International Journal of Law Research and Studies (IJLRS)
Vol. (5), No. (2)
IJLRS
February 2026
المجلة الدولية للبحوث والدراسات القانونية
الإصدار (5)، العدد (2)

صعوبات القانون الجنائي الموريتاني في مواجهة جرائم التكنلوجيا الحديثة

محمد سعيد العالم
دكتوراه في القانون الخاص والعلوم الجنائية من جامعة المنار بتونس
أستاذ قانون خاص متعاون بكلية الحقوق والعلوم السياسية بجامعة نواكشوط، الجمهورية الإسلامية الموريتانية
alemmedsaid@gmail.com

المخلص بالعربية

يتناول هذا البحث موضوع صعوبات القانون الجنائي الموريتاني في مواجهة جرائم التكنولوجيا الحديثة، من خلال تحليل الإطارين الموضوعي والإجرائي في المنظومة الجنائية الموريتانية، مسلطاً الضوء على ثغرات السياسة الجنائية التي أنتهجها المشرع في هذا المجال. ويوضح البحث أن التطور التقني الهائل أفرز أنماطاً جديدة من الإجرام، في حين ظل القانون الجنائي الموريتاني الذي يعتمد على آليات تقليدية تعيق فعالية المواجهة. كما يركز البحث على الصعوبات المرتبطة بطبيعة الجريمة المعلوماتية، وضعف الوسائل التقنية والإثباتية، وغياب الخبرة المتخصصة لدى جهات التحقيق. ويشير البحث إلى مشكلة الإحجام عن التبليغ من قبل المؤسسات، وصعوبة التعاون الدولي في الجرائم العابرة للحدود.

وفي النهاية يقدم البحث جملة من الاقتراحات والحلول العملية التي ستساهم في تطوير صياغة التشريع الوطني المرتبط بحقوق حريات الأفراد مثل سرية الاتصالات والحياة الخاصة، وضبط القواعد التي تمنح حق التنصت الهاتفي والمراقبة السلكية واللاسلكية، وتوسيع صلاحيات القضاء في التفتيش الإلكتروني، وإنشاء هيئة وطنية للأمن السيبراني، والمصادقة على اتفاقية بودابست لتعزيز التعاون الدولي في مكافحة الجريمة المعلوماتية، إضافة إلى الدعوة إلى ضرورة تدريب سلطات البحث والادعاء في هذا المجال مما سيعزز من قدرتهم على استيعاب فهم النصوص التشريعية المرتبطة بواقع الاتصال والتقنيات الحديثة.

الكلمات المفاتيح: القانون الجنائي الموريتاني، جرائم التكنلوجيا الحديثة، الجريمة المعلوماتية، السياسة الجنائية في الفضاء السيبراني.

International Journal of Law Research and Studies (IJLRS)
Vol. (5), No. (2)
IJLRS
February 2026
المجلة الدولية للبحوث والدراسات القانونية
الإصدار (5)، العدد (2)

Difficulties of Mauritanian criminal law in confronting modern technology crimes

Mohamed Said Alem
PhD in Private Law and Criminal Sciences from Al-Manar University, Tunisia
Adjunct Professor of Private Law, Faculty of Law and Political Science, University of Nouakchott, Islamic Republic of Mauritania
alemmedsaid@gmail.com

Abstract

This study addresses the challenges faced by Mauritanian criminal law in confronting modern technology-related crimes, through an analysis of both the substantive and procedural frameworks of the Mauritanian criminal justice system. It highlights the gaps inherent in the criminal policy adopted by the legislator in this field. The research demonstrates that the enormous technological development has generated new patterns of criminal behavior, while Mauritanian criminal law continues to rely on traditional mechanisms that hinder an effective response. The study also focuses on the difficulties stemming from the nature of cybercrime, the weakness of technical and evidentiary tools, and the lack of specialized expertise among investigative authorities. In addition, the research points to the problem of institutions' reluctance to report incidents and the challenges of international cooperation in cross-border cybercrimes.

Finally, the study presents a set of practical proposals and solutions aimed at improving the drafting of national legislation related to individual rights and freedoms—such as the confidentiality of communications and the right to privacy—regulating the rules governing lawful telephone interception and electronic surveillance, expanding judicial powers in electronic searches, establishing a national cyber security authority, and acceding to the Budapest Convention to enhance international cooperation in combating cybercrime. The study also calls for the training of investigative and prosecutorial authorities in this field, in order to strengthen their ability to understand and apply legislative texts in light of contemporary communication technologies.

Keywords: Mauritanian Criminal Law, Modern Technology Crimes, Cybercrime, Criminal Policy in Cyberspace.

المقدمة

يعيش العالم بفضل تطور العقل البشري ثورة حقيقية في مجال التقدم العلمي والتقني والتكنلوجي، الشيء الذي شكل منعطفاً تاريخياً في حياة الأفراد والمجتمعات بفضل ظهور شبكات المعلومات، ووسائل الاتصال الحديثة وبرامج الذكاء الاصطناعي. [1]

ورغم أهمية هذه الوسائل، فإنها أصبحت بيئة حاضنة للجرائم المستحدثة والتي أصبحت تعرف بالجرائم الإلكترونية أو ما يسمى بالجرائم الافتراضية، أو جريمة الفضاء الإلكتروني. [2]

هذا النوع من الجرائم المستحدث أدى إلى ميلاد فقه جنائي يتميز بطابعه الخاص، وهو ما كان له أثر في سن بعض القوانين لعدة بلدان غربية وعربية، ولم يكن المشرع الموريتاني بمنىء عن التوجه العالمي لصد هذه الجرائم، إذ بدأ في تنظيم المسائل المتعلقة بالإلكترونيات بدءً في عام 2006 من خلال قانون الأداء الإلكتروني، ثم قانون رقم 2013-025 المتعلق بالاتصالات الإلكترونية، ثم قانون رقم 2017- 020 والمتعلق بحماية البيانات ذات الطابع الشخصي، وكذلك قانون 2018 -022 المتعلق بالمبادلات الإلكترونية، إضافة إلى المصادقة على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المؤرخة في 21\12\ 2010.

وقد أفرد الجريمة الإلكترونية بقانون خاص وهو القانون رقم 2016-007 الصادر بتاريخ 20 يناير 2016.

تعريف مصطلحات موضوع البحث

القانون الجنائي:

تقليدياً يعرف القانون الجنائي بتعريفات متعددة ومتنوعة، فيعرفه البعض بأنه القانون الذي يهتم بدراسة قواعد الجريمة والعقاب، وبالتالي فهو القانون الذي يحدد الجريمة ويضع لها عقابا،[3] كما تختلف تسميته حسب كل تشريع معين، فهناك من يطلق عليه عبارة "قانون العقوبات" وهناك من يطلق عليه عبارة "القانون الجنائي" أو" القانون الجزائي" ومهما اختلفت التسميات فإن القانون الجنائي فهو القانون الذي يهتم بدراسة السلوكيات الإجرامية ويضع لها عقاباً وفق تشريع معين.

كما نجد بعض الفقهاء يتبنى تعريفاً آخر أكثر دقة وشمولية للقانون الجنائي حيث يعتبر أن القانون الجنائي هو "القانون المتكون من مجموع القواعد الموضوعية والإجرائية المطبقة عادة على الجنايات والجنح والمخالفات"[4] فهذا التعريف يبدو أكثر شمولية فهو يشمل أنواع الجرائم بمختلف خطورتها من حيث

[1] علي كحلون: الجرائم المتعلقة بالمحتوى المعلوماتي، مجلة القضاء والتشريع نوفمبر 2003، ص 12، 13، 15.
[2] محاضرة الوفد التونسي في المؤتمر التاسع لرؤساء المحاكم العليا: الجرائم الإلكترونية الواقعة على الأشخاص في القانون التونسي، بيروت، 17-19-2018، ص 1.
[3] Patrick klob: Laurence Leturmy: Droit pénal général, Gaulino lextenso, 11 Edition, France, 2017, p 22.
[4] Merle et vitu: traité de droit criminel problème généraux de la Science criminelle , Droit pénal général, Cujas, T1, 7éme édition, 1997, p49.

الجناية والجنحة والمخالفة، ومن حيث الإجراءات الجنائية، إذ يحيلنا هذا التعريف إلى فروع القانون الجنائي المتنوعة، وهي ثلاثة فروع تقليدية القانون الجنائي العام، والقانون الجزائي الخاص، والإجراءات الجنائية. [5]

جرائم التكنولوجيا:

عرفها البعض بأنها: "عبارة عن نشاط إجرامي تستخدم فيه تقنية الحاسب الآلي بطريقة مباشرة أو غير مباشرة كوسيلة أو هدف لتنفيذ الفعل الإجرامي".

ومن الناحية القانونية فهي كل نشاط جنائي يمثل اعتداء على برامج الحاسب الآلي، ومهما تعددت وتنوعت تسميات ومصطلحات هذا النوع من الجرائم، فإن الجرائم المرتبطة بالحاسوب سواء كان وسيلة لها أو هدفاً لها فإنها تأخذ بعض الصور المتمثلة أساساً في بعض الأفعال الغير مشروعة مثل الاستخدام السيئ للحاسوب، أو اختراق النظم المعلوماتية، أو الاحتيال المعلوماتي، وغيرها من الأفعال الغير المشروعة. [8,7,6]

أهداف البحث

- تحليل مدى نجاعة المنظومة الجنائية الموريتانية (الموضوعية والإجرائية) في التصدي لجرائم التكنولوجيا الحديثة، وخاصة الجرائم المعلوماتية.
- تحديد الثغرات والصعوبات التي تواجه القانون الجنائي الموريتاني في التعامل مع الجرائم الإلكترونية، سواء من حيث النصوص أو من حيث التطبيق العملي.
- إبراز أوجه القصور في القواعد الموضوعية والإجرائية، مثل ضعف وسائل البحث، وصعوبة الإثبات، وعدم ملاءمة الإجراءات التقليدية مع الطبيعة التقنية لهذه الجرائم.
- تقييم فعالية الأجهزة القضائية وجهات التحقيق في مواجهة هذه الجرائم، ورصد العقبات المرتبطة بنقص الخبرة والتكوين التقني.
- اقتراح حلول ومقترحات إصلاحية من شأنها تمكين التشريع الموريتاني من مجاراة التطور التكنولوجي ومكافحة الجريمة المعلوماتية بفعالية أكبر.

إشكالية البحث

هل وفق المشرع الموريتاني في إرساء منظومة جنائية موضوعية وإجرائية قادرة على التصدي لجرائم التكنولوجيا الحديثة؟

---

[5] RASSAT (ML), op.cit, p54.

[6] أمال فكيري: إشكالات الإثبات والاختصاص يفي جرائم تكنولوجيا الإعلام والاتصال العابرة للحدود، مجلة العلوم القانونية والسياسية، عدد17 لسنة 2018ص 630.

[7] Salangeghenauti-Heli: la cybercriminalité 1er Edition presses polytechniques et universitaire Bomande, LA usanne, 1er Edition 2009, p 16.

[8] Myriam Quémener: cyber fraude, Revue Banque 1er Edition Paris, 2011, p 9.

خطة البحث

المبحث الأول: الصعوبات الموضوعية في مواجهة جرائم التكنلوجيا الحديثة:
- المطلب الأول: صعوبات مرتبطة بطبيعة الجريمة.
- المطلب الثاني: صعوبات مرتبطة بجهات التحقيق.

المبحث الثاني: الصعوبات الإجرائية في مواجهة جرائم التكنلوجيا الحديثة:
- المطلب الأول: العوائق على مستوى الإثبات.
- المطلب الثاني: العوائق الإجرائية العابرة للحدود.

المبحث الأول: الصعوبات الموضوعية في مواجهة جرائم التكنلوجيا الحديثة

يقصد بالصعوبات على مستوى القواعد الموضوعية الإشكاليات القانونية المتعلقة بالنص التشريعي في شقيه التجريمي والعقابي من جهة، وبالطبيعة الخاصة لجرائم التكنلوجيا الحديثة[9]من جهة أخرى، التي تواجهه رجال القانون عند تطبيق النصوص الموضوعية الهادفة إلى حماية الأفراد وحقوقهم. [10]

فالجريمة في المجال التكنلوجي نظراً لطابعها الخاص، فإنها فرضت بعض الحدود الموضوعية التي قد تشكل عائقاً أمام فاعلية القانون الجنائي،[11] وهو ما سنحاول تناوله في هذا المبحث من خلال الصعوبات الموضوعية التي فرضتها طبيعة الجريمة (مطلب 1) وكذلك الحدود الموضوعية المرتبطة بجهات التحقيق (مطلب 2).

المطلب الأول: صعوبات موضوعية مرتبطة بطبيعة الجريمة:

إن الحماية الجنائية التي أحاطها المشرع لهذا النوع المستحدث من الجرائم تعرف بعض الحدود والصعوبات، نظراً إلى طبيعتها، والخصوصية التي تتميز بها، وقد تجلى ذلك في عدة مظاهر، وللحديث عن هذه الحدود فإننا نخصص فقرتين لذلك القصور التشريعي للنص (فقرة الأولى) حدود فرضها أطراف الجريمة. (لفقرة الثانية).

الفقرة الأولى: قصور تشريعي متعلق بالنص:

كرس المشرع الموريتاني جملة من القواعد التشريعية الموضوعية الهامة في إطار مواجهة جرائم التكنلوجيا الحديثة، وذلك ضماناً لحسن سير تطبيق القانون، واحتراماً لحقوق المتهم، مثل احترام الحياة الخاصة للفرد، إضافة إلى ضرورة احترام حرمة المسكن وسرية الاتصالات، وافتراض مبدأ قرينة البراءة.

هذه الضمانات التشريعية والدستورية، والتي فرضها المشرع وإن كانت ضرورية لاحترام الإنسان إلا أنها

[9] عبد القادر القحطاني: *الجرائم المعلوماتية: دراسة مقارنة في القانونين الجنائيين التقليدي والمعلوماتي، دار الفكر الجامعي*، الإسكندرية، الطبعة الثانية، 2018، ص. 77–80.

[10] سلوى التوي: الحماية الجزائية للحياة الخاصة، مذكرة ماجيستر، كلية الحقوق والعلوم السياسية بتونس، 1996-1997، ص 72.

[11] Jean Pradel*: Droit pénal spécial,* 20e édition, Cujas, Paris, 2020, p. 615–618.

وبالنظر إلى طبيعة الجريمة في المجال المعلوماتي لم توفر الحماية الكافية لحقوق الأفراد حيث أفرز تطبيق النص الجنائي عديد الإشكاليات والخروقات القانونية، مثل شرط الإذن بالتفتيش، والمساس بالحياة الخاصة للمتهم ووضعية جريمة الشروع وهو ما سنتناوله في النقاط التالية:

أ. شرط وجود الإذن بالتفتيش:

يعرف التفتيش بأنه "الاطلاع على محلّ منحه القانون حرمة خاصة وذلك من أجل كشف الحقيقة عن جريمة معينة[12]"، وبالتالي فإن هدف التفتيش هو الكشف عن الحقيقة، والعثور عن أشياء تساعد على إظهارها[13]، وهو من صلاحيات ضباط الشرطة القضائية ووكلائهم سواء كان ذلك بإشراف من وكيل الجمهورية أو بصورة تلقائية،[14] وذلك حسب مقتضيات المادة 67 من مجلة الإجراءات الجنائية الموريتانية، كما حددت نفس المجلة أوقاتاً خاصة للتفتيش فيما عدا الحالات التي ينص عليها القانون، غير أن تطبيق التفتيش في العالم الواقعي يختلف عن التفتيش في العالم الافتراضي، الشيء الذي لم يتفطن اليه المشرع الموريتاني، ذلك أنه على سبيل المثال في حالة وجود جريمة معلوماتية معينة، وكانت اللحظة تقتضي الوصول إلى بيانات معينة مطلوبة في نظام معلوماتي داخل التراب الوطني، فإنه لا يمكن الوصول إليها مباشرة، إذ أن تمديد التفتيش إليها بصفة سريعة غير ممكن إلا إذا كان ذلك جائزاً قانوناً، أي خضوع التفتيش الإلكتروني لقواعد التفتيش التقليدية التي نظمتها مجلة الإجراءات الجنائية بقواعدها الشكلية والموضوعية، وهو ما يعني أن عدم احترام شروط التفتيش قد يترتب عنه بطلان الإجراءات.

هذ الشرط قد يحد من نجاعة القانون الجنائي، إذ أن التفتيش في المجال المعلوماتي حين يخضع للشروط التقليدية للتفتيش، فإنه قد يوفر فرصة للجناة، وبالتالي بإمكانهم تدمير الآثار، وإخفائها، وبالتالي الإفلات من العقاب، لذلك كان على المشرع منح صلاحيات أكثر توسعاً من مجرد تمديد التفتيش، مثل ما ذهب إليه المشرع اليوناني في المادة 251 من مجلة الإجراءات الجنائية إذ تخول هذه المادة للسلطات إمكانية القيام بأي شيء ضروري لجمع وحماية الدليل الجنائي. [15]

ويفسر الفقه الجنائي عبارة أي شيء بأنها تمتد لتشمل ضبط البيانات المخزنة في الذاكرة الداخلية للحاسب الآلي. [16]

---

[12] فتحي محمد أنور عزت: الأدلة الإلكترونية، في المسائل الجنائية والمعاملات المدنية، دار الفكر والقانون للنشر والتوزيع، الطبعة 1، القاهرة، 2010 ص 664.

[13] مساهمة الوفد التونسي في المؤتمر التاسع لرؤساء المحاكم العليا: مرجع سابق، ص 21.

[14] الأمر القانوني رقم 2007-036 المؤرخ في 17 أبريل 2007 يتضمن مراجعة قانون الإجراءات الجزائية.

[15] **jean-Baptiste Perrier**: *La perquisition numérique et les garanties procédurales,* Revue de science criminelle, Dalloz, Paris, 2018, pp. **412.**

[16] **حمد جلال أبو زيد:** *التفتيش الإلكتروني في ضوء الفقه والقضاء: دراسة مقارن* دار الجامعة الجديدة، الإسكندرية، الطبعة 1 2020، ص145.

ومن الأمثلة على قصور النص الجنائي الموريتاني حين يتعلق الأمر بالتفتيش الإلكتروني ما نصت عليه المادة 75 من قانون حماية المعطيات ذات الطابع الشخصي رقم 020-2017 الصادر بتاريخ 15 نوفمبر 2017 ..أنه في حالة اعتراض مسؤول الأماكن لا يمكن التفتيش إلا بإذن من السلطة القضائية المختصة التي يقع الأماكن المراد تفتيشها في دائرة اختصاصها ..."[17]، فتوقف شرط التفتيش على إذن من السلطة القضائية يحد من نجاعة التفتيش، إذ كان على المشرع أن ينص على أن التفتيش أو الإذن به يمكن أن يكون شفهيا وهو ما يتماشى مع طابع السرعة الذي تتميز به الجريمة المعلوماتية، وفي هذا الإطار نذكر بالأسلوب الأمريكي لتنفيذ عملية تفتيش نظم الحاسب الآلي، وهو اقتحام المكان بصورة سريعة ومن كافة منافده، وإبعاد المشتبه فيه عن كافة أنظمة ومعدات الكومبيوتر المتواجدة في المكان على الفور حتى لا يتمكنوا من تشويه أو تدمير أي دليل إلكتروني،[18] ويتم إدخال المشتبه فيهم إلى غرفة لا توجد بها أية أجهزة الكومبيوتر، إضافة إلى الحراسة المشددة وفي هذه الحالة يتم تقديم إذن التفتيش الصادر من النيابة إليهم. [19]

نخلص إلا أن الإذن بالتفتيش في المجال المعلوماتي والذي عادة يكون محله البرامج والكيانات المنطقية والبيانات المسجلة في ذاكرة الحاسب، أو مخرجاتها أو في دفتر يومية التشغيل، وسجل المعاملات، أن يحظى بصلاحيات أوسع للسلطة القضائية حتى لا يحدّ ذلك من غاية التفتيش[20]، داخل الأنظمة المعلوماتية، والتي تهدف أساساً في استرداد ما تحتويه تلك البيانات والمعلومات المخزنة داخل نظام معلوماتي معين أو في جزء منه وهو ما يتطلب إجراء خاص وموسعاً. [21]

ب. المساس بالحياة الخاصة للمتهم:

الحق في السرية والحياة الخاصة من الحقوق الدستورية التي كرسّها المشرع الموريتاني في الفقرة الأخيرة من المادة 13 من الدستور" ..تصون الدولة شرف المواطن وحياته الخاصة وحرمة شخصه ومسكنه ومراسلاته... "[22] وكذلك المادة 12 من الإعلان العالي لحقوق الإنسان "لا يعرض أحد لتدخل تعسفي في حياته الخاصة أو أسرته أو مسكنه أو مراسلاته"[23]، إضافة إلى بعض القوانين الأخرى التي كرست حرمة السريّة للفرد سواء الحق في حرمة المسكن أو سريّة الاتصالات، ومن هذه القوانين مثل القانون حماية الطفل، وقانون حماية المعطيات الشخصية، وقانون الاتصالات التي توفر كلها حماية الأفراد في خصوصيتهم من حيث حفظ البيانات الشخصية، وحظر الاستماع أو رصد محتوى

[17] المادة 74 من قانون حماية المعطيات الشخصية رقم 020-2017 الصادر بتاريخ 15 نوفمبر 2017.
[18] مصطفى مجدي هرجة: التفتيش في الجرائم المعلوماتية: دراسة مقارنة بين القانونين المصري والفرنسي، دار النهضة العربية، القاهرة، الطبعة الأولى، 2019، ص. 112–115.
[19] عبد الفتاح بيومي حجازي: مبادئ الإجراءات الجنائية في جرائم الكومبيوتر والانترنت، درا الكتب القانونية، القاهرة، 2007، ص 390.
[20] علي عدنان الفيل: إجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية، الإسكندرية، 2011، ص 40.
[21] فتحي محمد أنورت عزّت: مرجع سابق، ص 642.
[22] المادة 13 من دستور الجمهورية الإسلامية الموريتانية الصادر بموجب الأمر القانوني رقم 91-022 بتاريخ 20 يوليو 1991.
[23] المادة 12 من الإعلان العالمي لحقوق الإنسان.

الاتصالات الهاتفية أو نقلها أو استخدامها أو الكشف عنها بدون ترخيص قضائي.

هذا الزخم التشريعي الذي أحاط به المشرع سرية الحياة الخاصة للأفراد لم يكن بتلك القوة، إذ أنه وتماشياً مع طبيعة جرائم التكنلوجيا الحديثة منح المشرع بعض الصلاحيات الواسعة للسلطة القضائية في المواد 45 و46 في القانون رقم 2016-007 الصادر بتاريخ 20 يناير 2016 المتعلق بالجريمة المعلوماتية[24]، وكذلك في المادة 40 من قانون مكافحة غسل الأموال وتمويل الإرهاب رقم 2019-07 الصادر بتاريخ 20 فبراير 2019 التي قد تشكل اعتداء على سرية الاتصالات وعلى الحياة الخاصة للمتهم والتي هي محمية دستورياً وقانونياً. [25]

فالمشرع وإن كان نجح في فرض حماية خاصة لسرية ومراسلات المتهم، إلا أنه أغفل جوانب أخرى، والتي تتمثل أساساً في كيفية في سن قواعد تضمن بشكل كبير ضبط محكم لمشروعية التنصت الهاتفي بإجراءات أكثر احتراماً للفرد ولعائلته.

ولئن كان المشرع قد منح حق التنصت الهاتفي على المتهم من طرف قاضي التحقيق أومن ينوبه مثل قاضي التحقيق، لكنه لم يبين كيفية ذلك، بل أنه منح ذلك الإجراء لسلطات البحث بشكل عام دون إلزامهم باحترام الكثير من الشروط التي قد تضمن حسن سير عملية التنصت الهاتفي، وهو ما قد ينجر عنه تعسف في حق المتهم وبالتالي خرق الضمانات الدستورية والقانونية.

هذ الفراغ التشريعي يجب عليه تداركه، مثلما سارت عليه التشريعات الأخرى[26] فمثلاً المشرع الجزائري وضح طريقة التنصت الهاتفي بطريقة أكثر تفصيلاً ودقة وهو ما من شأنه ضمان حقوق المتهم، إذ يحرّر ضابط الشرطة القضائية أو المأذون له من طرف قاضي التحقيق المختص محضر عن كل عملية اعتراض للمراسلات وتسجيل الأصوات والتقاط للصور، كما يذكر ضابط الشرطة القضائية المأذون له في المحضر تاريخ وساعة بداية هذه العمليات والانتهاء منها، بحيث يشمل المحضر على كل البيانات المذكورة سابقاً، وأن تكون محددة "تحديداً نافياً للجهالة وبحيث أن يشتمل المحضر على توقيع محرره في نهايته" إضافة إلى أن تضمن أو تنسخ هذه البيانات وتضاف إلى ملف المتهم، وترجمتها إن اقتضت الضرورة ذلك. [27]

إن مثل هذه الإجراءات وضرورة التنصيص عليها كان المشرع الموريتاني أن يضمنه في القوانين الجنائية المتعلقة بجرائم التكنلوجيا الحديثة حماية للمتهم، باعتبار أن استراق السمع والتنصت الهاتفي من الإجراءات والخطيرة والتي يجب عند تشريعها وضع ضمانات حقيقية. [28]

---

[24] القانون رقم 2016-007 الصادر بتاريخ 20 يناير 2016 المتعلق بالجريمة المعلوماتية. المواد 45 و46 من

[25] المادة 40 من قانون مكافحة غسل الأموال وتمويل الإرهاب رقم 2019-07 الصادر بتاريخ 20 فبراير 2019.

[26] **Pierre Truche & Jacques Buisson**, *Les interceptions des communications et les libertés fondamentales*, editions Dalloz, Paris, 2017, pp. **210–214**.

[27] أمحمد أبو زينة أمنة: مرجع سابق، ص 70.

[28] عبد الفتاح بيومي حجازي: مرجع سابق، ص 374.

ت. وضعية جريمة الشروع في جرائم التكنلوجيا:

يعتبر من النتائج الخطيرة لعدم وضوح الركن المادي في هذا النوع من الجرائم، هي وضعية المحاولة أو الشروع في الجريمة المعلوماتية. [29]

إن جريمة الشروع مبدئياً لا تكون مناطاً للعقاب إلا إذا توفرت أركان ثلاثة أولها البدء في التنفيذ أو العدول عنه لأسباب خارجة الإرادة، واتجاه النية إلى ارتكاب الجريمة، وهو ما يعني بطبيعة الحال أن الركن المادي في الشروع ناقص عن الركن المادي في الجريمة التامة.

فهذه الأخيرة تكون مستوفية للأركان في حين أن المحاولة تكون ناقصة لتخلف أحد أركانها وهو النتيجة أو الأثر المترتب عن عنها. [30]

غير أن المشرع الموريتاني في إطار الجريمة المعلوماتية لم يلتزم بهذه المبادئ بل سوى بين الشروع والجريمة التامة، وبذلك يخرج عن القواعد الأصولية للقانون الجنائي، ومن ذلك ما جاء في قانون غسل الأموال وتحديداً المادة 2 حيث عدد الأفعال المكونة لجريمة غسل الأموال واعتبر أن الشروع فيها كالجريمة ذاتها. [31]

وهو ما نجده أيضاً في جريمة المحاولة إلى النفاذ إلى النظام المعلوماتي في المادة 6 من رقم 2016-007 من القانون المتعلق بالجريمة المعلوماتية على أنه "كل من يقوم أو يحاول القيام عن قصد وبدون حق بالنفاذ إلى كل أو جزء من نظام معلوماتي يعاقب...". [32]

لا يخفى من هذه النصوص القانونية تبني المشرع لفكرة المساواة بين المحاولة والجريمة التامة في إطار جرائم التكنلوجيا الحديثة، وهو توجه غير سليم خصوصاً في أن هذه الجرائم تتميز بطابعها الشكلي، أي أنها تقوم بمجرد صدور السلوك المجرد الذي لا نتيجة فيها، فيرى بعض الفقه أنها في جوهرها تعد شروعاً ولا يمكن تصور الشروع في الشروع أو المحاولة داخل المحاولة.

الشيء الأكيد أن الاعتبار الذي بنى عليها المشرع رؤيته ربما يعود في المقام الأول إلى أسباب لعل من أبرزها في المقام الأول هو رغبة المشرع في تبني منهج وقائي من الجريمة، غير أن ما يثير الإشكال أكثر هو أن المحاولة لا يمكن تصورها في جميع الحالات ذلك أنه في بعض الجرائم التقنية لا يمكن تصور الشروع وذلك لمانع يتعلق بالركن المادي للجريمة ذاتها،[33] فالذي أكّده الفقه وأجمع عليه أن الشروع في الجريمة لا يمكن تصوره في الجرائم السلبية أو جرائم الامتناع بحجة أنّها جرائم تحصل بمجرد الامتناع دون التوقف على نتيجة محددة أو ضرر معين بذاته. [34]

---

[29] **Hervé Croze**, *Le droit pénal des technologies de l'information*, Éditions LexisNexis, Paris, 2019, pp. **157–160**.

[30] القاضي مصطفي اليحياوي: المحاولة الإجرامية، دراسة مقارنة على ضوء القانون وفقه القضاء، اوروبيس للطباعة، ط1، تونس، 1998، ص11.

[31] المادة 2 من القانون 2019-017 الصادر بتاريخ 20 يناير 2019 المتعلق بمكافحة غسل الأموال.

[32] المادة 6 من القانون رقم 2016-007 الصادر بتاريخ 20 يناير 2016 المتعلق بالجريمة المعلوماتية.

[33] القاضي مصطفى اليحياوي: المرجع السابق، ص11.

[34] محمود داوود يعقوب: المسؤولية في القانون الاقتصادي، دراسة مقارنة بين القوانين العربية والقانون الفرنسي، منشورات الحلبي الحقوقية، بيروت، 2008، ص 86.

الفقرة الثانية: حدود فرضها أطراف الجريمة:

إن خصوصية هذا النوع من الجرائم المستحدث ألقى بظلاله أيضاً على أطراف الجريمة مما شكل تحدياً آخر للقانون الجنائي من حيث عقلية الضحية، وكذلك نوعية الجاني، الشيء الذي يفرض بعض الحدود الموضوعية المتعلقة بأطراف الجريمة.

أ. مهارة المجرم المعلوماتي:

تشكل مهارة المجرم المعلوماتي عائقاً أمام نجاعة وفاعلية القانون الجنائي الموريتاني في مواجهة جرائم التكنلوجيا الحديثة، نظراً إلى الصفات التي تميزه عن غيره، فهو يتميز بالذكاء المفرط، فعادة ما يكون من الحاصلين على الشهادات العلمية، ومن النوابغ، ولعل أشهر مثال على ذلك هو الطالب الأمريكي LAN MURPHY الذي عمد سنة 1981 صحبة البعض من أصدقائه إلى استعمال خط هاتفي للدخول إلى الملفات المخزنة بكومبيوتر الحكومة الأمريكية والاطلاع على معلومات سريّة. [35]

كما أن المجرم المعلوماتي له القدرة الفائقة على اختراق الشبكات وكسر كلمات المرور أو الشفرات[36]، إذ عادة ما يوظف مهارته في كيفية عمل الحواسيب، وكيفية تخزين البيانات والتحكم في أنظمة الشبكة والدخول غير المصرح به إلى الأنظمة المعلوماتية مرات ومرات فهو مجرم متعود يعود إلى الجريمة مرات ومرات إضافة إلى الاحترافية والذكاء، في تدمير المعطيات، وطمس الآثار. [37]

ومن الأمثلة على هؤلاء النوابغ في دولة تونس، فقد عرضت على أنظار القضاء القضية عدد 11772 المحكوم فيها بتاريخ 13-04-2005 والتي تفيد بأن بعض الموظفين بأحد البنوك التونسية استولوا على مبلغ 205 مليون دينار، مستغلين بذلك إشرافهم على أحد المصالح فروع البنك المذكور، إضافة إلى قضية البنك التونسي القطري للاستثمار والتي عرضت على القضاء وكان المجرم فيها قد تمكن وهو موظف بالبنك من الحصول على ثلاث مليارات من الميلمات من خلال إدخال تعديلات على الأنظمة المعلوماتية للبنك جعلت الموازنات المالية للبنك تظهره محقق للأرباح بينما هو متحمل لخسارة طائلة. [38]

ويتضح مما سبق القدرة الفائقة للمجرم المعلوماتي على ارتكاب الجرائم داخل الأنظمة المعلوماتية، كما أنه عادة ما يكون موظفا لدى البنوك والمؤسسات، الشيء الذي جعل المشرع الموريتاني يحمل المسؤولية الجزائية للذات المعنوية، في حالة عدم الانتباه والرقابة التي تؤدي إلى ارتكاب مثل هذه

[35] منية الزغلامي: الإثبات في جرائم الاتصال، رسالة ماجستير، كلية الحقوق والعلوم السياسية بتونس، 2007، ص 102.
[36] **Jean-Paul Pinte***: Cybercriminalité et compétences techniques des auteurs d'infractions* numerique, Éditions L'Harmattan, Paris, 2019, pp. **67–71**
[37] محمد علي قطب: الجرائم المعلوماتية وطرق مواجهتها، مركز الإعلام الأمني، الأكاديمية الملكية للشرطة، ص 10.
[38] الهاشمي الكسراوي: مرجع سابق.

الجرائم وفي هذا السياق تتنزل مقولة العميد CARBONNIER "إن تطور الأساليب والتقنيات يؤدي إلى ظهور إشكال حديثة وجديدة من الانحراف، وبالتالي تطور نوعية المجرمين" [39, 40].

فعادة ما يقوم المجرم المعلوماتي باختراق الأنظمة المعلوماتية بواسطة عدة طرق مثل قرصنة البرامج، وحصان طروادة المعروف، وهو زرع بعض الأوامر خلسة في برنامج معين، وهو برنامج يعدّ خصيصاً ليتم اقتحامه خفية في أحد برامج الكومبيوتر[41]، إضافة إلى القنابل المنطقية أو الموقوتة وهي عبارة عن برامج محمية تزرع داخل النظام المعلوماتي بحيث تبقى ساكنة وغير مكتشفة لمدة قد تصل إلى شهر، إضافة إلى تقنية "spamming" والتي تتمثل في تنفيذ هجمات ضدّ مواقع الواب وذلك بإرسال عدد هائل من الرسائل الإلكترونية بشكل يجعل الموقع عاجزا عن أداء مهمته ويجعلها تشتغل ببطء كبير. [42]

هذه إذا هي مواصفات ومهارات المجرم المعلوماتي، والتي هي نتيجة طبيعية لتطور وسائل التقنيات الحديثة، وظهور ما أصبح اليوم يعرف "délinquance informatique"[43] وهذه هي وسائله التي تستعملها في عالم لا مرئي بعيداً عن مراقبة الأجهزة الجنائية، الشيء يحد من نجاعة الحماية الجنائية نظراً إلى قدراته الخارقة، كما تشكل عقلية الضحية أو المجني عليه حداً من حدود الحماية الجنائية في التشريع الموريتاني.

ب. عقلية المتضرر في مجال جرائم التكنلوجيا الحديثة:

إن ما يزيد من صعوبة اكتشاف الجريمة، هو أن الضحية في المجال الافتراضي غالباً ما يكون مصرفاً أو بنكاً أو مؤسسات مالية، أو مشروعاً صناعياً ضخماً، ولذلك فإن مثل هذه المؤسسات عادة ما تلجأ إلى عدم الشكوى وعدم التبليغ عن الجرائم التي تلحق بها حرصاً على سمعة الشركة، ولذلك تلجأ للتكتم على هذه الاعتداءات، وهو ما يعرف بقانون الصمت "le droit du silence"، الشيء الذي جعل نسبة الشكاوى التي تقدم إلى المحاكم لا تتعدى نسبة 10% من الجرائم والتي تفطنت إليها المؤسسات. [44]

وكما ذكرنا سابقاً فإن حجم الخسائر المادية كبير جداً، ورغم ذلك فإن المؤسسات تتخير عدم التبليغ، ولا أدل على ذلك من حجم الخسائر التقديرات التي نشرها المركز الوطني لجرائم الحاسب

[39] Romain BOOS : la lutte contre la cybercriminalité au regard de l'action des Etats thèse Doctorat université de lorraine France 2016 P 23.

[40] منية الزغلامي: مرجع سابق، ص 103.

[41] حسن طاهر داوود: مرجع سابق، ص 24.

[42] منية بن ترايديت غمارسة: جرائم المعلوماتية في القانون التونس والقانون المقارن والقانون الدولي، دار الكتاب بتونس، 2015 تونس، ص 64.

[43] Romain BOOS op cite P 31.

[44] مروى عليمي: التحقيق في الجرائم المعلوماتية، شهادة لنيل مذكرة ماجيستر، كلية الحقوق والعلوم السياسية بتونس، 2013-2014، ص 49.

الآلي في الولايات المتحدة الأمريكية حوالي 500 مليون دولار سنوياً. [45]

هذه الإحصائيات لم تغير شيئاً في عقلية المجني عليه، إذ مازالت نسبة التبليغ أمام المحاكم ضئيلة جداً، وفي موريتانيا شبه منعدمة، إذ من خلال تواصلنا مع عديد شركات الاتصال والمؤسسات والبنوك، ترفض هذه المؤسسات مدنا بأي إحصائيات وأي مشاكل تعرضت لها من هذ القبيل، إذ تفصل التكتم على الاعتداء نظراً المنافسة، والضوابط المتعلقة بالتسويق التجاري[46]، كما أن هناك عامل آخر وراء تكتم المؤسسات على عملية قرصنة الأنظمة المعلوماتية، وهو أن الإفصاح عن عمليات بالاعتداء على هذه الأنظمة، قد يثير اهتمام المجرمين الناشطين في هذا المجال[47]، وهو عامل منطقي باعتبار أن المجرم المعلوماتي بمجرد سماعه لضعف الأنظمة المعلوماتية في مؤسسة معينة فإنه يتصيد لتلك الثغرات الأمنية ويجعلها هدفاً له، ولذلك فإن المؤسسات عادة ما تلجأ إلى الشخص الذي اخترق النظم المعلوماتية للمؤسسة وتطلب منه عدم الإفصاح عن هذ الاختراق، بل أنها تخضع لرغباته، إذ عادة ما يطلب الجاني من المؤسسة بعض الطلبات، وكمثال على ذلك الموظف الإنكليزي الذي تولى الاستيلاء على أموال طائلة من ثلاث مؤسسات كان يشرف على مصالح محاسبتها وفي كل مرة يقع اكتشاف أمره يطلب من صاحب المؤسسة أن يسلمه شهادة تخول له الحصول على عمل لدى شركات أخرى، وكان صاحب المؤسسة يستجيب لطلبه خوفاً من إفشاء الأمر، وقد أمكن له الحصول على حوالي أربعين ألف دولار من خلال تلك الأعمال. [48]

ومن العوامل التي ترتبط بعدم كشف الجريمة وتمثل صعوبة لأجهزة القانون الجنائي داخل هذه المؤسسات هي عدم إدراك خطورة هذه الجرائم من قبل المسئولين بالمؤسسات، وكذلك عدم معرفة مدراء الأنظمة الحاسوبية أو مسئولي الشركات أن مثل هذه الأفعال يشكل أفعالاً إجرامية يعاقب عليها القانون، كما أن الإفصاح عن التعرض لجريمة معينة واقعة على الأنظمة المعلوماتية قد يعرض الموظف نفسه للحرمان من وظيفته حين يتعرض لجريمة ناتجة عن اختراق الأنظمة المعلوماتية التي تحت رقابته أو إدارته[49]، ولذلك يلجأ مسئول الأنظمة المعلوماتية إلى التكتم على هذه الأفعال المرتكبة ضدّ الحاسب الآلي وهو ما يعرف "chiffre noir" حيث لا يعلم الضحية شيئاً عنها إلا عندما يكون هدفاً للعيش المعلوماتي، وحتى عندما يعلمون فإنهم يرفضون التبليغ. [50]

ويتضح من هذه العوامل أن عقلية المتضرر أو الضحية تشكل عائقاً للقانون الجنائي في إطار مواجهة الجرائم الحديثة، نظراً لهذه العوامل، وليست هذه العوامل وحدها التي تحد من اكتشاف الجريمة بل هناك صعوبة أخرى موضوعية المتعلقة بجهات التحقيق.

---

[45] سيدي طنطاوي: الجريمة المعلوماتية، المركز الديمقراطي العربي، 2018.

[46] Dominique Leprêtre: *Cybercriminalité et gestion des incidents dans les entreprises*, Éditions Dunod, Paris, 2018, pp. 92–

[47] مروى عليمي: مرجع سابق، ص 50.

[48] مروى عليمي: نفس المرجع، ص 52.

[49] علي عدنان الفيل: مرجع سابق، ص 80-83.

[50] عبد العالي الديربي، محمد صادق اسماعيل: مرجع سابق، ص 54.

المطلب الثاني: الحدود الموضوعية المرتبطة بجهات التحقيق:

إنّ النمط الحديث للجرائم المستحدثة والمرتبطة بالأنظمة المعلوماتية أفرز بعض الصعوبات الموضوعية المرتبطة بجهات التحقيق بكونها الجهاز القضائي المسئول عن البحث في ميدان هذا النوع من الجرائم، إذ أن هذا النمط الجديد من الجرائم المستحدثة لم يعدّ التبليغ عنه بالطرق المعروفة، ولم يعد المجرم ذلك المجرم المفتول العضلات والذي يحمل سلاحاً نارياً، بل إن المجرم أصبح يعيش في عالم افتراضي غير ملموس بعيداً عن المراقبة والتتبع، كما أن الضحية عادة ما يلجأ إلى التكتم والصمت، وكما أشرنا ليبقى عائق المسؤولية ملقى بدرجة كبيرة إلى جهات التحقيق، وهو ما أفرز صعوبات موضوعية مرتبطة بهذه الجهات مثل نقص الخبرة (فقرة 1) والإحجام عن تبليغ الاعتداءات (فقرة 2).

الفقرة الأولى: نقص خبرة جهات التحقيق:

يشكل المستوى المتدني لرجال الأمن والمتحققين في مجال التكنولوجيا خير معين لمرتكبي جرائم الحاسب الآلي، وقد أثبتت الوقائع أن هناك جرائم من جرائم الحاسب الآلي يتم ارتكابها على مرأى ومسمع من رجال الأمن بل قام بعض رجال الأمن والتحقيق بتقديم المساعدة لهؤلاء دون قصد وعن جهل[51]، ومن هنا يتأكد لنا الصعوبات الحقيقية التي تواجه جهات التحقيق للكشف عن هذه الجرائم، ولئن كان المشرع الموريتاني قد أوجب الاستعانة بشخص مؤهل في المجال المعلوماتي لضبط جرائم الحاسب الآلي في القانون رقم 2016-007 الصادر بتاريخ 20 يناير 2016 المتعلق بالجريمة المعلوماتية، إلاّ أن ذلك لا يكفي فمظاهر النقص التي تعاني منه هذه الجهات كثيرة وعديدة سنذكر منها لا الحصر:

- ضخامة المعلومات الموجودة على الشبكة مما يصعب معه التحقيق.
- الإنترنت بيئة خصبة للسلوك الإجرامي.
- التطور السريع للتقنية الجديدة. [52]
- نقص في المهارة الفنية للمحقق.
- عدم توفر المعرفة بأساليب الحاسب الإلكتروني لا سيما وأن للعاملين في مجال الحاسبة الإلكترونية مصطلحات علمية خاصة، ويستخدمون لغة متطورة في هذا المجال. [53]
- عدم تدريب جهات التحقيق.
- عدم اهتمام المحقق باستخدام وسائل الحديثة.
- عدم توفر الأجهزة المناسبة للتحقيق.
- ولهذا فقد اهتمت الكثير من الدول كما أسلفنا بجرائم الاعتداء الأنظمة المعلوماتية، وأحدثت مراكز متخصصة في المجال، ففي أمريكا توجد وحدة متخصصة في المجال من ضمن مكتب التحقيقات

[51] محمد الأمين البشري: التحقيق في جرائم الحاسب الآلي، المجلة العربية للدراسات الأمنية والتدريب، المجلد 15 العدد 3 الإمارات، ص 351.
[52] مروى عليمي: مرجع سابق، ص 54.
[53] علي عدنان الفيل: مرجع سابق ص 84.

الفيدرالي "FBI". [54]

- ومن أجل تخطي هذه المعوقات المرتبطة بجهات التحقيق فإن هذه الوحدة توصي جهات التحقيق باتباع بعض الخطوات.
- تبادل المعلومات بين المحقق وخبير الحاسبة الإلكترونية، وذلك قبل البدء في التحقيق، وأخذ أقوال الشهود، بحيث يشرح المحقق للخبير أهميته وطريقة توجيه الأسئلة إليهم، ومن جهة أخرى يقوم المحقق بشرح الأبعاد الفنية، والنقاط التي ينبغي استجلابها من الأشخاص.
- حصر النقاط المطلوب استجلابها من قبل الخبير والمحقق قبل البدء في التحقيق ليتولى المحقق بعد ذلك ترتيب النقاط.
- التنسيق بين المحقق والخبير في الحصول على البيانات المخزنة في النظام المعلوماتي[55]، كما يجب على الخبير المعلوماتي الذي يتم ندبه عن طريق جهات التحقيق أن يتوفر على بعض المهارات التالية:

  - اجتياز امتحان محلل الجرائم السبرانية. [56]
  - بكلوريا في نظم المعلوماتية.
  - خبرة عملية لا تقل عن أربع سنوات.

وعادة ما يكون هؤلاء مختصون في النظم المعلوماتية مثل أخصائي في الأمن السيبراني، محلّل اختصاص في الجرائم السبرانية وغيرهم. [57]

وتمثل هذه الحلول والخطوات عملية تكميلية بين جهات التحقيق والخبير المعلوماتي، إذ تكمل الخبرة نواقص جهات التحقيق، وبالتالي تشكيل فريق قادر على تجاوز مثل هذه الصعوبات، ولا يشكل نقص الخبرة عائق وحده لسلطات البحث، وإنما هناك عائق آخر يتمثل في الإحجام عن التبليغ.

الفقرة الثانية: الإحجام عن تبليغ الجرائم الافتراضية:

يشكل عدم الإبلاغ عن الاعتداءات على الأنظمة المعلوماتية عائقاً أمام كشف الجريمة، لأن الجريمة في المجال المعلوماتي لا تصل إلى سلطات التحقيق بالطرق التقليدية، وذلك لصعوبة اكتشافها من قبل الأشخاص أو المؤسسات، وبالتالي فإن الإحجام عن التبليغ من الطرف المعني، يجعل سلطات البحث تتحمل مسؤوليتها في ضبط هذا النوع من الجرائم، إذ تلجأ لرصد ميدان حركات المعاملات التجارية داخل المؤسسات وحولها، وذلك عن طريق جمع المعلومات السرية عن حركة وتداول الأموال والممتلكات[58]،

---

[54] سليمان مهجع العنزي: مرجع سابق ص 117.
[55] علي عدنان الفيل: مرجع سابق، ص 85.
[56] François Falletti: *Cybercriminalité et coopération judiciaire internationale, Revue* Internationale de Droit Pénal, Vol. 90, n°3, 2019, p. 545–548.
[57] محمد الأمين البشري: الأساليب الحديثة للتعامل مع الجرائم المستحدثة من طرف أجهزة العدالة الجنائية، محاضرة ألقيت في الحلقة العلمية (تحليل الجرائم المستحدثة والسلوك الإجرامي) الإمارات 2011، ص 22-23.
[58] عبد الفتاح بيومي حجازي: مرجع سابق، ص 114.

الشيء الذي يربط بين جهات التحقيق وعملية التتبع، لكي تتمكن من رصد الجرائم الواقعة على الأنظمة المعلوماتية، إذ أنه في الجريمة التقليدية يتم الإبلاغ عن طريق الشكوى بينما يتعقد الأمر في المجال المعلوماتي، ولذلك فإن هناك بعض المصادر على الجهات التحقيق أن ترصد حركة المجرمين فيها مثل أدلة الهاتف، حسابات البنوك سجلات العمليات البنكية، إعلانات إفلاس البنوك التاريخ المالي للأفراد والمؤسسات، سجلات المشتركين في الخدمات العامة، شركات التأمين وغيرها من مصادر التحقيق الجنائي في جرائم الإنترانت[59]، ولهذا فإن التبليغ عن هذه الجرائم في المجال المعلوماتي دائماً يكون بإحدى الطرق التالية:

- تلقي أجهزة التحقيق معلومات عن أشخاص يمارسون أنشطة تندرج تحت تعريف الجريمة المعلوماتية.
- توافر معلومات عن نشر فيروسات تخريبية عبر شبكة الإنترنت.
- توافر معلومات عن وقوع عمليات قرصنة قضائية للمعلومات. [60]

نخلص من ذلك إلى أهمية الإبلاغ عن الجريمة المعلوماتية في عمل التحقيق والاستدلال، إذ يمثل الإحجام عن الإبلاغ أهم وأخطر المشكلات التي تتعلق بعملية الإبلاغ، إذ يحجم البعض وخاصة الشركات والمؤسسات عن التبليغ عن الاعتداء ومن أجل تفعيل عملية الإبلاغ عن الجريمة المعلوماتية، ما طالب به البعض في الولايات المتحدة الأمريكية بأن تتضمن القوانين المتعلقة بجرائم الحاسب الآلي توصيات تلزم موظفي الجهة المجني عليها أياً كانت بضرورة إبلاغ عما يصل إلى علمهم من جرائم، إلا أنه ولدى عرض هذا المقترح على لجنة خبراء مجلس أوروبا[61] تم رفضه لسبب قانوني مؤداه أن المجني عليه وهو الشركة التي ارتكبت في حقها جريمة معلوماتية سوف تصبح متهمة بعد أن كانت مجنياً عليها، ولذلك وردت اقتراحات بديلة بلاغ جهة خاصة أو بإبلاغ سلطات إشرافية[62]، كما أنه من صعوبات الإبلاغ عن هذه الجرائم على نطاق دولي عدم وجود شبكة عالمية لتداول المعلومات الأمنية كما هو الحال في شبكة "يوريول" التي تعمل حالياً في إطار الشرطة الدولية بمعزل عن الشبكات العامة المستخدمة.

يلاحظ في هذا السياق غياب وكالة وطنية في موريتانيا معنية بالسلامة المعلوماتية، على غرار الموجود في تونس، والتي تم إنشاؤها بموجب القانون عدد 5 لسنة 2004 المؤرخ في 3 فيفري 2004، حيث تعدّ هذه الوكالة تقريراً سنوياً عن جرائم القرصنة على المؤسسات أو البنوك، وهو أمر قد يطرح حلا لمشكلة عدم الإبلاغ، وعلى المشرع الموريتاني أن يتجه على هذا النحو[63] إذ أن إحداث هيئة وطنية للسلامة المعلوماتية

---

[59] سليمان مهجع العنزي: مرجع سابق، ص 23.
[60] مروى عليمي: مرجع سابق، ص 52.
[61] Serge Sur & Olivier Cahn, *Cybercriminalité et droit international*, Presses Universitaires de France (PUF), Paris, 2018, p. 302.
[62] حمد بن عبد الله الفالح: *التعاون الدولي في مكافحة الجرائم المعلوماتية: دراسة مقارنة*، دار الميمان للنشر، الرياض، الطبعة/ الأولى، 2021، ص. 201–204.
[63] منية بن ترادیت غمارسة: مرجع سابق، ص 119.

في موريتانيا قد يضع حداً لمعضلة الصعوبات المتعلقة بالإبلاغ هذه الصعوبات الموضوعية التي تحدّ من الحماية الجنائية في القانون الموريتاني. [64]

وإلى جانب الصعوبات الموضوعية للقانون الجنائي الموريتاني في مواجهة جرائم التكنلوجيا الحديثة توجد صعوبات على المستوى الإجرائي.

المبحث الثاني: الصعوبات الإجرائية في مواجهة جرائم التكنلوجيا الحديثة

يشكل الطابع التقني لهذه الجرائم الحديثة عائقاً إجرائياً أم سلطات البحث والتتبع، إذ يختلف مسار التتبع في الجرائم في المجال المعلوماتي عن التتبع في الجرائم التقليدية، حيث أن الجريمة التقليدية يسهل الوقوف على آثارها المادية، ومعاينتها، وضبط الوسائل المادية المفيدة لإظهار الحقيقة، إضافة إلى أن الدليل المادي في الجرائم التقليدية يتمتع بقوة ثبوتية أمام القضاء، غير أن الأمر يختلف في المجال الافتراضي.

وبناء على ذلك سنخصص هذا المبحث للصعوبات المتعلقة بالحماية الإجرائية في المجال المعلوماتي، على أن يتم ذلك في مطلبين، (المطلب الأول) الصعوبات العملية على مستوى الإثبات، وفي (المطلب الثاني) الصعوبات الإجرائية العابرة للحدود.

المطلب الأول: صعوبات على مستوى الإثبات:

يفترض في أي جريمة أن تقوم سلطات الضابطة العدلية بمعاينة الجريمة وجمع الأدلة المتعلقة بالجريمة بغاية إظهار الحقيقة، وإدانة المجرمين، غير أن هذه الإجراءات تتعقد نوعاً ما في المجال المعلوماتي، وهو ما يطرح عدة صعوبات إجرائية تحد من فاعلية القانون الجنائي، وخصوصاً على مستوى الإثبات، وتتلخص تلك الصعوبات في صعوبة المعاينة (الفقرة الأولى) وكذلك في حالة المعاينة وضبط الأدلة، فإن الدليل ذاته يطرح بعض الصعوبات، صعوبات متعلقة بالدليل (الفقرة الثانية).

الفقرة الأولى: صعوبة المعاينة:

يعرف الفقه المعاينة بأنها "رؤية بالعين لمكان أو شخص أو شيء لإثبات حالة وضبط كل ما يلزم لكشف الحقيقة"[65]، وتبعاً لذلك فإن المعاينة الانتقال إلى عين المكان، أي إلى مسرح الجريمة، كما تعدّ المعاينة من أهم وسائل الإثبات[66]، غير أن المعاينة في جرائم التكنلوجيا الحديثة، تعرف بعض الصعوبات نظراً إلى الانتقال إلى مسرح الجريمة المعلوماتية والذي يتسم أحياناً بالصعوبة.

---

[64] Éric Caprioli*: La cybersécurité et la coopération internationale*, Éditions Larcier, Bruxelles, 2019, p. 415.

[65] مساهمة الوفد التونسي في مؤتمر بيروت لرؤساء محاكم العرب: مرجع سابق، ص 22.

[66] منية بن ترايديت غمارسة: مرجع سابق، ص 125.

وتتمثل هذه الصعوبة على مستويين، صعوبة تحديد مكان الجريمة (أ) وكذلك ضعف وسائل البحث التقليدية (ب).

أ. صعوبة تحديد مكان الجريمة:

حتى تتحقق المعاينة وتجني ثمارها، بعض التشريعات الجنائية تسلط عقاباً جنائياً على كل من يحدث تعديلاً أو تغييراً في مكان وقوع الجريمة[67]، غير أن مسرح الجريمة في المجال المعلوماتي هو مسرح افتراضي، وبالتالي يصعب تحديده، ورصده بدقة، وذلك نتيجة بعض الأسباب:

- السبب الأول: إن الجريمة المعلوماتية لا تخلف أثاراً مادية حيث يتم الاعتداء على برامج الحاسب الآلي.
- السبب الثاني: أن كثيراً من الأشخاص يترددون على مسرح الجريمة خلال الفترة الزمنية التي غالباً ما تكون طويلة نسبياً ما بين وقوع الجريمة وحتى اكتشافها، وهو ما يتيح الفرصة للجاني لكي يعبث أو يتلف، الآثار المادية للجريمة، مما يجعل تحديد مسرح الجريمة في الجرائم المعلوماتية في غاية الصعوبة[68]، ولذلك يرى البعض من الفقه الجنائي ضرورة تتبع عدة ضوابط عند معاينة مسرح الجريمة من قبل جهات التحقيق ومن تلك الضوابط ما نصت عليه اتفاقية بودابست للإجرام الإلكتروني، الحفظ السريع للبيات، والتقاط البيني[69] وغيرها من الإجراءات.

من جانبه يوصى خبراء الأمن المعلوماتي، بحفظ الأدلة الأصلية على حالتها أيضاً أخذ نسخ على وسائط جديدة ومؤمنة ولا تحمل أية بيانات سابقة، كما يجب حفظ الأدلة مرقمة وموثقة في جميع مراحل ضبطها، ونقصها، وحفظها[70]، كما يوصي خبراء الأمن المعلوماتي المحقق الجنائي، والخبير المعلوماتي الذي تنتدبه السلطة القضائية عند معاينة مسرح الجريمة إلى ضرورة امتلاك نظام كشف الاختراق Intrusion "Détection System، كما على المحقق ألا يضيع الوقت، وأن يعمل مع فريقه فور علومه بالحادثة، تنسيقاً واستشارة وتنفيذاً. [71]

ويتعين أيضاً عند مسرح الجريمة وضع اعتبارات أخرى ضرورة توفير معلومات مسبقة عن مكان الجريمة ونوع الأجهزة المتوقع مداهمتها، وكذلك مداهمة شبكاتها.

- حصر عدد أنواع الأجهزة المحتمل تورطها في الجريمة، وذلك لتحديد إمكانية التعامل معها من الناحية الفنية من حيث الضبط والتأمين وحفظ الملفات Back up إعداد خريطة للموقع الذي

---

[67] منية بن ترادیت غمارسة: نفس الصفحة.
[68] اتفاقية أوروبا للإجرام المعلوماتي.
[69] تفاقية بودابست لمكافحة الجريمة الإلكترونية **2001 (Convention on Cyber crime).**
[70] محمد لمين البشري: مرجع سابق، ص 39.
[71] Council of Europe: Convention on Cybercrime, Budapest, 23 November 2001.

تتم الإغارة عليه، وتحديد مواقع الأجهزة وأن يتم ذلك بسريّة تامة. [72]

- وضع حراسة كافية على مكان المعاينة ومراقبة التحركات داخل مسرح الجريمة، بل ورصد الاتصالات الهاتفية من وإلى مكان مسرح الجريمة مع إبطال مفعول أجهزة الهاتف الجوال التي قد ساعد بطريقة فنية في تدمير أدلة الجريمة المعلوماتية. [73]

ويجب التفريق في حالة معاينة مسرح الجريمة المعلوماتية بين حالتين:

- معاينة الجرائم الواقعة على المكونات المادية للحاسوب، كشاشة العرض ومفاتيح التشغيل والأقراص وغيرها من مكونات الحاسوب ذات الطابع المادي، وهذه الحالة لا تثير أي مشكلة بالنسبة لجهات التحقيق إذ يمكنهم التحفظ على الأشياء المادية.
- أما الحالة الثانية فهي معاينة الجرائم الواقعة على المكونات غير المادية للحاسوب (software) كتلك الواقعة على برامج الحاسوب وبياناته. [74]

هذه المكونات هي التي تثير صعوبة بالنسبة لمعاينة مسرح الجريمة فيها، ولذلك فإن المعاينة هنا ويجب أن تتم تحت إشراف، أو من طرف فريق متخصص أو الخبير المعلوماتي، ففي فرنسا هذه المهمة يتم تنفيذها عن طريق 13 شرطي مكونين في هذا المجال ويعرفون كيف يتصرفون مع البرامج والتطبيقات اللامادية داخل الحاسوب الآلي. [75]

نخلص من ذلك أن الجريمة في المجال المعلوماتي والتي ترتكب داخل الحاسب الآلي يصعب تحديد مسرح الجريمة فيها، وبالتالي ضبطها. [76]

إن صعوبة تحديد مسرح الجريمة ناتج عن الطبيعة الافتراضية للجريمة كما أنه أيضاً يصعب في حالة الاعتماد على وسائل البحث التقليدية.

ب. ضعف وسائل البحث التقليدية:

يقصد بوسائل البحث التقليدية التفتيش، والخبرة والشهادة والاختبار إن اقتضى الأمر، هذه تعد من الوسائل التقليدية الناجعة لاكتشاف الجريمة، غير أنها تصبح ضعيفة وغير ناجعة في مواجهة جرائم التكنلوجيا الحديثة.

ويتجلى هذا الضعف بوضوح حيث أنه مثلاً في التفتيش حسب القواعد العامة يخضع لضوابط زمنية معينة، وإن كان المشرع الموريتاني قد استحدث نظاماً جديداً للتفتيش إلا أنه لم يخرج عن

---

[72] عبد الفتاح بيومي حجازي: مرجع سابق، ص 187.
[73] منية بن ترايديت غمارسة: مرجع سابق، ص 126.
[74] براهيم، خالد ممدوح. *الدليل الجنائي الرقمي وحجيته في الإثبات*، الطبعة الأولى، الإسكندرية: دار الفكر الجامعي، 2021، ص. 52–57.
[75] أمحمدي بوزينة أمنة: مرجع سابق، ص 61-62.
[76] Ghernaouti-Hélie, Solang*: ،Cybercriminalité : comprendre, prévenir, réagir* ،1ère édition (Dunod) ،Paris: Dunod ، 2023 p. 140.

المبادئ العامة، وبالتالي لم ينص تشريعياً على ضرورة اعتبار التفتيش في الجريمة المعلوماتية غير خاضع للضوابط الزمنية، وهو اتجاه محل نقد، لأن التفتيش في الجرائم المعلوماتية لن يؤتي أكله إذا ظل مرتهنا لنفس القواعد التقليدية.

- **الشهادة:** وهي من الوسائل التقليدية لسلطات البحث، وتعرف بأنها "الأقوال التي يدلى بها غير الخصوم أمام سلطة تحقيق بشأن جريمة وقعت سواء كانت تتعلق بثبوت الجريمة وظروف ارتكابها أو إسنادها إلى متهم أو براءته منها[77]" ولهذا فإن العثور على شاهد يعتبر مكسباً كبيراً للعدالة، غير أن الشهادة في المجال المعلوماتي تختلف عن الشهادة في الجريمة التقليدية. [78]

فالشاهد في الجريمة المعلوماتية هو صاحب الخبرة والذي تكون لديه معلومات جوهرية وهامة وضرورية للولوج في نظام المعالجة الآلية للبيانات[79]، إذا كانت مصلحة التحقيق تقتضي ذلك ويطلق عليه "الشاهد المعلوماتي" ويشمل الشاهد المعلوماتي بهذا المفهوم عدة طوائف:

1. القائم على تشغيل المحاسبة الإلكترونية.
2. المبرمجون.
3. المحللون.
4. مهندسو الاتصالات. [80]

ويختلف الخبير المعلوماتي عن الشاهد المعلوماتي، فالشاهد يقدم إلى القاضي معلومات حصلها بالملاحظة الحسيّة، أما الخبير فإنه يقدم إلى القاضي تقارير توصل إليها بتطبيق قوانين علمية.

وقد يجمع الشخص بين صفتي الشاهد والخبير وأثير إشكال يتعلق بمدى إجبار الشاهد المعلوماتي على تقديم دليل فني يتعلق بالجريمة؟ أي هل على الشاهد المعلوماتي القائم على نظام معلوماتي أن يدلي بالكشف عن الشفرات أو كلمات السير التي يكون علم بها[81]، وهناك اتجاهين في هذا الصدد:

- **الاتجاه الأول:** يرى أنه ليس من واجب الشاهد المعلوماتي الإفصاح عن كلمات المرو ر الخاصة، وهذا الاتجاه يميل إليه الفقه الألماني الذي يرى أن الالتزام بأداء الشاهد لا يتضمن هذا الواجب.
- **الاتجاه الثاني:** ويميل إليه الفقه الجنائي الفرنسي حيث يرى الفقه الفرنسي أن القواعد في مجال الإجراءات الجنائية تحتفظ لسلطانها في مجال المعلوماتية، ومن ثم يتعين على الشهود من حيث المبدأ الالتزام بتقديم شهادتهم، ومن ثم يجب عليهم الإفصاح عن كلمات السرّ والمرور التي يعلمون بها، غير أن الفقه الجنائي الفرنسي يرى أن رفض إعطاء المعلومات المطلوبة غير معاقب

---

[77] علي عدنان الفيل: مرجع سابق، ص 61.
[78] مصطفى محمد موسى: *التحقيق الجنائي في الجرائم المعلوماتية: أساليب وتقنيات*، دار النهضة العربية القاهرة، 2018، ص. 72–78.
[79] Jean-Michel Bruguière*: La criminalistique numérique : principes et pratiques*, L'Harmattan, Paris, 2020, p. 101–107.
[80] علي عدنان الفيل: مرجع سابق، ص 62-63.
[81] عبد الفتاح بيومي حجازي: مرجع سابق، ص 37.

عليه جنائيا إلاّ في مرحلة التحقيق والمحاكمة. [82]

نخلص من ذلك أن الوسائل التقليدية للكشف عن الجريمة مثل المعاينة والحجز والتفتيش، والشهادة، أصبحت غير ناجعة في المجال المعلوماتي، وهوما يتعين على السلطات القضائية أن تنظر فيه بجدية، حيث لا مناص في المجال المعلوماتي من تدريب سلطات البحث والتحقيق على هذا النمط الجديد من الجرائم المستحدثة، حتى يتمكن رجال الشرطة القضائية من تجاوز هذه الصعوبات.

وتقابل هذه الصعوبات على مستوى صعوبة المعاينة صعوبات أخرى تتمثل في الدليل ذاته.

الفقرة الثانية: صعوبات متعلقة بالدليل الإلكتروني:

يعرف الدليل الجنائي بأنه "هو الوسيلة التي يستعين بها القاضي للوصول إلى اليقين القضائي الذي يقيم عليه حكمه في ثبوت الاتهام المعروض عليه". [83]

ويتبين من هذا التعريف أهمية الدليل في حسم الدعوى الجنائية المعروضة على القضاء، ولا يثير الدليل في الجريمة التقليدية كبير إشكال، إذ أنه يتجسد غالباً في وسائل مادية مثل ضبط أدوات الجريمة كالأسلحة النارية، وآلات القتل، وغيرها[84]، غير أنه في المجال المعلوماتي لم يعد الدليل مرئياً ملموساً[85]، كما أنه لم يعد بتلك القوة الثبوتية، وهو ما يطرح عدة عوائق تتعلق أولاً بخفاء الدليل (أ) وثانياً بنسبية حجية الدليل (ب).

أ. خفاء الدليل الإلكتروني:

يشكل خفاء الدليل الإلكتروني عائقاً حقيقياً أم سلطات البحث، فالدليل له أهمية كبرى في سائر الدعوى الجنائية، لذلك فإن خفاءه في عالم افتراضي، وسرعة طمسه، يعقد مهمة جهات البحث، نظراً إلى نقص الخبرة، وعدم التكوين المستمر في مجال الحاسب الآلي.

ويرى جانب من الفقه الجنائي أن متطلبات العدالة الجنائية تفرض على أجهزة الدولة أن تتحمل كامل مسؤوليتها نحو اكتشاف الجرائم وضبط المجرمين، ومحاكمتهم. [86]

إن هذه المسؤولية تبقى محدودة وخصوصاً حين يتعلق الأمر بالدليل الإلكتروني، وعدم وضوحه وعدم رؤيته، فهو دليل افتراضي غير ملموس ويعرفه البعض بأنه "الدليل الذي يجد له أساساً في العالم الافتراضي ويقود إلى الجريمة". [87]

---

[82] علي عدنان الفيل: مرجع سابق، ص 65.
[83] تشوار جيلاني: مرجع سابق، ص 256.
[84] أحمد فتحي سرور، *الوسيط في قانون الإجراءات الجنائية*، دار النهضة العربية، القاهرة، الطبعة السابعة، 2015، ص 312.
[85] Jean Pradel, *Procédure pénale*, Éditions Cujas, Paris, 2018, pp. 245.
[86] مصطفى محمد موسى: *التحقيق الجنائي في الجرائم المعلوماتية: أساليب وتقنيات*، دار النهضة العربية، القاهرة، 2018، ص. 85–90.
[87] فتحي محمد أنورت عزت: مرجع سابق، ص 635.

ويعرفه البعض الآخر "بأنه مجموعة البيانات والمعطيات التي يتم جمعها وحفظها بواسطة الأنظمة المعلوماتية أو الإلكترونية والتي من شأنها أن تكون صالحة للاستدلال أمام القضاء"...[88]".

ويتلخص من هذه التعريفات أن الدليل في المجال المعلوماتي هو دليل افتراضي يتم استخلاصه بواسطة الأنظمة المعلوماتية، وبالتالي تكمن صعوبة رصده واستخلاصه، والاستعانة بالدليل الرقمي في عالم افتراضي، يثير بعض الصعوبات المتعلقة بعدم تطابق الدليل الرقمي مع الصيغة التقليدية للدليل القانوني، سيما إذا علمنا أن الدليل الذي يتم استنباطه في إطار المعلوماتية إنما هو دليل مستوحى من قاعدة مجهولة أو خوادم غامضة ليس من السهولة التوصل إليها. [89]

وحتى إذا كان المشرع الموريتاني قد اعترف بالدليل الإلكتروني في بعض القوانين التي نذكر منها القانون رقم 2018-022 المتعلق بالمعاملات الإلكترونية وتحديداً في المادة 16 وكذلك في الأمر القانوني رقم 2006-031 المتعلق بوسائل الدفع وعمليات التجارة الإلكترونية، غير أن الصعوبة تكمن في طبيعة الدليل وصعوبة استخلاصه.

فالمجرم المعلوماتي يمكنه في إطار البيئة المعلوماتية وعن طريق نبضات إلكترونية يمكنه العبث في بيانات الحاسب وبرامجه وذلك في وقت قياسي، وهذه البيانات التي يتم العبث بها قد يتم محو الدليل منها في زمن قياسي أيضاً قبل أن تصل آلية يد العدالة، سيما وأن عملية الضبط لا تتم إلاّ عن طريق خبير أو فني متخصص. [90]

نستخلص مما سبق أن الدليل في إطار الجريمة المعلوماتية هو دليل غير مرئي وخفي وهو ما يطرح عدة صعوبات على مستوى الإثبات والبحث عن أدلة الجريمة، كما أن الدليل الرقمي لا يتمتع بتلك القوة الثبوتية، وهو ما يشكل صعوبة أخرى.

ب. نسبية حجية الدليل الإلكتروني:

اعتماداً على مبدأ حرية الإثبات في المادة الجنائية فإنه يمكن الاستناد إلى أي دليل يساعد في كشف الحقيقة سواء كان دليلاً مادياً **"أو إلكترونياً".**

وقد ذهب الأستاذ "أسوانسوان" إلى أن الدليل يجب أن يخضع للشروط التالية:

1. تحديد ما يعد دليلاً وتعينه وارتباطه بالمسألة المطلوبة إثباتها أو نفيها.
2. أن يكون مقبولاً لدى المحكمة.
3. أن يكون قوياً ومؤثراً.
4. أن يكون مشروعاً.

[88] مساهمة الوفد التونسي في مؤتمر رؤساء محاكم التعقيب: مرجع سابق، ص 23.
[89] فتحي محمد أنورت عزت: نفس المرجع، ص637.
[90] عبد الفتاح بيومي حجازي: مرجع سابق، ص 67.

5. أن يتم الحصول عليه بطريقة مشروعة. [91]

ولعل هذا الشرط الأخير بقبول الدليل والاعتراف به يعدّ عائقاً أمام الاعتراف بحجية الأدلة المستخرجة من وسائل الاتصال، نظراً إلى أن الدليل قد يكون استخراجه في مجال المعلوماتية بشكل غير مشروع، وخصوصاً إذا تعلق الأمر بالحياة الشخصية للأفراد.

وفي هذا السياق في فقه القضاء المقارن نذكر قضية "Sacrafo" حيث قامت المباحث الأمريكية الفيدرالية "FBI" بطلب إذن مراقبة حاسوب المدعو "Sacrafo" لكونه يتعامل بالإنترنت بشكل إجرامي، وحين تقدمت بطلب إذن لكي تجري هذه المراقبة على حساب المدعو رفض القاضي الدليل المستمد من هذه المراقبة لكونها تشكل اعتداء على الحياة الخاصة. [92]

ومن المسلم به في القانون الجنائي أن سلطة القاضي في تقدير الأدلة يحكمها مبدأ الاقتناع الشخصي للقاضي الجنائي أو حريته في تكون قناعته، فالقاضي يجوز له تقدير الأدلة المطروحة أمامه، لكن بشروط أن يكون الدليل معترف به قانوناً.

إن مسألة تقدير الأدلة هي مسألة موضوعية لأن الأدلة جميعها لا تخطر أمام القاضي الجنائي بالقوة الحاسمة في الإثبات بل تخضع لقناعته بها، وهو ما يصعب في الدليل الإلكتروني، نظراً إلى أن الدليل الإلكتروني هو دليل مستوحى من قاعدة مجهولة والقاضي الجنائي هو رجل قانون يفتقد للثقافة المعلوماتية والتقنية، وهو ما يحتم عليه الاستعانة بالخبرة الفنية التي قد يعطي للدليل الإلكتروني قيمة في الإثبات مع وجود احتمالات الخطأ الواردة علمياً وفنياً.

ومع احتمال خطأ الوارد من قبل الخبير المعلوماتي، ونقص الثقافة المعلوماتية للقاضي الجنائي، فهل سيكون للدليل الإلكتروني تأثيره على قناعة القاضي؟ [93]

نلخص من ذلك أن الدليل الرقمي لا يرقى إلى الدرجة التي يرقى إليها الدليل المادي، ولهذا فإن الفقه الجنائي استثارته هذه النقطة في إبراز أهمية قبول الدليل الرقمي المستمد من آلات غير ذكية، كما هو الشأن في كاميرات المراقبة وغيرها وهي أدلة مقبولة أمام المحاكم. [94]

ولعل هذا ما جعل الاتحاد الأوروبي منذ منتصف الثمانيات يوجه نداءً إلى الدول الأوروبية للاعتراف بالوثيقة الإلكترونية، والإقرار بحجيتها ومساواتها بالوثائق الكتابية من حيث الحكم.

وفي هذا الإطار اعترف المشرع الأردني بالمستخرجات الإلكترونية في قانون الأوراق المالية رقم 23 لسنة 1997[95]، وفي تونس فقد اعترف المشرع بالوثيقة الإلكترونية في القانون عدد 53 سنة 2000

[91] منية الزغلامي: مرجع سابق، ص 82.
[92] فتحي محمد أنورت عزت: مرجع سابق، ص 636.
[93] تشوار الجيلاني: مرجع سابق، ص 268.
[94] فتحي محمد أنورت عزت: مرجع سابق، ص 639.
[95] منية الزغلامي: مرجع سابق، ص 84.

والمؤرخ في 13 جوان 2000، كما اعترفت محكمة التعقيب التونسية بالفاكس كوسيلة إثبات صلب القرار التعقيبي مدني تحت عدد 271. [96]

أما بالنسبة إلى الأدلة الناتجة عن عملية التنصت الهاتفي والتسجيل الخفي بواسطة جهاز الالتقاط، فإن الدولة المصرية تعتبر أن الدليل المستمد من التنصت الهاتفي مقبولاً متى تم وفقاً للقانون، كما أن التسجيل الصوتي بشكل عام مقبول إذا كان قد تم في محل عام.

وقد جرمت المادة 409 من القانون الجنائي المصري استراق السمع أو التسجيل انقل المحادثات أو نقل صورة شخص في مكان خاص يغير رضاء المجني عليه. [97]

أما في موريتانيا تغيب حتى الآن الأحكام القضائية المتعلقة بالإثبات بالوسائل الإلكترونية لكن المشرع اعترف بالوثيقة الإلكترونية في أكثر من مناسبة، في المادة 2 من القانون رقم 031-2006 المتعلق بأدوات الأداء وعمليات التجارة الإلكترونية وكذلك في المادة 8 من القانون عدد 003-2011 المتضمن مدونة الحالة المدنية، والمادة 1 من القانون عدد 022-2018 المتعلق بالمبادلات الإلكترونية، والمادة 2 من القانون رقم 019-2019 المتعلق بمدونة التحكيم، كما أعطى للوثيقة الإلكترونية نفس القوة التي تتمتع بها الوثيقة الكتابية.

ويبقى الإشكال المطروح هو قبول الدليل المستمد من الحاسب الآلي ومدى اقتناع القاضي، وهو ما يضعف من حجيته.

نخلص مما تقدم أن الصعوبات المتعلقة بالإثبات تتلخص في معاينة صعوبة الجرائم الإلكترونية، وكذلك بالصعوبات المتعلقة بالدليل الرقمي ذاته، ولا تقف الصعوبات الإجرائية عند هذا الحدّ بل هناك صعوبات إجرائية عابرة للحدود.

المبحث الثاني: الحدود الإجرائية العابرة الحدود

إن جرائم التكنلوجيا الحديثة هي جريمة ذات طابع دولي، وعابرة للحدود، وهو ما يعني أن الركن المادي للجريمة قد يتفرق بين دولة وأخرى، أو بين عدة دول[98]، فأحياناً يتم الاعتداء على الأنظمة المعلوماتية من خارج الحدود، وأحياناً يكون الجاني داخل الإقليم الوطني، لكن فور علومه بإجراءات ضدّه قد يقوم بنقل المعلومة خارج الحدود، من أجل حفظها أو تخزينها في نظام معلوماتي آخر، وهذا يؤدي إلى تفكك وتفريع الركن المادي للجريمة[99]، الشيء الذي يطرح عدة صعوبات تتلخص أساساً، في التفتيش عن بعد (الفقرة الأولى) إضافة إلى صعوبة تنفيذ الأحكام خارج الوطن.

---

[96] مساهمة الوفد التونسي في مؤتمر رؤساء المحاكم التعقيب: ص 6.

[97] منية الزغلامي: مرجع سابق، ص 86.

[98] Xavier Latour, *La criminalité informatique et les défis de la compétence internationale*, Revue Internationale de Droit Pénal, Paris, 2019, pp. 89–95.

[99] سليمان محمد عبد العزيز، *إشكاليات الاختصاص المكاني في الجرائم المعلوماتية: دراسة فقهية، دار الجامعة الجديدة*، الإسكندرية، الطبعة 1، 2021، ص، 203-208.

الفقرة الأولى: التفتيش من خارج الحدود:

يواجه القانون الجنائي الموريتاني صعوبة تتعلق بمسألة التفتيش من بعد أو النفاذ من خارج الحدود، حيث يطرح هذا الإجراء معوقات أمام سلطة الادعاء، وقد أثارت هذه النقطة الكثير من الخلاف بين الأنظمة القانونية.

نصّ المشرع الموريتاني في المادة 39 من قانون رقم 2016-007 المتعلق بالجريمة السبرانية على أن التفتيش من خارج الحدود الموريتانية مربوط بالاتفاقيات الدولية[100]، إذ لا يجوز تفتيش النظم المعلوماتية خارج الحدود الدولة الموريتانية إلا إذا كانت هناك اتفاقية دولية تنص على ذلك.

وانطلاقاً من هذه المادة يمكن القول بأن المشرع الموريتاني اتجه في اتجاه الرأي القائل بضرورة احترام سيادة الدول، غير أنه في ظل غياب الاتفاقيات الدولية والثنائية للدولة الموريتانية في هذا المجال فإن هذا الإجراء سيسمح بطمس الكثير من الأدلة، وإفلات المجرمين، وهنا تتجلى أهمية التعاون الدولي، إذ أنه في حالة إذا ما كانت هناك معلومات مطلوبة خارج الحدود الموريتانية، وفي حالة غياب اتفاق دولي اتفاق دولي فإن هذا سيضعف الملاحقة القضائية.

وفي هذا السياق ندعو المشرع الموريتاني إلى ضرورة تعجيل المصادقة على اتفاقية أوروبا المتعلقة بالجريمة الإلكترونية، إذ أنه وحتى هذه اللحظة لم يصادق عليها، مع العلم أنه في سنة 2018 عقدت الدولة الموريتانية وروشة تحسيسية بالتعاون مع مجلس أوروبا لإعداد مسار انضمام موريتانيا إلى اتفاقية بواد ست، وذلك يوم 17 ديسمبر 2018، لكنها لم توقع حتى الآن. [101]

إن التوقيع على هذه الاتفاقية سيعزز من مكافحة جرائم التكنلوجيا الحديثة، وستسمح هذه الاتفاقية بالنفاذ أو التفتيش من خارج الحدود. [102]

أن التفتيش الإلكتروني العابر للحدود لابد وأن يتم في إطار اتفاقية دولية أو اتفاقية ثنائية خاصة تجيز امتداد التفتيش بين الدول المعنية، وبالتالي فإنه لا يجوز القيام بالتفتيش العابر للحدود في غياب اتفاقية أو على الأقل الحصول على إذن الدولة الأخرى.

وكتطبيق لهذا الإجراء في فقه القضاء المقارن فقد حدث في ألمانيا أثناء جمع إجراءات التحقيق عن جريمة غش وقعت في بيانات حاسبة إلكترونية فقد تبين وجود اتصال بين الحاسبة الإلكترونية المتواجدة في المانيا وبين شبكة اتصال في سويسرا حيث يتم تخزين البيانات المشروعات فيها، وعندما أرادت سلطات التحقيق الألمانية ضبط هذه البيانات فلم تتمكن من ذلك إلا عن طريق التماس المساعدة الذي تم

[100] المادة 39 من قانون رقم 2016-007 من القانون المتعلق بالجريمة الإلكترونية.

[101] Sahramedias.net تاريخ النظر 05-05-2025-

[102] علي كحلون: مرجع سابق، ص 112.

بالتبادل بين الدولتين. [103]

وفي سياق آخر اعتقدت الشرطة اليابانية بأن مجموعة من المخربين قد استخدمت أجهزة الحاسبة الإلكترونية في الصين والولايات المتحدة الأمريكية في مهاجمة العديد من المواقع الخاصة للحكومة اليابانية، وقد طالبت اليابان كل من بكين وواشنطن بتسليم بيانات الدخول المسجلة على أجهزة الحاسبة الإلكترونية حتى تتمكن من الوصول إلى جذور العملية الإرهابية. [104]

يتضح من ذلك أن التفتيش الإلكتروني عن بعد غير ممكن دون التوصل إلى صيغة اتفاق دولي على النحو الذي يحقق مشروعية إجراء التفتيش، ومن ثم سيكون هذا الإجراء فاقداً لمعناه أمام القضاء، فإذا حدث وقامت جهة تحقيق في دولة ما بإجراء تفتيش عن بعد حتى في فرضية تحديد هوية حاسوب وكذلك هوية صاحبه، فإن المشكلة سوف تبرز ليس أمام قضاء تلك الدولة فحسب، وإنما قضاء الدولة التي تم فيها التفتيش المذكور أيضاً، وهو ما سيجعل مشكلة الشكل هذه عرضة لهدم أية دعوى جنائية. [105]

هذا الرأي الفقهي يعززه تقرير المجلس الأوروبي الذي يعتبر أن الاختراق المباشر يعد انتهاكاً لسيادة دولة أخرى ما لم توجد اتفاقية دولية بهذا الشأن. [106]

وكخلاصة نستنتج أن التفتيش الإلكتروني عن بعد غير ممكن دون وجود صيغة دولية وهو ما يعد عائقاً أو من الصعوبات الإجرائية التي تعترض سلطة الادعاء، وبالتالي لا مناص من التعاون الدولي في هذا المجال، كما يطرح تنفيذ الأحكام خارج الدولة صعوبة إجرائية أخرى.

الفقرة الثانية: صعوبة تنفيذ الأحكام خارج الإقليم:

إن قوانين العالم والأنظمة التشريعية لا تجمع بالضرورة على رأي واحد، ومن ثم كانت الصعوبة ومن المبادئ العامة في القانون الجنائي أن تحديد العقوبة المستوجبة والمحكمة المختصة يخضعان لمبدأ الاختصاص الترابي أي أن القانون المنطبق هو قانون مكان ارتكاب الجريمة، وفي حالة تنازع القوانين يحدد كل قانون وطني مجال انطباقه بدون التنسيق مع بقية القوانين الأخرى.

وفي هذا الإطار فإنه في حالة ارتكاب جريمة من طرف مواطن على أرض دولة أجنبية فإن اختصاص المحاكم الوطنية ينعقد للنظر في هذه المسألة، وهو مبدأ معروف مبدأ الاختصاص الشخصي، وهنا لا مشكلة بل أن المشكلة تتمثل في أنه في حالة صدور حكم من طرف المحاكم الوطنية في حق مواطن خارج الحدود، فإن تنفيذ هذا الحكم يصطدم بعواقب تنازع القوانين، وبالتالي عدم تنفيذ هذا الحكم وهذه من الصعوبات الإجرائية التي تعترض القانون الجنائي الموريتاني في مواجهة جرائم التكنلوجيا الحديثة.

[103] علي عدنان الفيل: مرجع سابق، ص 46.
[104] علي عدنان الفيل: مرجع سابق، ص 47.
[105] فتحي محمد أنورت عزت: مرجع سابق، ص 645.
[106] عبد الفتاح بيومي حجازي: مرجع سابق، ص 383.

ولقد تعرض فقه القضاء الفرنسي إلى مسألة تنفيذ الأحكام التي تصدرها المحاكم الفرنسية في خصوص الجرائم المعلوماتية والتي يكون مرتكبها خارج فرنسا، ومن ذلك القضية المعروفة بقضية YAHOO ذلك أنه بتاريخ 2000/11/20 أصدرت محكمة باريس قرارا يلزم شركة "ياهو" بإيجاد حلول فنية من شأنها أن تمنع مستعملي شبكة الإنترنت من الدخول إلى موقع البيع بالمزاد العلني والذي يتم عبره بيع بعض الأمتعة والأغراض التي لها علاقة بالنازية والتي تعتبر القانون الفرنسي أن مجرد مشاهدتها يشكل جريمة الفصل 645-1 من المجلة الجنائية الفرنسية، وقد كان هذا القرار مرفوقاً بتقرير من هيئة خبراء توضح الطريقة الفنية التي يمكن بها تنفيذ ذلك القرار، غير أن القضاء الأمريكي رفض قبول ذلك القرار معتبراً إياه يتناقض مع مبادئ الدستور الأمريكي الذي يخول حرية التعبير.

نخلص من ذلك أن عديد الإشكاليات قد تطرح عندما يتعلق الأمر بجعل الأحكام الأجنبية نافذة داخل دولة ما، وذلك يرجع إلى الأنظمة القانونية المختلفة. [107]

وقد حاولت في هذا الإطار الاتفاقية الأوروبية "اتفاقية بودابست" تحديد الاختصاص المتعلقة بالأنظمة المعلوماتية، وقد وضعت هذه الاتفاقية مبدأ الاختصاص الترابي كقاعدة عامة بحيث يعود الاختصاص إلى مكان ارتكاب الجريمة[108]، فتختص المحاكم الوطنية إذا كان الفاعل والنظام المعلوماتي يوجدان على الإقليم الوطني، أو أن يكون أحدهما موجود على التراب الوطني دون الآخر، فمثلاً وجود الفاعل داخل الإقليم والنظام المعلوماتي خارج الإقليم والعكس بالعكس، وطبعاً يلحق بالاختصاص الترابي الإقليم الحكمي والاعتباري، كما اعتمدت الاتفاقية على مفهوم الجنسية لضبط الاختصاص، فإذا ارتكبت الجريمة ببلاد أجنبية أو خرجت عن اختصاص أي دولة في العالم. فيعود الاختصاص إلى الدولة التي ينسب إليها المتهم من حيث الجنسية، كما تبقى الاتفاقية في نهاية الأمر الحرية إلى القوانين الوطنية.

وفي حالة لحق ضرر بعده أنظمة معلوماتية موجودة بعدة بلدان بواسطة الفيروسات المعلوماتية، أرشدت الاتفاقية ضرورة التشاور بين الدول المتعاقدة لتحديد الجهة المختصة، ويمكن أن ينتمي التشاور إلى إسناد الاختصاص إلى دولة معينة، كما يمكن أن ينتهي إلى توزيع الاختصاص بين عدة دولة وفي نقاط معينة، ولم تجعل الاتفاقية هذا التشاور وجوبي، بل إنه اختياري ويمكن لأي دولة عدم الاستجابة له. [109]

خاتمة البحث

يتبيّن من خلال هذه الدراسة أن المشرّع الموريتاني، رغم استجابته النسبية لمتطلبات مواجهة الجرائم المعلوماتية عبر إصدار قوانين خاصة وتنظيم آليات الحماية الموضوعية والإجرائية، ما زال يواجه عوائق حقيقية تحدّ من نجاعة هذه المنظومة التشريعية. فقد أظهرت المعالجة الموضوعية أن طبيعة الجريمة

[107] الهاشمي الكسراوي: مجلة القضاء والتشريع، مرجع سابق ص 22.
[108] علي كحلون مرجع سابق، ص 117.
[109] علي كحلون مرجع سابق، ص 119.

المعلوماتية، وما تتميز به من سرعة، وخفاء، وتعقّد تقني، قد فرضت حدوداً تشريعية وواقعية تجعل تتبع هذه الجرائم وضبط مرتكبيها مهمة شديدة الصعوبة. كما بيّنت الدراسة أن أطراف الجريمة—سواء الجاني المتمتع بمهارات تقنية عالية، أو الضحية المتحفظة عن التبليغ—يسهمان في تضييق هامش فعالية الحماية القانونية.

أما على المستوى الإجرائي، فقد تبيّن أن معضلات الإثبات، وصعوبة المعاينة، وضعف الوسائل التقليدية، إضافة إلى محدودية حجية الدليل الرقمي، تجعل من التحقيق في هذا النوع من الجرائم عملية معقدة تتطلب أدوات جديدة لا يوفرها النظام الحالي. كما أن غياب التعاون الدولي وتشتت الاختصاص عند امتداد الركن المادي للجريمة خارج الحدود، يزيد من صعوبة تفكيك السلوك الإجرامي والوصول إلى الجناة.

وبناء على مجموع هذه المعطيات، يتضح أن القانون الجنائي الموريتاني لا يزال غير قادر بشكل كامل على التصدي بفعالية لجرائم التكنولوجيا الحديثة، مما يستوجب مراجعة تشريعية وإجرائية شاملة تتلاءم مع الطبيعة التقنية المتسارعة لهذا النمط من الجرائم.

توصيات البحث

- **إحداث هيئة وطنية متخصصة في مكافحة الجرائم المعلوماتية** تكون مهمتها جمع وتحليل الأدلة الرقمية، والإشراف على عمليات التتبع الإلكتروني، وتلقي التبليغات، على غرار التجارب المقارنة (فرنسا، تونس).
- **تعديل التشريعات الجزائية والإجرائية** لجعل إجراءات التفتيش والمعاينة والحجز أكثر مرونة وسرعة، بما يتناسب مع الطابع الزمني الحرج للجريمة المعلوماتية، مع النص على إمكانية الإذن الشفهي في حالات الضرورة، إضافة إلى ضرورة.
- إحكام صياغة القواعد الموضوعية المتعلقة بالتنصت الإلكتروني، وسرية الاتصالات، والحياة الخاصة بالأفراد.

تطوير منظومة الإثبات، عبر تكريس حجية الدليل الإلكتروني بنصوص واضحة، وتنظيم طرق استخراجه وحفظه، وإرساء ضوابط تضمن سلامته ومشروعيته وتجعل تقديره أكثر وضوحاً أمام القضاء.

- **تكوين متخصص ومستمر لجهات التحقيق والقضاة** من أجل رفع كفاءة التعاطي مع الأدلة الرقمية والأدوات التقنية المستعملة في الجريمة المعلوماتية، وإنشاء فرق مشتركة بين المحققين والمهندسين والخبراء.
- **فرض إلزامية التبليغ عن الجرائم المعلوماتية** بالنسبة للبنوك والمؤسسات الكبرى، مع توفير حماية قانونية للمؤسسات المبلّغة تجنبها مخاطر السمعة، بما يسهم في كشف عدد أكبر من الجرائم.

Liste des références المراجع

أولاً: القوانين الموريتانية:

1. قانون الأداء الإلكتروني (2006).
2. القانون رقم 2013-025 المتعلق بالاتصالات الإلكترونية.
3. القانون رقم 2017-020 المتعلق بحماية البيانات ذات الطابع الشخصي الصادر بتاريخ 15 نوفمبر 2017.
4. القانون رقم 2018-022 المتعلق بالمبادلات الإلكترونية.
5. القانون رقم 2016-007 المتعلق بالجريمة المعلوماتية الصادر بتاريخ 20 يناير 2016.
6. مجلة الإجراءات الجنائية الموريتانية - المادة 67.
7. قانون حماية المعطيات ذات الطابع الشخصي رقم 2017-020.
8. قانون مكافحة غسل الأموال وتمويل الإرهاب رقم 2019-07 الصادر بتاريخ 20 فبراير 2019.
9. قانون حماية الطفل (موريتانيا).
10. قانون الاتصالات (موريتانيا).

ثانياً: الأبحاث والدراسات:

1. علي كحلون: الجرائم المتعلقة بالمحتوى المعلوماتي، مجلة القضاء والتشريع نوفمبر 2003.
2. محاضرة الوفد التونسي في المؤتمر التاسع لرؤساء المحاكم العليا: الجرائم الإلكترونية الواقعة على الأشخاص في القانون التونسي، بيروت، 17-19-2018.
3. أمال فكيري: إشكالات الإثبات والاختصاص يفي جرائم تكنولوجيا الإعلام والاتصال العابرة للحدود، مجلة العلوم القانونية والسياسية، عدد17 لسنة 2018.
4. عبد القادر القحطاني: الجرائم المعلوماتية: دراسة مقارنة في القانونين الجنائيين التقليدي والمعلوماتي، دار الفكر الجامعي، الإسكندرية، الطبعة الثانية، 2018.
5. الحماية الجزائية للحياة الخاصة، مذكرة ماجيستر، كلية الحقوق والعلوم السياسية بتونس، 1996-1997.
6. فتحي محمد أنور عزت: الأدلة الإلكترونية، في المسائل الجنائية والمعاملات المدنية، دار الفكر والقانون للنشر والتوزيع، الطبعة1، القاهرة، 2010.
7. حمد جلال أبو زيد: التفتيش الإلكتروني في ضوء الفقه والقضاء: دراسة مقارن دار الجامعة الجديدة، الإسكندرية، الطبعة 2020.
8. مصطفى مجدي هرجة: التفتيش في الجرائم المعلوماتية: دراسة مقارنة بين القانونين المصري والفرنسي، دار النهضة العربية، القاهرة، الطبعة الأولى، 2019.
9. عبد الفتاح بيومي حجازي: مبادئ الإجراءات الجنائية في جرائم الكومبيوتر والإنترنت، درا الكتب القانونية، القاهرة، 2007.
10. علي عدنان الفيل: إجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية، الإسكندرية.

11. القاضي مصطفي اليحياوي: المحاولة الإجرامية، دراسة مقارنة على ضوء القانون وفقه القضاء، أوروبيس للطباعة، ط1، تونس، 1998.
12. منية الزغلامي: الإثبات في جرائم الاتصال، رسالة ماجستير، كلية الحقوق والعلوم السياسية بتونس، 2007.
13. محمد علي قطب: الجرائم المعلوماتية وطرق مواجهتها، مركز الإعلام الأمني، الأكاديمية الملكية للشرطة.
14. منية بن ترايديت غمارسة: جرائم المعلوماتية في القانون التونس والقانون المقارن والقانون الدولي، دار الكتاب بتونس، 2015 تونس.
15. مروى عليمي: التحقيق في الجرائم المعلوماتية، شهادة لنيل مذكرة ماجيستر، كلية الحقوق والعلوم السياسية بتونس، 2013-2014.
16. محمد الأمين البشري: الأساليب الحديثة للتعامل مع الجرائم المستحدثة من طرف أجهزة العدالة الجنائية، محاضرة ألقيت في الحلقة العلمية (تحليل الجرائم المستحدثة والسلوك الإجرامي) الإمارات 2011.
17. براهيم، خالد ممدوح: الدليل الجنائي الرقمي وحجيته في الإثبات، الطبعة الأولى، الإسكندرية: دار الفكر الجامعي، 2021.
18. مصطفى محمد موسى: التحقيق الجنائي في الجرائم المعلوماتية: أساليب وتقنيات، دار النهضة العربية القاهرة، 2018.
19. احمد فتحي سرور، الوسيط في قانون الإجراءات الجنائية، دار النهضة العربية، القاهرة، الطبعة السابعة، 2015.
20. Jean Pradel, Procédure pénale, Éditions Cujas, Paris, 2018.
21. Patrick klob: Laurence Leturmy: Droit pénal général, Gaulinolextenso, 11 Edition, France, 2017.
22. Merle et vitu: traité de droit criminel problème généraux de la Science criminelle, Droit pénal général, Cujas, T1, 7éme édition, 1997.
23. Salangeghenauti-Heli: la cybercriminalité 1er Edition presses polytechniques et universitaire Bomande, LA usanne, 1er Edition 2009.
24. Myriam Quémener: cyber fraude, Revue Banque 1er Edition Paris, 2011.
25. Jean Pradel:Droit pénal spécial, 20e édition,Cujas, Paris, 2020.
26. Jean-Baptiste Perrier:La perquisition numérique et les garanties procedurals.
27. Revue de science criminelle, Dalloz, Paris, 2018.
28. Pierre Truche& Jacques Buisson, Les interceptions des communications et les libertés fondamentales, editions Dalloz, Paris, 2017.
29. Hervé Croze, Le droit pénal des technologies de l'information, Éditions LexisNexis, Paris, 2019.

30. Jean-Paul Pinte: Cybercriminalité et compétences techniques des auteurs d'infractions numerique, ÉditionsL'Harmattan, Paris, 2019.
31. Romain BOOS: la lutte contre la cybercriminalité au regard de l'action des Etats thèse Doctorat université de lorraine France 2016.
32. Dominique Leprêtre: Cybercriminalité et gestion des incidents dans les entreprises, Éditions Dunod, Paris, 2018.
33. François Falletti: Cybercriminalité et coopération judiciaire internationale, Revue Internationale de Droit Pénal, Vol. 90, n°3, 2019.
34. Serge Sur & Olivier Cahn, Cybercriminalité et droit international, Presses Universitairesde France (PUF), Paris, 2018.
35. Éric Caprioli:La cybersécurité et la coopération internationale, Éditions Larcier, Bruxelles, 2019.
36. Council of Europe: Convention on Cybercrime, Budapest, 23 November 2001.
37. Ghernaouti Hélie, Solan: Cybercriminalité: comprendre, prévenir, réagir1،ère édition (Dunod) ،Paris: Dunod 2023 .
38. Jean Michel Bruguière:La criminalistique numérique: principes et pratiques, L'Harmattan, Paris, 2020.