإثبات الجرائم السيبرانية

رغم المزايا التي يتيحها الذكاء الاصطناعي في مجال الإثبات الجنائي من حيث سرعة المعالجة ودقة التحليل، إلا أن توظيفه يثير إشكالات عميقة على المستويين القانوني والأخلاقي. فمسألة حجية الدليل المستخلص بواسطة الخوارزميات ما زالت محل نقاش، بالنظر إلى صعوبة إخضاع هذه النتائج لرقابة قضائية كاملة، في ظل ما يُعرف بظاهرة "الصندوق الأسود" التي تجعل منطق اشتغال الأنظمة غير شفاف.

وهذا الوضع يضع القاضي الجنائي أو الزجري أمام تحديات تتعلق بمدى إمكانية الاعتماد على نتائج تقنية لا يفهمها كليًا، خاصة وأن تكوين قناعته القضائية يفترض وضوح الأدلة وشفافيتها. فإذا كان القانون الإماراتي قد خطى خطوات متقدمة من خلال تحديث منظومتها التشريعية في القانون الاتحادي رقم 34 لسنة 2021 لمكافحة الشائعات والجرائم السيبرانية، فإن القانون المغربي ما يزال محكومًا بنصوص محدودة مثل القانون 07.03 والقانون 09.08، وهي نصوص لا تستوعب بعد التطورات التقنية المرتبطة بالذكاء الاصطناعي ولا تمنحه حجية مستقلة في الإثبات.

وتزداد الإشكالية تعقيدًا عند ربط توظيف الذكاء الاصطناعي بالموازنة بين الفعالية الأمنية وضمان الحقوق الأساسية للأفراد، وعلى رأسها الحق في الخصوصية وحماية المعطيات الشخصية. فبينما يميل التشريع المغربي إلى تغليب حماية هذه الحقوق في مواجهة أي توسع غير مبرر في جمع البيانات ومعالجتها، يظهر في التجربة الإماراتية توجه أكثر صرامة نحو ضبط الفضاء الرقمي، حتى ولو اقتضى الأمر التضييق النسبي على بعض الحريات الرقمية، انسجامًا مع رؤية استراتيجية للأمن السيبراني.

غير أن غياب إطار تشريعي صريح في كلا البلدين بشأن تحديد شروط استخدام الذكاء الاصطناعي كوسيلة للإثبات يظل ثغرة قائمة، تفرض ضرورة تطوير قواعد واضحة تحدد معايير الشفافية والمساءلة، وتضمن التوفيق بين متطلبات العدالة الجنائية وصيانة الحقوق الدستورية.

الخاتمة:

خلصت هذه الدراسة إلى أن الجرائم السيبرانية أفرزت إشكالات قانونية وإثباتية غير مسبوقة، بالنظر إلى طبيعتها التقنية وتعقيد أساليب ارتكابها، وهو ما جعل وسائل الإثبات الجنائي التقليدية عاجزة، في كثير من الحالات، عن مسايرة هذا النمط المستحدث من الإجرام. وقد بينت الدراسة أن تقنيات الذكاء الاصطناعي تشكل أداة فعّالة في كشف الجرائم السيبرانية، وتتبع مرتكبيها، وتحليل الأدلة الرقمية، بما تتيحه من قدرات عالية على المعالجة والتحليل والاستنتاج.

غير أن توظيف هذه التقنيات في المجال الجنائي يظل مشروطًا بتوفر إطار قانوني واضح ومتكامل، يضفي الحجية القانونية على الأدلة المستمدة منها، ويكفل في الوقت ذاته احترام الحقوق والحريات الأساسية، ولا سيما قرينة البراءة، وضمانات المحاكمة العادلة، وحماية المعطيات ذات الطابع الشخصي. كما أظهرت الدراسة المقارنة بين التشريع الإماراتي والمغربي وجود تفاوت ملحوظ في مستوى التأطير القانوني للأدلة الرقمية وتوظيف التقنيات الحديثة، حيث اتجه المشرع الإماراتي نحو تبني مقاربة تشريعية أكثر مرونة واستباقية، في حين لا يزال التشريع المغربي في حاجة إلى مزيد من التحيين والتطوير لمواكبة التحولات التكنولوجية المتسارعة.

وانطلاقًا من هذه النتائج، توصي الدراسة بضرورة تدخل المشرع بنصوص صريحة تنظم استعمال تقنيات الذكاء الاصطناعي في مجال الإثبات الجنائي، مع إقرار ضوابط قانونية وتقنية دقيقة تضمن سلامة الأدلة الرقمية وموثوقيتها. كما يؤكد على أهمية تعزيز التكوين المتخصص لفائدة القضاة وأجهزة الضبط القضائي في الجانبين القانوني والتقني، وتكريس التعاون المؤسسي بين الخبراء التقنيين والسلطات القضائية المختصة. وتوصي الدراسة، أخيرًا، بتطوير آليات الرقابة القضائية على استخدام الذكاء الاصطناعي، بما يحقق التوازن بين متطلبات مكافحة الجرائم السيبرانية من جهة، وصون ضمانات المحاكمة العادلة وحماية الحقوق والحريات الفردية من جهة أخرى.

المراجع:

أولًا: المراجع العربية

أحادوش، أسماء. (2011-2012). *الإثبات الجنائي في الجرائم المعلوماتية*. بحث لنيل دبلوم الماستر في القانون الجنائي والعلوم الجنائية، كلية العلوم القانونية والاقتصادية والاجتماعية، جامعة محمد الأول/ السنة الجامعية.

الأموي، عز الدين بن أمين. (2021). *الجرائم المعلوماتية في ضوء التشريع والقضاء المغربي واليمني*. المكافحة الموضوعية والإجرائية، دراسة مقارنة، الطبعة الأولى، مكتبة دار السلام.

جعفر، علي محمد. (2013). *السياسة الجزائية في ظل نظام العولمة*. الطبعة الأولى، مطبعة مجد للدراسات والنشر والتوزيع.

العلمي، عبد الواحد. (2017). *شرح في القانون الجديد المتعلق بالمسطرة الجنائية*. الجزء الثاني، التحقيق الإعدادي والمحاكمة، الطبعة الخامسة، مطبعة دار السلام.

علي، رزق سعد. (د.ت). استخدام تقنيات الذكاء الاصطناعي وتحليل البيانات في الكشف عن الجرائم، *مجلة الدراسات القانونية والاقتصادية*.

الغماري، جواد. (2024). *حماية المستهلك، شرع عملي مبسط*. الطبعة الأولى، مطبعة صناعة الكتاب.

فكري، أيمن عبد الله. (2014). *الجرائم المعلوماتية، دراسة مقارنة في التشريعات العربية والأجنبية*. الطبعة الأولى، مطبعة القانون والاقتصاد.

نعمان، ضياء علي أحمد. (2011). *الغش المعلوماتي، الظاهرة والتطبيقات*. سلسلة الدراسات القانونية في المجال المعلوماتي، العدد 1، الطبعة الأولى، المطبعة والوارقة الوطنية.

ثانيًا: المراجع الأجنبية

Ikwu, R., Giommoni, L., Javed, A., Burnap, P., & Williams, M. (2023). Digital fingerprinting for identifying malicious collusive groups on Twitter. *Journal of Cybersecurity*, 9(1). [CrossRef]

ثالثًا: ترجمة المراجع العربية

Ahadoush, A. (2012). *Criminal evidence in cybercrimes*. Master's diploma thesis in Criminal Law and Criminal Sciences, Faculty of Legal, Economic, and Social Sciences, Mohammed First University. [In Arabic]

Al-Alami, A. W. (2017). *Commentary on the new law relating to the Criminal Procedure Code* (Vol. 2, Preliminary investigation and trial, 5th ed.). Dar Al-Salam Press. [In Arabic]

Al-Amwi, I. B. A. (2021). *Cybercrimes in light of Moroccan and Yemeni legislation and judiciary: Substantive and procedural confrontation (A comparative study)* (1st ed.). Dar Al-Salam Library. [In Arabic]

Al-Ghamari, J. (2024). *Consumer protection: A simplified practical legal approach* (1st ed.). Book Industry Press. [In Arabic]

Ali, R. S. (n.d.). The use of artificial intelligence techniques and data analysis in crime detection. *Journal of Legal and Economic Studies*. [In Arabic]

Fikri, A. A. (2014). *Cybercrimes: A comparative study of Arab and foreign legislations* (1st ed.). Law and Economics Press. [In Arabic]

Jaafar, A. M. (2013). *Criminal policy under the globalization system* (1st ed.). Majd Press for Studies, Publishing, and Distribution. [In Arabic]

Naaman, D. A. A. (2011). *Information fraud: Phenomenon and applications* (1st ed.). Legal Studies Series in the Information Field (No. 1). National Printing and Paper Press. [In Arabic]