القصور التشريعي الجنائي في مجال الجريمة المعلوماتية في التشريعين المغربي والجزائري

Criminal legislative shortcomings in the field of information crime in Moroccan and Algerian legislation

رمضاني فاطمة الزهراء*، أستاذة محاضرة أ
جامعة ابي بكر بلقايد، تلمسان، الجزائر
fatimazohra.ramdani@univ-tlemcen.dz

بدراني علي، أستاذ محاضر ب
المركز الجامعي عبد الله مرسلي تيبازة

تاريخ الارسال: 2021/08/11	**تاريخ القبول:** 2022/01/26	**تاريخ النشر**: 2022/06/10

ملخص :

تعد الجريمة المعلوماتية من أكبر التحديات التي نواجهها في عالمنا المعاصر، وقد كانت الولايات المتحدة الأمريكية بين الدول الأولى التي خصصت تشريع مستقل بشأن جرائم الكمبيوتر، .فهذه المقالة العلمية تحاول تسليط الضوء على التأثير السلبي للثورة المعلوماتية وما نتج عنها من جرائم إلكترونية، لإلقاء الضوء على جهود المشرعين المغربي و الجزائري في تقنين هذه الجرائم، ومعالجتها، ومدى اهتمام كل من المشرع المغربي و الجزائري بتنظيمها والتصدي لها من خلال التعديلات التي أدخلها على القوانين العامة والخاصة ذات العلاقة، وأهمها قانون العقوبات وقانون الإجراءات الجزائية حتى يواكب التشريعات العالمية التي سبقته في سن قوانين خاصة بالجريمة الإلكترونية، وأكثر من ذلك التعرض لمكامن القصور فيهما لتقديم مقترحات لإثراء التشريعين في هذا الخصوص. فالإشكالية الأساسية التي نبحث فيها هي: ما مدى وفاء وفعالية هذه التشريعات في مكافحة هذه الجرائم الخطيرة، وما مدى نجاعة قواعدها الموضوعية والإجرائية في تحقيق الردع العام؟ ثم كيف يمكن سد الفراغات والنقائص الملموسة على أرض الواقع؟

الكلمات المفتاحية: قانون العقوبات؛ قصور التشريع؛ جريمة الكترونية؛ قضاء متخصص.

المؤلف المرسل: رمضاني فاطمة الزهراء

Abstract:

Information crime is one of the biggest challenges we face in our contemporary world, and the United States of America was among the first countries to dedicate independent legislation on computer crimes. This scientific article attempts to shed light on the negative impact of the information revolution and the resulting cybercrime, to shed light on the The efforts of Moroccan and Algerian legislators in codifying these crimes, addressing them, and the extent to which both the Moroccan and Algerian legislators are interested in organizing and addressing them through the amendments made to the relevant public and private laws, the most important of which are the Penal Code and the Code of Criminal Procedure in order to keep pace with the global legislation that preceded it in enacting laws Specific to cybercrime, and more than that, an exposure to the deficiencies in both of them to present proposals to enrich the two legislations in this regard The basic problem that we are discussing is: What is the extent of the fulfillment and effectiveness of these legislations in combating these serious crimes, and how effective are their substantive and procedural rules in achieving general deterrence? Then how can the blanks and tangible shortcomings be filled on the ground?

Keywords : Penal Code ; insufficiency of legislation; cyber crime; Specialized court.

مقدمة:

تميز القرن العشرين باختراعات هائلة على المستوى التقني بفضل ظهور وانتشار استعمال الكمبيوتر واستحداث شبكات المعلومات، حتى أصبح يعرف بقرن المعلوماتية أو le siècle de l'informatique [1]، ورغم ما تقدمه هذه التقنيات من خدمات هامة في جميع القطاعات خاصة ما يتعلق بنقل المعلومات وتنظيم المعاملات بين الأفراد، إلا أنها تعتبر سلاح ذو حدين فهي من جهة تسهل رفع كفاءات وقدرات الإنسان والحفاظ على أمنه وراحته واستقراره، ومن جهة أخرى أدت إلى تطوير وتحديث وتسهيل استغلالها لارتكاب جرائم لم يكن يعرفها الإنسان من قبل [2]. فهذه الجرائم تقنية، تنشأ في الخفاء وتوجه للنيل من الحق في المعلومات

المنقولة عبر نظم وشبكات المعلومات من الإنترنت، وتظهر مدى خطورتها في الاعتداءات التي تمس الحياة الخاصة للأفراد، وفي مدى إشاعتها فقدان الثقة بالتكنولوجيات الحديثة، إلى جانب تهديد الأمن والسيادة الوطنيين.

كما أن تطور المعلوماتية وتطبيقاتها المتعددة أدى إلى بروز مشاكل قانونية جديدة: فيما يعرف بأزمة القانون الجنائي في مواجهة واقع المعلوماتية. إن محاولة حل هذه المشاكل تفرض البحث في الأوضاع القانونية القائمة ومدى وملاءمتها لمواجهة هذه المشاكل، ولما كان القاضي الجزائي مقيدا عند نظره في الدعوى الجنائية بمبدأ شرعية الجرائم، فإنه لن يستطيع أن يجرم أفعالا لم ينص عليها المشرع حتى ولو كانت أفعالا مستهجنة وعلى مستوى عال من الخطورة الإجرامية، كما لا يستطيع معاقبة الأفراد على أفعال غير مجرمة مهما كانت نتائجها السلبية على الواقع العملي.

وقد كانت السويد، الدولة السباقة لسن تشريعات ضد جرائم الإنترنت أو الجرائم المعلوماتية، وقد تم التنظيم القانوني لموضوع جرائم المعلوماتية أو جرائم المساس بأنظمة المعالجة الآلية للمعطيات، في الجزائر بأول نص تشريعي في مجال الإجرام المعلوماتي، يحمل الرقم 01-09، الصادر في 26 جويلية 2001 بموجب المواد 144 مكرر و146 و144 مكرر 1 و144 مكرر 2 و146 من قانون العقوبات الجزائري والمتعلق بجريمة القذف والسب إزاء رئيس الجمهورية أو فيما يخص دين الاسلام، أو ضد الهيئات العمومية، حيث أدرج المشرع فيها لأول مصطلح وسيلة إلكترونية أو معلوماتية وبعدها جاء القانون رقم 04- 15 المؤرخ في 10 نوفمبر 2004 في الفصل السابع مكرر تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات من المواد 394 مكرر الى المواد 394 مكرر 7 ، ولقد تم تعديل هذا القانون بموجب القانون رقم 09 – 04 المؤرخ في 14 شعبان 1430 الموافق لـ 05 أوت 2009 والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها، أما في المغرب الشقيق، فإهتمام المشرع بهذه المسألة يرجع لمعاناة القضاء المغربي، عندما وضعت أمامه قضايا تتعلق بالجرائم المعلوماتية بدءا من سنة 1985، والتي استند في حلها لأحكام القانون الجنائي، فلسد الفراغ التشريعي

الذي عانت منه المنظومة التشريعية المغربية، تمت مجموعة من تعديلات لتتميم مجموعة القانون الجنائي بالقانون رقم 03-07 فيما يتعلق بالإخلال بسير نظم المعالجة الآلية للمعطيات، ويحتوي هذا القانون على تسعة فصول(من الفصل 3-607 إلى الفصل11-607 من مجموعة القانون الجنائي المغربي([3])، رغم أنه في سنة 2000 سبق له وأن تعرض لحماية برامج الحاسب الآلي بقانون حق المؤلف رقم 00-2 المتعلق بحقوق المؤلف والحقوق المجاورة([4]).

أهداف الدراسة:

تهدف الدراسة إلى التعرف على كيفية معالجة واهتمام كل من المشرع المغربي والجزائري بتنظيم الجريمة الالكترونية والتصدي لها من خلال التعديلات التي أجرياها على تشريعيهما، حيث تحاول تسليط الضوء على التأثير السلبي للثورة المعلوماتية وما نتج عنها من جرائم إلكترونية، لإلقاء الضوء على جهود المشرعين المغربي والجزائري في تقنين هذه الجرائم ومعالجتها، ومدى اهتمام كل منهما بتنظيمها والتصدي لها من خلال التعديلات التي أدخلاها على قوانين العقوبات والإجراءات الجزائية فيهما، حتى يواكبا التشريعات العالمية التي سبقتهما في سن قوانين خاصة بالجريمة الإلكترونية، وأكثر من ذلك التعرض لمكامن القصور فيهما لتقديم مقترحات لإثراء التشريعين في هذا الخصوص.

أهمية البحث في الموضوع:

تكمن أهمية المداخلة في أنها ترتبط بأحد المحاور الهامة للملتقى المرتبطة **بالمنظومة القانونية والتشريعية المقارنة،** في أحد عناصرها الهامة المتعلقة ب « مواءمة التشريعات للتطبيقات التقنية الحديثة » .إذ نحاول تسليط الضوء على دور المشرعين الجديد في الحد من انتشار الجريمة الالكترونية ، ومدى تكريسه واقعيا من خلال ربطه بالتجربة الميدانية من خلال تقديم بعض الأرقام عندما يتطلب الأمر ذلك، على سبيل الاستشهاد.

فالإشكالية الأساسية التي نبحث فيها هي:

ما مدى وفاء وفعالية هذه التشريعات في مكافحة هذه الجرائم الخطيرة، وما مدى نجاعة قواعدها الموضوعية والإجرائية في تحقيق الردع العام؟ ثم كيف يمكن سد الفراغات والنقائص الملموسة على أرض الواقع؟

1-ربما تمكن المشرعين الجزائري والمغربي من التصدي لهذه الظاهرة الجديدة المرتبطة بالآثار السلبية للتطور التكنولوجي، بضبط العناصر الموضوعية والإجرائية المتعلقة بتحقيق الردع الجنائي المتعلق بها؟

2-ربما العكس من ذلك، رغم محاولة مسايرة التشريعات المقارنة، إلا أن معالجة التشريعين لهذه الظاهرة، لم تكن بالمقدار الناجع في التصدي لهذه الظواهر.

منهج الدراسة:

وقد إستعان الباحثان بالمنهج الوصفي، والمقارن، وتحاول الدراسة التوصل إلى مجموعة من النتائج تمثل أبرزها: في تقديم توصيات لإثراء التشريعين للقضاء أو على الأقل الحد من مكامن القصور فيهما، من خلال المحورين الأساسين التاليين:

الفقرة الأولى: النقص الموضوعي في التشريعين المغربي والجزائري.

الفقرة الثانية: النقص الإجرائي في التشريعين المغربي والجزائري.

الفقرة الأولى: النقص الموضوعي المتعلق بالجريمة المعلوماتية في التشريعين المغربي والجزائري.

كفل الدستور المغربي لسنة2011([5]) والتعديل الدستوري الجزائري لسنة 2020 [(6)] حماية الحقوق الأساسية والحريات الفردية ([7])، وضمنا عدم انتهاك حرمة الإنسان. وقد تم تكريس هذه المبادئ الدستورية في التطبيق بواسطة قانون العقوبات والإجراءات الجنائية وقوانين خاصة أخرى والتي تحظر كل مساس بهذه الحقوق. وكما سبقت الإشارة الجرائم المعلوماتية تعد صنفًا مستحدثًا من الجرائم، وهي من أكبر التحديات التي نواجهها في عالمنا المعاصر، والحديث عن هذه التحديات يتطلب التعرف على تحديها للقواعد التقليدية للتجريم والعقاب، سوآءا من خلال خصوصيتها وتميز أركانها طبقًا لمبدأ شرعية الجرائم والعقوبات، أو من حيث تعدد صورها وصعوبة تحديد القائمين بها. ولما كانت الجرائم المعلوماتية من الموضوعات الحديثة التي فرضت نفسها على المستوى الوطني والدولي على حد

سواء، فإن السؤال الذي يطرح في هذا الصدد: هل للجريمة المعلوماتية طبيعة خاصة تميزها عن غيرها من الجرائم أم أنها من قبيل الجرائم التقليدية؟ إن الاجابة على هذا السؤال تقتضي لا محالة تعريفها وتحديد موضوعها(أولا)، ثم التعرض لها كظاهرة إجرامية لها خصوصياتها(ثانيا) وصورها(ثالثا).

أولا: صعوبة تحديد طبيعة الجريمة الالكترونية في التشريعين المغربي والجزائري:

يلاحظ عدم وجود اتفاق على مصطلح معين للدلالة على هذه الظاهرة المستحدثة، فهناك من يطلق عليها الغش المعلوماتي، أو الاختلاس المعلوماتي أو الجريمة المعلوماتية([8]). ومن التعاريف المعطاة لها فقها "أنها تشمل أي جريمة ضد المال مرتبط باستخدام المعالجة الآلية للمعلوماتية"([9]). بينما ترى الدكتورة "غنية باطلي"، أن استعمال مصطلح الجريمة الالكترونية من شأنه أن يدخل في مفهومها جرائم الحاسوب وغيرها من الجرائم التي يسميها البعض بالجرائم المعلوماتية والغش المعلوماتي أو جرائم الاعتداء على معطيات الحاسب الآلي وجرائم الانترنيت، وبالتالي فيه من التوسع ما ينطوي تحت جوانبه العديد من السلوكيات الضارة بالأفراد والجماعة، مما جعل المشرع يعزز الحماية الجنائية، فلا يستطيع المجرم أن يتحايل ويحقق مآربه عن طريق استغلال التقدم العلمي، وما قد يجلبه من إمكانيات لم تكن في ذهن المشرع وقت وضع النصوص([10]).

وعلى خلاف المشرع المغربي الذي لم يعط تعريف للجريمة الالكترونية وترك الأمر للفقه والقضاء واكتفى بسن عقوبات صارمة لها في القانون الجنائي، نجد أن المشرع الجزائري قد اصطلح على تسميتها "الجرائم المتصلة بتكنولوجيا الإعلام والاتصال"، وعرفها بموجب المادة الثانية من القانون 09 – 04 ([11]) بأنها "جرائم المساس بأنظمة المعالجة الآلية للمعلومات المحددة في قانون العقوبات أو أية جريمة ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الالكترونية." فما يلاحظ على هذا التعريف ما يلي:

أولا: أن المشرع الجزائري قد اعتمد على الجمع بين عدة معايير لتعريف الجريمة الإلكترونية، أولها: معيار وسيلة الجريمة وهو نظام الاتصالات الالكتروني، وثانيها معيار موضوع الجريمة المساس بأنظمة المعالجة الآلية للمعطيات، وثالثها معيار

القانون الواجب التطبيق أو الركن الشرعي للجريمة المنصوص عليها في قانون العقوبات.

ثانيا: كما اعتمد المشرع الجزائري على معيار رابع في تحديد نطاق الجريمة الالكترونية، كونه أقر أن الجريمة الالكترونية ترتكب في نظام معلوماتي أو يسهل ارتكابها عليه، وهذا ما يوسع من نطاق مجال الجرائم الالكترونية في القانون الجزائري.

باختصار يمكننا تعريف الجريمة الالكترونية بأنها "كل سلوك غير مشروع يمس بالنظام المعلوماتي المادي أو المعنوي وبمس بالأشخاص أو الأموال أو أمن الدولة". فالجريمة الالكترونية مثل الجرائم التقليدية تعرف من خلال أركانها :أي توفر الركن الشرعي المتمثل في النص القانوني المجرم للفعل، ثم الركن المعنوي المتكون من العلم بعناصر الجريمة وإرادة القيام بها، فالقصد الجنائي العام متوافر في جميع الجرائم الالكترونية دون أي استثناء ولكن هذا لا يمنع أن بعض الجرائم الالكترونية تتوافر فيها القصد الجنائي الخاص (مثلا: جرائم تشويه السمعة عبر الانترنيت، وجرائم نشر الفيروسات عبر الشبكة)، أما الركن المادي لهذه الجريمة فيتمثل في عدة صور بحسب كل فعل ايجابي مرتكب مثلا: جريمة الغش المعلوماتي : الركن المادي فيها هو تغيير الحقيقة في التسجيلات الكترونية أو المحررات الإلكترونية.

ثانيا: خصوصية الجريمة الالكترونية:

إذا كانت الجريمة التقليدية تحتاج إلى مجهود بدني في ارتكابها كالقتل، السرقة... ، فالجرائم الالكترونية لا تتطلب أدنى مجهود عضلي، بل تعتمد على المجهود الذهني والتفكير العلمي المدروس القائم عن معرفة تقنية ممتازة بالحاسب الآلي، والتعامل السليم مع الشبكة العنكبوتية، وهو ما دفع البعض إلى تسميتها بالجرائم الناعمة([12]). فالجاني في هذا النوع من الجرائم له مميزات عن الجناة العاديون**(أ)**، كما أن الكثير من المجني عليهم يمتنعون عن ابلاغ السلطات المختصة خشية على سمعتهم ومكانتهم**(ب)**، فمعظم الجرائم الالكترونية يتم اكتشافها بالصدفة وبعد وقت طويل من ارتكابها، مما يصعب الاحتفاظ الفني بآثارها أن وجدت، ويجعلها تحتاج لخبرة فنية خاصة يتعذر على المحقق التقليدي نيلها أو التعامل معها ما يجعل الاثبات فيها

صعب جدا([13])، ومع انتشار شبكة الاتصالات العالمية والانترنت أمكن ربط أعداد هائلة لا حصر لها من الحواسيب عبر العالم بهذه الشبكة حيث يمكن أن يكون الجاني في بلد و المجني عليه في بلد آخر مما يعطيها بعدا عالميا.

(أ). المجرم المعلوماتي: بما أن المجرم المعلوماتي يرتكب جرائمه وهو يمارس وظيفته في مجال

الحاسوب، فذا يفترض إنسان اجتماعي ويقوم بواجباته ويمارس حقوقه الاجتماعية والسياسية عاديا، يمتاز بالاحترافية وبقدر كبير من الذكاء.

فالمجرم المعلوماتي، قد يقوم بالتلاعب في بيانات وبرامج الحاسوب لكي يمحو هذه البيانات، أو يعطل استخدام البرامج، كما قد يزرع الفيروسات في هذه البرامج أو يستخدم القنابل المنطقية أو الزمنية أو برامج الدودة لكي يشل حركة النظام المعلوماتي، ويجعله غير قادر على القيام بوظائفه الطبيعية. ويطلق على الجناة في جرائم الإنترنت اسم القراصنة، ويمكن حصر هؤلاء في ثلاثة فئات :

أ -الهاكرز: ويُطلق هذا الاسم على القراصنة الذين يتّخذون من الجرائم الإلكترونية والقرصنة هواية أو فضولا ليس أكثر ويكون غرضها تخريبيّاً، وتكون غالباً من الفئة الشبابية المصابة بهوس التعمق بالمعلومات الإلكترونية والحاسوب([14]).

ب -الكراكرز: وهم القراصنة المحترفون، ويعد هذا النوع من أكثر أنواع مرتكبي الجرائم الإلكترونية خطورة، ويكون القراصنة من هذه الطائفة ذوي مكانة اجتماعية عادية أو متخصصين في العلوم الإلكترونية.

ت -الطائفة الحاقدة :تستهدف غالباً هذه الطائفة المنظمات والمنشآت وأرباب العمل، ويكون الهدف من ارتكابها للجريمة بحق هذه الأطراف عادة بغية الانتقام والحصول على المنفعة المادية أو السياسية، وقد يكون تطرف أو جوسسة ([15]).

(ب). ضحية الإجرام المعلوماتي: الجرائم المعلوماتية هي جرائم فنية تتطلب من المجرم مهارات تقنية معينة في مجال الحاسوب، لا تتوفر في الشخص العادي، فلا عنف فيها، ولا آثار اقتحام لسرقة الأموال، وإنما هي أرقام وبيانات تتغير أو تمحى من السجلات المخزنة في ذاكرة الحاسوب، و عليه يستطيع الجاني تدمير دليل الإدانة في أقل من ثانية، مما يجعل المجني عليه يجحم عن مساعدة السلطات المختصة في

إثبات الجريمة والكشف عنها، وحتى في حالة الإبلاغ، فإن المجني عليه لا يتعاون مع جهات التحقيق خوفا مما يترتب عليه من دعاية مضرة وضياع ثقة المساهمين، حيث يكون المجني عليه عادة بنكا أو مؤسسة مالية أو مشروع صناعي ضخم يهمه المحافظة على ثقة عملائه وعدم اهتزاز سمعته أكثر من اهتمامه بالكشف عن الجريمة ومرتكبها، ولذلك يفضل المجني عليه تقديم ترضية سريعة لعمليه وينهي الأمر داخليا حتى لا يفقده.

(ج). موضوع الجريمة المعلوماتية: في معظم حالات ارتكاب الجريمة المعلوماتية نجد أن الجاني يتعمد التدخل في مجالات النظام المعلوماتي المختلفة ومنها:

.1مجال المعالجة الإليكترونية للبيانات: من حيث تجميعها أو تجهيزها حتى يمكن إدخالها إلى جهاز الحاسوب وذلك بغرض الحصول على معلومات.

2. مجال المعالجة الإلكترونية للنصوص والكلمات الإلكترونية: وهي طريقة أتوماتيكية تمكن مستخدم الحاسوب من كتابة الوثائق المطلوبة بدقة متناهية بفضل الوسائل التقنية الموجودة تحت يده وبفضل إمكانيات الحاسوب، من تصحيح وتعديل ومحو وتخزين وطباعة واسترجاع وطباعة وهي إمكانيات لها علاقة وثيقة بارتكاب الجريمة.

هذا وتكمن الطبيعة الخاصة لهذه الجرائم، في قدرة شبكة المعلومات على نقل وتبادل معلومات ذات طابع شخصي وعام في آن واحد مما يؤدي إلى ارتكاب الفعل، والسبب في ذلك توسع بنوك المعلومات بأنواعها، علاوة على رغبة الأفراد وسعيهم إلى ربط حواسيبهم بالشبكة. **فصعوبة التكييف القانوني لهذه الجرائم تكمن في طبيعتها الخاصة**، بحيث أن القواعد التقليدية لم تكن مخصصة لهذه الظواهر الإجرامية المستحدثة، وبالتالي تطبيقها على هذا النوع من الجرائم يثير مشاكل عديدة في مقدمتها مسألة الإثبات، ومتابعة مرتكبيها وعلى ضوء الاعتبارات السابقة يمكن القول بأن هذه الجرائم تتمتع بطبيعة قانونية خاصة.

ثالثا: أهم الجرائم الالكترونية في القانون العقابي المغربي والجزائري.

الجرائم الالكترونية ليست نوعا واحدا، وإنما تختلف حسب الأساس والمعيار الذي يقسمها به الفقهاء، إذ يصف الأستاذ" يونس عرب" تصنيف الجريمة

الالكترونية تبعا لمساسها بالأشخاص والأموال بأنه الشائع في الدراسات والأبحاث الأمريكية، كما أنه المعيار المتبع في تقسيم الجرائم الإلكترونية في مشروعات القوانين النموذجية وأشار في هذا الصدد إلى مشروع نموذجي يسمى :" Model State Computer Crime Code ([16]).

لذا سوف نعرج في هذه النقطة على هذا التقسيم المشار إليه، لنرى ما إذا كان قانون العقوبات النافذ في المغرب والجزائر قادرين على التصدي لتلك الجرائم بحسب هذا التصنيف، أم أنه قاصر على معالجتها. حيث قسم المشرع الجنائي المغربي الجرائم المعلوماتية إلى: ماسة بالأموال، وماسة بالأشخاص. فجرائم الأموال هي الجرائم التي تنال بالاعتداء أو تهدد بالخطر الحقوق ذات القيمة المالية، ويدخل في نطاق هذه الحقوق كل حق ذي قيمة اقتصادية وداخل لذلك في دائرة التعامل([17]). وأهمها في التشريع المغربي:

-التزوير والإتلاف المعلوماتي: تعتبر جرائم الإتلاف والتزوير المعلوماتي من أكثر الجرائم شيوعا، وتطرق لها المشرع المغربي في إطار الفصل 607 /6 من القانون الجنائي: "يعاقب بالحبس من سنة إلى ثلاث سنوات وبالغرامة من 10000 إلى 2000000 درهم أو بإحدى هاتين العقوبتين فقط كل من أدخل معطيات في نظام المعالجة الآلية للمعطيات أو أتلفها، أو حذفها أو غير المعطيات المدرجة فيه أو غير طريقة معالجتها أو طريقة إرسالها عن طريق الاحتيال" ([18]). أما فيما يتعلق بالتزوير وهو تغيير الحقيقة بقصد الغش، ويكون بإحدى الطرق المقررة بالقانون في محرر يحميه القانون" ([19]) فقد نص المشرع المغربي على جريمة التزوير المعلوماتي في المادة 607 /7 من القانون الجنائي بالعقاب عليه بالحبس من سنة إلى خمس سنوات وبغرامة من 10000 إلى 1000000 ، ويلاحظ من تحليل المادة 7/607 من القانون الجنائي، أنها تنطبق على تزوير بطاقات الائتمان أو ما يسمى ببطاقات الدفع الممغنط، Les cartes monétiques وفي مجال شديد الصلة بأعمال البنوك.

كما تعتبر القرصنة وغسيل الأموال في مجال المعلوميات، من الجرائم المعلوماتية التي تتكبد فيها الدولة خسارات تعد بمليارات الدولارات، فالشراءات والبيوع عبر الأنترنيت بواسطة هذه البطاقات أصبحت الوجهة المفضلة لدى مستعملي الشبكات.

فيكفي التوصل للأرقام السرية للبطائق البنكية حتى يتمكن الجناة من استخلاص مبالغ مالية مهمة من الشبابيك الأوتوماتيكية للبنوك.

ومن الجرائم المعلوماتية الماسة بالأشخاص جرائم التجسس والإرهاب الإلكتروني، فقد تطورت عمليات التجسس الإلكتروني الذي يتم عن طريق إدخال ملف تجسس إلى المجني عليه ويسمى هذا الملف "حصان طروادة"، وفي حالة إصابة الجهاز بملف التجسس يقوم على الفور بفتح أحد المنافذ في جهاز الشخص المجني عليه، وهذا المنفذ هو الباب الخلفي لحدوث اتصال بين جهاز الشخص المجني عليه وجهاز المخترق. فالتجسس هي جريمة قديمة نص عليها المشرع المغربي في الفصل 185 "يعد مرتكبا لجناية التجسس ويعاقب بالإعدام كل أجنبي ارتكب أحد الأفعال المبينة في الفصل 181 فقرة 2-3-4 و5 والفصل 182". حيث عاقب عليها بأشد العقوبات وهي الإعدام. إلا أن التجسس الإلكتروني هو أحد أشكال التجسس الحديث فعلى المشرع التدخل لإنشاء قواعد قانونية لزجر التجسس على الأشخاص.

هذا وقد عرف المشرع المغربي القذف في المادة 442 من القانون الجنائي حيث نص "يعد قذفا ادعاء واقعة أو نسبتها إلى شخص أو هيئة إذا كانت هذه الواقعة تمس شرف أو اعتبار الشخص أو الهيئة التي نسبت إليها". ثم عرف السب: "السب كل تعبير شائن أو عبارة تحقير أو قدح تتضمن نسبة أية واقعية معينة".[20] ونص أيضا في الفصل 444 "القذف والسب العلني يعاقب عليهما وفق الظهير رقم 378-58-1 المؤرخ في 3 جمادى الأولى 1378 موافق 15 فبراير 1958 المعتبر بمثابة قانون الصحافة".

فإذا كانت هذه الفصول تقع تحت طائلة النصوص القانونية التي تجرم تلك الأفعال متى تمت بطرق تقليدية. وعليه، فإن جريمة القذف والسب وتشويه سمعة الأشخاص التي تتم بالطرق الحديثة باستخدام شبكة الأنترنيت بواسطة إنشاء مواقع يكون هدفها فقط القذف أو السب أو التشهير بشخص معين أو بدولة من الدول أو بدين من الأديان، أو من خلال إنشاء المواقع المعادية التي تهدف إما إلى الإساءة إلى دين معين من الأديان ونشر الأفكار السيئة عنه، أو الإساءة إلى بلد معين وإلى مواقف

قادته السياسيين من قضاياه الوطنية، أو حتى إلى شخص معين بما يمثله من مواقف سواء دينية أو سياسية أو وطنية، وما إلى ذلك.

أما في الجزائر، فلقد أحدث المشرع الجزائري قسما في قانون العقوبات هو السابع مكرر من الفصل الثالث الخاص بجرائم الجنايات والجنح ضد الأموال، تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات، من خلال المواد 394 مكرر، و399 مكرر 1، 394 مكرر2، 394 مكرر 3، والمادة 394 مكرر4، والمادة 394 مكرر 5، والمادة 394 مكرر 6، والمادة 394 مكرر 7، وباستقرائنا لهذه المواد يتضح أن المشرع الجزائري قد قسم الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، أو الجرائم الالكترونية إلى الطوائف التالية:

الطائفة الأولى: طبقا للمادة 390 مكرر من قانون العقوبات، وهي جرائم الولوج إلى المعطيات المعالجة آليا عن طريق الغش والتزوير وكذا جريمة الحذف والتغيير والتخريب في هذه المعطيات ويعاقب الجاني بعقوبة 3 أشهر إلى سنة وبغرامة من خمسين ألف إلى مائة ألف دينار وتضاعفت العقوبة إذا ترتب عن الفعل الإجرامي حذف أو تغيير المعطيات، كما يعاقب الجاني بـ 6 أشهر إلى سنتين وغرامة من خمسين ألف إلى مائة وخمسين ألف دينار وفي حالة التخريب النظام المعلوماتي.

الطائفة الثانية: الجرائم الإلكترونية بواسطة النظام المعلوماتي وأهمها استعمال أو إفشاء أو نشر معلومات منصوص عليها في قانون العقوبات، وكذا البحث أو التجميع في معطيات مخزنة في نظام معلوماتي، كجرائم التحويل الالكتروني والسطو والنصب والاحتيال والسلب وغيرها، وهذا ما نصت عليه المادة 394 مكرر 2، وعقوبتها من شهرين إلى 3 سنوات وبغرامة 1000.000دج إلى 5000.000دج.

الطائفة الثالثة: الجرائم الالكترونية المتعلقة بأمن الدولة ومؤسساتها كجرائم التجسس والإرهاب وعقوبتها تضاعف عقوبة الطائفة الثانية لخطورتها طبقا للمادة 394 مكرر 3.

الطائفة الرابعة: الجرائم الإلكترونية للشخص المعنوي، حيث نص المشرع الجزائري على خلاف التشريعات المقارنة الأشخاص المعنوية بنص خاص وعقوبتها تعادل

خمس مرات الجرائم المرتكبة من طرف الشخص الطبيعي طبقا للمادة 394 مكرر4 من قانون العقوبات الجزائري.

كما عاقب المشرع الجزائري على الشروع في الجريمة الالكترونية، كما هو الحال في الجريمة العادية أو التقليدية بنفس العقوبة للجريمة الكاملة مع تكييفها جنحة وفقا لقانون العقوبات الجزائري، كما نص كذلك على الاشتراك في الجريمة الإلكترونية كما هو الحال في الجريمة العادية ويأخذ الشريك في الجريمة الإلكترونية نفس العقوبة المقررة للشريك في الجريمة العادية أو التقليدية طبقا لقانون العقوبات الجزائري.

ويلاحظ أن المشرع الجزائري، قد توسع في نطاق الجرائم الالكترونية سواء وقعت على النظام المعلوماتي أو بواسطته، وسواء وقعت على الأشخاص أو الأموال أو على أمن الدولة ومؤسساتها، كما أقر جريمة جديدة إلكترونية وهي جريمة الاتفاق الجنائي الكترونيا رغم أنها من الأعمال التحضيرية لارتكاب الجريمة وشدد عقوبتها وذلك خشية استعمال النظام المعلوماتي كوسيلة لارتكاب الجريمة وتسهيلها.

وما يعاب على المشرع الجزائري عدم إفراد معيار واضح وواحد في تقسيم الجرائم الالكترونية وتحديد عقوبتها، وكان من الأحسن إتباع المنهاج المتبع من طرف الفقه وهو تقسيمها إلى جرائم واقعة على النظام المعلوماتي وجرائم واقعة بواسطة النظام المعلوماتي، بعد تحديد المصطلحات الخاصة بها لتسهيل فهم ماهيتها، طبقا للمادة 394 مكرر 5 من القانون 04 – 15 المعدل والمتمم لقانون العقوبات.

الفقرة الثانية: القصور الإجرائي المتعلق بجرائم الانترنيت في القانونين المغربي والجزائري

تعرضنا في الفقرة السابقة إلى المشكلات الموضوعية التي تثيرها الجرائم المعلوماتية، في تطبيق القواعد التقليدية لقانون العقوبات، الذي صيغت نصوصه لمواجهة سلوكيات مادية ترتكب في عالم ملموس، واتضح لنا أن الجريمة المعلوماتية ترتكب باستخدام التقنية المعلوماتية في فضاء افتراضي مفرغ cyberspace، فإذا كان ذلك هو حال القواعد الموضوعية للتجريم والعقاب، فما هو حال القواعد الإجرائية [21] لهذا الفرع من القانون الجنائي ؟

فهذه الجريمة ترتكب في مسرح الكتروني، يختلف كلياً عن المسرح التقليدي، الذي ترتكب فيه الجريمة العادية، حيث يتم الاستدلال عليها وضبطها واثباتها بالوسائل التقليدية المتمثلة في اجراءات الاستدلال والتحقيق، وهنا يثور التساؤل حول مدى صلاحية هذه الإجراءات لضبط وإثبات جريمة ارتكبت في عالم افتراضي غير ملموس؟ أما إذا ارتكبت الجريمة عبر الشبكة العنكبوتية الدولية (الانترنت) تزداد العقبات القانونية صعوبة، فلا نكون أمام مشكلات إجرائية تخص ضبط الجريمة واثباتها فحسب، بل نجد أنفسنا أمام مشكلة أكثر تعقيداً تتمثل في تحديد الاختصاص القضائي المرتبط بالقانون الواجب التطبيق على هذه الجريمة، وهو ما يتطلب منا التطرق إلى مشكلات التحقيق في الجريمة المعلوماتية واثباتها (أولا)، قبل التطرق إلى الحديث عن مسرح الجريمة المعلوماتية (ثانيا) ثم مشكلات الاختصاص بنظر الجريمة المعلوماتية (ثالثا).

أولا: خصوصية التحقيق والإثبات في الجريمة الالكترونية:

كقاعدة عامة تختص النيابة العامة وحدها دون غيرها في تحريك الدعوى العمومية ومباشرتها في كافة الجرائم ([22]) ويتولى مأموري الضبط القضائي البحث والاستقصاء عن الجرائم ومرتك

بيها وجمع الاستدلالات التي تلزم للتحقيق في الدعوى ([23]).

وقد نظم قانوني الإجراءات الجزائية المغربي والجزائري بالتفصيل إجراءات التحري وجمع الأدلة والتحقيق في الجرائم، ولكن هل هذه الإجراءات تستطيع أن تنظم عملية التحقيق في الجريمة الإلكترونية؟

بالنسبة لمتابعة الجريمة الإلكترونية تتم بنفس الإجراءات التي تتبع بها الجريمة التقليدية، كالتفتيش والمعاينة واستجواب المتهم والضبط والتسرب والشهادة والخبرة. غير أن المشرع الجزائري نص على تمديد الاختصاص المحلي لوكيل الجمهورية في الجرائم الإلكترونية في المادة 37 من قانون الإجراءات الجزائية [(24)]

ففي مرحلة جمع الاستدلالات (التحقيق الأولي) : التي يقوم فيها مأموري الضبط القضائي بمجموعة من الإجراءات لجمع الأدلة قبل إحالة هذه الاستدلالات للنيابة العامة، **ضبط الجرائم المعلوماتية يوجب على ضابط الشرطة القضائية الانتقال**

لمكان ارتكاب الجريمة وهذا ما نصت عليه المادة 57 /1من قانون المسطرة الجنائية المغربي، والهدف من هذا لانتقال الفوري ضرورة الحفاظ على الأدلة القابلة للاندثار وعلى كل المواد التي تفيد خلال تحريات الضابطة القضائية في إظهار الحقيقة ([25]). **إذ يتم معاينة الجريمة وضبطها، وهي مسألة مهمة** فالمحقق الذي يقوم بمعاينة الجريمة المعلوماتية يجب أن يكون ملمًا بمهارات هذه التقنية، مثل القدرة على استخدام برامج Time stamp وهي التي يمكن عن طريقها تحديد الزمن الذي تم فيه السلوك الاجرامي. وقد يقتضي الأمر الاستعانة بخبير للتعرف على طبيعة المادة أو نوعها إذا كان ذلك يحتاج لرأي المتخصص، وفي هذه الحالة يتم إرسال هذه الأشياء إلى الخبير، لنكون بصدد إجراء آخر من إجراءات التحقيق وهو الخبرة، فالخبرة هي أحد أهم وسائل جمع الأدلة، فالخبير يأخذ حكم الشاهد من حيث الحجية أو القوة في الإثبات.

أما المرحلة الموالية أي التحقيق الابتدائي، فتقوم النيابة العامة فيها بدور في التحقيق والاستجواب في الجريمة الالكترونية، وهي المرحلة الأهم، لذلك أجاز قانون الإجراءات الجزائية لوكيل النيابة الاستعانة بالخبراء المختصين لإثبات حالة الجريمة المرتكبة تحت إشراف وكيل النيابة وبحضوره إذا قدر أن مصلحة التحقيق تستدعي ذلك، وهنا نصطدم بالعقبة الأساسية أمام معاينة الجريمة المعلوماتية التي ترتكب داخل الفضاء المعلوماتي، فالمحقق في هذه الحالة يتعامل مع بيئة مليئة بالنبضات الإليكترو مغناطيسية، والبيانات المخزنة داخل نظام معلوماتية شديدة الحساسية، ولا يتعامل مع أوراق أو أسلحة أو أشياء قابلة للربط، وهو ما يؤكد القواعد الإجرائية التقليدية التي سنت لتواجه سلوكًا ماديًا يرتكب بواسطة آلات أو أدوات قابلة للربط والتحريز.

أما بالنسبة **لعملية التفتيش** الذي يعد من أعمال التحقيق لا يتم إلا بمذكرة من قبل النيابة العامة أو في حضورها، بناء على اتهام موجه إلى شخص يقيم في المنزل المراد تفتيشه بارتكاب جناية أو جنحة أو باشتراكه في ارتكابها، أو لوجود قرائن قوية على أنه يحوز أشياء تتعلق بالجريمة، ويجب أن تكون مذكرة التفتيش مسببة. وقد نص المشرع الجزائري على التفتيش في المادة 45 الفقرة 7من قانون الإجراءات

الجزائية، حيث أعتبر أن التفتيش المنصب على المنظومة المعلوماتية يختلف عن التفتيش المتعارف عليه في القواعد الإجرائية العامة من حيث الشروط الشكلية والموضوعية، فالتفتيش وإن كان إجراء من إجراءات التحقيق قد أحاطته المشرع بقواعد صارمة، وبالتالي لا تطبق الأحكام الواردة في المادة 44 من قانون الإجراءات الجزائية إذا تعلق الأمر بالجرائم ٱلكترونية. **غير أنه بالرجوع إلى القانون المغربي يتضح أن المشرع حدد مسطرة التفتيش بشروط، بحيث لابد من احترام حرمة المسكن التي يعتبر حق دستوري طبقا للفصل 24 من دستور 2011، لأن التفتيش يهدف إلى الكشف عن الجريمة أثناء التلبس بها أو بعد ارتكابها وذلك أملا في العثور على أدلة وحجج خلفها المشبه فيه خلفه، وبالتالي جعل التفتيش ينصب على المنزل حسب المادة 62 من قانون المسطرة الجنائية وفرض له شروط .**

مما يطرح التساؤل حول إمكانية تفتيش النظام المعلوماتي باعتبار هذه الجرائم المستحدثة لم يتطرق المشرع إلى شروط تفتيشها، حيت تكمن مشكلة تفتيش شباك الحاسب الآلي في أنها تكون ممتدة في دولة أو عدة دول، لدى فقد يرتبط حاسوب يمتلكه المتهم أو في حيازته بأخر يمتلكه غير المتهم في حيازته وقد يكون هذا الارتباط داخل حدود الدولة الواحدة أو خارج حدودها فهناك من الدول من تتطرق لهذه الإمكانية، كما أن المشرع المغربي لم يعترف بالمستندات و الدعائم الالكترونية إذا تم حجزها في التفتيش كأداة لإثبات الجريمة خاصة أن المادة 59 السالفة الذكر قاصرة على الوثائق فقط.

ونرى في اعتقادنا المتواضع، أنه مادام المشرع قد صادق على اتفاقية بودابست 2014 وكما جعل الاتفاقيات تسمو على الدستور من خلال ديباجة دستور 2011 فإن كان يجب عليه مسايرة المادة 19 من الاتفاقية حتى يتم الاتفاق بين النصوص الوطنية و المعايير الدولية وذلك بإدراج تفتيش الحاسب الآلي ضمن ما جاء في نصوص المواد 59 ، 60، 62 من قانون المسطرة الجنائية المتعلقة بالتفتيش(26).

ويتم **ضبط جميع الأشياء** التي يعثر عليها أثناء إجراء التفتيش والمتعلقة بالجريمة وتحرز وتحفظ وتثبت في محضر التفتيش وتحال إلى الجهات المختصة. ويحرر محضر

التفتيش من قبل القائم عليه، ويذكر فيه الأشياء التي تم ضبطها والأمكنة التي وجدت فيها ويوقع عليه ومن حضر إجراءات التفتيش.

ويستوي أن تكون ملكا للمشتبه فيه أو لغيره، حيث تتم المعاينة في مكان الجريمة أو في أي مكان آخر له علاقة بالجريمة أو بآثارها. وهذا ما حددته الفصول 57-59-64-2/65 من قانون المسطرة الجنائية المغربي. وإن حجز المكونات المادية للحاسب الآلي لا يطرح أي إشكال فإن الأخير يثور في حالة حجز المكونات المعنوية خصوصا على الوسيلة الناجعة التي سيتحقق بها هذا النوع من الحجز. فالرجوع إلى مقتضيات المادة 59 من قانون المسطرة الجنائية نجدها لا تستوعب مفهوم الحجز للمكونات المعنوية. ولتجاوز هذا النقص فقد عمل المشرع المغربي من المادة 59 من مشروع قانون المسطرة الجنائية بالتنصيص على" يتم حجز المعطيات والبرامج المعلوماتية الضرورية لإظهار الحقيقة بوضع الدعامات المادية المتضمنة لهذه المعلومات رهن إشارة العدالة أو يأخذ نسخ منها"....

كما أجاز المشرع الجزائري **مراقبة المحادثات السلكية واللا سلكية**، وإجراء تسجيلات لأحاديث واعتراض المراسلات وتسجيل الأصوات والتقاط الصور حسب المادة 65 مكرر 5/ 10 من قانون الإجراءات الجنائية في إطار تحقيق بأمر من السلطة القضائية أو قاضي التحقيق أو النيابة.

غير أنه طبقا لقانون الإجراءات المعدل والمتمم في الفصل الرابع تحت عنوان "في اعتراض المراسلات وتسجيل الأصوات والتقاط الصور". نصت المادة (65 مكرر5/3) على أنه في حالة ضرورة التحري أو التحقيق في مجموعة من الجرائم من ضمنها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات يجوز لوكيل الجمهورية المختص أن يأذن بالاعتراض ووضع ترتيبات تقنية دون موافقة المعنيين من أجل التقاط وتثبيت وبث وتسجيل الكلام المتفوه به بصفة خاصة أو سرية في أماكن خاصة أو عامة.

كما نص على جواز التوقيف للنظر في جريمة المساس بأنظمة المعالجة في المادة 51 الفقرة 6، أما بالنسبة لنصوص إجراءات التحقيق والمحاكمة تطبق عليها نفس إجراءات الجريمة التقليدية.

إلى جانب هذا تثار مسألة مدى حجية المخرجات الإلكترونية في الإثبات الجنائي، فللمخرجات الإلكترونية أنواع مختلفة، فهي تتنوع بين مخرجات ورقية، ومخرجات لا ورقية، وهي المعلومات المسجلة على الأوعية الممغنطة كالأشرطة والأقراص المرنة Floppy Diskالقرص الصلب Hard Disk وغيرها من الأوعية التي أصبحت في تطور مستمر، حتى وصلت إلى أقراص الـ flash discsالتي أصبحت تتميز بسعات كبيرة للتخزين، خاصة أنه تواجهنا مشكلة أساسية تتعلق بصعوبة التمييز بين المحرر وصورته أو بين الأصل والصورة، ذلك لأننا نتعامل مع بيئة الكترونية تعمل بالنبضات والذبذبات والرموز والأرقام، وهو ما يستحيل معه تطبيق القواعد الخاصة بالمحررات العرفية.

ثانيا: مسرح الجريمة الالكترونية: يعرف مسرح الجريمة بأنه كل مكان اتصل بالنشاط الإجرامي الذي ترتب عليه وقوع الجريمة أو حوى دليلا يتصل بها ([27]) وكما نعلم، أن أول مهمة لرجال الضبط القضائي بمجرد علمهم بوقوع جريمة، هي الانتقال إلى مسرح الجريمة وتأمينه إلى حين حضور وكيل النيابة المختص لمباشرة عمله وإجراء كافة التحقيقات اللازمة في مسرح الجريمة؛ من سماع شهود وتنظيم محضر كشف على مسرح الجريمة وتوصيفه بدقة وضبط أدوات الجريمة الموجودة في مسرح الجريمة لمواجهة المتهم بها حين استجوابه.

في الجرائم العادية، مسرح الجريمة واضح المعالم، وكل ما يتطلبه من مأمور الضبط القضائي ووكيل النيابة المحقق معاينته وتحديد أوصافه وضبط ما فيه من أدوات جرمية، بينما مسرح الجريمة الالكترونية ليس واضحا، فالبحث فيه سيتم باستخدام الأجهزة الالكترونية، والأجهزة أو الأدلة الإلكترونية لها أشكال مختلفة، فقد تكون كمبيوتر وقد تكون هاتف خلوي، وطريقة ضبط الأجهزة الإلكترونية ليس بالأمر البسيط، فقد تكون جهاز كمبيوتر واحد وقد تكون عدة أجهزة، وقد يكون الجهاز في حالة تشغيل.

فالمحقق الذي ينتقل إلى مسرح جريمة الإلكترونية يجب أن يكون على دراية كافية في الجريمة الالكترونية حتى يتمكن من تحديد الدليل الذي يبحث عنه، وعليه

يتوجب على المحقق في محضر الكشف على مسرح الجريمة مراعاة الأمور التالية([28]) :

1. تصوير الحاسب والأجهزة الطرفية المتصلة به، على أن يتم تسجيل وقت وتاريخ ومكان التقاط كل صورة.

2. العناية بملاحظة الطريقة التي تم بها إعداد النظام.

3. ملاحظة وإثبات حالة التوصيلات والكابلات المتصلة بكل مكونات النظام حتى يمكن إجراء عمليات المقارنة والتحليل حين عرض الامر فيما بعد على المحكمة.

4. عدم نقل أي مادة معلوماتية من مسرح الجريمة قبل إجراء اختبارات للتأكد من خلو المحيط الخارجي لموقع الحاسب من أي مجال لقوى مغناطيسية يمكن أن يتسبب في محو البيانات المسجلة.

5. التحفظ على معلومات سلة المهملات من الاوراق الملقاة او الممزقة وأوراق الكربون المستعملة والشرائط والأقراص الممغنطة غير السليمة، وفحصها، ويرفع من عليها البصمات ذات الصلة بالجريمة.

6. التحفظ على مستندات الإدخال والمخرجات الورقية للحاسب ذات الصلة بالجريمة، لرفع ومضاهاة ما قد يوجد عليها من بصمات.

7. قصر مباشرة المعاينة على الباحثين والمحققين الذين تتوافر لهم الكفاءة العلمية والخبرة الفنية في مجال الحاسبات.

ثالثا: الاختصاص بنظر الجريمة المعلوماتية: خلصنا مما سبق إلى عدم كفاية القواعد التقليدية للخبرة والمعاينة، وعدم ملاءمتها لإثبات الجرائم المعلوماتية، فهل تستجيب القواعد الخاصة بتحديد نطاق تطبيق القانون من حيث المكان، فكيف يمكن تحديد مكان وقوع الجريمة المعلوماتية؟ وإذا كانت هذه الجريمة ترتكب في مجال افتراضي غير محدد جغرافيًا فهل يمكن ربط هذه الجريمة بدولة ما دون أخرى؟

إن الاجابة على هذا التساؤل تتطلب ضرورة الحديث عن لامركزية الفضاء المعلوماتي، قبل تناول التعاون الدولي لملاحقة الجريمة المعلوماتية.

إن القواعد العامة التي تحكم نطاق تطبيق النصوص الجنائية – التي تتمثل في مبدأ اقليمية النص الجنائي والاستثناءات الواردة عليه – تقتضي تطبيق النص الجنائي على كل الجرائم الواقعة في إقليمه، إلا في أحوال خاصة نص عليها المشرع تبين حالات يطبق فيها القانون الوطني على جرائم ارتكبت خارج إقليمه.

وكون الجريمة المعلوماتية ترتكب في مسرح غير قابل للتحديد الجغرافي، جعل ضرورة للتفكير في التعاون بخصوص مكافحتها، وهو ما حدا المجلس الأوروبي إلى عقد اتفاقية بوداست COUNCIL السابق الإشارة إليها، والتي قدمت صورًا لمكافحة هذه الجرائم ونصت المادة 22 منها على أن لكل طرف اتخاذ الإجراءات التشريعية وغيرها التي يراها لازمة لكي يحدد اختصاصه بالنسبة لكل جريمة تقع وفقًاً لما هو وارد في المواد من 2 إلى 11 من الاتفاقية الحالية ([29]).

ولم ينص القانون المغربي بشأن الجرائم المعلوماتية على أية قواعد لتحديد الاختصاص بنظر هذه الجرائم.

فإن كان الفقه الجنائي اليوم قبل فكرة تطبيق القانون الأجنبي لمواجهة الجريمة عبر الوطنية ما أظهر ضرورة تجاوز فكرة تلازم الاختصاص الجنائي القضائي و التشريعي فيلزم من باب أولى قبول هذه الفكرة والتوسع فيها بالنسبة لجرائم ترتكب في الفضاء السيبراني الذي يتجاوز الحدود والقارات، وبذلك نصل إلى ضرورة التفكير في وضع ضوابط إسناد جنائية لتحديد الاختصاص الموضوعي والإجرامي بعد أن تصنف إلى فئات مختلفة تشكل كل فئة فكرة مسندة تتضمن المصالح الواجب حمايتها جنائيًا على المستوى العالمي لوضع ضوابط إسناد تشير إلى القانون الواجب التطبيق. فالجريمة المرتكبة عبر شبكة الإنترنت جريمة عابرة للحدود والقارات، وهو ما يدرجها ضمن موضوعات القانون الجنائي الدولي.

كل هذه الوسائل القانونية والقضائية لمكافحة الجريمة الالكترونية قد أقرتها الجزائر سواء في القانون 15/04 المعدل والمتمم لقانون العقوبات أو القانون 04/09 المتعلق بالجرائم المتصلة بتكنولوجيا الإعلام والاتصال حيث أقر المشرع الجزائري موضوع التعاون والمساعدة القضائية في مجال مكافحة الجريمة الالكترونية وذلك في الفصل السابع من هذا القانون. كما أقر القانون الجزائري الحماية القانونية لنظم

المعلومات في قوانين خاصة منها قانون التأمينات الاجتماعية 01/08 المؤرخ في 2008/01/23، وقانون الملكية الأدبية والفكرية 05/03 المؤرخ في 2003/07/23 والقانون 03/15 المتعلق بعصرنة العدالة، والقانون المتعلق بالمواصلات السلكية واللاسلكية 03/2000.

الخاتمة:

إن الجرائم المعلوماتية تعد من الموضوعات الحديثة التي فرضت نفسها بقوة على المستوى الوطني والدولي على حد سواء، والتي تطرح على المشرع الجنائي ضرورة مواجهتها بترسانة قانونية حاسمة ورادعة لمكافحتها وعقاب مرتكبيها. وإذا كان التطور المتجدد والسريع للمعلوميات يحجم صورة التجريم الحالية عن مواكبة ما يطرأ من صور إجرامية مستحدثة إلا أن وضع قواعد قانونية تنظم أوجه الحماية الجنائية أفضل بكثير من ترك ما يستجد على الساحة الجنائية دون حماية، وهذا ما يقع على عاتق الفقه بداية بوضع نظرية عامة تسهم في صياغة المشرع للنصوص التشريعية وتساعد على القضاء على تفسير النصوص وتكييف الوقائع([30]). وبعد هذه الدراسة المتواضعة تجلى لنا أن هذا النوع من الجرائم يعد من أكثرها خطورة، ذلك لما تتميز به هذه الجريمة من خصائص تحديا للقوانين والقضاء وجميع الوسائل القانونية لمكافحتها.

حيث اتسمت الجريمة الالكترونية بطبيعة خاصة وجدت صعوبة في وضع تعريف عام جامع وموحد لها، كما أن طبيعتها الخاصة تجلت في خصائصها المتميزة، والمتمثلة في أنها جريمة عابرة للحدود باعتبارها ترتكب بواسطة الحاسوب أو في مجال الحاسب الآلي، كما تميزت بسرعة تنفيذها والتطور المتسارع في ارتكابها، ومما أعطاها خصوصية أكثر الخصائص التي يتميز بها المجرم المعلوماتي وأشكاله، حيث لا يلجأ إلى العنف كما هو الحال في المجرم التقليدي، بل يتميز بالذكاء والمهارة والسلطة والمعرفة. في ظل هذه الخصائص المميزة للجريمة الالكترونية، وقفت القوانين والنظم القانونية عاجزة عن مكافحتها نظرا للعدد الهائل من هذه الجرائم المتطورة بتطور تقنية المعلومات، حيث أصبح مبدأ" لا جريمة ولا عقوبة الا بنص"

لا يتسع لمكافحة هذا النوع من الجرائم، بل يجب التوسع في تفسيره لإيجاد التكييف القانوني السليم للجرائم الالكترونية المستحدثة.

وترتيبا على ذلك، لجأت القوانين المقارنة الى تبني فكرة المساعدة القضائية والتعاون التشريعي والقضائي في مجال مكافحة هذه الجرائم، حيث تم ابرام العديد من الاتفاقيات الثنائية والدولية من اجل ايجاد القانون الواجب التطبيق والقضاء المختص بها.

كما تم عقد الكثير من المؤتمرات والندوات في إطار مؤتمر الامم المتحدة أو الاتحاد الاوربي أو الاتحاد الإفريقي للتصدي لهذه الجرائم ذات البعد العالمي.

ورغم اهتمام المشرع الجزائري بالجرائم الالكترونية و بالعقوبات المقررة لها إلا أن النص عليها في قانون العقوبات أو في القانون 09-04 فقط لا يكفي لمواجهة الانتشار الرهيب والتطور السريع لهذا النوع من الجرائم الالكترونية، بل يجب إصدار قانون خاص بها، حيث ينص في الفصل الأول منه على المصطلحات الخاصة بهذه الجرائم ومرتكبيها ووسائل ارتكابها نظرا لخصوصية مرتكبيها ووسائل ارتكابها وتخص الفصول اللاحقة أنواع هذه الجرائم والعقوبات المقررة لها، مع ضرورة تشديد عقوباتها نظرا للآثار السلبية التي تخلفها على أموال المؤسسات العامة وعلى خصوصية الأشخاص وشرفهم وحتى على أمن الدولة. وعليه لمسايرة تطور الجرائم الالكترونية، نوصي المشرعين الجزائري والمغربي بالحلول والمقترحات التالية:

1-وجوب تعديل قانون العقوبات وقانون الإجراءات الجزائية بما يتلاءم مع أنواع الجرائم الالكترونية أو إصدار قانون خاص بالجرائم الالكترونية وطرق مكافحتها.

2-إنشاء محاكم متخصصة بالجرائم الإلكترونية، أو على الأقل غرف متخصصة في كل المجالس القضائية لمجابهة هذه الظاهرة.

3-ضرورة تخصيص شرطة جنائية خاصة بجرائم الانترنيت في كل ولاية، مع تكوين عناصر من خبراء لهذا الشأن.

4-تعزيز التعاون والمساعدة الوطنية والدولية في مجال مكافحة جرائم الانترنيت.

5-تكوين رجال الشرطة مختصين وقضاة في مجال مكافحة هذا النوع من الجرائم.

6- تكوين هيئة وطنية لمراقبة ومتابعة جرائم الانترنيت، وتزويد البرلمانات بكل التطورات الحاصلة في هذا المجال لتحيين النصوص القانونية المتعلقة بهذا الموضوع، ولما لا انشاء هيئات استشارية في هذا المستوى، خاصة بالمجال القانوني الموضوعي والإجرائي في مجال مكافحة الجرائم الإلكترونية.

الهوامش

[1]- غنية باطلي، الجريمة الالكترونية (دراسة مقارنة) ، الدار الجزائرية للنشر والتوزيع، الجزائر، 2015، ص 05.

[2] -سميت بالجرائم الالكترونية Les infraction électronique أو الجرائم المعلوماتية les infraction Informatique أو جرائم الانترنيتCriminalité par internet ، وهذه المصطلحات كلها تعبر عن مجموعة الجرائم المرتبطة بالأنظمة الالكترونية والشبكة المعلوماتية وخصوصا على شبكة الانترنيت. للمزيد أنظر: يونس عرب، جرائم الكمبيوتر والانترنيت المعنى والخصائص والصور واستراتيجية المواجهة القانونية، أكتوبر 2006، مقال منشور على الموقع الالكتروني:

doc.abhatoo:net.ma/img/doc/dios.doc,p1-6

[3] - هذا القانون يشكل الباب العاشر من الجزء الأول من الكتاب الثالث من القانون الجنائي المغربي تحت عنوان: المس بنظم المعالجة الآلية للمعطيات. وقد صدر بتنفيذه الظهير الشريف رقم197-03-1 بتاريخ 16رمضان1424 الموافق ل 11 نونبر2003.

[4] - ونظرا لربط المشرع المغربي خطورة انتشار الإجرام المعلوماتي بأثرها على أمن واستقرار المجتمع المغربي، فقد جرمها بشكل صريح كوسيلة للقيام بأفعال إرهابية لها علاقة عمدية بمشروع فردي أو جماعي يهدف إلى المس الخطير بالنظام العام من خلال القانون رقم 03-03 المتعلق بمكافحة الإرهاب. وقد سار المشرع المغربي مع التوجه التشريعي في العديد من الدول التي تهدف تحقيق حماية فعالة للبيانات الشخصية، فأصدر القانون رقم 09-08 المتعلق بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي بتاريخ 18 فبراير 2009.

[5] - تم تعديل الدستور الجزائري في سنة 2020، بالمرسوم الرئاسي رقم 20-442، المؤرخ في 2020/12/30، الجريدة الرسمية رقم 82 لنفس التاريخ، التعديل حدث على الدستور الصادر بالقانون 16-10 الصادر في6 مارس2016، المتضمن التعديل الدستوري، الجريدة الرسمية رقم 14 الصادرة في07مارس2016، تم تعديل الدستور الجزائري في سنة 2020، بالمرسوم الرئاسي رقم 20-442، المؤرخ في 2020/12/30، الجريدة الرسمية رقم 82 لنفس التاريخ.

[6] - الدستور المغربي لسنة 20011، الصادر بالظهير الشريف 91.11.1 صادر في 29يوليو2011المتعلق بتنفيذ نص الدستور، الجريدة الرسمية 5964 الصادرة في 30يوليو2011، ص3600.

[7] - جاء في المادة38 من دستور 2020: "تضمن الدولة الحقوق الأساسيّة والحريات"، والتي يقابلها الفصل 21من الدستور المغربي لسنة 2011، ثم المادة 74":حرّيّة الإبداع الفكريّ، بما في ذلك أبعاده العلمية والفنّية مضمونة". يحمي القانون الحقوق المترتبة على الإبداع الفكري"، ثم المادة 39:"تضمن الدولة عدم انتهاك حرمة الإنسان" المادة 55: "يتمتع كل مواطن بالحق في الوصول إلى المعلومات والوثائق والاحصائيات، والحصول عليها وتداولها". والتي يقابلها الفصول 24،25،26 على التوالي من الدستور المغربي.

[8]- محمد علي العريان: "الجرائم المعلوماتية"، دار الجامعة الجديدة للنشر، 2004، ص 43.

[9]- مشار إليه لدى: محمد سامي الشوا: "ثورة المعلومات وانعكاساتها على قانون العقوبات". دار النهضة العربية، القاهرة، 1994، ص15.

[10] -غنية باطلي، المرجع السابق، ص12.

[11]-القانون 09-04 مؤرخ في 23يوليو 2009يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، الجريدة الرسمية رقم 47ل 16 أوت2009.

[12] - د.عبد الفتاح مراد، شرح التحقيق الجنائي الفني والبحث الجنائي، دار الكتب والوثائق المصرية، 2006، ص 46.

[13] - د.هشام محمد رستم، الجرائم المعلوماتية، أصول التحقيق الجنائي الفني مجلة الأمن والقانون، العدد2، دبي، 1999، ص24.

[14]- محمد علي العريان، جرائم الحاسب الآلي وأمن البيانات، بيروت، 2002، ص 64.

[15] - د.عبد الفتاح مراد، المرجع السابق، ص 65.

[16] -عرب، يونس، إيجاز في المفهوم والنطاق والخصائص والصور والقواعد الإجرائية للملاحقة والإثبات، ورقة عمل مقدمة إلى مؤتمر الامن العربي 2002 – تنظيم المركز العربي للدراسات والبحوث الجنائية - ابو ظبي 10-12 /2/ 2002 ص 10 – 13.

[17]- ذ. نور الدين العمراني، "شرح القانون الجنائي الخاص"، 2005، ص 280.

[18]- القانون الجنائي وفق آخر التعديلات: قانون رقم 07.03 المتعلق بالإخلال بسير نظم المعالجة الآلية للبيانات. منشورات المجلة المغربية لقانون الأعمال والمقاولات، 2007.

[19]- هدى حامد قشقوش،" جرائم الحاسوب الإلكتروني"، دار النهضة العربية، 1992، ص 119.

[20]- نص عليه الفصل 443 من القانون الجنائي المغربي.

[21] - وهو ذلك الفرع الذي يتأسس في كل النظم القانونية المختلفة على مبدأ دستوري هو الشرعية، أي شرعية التجريم والعقاب، الذي تنبثق عنه قاعدة الشرعية الإجرائية.

[22] -المادة 36 من قانون المسطرة الجنائية كما تم تعديله وتتميمه بمقتضى القانون رقم 23.05 والقانون رقم 24.05، الجريدة الرسمية عدد 5374 بتاريخ فاتح ديسمبر2005، تقابلها المادة 29 من الأمر رقم 66-155 المؤرخ في 8يونيو 1966، المتضمن قانون الإجراءات الإجراءات الجزائية، المعدل والمتمم بالقانون رقم 17-07 مؤرخ في 27 مارس سنة2017، الجريدة الرسمية رقم 20 ل 29مارس 2017.

[23] -المادتين 16 و12 على التوالي من قانوني الإجراءات الجزائية المغربي والجزائري.

[24] -تم إضافة هذا التعديل بالقانون 04-04 المؤرخ في 10نوفمبر 2004، الجريدة الرسمية 71 لنفس السنة.

[25] - وتنص المادة 99 من قانون المسطرة الجنائية على أنه:" يجوز لقاضي التحقيق ان ينتقل إلى أي مكان لإجراء المعاينات المفيدة، أو للقيام بالتفتيش، ويشعر بذلك النيابة العامة التي لممثلها الخيار في مرافقته... " .إلا انه و بالرجوع إلى المادة 57 من قانون المسطرة الجنائية نجد أن المشرع قد ألزم ضباط الشرطة القضائية بالانتقال الفوري إلى مكان ارتكاب الجريمة ايضا وإجراء المعاينة المفيدة في الحفاظ على الأدلة القابلة للاندثار، وعلى ما يمكن أن يساعد على إظهار الحقيقة وحجز الأدوات التي استعملت في ارتكاب الجريمة أو التي كانت معدة لارتكابها.

[26] - وبالرجوع إلى مشروع قانون المسطرة الجنائية نجد أن المشرع تدارك الأمر من خلال المادة 59 بتدارك النقص حيت ضمن المعطيات الإلكترونية بجانب المستندات والأوراق المادية والتفتيش الإلكتروني

[27]- المعايطة عمر منصور المعايطة، الطب الشرعي في خدمة الأمن والقضاء، جامعة نايف العربية للعلوم الأمنية، الرياض، 2007، ص 53.

[28]- ظاهرة الإجرام الإلكتروني ومخطرها، أكاديمية شرطة دبي، مركز البحوث والدراسات تاريخ الانعقاد: 26 نيسان 2003 تاريخ الانتهاء: 28 نيسان 2003 الدولة: دبي ء الامارات العربية المتحدة. http://www.th3professional.com/2010/11/blog-post_5845.html)

[29] -تم عقدها في 8 نوفمبر 2001، مجلس وزراء أوروبا.

[30] -بدون مؤلف، الجرائم المرتبطة بتكنولوجيا المعلومات، مقال منشور على رابط الانترنيت:7o9o9.blogspot.com ،ص3.