الإطار القانوني المغربي للجرائم الإلكترونية بين التشريع الوطني والاتفاقيات الدولية


أمين السحيمي
إطار تربوي
الأكاديمية الجهوية للتربية والتكوين لجهة الشرق وجدة، المغرب.

د. عبد المجيد بوفرعة
باحث في اللغة العربية وآدابها
الأكاديمية الجهوية للتربية والتكوين لجهة الشرق وجدة، المغرب

ملخص:

يشهد العالم تطورًا سريعًا في مجال التكنولوجيا، مما أدى إلى ظهور جرائم إلكترونية تتطلب تشريعات خاصة لمواجهتها. في المغرب، تم تطوير إطار قانوني لمكافحة الجرائم الإلكترونية يجمع بين التشريعات الوطنية والالتزامات الدولية. يتناول هذا الإطار القوانين الوطنية التي تم وضعها لحماية الأفراد والمؤسسات من الجرائم المرتبطة بالتكنولوجيا الرقمية، مثل قانون مكافحة جرائم الإنترنت. كما يسلط الضوء على دور المغرب في الاتفاقيات الدولية التي تهدف إلى تعزيز التعاون العالمي في مكافحة هذه الجرائم، وضمان توافق التشريعات المحلية مع المعايير الدولية.

كلمات مفتاحية: الجريمة الإلكترونية - جرائم الإنترنت - التشريع المغربي - المعاهدات الدولية - المكافحة.

الاستشهاد المرجعي بالدراسة:

السحيمي، أمين. بوفرعة، عبد المجيد (2024، شتنبر). الإطار القانوني المغربي للجرائم الإلكترونية بين التشريع الوطني والاتفاقيات الدولية. مجلة البحث في العلوم الإنسانية والمعرفية، المجلد 1، العدد 6، السنة الأولى، ص 234-272.

Abstract:

The world is witnessing rapid advancements in technology، leading to the emergence of cybercrimes that necessitate specific legislation to combat them. In Morocco، a legal framework has been developed to counter cybercrimes، combining both domestic legislation and international commitments. This framework encompasses national laws enacted to protect individuals and institutions from crimes related to digital technology، such as the Cybercrime Law. It also highlights Morocco's role in international conventions aimed at strengthening global cooperation in combating these crimes and ensuring the alignment of domestic legislation with international standards.

Keywords : Cybercrime - Internet crimes - Moroccan legislation - International treaties – prevention.

مقدمة

شهد العالم تحولًا كبيرًا في العقود الأخيرة من القرن العشرين بفعل الثورة التكنولوجية، حيث أدت هذه التقنيات الجديدة إلى ظهور أشكال جديدة من الجريمة لم تكن معتادة سابقًا. يُطلق عليها "الجرائم الإلكترونية"، وتعتمد هذه الجرائم على استخدام أجهزة الحاسوب وشبكة الإنترنت ومجموعة متنوعة من البرامج التقنية.

وتمتاز الجريمة الإلكترونية في كونها عابرة للحدود، تحدث في مكان معين وضحاياها في مكان آخر، إلى جانب السرعة في تنفيذها والسرعة في إتلاف الأدلة ومحو آثارها، ناهيك عن كونها ترتكب من طرف أشخاص غير عاديين يتمتعون بذكاء خارق وتقنية عالية في التعامل مع التقنية المعلوماتية وأجهزة الحاسوب.

حيث أصبحت الجرائم الإلكترونية تشكل تهديدًا حقيقيا لكافة المجتمعات، لكون الأنظمة والأدوات الإلكترونية أصبحت أساسية في حياة الناس وتحمل الكثير من الثروات والمعلومات الحساسة، كما باتت تتسبب في أضرار كبيرة تتفوق على الجرائم التقليدية، وذلك بفضل سهولة ارتكابها وتوفر المعرفة التقنية للجناة، فضلاً عن الفوائد المادية والمعنوية التي تجنيها هذه الجرائم، مما جعل من الضروري خلق تعاون دولي وإقليمي لمكافحتها، وضع قواعد ونظم معقدة للتعامل معها، بالإضافة إلى ضرورة تطوير مهارات أطر خاصة لكشفها ومواجهة هذا التحدي الفني الفريد.

وفي هذا السياق يجب أن نشير إلى ما قاله أستاذ القانون الجنائي الفرنسي الشهير "جورج لبفاستر" إنّ هناك ما يسمى "**بوطنية**" السياسة التشريعية، بمعنى أن لكل دولة سياسة تشريعية تتبعها، وبالتالي لا يتصور أن تتطابق سياستان

تشريعيتان لدولتين أو أكثر تطابقاً تاما في ضوء المتغيرات الاجتماعية والاقتصادية والأمنية والسياسية لكل منها[1].

أهداف البحث

يسعى البحث إلى تحقيق الأهداف التالية:

- التعريف بالجرائم الإلكترونية وأنماطها أركانها وأنواعها المرتكبة، باعتبارها سلوكات لها آثار سلبية وخيمة على المجتمعات؛
- الوقوف على مدى إحاطة التشريعات المغربية بجوانب الجرائم الإلكترونية ومعاقبة مرتكبيها؛
- إبراز مواكبة المشرع المغربي للتطورات المتسارعة في عصر الثورة الرقمية ومدى تمكنه من الحفاظ على المجتمع من كافة المخاطر وتهديدات للجرائم الإلكترونية؛

أهمية البحث

تتمثل أهمية البحث فيما يلي:

- استجلاء مفهوم الجريمة الإلكترونية وخصائصها وأركانها؛
- تعرف الاتفاقيات والمعاهدات الدولية والسياسة التشريعية المغربية في الإحاطة بجميع جوانب الجريمة الإلكترونية، ومدى مواكبتها والثورة الرقمية التي يعرفها العالم؛
- تبين موقف المشرع المغربي حيال الجرائم الإلكترونية، والأفعال والسلوكيات التي تشكل جريمة إلكترونية من وجهة نظره؛

[1] عبيد صالح حسن، ***سياسة المشرع الإماراتي لمواجهة الجرائم الإلكترونية***، دورية الفكر الشرطي، المجلد الرابع والعشرون. العدد الرابع العدد رقم (95). أكتوبر 2015م، الإمارات العربية المتحدة، صفحة 24

إشكالية البحث

تتجلى مشكلة البحث في تأثير الجرائم الإلكترونية بأشكالها المتنوعة على المجتمع، باعتبارها تشكل تهديدا مستمرا للتقدم التنموي للمجتمع ولأنشطته الاقتصادية والإدارية والمالية، بسبب التطور الهائل في الأدوات الرقمية والإلكترونية والثورة المعلوماتية، كما تشكل خطورة كبيرة على أمن المجتمع ووحدته بسبب طابع بعض أنماطها العابر للحدود، مما يتطلب مما يتطلب ترسانة قانونية وتشريعية دقيقة وذات فاعلية كبيرة لمواجهة هذه الجرائم والتكيف مع تطورها المستمر وتنوعها.

إن الخصوصيات التي تطبع الجرائم المعلوماتية سواء من حيث طبيعة مرتكبيها أو من حيث المضمون أو من حيث التطبيق القضائي تطرح أمامنا تساؤلات أساسية حول الكيفية التي تعامل بها التشريع المغربي من أجل إحتواء هذا النوع من الجرائم سواء من خلال تبني النصوص المجرمة الكفيلة بتحقيق استراتيجيات موازية ترمي إلى خلق تنسيق بين مختلف الأجهزة المعنية من أجل مواجهة هذه الجرائم، كما يمكن التساؤل عن الخصوصيات التي تميز هذا النوع من الإجرام على المستوى التطبيق العملي.[1]

ومن هنا تأتي إشكالية البحث التي يمكن صياغتها على الشكل الآتي:

"ما مدى قدرة المشرع المغربي على التصدي للجريمة الإلكترونية وقدرته علي على التكيف مع تطورها الدائم؟"

تساؤلات البحث

يسعى هذا البحث إلى الإجابة على التساؤلات التالية:

- ماهية الجريمة الإلكترونية؟

[1] علال فالي، ***خصوصية الجريمة المعلوماتية***، مقال بمجلة القضاء التجاري الثاني، الرباط، 2013، ص123.

- ما هي أنواع الجريمة الإلكترونية؟
- ما هي خصائص وأركان الجريمة الإلكترونية؟
- ما هي المعاهدات والقوانين المغربية التي تأطر التعامل مع الجرائم الإلكترونية؟

منهجية البحث

يعتمد إجراء هذا البحث على المنهج الوصفي التحليلي، عبر الوصف والبيان لماهية الجرائم الإلكترونية وأنماطها وخصائصها وأركانها ومخاطرها، وتعرف الاتفاقيات والمعاهدات الدولية وكذا التشريعات المغربية التي تحيط بالجريمة الإلكترونية، وبيان مدى تطورها وتكيفها وقدرتها على التعامل مع جميع أنواع الجرائم الإلكترونية.

خطة البحث

سيتم تقسيم البحث على الشكل التالي:

الفصل الأول سيتم التطرق إلى الإطار النظري، حيث يتناول **المبحث الأول**: مفهوم الجريمة **الإلكترونية**، من خلال المطلب الأول: تعريف الجريمة الإلكترونية، والمطلب الثاني: خصائص الجريمة الإلكترونية، والمطلب الثالث: أنواع الجريمة الإلكترونية، **والمبحث الثاني:** أركان الجريمة الإلكترونية، من خلال المطلب الأول: الركن المادي للجريمة الإلكترونية، والمطلب الثاني: الركن المعنوي للجريمة الإلكترونية.

أما **الفصل الثاني** سيتطرق للمعالجة القانونية للجريمة الإلكترونية، من خلال **المبحث الأول**: اتفاقيات ومعاهدات دولية منظمة للجرائم الإلكترونية **والمبحث الثاني:** التشريعات المغربية المرتبطة بالجريمة الإلكترونية، ثم خاتمة وخلاصات وتوصيات.

الفصل الأول: الإطار النظري للبحث

المبحث الأول: مفهوم الجريمة الإلكترونية

تعد الجريمة الإلكترونية واحدة من الآثار السلبية التي نتجت عن التقنية العالية، حيث استحوذت اهتمام العديد من الفقها، ونتيجة لهذا الاهتمام، ظهرت عدة مصطلحات للإشارة إلى هذه الجرائم، منها "جرائم الحاسوب"، و"جرائم التقنية العالية"، و"جرائم المعلوماتية"، و"جرائم الغش المعلوماتي"، وصولاً إلى "جرائم الإنترنت". ويعتبر عدم التوصل إلى استقرار على مصطلح واحد للإشارة إلى الجريمة الإلكترونية من بين التحديات التي تواجه فهمها وتصنيفها.

وعندما نتطرق الى تعريف الجريمة الإلكترونية يتبين لنا أن لها نفس قالب الجريمة العادية، ولكن حين الخوض في التعريف والأركان فإننا سنتفاجأ بالفرق الكبير بين الجريمتين فمن عالم واقعي إلى عالم افتراضي أوجدته الثورة التكنولوجية فهذه الأخيرة باعتبارها جريمة مستحدثة نسبيا أثارت ضجة في الأوساط الفقهية بخصوص تحديد ماهيتها وخصائصها والأفعال الإجرامية في نطاقها، لذلك ارتأينا التعرض لماهية الجريمة الإلكترونية. [1]

المطلب الأول: تعريف الجريمة الإلكترونية

تنوعت التصورات حول تعريف الجريمة الإلكترونية، حيث اعتمد كل رأي تفسيراً لها بناءً على الزاوية التي نظر من خلالها، أو استنادًا إلى وسيلة ارتكابها، أو موضوعها، أو مدى توفر المعرفة بتقنية المعلومات لدى مرتكبها، أو بناءً على معايير أخرى حسب وجهة نظر القائلين بها. وقد أدى هذا التنوع عدم الاستقرار حول تعريف محدد للجريمة الإلكترونية، حيث قام مكتب تقييم التقنية في الولايات المتحدة بتعريفها من خلال تحديدها كـ "الجرائم التي تعتمد بيانات الحاسوب وبرامج

[1] خالد ممدوح إبراهيم، ***الجرائم المعلوماتية***، مطبعة دار الفكر الجامعي، الإسكندرية، الطبعة الأولى، 2009، ص 60.

المعلومات بشكل رئيسي"، وفي هذا السياق، تم تحديدها أيضًا على أنها "نشاط جنائي يشكل اعتداءً على برامج وبيانات الحاسوب"، وأيضًا بأنها "كل استخدام غير مشروع لتقنية المعلومات، يهدف إلى الاعتداء على أي مصلحة مشروعة، سواء كانت مادية أو معنوية".

كما أشارت الأمم المتحدة في المدونة الصادرة عنها بشأن الجريمة المعلوماتية، إلى الخلاف الواقع بين الخبراء حول ماهية العناصر المكونة لجرائم الكمبيوتر أو حتى المتعلقة بالكمبيوتر ولعل ذلك ما يفسر عدم التوصل إلى تعريف متفق علية دوليا لهذه المصطلحات وإن كان هؤلاء قد اتفقوا ضمنيا على وجود ظاهرة تتزايد بمعدلات عالية لتلك الجرائم.[1]

وتتكون الجريمة الإلكترونية (cyber crimes) من مقطعين هما الجريمة والإلكترونية، حيث يستخدم مصطلح **الإلكترونية** لوصف فكرة جزء من الحاسب أو عصر المعلومات، أما **الجريمة** فهي السلوكيات والأفعال الخارجة على القانون. والجرائم الإلكترونية هي " المخالفات التي ترتكب ضد الأفرا د أو المجموعات بدافع الجريمة وبقصد إيذاء سمعة الضحية أو أذى مادي او عقلي للضحية مباشر او غير مباشر باستخدام شبكات الاتصالات مثل الإنترنت مثل غرف الدردشة، والبريد الإلكتروني، والموبايل.[(2)]

كما يمكننا القول إن الجريمة الإلكترونية هي "جريمة ذات الطابع المادي، التي تتمثل في كل سلوك غير قانوني من خلال خسارة مقابلة وغالباً ما يكون هدف هذه

[1] عبد العالي الدربي ومحمد صادق إسماعيل، "الجرائم الإلكترونية" دراسة قانونية قضائية مقارنة، الطبعة الأولى، القاهرة، ص 42.

[2] ذياب موسي البداينة، ورقة عمل بعنوان الجرائم الالكترونية المفهوم والاسباب، عمان المملكة الاردنية الهاشمية، 2014، الملتقي العلمي الجرائم المستحدثة في ظل المتغيرات والتحولات الاقليمية والدولية خلال الفترة 2-9/4 لعام 2014.

الجرائم هو القرصنة من أجل سرقة أو إتلاف المعلومات الموجودة في الأجهزة ومن ثم ابتزاز الأشخاص باستخدام تلك المعلومات". [1]

وبدوره بم يعمل المشرع المغربي على تحديد إطار واضح أو تعريف دقيق ومحدد للجريمة الإلكترونية، وذلك حسب ما ذهب إليه البعض جاء بهدف عدم حصر القاعدة التجريمية في إطار معين نتيجة للتطور العلمي والتقني الذي تعرفه التقنيات الإلكترونية.

خلاصة لما سبق يمكن إجمال الجريمة الإلكترونية "بأنها **سلوكيات غير قانونية** يقدم على ارتكابها فرد أو مجموعة من الأفراد **بواسطة الأجهزة الذكية والمو اقع الإلكترونية** بهدف تحقيق مكاسب مختلفة، ويكون ذلك عن طريق ابتزاز الضحية وتهديدها وتخريب صورتها أمام المجتمع الواقعي والافتراضي، أما بحسب وجهة نظر المجتمع الدولي فقد اعتبر الجريمة الالكترونية بأنها ممارسات وأعمال تتعلق بجهاز الحاسوب تسعى لتحقيق مكاسب مادية او شخصية او التسبب بضرر". [2]

المطلب الثاني: خصائص الجريمة الإلكترونية

تتميز الجريمة الإلكترونية بعدة خصائص تميزها عن الجرائم التقليدية، ومن بين هذه الخصائص:

1. عابرة للحدود:

إن قدرة تقنية الإنترنت على اختصار المسافات، انعكست على طبيعة الأعمال الإجرامية ولم تعد الجريمة محلية، بل أصبحت عالمية، والجريمة الإلكترونية يرتكبها

[1] ورقة عمل، الجرائم الالكترونية، مديرية تكنولوجيا المعلومات، قسم نظم المعلومات شعبة امنية المعلومات، دولة العراق

[2] رؤى احمد جرادات وماسة سامر شيب، موسوعة ودق القانونية، رابط الموقع: https://wadaq.info، تاريخ الاطلاع: 22 نونبر 2023

صاحبها عن بعد وهو يعني عدم التواجد المادي للجرم المعلوماتي في مكان الجريمة.[1]

أي عدم وجود القيود الجغرافية، حيث يمكن للمجرمين تنفيذ جرائمهم عبر العالم أجمع، نظرا كون العالم متصل أو مترابط بشبكة واحدة من الاتصالات من خلال الأقمار الصناعية والفضائيات والإنترنت، جعل انتشار جريمة أمرا سلسا وشائعا، لا يعترف بالحدود الإقليمية للدول، ولا بالمكان ولا بالزمان.

2. التعقيد والتنوع:

تنوع الجرائم: تشمل الجرائم الإلكترونية مجموعة واسعة من الأنشطة الإجرامية، مثل اختراق الأمان، والاحتيال الإلكتروني، وانتشار البرمجيات الخبيثة.

تعقيد الأساليب: يستخدم الجناة تقنيات متقدمة ومعقدة لتنفيذ جرائمهم، مما يجعل من التحقيق والكشف عنها أمورًا صعبة.

3. السرعة والفورية:

يمكن أداء الجرائم الإلكترونية بشكل فوري وسريع، مما يزيد من صعوبة اكتشافها ومحاكمة المتورطين. حيث لأنه "بضغطة واحدة على لوحة المفاتيح يمكن أن تنتقل ملايين الدولارات من مكان إلى آخر، وهذا لا يعني إنها لا تتطلب الإعداد قبل التنفيذ أو استخدام معدات وبرامج معينة." [2]

4. التنفيذ عن بعد:

لا تتطلب جرائم الإلكترونية بالضرورة وجود الفاعل في مصرح الجريمة، بل يمكن للفاعل تنفيذ جريمته وهو في دولة بعيدة كل البعد عن الضحية سواء كان من خلال الدخول للشبكة المعنية أو اعترض عملية تحويل مالية أو سرقة معلومات هامة أو تخريب.[3]

---

[1] خالد ممدوح إبراهيم، ***أمن الجريمة الإلكترونية***، الدار الجامعية – الإسكندرية، 2008، ص 44 .

[2] عبد العالي الدربي ومحمد صادق إسماعيل، مرجع سابق، الصفحة 55.

[3] المرجع نفسه، الصفحة 55.

5. جرائم ناعمة:

وهي بخلاف الجريمة التقليدية التي تتطلب استخدام الأدوات وممارسة العنف أو استعمال الآلات الحادة مثل جرائم الإرهاب والمخدرات والسرقة والسطو المسلح، إلا أن الجرائم الالكترونية فهي جرائم ناعمة لا تتطلب عنف، فمثلا عملية السطو على أرصدة بنك لن تستنزف أي خسائر بشرية أثناء نقل البيانات من حاسب إلى آخر مقابل السطو التقليدي الذي يمكن أن يؤدي إلى اشتباكات أو إطلاق نار مع رجال الأمن.

6. الجاذبية:

نظرا لما تمثله سوق الكمبيوتر والإنترنت من ثروة كبيرة للمجرمين أو الأجرام المنظم. فقد غدت أكثر جذبا لاستثمار الأموال وغسلها وتوظيف الكثير منها في تطوير تقنيات وأساليب تمكن الدخول إلى الشبكات وسرقة المعلومات وبيعها أو سرقة البنوك أو اعتراض العمليات المالية وتحويلا مسارها أو استخدام أرقام البطاقات...الخ.

7. الأثر على الأفراد والمؤسسات:

يمكن للجرائم الإلكترونية أن تؤثر على الأفراد والشركات على نطاق واسع، سواء من حيث الخسائر المالية أو التأثير على الخصوصية الشخصية، ثم قد يتعدى تأثيرها ليهدد نظام القيم والنظام الأخلاقي خاصة في المجتمعات المحافظة والمغلقة.

8. التحديات القانونية:

تعقيد التشريعات: يواجه القانون تحديات في مواكبة التطورات التكنولوجية، وتحديد القوانين الملائمة لمعاقبة مرتكبي الجرائم الإلكترونية.

9. صعوبة الإثبات والاكتشاف

الجريمة الإلكترونية تفتقر لوجود الآثار التقليدية للجريمة (مثل: بصمات. تخريب، شواهد مادية) ويسهل محو الدليل أو تدميره في زمن متناه القصر، فهي

مجرّد أرقام تتغير في السجلات، ومعظمها تم اكتشافها بالصدفة وبعد وقت طويل من ارتكابها.

وتعود أسباب صعوبة إثباتها إلى أن متابعتها واكتشافها من الصعوبة بمكان، حيث أنها لا تترك أثراً فما هي إلا أرقام تدور في السجلات. كما أن الجرائم التي لم تكتشف هي أكثر بكثير من تلك التي كشف عنها.[1]

10. عدم الإبلاغ

ناذرا ما يتم الإبلاغ عن الجريمة الإلكترونية إما لعدم اكتشاف الضحية لها، أو خوفا من التشهير، لذا نجد أن معظمها يكتشف بالمصادفة وبعد وقت طويل من ارتكابها.

فهذه الخصائص تبرز تعقيد وتحديات مكافحة الجريمة الإلكترونية، وتؤكد على ضرورة التعاون الدولي وتطوير التقنيات الأمنية للتصدي لها بفعالية.

المطلب الثالث: أنواع الجريمة الإلكترونية

مع تطور أجهزة الحاسوب وبرامجه بزغت معه العديد من أنواع الجرائم الإلكترونية، إلا أننا في هذا البحث سنكتفي بأنواع أساسية يمكن إجماليها فيما يلي:

جرائم الابتزاز والتهديد للأفراد: هو ما يمارسه المبتز من تهديد للمجني عليه بعد حصوله على معلومات تخص المجني عليه كالتسجيلات الصوتية، أو الصور الشخصية بهدف تحقيق رغباته التي يسعى إليها، سواءً أكانت مادية أو معنوية.[2]

التشهير الإلكتروني بحق الأشخاص من خلال الذم والتحقير والقدح، وذلك عن طريق نشر معلومات عن شخص او هيئة معينة تنسب اليها بشكل مباشر.

---

[1] عبد الصبور عبد القوي على مصري، المحكمة الرقمية والجريمة المعلوماتية، مكتبة القانون والاقتصاد، الرياض، طبعة الأولى، 2012، ص 51.

[2] ممدوح رشيد مشرف الرشيد، **الحماية الجنائية للمجني عليه من الابتزاز**، المجلة العربية للدراسات الأنية، المجلد: 33، العدد: 70، ص: 199.

الجرائم الإلكترونية السياسية التي تعنى باستهداف الأمور السياسية الحساسة والهامة في الدولة، والتطفل على امن الدولة وسرقة المعلومات من خلال انتهاك المواقع العسكرية والسياسية التابعة للدولة.

الجرائم الإلكترونية لتزوير الهوية: وذلك من خلال انتحال شخصيات الافراد على مواقع التواصل بسرقة معلوماتهم الشخصية واستخدامها لأغراض غير قانونية.

جرائم ضد الملكية: وتكون عن طريق نشر روابط تؤدي الى الوصول الى الأجهزة وسرقة ما فيها من بيانات وبرامج وتعطيل تلك الأجهزة إما بشكل كلي او جزئي.

أو بعبارة أخرى هي انتقال برمجيات ضارة المضمنة في بعض البرامج التطبيقية والخدمية، أو غيرها لتدميرالأجهزة أو البرامج المملوكة للشركات أو الأجهزة الحكومية أو البنوك أو حتى ممتلكات شخصية.[1]

المبحث الثاني: أركان الجريمة الإلكترونية

على غرار الجريمة التقليدية يتوقف وجود الجريمة الإلكترونية على توفر ثلاثة أركان أساسية تسمى بالأركان العامة للجريمة وهي الركن القانوني والمتمثل في النصوص القانونية التي تدين الجرم، والركن المادي المتمثل في السلوكيات والأفعال المادية المجرمة، والركن المعنوي المتمثل في القصد الجنائي للجريمة الإلكترونية.

المطلب الأول: الركن القانوني

نقصد بالركن القانوني للجريمة الإلكترونية أو توافر السند القانوني لتجريم الفعل، وذلك تطبيقا لمبدأ الشرعية بأن "لا جريمة ولا عقوبة إلا بنص" فلا يجوز

[1] كامل مطر، **الجريمة الالكترونية**، ورقة بحثية، ص 13.

القياس في التجريم،[1] والجرائم الإلكترونية حديثة وذات تقنية عالية، ووضع نصوص خاصة بها ليس بالأمر السهل.

المطلب الثاني: الركن المادي

لتتكون الجريمة لابد من ارتكاب فعل مادي محسوس يعاقب عليه القانون، فالجريمة ليست مجرد وجود نية إجرامية، إذا لابد لهذه النية من أن تتجسد في فعل مادي محسوس، ويقوم على طبيعة السلوك الإجرامي بالإضافة إلى النتيجة الحاصلة والعلاقة السببية.

المطلب الثالث: الركن المعنوي

وهو القصد الجنائي للجريمة الإلكترونية والذي بموجبه يتم القيام بالجريمة كما يقصد به الحالة النفسية والمزاجية لمرتكبي الجرائم الإلكترونية. ويعني كذلك العلم بعناصر الجريمة، بالتالي فإن هذا الركن يتكون من علم وإرادة، ويشترط توافر معرفة كاملة وإرادة واعية لدى المجرم لتنفيذ السلوك الإجرامي وبعوامل الجريمة والوسائل المستخدمة لتنفيذها.

الفصل الثاني: المعالجة القانونية للجريمة الإلكترونية

المبحث الأول: اتفاقيات ومعاهدات دولية منظمة للجرائم الإلكترونية

المطلب الأول: اتفاقية بيرن لحماية المصنفات الأدبية والفنية (9 شتنبر 1886) التي تديرها المنظمة العالمية للملكية الفكرية

تعد أهم الاتفاقيات، وذلك نظرا لتميزها وثرائها بمجموعة من الأحكام تحفظ حقوق المؤلف وكذا لمواكبتها لكل جديد في المعرفة وحماية المصنفات الرقمية، حيث أبرمت هذه الاتفاقية سنة 1886 وتم تنقيحها في باريس سنة 1896، وفي بيرن سنة 1908، واستكملت في بيرن سنة 1914، وتم تنقيحها في روما سنة 1928، وفي

[1] حنان ريحان مبارك، الجرائم المعلوماتية، دراسة مقارنة، منشورات الحلبي الحقوقية، ط1، 2014، ص56.

بروكسيل سنة 1948، وفي ستوكهولم سنة 1967، وفي باريس سنة 1971، وجرى تعديلها سنة 1979. تتناول اتفاقية بيرن حماية المصنفات وحقوق مؤلفيها، حيث تشمل المصنفات كل إنتاج في المجال الأدبي والعلمي والفني ،أيا كانت طريقة أو شكل التعبير عنه، وذلك ما نصت عليه المادة 2(1) من الاتفاقية، ولقد صادق المغرب على العديد من المعاهدات الدولية المتعلقة بحماية الملكية الفكرية وخاصة حقوق المؤلف، وأبرم العديد من الاتفاقيات المتعددة الأطراف والاتفاقيات الثنائية في هذا المجال، ويعد ثاني دولة عربية تصادق على اتفاقية برن بعد تونس، حيث انضم إليها المغرب بتاريخ 16 يونيو 1917، وصادق على آخر عقد تعديلي لها بباريس 24 يوليوز 1971 وبتاريخ 17 فبراير 1987 (الجريدة الرسمية عدد 1326 الصفحة 517، جريدة رسمية عدد 2019 صفحة 1698، جريدة رسمية عدد 3879 صفحة 220).

المطلب الثاني: اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية سنة 2000

تعد اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية، التي اعتمدت بموجب قرار الجمعية العامة للأمم المتحدة 25/55 المؤرخ في 15 تشرين الثاني/نوفمبر 2000، إطاراً قانونياً دولياً يمكن استخدامه لمكافحة الجريمة الإلكترونية من خلال تشجيع التعاون وتعزيز القدرات الوطنية والدولية.

عالجت هذه الاتفاقية كل ما يتعلق بالمساعدة القانونية المتبادلة في مجال مكافحة الجرائم المنظمة عبر الوطنية، كما أنها دعت جميع الدول إلى إبرام اتفاقيات قصد تعزيز محاربة الجرائم الالكترونية وتعزيز التعاون على منع هذه ومكافحتها بمزيد من الفعالية.

وصادق المغرب على هذه الاتفاقية، كما تم نشرها في الجريدة الرسمية رقم 5186 الصادرة يوم الخميس 12 فبراير 2004 بناء على محضر إيداع وثائق مصادقة المغرب على الاتفاقية المذكورة الموقع بنيويورك في 20 شتنبر 2002.

المطلب الثالث: اتفاقية بودابست لمكافحة الجرائم المعلوماتية بتاريخ 8 نونبر 2001

تعتبر هذه الاتفاقية من أهم الاتفاقيات الرامية إلى مكافحة الجرائم الإلكترونية عن طريق وضع نظام تعاون دولي يتميز بالسرعة و الفعالية في التنفيذ، بهدف وضع سياسة جنائية موحدة تمكن من ملاحقة المخلين بالأمن المعلوماتي والتنسيق بين التشريعات الوطنية لتسهيل مكافحة الإجرام المعلوماتي وخاصة على مستوى إجراءات التحقيق، ولقد صادق المغرب من خلال مجلس الحكومة بتاريخ 20 دجنبر 2012 على مشروع القانون رقم 12-136 الذي يوافق بموجبه على اتفاقية "بودابيست" المتعلقة بالجريمة المعلوماتية، حيث صدر فيما بعد القانون 136.12 الموافق بموجبه على هذه الاتفاقية وكذا على برتوكولها الإضافي الموقع بستراسبورغ بشأن تجريم الأفعال ذات الطبيعة العنصرية وكراهية الأجانب التي ترتكب عن طريق أنظمة الكمبيوتر في 28 يناير [8]2003، وذلك بتاريخ 29 ماي 2014، وفقا للظهير الشريف رقم 1.14.85الصادر في 12 ماي 2014 بالجريدة الرسمية عدد 6260 (الصفحة 4711).

وتجدر الإشارة إلى أن لمقتضيات المتعلقة بالقواعد الإجرائية اتخذت حيزا هاما ضمن أحكام اتفاقية بودابست، وذلك من خلال تخصيص 22 مادة من أصل48 مادة مكونة للاتفاقية المذكورة للقواعد الإجرائية، حيث تم التأكيد على ضرورة اعتماد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لإقرار القواعد الإجرائية الواردة في الاتفاقية لأغراض الأبحاث والإجراءات الجنائية.

كما تضمنت هذه الاتفاقية آليات التعاون بين الدول في مجال الإجراءات بهدف إجراء تحقيقات أكثر فعالية فيما يتعلق بالجرائم الإلكترونية، حيث يمكن لإحدى الجهات أن تطلب من جهة أخرى أن تأمر أو تفرض حماية سريعة وبطريقة مختلفة لبيانات مخزنة في نظم معلوماتية داخل حدود هذه الجهة الثانية لتسهيل

عملية البحث عنها والوصول إليها، فبهذه الآلية يصبح الوصول إلى البيانات المخزنة خارج الحدود ممكنا وسهلا لأي جهة تود أو تطلب ذلك.

وقد عالجت هذه الاتفاقية في الفصل الثاني الجرائم المستحدثة التي ينبغي على القانون الجنائي أخذها بعين الاعتبار والعقوبات المطبقة على مرتكبيها.

وهكذا فقد عرضت لمجموعة من الجرائم نذكر منها:

- الولوج غير المشروع إلى النظام المعلوماتي؛
- الاعتراض غير القانوني على النظام المعلوماتي؛
- المساس بسلامة البيانات عن طريق إتلافها أو محوها أو إفسادها؛
- التزوير والغش المعلوماتي، وذلك عن طريق إدخال مثلا بيانات وهمية أو تغييرها أو حذفها؛
- الجرائم المتعلقة بالتعدي على سلامة النظام المعلوماتي.

وكذلك تطرقت الاتفاقية في الفصل الثالث إلى تحديد القواعد الواجب إتباعها في تسليم المجرمين وسبل تعزيز الحماية من الجرائم التقليدية والمعلوماتية.

وبينت طرق ربط الاتصال بين الدول الأعضاء من خلال النص على أن لكل دولة نقطة اتصال تعمل باستمرار على مدار 24 ساعة وطيلة أيام الأسبوع، وذلك بهدف ضمان تقديم المساعدة الفورية والفعالة أثناء التحقيق من الجرائم المرتبطة بنظم وبيانات إلكترونية، أو جمع الأدلة ذات الطابع الالكتروني عن هذه الجرائم.

ونظرا لأهمية التنسيق على مستوى الاتصالات، فإنها لم تغفل الجانب التقني، وهو ما يتجلى خلال إلزام الدول الأعضاء باعتماد وسائل اتصال جد متطورة وآمنة.

مما سبق، لا يمكننا أن ننكر أن هذه الاتفاقية شكلت خطوة هامة في مواجهة الجرائم العابرة للقارات، إلا أنه ما يمكننا أن نآخذها عليه، أنها أولت أهمية كبرى

للإجراءات الجنائية، لا سيما فيما يخص مرحلة التحقيق والملاحقة القضائية، ولم تولي الاهتمام للأحكام الموضوعية، فتركت الحرية للبلدان في سن تشريعات وطنية تلائم خصوصياتها، مما أدى إلى وجود اختلافات تشريعية عديدة وشاسعة بين هذه الدول، وخلق نوعا من التضارب بين هذه التشريعات.

المطلب الرابع: الاتفاقية العربية لمكافحة جرائم تقنية المعلومات

تهدف هذه الاتفاقية إلى تعزيز التعاون وتدعيمه بين الدول العربية في مجال مكافحة جرائم تقنية المعلومات، لدرء أخطار هذه الجرائم وحفاظا على الأمن الرقمي للدول العربية، ومصالحها، وسلامة مجتمعاتها، وأفرادها.

ولقد صادق المغرب على هذه الاتفاقية، حيث صدر بظهير شريف رقم 1.13.44 الصادر في فاتح جمادى الأولى 1434 الموافق 13 مارس 2013 القانون 75.12 الموافق بموجبه على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، الموقعة بالقاهرة في 21 دجنبر 2010، والمنشور بالجريدة الرسمية عدد 6140 (الصفحة 3023).

إلا أنه من جملة ما يآخذ على هذه الاتفاقية أن العديد من موادها يستخدم مصطلحات فضفاضة، سواء تعلق الأمر بالتجريم أو بجمع البيانات والمعلومات عن المستخدمين أو حتى المبادئ العامة التي استندت عليها، مما يمكنه أن يؤثر سلبا على الحقوق والحريات التي تتصل بحرية التعبير والحق في الخصوصية، وبشكل عام تفتقد الاتفاقية مراعاة مبادئ الشفافية والوضوح والتناسب في صياغة موادها، مما يمكنه أن يشكل قيدا على نطاق واسع للنشاط الرقمي.

المبحث الثاني: التشريعات المغربية المرتبطة بالجريمة الإلكترونية

لقد برهن المشرع المغربي من خلال بعض التشريعات أنه مصر على الانتقال من مرحلة التعامل الورقي إلى مرحلة التعامل الالكتروني، وسنعرض هذه التشريعات والتي تتمثل في الجريمة الالكترونية في القانون الجنائي المغربي الذي خصص لها حيزا مهما، وبالإضافة إليه توجد تشريعات أخرى تناولت بعض القضايا التي لها صلة بالجريمة الالكترونية:

المطلب الأول: الجريمة الإلكترونية في القانون الجنائي المغربي.

- **القانون رقم 07.03 المتعلق بمكافحة جرائم المس بنظم المعالجة الآلية للمعطيات**

اتخذت الجريمة الإلكترونية في المملكة المغربية خلال العقود الأخيرة صورا متعددة، مما دفع المشرع إلى سن تشريع مهم، لكونه صدر لسد الفراغ التشريعي في مجال مكافحة الجرائم المعلوماتية، وهو القانون رقم 03-07 بشأن تتميم مجموعة القانون الجنائي فيما يتعلق بالإخلال بسير نظم المعالجة الآلية للمعطيات، ويحتوي هذا القانون على تسعة فصول (من الفصل 3-607 إلى الفصل 11-607 من مجموعة القانون الجنائي المغربي) [1]. وأول ما يلاحظ هو عدم قيام المشرع المغربي بوضع تعريف لنظام المعالجة الآلية للمعطيات، ويبدو أن المشرع قصد ذلك، بحيث ترك ذلك للفقه والقضاء، هذا الأخير المكلف بتطبيق بنود هذا التشريع، ثم إن المجال المعلوماتي هو مجال حديث ومتجدد، وبالتالي فإن أي تعريف يتم وضعه قد يصبح متجاوزاً فيما بعد، في ضوء التطور المذهل لقطاع تكنولوجيات الاتصالات والمعلومات، وعليه، فقد أحسن المشرع المغربي عند عدم وضعه لتعريف خاص بنظام المعالجة الآلية للمعطيات.

[1] عبد السلام بنسليمان، الاجرام المعلوماتي في التشريع المغربي: دراسة نقدية مقارنة في ضوء آراء الفقه وأحكام القضاء، ص 74.

وعند رجوعنا للقانون الفرنسي مثلا بشأن الغش المعلوماتي لسنة 1988[1]، نلاحظ أن هذا التشريع كذلك لم يحدد مفهوم نظام المعالجة الآلية للمعطيات، بل اقتصر على بيان أوجه الانتهاكات المتعلقة بهذا النظام وعقوباتها.

ولعل القراءة الشمولية لمقتضيات هذا التشريع المغربي تمكننا من حصر الأفعال المجرمة التالية:

1. الدخول الاحتيالي إلى مجموع أو بعض نظام للمعالجة الآلية للمعطيات.
2. البقاء في نظام للمعالجة الآلية للمعطيات بعد الدخول خطأ فيه.
3. حذف أو تغيير المعطيات المدرجة في نظام المعالجة الآلية للمعطيات أو التسبب في اضطراب في سيره.
4. العرقلة العمدية لسير نظام المعالجة الآلية للمعطيات أو إحداث خلل فيه.
5. إدخال معطيات في نظام للمعالجة الآلية للمعطيات أو إتلافها أو حذفها منه أو تغيير المعطيات المدرجة فيه، أو تغيير طريقة معالجتها أو طريقة إرسالها بشكل احتيالي.
6. التزوير أو التزييف لوثائق المعلوميات أيا كان شكلها إذا كان من شان التزوير أو التزييف الحاق ضرر بالغير.
7. استعمال وثائق معلوميات مزورة أو مزيفة.
8. صنع تجهيزات، أو أدوات، أو إعداد برامج للمعلوميات، أو أية معطيات أعدت أو اعتمدت خصيصا لأجل ارتكاب هذه الجرائم أو تملكها أو حيازتها أو التخلي عنها للغير أو عرضها رهن إشارة الغير.

[1] خالد عثماني، مكافحة الجريمة الالكترونية في ضوء التشريع المغربي، مجلة العلوم الجنائية، ص 39.

9. محاولة ارتكاب الجرائم المذكورة.

10. المشاركة في عصابة أو اتفاق لأجل الإعداد لواحدة أو أكثر من هذه الجرائم.[1]

يعد القانون رقم 07.03 المتعلق بمكافحة جرائم المس بنظم المعالجة الآلية للمعطيات من أهم النصوص التي أضيفت لمجموعة القانون الجنائي المغربي من أجل سد الفراغ في مجال مكافحة الجريمة الإلكترونية، ويحتوي هذا القانون على تسعة فصول من 607.3 إلى 607.11 من مجموعة القانون الجنائي المغربي، حيث وضعت هذه الفصول الإطار القانوني الخاص بتجريم الأفعال التي تعتبر جرائم ضد نظم المعالجة الآلية للمعطيات ، غير المشروع للنظام المعلوماتي، أو البقاء فيه، أو تغيير المعطيات داخل هذا النظام، حيث ساوى المشرع في قيام المسؤولية الجنائية بين الولوج إلى جزء من النظام والولوج إلى كامل النظام، المهم أن يكون ذلك قد تم عن طريق الاحتيال[2].

وعلى خلاف بعض التشريعات التي قيدت تجريم الدخول بضرورة توافر قصد جنائي خاص لدى المتهم، يتجلى في ضرورة التأثير في نظام المعالجة كما هو الحال بالنسبة للقانون الألماني، فإن المشرع المغربي أورد هذا التجريم (الولوج أو الدخول) بشكل مطلق دون استلزام قصد خاص أو شرط معين، حيث تقع الجريمة بمجرد القيام بهذا النشاط المجرم، ولا يهم أن تحدث نتيجة معينة، فهي جريمة خطر وليس جريمة ضرر، المهم أن العملية تمت، سواء كان المتهم عالما بعدم موافقة صاحب النظام أو غير عالم بذلك، ومن جهة أخرى، يتضح أن المشرع المغربي قد أضفى صفة عدم المشروعية على فعل الدخول متى كان هذا الأخير مقصودا أي بإرادة الجاني، أما إذا كان مصادفة وهو ما يسمى بالدخول العرضي أو بطريق الخطأ، فإن عدم

[1] خالد عثماني، مكافحة الجريمة الالكترونية في ضوء التشريع المغربي، مجلة العلوم الجنائية، ص 39.

[2] محمد جوهر: خصوصيات زجر الإجرام المعلوماتي، المجلة المغربية للقانون والاقتصاد والتدبير، العدد52، 2006، ص87.

المشروعية تنتفي عنه لكن شريطة الانسحاب فور اكتشاف الدخول الخطير، أما إذا بقي فيه، فيعتبر دخوله منذ ذلك المدة كالبقاء غير المشروع.

والدليل على أن هذه الجريمة تعد جريمة شكلية، هو ان المشرع المغربي قد شدد عقوبة الولوج، كما هو وارد في الفقرة الأولى من الفصل 607.3، إذا ترتب عليه ضرر كحذف أو تغيير المعطيات والبيانات المدرجة في نظام المعالجة.

في حين نص، الفصل 607-4 على معاقبة كل من دخل إلى مجموع أو بعض من نظام المعالجة الآلية، عن طريق الاحتيال، يفترض أنها تتضمن معلومات تخص الأمن الداخلي أو الخارجي للدولة وتهم الاقتصاد الوطني، وشدد العقوبة في حق الموظفين أو المستخدمين الدين يرتكبون هذا الفعل وكذلك في حق الأشخاص الذين يترتب عن دخولهم بواسطة الاحتيال للأنظمة المشار إليها حذف أو اضطراب في سير النظام أو تغيير للمعطيات المدرجة. [1]

كما نجد أن الفصل 607-5 يعاقب كل من عرقل عمدا سير نظام المعالجة الآلية أو أحدث فيه خللا، حيث منح هذا الفصل سلطة تقديرية واسعة في إدخال كل سلوك بإمكانه عرقلة سير النظام أو إحداث خلل فيه، وهذا الأمر من شأنه أن يخل بمبدأ الشرعية الجنائية الذي يقضي بضرورة تحديد وحصر الأفعال الجنائية المجرمة حتى يكون الشخص على بينة من أمره، حتى تتحقق بذلك الإرادة السليمة في إتيان الفعل المجرم من عدم إتيانه.

أما فيما يخص النشاط الإجرامي لجريمة الاعتداء على المعطيات، ينص الفصل 607-6 على معاقبة "..من أدخل معطيات في نظام المعالجة الآلية للمعطيات أو أتلفها أو حذفها منه أو غير المعطيات المدرجة فيه، أو غير طريقة معالجتها أو طريقة إرسالها عن طريق الاحتيال"، وعليه فكل واحد من هذه الأفعال يشكل جريمة

[1] محمد جوهر: خصوصيات زجر الإجرام المعلوماتي، مرجع سابق، ص87.

مستقلة وقائمة بذاتها، فلتقوم الجريمة يكفي أن يتحقق أحد هذه الأفعال كالإتلاف أو التغيير مثلا.

وتجدر الإشارة هنا، إلى أن هذه العملية، لا يمكنها أن تتم إلا إذا ولج المتهم إلى النظام عن طريق الاحتيال، مما يدفعنا إلى التساؤل عن جدوى التنصيص على جريمة الحذف باعتبارها ظرف تشديد من خلال الفصل 607-3، لذا يجب على المشرع أن يتدخل من أجل ضبط هذه الصورة ووضع حد لكل غموض من شأنه أن يلتبس على القاضي وهو بصدد إعمال النصوص القانونية على الوقائع المعروضة عليه.

كما فرض الفصل 607-7 عقوبات على التزوير وتزييف وثائق المعلوميات لمن يستعمل وثائق معلوماتية وهو يعلم أنها مزيفة أو مزورة، وفي هذا الصدد نجد الأستاذ محمد علمي مشيشي الإدريسي يرى أن الإحالة الضمنية لهذه المادة على القواعد العامة لا يمكن قبولها لا منطقيا ولا قانونيا نظرا لما يتميز به الزور المعلوماتي من خصوصيات لا يمكن أن تنفع معها الحلول المتبناة في جرائم الزور الكلاسيكية ويفضل اشتراط الوسيلة المستعملة على أن تكون تكنولوجية لتكون منسجمة بالتالي مع مفهوم الجريمة المعلوماتية.[1]

كما يلاحظ على هذا القانون أنه ربط تحقق جرائم التزوير والتزييف بشرط الإضرار بالغير، فمثلا لا يكفي لحصول جريمة التزوير إحداث تغيير في بطاقة الائتمان، وإنما يشترط حدوث الضرر بالغير.[2]

وعلى الرغم مما يمكن أن نبديه من ملاحظات بشأن الفصل 607-7 إلا أن ذلك لا يمنع من القول بأن المشرع المغربي قد أحسن صنعا حينما تدخل بهذا النص

[1] محمد علمي مشيشي الإدريسي، دراسة مقارنة حول ملاءمة مشروع القانون الجنائي مع المبادئ والقواعد المعتمدة في منظومة حقوق الإنسان، مس، ص215.

[2] عبد الجبار الحنيص، الحماية الجزائية لبطاقة الائتمان الممغنطة من التزوير، مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، المجلد 24، العدد الثاني، 2008، ص 167.

ليضع حدا للجدل الفقهي والقضائي الذي كان مثارا بشأن مدى اعتبار جريمة التزوير قائمة في حالة تزوير المعلومات والبيانات المخزنة بشكل الكتروني، وذلك من خلال العقاب مثلا على تزوير البطاقات واستعمالها لأغراض بنكية مثلا.

وفيما يخص المحاولة أو الشروع في الجرائم الواردة في هذا القانون، فقد نص المشرع المغربي صراحة على أن المحاولة تعاقب بنفس عقوبة الجريمة التامة كما يبدو من خلال الفصل 8-607، في حين يعرض الفصلان 9-607و 10-607 للمشاركة في الجرائم الماسة بنظم المعالجة الآلية للمعطيات، حيث أكد الفصل الأول على تطبيق نفس عقوبة الجريمة المرتكبة أو العقوبة المطبقة على الجريمة الأشد على كل من اشترك في عصابة أو اتفاق تم لأجل الإعداد لواحدة أو أكثر من الجرائم المنصوص عليها في هذا الباب إذا تمثل الإعداد في فعل أو أكثر من الأفعال المادية.

أما الفصل الثاني فقد عاقب على المشاركة والمساعدة إما بصنع تجهيزات، أو أدوات، أو إعداد برامج للمعلوميات مخصصة لأجل ارتكاب الجرائم المعاقب عليها في هذا الفصل أو تملكها أو حيازتها أو التخلي عنها للغير [1]، فمن خلال هذا الفصل نجد المشرع المغربي لم ينص على عنصر العمد في هذه الجريمة، تماشيا مع ما أشارت إليه اتفاقية بودابست، بغية الوقوف على ميولات وانطباعات شخصية الجاني والتحقق من نيته وإرادته في إتيان الأفعال المنصوص عليها في هذا الفصل.

وقد خص المشرع المغربي الفصل 11-607 لتحديد العقوبات الإضافية المقررة لجرائم المس بنظام المعالجة الآلية للمعطيات، والمتمثلة في المصادرة والحرمان من الحقوق الوطنية أو المدنية أو العائلية الواردة في الفصل 26 من القانون الجنائي[2] والحرمان من مزاولة الوظائف العمومية أو نشر الحكم الصادر بالإدانة، حيث باستقراء هذا الفصل، نجد أن المشرع المغربي وكإجراء تحفظي أجاز للمحكمة مع

[1] خالد عثماني، مكافحة الجريمة الالكترونية في ضوء التشريع المغربي، مجلة العلوم الجنائية المرجع نفسه، ص 40.
[2] الذي يحيل عليه الفصل 40 من ذات القانون.

مراعاة حقوق الغير حسن النية أن تحكم بمصادرة الأدوات التي استعملت في ارتكاب هذه الجرائم، مع الاحتفاظ للمحكمة بحق الحكم بتدابير وقائية أخرى.

وهكذا يتبين لنا باستقراء هذه النصوص، يمكننا إبداء مجموع من الملاحظات:

في البداية يمكننا الإشارة إلى أن المشرع المغربي لم يضع تعريفا لنظام المعالجة الآلية للمعطيات، ويبدو أن المشرع وكعادته ترك ذلك للفقه والقضاء، لأن المجال المعلوماتي مجال يتطور باستمرار وبوتيرة سريعة.

كما يمكننا أن نستشف من خلال قراءتنا لمضامين الفصول المتعلقة بمكافحة جرائم المس بنظم المعالجة الآلية للمعطيات، أن الأفعال المجرمة تنصب على البيانات أو المعطيات بشكل أساسي، أو ما يسميه بعض الفقه بالأملاك غير المادية[1]، وفي ذلك خروج عن التقسيم المتعارف عليه، من تقسيم الجرائم إلى جرائم تمس الأشخاص أو الأموال، وإن كانت البيانات والمعطيات تنطوي على أعمال إجرامية لها قيمة مالية أو اقتصادية أو معرفية أو شخصية...، إلا أن الملاحظ على هذا المستوى أن المشرع المغربي اكتفى بعبارة البيانات دون أن يضيف لها مصطلح المعلوماتية، وهو خطأ يجب تداركه، لأن البيانات يمكن أن تكون غير معلوماتية، وأن ما يميز البيانات في هذا المجال هو الصفة المعلوماتية التي تتمتع بها في علاقتها بالبيانات والمعطيات المادية.[2]

لم تشر النصوص السابقة إلى الاعتداء المادي على الأجهزة وأدوات الحاسب الآلي بالسرقة أو التخريب أو الإتلاف وذلك إيمانا من المشرع المغربي بأنها جرائم عادية تخضع للقانون الجنائي التقليدي كالسرقة.

---

[1] Mohamed ouzgane la criminalité informatique au regard du droit pénal marocain، centre marocain des études juridiques، Hommage au professeur Jallal Essaid، Tome I، 2005، p 236.

[2] عبد السلام بنسليمان، الإجرام المعلوماتي في التشريع المغربي: دراسة نقدية مقارنة في ضوء آراء الفقه وأحكام القضاء44 مرجع سابق، ص 67 – 68.

كما أن المشرع المغربي لم يتعرض إلى جريمة التحايل على الحاسوب الآلي وذلك بتحويل ونقل الأموال المتحصلة من الجرائم لغسلها أو تبييضها وذلك لتمويه مصدرها.

من خلال استقراء النصوص السابقة، يمكننا القول أن المفاهيم التي اعتمدها المشرع لتحديد الجرائم الماسة بنظام المعالجة الآلية للمعطيات بالعمومية والفضفاضة، الأمر الذي يكرس الضبابية والغموض في تحديد مضمون نطاقها وحدود متابعة مرتكبيها.

المطلب الثاني: تشريعات أخرى تناولت الجريمة الإلكترونية.

هناك مجموعة من المقتضيات الزجرية المتفرقة في تشريعات أخرى ذات علاقة بالمجال المعلوماتي، ونعرضها كالتالي:

- القانون رقم 53.05 المتعلق بالتبادل الإلكتروني للمعطيات القانونية (المصادقة الالكترونية)

يشير القانون رقم 53.05 إلى القانون المتعلق بالمصادقة الإلكترونية والتوقيع الرقمي. تم اعتماد هذا القانون لتنظيم وتشجيع استخدام التوقيع الإلكتروني والمصادقة الإلكترونية في المعاملات الرسمية والتجارية.

صدر هذا القانون في العام 2007 ويهدف إلى توفير إطار قانوني لضمان سلامة وثوقية المعاملات الإلكترونية والتبادل الإلكتروني للمعلومات في المغرب. ينص القانون على معايير استخدام التوقيع الإلكتروني ويحدد الإجراءات اللازمة للمصادقة الإلكترونية.

تم اعتماد القانون رقم 53.05 في المغرب لتعزيز وتنظيم استخدام التوقيع الإلكتروني والمصادقة الإلكترونية في المعاملات الرسمية والتجارية، وهو يشكل إطارًا

قانونيًا للتعامل مع المستجدات التكنولوجية في مجال الاتصالات والتبادل الإلكتروني للمعلومات.

من بين النقاط الرئيسية التي يتناولها القانون:

التوقيع الإلكتروني: يحدد القانون معايير وشروط استخدام التوقيع الإلكتروني ويعترف به كوسيلة قانونية معترف بها للتصديق على المعاملات.

المصادقة الإلكترونية: يتناول القانون كيفية تحقيق المصادقة الإلكترونية وضمان أمان المعلومات الرقمية.

المعاملات الرسمية: يوفر القانون إطارًا قانونيًا لاعتماد التوقيع الإلكتروني في المعاملات الرسمية والوثائق القانونية.

الجرائم الإلكترونية: يتعامل القانون مع قضايا الجرائم الإلكترونية ويحدد عقوبات للتلاعب غير القانوني بالمعلومات الرقمية.

يعتبر هذا القانون خطوة مهمة نحو تعزيز التبادل الإلكتروني للمعلومات وتطوير بيئة أعمال رقمية في المغرب.

- القانون رقم 43.20 المتعلق بخدمات الثقة بشأن المعاملات الإلكترونية.

يعاقب بالحبس من سنة إلى خمس سنوات وبغرامة من 10.000 إلى 100.000 درهم، كل من استعمل، بوجه غير قانوني، معطيات إنشاء التوقيع الإلكتروني أو إنشاء الخاتم الإلكتروني التي تخص الغير.

- القانون رقم 09.08 المتعلق بحماية الأشخاص الذاتيين

تثير المعاملات الإلكترونية مشكلات عديدة بشأن توفير الحماية القانونية للمستهلك عند قيامه بالتعاقد الإلكتروني، ولذلك كان المستهلك في حاجة لتوفير حماية قانونية لبياناته، فلقد أصبحت البيانات الشخصية المعالجة إلكترونيا ذات أهمية على المستوى الدولي، وقد سار المشرع المغربي مع التوجه التشريعي في العديد

من الدول التي تهدف تحقيق حماية فعالة للبيانات الشخصية، فأصدر القانون رقم 08-09 المتعلق بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي بتاريخ 18 فبراير 2009، ولقد جاء هذا القانون بمجموعة من النصوص التي تحمي عمليات المعالجة وتحمي المعطيات الشخصية المعالجة، ومن أهم المواد نجد المادة53 التي عاقبت بالغرامة من 20000درهم إلى 200000 درهم في حالة رفض المسؤول عن المعالجة حقوق الولوج أو التصريح أو التعرض المنصوص عليها في المواد7 و 8 و9 من القانون رقم 08 -09، كما جرمت المادة 63 عملية نقل معطيات ذات طابع شخصي نحو دولة أجنبية خرقا لأحكام المادتين 43و44 من هذا القانون.

- القانون 31.08 المتعلق بحماية المستهلك

لتحقيق حماية المستهلك المتعامل إلكترونيا، نص المشرع المغربي من خلال القانون رقم 31.08 [1] المتعلق بتحديد تدابير حماية المستهلكين. حيث نص هذا القانون في المادة 175 على عقوبة تتمثل في غرامة من 10.000 إلى 50.000 درهم بالنسبة للمورد الذي يرسل (خلافا لأحكام المادة 23 أعلاه) أي إشهار عن طريق البريد الإلكتروني دون الموافقة المسبقة والحرة والصريحة للمستهلك بعد إخباره كما يعاقب بنفس العقوبة كل من قام بإرسال إشهار عن طريق البريد الإلكتروني عندما يتم:

- استعمال البريد الإلكتروني أو هوية الغير.
- تزييف أو إخفاء أي معلومة تكمن من تحديد مصدر الرسالة الموجهة عبر البريد الإلكتروني أو مسارها إرسالها.[2]

[1] ظهير شريف رقم 1.11.03 صادر في 14 من ربيع الأول 1432 (18 فبراير 2011) بتنفيذ القانون رقم 31.08 القاضي بتحديد تدابير حماية المستهلك المنشور بالجريدة الرسمية عدد 5932، الصادرة بتاريخ 3 جمادى 1432 (17 أبريل 2011) ص 1072.

[2] عبد الرحيم بوعبيدة، ضياء أحمد علي نعمان، ص 177 – 178.

- القانون 24.96 المتعلق بالبريد والمواصلات

بالرجوع إلى القانون رقم 24.96 [1] لسنة 1996 المتعلق بالبريد والمواصلات، نلاحظ أنه خصص مجموعة من المقتضيات الزجرية في حق كل شخص استغل نظام المعلوميات للاعتداء على مجال البريد والمواصلات، كما هو الشأن في حالة إنجاز إرسال راديوي إذا استخدم فيه عمدا رمز نداء من السلسلة الدولية مخصصا لمحطة تابعة للدولة أو لمحطة تابعة للشبكة العامة للمواصلات أو لمحطة خصوصية مرخص لها من طرف الوكالة الوطنية لتقنين المواصلات، أو القيام ببعض الأفعال المنصوص عليها في المادة 83.[2]

- القانون 2.00 المتعلق بحقوق المؤلف والحقوق المجاورة

أقرت أغلب التشريعات حماية برامج الحاسب الآلي بقانون حق المؤلف، بحيث أدرجت برامج الحاسب الآلي ضمن المصنفات الفكرية الخاضعة لنصوص قانون حق المؤلف، ومنها القانون المغربي 00-2 المتعلق بحقوق المؤلف والحقوق المجاورة، حيث تم وضع مقتضيات جنائية خاصة في القانون المتعلق بحقوق المؤلف، ومن بينها ما جاءت به المادة 64 التي عاقبت بالحبس من شهرين إلى 6أشهر وغرامة من 10000 درهم إلى 100000 درهم أو بإحدى هاتين العقوبتين فقط لكل من قام بطريقة غير مشروعة بقصد الاستغلال التجاري بخرق متعمد، كما تطبق نفس

[1] الصادر الأمر بتنفيذه بموجب ظهير شريف رقم 1.97.162 بتاريخ 2 ربيع الآخر 1418 (7 أغسطس 1997)، والمنشور بالجريدة الرسمية عدد 4518، بتاريخ 18.09.1997، الصفحة 3721.

[2] تنص المادة 83 على ما يلي: "يعاقب بالحبس من شهر إلى سنتين وبغرامة من 10000 إلى 200000 درهم:

- كل من أحدث أو أمر بإحداث شبكة مواصلات دون الحصول على الترخيص المنصوص عليه في المادة الثانية أعلاه أو استمر في استغلال شبكته خرقا لمقرر التوقيف أو سحب الترخيص.
- كل من قدم أو أمر بتقديم خدمة مواصلات دون الحصول على الترخيص المنصوص عليه في المادة الثانية أعلاه أو استمر في تقديم الخدمة بعد صدور مقرر توقيف أو سحب الترخيص.
- كل من أحدث الشبكات أو التجهيزات الراديو كهربائية المشار إليها في المادة 19 أعلاه مخالفا بذلك..."

العقوبة على أفعال استيراد وتصدير نسخ منجزة خرقا للقانون وعدة أعمال ينص عليها القانون وبالأخص ما له علاقة بالتكنولوجيا الحديثة.

- القانون 02.99 المتعلق بمكافحة استغلال المعلوميات من أجل ارتكاب جريمة جمركية

ينص البند 7 من الفصل 281 [1] من مدونة الجمارك والضرائب غير المباشرة على أنه: "تشمل الجنح الجمركية من الطبقة الثانية...:

كل عمل أو مناورة تنجز بطرق معلوماتية أو الكترونية، ترمي إلى حذف معلومات أو برامج النظام المعلوماتي للإدارة، أو تغييرها أو إضافة معلومات أو برامج إلى هذا النظام، عندما بنجم عن هذه الأعمال أو المشاورات التملص من رسم أو مكس أو الحصول بصفة غير قانونية على امتياز معين".

إضافة إلى ذلك، نجد المشرع قد وسع تعريفه للوثيقة في مجال المعاملات الجمركية، وهو بمثابة مفهوم حديث للوثيقة أو المحرر ليتناسب مع المجتمع الرقمي[2]، ويبدو ذلك جليا من خلال الفصل الأول من مدونة الجمارك والضرائب غير المباشرة، حيث نص على ما يلي:" يقصد في هذه المدونة والنصوص المتخذة لتطبيقها... :

الوثيقة: كل حامل مجموعة من المعطيات أو المعلومات كيفما كانت نوعية الطريقة التقنية المستعملة مثل الورق والأشرطة الممغنطة والأسطوانات اللينة والأفلام الدقيقة"...

[1] مصادق عليها بمقتضى الظهير الشريف رقم 1.77.339 بتاريخ 25 شوال 1397 (9 أكتوبر 1977) كما وقع تغييرها وتتميمها على الخصوص بمقتضى القانون رقم 02.99 المصادق عليه بالظهير الشريف 1.00.222 المؤرخ في 2 ربيع الأول 1421 الموافق ل 5 يونيو 2000.

[2] أمين اعزان، الجريمة المعلوماتية. ص23، مقال منشور على الرابط التالي:

https:/iefpedia.com/arabwp-wp-content/uploads1

كما نجد الفصل 203 من الجزء الثامن المكرر قد نظم أحكام إيداع التصاريح المفصلة والموجزة وسندات الإعفاء مقابل كفالة، والتي تتم بطرقة الكترونية أو معلوماتية.

- القانون 03-03 المتعلق بمكافحة الإرهاب

فطن المشرع المغربي لخطورة انتشار الإجرام المعلوماتي وأثر ذلك على أمن واستقرار المجتمع المغربي، حيث يعد القانون المغربي رقم03-03 المتعلق بالإرهاب أول تشريع مغربي يشير بشكل صريح للإجرام المعلوماتي كوسيلة للقيام بأفعال إرهابية لها علاقة عمدية بمشروع فردي أو جماعي يهدف إلى المس الخطير بالنظام العام بواسطة التخويف أو الترهيب أو العنف.

فالفصل 1-218 حدد بعض الأفعال المجرمة على سبيل الحصر، من بينها الجرائم المتعلقة بنظم المعالجة الآلية للمعطيات (الفقرة7)، وذلك بعد محاولة تحديد مفهوم الإرهاب في مستهل هذا الفصل.

فلقد جرم المشرع المغربي الأعمال الإرهابية التي ترتكب بواسطة المعلوميات وهو ما نستشفه من خلال قراءة البند السابع من الفصل 218 -1 من القانون الجنائي المغربي [1]، الذي يتضح من خلاله أنه إذا كان ارتكاب جرائم المس بنظم المعالجة الآلية للمعطيات له علاقة عمدية بمشروع فردي أو جماعي يهدف إلى المس الخطير بالنظام العام بواسطة التخويف أو الترهيب أو العنف فإن ذلك يشكل جريمة إرهابية.

[1] أضيفت هذه المادة إلى مجموعة القانون الجنائي بموجب القانون رقم 03-03 المتعلق بمكافحة الإرهاب الصادر بتاريخ 28 ماي 2003 المنشور بالجريدة الرسمية عدد 5112 بتاريخ 29 ماي 2003.

- القانون 03-24 المتعلق بمكافحة الاعتداء على المرأة والطفل بواسطة وسائل التكنولوجيا الحديثة

لقد شكلت سنة 2003 مصادفة محطة زمنية للاهتمام بالإجرام المعلوماتي بالمغرب، بحيث تم تمت إضافة جديدة للترسانة التشريعية المغربية فيما يخص مكافحة هذا النمط الجديد من الجرائم، بحيث صدر في نفس السنة القانون رقم 03-24 المتعلق بتعزيز الحماية الجنائية للطفل والمرأة، وقد عمل هذا التشريع على تغيير وتتميم بعض نصوص مجموعة القانون الجنائي المغربي خصوصا فيما يخص الجرائم الماسة بنظام الأسرة والأخلاق العامة.[1]

وباستقراء مقتضيات هذا التشريع، نلاحظ ان هناك فصلين مرتبطين بموضوع هذه الدراسة، وهما الفصل1-503 والفصل2-503، فالفصل 1-503 من المجموعة الجنائية المغربية ملأ فراغا تشريعيا، بحيث عاقب على جريمة التحرش الجنسي. وفي رأينا قد جاء هذا النص بصيغة تسمح للقاضي بتطبيقه على كل صور التحرش الجنسي التي تقع عبر وسائل الاتصال الحديثة كالانترنت. وقد حدد هذا الفصل العقوبة من سنة الى سنتين حبسا والغرامة من خمسة ألاف إلى خمسين الف درهم.[2]

أما الفصل 2-503 من المجموعة الجنائية المغربية فقد جرم كل صور التحريض أو التشجيع أو تسهيل استغلال أطفال تقل سنهم عن ثمان عشرة سنة في مواد اباحية، وهو ما يصطلح عليه في مجال القانون المعلوماتي بالبورنوغرافية الطفولية التي تستخدم فيها الوسائل المعلوماتية بشكل مكثف، والحقيقة يحسب للمشرع المغربي انه استغل فرصة إصدار القانون رقم 03-24 بإضافة هذا الفصل

[1] والتي تتضمن مقتضيات ذات علاقة بموضوع الدراسة.

[2] ينص الفصل1-503(يعاقب بالحبس من سنة إلى سنتين وبالغرامة من خمسة آلاف إلى خمسين ألف درهم، من اجل جريمة التحرش الجنسي، كل من استعمل ضد الغير أوامر، أو تهديدات أو وسائل للإكراه أو أية وسيلة أخرى مستغلا السلطة التي تخولها له مهامه، لأغراض ذات طبيعة جنسية)

المهم بعقوبات مشددة، والذي يحقق بدون شك حماية فعالة للطفل المغربي من مخاطر المواد الإباحية الطفولية الموجودة في مواقع الانترنت على وجه الخصوص، وبالتالي يملأ فراغا تشريعيا في مجموعة القانون الجنائية المغربي.[1]

تعتبر الحماية الجنائية للمرأة والطفل من أهم المستجدات التشريعية التي أدخلت على مجموعة القانون الجنائي بمقتضى القانون رقم 03-24 [2]، وبالرجوع إلى مضامين هذا القانون، نجده ينص على مقتضيات جنائية تهم الجريمة المعلوماتية، ويتعلق الأمر بالفصلين 503- 1و 503- 2. [3]

فباستقراء مقتضيات الفصلين السابقين، نلاحظ أن الفصل الأول ملأ فراغا تشريعيا، بحيث عاقب على جريمة التحرش الجنسي، وقد جاء هذا النص بصيغة تسمح للقاضي بتطبيقه على كل صور التحرش الجنسي التي تقع عبر وسائل الاتصال الحديثة كالإنترنت، وإن كان هذا الفصل أغفل تحديد الوسائل التي يمكن أن يتم بها هذا التحرش (إشارات، أقوال كتابات، مراسلات،...)[4]، فباستعمال المشرع للعبارة

[1] ينص الفصل2-503 (يعاقب بالحبس من سنة إلى خمس سنوات وغرامة من عشرة آلاف إلى مليون درهم كل من حرض أو شجع أو سهل استغلال أطفال تقل سنهم عن ثمان عشرة سنة في مواد إباحية، وذلك بأطهار أنشطة جنسية بأية وسيلة كانت سواء أثناء الممارسة الفعلية أو بالمحاكاة أو المشاهدة أو أي تصوير للأعضاء الجنسية للأطفال يتم لأغراض ذات طبيعة جنسية)

[2] المتعلق بتغيير وتتميم مجموعة القانون الجنائي، الصادر بتنفيذه ظهير شريف رقم 1.03.207 بتاريخ 16 من رمضان 1424 (11 نونبر 2003) منشور بالجريدة الرسمية عدد 5175 بتاريخ 12 ذو القعدة 1424 الموافق ل 5 يناير 2004، الصفحة 121.

[3] حيث ورد فهما على التوالي ما يلي:

- " يعاقب بالحبس من سنة إلى سنتين وبالغرامة من خمسة آلاف إلى خمسين ألف درهم؛ من أجل جريمة التحرش الجنسي كل من استعمل ضد الغير أوامر أو تهديدات أو وسائل للإكراه أو أية وسيلة أخرى مستغلا السلطة التي تخولها له مهامه. لأغراض ذات طبيعة جنسية"
- "يعاقب بالحبس من سنة إلى خمس سنوات وغرامة من عشرة آلاف إلى مليون درهم كل من حرض أو شجع أو سهل استغلال أطفال تقل سنهم عن ثمان عشرة سنة في مواد إباحية؛ وذلك بإظهار أنشطة جنسية بأية وسيلة كانت سواء أثناء الممارسة الفعلية أو بالمحاكاة أو المشاهدة أو أي تصوير للأعضاء الجنسية للأطفال يتم لأغراض ذات طبيعة جنسية"

[4] خالد عثماني. مكافحة الجريمة الالكترونية في ضوء التشريع المغربي. مجلة العلوم الجنائية، ص 42.

الفضفاضة " أي وسيلة"، يسمح للقاضي –إعمالا لسلطته التقديرية الواسعة- بتطبيق مقتضيات هذا النص على كل صور التحرش الجنسي أيا كانت وسيلته، ومن ذلك التحرش الجنسي الذي يقع عبر وسائل الاتصال الحديثة.[31]

كما يمنح الفصل الثاني نفس السلطة فيما يخص تحريض واستغلال القاصرين جنسيا، فقراءة عبارة "أي وسيلة" تتضمن في طياتها تعبيرا عن جميع الوسائل التي ترتكب بها هذه الجرائم، وضمناه وسائل التكنولوجيا الحديثة مثل الانترنيت والحاسوب.[1]

ونرى أنه على المشرع المغربي أن يأخذ بالمقتضيات المنصوص عليها في المادة 9 من اتفاقية بودابست التي تجرم البيدوفيليا عبر الإنترنت، فبالرجوع إلى هذه المادة نجدها تجرم عددا من صور البيدوفيليا عبر الإنترنت، منها إنتاج صور الأطفال الفاضحة بغرض توزيعها عبر نظام معلوماتي.[2]

بيد أنه بالرجوع إلى الفقرة الثانية من الفصل 503-2 من القانون الجنائي، يتضح صعوبة إقحام وسائل التكنولوجيا الحديثة ضمن أحكام هذه الفقرة التي

---

[1] عبد السلام بنسليمان. الإجرام المعلوماتي في التشريع المغربي: دراسة نقدية في ضوء آراء الفقه وأحكام القضاء"، مرجع سابق، ص:41. 42.

[2] Article 19، infractions se rapportant à la pornographie enfantine :

- Chaque partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale، conformément à son droit interne، les comportements suivants lorsqu'ils sont commis intentionnellement et sans droit:
- La production de pornographie enfantine en vue de sa diffusion par le biais d'un système informatique ;
- L'offre ou la mise à disposition de pornographie enfantine par le biais d'un système informatique ;
- La diffusion ou la transmission de pornographie enfantine par le biais d'un système informatique ;
- Le fait de se procurer ou de procurer à autrui de la pornographie enfantine par le biais d'un système informatique ;

La possession de pornographie enfantine dans un système informatique ou un moyen de stockage de données informatiques. »

عددت مجموعة من الأفعال الجريمة البيدوفيلية، فقد ورد فيها ما يلي:" تطبق نفس العقوبة على كل من قام بإنتاج أو توزيع أو نشر أو استيراد أو تصدير أو عرض أو بيع أو حيازة مواد إباحية من هذا النوع."

- القانون رقم 13.108 المتعلق بالقضاء العسكري

بالرجوع إلى الظهير الجديد المتعلق بالعدل العسكري[38]، نلمس مواكبته للتطور التكنولوجي ومسايرة العصر، حيث أدخل المشرع ضمن مقتضيات هذا القانون تجريم استغلال المعلوميات بغرض ارتكاب جرائم عسكرية، ويستشف ذلك من خلال قراءة الباب الثاني عشر من نفس القانون، وذلك تحت عنوان:" في الجرائم الماسة بنظم المعالجة الآلية للمعطيات والجرائم الماسة بنظم ووسائل الاتصال التابعة للدفاع الوطني (المادتان 209 و210)، حيث عاقب المشرع في المادة 209 على الأفعال المنصوص عليها في الفصول من607-3 إلى607-10 من القانون الجنائي إذا مست بنظم المعالجة الآلية للمعطيات التابعة للدفاع الوطني أيا كانت الدعامة أو الوسيلة المستعملة لارتكاب هذه الجرائم وذلك بعقوبة السجن من خمس إلى عشر سنوات ، وبغرامة من 10000 إلى 2000000 درهم، وتضاعف هذه العقوبات إذا ارتكبت الأفعال أعلاه وقت الحرب أو أثناء العمليات العسكرية أو لفائدة عصابة ثائرة أو جماعة ثائرة أو جهة أجنبية

أما المادة 210، فقد عاقبت بنفس العقوبات المشار إليها أعلاه كل من عيب أو أتلف أو خرب نظم ووسائل الاتصال التابعة للدفاع الوطني أو اخترقها أو عرقلها أو قام بتسجيل مضمونها أو بأخذ نسخ منها أو حجزها أو قام بالتشويش عليها.

ومن خلال قراءة هذه النصوص، يمكننا أن نسجل ملاحظتين بارزتين، الأولى تتمثل في الفرق الشاسع بين الغرامة في حدها الأدنى المتمثل في 10000درهم وحدها الأقصى الذي يصل إلى 2000000درهم.

أما الملاحظة الثانية، فتهم هزالة الغرامة المالية، حيث إنها لا تتعدى 20000 درهم في حدها الأدنى عند مضاعفة هذه العقوبات، وخاصة إذا ارتكبت هذه الأفعال وقت الحرب، أو أثناء العمليات العسكرية، وبالتالي فهي غرامات ضعيفة جدا مقارنة مع حجم وجسامة الأفعال المرتكبة، والتي تمس الدفاع الوطني.

- القانون 103.13 المتعلق بالعنف ضد النساء

يندرج هذا القانون في إطار الجهود التي يقوم بها المغرب من أجل محاربة ظاهرة العنف ضد النساء، ولقد صادق عليه مجلس النواب في 20 يوليوز 2016، قبل أن يحيله على مجلس المستشارين، حيث تم تقديمه في 2 غشت 2016، وشرع بمناقشته مناقشة عامة في 31 أكتوبر2017، ثم صادق عليه في الأخير في مجلس النواب يوم الأربعاء 14 فبراير 2018 -168 – نائبا وعارضه -55- آخرون ، ومن بين مزايا هذا القانون أنه تطرق للعنف ضد المرأة بجميع أشكاله، بما فيها العنف الالكتروني الذي يعد عنفا مرتبطا بالمجال الرقمي، حيث يهدف الفصل 448.1 منه إلى حماية الحياة الخاصة الرقمية للنساء عبر تجريم أفعال التقاط أو تسجيل أو بث أو توزيع أقوال أو معلومات تخصهن بطريقة غير مشروعة، غير أنه من ضمن ما يؤاخذ على هذا النص أنه غير قادر على تجريم كل أنواع الجرائم ذات الطبيعة الجنسية المتعلقة بالفضاء الرقمي، مما يجعل العديد منها يبقى خارج دائرة التجريم والعقاب، ولذا من الضروري تعديله إسوة بالمشرع الفرنسي الذي تدارك الأمر.

الخاتمة

تتميز الجريمة الإلكترونية بنوع من الخصوصية، وذلك بالنظر إلى طابعها اللامادي، وصعوبة إثباتها، وهو ما يقتضي ضرورة سن تشريع خاص بها، لعدم كفاية النصوص الجنائية التقليدية، كالنصب وخيانة الأمانة والتزوير للإحاطة بها، مع وجوب ملائمة الجهاز القضائي بكل مكوناته، مع هذا النوع من الجرائم، وذلك من خلال إحداث شرطة قضائية متخصصة في هذا المجال، تجمع بين التكوين القانوني

والتكوين التقني، وانفتاحها على باقي الأجهزة الأمنية، للدول الرائدة في مكافحة هذه الجرائم، في إطار التعاون الأمني والدولي، كما يجب فتح أفاق التكوين والتدريب لمختلف المتدخلين في الميدان، من قضاة ومحامين وخبراء....بما يدعم خبراتهم، في اتجاه فهم طبيعة هذه الجرائم وإشكالاتها، ويجب العمل، أيضا على تحديث وسائل الإثبات، بحيث تساعد القاضي في حل النزاعات المتعلقة بالجرائم الإلكترونية، ومسايرة الاجتهاد القضائي لثورة المعلومات، من خلال قبول الأدلة المستمدة من أجهزة الحاسوب، كلما كانت مقنعة له.

لائحة المصادر والمراجع

المراجع العربية:

- عبيد صالح حسن، سياسة المشرع الإماراتي لمواجهة الجرائم الإلكترونية، دورية الفكر الشرطي، المجلد الرابع والعشرون، 2015، الإمارات
- علال فالي، خصوصية الجريمة المعلوماتية، مقال بمجلة القضاء التجاري الثاني، الرباط، 2013
- خالد ممدوح إبراهيم، الجرائم المعلوماتية، مطبعة دار الفكر الجامعي، الإسكندرية، الطبعة الأولى، 2009
- عبد العالي الدريبي ومحمد صادق إسماعيل، "الجرائم الإلكترونية" دراسة قانونية قضائية مقارنة، الطبعة الأولى، القاهرة
- ذياب موسي البداينة، ورقة عمل بعنوان الجرائم الالكترونية المفهوم والاسباب، عمان المملكة الاردنية الهاشمية، 2014، الملتقي العلمي الجرائم المستحدثة في ظل المتغيرات والتحولات الاقليمية والدولية خلال الفترة 2-9/4 لعام 2014.
- ورقة عمل، الجرائم الالكترونية، مديرية تكنولوجيا المعلومات، قسم نظم المعلومات شعبة امنية المعلومات، دولة العراق
- رؤى احمد جرادات وماسة سامر شيب، موسوعة ودق القانونية، رابط الموقع: https://wadaq.info
- خالد ممدوح إبراهيم، أمن الجريمة الإلكترونية، الدار الجامعية – الإسكندرية، 2008
- عبد الصبور عبد القوي على مصري، المحكمة الرقمية والجريمة المعلوماتية، مكتبة القانون والاقتصاد، الرياض، طبعة الأولى، 2012
- ممدوح رشيد مشرف الرشيد، الحماية الجنائية للمجني عليه من الابتزاز، المجلة العربية للدراسات الأنية، المجلد: 33، العدد: 70،

- كامل مطر، الجريمة الالكترونية، ورقة بحثية
- حنان ريحان مبارك، الجرائم المعلوماتية، دراسة مقارنة، منشورات الحلبي الحقوقية، ط1، 2014
- عبد السلام بنسليمان، الاجرام المعلوماتي في التشريع المغربي: دراسة نقدية مقارنة في ضوء آراء الفقه وأحكام القضاء
- خالد عثماني، مكافحة الجريمة الالكترونية في ضوء التشريع المغربي، مجلة العلوم الجنائية
- محمد جوهر: خصوصيات زجر الإجرام المعلوماتي، المجلة المغربية للقانون والاقتصاد والتدبير، العدد52، 2006
- محمد علمي مشيشي الإدريسي، دراسة مقارنة حول ملاءمة مشروع القانون الجنائي مع المبادئ والقواعد المعتمدة في منظومة حقوق الإنسان،
- عبد الجبار الحنيص، الحماية الجزائية لبطاقة الائتمان الممغنطة من التزوير، مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، المجلد 24، العدد الثاني، 2008
- عبد السلام بنسليمان، الإجرام المعلوماتي في التشريع المغربي: دراسة نقدية مقارنة في ضوء آراء الفقه وأحكام القضاء44 مرجع سابق،
- ظهير شريف رقم 1.11.03 صادر في 14 من ربيع الأول 1432 (18 فبراير 2011) بتنفيذ القانون رقم 31.08 القاضي بتحديد تدابير حماية المستهلك المنشور بالجريدة الرسمية عدد 5932، الصادرة بتاريخ 3 جمادى 1432 (17 أبريل 2011)
- عبد الرحيم بوعبيدة، ضياء أحمد علي نعمان،
- أمين اعزان، الجريمة المعلوماتية.
- خالد عثماني. مكافحة الجريمة الالكترونية في ضوء التشريع المغربي. مجلة العلوم الجنائية.

- عبد الحميد المليجي، الجريمة الإلكترونية: مدخل إلى الإطار المفاهيمي، مجلة المنارة للدراسات القانونية والإدارية، https://revuealmanara.com، اطلع عليه بتاريخ: 24 نونبر 2023.

المراجع الأجنبية:

- Mohamed ouzgane la criminalité informatique au regard du droit pénal marocain، centre marocain des études juridiques، Hommage au professeur Jallal Essaid، Tome I، 2005،