137 **Original Article** Arab Journal for Security Studies 2022; Volume 38 Issue (2), 137-145

Naif Arab University for Security Sciences
Arab Journal for Security Studies
المجلة العربية للدراسات الأمنية
https://journals.nauss.edu.sa/index.php/ajss

AJSS

Legislative Control of Certain Forms of CyberCrimes & Cybercriminals

المكافحة التشريعية لبعض صور الجرائم المعلوماتية وأصناف المجرم المعلوماتي

يونس نفيد
كلية العدالة الجنائية، جامعة نايف العربية للعلوم الأمنية، المملكة العربية السعودية

Youness Nafid
College of Criminal Justice, Naif Arab University for Security Sciences, Saudi Arabia

Received on 09 Oct. 2022, Accepted on 21 Nov. 2022, Available online on 12 Dec. 2022

Abstract

Recently, world states have witnessed the spread of a special type of crime, namely cybercrime, therefore it has become imperative to develop legislation to combat it.

Nevertheless, in view of the peculiarity of cybercrime, world states sought to adopt the latest cybercrime tracking technologies, as well as to allocate special criminal investigation teams for such crimes.

This study is conducted with the aim to explore the latest Moroccan legislation to combat certain types of cybercrime and to compare them with legislation adopted in other countries, as well as to identify the types of cybercriminals.

The study concluded several findings and recommendations, the most salient of which are:

- Moroccan legislation has identified the most important characteristics and types of cybercrime and developed laws governing it.
- Emphasis should be placed on speedy intervention. This can be achieved by establishing security team specialized in speedy intervention and seizure of suspects. In addition, it is of paramount importance to accelerate mechanisms to enact and amend cybercrime prevention laws, such as to create a legislative committee for this type of crime.
- International conventions should be ratified by other states, especially those related to international judicial cooperation in this field.

Keywords: *Security Studies, Cybercrime, Information Systems, Automated Data.*

المستخلص

عرفت دول العالم في الآونة الأخيرة، انتشار نوع خاص من الجرائم، وهي الجرائم المعلوماتية، فكان لازمًا عليها أن تسارع إلى الاهتمام بإخراج نصوص تشريعية لمكافحة هذا الصنف من الجرائم.

وهو ما حدث، وكان عليها أيضًا تطوير وسائل تتبع هذه الجرائم من خلال اعتماد أحدث التكنولوجيات، وتخصيص فرق جنائية خاصة بالتحقيق في مثل هذه الجرائم؛ لما لها من خصوصية.

ولأجل ذلك فقد قررنا القيام بهذه الدراسة، من أجل الوقوف على أحدث التشريعات المغربية في مجال مكافحة بعض صور الجريمة المعلوماتية ومقارنتها ببعض التشريعات الأخرى، وكذلك من أجل تحديد أصناف المجرم المعلوماتي.

وتوصلنا بنهاية هذه الدراسة إلى عدة نتائج وتوصيات نذكر من بينها:

- التوصل إلى أهم خصائص هذا النوع من الجرائم، وكذا أهم صورها والأحكام المنظمة لها بالتشريع المغربي.
- التوصية بضرورة سرعة التدخل وذلك برصد فرق أمنية خاصة للتدخل السريع وضبط المشتبه فيهم بأسرع وقت، وكذا تسريع آليات إصدار وتعديل قوانين الحماية من مثل هذه الجرائم، كإحداث لجنة تشريعية خاصة بهذا النوع من الجرائم.
- التوصية بالمصادقة على الاتفاقيات الدولية من طرف باقي الدول، وخصوصًا المتعلقة منها بالتعاون القضائي الدولي في هذا المجال.

الكلمات المفتاحية: الدراسات الأمنية، الجرائم المعلوماتية، النظم المعلوماتية، المعالجة الآلية للبيانات.

* Corresponding Author: *Youness Nafid*
Email: ynafid@nauss.edu.sa
doi: 10.26735/BSUF7582

Production and hosting by NAUSS

1319-1241© 2022. AJSS. This is an open access article, distributed under the terms of the Creative Commons, Attribution-NonCommercial License.

1. المقدمة

عرفت جل التشريعات الدولية والوطنية طفرة نوعية في مجال تجريم الجريمة المعلوماتية ورصد عدة وسائل وسياسات وقائية للحد منها.

وهو الأمر الذي ألزم الدول بتطوير تقنيات التحقيق الجنائي واستعمال أحدثها لرفع كفاءة وقدرة المحققين من أجل مكافحة الجريمة المعلوماتية.

وتعرف الجريمة المعلوماتية بأنها عمل أو امتناع يأتيه الإنسان إضرارًا بمكونات الحاسب وشبكات الاتصال الخاصة به التي يحميها قانون العقوبات ويفرض لها عقابًا (الديربي، 2012 ، ص. 41).

كما عرفها البعض الآخر بأنها كل أشكال السلوك غير المشروع أو الضار بالمجتمع الذي يرتكب باستخدام الحاسب (الملط، 2006، ص. 84).

ولم يعرف المشرع المغربي الجريمة المعلوماتية في القانون رقم 07.03 كما فعلت باقي التشريعات، بل نص فقط على الأفعال التي تعد جرائم معلوماتية، ومن بين هذه الأفعال الدخول إلى مجموعة أو بعض أنظمة المعالجة الآلية للمعطيات عن طريق الاحتيال والبقاء فيها، إلى غير ذلك كما سنفصل فيما بعد.

حيث بادر المشرع المغربي كغيره من التشريعات الإقليمية والدولية إلى سن القانون رقم 07.03 المتعلق بالمساس بنظم المعالجة الآلية للمعطيات الذي يحتوي على تسعة فصول، تبدأ من الفصل 3.607 إلى 11.607 (القانون رقم 07.03 المتعلق بنظم المعالجة الآلية للمعطيات الصادر بتاريخ 22 ديسمبر 2003).

أهمية الدراسة

تكمن أهمية هذه الدراسة في خطورة هذه الجريمة على مصالح الأفراد، ومن ذلك تهديد حياتهم الشخصية، وكذلك تهديد ممتلكاتهم بالبنوك، وكذا من خلال انتهاك خصوصيتهم الشخصية وابتزازهم، ونشر الرذيلة والتحريض على الدعارة.

فقد أصبحت الجريمة تهدد أمن الدول واستقرارها، عبر اختراق أنظمة مؤسساتها المعلوماتية، وعبر انتهاك سيادة الدولة وتجاوز حدودها الإقليمية، وعبر تهديد البنية الإلكترونية للدول والمؤسسات.

فهذه الجرائم تعتدي حتى على الأنظمة العسكرية والأمنية لمختلف دول العالم، كما أن الاعتداءات المعلوماتية أصبحت تقلل من إيجابيات الأدوات والنظم الإلكترونية.

وبناءً عليه، قررنا أن نبحث وندرس هذا الموضوع الموسوم بـ «سبل مكافحة الجريمة المعلوماتية في التشريع المغربي» بشكل مختلف عن الدراسات السابقة، كما سنبرهن على ذلك لاحقًا وفق خطة البحث.

إشكالية الدراسة

تتمثل إشكالية الدراسة في مدى نطاق الحماية الجنائية التي أقرها المشرع المغربي لحماية الأفراد والمؤسسات من بعض صور الجريمة المعلوماتية وطنيًّا؟ وذلك بالمقارنة مع مجموعة من الدول الأخرى؟ وسندرس كل ذلك بعدما نجيب عن التساؤل المطروح حول ماهية صور هذه الجريمة وكذا صفات المجرم المعلوماتي؟

منهج البحث

سوف نوظف لدراسة هذا الموضوع مجموعة من المناهج العلمية، أهمها المنهج الوصفي، والمنهج المقارن، وكذلك المنهج التحليلي الاستنباطي في بعض الفقرات.

2. المطلب الأول: بعض صور الجريمة المعلوماتية وخصائص المجرم المعلوماتي

تتعدد صور الجريمة المعلوماتية بتعدد الأفعال المكونة لها، لذلك سوف نقتصر على ضرب بعض الأمثلة لها فقط (الفقرة الأولى).

كما تتعدد صفات المجرم المعلوماتي بصفات منفردة عن باقي أصناف المجرمين، وخصوصًا من حيث المؤهل العلمي، ومن حيث الذكاء، ومن حيث الكفاءة في المجال المعلوماتي (الفقرة الثانية).

2. 1 الفقرة الأولى: بعض صور الجريمة المعلوماتية

إذا كانت الجريمة المعلوماتية تتميز بالخصائص التالية: أنها جريمة مستحدثة، وتنفذ عن بعد، وعابرة للحدود (ممدوح، 2009، ص.77)، ومن الجرائم الناعمة (الديربي،2012، ص.56)، ويصعب إثباتها (حميشي، 2016، ص. 28)، فإن الجرائم الواقعة على النظام البرمجي أي النظام المعلوماتي المكون من البرامج الحاسوبية التشغيلية والتطبيقية تعتبر من بين صور الجريمة المعلوماتية، بالإضافة إلى الصورة المتمثلة في الاعتداء على المعلومات التي يحتويها النظام المعلوماتي.

يقصد بالبرامج كل ما تم إعداده بواسطة مبرمجين وخبراء متخصصين في التخطيط والبرامج لخدمة أهداف معينة (الملط، 2006، ص. 172).

حيث تتحقق هذه الصورة عندما يقوم المجرم المعلوماتي بتعديل البرنامج أو التلاعب فيه، أو بزرع برنامج فرعي غير مسموح به في البرنامج الأصلي؛ مما يسمح له بالدخول غير المشروع في العناصر الضرورية لأي نظام حاسوبي؛ وذلك بغية تحقيق ربح مادي (الملط، 2006، ص. 172).

كما تتحقق هذه الصورة كذلك عندما يتم تزويد البرنامج الأصلي بمجموعة تعليمات إضافية يسهل الوصول إليها بواسطة شفرة تسمح بالحصول على جميع المعطيات التي يتضمنها النظام الحاسوبي (جواحي، 2015-2014، ص. 24).

ومثال ذلك استعمال أسلوب المصيدة، الذي يتمثل في إعداد المبرمج برنامجًا به أخطاء وعيوب عمدًا لا يكتشف بعضها عند استخدام البرنامج؛ إذ يترك المبرمج ممرات خالية وفواصل وتفرعات في البرنامج حتى يستطيع فيما بعد تنفيذ التعديلات الضرورية بإدخال تفرعات إضافية يستطيع من خلالها الولوج داخل النظام المعلوماتي والوصول إلى كل المعلومات التي تحتويها الذاكرة (الملط، 2006، ص. 176).

ومثال ذلك توظيف وتصميم برنامج وهمي، من خلال قيام المبرمج بوضع برنامج وهمي يصعب اكتشافه يخصص لارتكاب الجريمة ومراقبة تنفيذها (جواحي، 2015-2014، ص. 25).

ونستنتج أن مثل هذه الجرائم هي دائمًا وغالبًا ما ترتكب من طرف فئة متمكنة من تقنيات المعالجة الآلية للمعلومات، بل ولها تكوين محترف في هذا المجال، وربما ذكاء خارق؛ مما يصعب مهمة المحققين في الوصول إلى الحقيقة.

فأما صورة استبدال المعلومات فتسمى بجرائم الغش أو التزوير المعلوماتي، كاستبدال رقم بآخر، وهو يشكل خطورة كبيرة؛ لأنه في حالة نجاحه يستمر فترة طويلة من الزمن (الملط، 2006، ص. 181).

أما مسح وحذف المعلومات، فيعد من أسهل طرق الإتلاف، وذلك كإزالة جزء من المعطيات المسجلة على دعامة الحاسوب والموجودة داخل النظام أو تحطيم تلك الدعامة أو نقل وتخزين جزء من المعطيات إلى المنطقة الخاصة بالذاكرة (الشوا، 1994، ص. 75).

2. 2 الفقرة الثانية: صفات المجرم المعلوماتي وأصنافه

يتصف المجرم المعلوماتي بمجموعة من الصفات، التي تجعله متميزًا عن باقي أصناف المجرمين، وسوف نلخص هذه الصفات فيما يلي:

- **التخصص:** المجرم المعلوماتي، مجرم متمكن من تقنيات المعلومات، حيث غالبًا ما يبحث هذا الصنف من المجرمين عن تكوين أنفسهم في مجال المعلومات بشكل ماهر، وخصوصًا تكوين أنفسهم في مجال تقنيات إنشاء التطبيقات الإلكترونية وكذا كيفية استعمالها.
- **الاعتياد:** المجرم المعلوماتي، من المجرمين الذين يعتادون الإجرام بصفة مستمرة، ولذلك نجد في معظم القضايا الجنائية أن هذا الصنف من المجرمين يكون قد اعتاد ارتكاب الجرائم المعلوماتية؛ مما يخلق له نوعًا من الثقة بالنفس في الاستمرار بتلك الخروقات.
- **الاحتراف:** المجرم المعلوماتي، مجرم محترف؛ لأنه يحترف هذا النوع من الإجرام لأغراض شخصية أو لتحقيق أرباح مادية أو غيرها من المصالح.
- **عدم اتصافه بالعنف:** المجرم المعلوماتي لا يتميز بالعنف، وذلك لطبيعة هذا النوع من الجرائم التي ترتكب جلها عن بعد وبشكل يعتمد على الحاسب الآلي وكذا شبكة الإنترنت.
- **المهارة:** المجرم المعلوماتي ذو مهارات عالية في مجال الاتصالات؛ حيث قد تكون هذه الخبرة مكتسبة عن طريق الممارسة المتكررة للأجهزة الإلكترونية (نعمان،2011، ص. 13)، حيث غالبًا ما تكتسب هذه المهارات عن طريق التجربة والهواية، ومن ثم الانتقال إلى توظيفها في مجال الإجرام.
- **الخبرة:** يتميز المجرم المعلوماتي برصيد معرفي عن طريق الخبرة والاحتكاك بالآخرين (كوبان، 2016، ص. 165)، وهذا الأمر هو ما يقوم به ويستعد له المجرم المعلوماتي بغية اكتساب المهارات والتقنيات اللازمة لتنفيذ مخططاته.
- **يمتلك أنظمة المعلومات:** يتميز كذلك المجرم المعلوماتي بتوافره على الإمكانات المعلوماتية التي سوف تمكنه من ارتكاب جريمته (الديربي، 2012، ص. 60)، ولذلك فالمجرم المعلوماتي دائم السعي لاقتناء أحدث ما عرفته التكنولوجيا في مجال نظم المعالجة الآلية للمعطيات.
- **الذكاء:** كما يكون المجرم المعلوماتي ذكيًا في مجال المعلومات (خليفة، 2007، ص. 36)، لأن طبيعة هذا النوع من الجرائم تحتاج إلى ذكاء في بعض الأحيان للقيام ولاحتراف تقنيات نظم المعالجة الآلية للمعطيات.

وقد يصنف المجرم المعلوماتي إلى عدة أصناف وفئات حسب الآتي:

- فئة المتسلين Prankesters: وهم الذين يرتكبون الجريمة رغبةً في التسلي والمزح، لكن بطريقة تؤذي الآخرين (الديربي، 2012، ص. 61).
- فئة الهاكرز (hackers): وهم الذين يقومون باختراق الحواجز الأمنية الخاصة بأنظمة الحواسيب الآلية غير المصرح لهم بالدخول إليها، بغية إثبات احترافيتهم في الاختراق، وقد تكون أهدافهم متعددة، وهذه الفئة تعد من أخطر المجرمين المعلوماتيين (الديربي، 2012، ص. 62).

ومثل ذلك قضية الجحيم العالمي التي تمكنت خلالها مجموعة أشخاص من اختراق مواقع البيت الأبيض، والجيش، ووزارة الداخلية الأمريكية، وقد أدين اثنان من هذه المجموعة، وقد

بينت التحقيقات أن هدفهم كان هو الاختراق وليس تدميريًا أو قرصنة المعلومات، وقد كلف التحقيق مبالغ مالية طائلة (فتح الله،2021، ص. 463).

- فئة الكراكرز (Crakers): وهم من أخطر الفئات المحترفة كذلك، حيث يقومون باختراق أنظمة آلات الحاسوب بغية الاطلاع على البيانات المخزنة به، بغية التلاعب بها أو اختلاسها (صغير، 2013، ص. 27).

ومن قضايا الاعتداء التي خلفتها الجرائم المعلوماتية في سبتمبر 2016، ما كشفت عنه شركة ياهوو -Yahoo- بشأن أكبر عمليات قرصنة وابتزاز لقاعدة بيانات مستخدميها التي اعتبرت من أكبر عمليات القرصنة في التاريخ لشركة تقنية، حيث حصل المجرمون المعلوماتيون على بيانات أكثر من 500 مليون مستخدم، وفي ديسمبر من نفس السنة تعرضت الشركة نفسها، لعملية قرصنة معلوماتية أخرى تتعلق بالاستيلاء على بيانات أكثر من مليار مستخدم أصبحت معروضة للبيع، منها كلمات السر وأسئلة الأمان وأرقام هواتف وتواريخ ميلاد، وقد أدت هذه العمليات إلى تخفيض أسهم الشركة الأمريكية اقتصاديًا وإعلاميًا بشكل كبير (فتح الله،2021، ص. 462).

ومثلهم كمثل المحاسب الذي يقوم بتخريب البرامج المعلوماتية، بعد فصله من العمل قصد تدمير البيانات الخاصة بحسابات وديون المؤسسة التي كان يعمل بها (فتح الله،2021، ص. 42).

فئة (Career Criminals): وتهدف هذه الفئة من خلال اختراقها للأنظمة الآلية بوسائل غير مشروعة إلى الحصول على منافع وأرباح مالية ومادية (الديربي، 2012، ص. 62).

ومثلهم كمثل المجرم الذي يسرق الأموال أو يقوم بتحويلها إلى حسابه الشخصي بمؤسسة بنكية معينة (صغير، 2013، ص. 38).

3. المطلب الثاني: مكافحة الجريمة المعلوماتية تشريعيًّا

يعتبر القانون رقم 07.03 المتعلق بالمساس بنظم المعالجة الآلية، كما أشرنا إليه سابقًا من القوانين الرادعة لمثل هذا النوع من الإجرام المعلوماتي؛ حيث تضمن هذا القانون عدة جرائم وعقوبات صارمة لمن يخالفه.

وذلك تكريسًا لمبدأ شرعية الجرائم والعقوبات، الذي مفاده لا جريمة ولا عقوبة ولا تدبير وقائيًا إلا بنص القانون.

فما بعض الجرائم المعلوماتية التي نص عليها هذا القانون المغربي؟ (الفقرة الأولى).

وما المعاهدات التي صادق عليها المغرب لمكافحة هذا النوع من الجرائم؟ (الفقرة الثانية).

3. 1 صور الجرائم المعلوماتية في التشريع المغربي

لا تسعنا هذه الدراسة لتحليل كل صور الجرائم المعلوماتية في التشريع المغربي، ولكن سنتطرق فقط للقوانين الزجرية التي أفردها المشرع المغربي من أجل تحقيق الأمن المعلوماتي؛ بغية حماية الأفراد والمجتمع من الجرائم المعلوماتية، ونذكر من بين هذه القوانين:

- القانون المتعلق بالأمن السيبراني، رقم 20.05 (القانون رقم 20.05 المتعلق بالأمن السيبراني).
- القانون المتعلق بجرائم نظم المعالجة الآلية للمعطيات، رقم 07.03 (القانون رقم 07.03 المتعلق بنظم المعالجة الآلية للمعطيات الصادر بتاريخ 22 ديسمبر 2003م).
- القانون المتعلق بالتبادل الإلكتروني للمعطيات القانونية، رقم 53.05 (القانون رقم 53.05 المتعلق بالتبادل الإلكتروني للمعطيات القانونية الصادر بتاريخ 30 نوفمبر 2007).
- القانون المتعلق بحماية المستهلك، رقم 31.08 (القانون رقم 31.08 القاضي بتحديد تدابير لحماية المستهلك، 2011 الصادر بتاريخ 18 فبراير 2011).
- القانون المتعلق بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي، رقم 08.09 (القانون رقم 08.09 المتعلق بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي الصادر بتاريخ فبراير 2009).

ولذلك سنشير بالدراسة فقط إلى صورتين من صور الجريمة المعلوماتية، كما تم النص عليهما وعلى عقوباتهما في القانون 07.03 المتعلق بجرائم نظم المعالجة الآلية للمعطيات، وهاتان الصورتان هما:

أولًا: جريمة الدخول الاحتيالي إلى نظام المعالجة الآلية للمعطيات.

ثانيًا: جريمة الاعتداء على منتجات النظام الآلي.

3. 1. 1 جريمة الدخول الاحتيالي إلى نظام المعالجة الآلية للمعطيات

نظم المشرع المغربي هذه الجريمة ضمن مقتضيات الفصل 3-607 من القانون رقم 07.03 المتعلق بالمساس بنظم المعالجة الآلية للمعطيات الذي ينص على ما يلي:

«يعاقب بالحبس من شهر إلى ثلاثة أشهر وبالغرامة من 2000 إلى 10000 درهم أو بإحدى هاتين العقوبتين فقط كل من دخل إلى مجموع أو بعض نظام المعالجة الآلية للمعطيات عن طريق الاحتيال.

ويعاقب بنفس العقوبة من بقي في نظام المعالجة الآلية للمعطيات، أو في جزء منه كان قد دخله عن طريق الخطأ وهو غير مخول له حق دخوله.

وتضاعف العقوبة إذا نتج عن ذلك حذف أو تغيير المعطيات المدرجة في نظام المعالجة الآلية للمعطيات، أو اضطراب في سيره».

حيث يتمثل الركن المادي لهذه الجريمة وفقًا لمقتضيات الفصل 3-607 من القانون رقم 07.03 المتعلق بالمساس بنظم المعالجة الآلية للمعطيات، في كل من أفعال الدخول إلى مجموع أو بعض نظام المعالجة الآلية للمعطيات عن طريق الاحتيال؛ حيث تعتبر هذه الجريمة من الجرائم الشكلية التي لا يستلزم فيها المشرع من القاضي الجنائي إثبات النتيجة، وكذا العلاقة السببية لتحققها.

وبناءً عليه فكل فعل من أفعال الدخول إلى نظم المعالجة الآلية للمعطيات، سواء بكلمة سر أو دون ذلك، تتحقق به جريمة الدخول الاحتيالي إلى نظام المعالجة الآلية للمعطيات.

ولذلك يدخل ضمن هذه الأفعال الاحتيالية التي يتحقق بها الركن المادي لهذه الجريمة على سبيل المثال ما يلي:

- الدخول لبريد إلكتروني خاص بالغير.
- وكذلك الدخول لتطبيق بنكي خاص بالغير.
- وكذلك الدخول إلى موقع محصن.

كما يشترط المشرع لتحقق هذه الجريمة توافر الركن المعنوي، الذي يتحقق بتوافر القصد الجنائي العام والقصد الجنائي الخاص، ويستنتج ذلك من خلال عبارة «... كل من دخل... عن طريق الاحتيال...، فلا بد وأن يكون الفاعل قد دخل عن طريق وسائل احتيالية لنظام المعالجة الآلية للمعطيات، وذلك سواء بإرسال رسالة للضحية بغرض نسخ كلمة السر أو بغيرها من الطرق».

ويعاقب على هذه الجريمة بالحبس من شهر إلى ثلاثة أشهر، وبالغرامة من 2000 درهم إلى 10000 درهم، أو بإحدى هاتين العقوبتين.

وهو نفس توجه المشرع الفرنسي، الذي يجرم كذلك الدخول غير المصرح به للنظام المعلوماتي كحماية غير مباشرة له، وذلك من خلال الفصل 1-323 من القانون الجنائي الفرنسي بالقسم الخاص بجرائم نظم المعالجة الآلية للمعطيات (www.legifrance.gouv.fr). ولقد عاقب المشرع الفرنسي على هذه الجريمة بعقوبة حبسية تقدر بسنتين حبسًا وبغرامة مالية تقدر بحوالي 60000 أورو.

وينهج المشرع البلجيكي نفس النهج في المادة 550 مكرر من قانون الإجرام المعلوماتي؛ حيث يعاقب بالحبس من ثلاثة أشهر إلى سنة وبالغرامة، أو بإحدى هاتين العقوبتين فقط، كل من دخل نظامًا معلوماتيًا، مع العلم أنه غير مرخص له بذلك. وإذا ارتكبت الجريمة عن طريق الاحتيال تشدد العقوبة وتصبح من ستة أشهر إلى سنتين (https://ticsipd.ch/protection-des-donnees/protection-des-donnees-en-belgique/).

ولا يقصد من مفهوم الدخول غير المصرح به الدخول المادي، بل الدخول المعنوي أي الاتصال بالنظام محل الحماية بالطرق الفنية المعلومة.

ومثل ذلك كمن يقوم بإقامة وصلة لربط خط الهاتف مع خط آخر للاتصالات عن بعد لإرسال واستقبال المعلومات أو كمن يقوم بإنشاء تحويلة أو من يلتقط من مسافة الإشعاعات التي تصدر عن النظم المعلوماتية (Tappolet , p351. 1988)، وتعرف هذه العملية باسم التداخل أو الالتقاط المعلوماتي (رستم، 1994، ص. 250).

كما عاقب المشرع المغربي بالعقوبة نفسها كل من دخل عن طريق الخطأ وبقي في النظام المعلوماتي أو في جزء منه وهو غير مسموح له بالدخول إليه.

وضاعف المشرع المغربي هذه العقوبة في الأحوال التي تتسبب فيها أفعال الدخول أو البقاء، في حذف أو تغيير أو تعديل للمعطيات المضمنة بنظام المعالجة الآلية للمعطيات أو أحدثت اضطرابًا في سيره واشتغاله.

والصيغة التي ذكر بها المشرع المغربي الدخول غير المشروع إلى نظام المعالجة الآلية للمعطيات تتحقق سواء أكان هذا الدخول مباشرًا أم غير مباشر، وسواء أكان هذا النظام محميًا أم لا، وسواء تم استعمال كلمة السر، أو تم ذلك عن طريق استخدام برنامج معين.

وتعتبر هذه الجريمة من الجرائم الشكلية التي لا تستلزم تحقق نتيجة مادية محددة، بل بمجرد إتيان الفعل الإجرامي المكون لها تتحقق الجريمة، ولو لم ينتج عنها أية خسائر أو أية أضرار.

كما شدد المشرع المغربي العقوبة في حالة إذا ما كانت تمس بالأمن الداخلي أو الخارجي للدولة أو أسرار الاقتصاد الوطني (الفصل 4-607 من القانون رقم 07.03 المتعلق بنظم المعالجة الآلية للمعطيات، 2003).

كما شدد المشرع العقوبة في حالة ترتبت نتيجة معينة عن ارتكاب هذه الجريمة المعلوماتية من طرف موظف أو مستخدم في أثناء مزاولة مهامه أو بسببها، أو إذا سهَّل للغير القيام بها، سواء أكانت النتيجة هي تغيير المعطيات والبيانات المضمنة بنظم المعالجة الآلية للمعطيات أو القيام بحذفها، أو كانت هي إحداث اضطراب في سير واشتغال النظام (الفصل 4-607 من القانون رقم 07.03 المتعلق بنظم المعالجة الآلية للمعطيات، 2003).

ومن التشريعات العربية التي تجرم مثل هذه الجريمة التشريع السعودي؛ حيث يعاقب في المادة الخامسة من نظام مكافحة جرائم المعلوماتية، كل شخص يقوم بالدخول غير المشروع لإلغاء بيانات خاصة، أو حذفها، أو تدميرها، أو تسريبها، أو إتلافها، أو تغييرها، أو إعادة نشرها.

ويقصد بالدخول غير المشروع وفق نظام مكافحة جرائم المعلوماتية السعودي: دخول الشخص بطريقة متعمدة إلى حاسب آلي ، أو موقع إلكتروني أو نظام معلوماتي ، أو شبكة حاسبات آلية غير مصرح لذلك الشخص بالدخول إليها (نظام مكافحة الجرائم المعلوماتية السعودي الصادر بتاريخ 1428/3/8هـ).

ويلاحظ أن المشرع السعودي قد قيد تجريم الدخول غير المصرح به لنظام الكمبيوتر (نظام مكافحة جرائم المعلوماتية السعودي الصادر بتاريخ 1428/3/8هـ)، فاشترط بأن يتوافر القصد الخاص لدى المتهم، المتمثل في ضرورة تأثير الدخول في نظام الكمبيوتر، سواء بإلغاء البيانات أو حذفها أو تدميرها أو تسريبها أو إتلافها أو تغييرها أو بإعادة نشرها، وهو نفس توجه القانون الألماني والكندي والياباني.

3. 1. 2 جريمة الاعتداء على منتجات النظام الآلي للمعطيات

تجرم مقتضيات الفصل 607-6 من مجموعة القانون الجنائي المغربي، كل من أدخل معطيات في نظام المعالجة الآلية للمعطيات أو أتلفها أو حذفها منه أو غيَّر المعطيات المدرجة فيه، أو غيَّر طريقة معالجتها، أو طريقة إرسالها عن طريق الاحتيال؛ وذلك كيفما كانت الوسيلة المعتمدة، سواء وسائل مادية أو معنوية (الفصل 607-6 من القانون رقم 07.03 المتعلق بنظم المعالجة الآلية للمعطيات، 2003).

حيث تكون وسائل الاعتداء مادية إذا وقعت هذه الأفعال على الأجهزة المادية للنظام، أو منعت من الوصول إليها.

وتكون هذه الوسائل معنوية إذا وقعت على الكيانات المنطقية للنظام، مثل البرامج والمعطيات (ممدوح، 2019، ص. 278)، ومن بين الاختراقات المعلوماتية التي كان لها تأثير عالمي اختراق الكونجرس الأمريكي بتاريخ أغسطس 2016، حيث تمكن أحد القراصنة الأمريكيين من نشر أرقام هواتف وعناوين البريد الإلكتروني لما يقارب 200 عضو ديموقراطي سابقين وحاليين في الكونغرس، في شهر أغسطس من عام 2016، وكان من ضمن المعلومات المنشورة رقم هاتف الأقلية الديمقراطية نانسي بيلوسي (عكور، 2014، ص. 5).

ومثل ذلك كمن يقوم بإعداد برامج تحتوي على فيروسات قصد بثها على شبكة الإنترنت؛ مما قد يهدم أنظمة المعالجة الإلكترونية أو يوقفها أو يفسدها أو يعدل معطياتها أو يعدل طريقة معالجتها.

كما جرم المشرع المغربي كذلك كل أفعال تزوير وتزييف الوثائق المعلوماتية بالنظام الآلي كيفما كان شكلها عندما يكون من شأنها إلحاق الضرر بالغير (فتح الله، 2021، ص. 458)، ويشمل التجريم استعمال هذه الوثائق المعلوماتية مع العلم بأنها مزورة أو مزيفة، وذلك للخطورة الإجرامية لمثل هذه الأفعال على الغير.

ونقصد بالتزوير كل فعل يقوم به الشخص من أجل الدخول إلى نظام المعالجة الآلية للمعطيات، بغرض تغيير أو محو هذه المعطيات، سواء أكانت مجمعة أو معالجة أو مرسلة بواسطة نظام معلوماتي معين، أو بغرض القيام بتغيير الاستعمال الممكن لهذه المعطيات.

وتبعًا لمقتضيات الفصل 607-6 من مجموعة القانون الجنائي المغربي، وكذا الفصل 133 من القانون الجنائي المغربي، تعتبر الجريمة المعلوماتية من الجرائم العمدية التي اشترط المشرع لتحققها توافر القصد الجنائي العام بعنصريه العلم والإرادة، فمثلًا جريمة الدخول والبقاء غير المشروع داخل نظام المعالجة الآلية للمعطيات، لا تقوم إلا بإثبات عنصر العمد المتمثل في ضرورة إثبات أن الدخول قد تم عن طريق الاحتيال، كما عاقب المشرع كذلك حتى على مجرد محاولة القيام بالجريمة المعلوماتية، إذا تحققت شروط هذه المحاولة.

3. 2 آليات اتفاقية بودابست لمكافحة الجريمة المعلوماتية دوليًّا

لقد أقرت اللجنة الوزارية لمجلس أوروبا هذه الاتفاقية بتاريخ 8 نوفمبر2001، وذلك في دورتها رقم 109، وقد تم إعطاء المجال للانضمام والتوقيع عليها بالمؤتمر الدولي الذي أقيم ببودابست بدولة المجر بتاريخ 23-11-2001، وهي من أهم الاتفاقيات التي تهدف إلى محاربة الجريمة المعلوماتية والتي صادقت عليها الكثير من الدول الأجنبية ومنها المملكة المغربية سنة 2018 .

ولقد تم اعتماد هذه الاتفاقية لإيجاد الحلول لمجموعة من الإشكالات التي طرحتها الدول لمكافحة ومحاربة هذه الجريمة، وذلك بحكم أن الجريمة المعلوماتية لا حدود لها، وهي من الجرائم العابرة للقارات، ولا تعترف بجغرافية الحدود.

كما طرحت عدة إشكالات على مستوى السلطات القضائية المختصة بها عندما تكون الجريمة عابرة للقارات، وهو نفس الإشكال الذي طرح بشأن السلطات الأمنية المختصة كذلك بالبحث في مثل هذه الأحوال.

ولقد أتت هذه الاتفاقية لتوحيد السياسة الجنائية في مجال مكافحة الجريمة المعلوماتية من طرف الدول الأعضاء فيها، كما

أسهمت في تكريس وتعزيز إجراءات وقواعد موحدة للتعاون القضائي الدولي، بالإضافة إلى تسهيل التنسيق بين مختلف الدول الأعضاء لمحاربة هذه الجريمة ومكافحتها.

وذلك إدراكًا منها للتغيرات العميقة التي أحدثتها الرقمية -dig italisation ، والتقارب convergence والعولمة المستمرة لشبكات الحاسب الآلي والقلق من استخدام هذه الشبكات والمعلومات الإلكترونية لارتكاب جرائم جنائية، واعترافًا منها بالحاجة للتعاون بين الدول والقطاع الخاص في مكافحة جرائم الإنترنت لحماية المصالح المشروعة في استخدام وتطوير تقنيات المعلومات.

وإيمانًا منها بأن مقتضيات هذه الاتفاقية سوف تغني عن الإجراءات الكلاسيكية المتمثلة في الإنابات القضائية التي تستغرق وقتًا كبيرًا لإنجاز الانتدابات القضائية؛ حيث دعت هذه الاتفاقية إلى تكريس آليات تعاون سريعة وفعالة ودقيقة لإجراء الأبحاث والتحقيقات الجنائية بأسرع وقت ممكن.

وبعد استقراء مقتضيات هذه الاتفاقية، نستعرض بعض الحلول التي قدمتها هذه الاتفاقية في مجال آليات التعاون القضائي بين الدول الأعضاء لمكافحة الجرائم أعلاه، والتي نذكر منها ما يلي (محمود، 2022، ص. 958):

- توحيد المفاهيم وتعريف مجموعة من المصطلحات الأساسية المتعلقة بالجريمة المعلوماتية بصفة عامة، وبالجرائم محل الدراسة بصفة خاصة، كنظام الحاسب Computer System، وبيانات الحاسب Computer Data، ومزود الخدمة Service Provider ، وبيانات حركة المرور Data Traffic.
- ألزمت الدول الأعضاء بالالتزام بمقتضيات هذه الاتفاقية، وخصوصًا التركيز على ضرورة تعاون الجهات المكلفة بوسائل الاتصالات مباشرة مع السلطات القضائية المختصة بالتحقيقات في مثل هذه الجرائم.
- تضمنت المبادئ العامة للتعاون القضائي الدولي بما في ذلك تسليم المجرمين المعلوماتيين بأسرع وقت وتحديد وسائل التعاون لتقديم كل ما من شأنه أن يسهل إجراءات البحث والتحقيق دون عراقيل أو بروتوكول.

وبناءً على هذه الاتفاقية يمكن إصدار أوامر إلى مقدمي الخدمات المتعلقة بمنظومة الحاسوب الآلي والإنترنت، مع إلزامهم بنفس الوقت بالحفاظ على السر المهني والبيانات المقدمة للجهات المختصة بالبحث والتحقيق الجنائيين.

4. الخاتمة

لقد وقفنا خلال هذه الدراسة على أهم خصائص المجرم المعلوماتي؛ وذلك بعد الإشارة إلى بعض صور الجريمة المنظمة. كما تطرقنا لأحكام بعض أنواع الجرائم المعلوماتية في التشريع المغربي والتشريع المقارن، خاصة منها جريمة الدخول الاحتيالي لنظام المعالجة الآلية للمعطيات وجريمة الاعتداء على منتجات النظام الآلي، لنخلص في الأخير إلى أهم اتفاقية دولية صادق عليها المغرب في مجال مكافحة الجريمة المعلوماتية ألا وهي اتفاقية بودابست.

ونرى أنه في ظل ازدياد الجرائم المعلوماتية، ما يزال العمل على تطوير آليات مكافحة هذا النوع من الجرائم الخطيرة قائمًا، وذلك من خلال التكثيف من عقد المؤتمرات والندوات الدولية، وكذا من خلال الاتفاقيات الدولية التي سوف تساعد في توحيد إجراءات ملاحقة المجرم المعلوماتي، وكذا في توحيد الإجراءات التي سوف تساعد في عملية التوقيف والمحاكمة بأسرع وقت ممكن.

كما يجب تكثيف التكوينات والتدريب في نفس المجال للساهرين على تتبع مثل هذه الجرائم، سواء تعلق الأمر برجال الشرطة القضائية، أو قضاة النيابة العامة، أو الشرطة العلمية المختصة بإنجاز الخبرات، أو هيئات الحكم.

ونظرًا لما يشكله هذا النوع من الإجرام من خطورة على الأفراد والمجتمع والعالم، وجب البحث عن السياسات التجريمية والعقابية بشكل مستمر، من أجل مكافحة هذه الجرائم أو على الأقل التقليل منها، ونذكر من التوصيات والمرتكزات التي قد تساعد في مكافحة هذه الجرائم:

- **الرقابة الأمنية:** تطوير مهارات الجهات الأمنية والقضائية المختصة بمحاربة مثل هذا النوع من الإجرام بشكل مستمر، وذلك تحت إشراف الباحثين والخبراء في الميدان، لكي يكون انسجام بين الجهات القضائية الساهرة على النظر في مثل هذه القضايا وبين الشرطة التقنية التي تهتم بالبحث والتحقيق تقنيًا وفنيًا.
- **التوعية الاجتماعية:** التركيز على التوعية المستمرة لأفراد المجتمع بضرورة الامتثال للقوانين الجاري العمل بها فيما يخص هذه الجرائم، وضرورة الوقاية السابقة عن طريق التحصين وعدم إفشاء الأسرار المتعلقة بالمعلومات، وذلك مثلًا كإرسال رسائل نصية تحذر من مشاركة الأرقام السرية الخاصة بهم مع الآخرين، وكذلك عبر التحذير من الاختراقات التي قد شهدتها بعض القضايا الراهنة.
- **التأكيد على مرتكزات السياسة الجنائية الإسلامية:** وذلك بالتركيز على مرتكزات السياسة الجنائية الإسلامية فيما يخص

محاربة الجريمة عامة، سواء منها التي تهدف إلى حماية الفرد أو التي تهدف إلى حماية المجتمع؛ وذلك من خلال الحث على القيم الدينية ودورها في كبح الاستعدادات الإجرامية.

- دعم البحث العلمي في مجال إنتاج مضادات الفيروسات، والحماية المضادة من كل الاعتداءات الإجرامية، ودعم الدول هذه الآليات ماديًّا لتكون في متناول الجميع.
- تنظيم الورشات والندوات التكوينية التحسيسية حول أحدث تقنيات مكافحة مثل هذا الإجرام.
- سرعة التدخل: وذلك برصد فرق أمنية خاصة للتدخل السريع وضبط المشتبه فيهم بأسرع وقت، وكذا تسريع آليات إصدار قوانين الحماية من مثل هذه الجرائم.
- المصادقة على الاتفاقيات الدولية، المتعلقة بالتعاون القضائي الدولي في هذا المجال، وخاصة منها اتفاقية بودابيست التي توحد المفاهيم المتعلقة بهذه الجريمة، وكذا لتسهيل التعاون القضائي الدولي فيما يتعلق بكل الإجراءات الجزائية.
- اعتماد إجراء الاختراق ضمن مقتضيات النظام الجزائي الإجرائي لمكافحة مثل هذا النوع من الإجرام، وذلك مع احترام الشرعية الدولية التي تكرس حق الأفراد في حماية معطياتهم الشخصية، وفي حماية حياتهم الشخصية، وسوف يمكن ذلك من رصد أخطر العصابات الإجرامية في المجال المعلوماتي.
- محاربة تهريب الأجهزة وضبط استعمالاتها عند الضرورة والتي قد تمكن من تسهيل اختراق أنظمة الحاسب الإلكتروني، وتمكين إدراة الجمارك من أحدث الوسائل والتقنيات لاكتشاف ذلك.

الإفصاح عن تضارب المصالح

يعلن (المؤلف) أنه ليس لديه أي تضارب في المصالح للمقالة المنشورة.

الإفصاح عن تمويل البحث

يعلن (المؤلف) أن البحث المنشور لم يتلق منحة مالية من أية جهة تمويل في القطاعات العامة أو التجارية أو المؤسسات غير الربحية.

المصادر والمراجع

أولًا: المراجع العربية:

جواحي، عبد الستار (2015-2014) جرائم الحاسوب: دراسة مقارنة بين الشريعة الإسلامية والقانون الجزائري، مذكرة لنيل شهادة الماستر في العلوم الإسلامية تخصص الشريعة والقانون.

حميشي، أحميدة (2016) جرائم المس بالنظم المعلوماتية في التشريع المغربي والمقارن، جريمة الإتلاف المعلوماتي نموذجًا، مجلة القانون والأعمال، عدد 14، ص.28.

خليفة، محمد (2007) الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري المقارن، الطبعة الأولى، دار الجامعة الجديدة.

الديربي، عبد العالي (2012م) الجرائم الإلكترونية، الطبعة الأولى، المركز القومي للإصدارات القانونية، القاهرة.

رستم، هشام فريد (1994) الجوانب الإجرائية للجرائم المعلوماتية، دراسة مقارنة، مكتبة الآلات الحديثة، أسيوط، طبعة.

الشوا، محمد سامي (1994) ثورة المعلومات وانعكاساتها على قانون العقوبات، الطبعة الأولى، دار النهضة العربية، القاهرة.

صغير، يوسف (2013) الجريمة المرتكبة عبر الإنترنت، مذكرة لنيل شهادة الماستر في القانون، كلية الحقوق والعلوم السياسية.

عكور، سومية (2014) الجرائم المعلوماتية وطرق مواجهتها، ورقة علمية قدمت بالملتقى العلمي للجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية، كلية العلوم الإستراتيجية، المملكة الأردنية الهاشمية، عمان، ص.5.

فتح الله، محمود رجب (2021) شرح جرائم الابتزاز الإلكتروني: دراسة تطبيقية مقارنة، دار الجامعة الجديدة للنشر، الإسكندرية.

القانون رقم 20.05 المتعلق بالأمن السيبراني (الصادر بتاريخ 25 يوليو 2020).

القانون رقم 53.05 المتعلق بالتبادل الإلكتروني للمعطيات القانونية (الصادر بتاريخ 30 نوفمبر 2007).

القانون رقم 07.03 والمتمم لمجموعة القانون الجنائي فيما يتعلق بالجرائم المتعلقة بنظم المعالجة الآلية للمعطيات (الصادر بتاريخ 22 دجنبر 2003م).

القانون رقم 31.08 القاضي بتحديد تدابير لحماية المستهلك (الصادر بتاريخ 18 فبراير 2011).

القانون رقم 08.09 المتعلق بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي) الصادر بتاريخ فبراير 2009).

كوبان، الناجم (2016) الطبعة الاستثنائية للجرائم المعلوماتية، مجلة القانون المغربي، عدد 32، ص. 165.

محمود، سعد عبد المجيد (2022) المجرم المعلوماتي، دار المطبوعات الجامعية، الإسكندرية.

ممدوح، خالد إبراهيم (2009) الجرائم المعلوماتية، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية.

الملط، أحمد خليفة (2006م) الجرائم المعلوماتية، الطبعة الثانية، الإسكندرية.

ثانيًا: المراجع الأجنبية:

- Tappolet , (1988)la fraude informatique, rev. Inter. crim. et pol. Techn. p 351.

المواقع الإلكترونية باللغات الأجنبية

www.legifrance.gouv.fr

موقع وزارة العدل البلجيكية:

https://ticsipd.ch/protection-des-donnees/protection-des-donnees-en-belgique/

موقع مجلس أوروبا.

https://www.coe.int/fr/web/cybercrime/the-budapest-convention