الجمهورية الجزائرية الديمقراطية الشعبية
République Algérienne Démocratique et Populaire

وزارة التعليم العالي والبحث العلمي
جامعة عين تموشنت بلحاج بوشعيب
كلية الحقوق

Ministère de L'enseignement Supérieur et de La Recherche Scientifique
Université Ain Témouchent Belhadj Bouchaib
Facultés de drois

الجريمة الإلكترونية في القانون المقارن

مذكرة تخرج مقدمة لنيل شهادة ماستر

تخصص قانون عام

من إعداد :

- **بن يخلف شيماء إيمان**
- **شرفي يسرى**

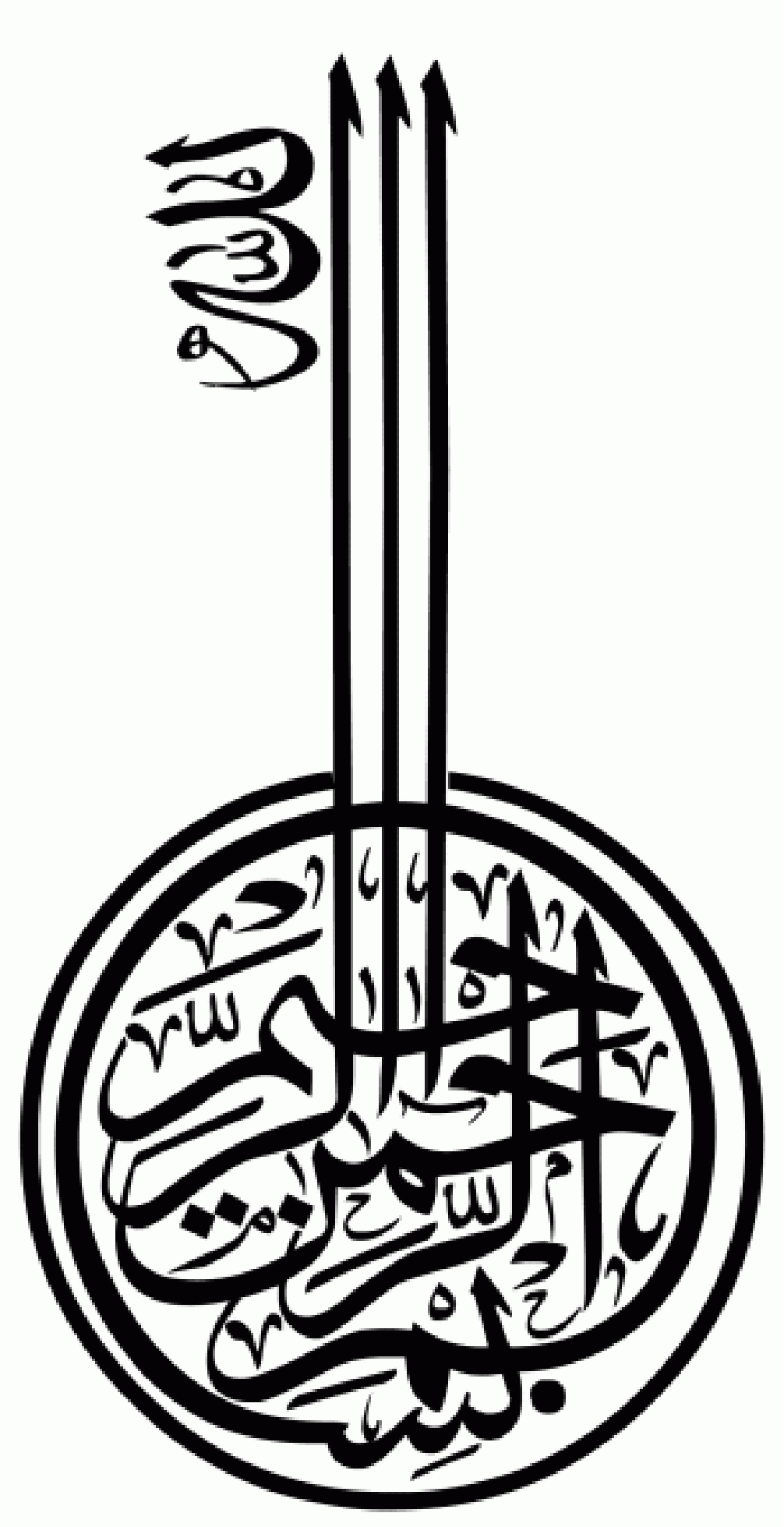
تحت إشراف الأستاذ(ة):

د / بوكايس سمية

أعضاء لجنة المناقشة

الاسم واللقب	الرتبة	مؤسسة الانتماء	الصفة
براهمي عبد الرزاق	**أستاذ محاضر "ب"**	جامعة بلحاج بوشعيب عين تموشنت	**رئيسا**
بوكايس سمية	**أستاذ محاضر "ب"**	جامعة بلحاج بوشعيب عين تموشنت	**مشرفا**
فوحال رياض	**أستاذ مساعد "ب"**	جامعة بلحاج بوشعيب عين تموشنت	**ممتحنا**

السنة الجامعية: 1444-1445 /2024/2023



شكروعرفان

نتقدم بالشكر لله تعالى الذي أنعمنا بالعقل والذكر ووهبنا روح العلم والمعرفة.

والصلاة والسلام على أشرف الخلق، فإن ماينا سب هذا المقام أن نذكر الفضل لأهله

الشكر والامتنان للدكتورة والأستاذة المشرفة بوكايس سمية على كل نصائحها وحسن تواضعها ، أسأل العلي القدير أن يزيدها رفعة وقدرا وعلما نافعا.

كما نتقدم بالشكر إلى كل أعضاء لجنة المناقشة المحترمة لتفضلهم بمناقشة المذكرة وإثرائها بآرائهم السديدة

كما نتوجه بجزيل الشكر إلى من ساعدنا على إتمام هذا البحث المتواضع وكان لنا عونا في القيام به

مع فائق الإحترام والتقدير

إهداء

الى من ربط الله طاعته بطاعتهما والدي العزيزين

الى من علمني معنى الكفاح، من زرع في نفسي قوة الإرادة، إلى من تعب من أجلي، إلى رمز التضحية، إلى أبي العزيز.

إلى من رفعتني بدعواتها ودعمها في كل خطوة، إلى أغلى ما في الوجود، إلى أمي الغالية.

أطال الله في عمرهما وبارك الله فيهما.

إلى شموع البيت إخوتي، وإلى روح قلبي جدتي فاطمة وعمتي عمارية وابنة خالي.

والى كل هؤلاء الذين تجاوزهم قلمي ولم يتجاوزهم قلبي.

إيمان

إهداء

أولا اشكر الله عز وجل على توفيقه لنا لإنجاز هذه المذكرة

أهدي تخرجي إلى من جرع الكأس فارغا ليسقيني قطرة حب

إلى من حصد الأشواك عن دربي ليمهد لي طريق العلم

إلى أبي رحمه الله

كما أهدي تخرجي وحصاد ما زرعته سنين طويلة في سبيل العلم

إلى أمي الحبيبة أطال الله في عمرها

الشكر موصول أيضا إلى أخوتي وكل من ساهم في مساعدتي في هذا العمل

وفي الأخير لا يسعنا إلى أن ندعوا من الله الكريم السداد والوفاق والعفاف

يسرى

قائمة أهم المختصرات

ج.ر: الجريدة الرسمية

د.س: دون سنة

د.ط: دون طبعة

ص: صفحة

ق : قانون

ق.إ.ج: قانون الإجراءات الجزائية

ق.ع.ج: قانون العقوبات الجزائري

PHKE: مركز احتيال المعلومات الوطني في الولايات المتحدة الأمريكية

OCDE: منظمة التعاون الاقتصادي والتنمية

مقدمة

أثرت التكنولوجيات الحديثة على الحياة العامة فأصبح من الحتمي تعميم الرقمنة عبر المؤسسات لخلق جو من التسهيلات لدى الأشخاص، ونتيجة لذلك ظهرت الجريمة الالكترونية أو السيبرانية في ظل سوء استخدام التقنيات الحديثة واستغلالها من طرف بعض الأفراد، فقد مرت الجرائم الإلكترونية بتطور تاريخي تبعا لتطور التقنية واستخداماتها، لذلك لقد مرت كل دولة بسلسلة من الأحداث أجربتها على تكييف قانونها الخاص للحد من هذه التجاوزات.

في مصر صدر القانون رقم 1750 لسنة 2018 ولائحته التنفيذية رقم 1699 لسنة 2020 بشأن مكافحة جرائم تقنية المعلومات،ولم يكن هو الخطوة الأولي في مجال التشريع المعلوماتى، بل سبقه العديد من الاجتهادات التشريعات التي تناولت تنظيم مجال التقنية المعلوماتية كان من بينها قانون حماية الملكية الفكرية، وقانون التوقيع الالكترونية، وقانون تنظيم الاتصالات وتكنولوجيا المعلومات، ولم يقف الأمر عند هذا الحد فقط، بل لقد كان حرص المشرع المصري في هذا الشأن عظيماً وضمن بنصوص الدستور المصري الصادر عام 2014 العديد من النصوص التشريعية المتعلقة بتنظيم تقنية المعلومات.[1]

أما في فرنسا فقد صدر قانون 6 يناير 1978م خاص بالمعالجة الإلكترونية للبيانات الاسمية وبينما كان مطروحاً للنظر أمام مجلس الشيوخ أعد لتعديل قانون حرية الاتصالات الصادر 1986م ليتفق مع التوجيهات الأوروبية الجديدة، تقدمت الحكومة الفرنسية بتعديل هذا المشروع يتعلق بإضافة مواد جديدة للقانون المذكور بشأن الإذاعة والتلفزيون مستهدفة الحكومة من هذا التعديل تعريف القائم على تقديم خدمة الإنترنت، وشروط ممارسة هذه الخدمة التي منها ضرورة الحصول على موافقة مسبقة كغيره ممن يقومون بتوفير خدمات الاتصالات السمعية والبصرية من المجلس الأعلى للإذاعة والتلفزيون.

وقد اعتبر جانب من الفقه أن المشروع عندما قام بتعريف الاتصالات السمعية والبصرية قد وسع في التعريف بحيث شمل خدمات الإنترنت من بين وسائل الاتصال، وعندما عرض المشروع على المجلس الدستوري قرر عدم دستورية الفقرتين (2) (3) من المادة (43) من المشروع استناداً إلى أن نص هاتين الفقرتين يخل ويقيد حرية الاتصال وتبادل الأفكار والآراء التي تعد من أسمى حقوق الإنسان الذي من حقه أن يتكلم ويكتب ويطبع بحرية طالما لم يسيء استخدام هذه الحرية التي حددها القانون، وكانت

[1] حاتم أحمد محمد بطيخ، تطور السياسة التشريعية في مجال مكافحة جرائم تقنية المعلومات(دراسة تحليلية مقارنة)، جامعة عين شمس، مصر، د.س، ص6.

مأخذ المجلس الدستوري على المشروع أنه لم يضع ضوابط يتم بمقتضاها إصدار الموجهات العامة والقرارات التي تصدر بناءً عليها وخصوصاً أنه قد يترتب عليها قيام المسؤولية الجنائية.[2]

وعقب فشل المشرع الفرنسي تنظيم استعمال الإنترنت في عام 1996 صدر القانون رقم 19 لسنة 1988 المتعلق ببعض الجرائم المعلوماتية مع التعديل الذي أدخل في سنة 1992.. ثم صدر قانون رقم 230 لسنة 2000 في شأن الإثبات والمتعلق بالتوقيع الإلكتروني، إلى غاية آخر تعديل من القانون العقوبات الفرنسي 29 جويلية 2023، نجده لم يتطرق إلى مفهوم الجريمة إلالكترونية وإنما استعمل مصطلح "المساس بأنظمة المعالجة الآلية للمعطيات ".في المواد من 1_313إلى 7_323من قانون العقوبات.[3]

أما الجزائر فقد عرفت هذا نوع من الجرائم بداية من سنة 2000 حين نص عليها في قوانين البريد[4]، إضافة إلى تخصيص نص كامل لها في قانون نوفمبر 2004 حينما عدل المشرّع الجزائري قانون العقوبات بإدراج وصف الجرائم الإلكترونية في الفصل السابع[5]، حيث استعمل عبارة "جرائم المساس بأنظمة المعالجة الآلية للمعطيات"، فمجرد الدخول إلى كمبيوتر شخص يعتبر جريمة الكترونية، والبقاء في الأنظمة وتغيير المعطيات وتعديلها وتزييفها يعد من أشكال هذه الجريمة.

ومؤخرا تشهد الجرائم الإلكترونية في بلدنا تزايداً ملحوظاً في الأعوام الأخيرة، مما يعكس التطور التكنولوجي واستخدام الإنترنت بشكل واسع. يتضمن نطاق الجرائم الإلكترونية في البلاد مجموعة متنوعة من الأنشطة غير القانونية، مثل الاحتيال الإلكتروني، واختراق البيانات، وسرقة الهوية، والابتزاز الإلكتروني.

وفقاً لتقارير رسمية، فإن عدد الجرائم المبلغ عنها زاد بشكل ملحوظ، حيث سجلت السلطات القضائية حوالي 1,500 جريمة إلكترونية في عام 2021، بارتفاع مقداره حوالي 25% عن العام السابق،

---

[2]المطردي، مفتاح بو بكر، الجريمة الإلكترونية، ورقة عمل مقدمة إلى المؤتمر الثالث لرؤساء المحاكم العليا في الدول العربية، السودان، 23-25\09\2012.

[3]رزاق بارة كريمة، الجريمة إلالكترونية المتعلقة بالأشخاص وفقا للتشريع الفرنسي والتشريع الجزائري، المركز الجامعي عبد الحفيظ بوالصوف ميلة – الجزائر، 18\01\2024، ص453.

[4]قانون رقم 2000-03 المؤرخ في جمادى الأولى عام 1421 الموافق 05 غشت سنة 2000، يحدد القواعد العامة المتعلقة بالبريد والمواصلات السلكية و اللاسلكية.

[5]لجريدة الرسمية العدد : 06 المؤرخة في 10 فيفري 2015

حيث أن الجرائم المالية تشكل نسبة كبيرة من هذه الجرائم، وتتركز في الاحتيال المالي عبر الإنترنت والتلاعب بالبيانات المالية للأفراد والشركات.[6]

أهمية الموضوع:

أهمية دراسة الجرائم الإلكترونية تتجلى في تأثيرها البالغ على الأفراد والمجتمعات على مستوى عالمي. فالتطور التكنولوجي السريع وانتشار استخدام الإنترنت أدى إلى زيادة تعدد وتنوع الجرائم الإلكترونية، مما جعلها تهدد الأمن القومي والاقتصادي والشخصي للأفراد والمؤسسات على حد سواء.

أسباب إختيار الموضوع:

من بين الأسباب التي كانت دافعا لنا لاختيار هذا الموضوع:

- رأينا أن الإنترنت قد وفرت فرصة ملائمة لذوي النفوس الضعيفة والمنظمات الإجرامية لتوظيفها في عملياتهم المختلف؛
- حداثة الموضوع بناءً على معرفتنا؛
- الرغبة في إثراء مكتبة الكلية بدراسة جديدة.

أهداف الدراسة:

تهدف هذه الدراسة إلى فهم ظاهرة الجرائم الإلكترونية فهم عميق، طبيعتها، وأساليب ارتكابها، والتقنيات المستخدمة فيها، ومنابعها، وتحليل السياسات والقوانين القائمة في مختلف الدول والمنظمات الدولية لمكافحة الجرائم الإلكترونية، وتقييم فعاليتها ومدى تكيفها مع التطورات التكنولوجية والتحديات الجديدة، وتقدير تأثيرات الجرائم الإلكترونية على الأفراد والمجتمعات والاقتصاديات، بما في ذلك التكاليف الاقتصادية والاجتماعية والنفسية للضحايا والمجتمعات المتأثرة.

الدراسات السابقة:

هناك العديد من الدراسات التي تناولت الجريمة الإلكترونية بشكل عام، ومن أبرز المراجع التي تعتبرها مخصصة تناولت الموضوع الجريمة الإلكترونية كتاب الجرائم الإلكترونية والوقاية منها في القانون

[6] عثمان لحياني، مقال بعنوان الدرك الوطني يكشف عن حصيلة الجرائم الإلكترونية بالجزائر عامي 2022 و2023، جريدة الشروق أونلاين، على الموقع www.echoroukonline.com، تاريخ الولوج: 2024/06/18 على الساعة 18:29.

الجزائري للدكتور يزيد بوحليط، ومقال الآليات الإجرائية للكشف عن الجريمة المعلوماتية للباحثة مجدوب نوال، والمذكرة آليات مواجهة الجريمة الإلكترونية في التشريع الجزائري للطالبتين عقباش بريزة مبارك حنان.

الصعوبات

- طبيعة الموضوع في حد ذاته وعدم معالجته كمقارنة بين عدة قوانين من قبل إذ وجدنا شح في الدراسات المقارنة على مستوى الجزائر؛
- صعوبة التنقل من مكان العمل ومكتبة الجامعة؛
- قصر الوقت المخصص لتحضير المذكرة.

- **طرح الإشكالية:**
- من خلال ما سبق يمكن أن نطرح الإشكالية الرئيسية الآتية:
- **هل النصوص القانونية المنظمة للجريمة الالكترونية كافية للحد من هذه الظاهرة في التشريعات المقارنة؟**

المنهج المتبع:

لدراسة هذا الموضوع دراسة علمية دقيقة قمنا باستخدام منهجين أساسين والذي اعتمدنا فيهاالأول المنهج الوصفي، الاقتباس المباشر والغير المباشر، الذي قمنا من خلاله وصف ظاهرة مهمة وهي إرتكاب الجرائم الإلكترونية وكيف ينظر إليها المشرع الجزائري ومختلف التشريعات المقارنة.

والثاني المنهج تحليل المضمون من خلال تحليل نصوص الاتفاقيات الدولية ومواد قوانين التشريعات المقارنة المتعلقة بموضوع البحث.

خطة الدراسة:

تهدف هذه المذكرة إلى دراسة الجرائم الإلكترونية من منظور القانون المقارن، مع التركيز على التشريعات الجزائرية ومقارنتها بالتشريعات الدولية. من خلال هذا النهج، نسعى إلى تقديم تحليل شامل للجهود المبذولة لمكافحة الجرائم الإلكترونية وتقييم فعالية هذه التشريعات. سيتناول **الفصل الأول ماهية الجريمة الإلكترونية**، من خلال تعريفها واستعراض خصائصها ودوافع ارتكابها بالإضافة إلى أركانها وأنواعها.

أما **في الفصل الثاني، سنستعرض آليات مكافحة الجريمة الإلكترونية في القانون المقارن،** مع التركيز على الوسائل التقنية والقانونية المستخدمة للكشف عن هذه الجرائم والتصدي لها.

الفصل الأول: ماهية الجريمة الإلكترونية في التشريع الجزائري والقانون المقارن

تمهيد

تعتبر الجريمة الالكترونية أو السيبرانية وليدة عن الاستعمال السيئ لثورة التكنولوجيا المعلوماتية، لهذا فهي تختلف عن الجريمة التقليدية في مضمونها وطبيعتها وأدواتها وطريقة ارتكابها، وحتى في خصوصيتها وخصوصية مرتكبيها، لذا كان لزاما علينا التعرض لكل تفاصيلها من أجل التعرف عليها وتحديد كل معالمها.

وعلى هذا الأثر قمنا بتقسيم هذا الفصل إلى مبحثين:

المبحث الأول: الإطار المفاهيمي للجريمة الالكترونية في التشريع الجزائري والقانون المقارن

المبحث الثاني: أركان وأنواع الجريمة الإلكترونية في التشريع الجزائري والقانون المقارن

المبحث الأول

الإطار المفاهيمي للجريمة الالكترونية في التشريع الجزائري والقانون المقارن

إن الجريمة الإلكترونية من الجرائم المستحدثة المرتبطة بمجال المعلوماتية، هذا ما يجعلها تختلف عن الجرائم التقليدية من خلال مضمونها وخصائصها، إذ أن سرعة انتشارها تجعلها تستهدف الأفراد والمجتمع والدول، من خلال هذا المبحث سنتطرق إلى تعريف الجريمة الإلكترونية في المطلب الأول، .ونعرج لمعرفة خصائصها ودوافع ارتكابها.

المطلب الأول

تعريف الجريمة الالكترونية في التشريع الجزائري والقانون المقارن

تعتبر الجرائم الإلكترونية من الظواهر الحديثة نظرا لارتباطها بتقنية متطورة هي تكنولوجيا المعلومات والاتصالات مما صعب من وضع تعريف جامع لها، ولإيجاد تعريف عام وشامل قمنا بتقسيم هذا المطلب إلى ثلاثة فروع حيث تطرقنا في الفرع الأول إلى تعريف الجريمة الالكترونية في مختلف القوانين وفي الفرع الثاني إلى تعريف الجريمة الالكترونية في القانون الدولي والاتفاقيات الدولية وأخيرا الفرع الثالث تناول تعريف الجريمة الالكترونية في الفقه.

الفرع الأول: تعريف الجريمة الالكترونية في مختلف القوانين

عالج المشرع الفرنسي الجريمة الإلكترونية منذ صدور القانون المتعلق بتكنولوجيا المعلومات والحريات رقم 78/17 الصادر في 6جانفي1978، بعد ذلك جاء قانون godfrain والمتعلق بالاحتيال عبر الكمبيوتر، رقم 19/88.

مما جعل من الممكن فرض عقوبات على حذف البيانات وتعديلها وكذلك الهجمات على أنظمة المعلومات. إلى غاية آخر تعديل من القانون العقوبات الفرنسي 29 جويلية ،2023 نجده لم يتطرق إلى مفهوم الجريمة الإلكترونية وإنما استعمل مصطلح "المساس بأنظمة المعالجة الآلية للمعطيات ".في المواد من 1-313 إلى 7_323من قانون العقوبات[1].

[1]رزاق بارة كريمة، الجريمة الالكترونية المتعلقة بالأشخاص وفقا للتشريع الفرنسي والتشريع الجزائري، المجلة الجزائرية للحقوق والعلوم السياسية، المجلد 08، العدد 02، 2024، ص 454.

كما عرف المشرع المصري الجريمة الإلكترونية في قانون مكافحة جرائم تقنية المعلومات الصادر بالقانون رقم 175 لسنة 2018. وفقًا لهذا القانون، تُعرّف الجريمة الإلكترونية "كل فعل ارتكب متعمداً أو غير متعمد، باستخدام أية وسيلة من وسائل تقنية المعلومات يترتب عليه تعريض أحد الأشخاص أو المؤسسات أو الأجهزة أو الأنظمة أو الشبكات أو البيانات والمعلومات أو البرمجيات إلى أحد المخاطر أو الأضرار المنصوص عليها في هذا القانون".[1]

ينص القانون على مجموعة متنوعة من الجرائم الإلكترونية، تشمل:

جرائم الوصول غير المشروع: مثل اختراق الأنظمة أو الحسابات أو الدخول على بيانات أو برامج دون تصريح.

جرائم التزوير الإلكتروني: مثل تزوير الوثائق أو المستندات الإلكترونية.

جرائم المحتوى الإلكتروني غير المشروع: مثل نشر أو توزيع مواد غير قانونية أو محتوى ضار.

جرائم الاستيلاء على الأموال أو النصب الإلكتروني: مثل الاحتيال عبر الإنترنت أو الاستيلاء على بيانات بنكية.

جرائم انتهاك الخصوصية: مثل التجسس الإلكتروني أو انتهاك حرمة الحياة الخاصة.[2]

في هذا الشأن، اصطلح المشرع الجزائري على تسمية الجرائم الإلكترونية أو المعلوماتية بمصطلح الجرائم المتصلة بتكنولوجيا الإعلام والاتصال وعرفها بموجب أحكام المادة (02/1) من القانون رقم 04 – 9 مؤرخ في 5 غشت سنة 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها[3] على أنها : "جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية..."،

فنص على جرائم المساس بأنظمة المعالجة الآلية للمعطيات بموجب المواد 394 مكرر إلى 394 مكرر بقانون العقوبات الجزائري[4]، وإن كان استعمال هذا المصطلح ينصرف وفقا لدلالة الكلمة إلى

[1] المادة 01 من قانون مكافحة جرائم تقنية المعلومات رقم 175 لسنة 2018 الباب الأول.

[2] المواد من 02 الى 7 من نفس القانون.

[3] القانون رقم 09 – 04، مؤرخ في 5 أوت سنة 2009 ، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

[4] المواد من (394) – 394 مكرر (7) من قانون العقوبات الجزائري رقم 04-15 المؤرخفي 10 نوفمبر 2004.

المعلومات والنظام الذي يحتوي عليها بما في ذلك شبكة المعلومات، وهو بذلك يتوافق مع موقف المشرع الفرنسي في أن نظام المعالجة الآلية للمعطيات يشمل أيضا شبكة المعلومات وفقا للقانون الصادر سنة 1978، بمعنى أنه يشمل جميع العمليات التي تتم بواسطة الوسائل الإلكترونية.

غير أن هذا المصطلح يقتصر على الجرائم التي تستهدف النظام فقط ليخرج بذلك من نطاقه ما دون ذلك من الجرائم التي يكون فيها نظام المعالجة الآلية للمعطيات وسيلة لارتكابها. وانطلاقا من فحوى هذه المادة نستنتج أن المشرع الجزائري قسم هذه الجرائم المستحدثة الى ثلاثة أنواع:

- جرائم المساس بأنظمة المعالجة الآلية للمعطيات.
- جرائم ترتكب أو يسهل ارتكابها عن طريق المنظومة المعلوماتية.
- جرائم ترتكب أو يسهل ارتكابها عن طريق نظام للاتصالات الإلكترونية.[1]

الفرع الثاني: تعريف الجريمة الالكترونية في القانون الدولي والاتفاقيات الدولية

عرفتها منظمة التعاون الاقتصادي والتنمية (OCDE) بأنها كل فعل أو امتناع من شأنه الاعتداء على الأموال المادية والمعنوية يكون ناتجا بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية[2].

كما عرفت المادة (01) من القانون العربي النموذجي الموحد بشأن مكافحة سوء استخدام تكنولوجيا المعلومات والاتصال لسنة 2003 الجرائم الإلكترونية على أنها : " كل فعل مؤثم يتم ارتكابه عبر أي وسيط إلكتروني، وعرفت المادة نفسها الوسيط الإلكتروني على أنه:" شبكة الحاسب الآلي أو الانترنيت أو أي شبكة إلكترونية أخرى[3]، أو هي : " مجموعة المخالفات التي تقع على شبكات الاتصال عموما وعلى شبكة الإنترنت خصوصا.[4]

كما عرفتها الاتفاقية الأوروبية للجرائم السيبرانية (اتفاقية بودابست)، بأنها كافة النشاطات غير القانونية أو غير المشروعة المرتبطة بأجهزة الكمبيوتر وباستخدام الشبكة العنكبوتية، وصنفت هذه الاتفاقية الجرائم المرتكبة إلى عدة فئات منها الجرائم التي ترتكب ضد سلامة المعلومات وخصوصيتها،

---

[1] رشيدة بوكر ، جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري والمقارن، منشورات الحلبي الحقوقية، بيروت، لبنان، 2012، ص 36.

[2] Alain Bensoussan, L'informatique et le droit. Memento Guide. édition Hermes, Paris, France, Tome 1, 1994,p.365.

[3] حنان ريحان مبارك المضحكي، الجرائم المعلوماتية دراسة مقارنة، منشورات الحلبي الحقوقية، بيروت،2014، ص 28

[4] تم إعداد القانون الاسترشادي العربي الموحد بشأن مكافحة سوء استخدام تكنولوجيا المعلومات والاتصال من قبل لجنة مشتركة بين المكتب التنفيذي لمؤتمر وزراء العدل العرب والأمانة العامة لجامعة الدول العربية، وتم إقراره سنة 2003.

والجرائمذات الصلة بالكمبيوتر، والجرائم المتعلقة بمحتوي الكمبيوتر، والجرائم المتعلقة بالعلامات التجارية والملكية الفكرية.[1]

ومن بين هذه التعريفات أيضاً التعريف الذي ورد في الإجابة البلجيكية على الاستبيان الذي أجرته منظمة التعاون الاقتصادي والتنمية عام ١٩٨٢ حول الغش المعلوماتى، بأنها كل فعل أو امتناع من شأنه الاعتداء على الأموال المادية أو المعنوية يكون ناتجاً بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية.[2]

ويعد هذا التعريف الأخير من وجهة نظرنا من أفضل التعريفاتا لتي قيلت في تعريف الجريمة التقنية وأوقعها والتي تمثل تجسيداً حقيقياً للجريمة التقنية على الرغم من اتساعه وشموليته.

وباستقرائنا لمختلف التعريفات نجد أن تعريف منظمة التعاون الاقتصادي والتنمية السابق الذكر يتسم بالوضوح والشمول وذلك للأسباب الآتية:

– تحديد لماهية السلوك الإجرامي للجريمة، إذ شمل كل من الفعل الإيجابي والسلوك السلبي المتمثل في الامتناع.

– اعتماد تعريف واسع يتيح الإحاطة الشاملة قدر الإمكان بظاهرة الجرائم التقنية، وذلك لربطه بين الجريمة وأي تدخل للتقنية المعلوماتية بصفة مباشرة أو غير مباشرة كما تتسم هذه التقنية بالتطور المستمر.

– يعبر عن الطابع التقني المميز الذي تنطوي تحته أبرز صور الجريمة الإلكترونية.

– يتيح إمكانية التعامل مع التطورات المستقبلية في مجال تقنية المعلوماتية ونظم الاتصالات.

الفرع الثالث: تعريف الجريمة الالكترونية في الفقه

مما يلاحظ في هذا الشأن هو عدم وجود اتفاق سواء على المستوى التشريعي أو الفقهي على استعمال مصطلح معين للدلالة على هذا الظاهرة الجرمية الناشئة في بيئة الكمبيوتر والإنترنت، وهو

---

[1] انعقدت الاتفاقية الأوربية لجرائم الانترنت في بودابست بدولة المجر بتاريخ 2001/11/23 وتعتبر هي الأساس الأول للتعاون الدولي في مجال المكافحة الدولية للجريمة المنظمة عبر الانترنت، وقد تم توقيعها من ٣٠ دولة أوروبية بالإضافة إلى أربع دول غير أعضاء في المجلس. الأوروبي وهم كندا، الولايات المتحدة الأمريكية، اليابان، جنوب أفريقيا. للمزيد حول هذه الاتفاقية يراجع: د/ عمر محمد أبو بكر يونس– الجرائم الناشئة عن استخدام الانترنت، الأحكام الموضوعية والجوانب الإجرائية، رسالة دكتوراه، جامعة عين شمس، دار النهضة العربية، القاهرة، 2004، ص.198–200

[2] هشام فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة، أسيوط، 1994، ص30

اختلاف رافق مسيرة نشأة وتطور ظاهرة الإجرام المرتبط بتقنية المعلومات والاتصالات، فهناك من يطلق عليها مصطلح جرائم الغش المعلوماتي، أو الجرائم المعلوماتية، أو الجرائم الإلكترونية، أو جرائم الحاسب الآلي، أو جرائم تقنية المعلومات، أو الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، أو جرائم التكنولوجيا الحديثة أو جرائم الكومبيوتر والإنترنت، ويرجع السبب في ذلك إلى عدة عوامل منها التطور المستمر واللامتناهي لتكنولوجيا المعلومات والاتصالات، مما نتج عنه جرائم مستحدثة اختلفت التشريعات حول وضع مفاهيم موحدة لها.[1] وقد يكون السبب أيضا ترك المجال أمام المشرع لاحتواء التقنيات المتلاحقة في هذا الميدان، ولعدم حصر قاعدة التجريم في نطاق أفعال معينة تتبدل في المستقبل. ويثير هذا الإشكال العديد من التحديات أهمها صعوبة مواجهتها وتعذر الحلول المناسبة لمكافحتها سواء على المستوى الداخلي أو الدولي. ورغم هذه الصعوبات حاول الفقهاء جاهدين وضع مفهوم لهذه الجرائم المستحدثة اين برز اتجاهان هما:

أولاً: الاتجاه الضيق لمفهوم الجرائم الإلكترونية :

حاول هذا الاتجاه حصر مفهوم الجريمة الإلكترونية وربطها بعناصر عديدة كالحاسوب، أو مستخدمه، أو بموضوع الجريمة، حيث عرفها الفقيه ماروي (Merwe) على أنها: "الفعل غير المشروع الذي يستخدم في ارتكابه الحاسب الآلي"[2]

وهناك من عرفها على أنها " فعل غير مشروع تكون المعرفة بتقنية المعلومات أساسية لمرتكبه".[3]

أو هي: "الجريمة التي تقع بواسطة الحاسب الآلي أو عليه أو بواسطة شبكة الانترنيت"[4].

كما عرفت أيضا بأنها: "الجرائم التي تقع على جهاز الكمبيوتر أو داخل نظامه فقط"[5].

أو هي : "مجموعة المخالفات الجزائية التي تقع ضد شبكات الإعلام الآلي"[1].

---

[1]Nidal El Chaer, La Criminalité Informatique Devant La Justice Pénale, édition juridique sader, Beyrouth, Liban, 2004, pp. 18-19.

[2]عبد العال الديربي ومحمد صادق إسماعيل، جرائم الفساد بين آليات المكافحة الوطنية والدولية : دراسة قانونية تطبيقية مقارنة، ط1، المركز القومي للإصدارات القانونية، القاهرة، 2012، ص 40.

[3]فايز الظفيري، الأحكام العامة للجريمة الإلكترونية، مجلة العلوم القانونية والاقتصادية، كلية الحقوق، جامعة عين شمس، مصر،العدد 2، 2002، ص485.

[4]عبد الفتاح بيومي حجازي، نحو صياغة نظرية عامة في علم الجريمة والمجرم المعلوماتي، دار بهجات للطباعة والتجليد، مصر، ط 1 2009 ، ص 19.

[5]خالد ممدوح ابراهيم، الجرائم المعلوماتية، ط1، دار الفكر الجامعي، الإسكندرية ، 2009، ص 74.

وفي تعريف آخر هي:"الأفعال غير القانونية المرتكبة بواسطة العمليات الإلكترونية والتي تمس بالنظام المعلوماتي أو بالمعطيات التي يحتويها ومهما كان الهدف من ذلك"[2].

من جانب آخر عرفها الفقيه روز بلات (Rosblat): كل نشاط غير مشروعموجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومة المخزنة داخل الكمبيوتر أو تلك التي يتم تحويلها عن طريقه"[3].

كما عرفها الفقيه الألماني تادمان (Tiedemann) على أنها : " كل أشكال السلوك غير المشروع الذي يرتكب باستخدام الحاسب"[4].

من جهة أخرى، عرفها مكتب تقييم التقنية فيالولايات المتحدة الأمريكية بأنها : "الجرائم التي تلعب فيها البيانات الكمبيوترية والبرامج المعلوماتية دورا رئيسيا"[5].

وعليه يربط أنصار هذا الاتجاه تعريفهم لهذه الجرائم بضرورة وجود الحاسوب الذي قد يكون أداة للجريمة أو هدفا لها، ناهيك عن وجود معارف مسبقة بتكنولوجيا الكمبيوتر ليس فقط من المجرم المعلوماتي، وإنما أيضا من القائمين على ملاحقة هذا النوع من الجرائم، وهذا يضيق على نحو كبير من الجريمة الإلكترونية التي هي في اتساع يوما بعد يوم تبعا لتطور تكنولوجيا المعلوماتية.

من جهة أخرى، هناك جرائم إلكترونية لا تتطلب هذا القدر كله من المعرفة على اعتبار أن المعلوماتية صارت متاحة للجميع مثل: إرسال رسالة نصية بالهاتف أو بالبريد الإلكتروني، أو نسخ بيانات من حاسوب... إلخ، كما أن حصر الجرائم الإلكترونية في موضوع الجريمة والتي تقع فقط على النظام المعلوماتي فيه تضييق بدوره ويندرج تحته نوع واحد من الجرائم الإلكترونية هي المسماة بجرائم المعالجة الآلية للمعطيات"، إذ يخرج من هذا النطاق جانب كبير من الأفعال غير المشروعة التي يستخدم الحاسب كأداة لارتكابها مثل: جرائم الاحتيال المعلوماتي[6] ، وبالتالي يتسم تعريف هذا الاتجاه للجرائم الإلكترونية بالنقصان، مما أدي الى ظهور اتجاه ثان مخالفله نتناوله فيما يأتي.

ثانياً : الاتجاه الموسع لمفهوم الجرائم الإلكترونية:

---

[1]Redouane Semlali, art-Cit,p.40, voir aussi. Frédérique Chopin, Les politiques publiques de lutte contre la cybercriminalité. Actualité Juridique Pénal, Editions Dalloz, 2009, p101

[2]Nidal El Chaer, Op. Cit.p.20

[3]عبد العال الديربي ومحمد صادق إسماعيل، المرجع السابق، ص 40.

[4]المرجع نفسه، ص 41.

[5]أحمد خليفة الملط، الجرائم المعلوماتية : دراسة مقارنة، دار الفكر الجامعى،الإسكندرية، 2005، ص 84.

[6]نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية، منشورات الحلبي الحقوقية، بيروت، لبنان، ط1، 2005، ص 30

على عكس الاتجاه السابق، يذهب فريق من الفقهاء إلى التوسع في مفهوم الجرائم الإلكترونية أو المعلوماتية وعدم حصرها في الحاسوب وحده أو في موضوع الجريمة أو في شخص مستخدمه، وإنما بالتقنية ذاتها المستخدمة في كافة الأجهزة المعلوماتية أو الإلكترونية، فيعرفونها على أنها " كل فعل إجرامي أو متعمد أيا كانت صلته بالمعلوماتية، ينشأ عنه خسارة بالمجني عليه، أو كسبا يحققه الفاعل"[1].

كما تعرف أيضا على أنها:"تلك الجرائم المرتكبة ضد الأملاك باستعمال التقنية المعلوماتية".[2]

إن هذه التعريفات واسعة تتيح الإحاطة الشاملة قدر الإمكان بظاهرة جرائم التقنية، كما أنها تعبر عن الطابع التقني أو المميز الذي تنطوي تحته أبرز صورها، كما أنه يتيح إمكانية التعامل مع التطورات التقنية المستقبلية، ويعرفها آخرون على أنها:"كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات أو بنقلها".[3]إذ يعتمد هذا التعريف على معيارين : أولهما وصف السلوك، وثانيهما اتصال السلوك بالمعالجة الآلية للبيانات أو نقلها، كما يجمع الفقه الفرنسي بصفة عامة على القول بأن فكرة الغش المعلوماتي (Fraude Informatique) التي تعادل جرائم الحاسب الآلي تشمل العديد من الأفعال المتنوعة.

حيث عرف كل من الفقيه ميشال (Michel) والفقيه ريدو (Redo) الجريمة المعلوماتية بأنها:"سوء استخدام الحاسب ويشمل الحالات المتعلقة بالولوج غير المصرح به الحاسب المجني عليه أو بياناته، وكذا الاستخدام غير المشروع البطاقات الائتمان وانتهاك ماكينات الحاسب الآلية بما تتضمنه من شبكات تحويل الحسابات المالية بطرق إلكترونية وتزييف المكونات المادية والمعنوية للحاسب وسرقة الحاسب الآلي في حد ذاته أو أي مكون من مكوناته"[4].

وبذلك تمثل هذه التعاريف المفهوم الموسع للجرائم الإلكترونية، والتي تتم بالحاسوب سواء كان هدفا لها أو وسيلة لارتكابها، أو عن طريق شبكة الإنترنت أو بأي وسيلة إلكترونية أخرى تظهر مستقبلا كوسائل الاتصال الحديثة مثل الهاتف النقال وجهاز الفاكس وغيرها.

مما لا شك فيه أن هذا الاتجاه ينطوي على توسع كبير لمفهوم الجرائم الالكترونية، فهي كل جريمة تتم بمساعدة الحاسوب أو في محيطه، أو عن طريق شبكة الإنترنت أو أجهزة الاتصال الحديثة. وبناء على التعريفات السابقة تتخذ الجريمة الإلكترونية صور عديدة، تتمثل في استخدام الحاسوب كوسيلة

---

[1] حنان ريحان مبارك المضحكي، المرجع السابق، ص 26

[2]أحمد خليفة الملط، المرجع السابق، ص 87.

[3] نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية، منشورات الحلبي الحقوقية ، بيروت، 2004، ص 30.

[4]Myriam Quéméner et Yves Charpenel, Op. Cit.p.8

لارتكاب الجرائم أو الاعتداء على الحاسوب نفسه ونظامه أو استخدام أي وسيلة إلكترونية أخرى توفرها التقنيات الحديثة، بمعنى آخر فإن الجرائم الإلكترونية تزاوج بين تقنية الحوسبة وتقنية الاتصالات الحديثة، فإذا عدنا للحقيقة الأولى المتصلة بولادة وتطور تقنية المعلومات نجد أن تقنية المعلومات تشمل فرعين جرى بحكم التطور تقاربهما واندماجهما، فرع الحوسبة وفرع الاتصال أما الحوسبة فتقوم على استخدام وسائل التقنية الإدارة وتنظيم ومعالجة البيانات في إطار تنفيذ مهام محددة تتصل بعلمي الحساب والمنطق، أما الاتصال فهو قائم على وسائل تقنية لنقل المعلومات بجميع دلالاتها، هذه الدلالات يحددها الأستاذ زياينغ إكزيوو (Zhange Yuexiao) (بالرسائل والأخبار والبيانات والمعرفة والوثائق والأدب والفكر والرموز والعلامات والإرشادات الخفية والأنباء المفيدة والسرية وغير ذلك)[1].

ونستخلص مما سبق أن اختلاف الفقه في وضع تعريف للجريمة المعلوماتية أو الإلكترونية مرده الاختلاف في المعيار المعتمد عليه والزاوية التي ينظر إليها كل اتجاه إلى هاته الجريمة المستحدثة، إلا أنه يمكن إعطاء تعريف ملخص تبعا لهذه الاتجاهات فهي سلوك غير مشروع معاقب عليه قانونا صادر عن إرادة جرمية محله معطيات الكمبيوتر " فالسلوك يشمل الفعل الإيجابي والامتناع عن الفعل، وهذا السلوك غير مشروع باعتبار المشروعية تنفي عن الفعل الصفة الجرمية ومعاقب عليه قانونا

إذ أن إسباغ الصفة الإجرامية لا يتحقق في ميدان القانون الجنائي إلا بإرادة المشرع ومن خلال النص على ذلك، ومحل جريمة الكمبيوتر هو دائما معطيات الكمبيوتر بدلالتها الواسعة بيانات مدخلة، بيانات ومعلومات معالجة ومخزنة ، البرامج بأنواعها المعلومات المستخرجة ، والمتبادلة بين الأنظمة المعلوماتية ... إلخ).

وأما الكمبيوتر فهو النظام التقني بمفهومه الشامل الذي يزاوج بين تقنيات الحوسبة والاتصال بما في ذلك شبكات المعلومات[2].

وعلى هذا الأساس فإن محاولة إعطاء تعريف لهذا النوع من الجرائم المستحدثة الذي يتم في بيئة افتراضية يجب أن يراعى فيه عدة اعتبارات منها:

1. يجب أن يتلاءم هذا التعريف مع فكرة عالمية المعلومات والاتصالات وأن يكون واضحا عالميا.

[1] يونس عرب صور الجرائم الإلكترونية واتجاهات تبويبها، ورقة عمل مقدمة ضمن ورشة عمل تطوير التشريعات في مجال مكافحة الجرائم الإلكترونية، هيئة تنظيم الاتصالات، مسقط، سلطة عمان يومي 2 و 4 أفريل، 2006 ، ص 7

[2] يونس عرب جرائم الكمبيوتر، المرجع السابق، ص ص 1-2

2. يجب مراعاة التطورات المتلاحقة في عالم الحوسبة والاتصال ويسمح باستيعاب كل ما يستجد من صور للجرائم الإلكترونية.

3. يجب توضيح خصوصية الجرائم الإلكترونية لما تحتويه على أشكال مختلفة للسلوك الإجرامي بحيث يظهرا جليا دور الحاسوب في ارتكاب هذه الجرائم.

المطلب الثاني

خصائص الجريمة الالكترونية ودوافع ارتكابها

تتميز الجريمة الالكترونية بخصائصها الفريدة مثل الخفاء والقدرة على التنفيذ عبر الحدود، وتتنوع دوافع ارتكابها حسب مرتكبها وعلى هذا تطرقنا في هذا المطلب إلى خصوصية الجرائم الإلكترونية في الفرع الأول وسمات مرتكبيها في الفرع الثاني ثم دوافع ارتكابها في الفرع الثالث.

الفرع الأول: خصائص الجرائم الإلكترونية

للجرائم الإلكترونية مجموعة من الخصائص التي تميزها عن غيرها من الجرائم التقليدية نلخصها فيما يلي:

أولا: عدم وضوح الجرائم المعلوماتية

تتسم الجرائم الناشئة عن استخدام الانترنت بأنها خفية ومستترة في أغلبها، لأن الضحية لا يلاحظها رغم أنها قد تقع أثناء وجوده على الشبكة، لأن الجاني يتمتع بقد ارت فنية تمكنه من جريمته بدقة مثلا عند إرسال الفيروسات وسرقة الأموال والبيانات الخاصة أو إتلافها، والتجسس وسرقة المكالمات وغيرها من الجرائم. كما أن وسيلة تنفيذها التي تميز في أغلب الأحيان بالطابع التقني الذي يضفي عليها الكثير من التعقيد بالإضافة إلى الأحجام عن الإبلاغ عنها في حالة اكتشافها لخشية المجني عليهم في فقدان عملائهم فضلا عن إمكانية تدمير المعلومات التي يمكن أن تستخدم كدليل الإثبات في مدة تقل عن الثانية الواحدة.[1]

حيث أن المجني يلعب دورا رئيسيا في صعوبة اكتشاف وقوع الجريمة المعلوماتية إذ تحرض أكثر الجهات التي تتعرض أنظمتها المعلوماتية لانتهاك أو تمنى بخسائر فادحة من جراء ذلك على عدم الكشف حتى بن موظفيها عما تعرض له وتكتفي عادة بإجراءات داخلية

إدارية دون الإبلاغ عنها السلطات المختصة تجنبا للأضرار أو بسمعتها ومكانتها وهو الثقةفي كفاءتها.[2]

[1] نهلا عبد القادر المومني، الجرائم المعلوماتية، ط2، دار الثقافة، الأردن،2017، ص 54.

[2] نهلا عبد القادر المومني، المرجع السابق، ص 56.

ثانيا : صعوبة إثبات الجرائم الإلكترونية

تتميز الجرائم الإلكترونية بصعوبة إكتشافها، لأنها تتم في بيئة غير تقليدية حيث تقع خارج إطار الواقع المادي الملموس لتقوم أركانها في بيئة الحاسوب والإنترنت مما يجعل الأمور تزداد تعقيدا لدى سلطات الأمن وأجهزة التحقيق والملاحقة.[1]

أما إذا اكتشفت وهي حالات قليلة مقارنة بما تم اكتشافه من الجرائم التقليدية فيكون ذلك بمحض الصدفة، وقد ترجع الأسباب التي تقف وراء الصعوبة في اكتشاف هذا النوع من الإجرام إلى عدم ترك هذه الجريمة لأي أثر خارجي بصورة مرئية.

كما أن الجاني يملك القدرة على تدمير دليل إدانته في أقل من ثانية مما يشكل عاملا إضافيا في صعوبة إكتشاف هذا النوع من الجرائم الذي تصل أدلة الإدانة فيها إلى حدود 20%.[2] ونظرا لما تتطلبه هذه الجرائم من تقنية لارتكابها فهي تتطلبه لاكتشافها والبحث عنها، وتستلزم أسلوب خاص في التحقيق والتعامل، الأمر الذي لم يتحقق في الجهات الأمنية والقضائية لدينا، نظرا لنقص المعارف التقية وهو ما يتطلب تخصص في التقنية لتحصين الجهاز الأمني والقضائي الذي يسعى للقضاء على هذه الظاهرة. كما أن القوانين التقليدية لم تعد قادرة على مواكبة السرعة الهائلة في التكنولوجيا والتي أدت إلى تطور الجريمة من خلالها، وظهور جرائم لم تكن موجودة في السابق، وباتت القوانين التقليدية القائمة عاجزة عن مواجهتها[3]. ما يشكل عائقا أساسيا أمام إثبات الجريمة المعلوماتية.

ثالثا : الأساليب المستخدمة في ارتكاب الجرائم الإلكترونية

إن الجرائم المعلوماتية تبرز ذاتيتها بصورة أكثر وضوحا في أسلوب ارتكابها وطريقتها فإذا كانت الجريمة التقليدية تتطلب نوعا من الأسلوب العضلي الذي قد يكون في صورة أوفي صورة الخلع أو الكسر وتقليد المفاتيح كما هو حال جريمة السرقة.[4]

---

[1] محمد عبيد الكعبي، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الإنترنت : دراسة مقارنة، دار النهضة العربية،القاهرة، 2009 ، ص4

[2] حسين صالح دويب القوانين العربية وتشريعات تجريم الجرائم الإلكترونية وحماية المجتمع المؤتمر السادس الجمعية المكتبات والمعلومات السعودية، 06 أفريل 2010.

[3] طارق الشدي، مرجع سابق، ص 55

[4] ذباب البدايئة، جرائم الحاسب والأنترنت، أبحاث الندوة العلمية لدراسة الظواهر الإجرامية المستحدثة وسبل مواجهتها، أكادمية نايف العربية للعلوم الأمنية 2009، ص 111 .

وتحتاج كذلك إلى وجود شبكة المعلومات الدولية الإنترنت مع وجود مجرم يوظف خبرته وقدراته على التعامل مع الشبكة للقيام بجرائم مختلفة كالتجسس أو اختراق خصوصيات الغير للتغرير بالقاصرين كل ذلك دون الحاجة لسفك الدماء.

رابعا: ضخامة الخسائر المادية والمعنوية

الجرائم الحاسب الآلي خسائر جسيمة على المستوى الإقتصادي[1]، سواء كانت بسرقة البرامج أو محوها، أو تدمير قاعدة البيانات، أو اختلاس مبالغ مالية من بعض الحسابات حيث تصل أحيانا الخسائر إلى ملايير الدولارات.

خامسا: التلوث الثقافي

إن جرائم الكمبيوتر لا تصيب الأثر المادي فحسب بل يتعدى ذلك ليهدد نظام القيم والأخلاق، خاصة في المجتمعات المحافظة، فنشر المواد الإباحية وغير الأخلاقية في بعض المجتمعات من شأنها أن تؤدي إلى هدم القيم والتلويث في هذه المجتمعات، كما قد يؤدي إلى التفسخ الاجتماعي الذي يؤثر سلبا على المجتمعات الإسلامية.[2]

سادسا : خاصية اشتراك الأشخاص في الإجرام الإلكتروني

تتميز الجريمة المعلوماتية عادة أنها تتم بتعاون أكثر من شخص على ارتكابها إضرار بالجهة المجني عليها، وغالب ما يشترك في إخراج الجريمة المعلوماتية إلى حيز الوجود شخص متخصص في تقنيات الحاسوب والإنترنت يقوم بالجانب الفني من المشروع الإجرامي وشخص آخر من المحيط أو من خارج المؤسسة المجني عليها لتغطية عملية التلاعب وتحويل المكاسب إليه.

والاشتراك أيضا في إخراج الجريمة المعلوماتية إلى حيز الوجود قد يكون إشراكا سلبيا وهو الذي يترجم بصمت من جانب من يعلم بوقوع الجريمة في محاولة منه لتسهيلها وإتمامها، وقد يكون اشتراكا إيجابيا وهو غالبا كذلك ما يتمثل في مساعدة فنية ومادية.

سابعا: الجريمة المعلوماتية جريمة عابرة للحدود

بعد ظهور شبكات المعلومات لم يعد هناك كحدود مرئية أو ملموسة تقف أمام نقل المعلومات عبر الدول المختلفة، فالمقدرة التي تتمتع بها الحواسيب وشبكاتها في نقل كميات كبيرة من المعلومات وتبادلها

[1] ذباب البدايئة، المرجع السابق، ص 112

[2] المرجع نفسه، ص 111

بين أنظمة يفصل بينها آلاف الأميال قد أدت إلى نتيجة مؤداها أن أماكن متعددة في دول مختلفة قد تتأثر بالجريمة المعلوماتية الواحدة في آن واحد[1].

والسهولة في حركة المعلومات عبر أنظمة التقنية الحديثة أيضا مما جعل بالإمكان ارتكاب جريمة عن طريق حاسوب موجود في دولة معينة بينما يتحقق الفعل الإجرامي في دولة أخرى هذه الطبيعة تتميز بها الجريمة المعلوماتية كونها جريمة عابرة الحدود خلقت العديد من المشاكل حول تحديد الدولة صاحبة اختصاص القضائي بهذه الجريمة[2].

فهل هي الدولة التي وقع بها النشاط الإجرامي، أم تلك التي أضرت مصالحها نتيجة لهذا التلاعب، كما أثارت الطبيعة أيضا الشكوك حول مدى فعالية القوانين القائمة في التعامل مع الجريمة المعلوماتية وبصفة خاصة فيما يتعلق بجمع وقبول الأدلة[3]. الحقيقة أن عملية التباعد الجغرافي بين الفعل وتحقيق النتيجة من أكثر الوسائل التي تثير الإشكالات في مجال الحاسوب، وبشكل خاص الإجراءات الجنائية والاختصاص والقانون والواجب الجرائم، ولعل هذه السمة تذكرنا بإرهاصات جرم المخدرات والاتجار بالرقيق وغيرها من الجرائم التي وقف تباين الدول واختلاف مستويات الحماية الجنائية فيها حائلا دون نجاعة أساليب مكافحتها، فلم يكن من يد غير الدخول في سلسلة اتفاقيات ومعاهدات دولية لمكافحتها[4].

وهكذا فإن جرائم الكمبيوتر في نطاق الظاهرة الاجرامية المستحدثة والتي لم تعد كذلكبالنظر إلى أول حالة موثقة للجريمة الإلكترونية والتي تعود لعام 1959 وبالنظر لنحو 36 عاما من التعايش الدولي مع صور مختلفة ومتغايرة من هذ الجرائم كالجرائم التي تنصب على معطيات الحاسوب بيانات ومعلومات وبرامج وتطال الحق في المعلومات، ويستخدم لاقترافها وسائل تقنية تقتضي استخدام الحاسوب بوصفه نظاما حقق التزاوج بين تقنياتالحوسبة والاتصالات.

جرائم الكمبيوتر والانترنت طائفة من الجرائم التي تتسم بسمات مخصوصة عن غيرها من الجرائم، فهي تستهدف معنويات وليست ماديات محسوسة ، وتثير في هذا النطاق مشكلات الاعتراف بحماية المال المعلوماتي إن جاز التعبير .

---

[1] نهلا عبد القادر المومني، الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، الطبعة الثانية، 2001، ص 59.

[2] Mascala corinne, Travaux de l'association «criminalité et contrat électronique», journées national Henir CAPITANT, paris, 2000, P119

[3] نائلة عادل فريد قورة ، جرائم الحاسب الاقتصادية، دراسة نظرية تطبيقية، دار النهضة العربية الإسكندرية، 2004، ص 54.

[4] جعفر حسن حاسم الطالبي، جرائم تكنولوجيا المعلومات، رواية جديدة للحريقة المعلوماتية، دار البداية، عمان، 2007، ص 92.

كما أنها تتسم بالخطورة البالغة نظرا لأغراضها المتعددة، ولحجم الخسائر الناجم عنها قياسا بالجرائم التقليدية، ولارتكابها من بين فئات متعددة تجعل من التنبؤ بالمشتبه بهم أمرا صعبا. إضافة لكونها تنطوي بذاتها على سلوكيات غير مألوفة، وبما أتاحته من تسهيل ارتكاب الجرائم الأخرى تمثل إيجاد وسائل تجعل ملاحقة الجرائم التقليدية أمرا صعبا متى ما ارتكبت باستخدام الكمبيوتر.

وتحقيق وتحري جرائم الكمبيوتر والانترنت والمقاضاة في نطاقها تنطوي على مشكلات وتحديات إدارية وقانونية تتصل ابتداء بمعيقات ومتطلبات عمليات ملاحقة الجناة، فان

الفرع الثاني: السمات الخاصة بالمجرم المعلوماتي

تتطلب الجريمة المعلوماتية مقدرة عقلية وذهنية خاصة لدى الجاني حيث أن الاعتداءات المرتكبة لا تتطلب إجراءات تميل إلى العنف بقدر ما تتطلب الماما بقدر معين من المعرفة، فهو مجرم ذو كفاءة عالية في مجال التقنية يحتاج إلى جهاز حاسوب موصول بشبكة الإنترنت إلى جانب درايته بمختلف الأنظمة المستعملة في هذا المجال ويمكن حصر هذه السمات على النحو التالي:

أولا: المهارة والخبرة المكتسبة لتنفيذ الفعل الإجرامي:

تعني المهارة والخبرة على التعرف بكافة الظروف التي تحيط بالجريمة المراد تنفيذها، وإمكانيات نجاحها، واحتمالات فشلها، فالجناة عادة يمهدون لارتكاب جرائهم بالتعرف على كافة الظروف المحيطة بهم، لتجنب الأمور غير المتوقعة التي من شأنها ضبط أفعالهم والكشف عنهم، وتميز المعرفة بمفهومها السابق مجرمي الانترنت، حيث يستطيع مجرم الانترنت أن يكون تصورا كاملا لجريمته.[1]

يتمتع مجرمي الانترنت بقدر لا يستهان به من المهارة بتقنيات الحاسوب والإنترنت، بل إن بعض مرتكبي هذه الجرائم هم من المتخصصين في مجال معالجة المعلومات آليا، فتنفيذ جريمة الإنترنت يتطلب قدار من المهارة لدى الفاعل التي قد يكتسبها المجال أو عن طريق الخبرة المكتسبة في مجال تكنولوجيا المعلومات.[2]

ان إجرام الإنترنت هو إجرام الأذكياء بالمقارنة بالإجرام التقليدي الذي يميل إلى العنف، فمجرم الإنترنت يسعى بشغف إلى المعرفة طرق جديدة مبتكرة لا يعرفها أحد سواه وذلك من أجل اختراق الحواجز الأمنية في البيئة الالكترونية ثم نيل مبتغاه.

---

[1] طارق إبراهيم الدسوقي عطية الأمن المعلوماتي النظام القانوني لحماية المعلوماتية، دار الجامعة الجديدة للنشر، الإسكندرية ، 2009 ، ص 176-177

[2] Mascala courinne, « criminalité et contrat électronique», Op.cit. p118

ثانيا : مجرم الانترنت يبرر ارتكاب جرائمه

يوجد شعور لدى مرتكب فعل إجرام الانترنت أن ما يقوم به لا يدخل في عداد الج ا رئم أو بمعنى آخر لا يمكن لهذا الفعل أن يتصف بعدم الأخلاقية وخاصة في الحالات التي يقف فيها السلوك عند قهر نظام الكمبيوتر وتخطي الحماية المفروضة حوله، حيث يفرق مرتكبو هذه الجرائم بين الإضرار بالأشخاص، الأمر الذي يعدونه غاية في اللاأخلاقية وبين الإضرار بمؤسسة أو جهة في استطاعتها اقتصاديا تحمل نتائج تلاعبهم.

إذ أن هؤلاء الأشخاص لا يدركون أن سلوكهم يستحق العقاب ويبدو أن الاستخدام المتزايد للأنظمة المعلوماتية، قد أنشأ مناخا نفسيا ملائما لتصور استبعاد فكرة الخير والشر، مما ساعد على عدم وجود احتكاك مباشر بالأشخاص ومما لا شك فيه أن هذا التباعد في العلاقة الثنائية بين الفاعل والمجني عليه يسهل المرور إلى الفعل غير المشروع ويساعد على لإيجاد نوع من الإقرار الشرعي الذاتي بمشروعية هذا الفعل.[1]

ثالثا : الإرتباك والخوف من كشف الجريمة

يتصف المجرمون عبر الانترنت بالخوف من كشف الجرائم المختلفة التي يرتكبونها وكذا افتضاح أمرهم، وبالرغم من هذا الخوف الذي يصاحب المجرمين على اختلاف أنماطهم، إلا أنها تميز مجرمي الانترنت بصفة خاصة، لما يترتب على كشف أمرهم من ارتباك مالي وفقد المركز الوظيفي في كثير من الأحيان.[2]

كما تساعد طبيعة الأنظمة المعلوماتية نفسها مجرمي الانترنت على الحفاظ على سرية أفعالهم، ذلك أن الكثير ما يعرض المجرم إلى اكتشاف أمره هو أن تحدث أمور أثناء تنفيذه لجريمته غير متوقعة لا يمكن التنبؤ بها، في حين أن أهم الأسباب التي تساعد على نجاح الجريمة المرتكبة عبر الانترنت هي آلات الحواسيب التي تؤدي عملها غالبا بطريقة آلية بحيث لا تتغير المراحل المختلفة التي تمر بها أي من العمليات التي يقوم بها من مرة إلى أخرى.

رابعا : الميل إلى تقليد المهارات في ارتكاب الجرائم

يبلغ الميل إلى التقليد أقصاه حينما يوجد الفرد وسط الجماعة، إذ يكون عندئذ أسهل وأسرع انسياقا لتأثير الغير عليه، ويظهر ذلك في مجال الجريمة المرتكبة عبر الانترنت، لأن أغلب الجرائم تتم من

[1] نهلا عبد القادر المومني، المرجع السابق، ص 55 .

[2] نفس المرجع، ص 79

خلال محاولة الفرد تقليد غيره بالمهارات الفنية مما يؤدي به الأمر إلى ارتكاب الجرائم . ولا شك أن ذلك نتيجة لعدم الاستواء في شخصية الفرد الذي يتأثر بخاصية

الميل إلى التقليد بسبب عدم وجود ضوابط أخلاقية يؤصلها الفرد في ذاته مما يحجم لديه غريزة التفاعل مع الوسط المحيط به، فينتهي به الأمر إلى التقليد وارتكاب الجريمة.[1]

خامسا : التخطيط والتنظيم

في عالم الشبكات الالكترونية وخاصة شبكة العالمية للأنترنت، كما هو الحال في العالم الحقيقي يقوم بمعظم الأعمال الإجرامية أفراد أو مجموعات صغيرة، حيث ترتكب أغلب الجرائم من مجموعة مكونة من عدة أشخاص يحدد لكل شخص دور معين ويتم العمل بينهم وفقا لتخطيط وتنظيم سابق على ارتكاب الجريمة، فغالبا ما يكون متضمنا فيها متخصص في الحاسبات يقوم بالجانب الفني من المشروع الإجرامي وشخص آخر من المحيط أو من خارج المؤسسة المجني عليها لتغطية التلاعب ولتحويل المكاسب إليه، كما أن من عادة من يمارسون التلصص والقرصنة على الحاسبات وشبكات المعلومات بصفة منتظمة حول أنشطن هم عقد المؤتمرات.[2]

سادسا : التكيف الاجتماعي

تعتبر هذه الخاصية امتدادا لسمة التخطيط والتنظيم، حيث أن التكيف الاجتماعي ينشأ بين مجموعة لها صفات مشتركة فمثلا جماعة صغار نوابغ المعلوماتية لا شك أنهم يتكيفون في أفكارهم فيما بينهم، وتنشأ بالتالي بينهم صفات وروابط تساعدهم على ارتكاب جرائمهم وتتعدى تلك الروابط والصلات النطاق المحلي بحيث تنشأ بينهم روابط دولية تتفق مع أفكارهم ومنهجهم في استثمار تلك المعرفة والتقدم العلمي، ولاشك أن إقامة تلك المؤتمرات الدولية في هؤلاء المجموعات خير دليل على وجود تلك الصلات والروابط الدولية بينها.[3]

بالإضافة إلى أن مجرمي الإنترنت هم عادة أناس اجتماعيون قادرين على التكيف في بيئتهم الاجتماعية، ولا يضعون أنفسهم في حالة عداء مع المجتمع الذي يحيط بهم، بل قادرين على التوافق والتصالح مع مجتمعهم باعتبارهم أناس مرتفعو الذكاء، بل أن خطورتهم الإجرامية قد تزداد إذا تمت زيادات تكيفهم الاجتماعي مع توافر الشخصية والدوافع الإجرامية لديهم.

---

[1] أيمن عبد الحفيظ الاتجاهات الفنية والأمنية لمواجهة الجرائم المعلوماتية، دون ذكر دار النشر، دون ذكر بلد النشر، ص 34

[2] هشام محمد فريد رستم، المرجع السابق، ص 436

[3] أيمن عبد الحفيظ، المرجع السابق، ص 16

سابعا : سلطة الشفرة التي يتميز بها المجرم المعلوماتي

وهي التي تمكنه من ارتكاب جريمته فقد تتمثل هذه السلطة في الشفرة الخاصة بالدخول إلى النظام الذي يحتوي على المعلومات والتي تعطي الفاعل مزايا متعددة كفتح الملفات وتعديل أو محو المعلومات التي تحتويها أو مجرد قراءتها أو كتابتها وقد تتمثل هذه السلطة في الحق في استعمال الكمبيوتر أو إجراء بعض التعاملات. وقد تكون هذه السلطة غير حقيقية كما في حالة استخدام شفرة الدخول الخاصة بشخص آخر.

ثامنا : الهدف من ارتكاب الجريمة

قد لا تختلف في الكثير من الأحيان عن الهدف من ارتكاب غيرها من الجرائم الأخرى، فالرغبة في تحقيق الربح المادي، وبطريق غير مشروع، يظل الهدف الأول من ارتكاب الجرائم الإلكترونية ، ثم يأتي بعد ذلك مجرد الرغبة في قهر نظام الكمبيوتر، وتخطي حواجز الحماية الدائرة حوله وأخيرا الانتقام في كثير من الأحيان من رب المسؤول في العمل أو من أحد الزملاء.

تاسعا : التطور في السلوك الإجرامي

يساهم وجود المجرم في الانترنت في جماعة إجرامية إلى التأثير في قدرته العقلية وسرعة اكتسابه المهارة التقنية التي تؤدي به إلى التمرد الذاتي على محدودية الدور الذي يقوم به في تنفيذ الجريمة إلى أعلى معدلات المهارة التقنية المتمثلة في اثبات قدرته على إرتكاب الجريمة.

الفرع الثالث: دوافع ارتكاب الجريمة الالكترونية

الدافع (الباعث)، الغرض، الغاية، تعبيرات لكل منها دلالته الاصطلاحية في القانون الجنائي، وتتصل بما يعرف بالقصد الخاص في الجريمة. هذه المسألة تثير جدلاً فقهياً وقضائياً واسعاً، ذلك أن القاعدة القضائية تقرر أن الباعث ليس من عناصر القصد الجرمي[1]، وأن الباعث لا أثر له في وجود القصد الجنائي[2]. وعلى الرغم من أن الاستخدام العادي للتعبيرات المشار إليها يجري على أساس ترادفها في الغالب، فإنها من حيث الدلالة تتمايز وينتج عن تمايزها آثار قانونية ذات أهمية كبيرة.

[1] محمود نجيب حسني، شرح قانون العقوبات / القسم العام، الطبعة السادسة، دار النهضة العربية، القاهرة، ص152.

[2] أحمد فتحي سرور، الوسيط في قانون العقوبات / القسم العام، الطبعة الخامسة دار النهضة العربية،القاهرة،1991 ص 427.

الباعث (الدافع) هو العامل المحرّك للإرادة الذي يوجه السلوك الإجرامي، كالمحبة، والشفقة، والبغضاء، والانتقام[1]. يُعتبر الباعث قوة نفسية تدفع الإرادة نحو ارتكاب الجريمة بغية تحقيق غاية معينة، وهو يختلف من جريمة إلى أخرى تبعاً لاختلاف الناس من حيث السن والجنس ودرجة التعليم وغيرها من المؤثرات، كما يختلف بالنسبة للجريمة الواحدة من شخص لآخر.[2]

أما الغرض، فهو الهدف الفوري المباشر للسلوك الإجرامي، ويتمثل في تحقيق النتيجة التي انصرف إليها القصد الجنائي أو الاعتداء على الحق الذي يحميه قانون العقوبات[3]. وأما الغاية، فهي الهدف البعيد الذي يرمي إليه الجاني بارتكاب الجريمة، كإشباع شهوة الانتقام أو سلب مال المجني عليه في جريمة القتل.

الأصل أن الباعث والغاية ليس لهما أثر قانوني في وجود القصد الجنائي الذي يقوم على عنصرين: علم الجاني بعناصر الجريمة، واتجاه إرادته إلى تحقيق هذه العناصر أو قبولها. ولا تأثير للباعث أو الغاية على قيام الجريمة أو العقاب عليها، فالجريمة تتحقق بتوافر عناصرها، سواء كان الباعث نبيلاً أو رذيلاً، وسواء كانت الغاية شريفة أو دنيئة. وإذا كانت القاعدة أن الباعث أو الغاية لا أثر لهما على قيام الجريمة، فإن القانون يسبغ عليهما في بعض الأحيان أهمية قانونية خاصة.

أولا: السعي لتحقيق الكسب المالي

يعد هذا الدافع، والذي يمثل في الحقيقة غاية الفاعل، من بين أكثر الدوافع تحفيزاً للجناة لارتكاب الجرائم الإلكترونية. خصائص هذه الجرائم، وحجم الربح الكبير الممكن تحقيقه من بعضها، خاصة غش الحاسوب أو الاحتيال المرتبط بالحاسوب، تعزز من هذا الدافع.

منذ بدايات ظاهرة الجرائم الإلكترونية، أشارت الدراسات إلى أن المحرك الرئيسي لأنشطة احتيال الكمبيوتر، ومن ثم احتيال الإنترنت، هو تحقيق الكسب المالي. ففي دراسة قديمة أشار إليها الفقيه Pctket، يظهر أن 65% من حالات الغش المرتبط بالحاسوب المُعلَن عنها كانت تهدف لاختلاس

[1] كامل السعيد، شرح الأحكام العامة في قانون العقوبات الأردني والقانون المقارن، الطبعة الثانية، دار الفكرللنشر والتوزيع ، عمان، 1983، ص226.

[2] كامل السعيد ، نفس المرجع، ص227.

[3] محمود نجيب حسني، مرجع سابق، ص480.

المال، وهي النسبة الأعلى مقارنة بجرائم أخرى تم استعراضها في هذه الدراسة (32% سرقة معلومات، 19% أفعال إتلاف، 15% سرقة وقت الحاسوب لأغراض شخصية).[1]

أما في الدراسات الحديثة، فإن هذا الدافع يظل مسيطراً ويعكس استمرار اتجاه مجرمي التقنية إلى السعي لتحقيق مكاسب مادية شخصية. ومن بين أهم هذه الدراسات المسحية والتقارير الإحصائية، تأتي الدراسات والتقارير الصادرة عن مركز احتيال المعلومات الوطني في الولايات المتحدة الأمريكية (PHKE).

ثانياً: الانتقام من رب العمل وإلحاق الضرر به

لقد لوحظ أن العاملين في قطاع التقنية أو المستخدمين لها في قطاعات العمل الأخرى، يتعرضون لضغوط نفسية ناجمة عن ضغط العمل والمشكلات المالية وطبيعة علاقات العمل المنفرة في حالات معينة. هذه الأمور قد تدفعهم إلى النزعة نحو تحقيق الربح، كما ذكرنا سابقاً، لكنها في حالات كثيرة تمثل دافعاً لبعض العاملين لارتكاب جرائم الحاسوب بهدف الانتقام من المنشأة أو رب العمل. وربما تكون أنشطة زرع الفيروسات في نظم الكمبيوتر النشاط الرئيسي والتقنية الأكثر شيوعاً لهذه الفئة التي تملك الأحقاد على رب العمل كدافع رئيسي لارتكاب الجريمة.

ثالثاً: الرغبة في قهر النظام والتفوق على تعقيد وسائل التقنية

يرى البعض أن الدافع إلى ارتكاب الجرائم في الطائفة الأولى (جرائم الحاسوب) يغلب عليه الرغبة في قهر النظام أكثر من شهوة الحصول على الربح. وعلى الرغم من أن الدراسات لا تظهر هذه الحقيقة بشكل مطلق، حيث يظل السعي لتحقيق الربح دافعاً أكثر تحريكاً لجرائم الحاسوب من الرغبة في قهر النظام، إلا أن الدافع الأخير يتجسد في نسبة معتبرة من جرائم الحاسوب، خاصة ما يعرف بأنشطة المتطفلين أو الدخلاء (hackers)، والمتجسدة في جرائم التوصل مع أنظمة الحاسب عن بعد، والاستخدام غير المصرح به لنظام الحاسوب، واختراق مواقع الإنترنت.[2]

يميل مرتكبو هذه الجرائم إلى إظهار تفوقهم ومستوى براعتهم، لدرجة أنه مع ظهور أية تقنية مستحدثة، يسعون إلى إيجاد الوسيلة لتحطيمها (أو التفوق عليها بشكل أصوب). ويتزايد شيوع هذا الدافع لدى فئة صغار السن من مرتكبي جرائم الحاسوب، الذين يمضون وقتاً طويلاً أمام حواسيبهم الشخصية

[1] جميل عبد الباقي الصغير، القانون الجنائي والتكنولوجيا الحديثة،الكتاب الأول، الجرائم الناشئة عن استخدام الحاسب الآلي، الطبعة الأولى، منشورات دار النهضة العربية، القاهرة، 1992،ص16.

[2] حسب ترجمة غرفة التجارة العربية البريطانية، والحاذق المأجور حسب ترجمة أستاذنا كامل السعيد

في محاولة لكسر حواجز الأمن لأنظمة الحواسيب وشبكات المعلومات، لإظهار تفوقهم على وسائل التقنية. وقد تناولنا أمثلة عديدة من هذه الحالات الواقعية فيما سبق، ونكتفي بالقول هنا، إن هذا الدافع هو أكثر الدوافع التي يجري استغلالها من قبل المنظمات الجرمية (مجموعات الجريمة المنظمة) لاستدراج محترفي الاختراق إلى قبول المشاركة في أنشطة اعتداء معقدة أو استئجارهم للقيام بالجريمة.

المبحث الثاني

أصناف الجريمة الإلكترونية في القانون المقارن

يتطلب للحديث عن أي جريمة، تقليدية كانت أو إلكترونية، التطرق الى أركانها حتى يمكن القول بوجود الجريمة وأنواعها وذلك لتعديد أشكالها وحصرها في مجموعات ليسهل التعامل معها وعلى هذا قمنا بتقسيم هذا المبحث إلى مطلبين حيث تطرقنا في المطلب الأول إلى أركان الجريمة الإلكترونية، ثم أنواعها في المطلب الثاني.

المطلب الأول

أركان الجريمة الإلكترونية

تقوم الجريمة بشكل عام على ركنين، هي:[1]

الركن المادي: وهو ماديات الجريمة التي تبرز به إلى العالم الخارجي.

الركن المعنوي: وهو الإرادة التي يقترن بها الفعل سواء في صورة القصد أو الخطأ.

وسيتم التعمق في هذين الركنين "المادي والمعنوي" في الجرائم الإلكترونية من خلال الفرعين التاليين.

الفرع الأول: الركن المادي في الجرائم الإلكترونية

من المشكلات العملية التي تثيرها الجريمة الإلكترونية طبيعة الركن المادي في الجريمة الإلكترونية، ذلك أن مفهوم أو مناط التجريم ينصب على نظام إلكتروني يساء استعماله أو يتم اقتحامه على نحو غير مشروع، بما يكون لذلك الاستعمال أو الاقتحام من أثر مادي ملموس يظهر إما في صورة تدمير للمعلومات، وهو ما يثير إمكانية الإتلاف العمدي للمنقولات، أو السرقة وذلك عن طريق إساءة استعمال بطاقات الائتمان، أو يثير شبهة التزوير عن طريق التلاعب في بيانات الحاسب الآلي، كما سنرى من خلال هذه الدراسة. إن السلوك الإجرامي في الجريمة الإلكترونية يرتبط دائما بالمعلومة المخزنة على الحاسب الآلي، أو تلك التي يتم إدخالها للحاسب الآلي، وصعوبة المشكلة أن السلوك الإجرامي قد

[1] الجبور، محمد. الوسيط في قانون العقوبات – القسم العام، دار وائل، عمان، ط1،2012، ص 59

يتحقق بمجرد ضغط زر في الحاسب فيتم تدمير النظام المعلوماتي أو حصول التزوير أو السرقة عن طريق التسلل إلى نظام أرصدة العملاء في البنوك أو إساءة استعمال بطاقات الائتمان.[1]

إن السلوك الإجرامي بوصفه عنصرا في الركن المادي في الجريمة التقليدية يتم رؤيته رؤى العين والتأكد منه كفعل القتل أو السرقة أو التزوير، ولكن صعوبة الجريمة الإلكترونية والركن المادي فيها خاصة أن الجريمة ترتكب عن طريق معلومات تتدفق عبر نظم الحاسب الآلي لا يمكن الإمساك ماديا بها، تماماً مثل التيار الكهربائي الذي يسري في توصيلة دون أن نراه[2]، لذلك يتعين تحليل السلوك الإجرامي في الجريمة الإلكترونية خاصة ما يتعلق فيها بفكرة المال في جرائم الاعتداء على المال العام أو الخاص، كما لا بد من عرض صور السلوك الإجرامي في الجريمة الإلكترونية.

إن النشاط أو السلوك المادي في الجريمة الإلكترونية يتطلب وجود بيئة رقمية وجهاز كمبيوتر واتصال بشبكة الإنترنت، ويتطلب أيضاً معرفة بداية هذا النشاط والشروع فيه ونتيجته، فعلى سبيل المثال يقوم مرتكب الجريمة بتجهيز الكمبيوتر لكي يحقق له حدوث الجريمة، فيقوم بتحميل الحاسب ببرامج اختراق، أو أن يقوم بإعداد هذه البرامج بنفسه، وكذلك قد يحتاج إلى تهيئة صفحات تحمل في طياتها مواد مخلة بالآداب العامة وتحميلها على الجهاز المضيف، كما يمكن أن يقوم بجريمة إعداد برامج فيروسات تمهيدا لبثها، وليس كل جريمة تستلزم وجود أعمال تحضيرية، وفي الحقيقة يصعب الفصل بين العمل التحضيري والبدء في النشاط الإجرامي في جرائم الكمبيوتر والإنترنت – حتى ولو كان القانون لا يعاقب على الأعمال التحضيرية – إلا أنه في مجال تكنولوجيا المعلومات، الأمر يختلف بعض الشيء، فشراء برامج اختراق، ومعدات لفك الشفرات وكلمات المرور، وحيازة صور دعارة للأطفال،فمثل هذه الأشياء تمثل جريمة في حد ذاتها[3].

إن النشاط أو السلوك المادي في الجريمة الإلكترونية يعد محلا لتساؤلات عديدة فيما يتعلق ببدايته أو الشروع في ارتكاب الجريمة، ومثل هذا النشاط يختلف عما هو الحال عليهفي العالم المادي، فارتكاب الجريمة عبر الإنترنت يحتاج بالضرورة إلى منطق تقني، وبدونهلا يمكن للشخص حتى الاتصال بالإنترنت، سواء كان بقصد ارتكاب جريمة أم لمجرد التصفح أو الدخول في الاتصال المباشر كالمحادثة وغيرها.

---

[1] معاشي سميرة، ماهية الجريمة المعلوماتية، بحث منشور في مجلة المنتدى القانوني، العدد السابع، جامعة محمد خيضر بسكرة، الجزائر، 2011، ص 280

[2] الفتاح بيومي حجازي، الإثبات الجنائي في جرائم الكومبيوتر والانترنت دار الكتب القانونية، 2007، ص 114.

[3] الفتاح بيومي حجازي ، المرجع السابق، ص 113.

وهذا السلوك المادي الإيجابي الممثل في المنطق التقني يجعل الجريمة عبر الإنترنت ذات طابع موحد بالضرورة، فهي تباشر من حيث السلوك أو النشاط المادي فيها، كأحد عناصر الركن المادي يضاف إلى فلسفة الركن المادي في الجريمة، مثل هذا الأمر تداركه المشرع الأردني حين نص على جرائم يمكن أن ترتكب عبر الكمبيوتر، ففي مثل هذه النصوص نجد المشرع الأردني يقرر صراحة عبارة ... إذا ارتكبت الجريمة باستخدام نظام معلومات أو الشبكة المعلوماتية ..... أو عبارة ..... باستخدام المعالجة الآلية للبيانات" ففي مثل هذه الحالات يكون المشرع الأردني مدركاً لمسألة الشروع في ارتكاب جريمة عبر الشبكة المعلوماتية المرتبطة بالإنترنت.[1]

لذلك يعد الدفع بعدم وجود قدرات تقنية حال الاتهام بارتكاب جريمة عبر الإنترنت من الدفوع الموضوعية الجوهرية التي تلتزم محكمة الموضوع بالرد عليه تفصيلا، وإلا عاب حكمها عيبا في التسبيب بما يسمح بقبول نقضه، ولقد جعلت الطبيعة الموحدة للجريمة عبر الإنترنت، من حيث اتحاد جميع أشكالها المادية في ضرورة استخدام الآلة كوسيط إلى ارتكابها أن اتصفت هذه الجريمة بالضرورة بالطابع التقني.[2]

ولكي يتوافر الركن المادي في الجريمة الإلكترونية، فلا بد من حصول النتيجة الإجرامية على أن ترتبط بالسلوك الإجرامي بعلاقة سببية.

الفرع الثاني: الركن المعنوي للجريمة الإلكترونية

الركن المعنوي هو الحالة النفسية للجاني، والعلاقة التي تربط بين ماديات الجريمة وشخصية الجاني، فالركن المعنوي هو المسلك الذهني أو النفسي للجاني باعتباره محور القانون الجنائي، ذلك أنه في إطار هذا الركن تتوافر كافة مقومات المسؤولية الجنائية، من علم وإرادة آثمة وقصد جرمي مع إقرار حق الدولة في العقاب الذي يبنى على هذه المقومات، لذلك يمكن تعريف الركن المعنوي بأنه: العلاقة التي تربط بين ماديات الجريمة وشخصية الجاني مرتكبها، وهذه العلاقة هي محل الأذناب في معنى استحقاق العقاب، ومن ثم يوجه إليه الوم القانون وعقابه.[3]

ويتوفر القصد الجنائي في حق الجاني في حالات ثلاثة، هي:

---

[1] راجع نصوص المواد (4، 5، 6 8 9 10) من قانون جرائم أنظمة المعلومات الأردني رقم (30) لسنة 2010م

[2] خالد ممدوح ابراهيم ، فن التحقيق الجنائي في الجرائم الإلكترونية، ط1، دار الفكر الجامعي، الإسكندرية، مصر، 2009، ص 100

[3] حسني، محمود نجيب، النظرية العامة للقصد الجنائي، دار النهضة العربية، ط2، 1971، ص 90

الأولى: إذا كان الجاني يتوقع ويريد أن يترتب على فعله أو امتناعه حدوث الضرر أو وقوع الخطر الذي حدث والذي يعلق عليه القانون وجود الجريمة. الثانية: إذا نجم عن الفعل أو الامتناع ضرر أو خطر أكثر جسامة مما كان يقصده الفاعل،وهي حالة جواز القصد التي ينص عليها القانون صراحة على إمكان ارتكابها بهذا الوصف. الثالثة: الحالات التي يعزى فيها القانون الفعل إلى الفاعل نتيجة لفعله أو امتناعه، أي حالات يفترض فيها القانون توافر القصد الجنائي لدى الجاني افتراضاً، وهو مستمد من أنه طالما أن النتيجة الجسيمة التي تحققه نشأت عن فعل الجاني، فمقتضى ذلك أن هذا الفعل كان صحيحا ًلإحداثها، ولكونه كذلك فإن الجاني يجب أن يتحمل نتائجه، توقعها أم لم يتوقعها. [1]

إن توافر الركن المعنوي في الجرائم الإلكترونية يعد من الأمور الهامة في تحديد طبيعة السلوك المرتكب وتكييفه لتحديد النصوص التي يلزم تطبيقها، إذ بدون الركن المعنوي لن يكون هناك سوى جريمة واحدة هي جريمة الدخول أو الولوج غير المشروع. فمثلاً إن التمييز بين جريمة الدخول غير المشروع على نظام المعالجة الآلية للبيانات وبين جريمة تجاوز الصلاحيات في الدخول على مثل هذا النظام، يعد تمييزا دقيقاً.

ففي جريمة تجاوز صلاحية الدخول، فإنه يلزم لتوافرها أن يكون هناك صلاحية للدخول على نظام ما، على أن تتوافر في داخل هذا النظام أنظمة معينة ليس من حق هذا الشخص الدخول عليها، فيقوم المذكور بالدخول عليه، ففي هذه الحالة لا تتوافر سوى جريمة واحدة، حيث إن المذكور يملك صلاحية الدخول على النظام الأساسي ولا يملك الدخول على أنظمة خالة فيها، إلا أن تكوين النشاط المادي هنا يلزم أن يكون السلوك الإجرامي مرتكباً في إطار نشاط ثان وليس النشاط الأول مثل هذا الأمر يجعل جريمة تجاوز صلاحيات الدخول معتبرا من الجرائم التي لا يتطلب فيها ركنا معنويا، وهذا الأمر محرم قانونا. ونتيجة لذلك فإن القضاء الأمريكي لم يستقر على حال بالنسبة لبعض الجرائم التي ترتكب باستخدام الإنترنت من حيث مدى تحديد ما إذا كانت تتطلب قصداً عاماً أم خاصاً، فذلك لا يمانع في تطلب قصد جنائي خاص في جريمة التهديد، إلا أنه يقر من جديد أنه يكفي بالقصد العام عن ذات الجريمة، كما هو الشأن في جريمة التهديد بالبريد الإلكتروني وعبر المجموعات الإخبارية وفق ما هو مقرر في القسم والقصد العام فيها، بينما يتم استدلاء معالمه من النظرة الموضوعية إلى السلوك الشخصي من مجموعة الظروف المحيطة بالجريمة بما في ذلك فحص الحالة العقلية المرتكب الجريمة.[2]

[1] الجبور، محمد، مرجع سابق، ص 238 وما بعدها.

[2] خالد ممدوح ابراهيم ، مرجع سابق، ص 109

أما في القضاء الفرنسي فإن منطق سوء النية يكتسح النصوص التي تطبق بشأن الإنترنت، حتى أن هذه الجرائم لا يمكن أن تدخل حيز التطبيق ما لم يتوافر سوء النية في منطق القصد الخاص وإرادة الإضرار، ومن ذلك ما هو مقرر في المادة (15-226) عقوبات فرنسي جديد التي تشترط سوء النية حين وجود عدوان على البريد الإلكتروني، وبما يجعل ذلك بالضرورة متطابقا مع ما هو مقرر في المادة (11.5 1-2) من تقنين البريد والاتصالات الصادر بالقانون المؤرخ 26/7/1996م التي تلزم وزير الاتصالات الفرنسي بالسهر على مبدأ احترام سرية الاتصالات.[1]

كذلك الحال لدى المشرع البريطاني، فالركن المعنوي في الجريمة الإلكترونية يتطلب أن تنصرف إرادة الجاني نحو الدخول إلى البيانات أو المعطيات المخزنة في أي حاسوب، إ ذجرم المشرع البريطاني الدخول غير المصرح به للنظام الإلكتروني بموجب المادة الأولى من قانون إساءة استخدام الحاسوب البريطاني لعام 1990م، وكذلك جرم الدخول غير المصرح به إلى النظام الإلكتروني بهدف ارتكاب جريمة أخرى بموجب المادة الثانية من نفس القانون.[2]

المطلب الثاني

أنواع الجريمة الإلكترونية

تعد الجريمة الالكترونية نشاطا إجراميا تستخدم فيه تقنية الحاسب الآلي بطريقة مباشرة أوغير مباشرة كوسيلة أو هدف لتنفيذ الفعل الإجرامي المقصود. وقبل التطرق إلى أهم آليات مكافحتها لا بأس وأن نشير إلى بعض أشكال هذه الجريمة الخطيرة .

ولابد من الإشارة إلى أن تصنيف الجريمة الإلكترونية أصعب من تصنيف الجريمة التقليدية وتستهدف الكثير من القطاعات من أشخاص معنويين وطبيعيين وحتى الدول أمنيا واقتصاديا، لذا لم يستقر الفقهاء ورجال القانون على تصنيف واحد وتحديد أنواعها، ويعود ذلك أيضا لتشعبها وسرعة تطورها فهناك من يعتمد على معيار الجرائم المعلوماتية المرتكبة على الحاسوب والجرائم المعلوماتية المرتكبة بواسطة الحاسوب. وهناك من يعتمد معيار الدافع الإجرامي والباعث على ارتكابها. واتجاه يعتمد على الوسيلة المستعملة والأسلوب المتبع لارتكاب الجريمة واتجاه آخر يأخذ بمعيار محل الجريمة أو الضحايا.

---

[1] موسى، مصطفى محمد، دليل التحري عبر شبكة الإنترنت، دار الكتب القانونية، مصر،2010، ص 143.

[2] الرواشدة سامي، والهياجنة أحمد،مكافحة الجريمة المعلوماتية بالتجريم والعقاب، المجلة الأردنية في القانون والعلوم السياسية، جامعة مؤتة – الأردن، المجلد (1)، العدد (3)، 2009، ص128.

وعليه سيتم التعرض إلى تصنيفين هامين للإلمام بكل الأنواع أين سنتعرض أولا لتصنيف يتعلق بأخطر واشهر انواع هذه الجريمة وبعدها نتطرق للتصنيف التقليدي حسب محل الجريمة.

الفرع الأول: تصنيفات الجريمة الإلكترونية حسب خطورتها في القوانين الدولية

أولا: جرائم التجسس الالكتروني وجرائم القرصنة

1/ جرائم التجسس الالكتروني: يعتمد هذا النوع من الجرائم على تقنيات عالية التقدم حيث لم يعد يقتصر التجسس على ما يتعلق بالمعلومات العسكرية أو السياسية بل تعداه إلى المجال الاقتصادي والتجاري والثقافي، و لقد ظهر هذا النوع من الجرائم خصوصا بعد أحداث الحادي عشر من سبتمبر التي شهدتها الولايات المتحدة الأمريكية[1]، و من الأساليب المعتمدة أسلوب إخفاء المعلومات داخل المعلومات بحيث يتم إخفاء تلك المعلومات المهمة و المستهدفة داخل معلومات عادية في جهاز الحاسب الآلي ومن ثم يتم تهريبها باستعمال أساليب متطورة لا يتم اكتشافها و لو ضبط الشخص متلبسا، و مثال ذلك : قيام شبكة دولية ضخمة للتجسس الالكتروني التي تعمل تحت إشراف وكالة الأمن القومية الأمريكية بالتعاون مع أجهزة الاستخبارات في كندا وبريطانيا لرصد المكالمات الهاتفية بهدف التعامل مع الأهداف غير العسكرية، ولا يقتصر الرصد على المحطات الموجهة إلى الأقمار الصناعية و الشبكات الدولية بل يشمل الاتصالات التي تجري عبر أنظمة الاتصالات الأرضية[2].

2/ جرائم القرصنة: اتسعت وتطورت صور القرصنة من خلال العثور على مواقع الانترنت لترويج البرامج المقرصنة مجانا أو بمقابل مبلغ رمزي مما ألحق العديد من الخسائر المادية الباهظة مما أدى بالشركات المتخصصة في صناعة البرامج إلى إنشاء منظمة خاصة لمراقبة وتحليل ما يعرف بسوق البرمجيات، ومنها منظمة اتحاد برمجي الأعمال التي أجرت دراسة حول ذلك وتبنت الحلول المناسبة[3].

ومثال ذلك: تعرض أنظمة تشغيل مايكروسوفت لبرامج الكومبيوتر العملية قرصنة مستعملين في ذلك عامل ذكي لبرامج الكومبيوتر يمكنه التجول بحرية عبر الشبكات لالتقاط المعلومات ونقلها دون قيام

[1] عبد الفتاح بيومي حجازي، الإثبات الجنائي في جرائم الكومبيوتر والانترنت، دار الكتب القانونية، 2007، ص13.
[2] عبد الفتاح مراد، شرح جرائم الكومبيوتر والانترنت دون ذكر دار النشر، ص 382.
[3] مرجع نفسه، ص 385.

المتسلل باختراق الكومبيوتر نفسه، حيث تم فتح تحقيق في هذا المجال[1]. كما يتم أيضا إرسال فيروسات لتخريب الجهاز و محتوياته حيث بمجرد كتابة كلمة أو فتح البرنامج الحامل للفيروس أو الرسالة البريدية المرسل معها الفيروس تتم إصابة الجهاز و من ثم يقوم بمسح محتوياته أو العبث بالملفات الموجودة فيه.

ثانيا: جرائم الإرهاب الالكتروني و الجرائم المنظمة

1/ جرائم الإرهاب الالكتروني: أدى التطور الالكتروني، و قيام ما يعرف بالحكومات الالكترونية إلى تغيير أنماط الجريمة الالكترونية ، وظهور ما يعرف بالإرهاب الالكتروني، حيث تم إنشاء لجنة خاصة لحماية البنية التحتية في الولايات المتحدة الأمريكية وتم تحديد الأهداف المحتملة من قبل الإرهابيين و هي مصادر الطاقة الكهربائية، والاتصالات، وشبكات الحاسب الآلي.

وما تجدر الإشارة إليه أنه بعد أحداث 11 سبتمبر 2001 تمت ممارسة الإرهاب الالكتروني ضد المواقع الإسلامية و العربية أيضا.

2/ الجرائم المنظمة:

تم استغلال الإمكانيات المتاحة في وسائل الانترنت لتخطيط وتمرير وتوجه المخططات الإجرامية وتنفيذ وتوجيه العمليات غر المشروعة بكل سهولة من خلال إنشاء مواقع خاصة بها على شبكة الانترنت لمساعدتها في إدارة العمليات، والترويج بتجارة المحذرات عبر الانترنت أيضا وتعليم كيفية زراعتها وصناعتها. وكذا جرائم غسل الأموال التي تعتمد على إخفاء المصدر غير المشروع الذي تكتسب منه الأموال.

حيث يجد المتصفح للانترنت مواقع عديدة تتحد عن غسيل الأموال غير المشروعة التي تتميز بالسرعة و إغفال التوقيع و استعمال بطاقات مزورة شبيهة ببطاقات البنوك المستخدمة التي تساهم في تحويل الأموال عبر الانترنت مع ضمان تشفير و تأمين العملية كل ذلك ساعد على سهولة و سرعة الجريمة دون ترك الأثر.

[1] هناك حادثة أخرى أطلق عليها "حادثة الأصدقاء الأعداء " حيث تمكن أحد الإسرائيليين من اختراق أنظمة معلومات حساسة سنة 1998 في كل من ال.و.م.أ وإسرائيل لمؤسسات عسكرية ومدنية و تجارية حيث تمت متابعة نشاطه من قبل محققين في ال.و.م.أ و تبين أن مصدر الاختراق هو جهاز الكومبيوتر، وتم فتح تحقيق في ذلك.

إضافة إلى العديد من الجرائم الأخرى كالجرائم الماسة بالتجارة الالكترونية من خلال الاستيلاء على بطاقات الائتمان، وكذلك الجرائم الاقتصادية كسرقة خطوط الهاتف والعبث بها وإتلافها، وتحويل الأرصدة النقدية وغيرها.

وعليه بالنظر إلى الطبيعة الخاصة التي تتميز بها الجريمة الالكترونية باستخدام الوسائل الالكترونية المستحدثة تمتد لتشمل البعد العالمي هذا الأخير الذي لا يتقيد بحدود دولة معينة وهذا ما يجعله ينعكس على آليات مكافحتها.[1]

الفرع الثاني: أنواع الجريمة الإلكترونية حسب معيار محل الجريمة:

تختلف الجريمة الالكترونية باختلاف محل الجريمة فممكن أن يكون الضحية شخصا أو دولة، أو أن تقع على مال.

أولا: الجرائم الواقعة على الأشخاص

هي الجرائم الالكترونية التي يكون ضحاياها الأشخاص الطبيعيين يمكن إجمالها في:

1- جرائم الملكية الفنية والادبية : حيث يتم الاعتداء على الأشخاص بالاستيلاء على مجهود المؤلف عن طريق الاستيلاء على بيانات عمله المخزنة في نظام المعالجة الآلية (بنك المعلومات). وعلى حقوق الملكية الفكرية أو حتى بالتقليد كما هو الحال في الملكية الصناعية.

2- الاعتداء على حرمة الحياة الخاصة للأشخاص: هذه الجرائم تمس الأفراد سواء في خصوصيتهم أو في سلامة شرفهم. حيث يحاول المجرم بعث الخوف في نفسية الضحية ببعث رسائل مجهولة المصدر عن طريق البريد الإلكتروني ، فتخاف الضحية من الفضيحة فحرمة الحياة الخاصة حق دستوري والمحافظة على الأسرار وعدم إفشائها سواء كانت مكالمات او محادثات ، فلا يجوز اختراق شبكة الاتصالات والتصنت عليها وانتهاك الخصوصية ، حيث تتم عن طريق اعداد ملف يحتوي على معلومات عن الضحية بدون علمه أو بعلمه مثل الأسرار التي يطلع عليه المحامي أو المحاسب أوالطبيب بمناسبة عمله ويستعملها ضده للابتزاز والتهديد[2].

[1] عبد الفتاح مراد، مرجع سابق، ص 384-385.

[2] غائم مرضي الشمري، الجرائم المعلومائية، ماهيتها خصائصها، كيفية التصدي لها قانونا، د س ، د ط، ص 56

3- انتحال الشخصية: وتطال هذه الجريمة الأشخاص وحتى المواقع ، حيث يستولي المجرم على البيانات والمعلومات الشخصية للضحية بعد اختراق المواقع بسبب سمعتها ومكانتها الاجتماعية والوظيفية أو من صلاحياتها للاستفادة منها ماديا ومعنويا بالاستدراج والتغرير.

4- جرائم السب والقذف: هي أكثر الجرائم انتشارا على شبكة الأنترنت ، عن طريق وسائل الاتصال بالكتابة أو البريد الإلكتروني أو غرف المحادثة ، بتوجيه وإسناد واقعة أو خدش شرف الأشخاص أو دون إسناد واقعة والهدف تشويه السمعة، كسبِّ الرسول صلى الله عليه وسلم أو رئيس الجمهورية[1].

5-الجرائم الماسة بالأخلاق : بصناعة ونشر الإباحية والجنس سواء البالغين او الأطفال خاصة، حيث يتم عرض صور الإباحية أو ممارسة الجنس بالإكراه حيث تستمر معاناة الضحايا بعد ارتكاب الجريمة بسبب إمكانية تناقل الصور عبر الأنترنت ، أو إراديا وتصوير القصر وحتى الإعلان عن الدعارة عن طريق الصور و التسجيلات المرئية (الفيديوهات) ، وهذه المواقع تشكل خطرا على القصر والأطفال خاصة لأنها في متناولالجميع وكما يعد الأنترنت اسهل طريقة وأكثر جاذبية لنشر الإباحية .

ثانيا: الجرائم الواقعة على الأموال .

1- جريمة التحويل الإلكتروني للأموال : من أهم نشاطات البنوك الإلكترونية عمليات تحويل ونقل الأموال للزبائن من حساب بنكي إلى حساب آخر ، والمعلومات المتعلقة بعملية التحويل فيقوم البنك بتحويل الأموال من حساب المدين إلى حساب الدائن ، عن طريق المقاصة الإلكترونية خلافا للتحويلات التقليدية من طرف بنك مؤهل ومرخص له بذلك ، عن طريق أجهزة الحاسوب فالجريمة تكون عندما يكون هذا التحويل غير قانوني وغير مشروع فتحول الأموال من حساب الضحية إلى حساب المعتدي أو حساب مستفيد أجنبي ، ويكون ذلك عن طريق:

التلاعب ببرامج التحويل الخاصة.

استعمال بطاقة شخص لسحب أمواله.

استعمال البيانات والمعلومات الشخصية في إصدار بطاقة ممغنطة ثانية باسم الزبون الضحية للقيام بالجريمة.

[1] غانم مرضي الشمري، المرجع نفسه، ص 136.

2- جريمة القمار عبر الأنترنت : ظهرت بظهور النوادي والكازينوهات الافتراضية التي انتشرت عبر المواقع الإلكترونية والخاصة بألعاب القمار لكن هذه المواقع غير مسموح بها في أغلب البلدان وغير مصرح لها بممارسة نشاطها حيث أصبحت فيما بعد مسرحا لجريمة غسيل الأموال[1].

3- جريمة غسيل الأموال : هي جريمة تقليدية تطورت عن طريق التطور التكنولوجي حيث يتم ارتكابها عن طريق تطهير الأموال التي يكون مصدرها غير مشروع ويتم استثمارها بطريقة شرعية عن طريق البنوك ، عن طريق نقلها بعملية اقتصادية ومالية للأموال من مصدر غير مشروع إلى دائرة الاقتصاد الشرعي ، والمصدر غير الشرعي يكون مخدرات او اختلاس ، ويتمثل ضرر وخطورة تبييض الأموال في ان ها تدخل الى الاقتصاد حيث أنها أموال غير مستقرة يمكن تحويلها إلى الخارج في أي وقت كما انها جريمة مركبة حيث تغطي على الجريمة الأولى، ولها إضرار أمنية واجتماعية وقانونية وسياسية.

4- تجارة المخدرات عبر الانترنت : حيث هناك مواقع تروج لاستهلاك المخدرات وكيفية إنتاجها وتعليم كيفية تصنيعها وطرق تسويقها وإنتاجها.

5 - السطو والسرقة الإلكترونية : قرصنة أرقام البطاقات الممغنطة.

6- التزوير الإلكتروني : من بين الجرائم الإلكترونية جريمة التزوير وهو من بين أخطر ما يقوم به المجرم المعلوماتي نظرا لما يتمتع به الحاسب الآلي من خطورة ، فيتم التزوير عن طريق الوسائل المتطورة كتزوير العملة عن طريق الماسح الضوئي وما يسببه ذلك من إضرار بالاقتصاد الوطني ، أو تقليد وتزييف الوثائق والمستندات الكترونيا أو التوقيع(المحررات الرسمية)[2].

ثالثا: الجرائم الواقعة على الدولة

وتتمثل أساسا في جريمتي المساس بأمن الدولة وكذلك الإرهاب الإلكتروني.

1-الإرهاب الإلكتروني: من اخطر الجرائم الإلكترونية جريمة الإرهاب المعلوماتي فالأنترنت أصبح مكانا لترويج الأفكار المنظمات الارهابية والتعبير عن معتقداتها، بمحاولة التأثير على المعتقدات الدينية لأفراد المجتمع وتقاليده مما يخلق الفوضى ويمس بأمن الدولة، أو تكون بتعاون بين عدة أفراد قصد الإضرار بالبلد وقد تكون بالإشادة بالأفعال الإرهابية المرتكبة ضد الدولة أو إلحاق الأذى بالمؤسسة

[1] غانم مرضى الشمري، المرجع السابق، ص 58

[2] عامر محمود الكسواني، التزويز المعلوماتي للعلامة التجارية، دار الثقافة للنشر والتوزيع، الأردن،2014، ص151.

العسكرية، عن طريق زرع الفيروسات المخربة أو تعطيل الأنظمة بالتنويه والإشادة بالإرهاب ضد دولة محددة بعينها واستغلال المؤيدين للفكر المتطرف[1].

2/جريمة التجسس على الدولة : ويكون في المجال الأمني والاقتصادي من طرف الدول المعادية بتجميع الأسرار وتموين بالأخبار فيكون التجسس على الأسرار العسكرية ، تمس بأمن الدولة وتتم عن طريق اختراق المواقع الحكومية والرئاسية او قرصنتها وبالتالي الاطلاع على أسرار الدولة العسكرية والاقتصادية. حيث ان استهداف الدفاع الوطني للدولة والهيئات العسكرية يتم بواسطة أشخاص أو منظمات يتواجدون خارج البلاد والتجسس يكون على المواقع والمنظمات والشخصيات العسكرية. ويتم على اقتصاد والمؤسسات الاقتصادية التابعة للدولة تكون من قبل عملاء من دولة معادية أو حتى صديقة لكشف الأسرار الاقتصادية، أو من شركة على شركة منافسة في نفس المجال فهي معلومات سرية مؤمنة لا يسمح بالاطلاع عليها لأنها أسرار دولة، لكن الاختراق يكشف عن الحماية وخاصة اذا كان نظام التأمين ضعيفا[2].

[1] مصطفى يوسف كافي، جرائم الفساد غسيل الأموال السياحة الارهاب الالكتروني المعلوماتية، مكتبة المجتمع العربي للنشر والتوزيع، الأردن ، ط1، 2014 ، ص 143

[2] خالد حسن أحمد لطفي، جرائم الأنترنت بين القرصنة الالكترونية وجرائم الابتزاز الالكتروني، دار الفكر الجامعي الإسكندرية، د ذ ط ، 2019، ص 38

خاتمة الفصل الأول:

في ختام هذا الفصل، تم استعراض الإطار المفاهيمي للجريمة الإلكترونية في التشريع الجزائري والقانون المقارن. تناولنا أولا تعريف الجريمة الإلكترونية من زوايا متعددة، شملت التشريعات المختلفة، القانون الدولي، والفقه القانوني، مما أتاح لنا فهمًا شاملاً لطبيعة هذه الجرائم وتباين التعريفات بين القوانين المختلفة.

ثم تم تحليل أركان وأنواع الجريمة الإلكترونية، حيث تطرقنا إلى الركنين المادي والمعنوي لهذه الجرائم، ثم استعرضنا أنواع الجريمة الإلكترونية وتصنيفاتها وفقًا للقوانين الدولية المختلفة.

من خلال هذا الفصل، تم بناء قاعدة معرفية متينة حول الجرائم الإلكترونية، مما يمهد الطريق للفصل القادم الذي سنتعمق فيه في دراسة سبل مكافحتها والإجراءات القانونية اللازمة لمواجهتها في التشريع الجزائري والقانون المقارن.

الفصل الثاني: الجوانب العملية للحدّ من الجريمة الإلكترونية في القانون المقارن

تمهيد0

في ضوء التزايد المستمر للجرائم الإلكترونية وتنامي تأثيرها السلبي على المجتمعات والاقتصادات العالمية، بات من الضروري البحث عن آليات فعالة لمكافحتها. يهدف هذا الفصل إلى استعراض الجهود المبذولة في القانون المقارن لمواجهة هذه الظاهرة المعقدة والمتغيرة بسرعة. سنستعرض الإطار التشريعي والمؤسسي في مختلف الدول، بالإضافة إلى السياسات والاستراتيجيات المعتمدة لمكافحة الجرائم الإلكترونية. من خلال هذا التحليل، سنتمكن من تحديد أفضل الممارسات وتقديم توصيات لتعزيز فعالية التشريعات الجزائرية في هذا المجال الحيوي.

وعلى هذا الأثر قمنا بتقسيم هذا الفصل الى مبحثين:

المبحث الأول:آليات مكافحة الجريمة الإلكترونية في القانون المقارن

المبحث الثاني:الجانب الإجرائي والتطبيقي للجريمة الإلكترونية

المبحث الأول

آليات مكافحة الجريمة الإلكترونية في القانون المقارن

يهدف هذا المبحث إلى استعراض آليات مكافحة الجريمة الإلكترونية في القوانين المقارنة، من خلال تحليل دور الأجهزة المختصة في التصدي للجريمة الإلكترونية في المطلب الأول بالإضافة إلى تقييم كيفية تصدي هذه التشريعات للجرائم الإلكترونية في المطلب الثاني ودورها في تعزيز الحماية الجزائية والتعاون الدولي لمكافحة هذه الظاهرة الناشئة في المطلب الثالث.

المطلب الأول

الأجهزة المختصة في مكافحة الجرائم الإلكترونية

سنتطرق في هذا المطلب إلى استعراض دور الأجهزة المختصة في مكافحة الجرائم الإلكترونية في الفرع الأول، نستعرض إلى أجهزة مكافحة الجرائم الإلكترونية في مصر، أما في الفرع الثاني فنركز على استراتيجيات الجزائر.

الفرع الأول: الأجهزة المختصة في مكافحة الجرائم الإلكترونية في مصر:

لقد وضع المؤتمر الأول لجمعيات قانون الإنترنت والذي عقد بالقاهرة في 27 سبتمبر 2004م اللبنة الأولى لإنشاء جمعيات ومنظمات أهلية للعمل التطوعي في مجال قانون الإنترنت، ومن هنا جاء تأسيس الجمعية المصرية لمكافحة جرائم المعلوماتية والإنترنت تلبية سريعة لدعوة المؤتمر التأسيسي لجمعيات ومنظمات قانون الإنترنت من جانب نخبة من القضاة ووكلاء النائب العام، والمحامون، والمحاسبون، والمصرفيون، والإعلاميون، ومهندسي تكنولوجيا المعلومات والاتصالات[1].

تعتبر الجمعية المصرية لمكافحة جرائم المعلوماتية والإنترنت منظمة غير حكومية خاضعة للقانون المصري ومشهرة تحت رقم (2176) لسنة 2005م وصدر قرار إشهارها بتاريخ 2005/08/05م.

إن انتشار تكنولوجيا المعلومات والاتصالات الجديدة على نطاق العالم أدى إلى ظهور أشكال من الجرائم المتصلة بالحواسيب والتي تشكل خطراً على سرية النظم الحاسوبية أو سلامتها أو توافرها بل يتعدى ذلك ليشكل خطراً متعاظماً على أمن البنى الأساسية الحرجة، وفضلاً عن ذلك فإن الابتكارات التكنولوجية تسفر عن أنماط مختلفة من الابتكار الإجرامي فعند مكافحة هذه الجرائم يواجه المحققون

[1] عبد الله عبد الله عبد الكريم، ماية الملكية الفكرية على شبكة الانترنت ، دار الجامعة الجديدة للنشر ، الاسكندرية ، 2008، ص 94.

وممثلو الادعاء العام والقضاة على السواء عدداً من المشاكل التي تنجم جزئياً عن الطابع غير الملموس للأدلة الرقمية وسرعة اختفائها، وعلاوة على ذلك فإن التحقيق في الجرائم المتصلة بالحواسيب وملاحقتها قضائياً غالباً ما يقتضيان تتبع النشاط الإجرامي وإثارته من خلال مجموعة متنوعة من مقدمي خدمات الإنترنت أو الشركات التي تقوم بذلك، ويتجاوز هذا التتبع أحياناً الحدود الوطنية، الأمر الذي يثير أسئلة صعبة تتعلق بالولاية القضائية والسيادة، وتفرض التحديات الخاصة بالجرائم المتصلة بالحواسيب إقامة تعاون دولي فعّال في هذا المجال، وبالتالي فإن ذلك يقتضي أن يكون لدى كل دولة في العالم الأدوات القانونية والإجرائية والتنظيمية اللازمة لذلك، كما أن زيادة وكثافة تكنولوجيا المعلومات والاتصالات وجني فوائد مجتمع المعلومات يؤدي أيضاً لزيادة الجرائم المتصلة بالحواسيب، وبالتالي فإنه من مصلحة الأمن الاقتصادي والأمن العام من تشريعات محلية لمكافحة الجرائم المتصلة بالحواسيب[1].

وتتمثل الأهداف المتوخاة من الجمعية بالتالي:[2]

نشر الوعي والقيام بحركة تثقيف اجتماعية، وقانونية، واقتصادية، وتنموية، للتعريف بالجرائم الناشئة عن استخدام الإنترنت.

إعداد الدراسات والبحوث حول العلاقة الرقمية بالقاعدة الموضوعية والإجرائية في القانون الجنائي والحث على تطويره.

إعداد ومتابعة التجمعات العلمية والأكاديمية، وحضور المؤتمرات والندوات المتعلقة بالجرائم ضد المعلوماتية، والجرائم الناشئة عن استخدام الإنترنت.

4 إعداد قاعدة إحصائية للجرائم ضد المعلوماتية والجرائم الناشئة عن استخدام الإنترنت.

5 تقديم الدعم والعون العلمي للمؤسسات والأفراد وكل من له مصلحة في مكافحة الجرائم الناشئة عن استخدام الإنترنت.

تنمية الكوادر البشرية في مجال مكافحة الإجرام عبر الإنترنت.

متابعة التقارير والدراسات والبحوث، والعمل على تشجيع البحث العلمي في مجال دراسةالجرائم الناشئة عن استخدام الإنترنت.

---

[1] عوض، محمد محيي الدين، مشكلات السياسة الجنائية المعاصرة في جرائم نظم المعلومات، دار الفكر العربي القاهرة، ط1، 2011، ص 158.

[2] أنظر الموقع الآتي : www.eapiic.org. إطلع عليه بتاريخ 2024/06/19 على الساعة 21:00.

أما بخصوص أنشطتها، فهي[1]:

إعداد المؤتمرات والندوات وورش العمل وإلقاء المحاضرات والمشاركة في كل ذلك والمساهمة مع المؤسسات الأخرى ذات العلاقة بأغراض الجمعية.

متابعة الفقه والقضاء المقارن في كل ما ينشر والمبادرة إلى تعميمها عن طريق إصدار المصنفات والمطبوعات.

التثقيف والتدريب وإنشاء مؤسسات تدريبية والمساهمة مع الغير فيها بقصد السعي إلى تطوير قانون الإجراءات الجنائية لكي يتفاعل مع الأدلة الرقمية.

إصدار الدوريات والنشرات والبحوث والعمل على نشرها، وتعميمها وبثها عبر الإنترنت.

تقديم الاستشارات والخدمات، وإعداد وتنفيذ الدراسات المتخصصة في مجالات عمل الجمعية.

المساهمة في تقديم خدمات البلاغ الرقمي ومتابعة هذا البلاغ.

تبادل الخبرات والزيارات والدراسات المشتركة مع الجهات المعنية بأهداف وأنشطة الجمعية.

نشر فكر ووعي قانون الإنترنت والسعي لدى المشرعين على كافة المستويات لقيام فرع قانون الإنترنت.

مكافحة كافة أشكال الجرائم التي تقع ضد المعلوماتية في كافة أشكالها الأجهزة والبرامج، والشبكات والمعلومات والبيانات، والأموال، ووسائل الاتصال، والجرائم ضد السمعة، والجرائم ضد الشخصية، والجرائم ضد الإنسانية، والجرائم الموجهة للأمن القومي في كافة أشكالها وصورها، وبالعموم مكافحة كافة الجرائم التي يكون الحاسب أداة من أدواتها أو هدفاً من أهدافها أو وسطاً لها.

وتسعى الجمعية للتعاون مع كافة قطاعات المجتمع وعلى الأخص كليات الحقوق وكليات المعلومات والحاسبات وشركات القطاع الخاص العاملة في مجال تكنولوجيا المعلومات والنقابات المهنية، والاتحادات العمالية، وكافة الوزارات والهيئات المعنية بميدان الجمعية، ومنظمات العمل المدني في مصر. كما تسعى الجمعية لعقد اتفاقيات تعاون فيما بينها وبين كافة الجهات المماثلة لها في كافة الدول العربية، كما تسعى الجمعية لدى جامعة الدول العربية لإنشاء جمعيات مثيلة في الأقطار العربية، وتؤكد الجمعية على دعمها ومؤازرتها للجمعية العربية القانون الإنترنت والالتزام بنظامها الأساسي، والالتزام

[1] عوض، محمد محيي الدين، مرجع سابق، ص 160.

بمقررات المؤتمر الدولي الأول لقانون الإنترنت الذي انعقد في مدينة الغردقة بجمهورية مصر العربية في شهر أغسطس سنة 2011م، وتؤكد على حصرها للانضمام لعضوية الجمعية العربية لقانون الإنترنت، وتسعى الجمعية للحصول على عضوية الجمعية الدولية لقانون الإنترنت فور الإعلان عن تأسيسها وقيامها خلال فعاليات المؤتمر الدولي الثاني لقانون الإنترنت، كما تسعى للتعاون مع الجهات المثيلة لها في كافة دول العالم للاستفادة بالخبرات السابقة في مجال عمل الجمعية[1].

الفرع الثاني: الأجهزة المختصة في مكافحة الجرائم الإلكترونية في الجزائر

وتتمثل في المراكز والوحدات التي إستحدثتها الدولة الجزائرية في مكافحة الجرائم الإلكترونية، سنتطرق لها تباعا في النقاط التالية:

أولا: المصلحة المركزية لمكافحة الجريمة المعلوماتية التابعة للمديرية العامة للأمن الوطني:

في إطار مجهودات المديرية العامة للأمن الوطني لمجابهة الإجرام السيبراني، تم إنشاء المصلحة المركزية للجريمة الإلكترونية التي عملت على تكييف التشكيل الأمني لمديرية الشرطة القضائية، استجابة من مصالح الأمن الجزائرية لمطلب الأمن المعلوماتي ومحاربة التهديدات الأمنية الناجمة عن الجرائم الإلكترونية. وقد كانت هذه المصلحة عبارة عن فصيلة شكلت النواة الأولى لتشكيل أمني خاص المحاربة الجريمة الإلكترونية على مستوى المديرية العامة للأمن الوطني والتي أنشأت سنة 2011 ليتم بعدها إنشاء المصلحة المركزية لمحاربة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال بقرار من المدير العام للأمن الوطني وأضيف للهيكل التنظيمي لمديرية الشرطة القضائية في جانفي2015. وتتمثل مهام هذه المصلحة فيما يلي:[2]

مساعدة مصالح الشرطة القضائية في مجال التحريات التقنية.

المشاركة في حماية الأنظمة المعلوماتية والفضاء السيبراني الوطني.

التعاون والمشاركة في التحقيقات والتحريات ذات البعد الوطني والدولي في مجال مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

[1] عوض، محمد محيي الدين، مرجع سابق، ص 162.

[2] م ش، المصلحة المركزية للجريمة الإلكترونية في مواجهة مجرمي العالم الإفتراضي، تاريخ الإسترداد 2021/02/08، بتاريخ 2016/02/13، تم الاطلاع عليه بتاريخ 2024/06/24 على الساعة: 21:06.

اليقظة المعلوماتية والبحث عن الشبكات المفتوحة، عن كل محتوى غير شرعي يشكل في حد ذاته جريمة في قانون العقوبات أو يكون مخالف للنظام العام.

المساهمة في التكوين المتخصص لعناصر الشرطة المتواجدين على مستوى فرق مكافحة الجريمة المعلوماتية على مستوى أمن الولايات.

ثانيا: نيابة مديرية الشرطة العلمية والتقنية التابعة للمديرية العامة للأمن الوطني:

أسندت المديرية العامة للأمن الوطني مهمة مكافحة الجريمة المعلوماتية لنيابة مديرية الشرطة العلمية والتقنية، وتضع هذه الأخيرة لخدمة هذا الهدف مصالح علمية مختصة بذلك، تتولى أعمال البحث والتحري بشأن الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، وهذه الوحدات هي: المخبر المركزي للشرطة العلمية والكائن مقره بالجزائر العاصمة المخبر الجهوي للشرطة العلمية قسنطينة و المخبر الجهوي للشرطة العلمية – وهران.

ويتولى كل مخبر سواء المركزي أو الجهوي لولاية وهران أو قسنطينة، مهام البحث والتحقيق وتحليل الأدلة الجنائية بمختلف أنواعها، ولأجل ذلك يضم كل مخبر دائرتين هما:

الدائرة العلمية : وتتولى أعمال البحث والتحقيق وتحليل الأدلة المتصلة بالمجال البيولوجي والطب الشرعي والكيمياء والمخدرات وكذلك تلك المتعلقة بمجال التسميم والحريق والمتفجرات كل منها على مستوى مخبر خاص.

الدائرة التقنية : وتتولى مهام البحث والتحقيق وتحليل الأدلة الجنائية الناتجة عن الجرائم التي تستعمل فيها الأسلحة والقذائف بمختلف أنواعها، إضافة إلى الجرائم المعلوماتية، وتباشر الإجراءات الخاصة بكل جريمة على مستوى دائرة مستقلة عن الأخرى[1].

ومن جانب آخر، تؤدي الشرطة الجزائرية دورا هاما في مجابهة الإرهاب السيبراني، وذلك من خلال:

- الدوريات الالكترونية خلايا اليقظة الإلكترونية لرصد أي تصرف مشبوه.
- محاولة تتبع الأثر الإلكتروني.
- التوعية والتحسيس عبر الفضاء السيبراني.

[1] حسين ربيعي، آليات البحث والتحقيق في الجرائم المعلوماتية (أطروحة دكتوراه في الحقوق تخصص قانون العقوبات والعلوم الجنائية) باتنة قسم الحقوق كلية الحوق والعلوم السياسية، جامعة باتنة 1 – الجزائر، 2015–2016، ص 177.

- العمل على تجفيف مصادر التمويل والتجنيد عبر الفضاء السيبراني.

ثالثا: المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني:

تم إنشاء المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني بموجب المرسوم الرئاسي رقم 04-183 المؤرخ في 26 يونيو 2004 المتضمن إحداث المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني، وهو مؤسسة عمومية ذات طابع إداري تحت وصاية وزير الدفاع الوطني ويمارس قائد الدرك الوطني سلطات الوصاية بتفويض منه وتتمثل المهام المسندة إليه حسب ما أقرته المادة 04 في :[1]

إجراء الخبرات والفحوص العلمية التي تخضع لاختصاص القضاة والمحققين أو السلطات المؤهلة، بناء على طلبهم، في إطار التحريات الأولية والتحقيقات القضائية، بغرض إقامة الأدلة التي تسمح بالتعرف على مرتكبي الجنايات والجنح.

تقديم المساعدة العلمية أثناء القيام بالتحريات المعقدة باستخدام مناهج الشرطة العلمية والتقنية الرامية إلى تجميع وتحليل الأشياء والآثار والوثائق المأخوذة من مسرح الجريمة.

المشاركة في الدراسات والتحاليل المتعلقة بالوقاية والتقليل من كل أشكال الإجرام.

تصميم وإنجاز بنوك معطيات طبقا للقانون، بما في ذلك المعطيات الخاصة بالبصمات الجينية، والتي ستكون في متناول المحققين والقضاة بغرض وضع المقاربات واستخلاص الروابط المحتملة بين المجرمين وأساليب النشاط الإجرامي.

المبادرة بالبحوث المتعلقة بالإجرام وإجراءها باللجوء إلى التكنولوجيات الدقيقة.

العمل على ترقية البحث التطبيقي وأساليب التحريات التي ثبتت فعاليتها في ميادين علم الإجرام والأدلة الجنائية على الصعيدين الوطني والدولي.

المشاركة في كل الملتقيات والمحاضرات والندوات الوطنية والدولية الضرورية في تطوير مستخدمي المعهد. تصور الأبحاث الموكلة إلى الغير وضمان متابعتها وتقديرها[2].

[1] المرسوم الرئاسي رقم 04-183، بتاريخ 26 جانفي 2004، المتضمن إحداث المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني وتحديد قانونه الأساسي، الجريدة الرسمية رقم ،41 بتاريخ 2004 27 يونيو.

[2] المرجع نفسه.

رابعا: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها:

نصت على إنشاء هذه الهيئة المادة 13 من القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، وحسب نص المادة الثانية من المرسوم الرئاسي 19-127، تعتبر الهيئة مؤسسة عمومية ذات طابع إداري تتمتع بالشخصية المعنوية والاستقلاليةالمالية توضع تحت سلطة وزارة الدفاع.[1]

وقد تم توضيح المهام التي أوكلت لهذه الهيئة، في المادة 14 من القانون 09-04 المذكور سابقا، والمتمثلة أساسا في :

أ- تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته.

ب- مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم ذات الصلة بتكنولوجيات الإعلام والاتصال بما في ذلك تجميع المعلومات وإنجاز الخبرات القضائية.

ج- تبادل المعلومات مع نظيراتها في الخارج قصد جمع كل المعطيات المفيدة في التعرف على مرتكبي الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وتحديد مكان تواجدهم.

وتعمل هذه الهيئة تحت إشراف ومراقبة لجنة مديرة يترأسها وزير العدل، وتضم أساسا أعضاء من الحكومة معنيين بالموضوع، ومسؤولي مصالح الأمن وقاضيين من المحكمة العليا يعينهما المجلس الأعلى للقضاء، وتضم الهيئة قضاة وضباطا وأعوانا من الشرطة القضائية تابعين لمصالح الاستعلامات العسكرية والدرك الوطني والأمن الوطني، وفقا لأحكام قانون الإجراءات الجزائية[2].

وتوضح المادة 04 من المرسوم الرئاسي رقم 15-261 المؤرخ في 08 أكتوبر 2015، المحدد لتشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، أن هذه الهئية تمارس المهام المنصوص عليها في المادة 14 من القانون 04-09 المذكورة سابقا، تحت رقابة السلطة القضائية طبقا لأحكام التشريع الساري المفعول، وتكلف بما يأتي:

اقتراح عناصر الاستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها .

---

[1] أميرة حوالف، معالم الجريمة المعلوماتية في القانون الجزائري. مجلة البحوث القانونية والسياسية – المجلد 03 ، العدد 16، 12 فيفري 2021، ص151.

[2] سمير بارة، الأمن السيبراني Cyper Security في الجزائر : السياسات والمؤسسات المجلة الجزائرية للأمن الإنساني، جويلية 2017، ص274.

تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها .

مساعدة السلطات القضائية ومصالح الشرطة القضائية في مجال مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، بما في ذلك من خلال جمع المعلومات والتزويد بها ومن خلال الخبرات الفضائية.

ضمان المراقبة الوقائية للاتصالات الإلكترونية قصد الكشف عن الجرائم المتعلقة بالأعمال الإرهابية والتخريبية والمساس بأمن الدولة.

تجميع وتسجيل وحفظ المعطيات الرقمية وتحديد مصدرها ومسارها من أجل استعمالها في الإجراءات القضائية.

السهر على تنفيذ طلبات المساعدة الصادرة عن البلدان الأجنبية وتطوير تبادل المعلومات والتعاون على المستوى الدولي في مجال اختصاصها.

تطوير التعاون مع المؤسسات والهيئات الوطنية المعنية بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

المساهمة في تكوين المحققين المتخصصين في مجال التحريات التقنية المتصلة بتكنولوجيات الإعلام والاتصال.

والمساهمة في تحديث المعايير القانونية في مجال اختصاصها.

خامسا: القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال :

تم إنشاء هذا القطب بموجب الأمر رقم 11/21 المؤرخ في 25 أوت 2021، المعدل والمتمم لقانون الإجراءات الجزائية والقاضي باستحداث القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، ويتواجد على مستوى محكمة مقر مجلس قضاء الجزائر[1]. وقد تم تحديد مفهوم الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وفقا لهذا القانون على أنها أي جريمة ترتكب أو يسهل ارتكابها استعمال منظومة معلوماتية أو نظام للاتصالات الإلكترونية أو أي وسيلة أخرى أو آلية

[1] المادة 211 مكرر من الامر 21-11 الصادر في 25 غشت 2021 المتمم لقانون الاجراءات الجزائية.

ذات صلة بتكنولوجيات الإعلام والاتصال. وقد أوكلت لهذا القطب الجزائي الوطني مهمتين أساسيتين تتمثلان في:[1]

– المتابعة والتحقيق في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال والجرائم المرتبطة بها.

الحكم في الجرائم المنصوص عليها في الباب السادس من الأمر رقم 11/21، إذا كانت تشكل جنحا.

المطلبالثاني

تصدي التشريعات المقارنة للجريمة الإلكترونية

في ظل التزايد المستمر للجرائم الإلكترونية وتعقيداتها، أصبحت الحاجة ملحة لتطوير تشريعات فعالة لمواجهتها. تختلف آليات التصدي للجريمة الإلكترونية من دولة لأخرى، حيث تتبنى كل منها نهجًا خاصًا بناءً على سياقاتها القانونية والثقافية. نستعرض فيما يلي كيفية تصدي بعض التشريعات المقارنة للجريمة الإلكترونية:

الفرع الأول: التشريع الفرنسي:

نص القانون رقم 78– 17 الصادر في فرنسا عام 1978م ، والخاص بالمعلوماتية على انشاء اللجنة الوطنية المعلوماتية والحريات مهمتها مراقبة حسن تطبيق القانون حيث نص فى المادة 14 منه على حماية البيانات الخاصية سواء كانت ملك الدولة أو الأشخاص ويعتبر هذا أول قانون ينظم الجوانب القانونية المتصلة بالمعلوماتية وأثرها على الخصوصية.

ونص قانون العقوبات الفرنسي من خلال تعديلاته بنصوص خاصة حيث اصدرت قانون رقم 19– 88 لسنة 1988م وهو أول تشريع فرنسي لتجريم بعض جرائم الحاسب الآلي وهو ما يعرف بقانون godfrain[2] حيث نصت بعض المواد.

نصت المادة 468 منه على تجريم القيام والدخول كلية أو جزئية داخل منظومة لمعالجة المعلومات بالحبس لمدة شهرين إلى سنة، وغرامة تتراوح بين10 ألاف فرانك ومئة ألف فرنك.[1]

---

[1] سميحة بلقاسم، حميد بوشوشة، الجريمة الإلكترونية بعد جديد للإجرام في الجزائر..واقعها وآليات مجابهتها، مجلة العلوم الإنسانية لجامعة أم بواقي، 2023/01/18، ص555.

[2] بعرة سعيد، الجريمة الإلكترونية في التشريع الجزائري، رسالة لنيل الماستر في الحقوق، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، 2015–2016، ص18

الفرع الثاني: التشريع الإماراتي:

أورد المشرع الأماراتي في قانون الاتحاد رقم 2 لسنة 2006م في شان مكافحة الجرائم المعلوماتية جملة من المصطلحات ذات دلالة قانونية حيث جرم العبث بالمعلومات الالكترونية والسرقة والاحتيال والاستيلاء على مستندات بغير وجه حق

الفرع الثالث: التشريع المصري

بدأ الاهتمام في مصر بمكافحة الجرائم الإلكترونية بعد انعقاد المؤتمرالتأسيسي لجمعيات قانون الإنترنت بالقاهرة في سبتمبر 2004م والمؤتمر الدولي الأول لقانون الإنترنتفي الغردقة 2005م.

تأسست الجمعية المصرية لمكافحة جرائم الإنترنت سنة 2005م وهي منظمة غير حكومية هدفها نشر الوعي وإعادة الدراسات والمؤتمرات حولالجرائم المعلوماتية.

أول قانون صدر بشأن تجريم بعض الأفعال المتعلقة بالنظم المعلوماتية هو قانون التوقيع الإلكتروني صدر سنة 2004م ، حيث جرم أفعالا تتعلق بالحصول على توقيع او وسيط أو محرر إلكتروني يدون وجه حق أو اعتراضه او تعطيله عن أداء وظيفته.[2]

الفرع الرابع: التشريع التونسي

يعتبر القانون التونسي المتعلق بالتجارة الإلكترونية رقم 83 لسنة 2000م الخاص بالمبادلات الإلكترونية والمؤرخ في 2000/8/9م، أول تشريع يتعرض للجرائم الإلكترونية حيث نصت المادة 48 من القانون التونسي أسرارا تعلق بالشفرة الخاصة بالتوقيع الإلكتروني من خلال فك الشفرة أو كلمة السر واستعمالها بدون وجه حق عوقب بالحبس مدة تتراوح بين ستة أشهر وسنتين وغرامة مالية بين الف إلى عشرة الاف دينار تونسي.[3]

الفرع الخامس: التشريع السعودي

جاءت المواد من الثالثة (3) إلى العاشرة (10) لتحديد أنواع الجرائم الإلكترونية والعقوبة المقررة عليها فمثلا المادة (3) يعاقب بالسجن مدة لا تزيد عن سنة وبغرامة لا تزيد عن خمسمائة الف ريال أو إحدى هاتين العقوبتين وكل من يتركب هذه الجرائم ومنها:

---

[1] المادة (44) من قانون المعالجة الإلكترونية والحريات الفرنسي

[2] بعرة سعيد، المرجع السابق، ص27.

[3] بعرة سعيد، المرجع السابق، ص28.

- التصنت على ما هو مرسل عن طريق شبكة المعلومات أو أحد أجهزةالحاسب؛
- الدخول غير المشروع لتهديد شخص أو ابتزازه لحمله على القيام بفعل أو الامتناع عنه
- الدخول غير المشروع على موقع الكترونى لإتلافه أو تعديله؛
- المساس بالحياة الخاصة، عن طريق إساءة استخدام الهواتف النقالة؛
- التشهير بالآخرين وإلحاق الضرر بهم عبر وسائل تقنيات المعلومات المختلفة.

كما نصت المادة الرابعة على أنه يعاقب بالسجن مدة لا تزيد عن ثلاث سنوات وبغرامة لا تزيد عن مليوني ريال كل شخص يرتكب الجرائم الآتية:

- الإستيلاء لنفسه أو لغيرة على مال منقول أو على سند أو توقيع هذا السند وذلك عن طريق الإحتيال أو اتخاذ اسم كاذب.
- الوصول دون مسوغ إلى معلومات بنكية أو إئتمانية أو بيانات متعلقة بملكية أوراق مالية أو معلومات للحصول على بيانات.[1]

المطلب الثالث

التعاون التشريعي الدولي والإقليمي لمكافحة الجريمة الإلكترونية

ترتكب الجريمة الإلكترونية في مسرح غير قابل للتحديد الجغرافي، إلا أنه يضم أكبر تجمع إنساني يتميز بارتباط وتشابك معقد ، وتتمثل أهم خصائصه في خلق آليات خاصة لفرض الالتزامات والإذعان لها مثل قطع الاتصال على مخترقي بعض القواعد، أو طردهم من المنتديات، لكن هذا التجمع الإنساني الضخم يفتقر إلى المعايير الأخلاقية المشتركة، وهو ما حدا المجلس الأوروبي إلى عقد اتفاقية بودابست عام 2001م بشأن الجرائم الإلكترونية، والتي قدمت صوراً لمكافحة الجرائم الإلكترونية، ونصت المادة (22) منها على أن لكل طرف اتخاذ الإجراءات التشريعية وغيرها التي يراها لازمة لكي يحدد اختصاصه بالنسبة لكل جريمة تقع وفقاً لما هو وارد في المواد من (2) إلى (11) من الاتفاقية الحالية عندما تقع الجريمة:

أ. داخل نطاق المحلي للدولة.

ب. على ظهر سفينة تحمل علم تلك الدولة.

[1] بعرة سعيد، المرجع السابق، ص29.

ج. على متن طائرة مسجلة في هذه الدولة.

د. بواسطة أحد رعاياها، إذا كانت الجريمة معاقباً عليها جنائياً في المكان الذي ارتكبت فيه، أو إذا كانت الجريمة لا تدخل في أي اختصاص مكاني لأي دولة أخرى.

ولكل طرف أن يحتفظ لنفسه بالحق في عدم تطبيق، أو عدم التطبيق إلا في حالاتوفي ظل شروط خاصة، قواعد الاختصاص المنصوص عليها في الفقرة الأولى (ب) و (د) منهذه المادة أو في أي جزء من هذه الفقرات.

وتنص الفقرة (4) من المادة نفسها على عدم استبعاد أي اختصاص ينعقد للقضاءالوطني طبقا للقانون المحلي، الفقرة (5) تنص على أنه في حالة حدوث تنازع في الاختصاص فإنه يجب أن يتم حله بالتشاور بين الدول الأطراف حول المكان الأكثر ملائمة، كما أفردتالاتفاقية بنداً خاصاً لضرورة التعاون بين الدول[1].

هذا ولم ينص القانون العربي النموذجي بشأن الجرائم الإلكترونية[2] على أي 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 والتشريعي، فيلزم من باب أولى قبول هذه الفكرة والتوسع فيها بالنسبة الجرائم ترتكب في الفضاء الافتراضي الذي يتجاوز الحدود والقارات، وبذلك تصل إلى ضرورة التفكير في وضع ضوابط إسناد جنائية لتحديد الاختصاص الموضوعي والإجرائي بعد أن تصنف الجرائم الإلكترونية إلى فئات مختلفة تشكل كل فئة فكرة مسندة تتضمن المصالح الواجب حمايتها جنائياً على المستوى العالمي لوضع ضوابط إسناد تشير إلى القانون واجب التطبيق[3].

إلا أن هذه القواعد يجب أن تتم صياغتها في إطار اتفاقيات دولية لأن الجريمة الدولية لا يمكن مواجهتها إلا بالتعاون الدولي، وهو أهم ما جاء في اتفاقية بودابست بشكل يسمح بتبادل التعاون سواء كان ذلك على مستوى جمع الأدلة أو تسليم المجرمين، وهو ما يعني أن المجتمع الدولي مقبلاً على توسع في

[1] عبد الله عبد الله عبد الكريم، مرجع سابق، ص 105 وما بعدها.

[2] اعتمدت جامعة الدول العربية عبر الأمانة الفنية لمجلس وزراء العدل العرب ما سمي بقانون الإمارات العربي الاسترشادي لمكافحة جرائم تقنية المعلومات وما في حكمها، وقد اعتمده بموجب قرار رقم 417 د 21 2004م، للتفصيل راجع عبد الله عبد الله عبد الكريم، مرجع سابق، ص 140 وما بعدها.

[3] المطرودي، مفتاح بو بكر، مرجع سابق، ص 27.

مجال التعاون القضائي الذي يتوقع أن يتم بين الأجهزة القضائية والأمنية بشكل مباشر نظراً لأن عامل الوقت في حفظ الأدلة الإلكترونية سوف يكون حرجاً ومتطلباً لسرعة الإنجاز[1].

وعلى الرغم من ضرورة التعاون الدولي بشأن مواجهة تحديات الجرائم الإلكترونية وتضافر الجهود من أجل تفعيله، إلا أن هناك العديد من العقبات التي تعترض سبيله، من أبرزها عدم وجود اتفاق عام بين الدول على مفهوم الجرائم الإلكترونية، وعدم وجود توافق بين قوانين الإجراءات الجنائية للدول بشأن التحقيق في تلك الجرائم، والنقص الظاهر في مجال الخبرة لدى الشرطة وجهات الادعاء والقضاء[2].

[1] البشري، محمد الأمين، التحقيق في جرائم الحاسب الآلي، دار الكتب القانونية، مصر،2009، ص 178.

[2] عوض محمد محيي الدين، مرجع سابق، ص 326-327

المبحث الثاني

الجانب الإجرائي والتطبيقي للجريمة الإلكترونية

يتناول هذا المبحث الجانب الإجرائي والتطبيقي للجريمة الإلكترونية، حيث يتم التركيز على إجراءات كشف الجرائم الإلكترونية ووسائل إثباتها في عدة سياقات قانونية في المطلب الأول، بينما يناقش المطلب الثاني وسائل إثبات الجريمة الإلكترونية وأهميتها في إقامة الدليل القانوني اللازم لمحاكمة المتهمين في هذا النوع من الجرائم، وعرض بعض النماذج التطبيقية للجرائم الإلكترونية في المطلب الثالث.

المطلب الأول

إجراءات كشف الجريمة الإلكترونية

استحدث المشرع قواعد إجرائية جديدة أكثر راهنية ومردودية تساعد الجهات المكلفة بالبحث والتحري عن الجريمة الإلكترونية والوصول إلى الدليل الرقمي والمتمثلة في كل من التسرب الإلكتروني وكذلك اعتراض المراسلات والمراقبة الإلكترونية ناهيك عن الإجراءات المرتبطة بالمعطيات.

الفرع الأول : التسرب الإلكتروني

تعد الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات واحدة من الجرائم التي أجاز المشرع أن يتم الاعتماد فيها على إجراء التسرب من أجل التحري فيها وذلك بموجب المادة 65 مكرر 05 من قانون الإجراءات الجزائية.[1]

إذ عرف المشرع إجراء التسرب من خلال المادة 65 مكرر 12 من قانون الإجراءات الجزائية، على أنه " قيام ضابط عون الشرطة القضائية تحت مسؤولية ضابط الشرط القضائية المكلف بتنسيق العملية بمراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة بإيهامهم أنه فاعل معهم أو شريك لهم".

وبذلك فالتسرب هو إجراء أو تقنية تسمح لضباط الشرطة القضائية بالتوغل داخل جماعة إجرامية، وذلك تحت مسؤولية ضباط الشرطة القضائية وبالتنسيق معهم.[2]

---

[1] الأمر رقم ،155/66المؤرخ في 08جوان ،1966، المتضمن قانون الإجراءات الجزائية المعدل والمتمم.

[2] معزيز أمينة، التسرب في قانون الإجراءات الجزائية الجزائري، مقال منشور في مجلة القانون والمجتمع، العدد11، 2019، ص247.

ومن ثم يتم الانضمام إلى أشخاص مشتبه فيهم من أجل الكشف عن نشاطهم الإجرامي وكسب ثقتهم مع إخفاء الهوية، وتقديم المتسرب نفسه على أنه شريك أو مساهم بالجريمة أو فاعل وبذلك فهو من أخطر إجراءات التحقيق لما ينطوي عليه من خطورة على المتسرب[1].

ونشير في هذا السياق إلى أن المشرع الجزائري عبر على التسرب بالاختراق بموجب المادة 56 من القانون رقم 01/06المتعلق بالوقاية من الفساد ومكافحته والتي تنص على أنه "من أجل تسهيل جمع الأدلة المتعلقة بالجرائم المنصوص عليها بهذا القانون يمكن اللجوء إلى التسليم المراقب، وإتباع أساليب تحري خاصة كالترصد الإلكتروني أو الاختراق على النحو المناسب وبموجب إذن من السلطات المختصة".[2]

وكضمانة للمتسرب وبهدف حمايته وعائلته من مخاطر التعدي عليه نصت المادة 65 مكرر من قانون الإجراءات الجزائية على أنه " لا يجوز إظهار الهوية الحقيقية لضباط أو أعوان الشرطة القضائية اللذين يباشرون عملية التسرب تحت هيئة مستعارة في أي مرحلة من مراحل الإجراء".

وحدد المشرع جملة من الضوابط الموضوعية والإجرائية يستوجب مراعاتها من أجل القيام باجراء التسرب، كالتالي:

أولا: الشروط الموضوعية لإجراء التسرب

هناك شرطين موضوعيين لإجراء التسرب تلخصهما فيما يلي:

أ- عنصر التسبيب

يعد عنصر التسبيب ضمانة هامة كونه تتضح من خلاله الأسباب المبررة التي دفعت بوكيل الجمهورية لإصدار الأمر بإجراء التسرب، وذلك تحت طائلة بطلان الإذن وكل الإجراءات، أي أن مفاده تبيان المبررات وكذلك الحجج التي بموجبها منحت الجهة القضائية الإذن بالتسرب لضباط الشرطة القضائية.

[1] معزيز أمينة، مرجع سابق، ص543.

[2]القانون رقم 01/06، المؤرخ في 20 فبراير، 2006 المتعلق بالوقاية من الفساد ومكافحته، الجريدة الرسمية للجمهورية الجزائرية، العدد،14، الصادرة في 08 مارس 2006.

ب- تحديد نوع الجريمة

إذ يتوجب تبيان نوع الجريمة التي بموجبها تم طلب إجراء التسرب بهدف التحقيق فيها، مع ضرورة أن تكون هذه الجرائم من ضمن الجرائم الخطيرة، والمحددة على سبيل الحصر بموجب المادة65 مكرر 05 سابق الإشارة إليها.

ثانيا: الشروط الإجرائية لإجراء التسرب

وتتجلى الشروط الإجرائية لإجراء التسرب كوسيلة للكشف عن الجريمة المعلوماتية في مايلي :

أ- الإذن القضائي

لا يجوز للعون القضائي مباشرة التسريب تلقائيا وبمحض إرادته، لأن ذلك مرهون على طلب الإذن المسبق من طرف وكيل الجمهورية قبل افتتاح التحقيق، باعتباره المكلف قانونا بإدارة نشاط الضبطية القضائية وممثلا للنيابة العامة[1]. وتبقى العملية تحت الرقابة المباشرة للجهة المصدرة للإذن، وذلك من أجل الحد من التعسف في استعمال الحق في التسرب الإلكتروني ويشترط أن يكون الإذن مكتوبا و ليس شفويا[2]، و إلا عد إجراء التسرب باطلا من منطلق أن العمل الإجرائي يجب أن يكون مكتوبا تحت طائلة البطلان مع احتوائه لجملة البيانات المطلوبة، ومن ذلك تحديد نوع الجريمة المتخذ بشأنها التسريب، وكذلكاسم ضابط الشرطة القضائية الذي قامت العملية تحت مسؤوليته.[3]

ب- تحديد مدة التسرب

إذ يتوجب أن يكون إجراء التسرب محدد بفترة زمنية، غير أنه إذا تقرر وقف العملية أو انقضت المهلة المحددة في الرخصة للتسرب و لم يتم تمديدها يمكن للعون المتسرب مواصلة النشاطات للوقت الضروري الكافي لتوقيف عمليات المراقبة في ظروف آمنة دون أن يكون مسؤولا جنائيا على أن لا يتجاوز ذلك 04 أشهر.

---

[1]فدوي عمارة، ،اعتراض المراسلات وتسجيل الأصوات كإجراء قضائي في المواد الجنائية، مقال منشور بمجلة العلوم الإنسانية، العدد 33، 2010، ص248.

[2]معزيز أمينة، مرجع سابق، ص252.

[3]جمال نجيمي، ،2011 إثبات الجريمة على ضوء الإجتهاد (دراسة مقارنة)، دار هومة، الجزائر، ص452.

وما تجدر الإشارة إليه هو أنه وبموجب المادة 26 من القانون رقم 20/05 المؤرخ في 28 أبريل 2020، والمتعلق بالوقاية من التمييز وخطاب الكراهية أجاز المشرع الجزائري لضباط الشرطة القضائية استعمال إجراء التسرب من أجل الكشف عن مرتكبي جرائم التمييز وخطاب الكراهية. وذلك عن طريق إيهامهم أنه فاعل معهم أو شريك لهم، وهو ما يعتبر من الصلاحيات المستحدثة للضبطية القضائية.[1]

الفرع الثاني : اعتراض المراسلات والمراقبة الإلكترونية

إن دراسة عملية اعتراض المراسلات كآلية للكشف عن الجريمة المعلوماتية تتطلب بالضرورة تحديد مفهوم اعتراض المراسلات والمراقبة الإلكترونية، بالإضافة إلى الوقوف على المراسلات التي يمكن أن تكون محلا لإجراء الاعتراض، مع تحديد الشروط الموضوعية والشكلية المتطلبة قانونا من أجل تبني عملية اعتراض المراسلات.

أولا : مفهوم عملية اعتراض المراسلات

يناط باعتراض المراسلات تلك العملية التي تسمح بمراقبة سرية المراسلات السلكية واللاسلكية في إطار البحث والتحري عن الجريمة، وجمع الأدلة والمعلومات حول الأشخاص المشتبه في ارتكابهم أو مشاركتهم في إرتكاب الجريمة.

وعرفت المادة 65 مكرر 05 عملية مراقبة المراسلات على أنها: " اعتراض أو تسجيل أو نسخ المراسلات التي تتم عن طريق قنوات أو وسائل الاتصال السلكية واللاسلكية ".

و لم تشر المادة المذكورة أعلاه لطبيعة هذه المراسلات مما يفتح المجال للمراسلات المكتوبة مهما كان شكلها (كتابة رموز أشكال (صور) ويستوي أن تكون ورقية أو رقمية، وسواء كانت بالفاكس أو تيلغرام أو لاسلكية مثل البريد الالكتروني و الهاتف النقال . استنادا إلى المفاهيم الواردة في المادة 02 من القانون رقم 09/04.[2]

[1] القانون رقم 20/05، المتعلق بالوقاية من التمييز وخطاب الكراهية، المؤرخ في 28 أبريل ،2020 الجريدة الرسمية للجمهورية الجزائرية، العدد 25، الصادرة في 29 أبريل 2020.

[2] القانون رقم 09/04 المؤرخ في 05 أوت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

وعلى ذلك فإن عملية الاعتراض أو المراقبة تتم عن طريق ترتيبات تقنية سرية، يتم وضعها دون موافقة الأشخاص المعنيين المشتبه فيهم بغرض التنصت والتقاط وتثبيت وتسجل البيانات المرسلة أو المحادثات التي أجراها المشتبه في أماكن عامة أو خاصة[1]، من أجل استعمالها كدليل لمواجهته.

كما تعد المراسلات عبر البريد الإلكتروني مجالا خصبا للربط والاتصال الإلكتروني (04/18) بين الأشخاص في مختلف أنحاء العالم وبوقت قياسي، ومن ثم يمكن إخضاعها العلمية الاعتراض والمراقبة للكشف عن الجرائم الإلكترونية (04/118).

ثانيا: الشروط المطلوبة في المراسلات محل الاعتراض

يشترط في المراسلات التي يمكن أن تكون محلا لإجراء الاعتراض أو المراقبة أن تتسم بالسرية والخصوصية، ولاشك أن ذلك لا يتحقق إلا في ظل توافر عنصرين هما:

– فحوى الرسالة والتي تنصب على معلومات أو أفكار سرية و شخصية.

– تحديد المرسل إليه ورغبته في عدم السماح للغير بالإطلاع على مضمون المراسلة.

مع الإشارة أن المشرع الجزائري لم يتبنى إجراء مراقبة الاتصالات الإلكترونية كإجراء للتحقيق القضائي، وكذلك التحري بموجب القانون رقم 09/04 بل أعطى تصريح للجهات القضائية باستعمال الاعتراض بهدف الوقاية من بعض الجرائم التي تشكل خطرا على أمن الدولة.

وإتماما لهذا الهدف تم استحداث الهيئة الوطنية الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال والتي أوكل لها القانون مهمة تنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال و مكافحتها مع السلطات القضائية، وذلك من خلال المادة 13 من القانون رقم 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها(04/09).

وبالتالي هي عبارة عن هيئة أو سلطة إدارية مستقلة تتمتع بالشخصية المعنوية والاستقلال المالي ومقرها بالجزائر العاصمة، تم تحديد تشكيلتها وعملها بموجب المرسوم الرئاسي رقم 261/15.[1]

[1]شيخ ناجية، أساليب البحث والتحري المتخذة في القانون رقم ،22/06، المعدل والمتمم لقانون الإجراءات الجزائية الجزائري، المجلة النقدية، 2017، ص293.

ثالثا: الشروط القانونية لاعتراض المراسلات

تبقى عملية الاعتراض أو مراقبة المراسلات مرهونة على توافر الشرط التالية:

توافر إذن مكتوب من الجهات القضائية المختصة، أي من طرف وكيل الجمهورية بمرحلة التحقيق الابتدائي، أو من طرف قاضي التحقيق بمرحلة التحقيق القضائي تحت طائلة بطلان الإجراء القضائي، ولاشك أن اشتراط الإذن هو إجراء حتمي من منطلق أسلوب اعتراض المراسلات السلكية واللاسلكية يتم دون علم المعنيين لأنه ورغم نجاعته في الكشف عن الجرائم المعلوماتية، إلا أنه يشكل اعتداء على سرية المراسلات والاتصالات ومساس بحرمة الحياة الخاصة التي كفلها الدستور[2]. ويشترط أن يتضمن الإذن طبيعة الجريمة التي تبرر الإجراء، مع ضرورة أن تكون من الجرائم التي يجوز منح الإذن فيها، بالإضافة إلى تحديد المراسلات المراد اعتراضها وتسجيلها وتحديد الأماكن المقصودة، سواء كانت أماكن عامة أو خاصة مع تحديد مدة الاعتراض والتي لا تتجاوز 04 أشهر قابلة للتجديد.

التسبيب أي تبيان دواعي اللجوء إلى الاعتراض و مراقبة المراسلات و تبيان مدى جدية تلك الدواعي ودورها إظهار الجريمة والجناة

تحديد الجرائم محل الاعتراض والمراقبة والتي يتوجب أن لا تخرج عن ما هو مقرر قانونا مع مراعاة سرية الإجراءات وكتمان السر المهني.

الفرع الثالث : الكشف عن الجريمة المعلوماتية عن طريق المعطيات

تلعب المعطيات دورا هاما في الكشف عن الجريمة المعلوماتية. ويتم الاستفادة منها إما عن طريق الحفظ و الإفشاء العاجلان، أو عن طريق تجميعها بوقتها الفعلي.

أولا : الحفظ والإفشاء العاجلان للمعطيات الإلكترونية

يعد الحفظ والإفشاء من الإجراءات المستحدثة للكشف عن الجريمة المعلوماتية والوصول إلى الدليل الرقمي، ونصت عليهما المادة 10 من القانون 09/04 المتعلق بالوقاية من الجرائم المتعلقة بتكنولوجيا الإعلام والاتصال ومكافحتهما (09/04أ.).

---

[1]المرسوم الرئاسي رقم ،261/15، المؤرخ في 08 أكتوبر 2015، المحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، الجريدة الرسمية للجمهورية الجزائرية، العدد 53، الصادرة في 08 أكتوبر 2015.

[2]المرسوم الرئاسي رقم 442/20، المؤرخ في 30 ديسمبر2020، المتعلق بإصدار التعديل الدستوري المصادق عليه في استفتاء 01 نوفمبر 2020، الجريدة الرسمية للجمهورية الجزائرية، العدد 82، الصادرة في 30 ديسمبر2020.

ومن ثم فإنه يقوم بهذا الإجراء مقدمي خدمات الإنترنيت أين يقومون بالحفظ عن طريق الحيازة بالأرشيف بهدف حماية المعطيات التي سبق وجودها في شكل مخزن، مما يحول دون تلفها أو تجرديها من صفتها أو حتى حالتها الأصلية وفق النماذج التي تراها ملائمة لوضع عملية الحفظ وموقع التنفيذ.

ومن ثم هناك نوع من المعطيات يمكن أن تكون محل تحفظ مع مراعاة جملة من الضوابط

يتم التطرق إليها فيما يلي.

أ-المعطيات محل التحفظ

حددت المادة 11 من القانون رقم 09/04 سابق الإشارة إليه، معطيات المرور التي يتعين على مقدم الخدمات التحفظ عليها بناءا على طلب من السلطات القضائية المختصة، والتي تتجسد فيما يلي :

- المعطيات التي تسمح بالتعرف على مستعملي الخدمة.
- المعطيات المتعلقة بالتجهيزات المستعملة بالاتصال ومن ذلك الإشارة إلى الرقم
- التسلسلي للجهاز وكذلك نوعه و طرق تشغيله.
- [19: المعطيات التي تسمح بالتعرف على المرسل والمرسل إليهم، ومن ذلك أرقام الهواتف أوعناوينهم.
- الخصائص التقنية وكذلك تاريخ ووقت و مدة الاتصال
- المعطيات المتعلقة بالخدمات التكميلية المطلوبة أو المعلومة المستعملة و مقدميها.

ب- الضوابط الواجب مراعاتها خلال عملية حفظ المعطيات

نظرا لكون عملية حفظ معطيات تمس الحق في الخصوصية، فقد حدد المشرع الجزائري ضوابط يتوجب على مقدم خدمة الانترنيت التقيد بها كالتالي :

- احترام المدة الزمنية المقررة لعملية الحفظ والتي حددها المشرع الجزائري بموجب المادة 11 من القانون 09/04 بسنة واحدة، إبتداءا من تاريخ التسجيل و بعد انقضاء المدة المقررة للحفظ يتوجب على مزود الخدمة السحب الفوري للمعطيات المخزنة من خلال اتخاذ التدابير التي تفيد عدم إمكانية الإطلاع عليها (09/04أ المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.)

– مراعاة سرية عملية التحفظ، إذ يلتزم مقدمو الخدمات بالحفاظ على سرية كل الإجراءات والتدابير التي تفرضها العملية طيلة الفترة المقررة، وتبقى الحكمة من هذا الالتزام هي مراعاة الحق في الخصوصية وتفادي تغيير البيانات أو محوها من طرف أشخاص.

الإفشاء العاجل لمعطيات السير على النحو المنصوص عليه بموجب المادة 10 من القانون 04/09.

ونشير في هذا السياق إلى عملية أخرى فعالة في التحقيق والكشف عن الجريمة المعلوماتية والمتجسدة في إنتاج البيانات المعلوماتية فهو إجراء حديث يتماشى وطابع الدليل المعلوماتي.[1]

إلا أن المشرع الجزائري لم ينص على هذا الإجراء كإجراء يمكن الاعتماد عليه في سبيل التحري، وهو ما يتطلب معه وعلى وجه الضرورة أن يتدارك المشرع الجزائري هذا السهو.

ثانيا: تجميع معطيات المرور بوقتها الفعلي

يتم جمع المعلومات المساعدة في عملية التحري من طرف مقدم خدمة الانترنيت، ويعرف هذا الأخير على أنه "أي كيان عام أو خاص يقدم لمستعملي خدماته القدرة على الإتصال بواسطة منظومة معلوماتية أو نظام للاتصالات، أو هو أي كيان يقوم بمعالجة أو تخزين معطيات الفائدة خدمة الاتصال (09/04أ).

وبالتالي فإنه يقع على عاتق مقدم خدمة الانترنيت (09-04) التعاون مع جهات البحث والتحري بهدف الوصول إلى الدليل الرقمي وذلك من خلال قيامه بما يلي:

- حفظ المعطيات التي تسمح بالتعرف على مستعمل الخدمة، وكذلك الخصائص التقنية ومدة الاتصال، بالإضافة إلى المعطيات التي تسمح بالتعرف على المرسل إليهم وعناوينهم المواقع التيتم الإطلاع عليها (09/04أ).
- مراعاة أن يكون حفظ المعطيات لمدة سنة واحدة إبتداءا من تاريخ التسجيل، وتقديمه لجهات التحقيق فور طلبها.

[1] شيخ ناجية، مرجع سابق، 294.

- التدخل الفوري لسحب المحتويات التي يسهل الإطلاع عليها بمجرد علمهم بطريقة مباشرة أو غير مباشرة بمخالفتها للقوانين، مع تخزينها أو جعل الدخول غليها غير ممكن.
- وضع ترتيبات تقنية تسمح بحصر إمكانية الدخول إلى الموزعات التي تحتوي معلومات مخالفة للنظام العام أو الآداب العامة، أو إخبار المشتركين لديهم بوجودها.

ونشير في هذا السياق أن امتناع مقدم خدمات الإنترنيت على التعاون مع السلطات، من شأنه تعريضه للعقوبة الإدارية وللمسائلة الجنائية (09/04أالمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها).

ومع بروز القانون 05/20 المتعلق بالوقاية من التمييز وخطاب الكراهية ومكافحتهما، والذي يصبو لوضع حد لكل تمييز وخطاب كراهية بغض النظر عن الوسيلة المستعملة سواء كانت تقليدية أو إلكترونية، نجد أن المشرع الجزائري وبموجب 21 منه أجاز للجهات القضائية المختصة بمناسبة التحقيق في هذه الجرائم أن تأمر مقدمي خدمات الانترنيت أو أي شخص آخر بتسليمها المعلومات والمعطيات المخزنة باستعمال وسائل تكنولوجيات الإعلام والاتصال.

كما يمكنها إصدار أمر إلى مقدمي خدمات الإنترنيت بالتحفظ الفوري للمعطيات المرتبطة بهذا النوع من الجرائم نظرا لخطورتها (20/05أ).

المطلب الثاني

وسائل إثبات الجريمة الإلكترونية

على الرغم من وجود تشابه كبير بين التحقيق في جرائم الإنترنت وبين التحقيق في الجرائم الأخرى فهي جميعاً تحتاج إلى إجراءات تتشابه في عمومها مثل المعاينة والتفتيش والشهادة والخبرة بالإضافة إلى جمع الأدلة، كما أنها تشترك في كونها تسعى إلى الإجابة على الأسئلة المشهورة لدي المحقق، ماذاحدث؟ وأين؟ ومتى؟ وكيف؟ ومن؟ ولماذا ؟

الفرع الأول: المعاينة

يرى البعض أن أهمية المعاينة تتضاءل في الجريمة المعلوماتية، وذلك لندرة تخلف أثار مادية عند ارتكاب الجريمة المعلوماتية، كما أن طول فترة الوقوع بين وقوع الجريمة وارتكابها وبين اكتشافها يكون له تأثير السلبي على الآثار الناجمة عنها سواء بسبب العبث أو المحو أو التلف لتلك الآثار[1].

ويقصد بالمعاينة أنها رؤية العين لمكان أو شخص أو أي شيء لإثبات حالته و ضبط كل ما يلزم لكشف الحقيقة ، و يقصد بها كذلك أنها إثبات مادي و مباشر لحالة الشخص و الأشياء والأمكنة ذاتصلة بالحادث.[2]

كما يقصد بالمعاينة الكشف الحسي المباشر لإثبات حالة شيء أو شخص، وتتم إما بانتقال المحقق إلى مكان أخر أو يجلب موضوع المعاينة إلى مقره كما في معاينة العملات المزورة أو الأشياء و الأسلحة و الأوراق التي استخدمت في اقتراف الجريمة أو مكان و أثار الجريمة أو الكشف عن المجني عليه لإثبات آثار الجريمة من ضرب أو جرح أو قتل أو فحص المدعى عليه لإثبات حالته المرضية أو ما تعرض لهمن ضرب وتعذيب.

فالمعاينة وسيلة بواسطتها يتمكن القاضي من الإدراك المباشر للجريمة ومرتكبها وقد تشمل النتائج المادية التي تخلفت عنها أو إثبات حالة الأماكن أو الأشياء أو الأشخاص التي لها علاقة بالجريمة أو إثبات الوسيلة التي استخدمت في ارتكابها أو المكان الذي وقعت فيه الجريمة.[3]

وتتم المعاينة بأية حاسة من الحواس، مثل المس والسمع والبصر والشم والتذوق. والمعاينة قد تكون شخصية فتنصب الملاحظة على شخص، ويستوي أن تتناول المعاينة المجني عليه أو المتهم كما إذا كان الغرض منها إثبات أثار الإكراه بالمجني عليه في جريمة السرقة، وقد يكون موضوع المعاينة شخصا على قيد الحياة. وفي الجرائم المعلوماتية تكون فرصة الحصول على الدليل الإلكتروني ضئيلة مقارنة مع الجرائم الأخرى.

أما الجهة التي أسندت إليها المهمة الخاصة بإجراء المعاينة فهي الشرطة القضائية التي عليها فيحال علمها بارتكاب جناية أو جنحة أن تخبر بها النيابة العامة و أن تنتقل في الحال إلى مكان ارتكاب

[1] عبد الفتاح مراد، شرح جرائم الكمبيوتر والانترنت دار الكتب والوثائق المصرية – 2005 ، ص 65.

[2] هشام محمد رستم مرجع سابق، ص 39

[3] عبد الفتاح بيومى حجازي, مرجع سابق، ص 92

الجريمة من أجل إجراء المعاينة كما ينبغي على الشرطة القضائية أن تحافظ على الأدلة القابلة للاندثار والتحفظ على مكان الجريمة و المحافظة على كل ما قد يوصل إلى الحقيقة.[1]

وفي كل الأحوال عند تلقي بلاغ عن وقوع جريمة إحدى الجرائم الإلكترونية والتأكد من صحة الخبر و البيانات المتضمنة في الخبر، يتم الانتقال إلى مسرح الجريمة من أجل المعاينة، ومسرح الجريمة المعلوماتية يختلف عن المسرح الخاص بالجريمة التقليدية كالقتل والسرقة.

وإن كانت الجريمة واردة في كل الجرائم، إلا أن أهميتها تتضاءل في بعض الجرائم مثل جريمة التزوير المعنوي وجريمة السب فإن المعاينة فيها غير ذات جدوى، أما معاينة الجريمة التقليدية والاطلاع على مسرح الجريمة فيها فيكون ذات أهمية متمثلة في تصور كيفية وقوع الجريمة و ظروف ملابسات ارتكابها، إلا أن إجراء المعاينة في الجريمة الإلكترونية يتقيد بعدة ضوابط أهمها:[2]

– تصوير الحاسب الآلي والأجهزة الطرفية المتصلة به، على أن يتم تسجيل وقت وتاريخ ومكان التقاطها.

– قطع التيار الكهربائي من موقع المعاينة لشل فاعلية الجاني من القيام بأي فعل من شأنه التأثير أو محو الآثار.

– إخطار الفريق الذي سيتولى المعاينة قبل موعدها بوقت كافي حتى يستعد من الناحية الفنية والعملية،وذلك لكي يضع الخطة المناسبة لضبط أدلة الجريمة حال معاينتها.

التحفظ على مستندات الإدخال والمخرجات الورقية للحاسب ذات صلة بالجريمة.

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

الفرع الثاني: التفتيش

عرفت الأنظمة الجنائية في مراحل تطورها أنواعاً من الإجراءات تنطوي على انتهاك لحقوق الفرد الأولية في سبيل تتبع الجناة ومحاكمتهم ومنها القبض والتفتيش فإذا ما تخلت يد العدالة عن التعرض الحقوق الأفراد أصبحنا إزاء فوضى إجرامية.

[1] ريان محمد عادل، جرائم الحاسب الآلي وأمن البيانات، بيروت، 2002، ص 46

[2] عبد الفتاح بيومي حجازي، مرجع سابق، ص 93.

ويعتبر التفتيش إجراء من إجراءات التحقيق، يهدف إلى البحث عن أشياء تتعلق بالجريمة، وكل ما يفيد بصفة عامة في كشف الحقيقة، سواء تعلق بالأشخاص أو بالأماكن وللتفتيش شروط موضوعية تتعلق بـ[1]:

أ- **بسببه:** وقوع جريمة بالفعل تعد جناية أو جنحة، وأن يوجه اتهام إلى الشخص المراد تفتيشه أو تفتيش مسكنه.

ب الغاية منه: ضبط أشياء تفيد في كشف الحقيقة.

والشروط الشكلية تتحدد بـ :

أ- أن يكون الأمر بالتفتيش مسببا.

ب- حضور المتهم أو من ينيبه أو الغير أو من ينيبه التفتيش.

ج تحرير محضر بالتفتيش.

ويثور السؤال عن إمكانية التفتيش وفقا للضوابط السابقة والغاية منه في مجال الجرائم الإلكترونية ؟ والغرض من هذا السؤال يتضح من أن التفتيش بالمعنى التقليدي يهدف إلى حفظ أشياء مادية تتعلق بالجريمة وتفيد في كشف الحقيقة، بينما البيانات الإلكترونية ليس لها بحسب جوهرها مظهر مادي ملموس في العالم الخارجي، ومع ذلك فيمكن أن يرد التفتيش على هذه البيانات غير المحسوسة عن طريقالوسائط الإلكترونية لحفظها وتخزينها كالأسطوانات والأقراص الممغنطة، ومخرجات الحاسب.

ولهذا فقد أجاز الفقه والتشريعات التي صدرت في هذا المجال إمكانية أن يكون محل لتفتيش البيانات المعالجة آليا، والمخزنة بالحاسب الآلي، ثم ضبطها والتحفظ عليها، أو ضبط الوسائط الإلكترونية التي سجلت عليها هذه البيانات والتفتيش في هذه الحالة يخضع لما يخضع له التفتيش بمعناه التقليدي من ضوابط وأحكام، فالتفتيش أو البحث في الشبكات الإلكترونية يسمح باستخدام الوسائل الإلكترونية للبحثفي أي مكان عن البيانات أو الأذلة المطلوبة.[2]

ومحل التفتيش وما يتبعه من ضبط يشمل البرامج أو الكيانات المنطقية Les logiciels . البيانات المسجلة في ذاكرة الحاسب أو في مخرجاته – السجلات المثبتة الاستخدام نظام المعالجة الآلية للبيانات – دفتر يومية التشغيل وسجل المعاملات – السجلات الخاصة بعمليات الدخول إلى نظام المعالجة الآلية

[1] منى الأشق، القانون والانترنت " تحدي التكيف والضبط "، بيروت، الناشر ش م م مصر، 2008، ص 70 .

[2] أمير فرج يوسف، مرجع سابق ص33

للبيانات، ويتعلق بها من سجلات كلمات السر، ومفاتيح الدخول، ومفاتيح فك الشفرة، ونظرا لكون التفتيش يتضمن تقييداً للحرية الفردية ويمثل اعتداء على حرمة الحياة الخاصة فيجب أن تتوافر فيه الضمانات القانونية اللازمة لصحته ومنها أن يتم صدور أمر قضائي مسبب بشأنه وأن يباشره الشخص أو الجهة المختصة (النيابة العامة، أو الشرطة القضائية).

ويحسب الأصل يجب أن يصدر إذن التفتيش مكتوباً إلا أن هذا الشرط يحمل بعض المخاطر أحيانا وذلك في حالة ما إذا كان البحث عن أدلة الجريمة يستدعي أن يتم التفتيش في مكان آخر في نظام معلوماتي آخر غير الذي صدر بشأن الإذن المكتوب صدر والمخاطر تتمثل في إمكانية قيام الجاني بتدمير، أو محو البيانات، أو نقلها، أو تعديلها، خلال الفترة التي يراد الحصول على إذن مكتوب بشأنها.

ولمواجهة هذه المخاطر، يرى البعض أن الإذن الأول بالتفتيش في مكان ما يجب أن يتضمن الإذن بتفتيش أي نظام معلوماتي آخر يوجد في أي مكان غير مكان البحث[1].

ويثير امتداد الإذن بالتفتيش إلى أماكن أو أنظمة أخرى غير الواردة في الإذن الأول بعض المشكلات، يتعلق أولها برفض صاحب المكان أو النظام الآخر مباشرة التفتيش لديه، يرى البعض فيهذه الحالة عدم استمرار أو امتداد البحث لديه إلا في حالتي التلبس، أو رضائه بالتفتيش.

ويرى البعض أنه في حالة امتداد الاختصاص، فيمكن أن يصدر الأمر بالإمداد شفويا من قاضي التحقيق، تحقيقا للسرعة المطلوبة، ثم يصدر فيما بعد الإذن المكتوب، وفي جميع الأحوال يجب أن يكون الإذن مسببا، لتتمكن الجهة القضائية من مراقبة مدى مشروعيته.[2]

وعموما فالتفتيش في الجرائم المعلوماتية يكون محله كل مكونات الحاسب الآلي سواء كانت مادية أو معنوية، وكذلك شبكات الاتصال الخاصة به، بالإضافة إلى الأشخاص الذين يستخدمون الحاسب الآلي محل التفتيش وتشمل جميع مكوناته، ويستلزم تفتيش الحاسب الآلي مجموعة من الأشخاص لديهم الخبرة والمهارة التقنية

[1] سلامى جلال، ففي حسين، الأدلة المتحصلة من الحاسوب وحجيتها في الإثبات الجنائي، د.ط، دار الكتب القانونية، مصر 2012، ص 113.

[2] عائشة بن قارة مصطفى، حجية الدليل الالكتروني في مجال الإثبات الجنائي دار الجامعة الإسكندرية – 2010، ص 76.

الفرع الثالث: الشهادة

يقصد بالشهادة بأنها تقرير الشخص لما يكون قد رأه أو سمعه بنفسه أو أدركه على وجه العموم بالحواس ويقصد بالشاهد في جرائم المعلوماتية بأنه الشخص الفني صاحب الخبرة المعلوماتية والتخصص في تقنية وعلوم الحاسب الآلي وشبكاته ويطلق على هذا النوع من الشهود مصطلح الشاهد المعلوماتيle témoin informatique تمييزا له عن الشاهد التقليدي. ويشمل الشاهد في الجرائم المعلوماتية عدة طوائف أهمها[1]:

1- القائم على تشغيل الحاسب الآلي : و هو المسئول عن تشغيل الحاسب الآلي و المعدات المتصلة به و يجب أن تكون لديه الخبرة الكبيرة في استخدام الجهاز كما يجب أن تكون لديه معلومات عن قواعد كتابة البرامج.

2 – المبرمجون: وهم الأشخاص الذين يأخذون على عاتقهم كتابة البرامج، وينقسمون إلى فئتين:

الفئة الأولى: هم مخططو البرامج التطبيقية و يقومون بالحصول على خصائص النظام المطلوب.

الفئة الثانية: وهم مخططو برامج النظم و يقومون باختيار و تعديل و تصحيح برامج النظام الحاسبالداخلية و إدخال أي تعديلات أو إضافات لها.

3- مهندسو الصيانة و الاتصالات: و هم المسئولون عن أعمال الصيانة الخاصة بتقنيات الحاسب وبمكوناته وشبكات الاتصال المتعلقة به.

4- المحللون : وهم الأشخاص الذين تأتي على عاتقهم مهمة التحليل الخاصة ببيانات نظام معين إلى وحدات مفصلة واستنتاج العلاقة الوظيفية منها، كما يقومون كذلك بتتبع البيانات داخل النظام عن طريق ما يسمى بمخطط تدفق البيانات واستنتاج الأماكن التي يمكن ميكنتها بواسطة الحاسب الآلي.

5- مديرو النظم: وهم الذين يوكل لهم أعمال الإدارة في النظم المعلوماتية.

6- طاقم عمليات البيانات: الذي يعد البيانات بالصورة التي يستطيع الكمبيوتر قراءتها (شريط أواسطوانة).

[1] سامى جلال حسين ، مرجع سابق، 118 ص.

7- **مهندس الصيانة الإلكترونية:**الذي يقوم على صيانة الجهاز الأصلي والتأكد من عمله بصورةصحيحة.

يتعين على الشاهد المعلوماتي أن يقدم إلى سلطات التحقيق ما يحوزه من معلومات جوهرية لازمة للولوج في نظام المعالجة الآلية للبيانات سعيا عن أدلة الجريمة بداخله، والسؤال الذي يطرح نفسه هل يلتزم الشاهد بطبع الملفات والإفصاح عن كلمات المرور والشفرات؟ هناك اتجاهان في هذا الصدد:

الاتجاه الأول: ويرى أنه ليس من واجب الشاهد وفقا للالتزامات التقليدية للشهادة أن يقوم بطبع ملف البيانات أو الإفصاح عن كلمة المرور أو الشفرات الخاصة بالبرامج المختلفة ويميل إلى هذا الاتجاه الفقه الألماني حيث يرى عدم التزام الشاهد بطبع البيانات المخزنة في ذاكرة الحاسب على أساس أن الالتزام بأداء الشهادة لا يتضمن هذا الواجب، وكذلك لا يجوز في تركيا إكراه الشاهد لحمله على الإفصاح عنكلمات المرور السرية أو كشف شفرات تشغيل البرامج المختلفة.[1]

الاتجاه الثاني: ويرى أنصار هذا الاتجاه أن من بين الالتزامات التي يتحمل بها الشاهد القيام بطبع ملفات البيانات أو الإفصاح عن كلمات المرور أو الشفرات الخاصة بالبرامج المختلفة حيث يرى اتجاه في الفقه الفرنسي أن القواعد العامة في مجال الإجراءات تحتفظ بسلطانها في مجال الإجراءات المعلوماتية ومن ثم يتعين على الشهود من حيث المبدأ الالتزام بتقديم شهادتهم المواد 62 109، 138 من قانون الإجراءات الجنائية الفرنسية ومن ثم يجب عليهم الإفصاح عن كلمات المرور السرية التي يعلمونها،ولكن رفض إعطاء المعلومات المطلوبة غير معاقب عليه جنائيا إلا في مرحلة التحقيق والمحاكمة.[2]

المطلب الثالث

بعض النماذج التطبيقية للجريمة الإلكترونية

[1] أمير فرج يوسف، مرجع سابق، ص41

[2] محمد عادل ريان، مرجع سابق، ص 58

الجرائم الإلكترونية تشكل طيفاً واسعاً من الأنشطة غير القانونية التي تتنوع في أهدافها وأساليبها.فيما يلي بعض النماذج البارزة لأنواع مختلفة من هجمات الجرائم الإلكترونية:

1. هجمات البرمجيات الخبيثة

هجوم البرمجيات الخبيثة هو إصابة نظام الكمبيوتر أو الشبكة بفيروس كمبيوتر أو أي نوع آخر من البرمجيات الخبيثة، ويمكن لمجرمي الإنترنت استخدام الكمبيوتر الذي اخترقوه بالمبرجيات الخبيثة لعدة أغراض، من بينها سرقة البيانات السرية واستخدام الكمبيوتر لتنفيذ أعمال إجرامية أخرى أو التسبب في إتلاف البيانات.

من الأمثلة الشهيرة على هجوم برمجية الفدية الخبيثة WannaCry، وهي جريمة إلكترونية عالمية حدثت في مايو 2017. كان WannaCry نوعًا من برامج الفدية، وهي برامج خبيثة تُستخدم في الابتزاز وأخذ الأموال عن طريق الاحتفاظ ببيانات الضحية أو جهازه وعدم إرجاعهما إلا مقابل فدية. استهدف برنامج الفدية هذا ثغرة أمنية في أجهزة الكمبيوتر التي تعمل بنظام التشغيل Microsoft Windows.

عندما وقع هجوم برنامج الفدية WannaCry، تأثر 230 ألف جهاز كمبيوتر في 150 دولة به! تعذر على المستخدمين الوصول إلى ملفاتهم، وتلقى كل مستخدم رسالة تطلب منه دفع فدية بعملة البتكوين من أجل استعادة الوصول إلى ملفاته.

وعلى الصعيد العالمي، سببت جريمة WannaCry الإلكترونية خسائر مالية قُدّرت بما يصل إلى 4 مليار دولار. لا يزال هذا الهجوم –حتى يومنا هذا– مشهورًا بسبب انتشاره وتأثيره.[1]

2. التصيد الاحتيالي

حملة التصيد الاحتيالي يتم فيها إرسال رسائل بريد إلكتروني عشوائية أو غيرها من أشكال التواصل بهدف خداع المستلمين لفعل بشيء يخترق أمنهم. قد تحتوي رسائل حملات التصيد الاحتيالي على مرفقات بها برمجيات خبيثة أو روابط لمواقع ضارة، أو قد تطلب من مستلمها الرد بمعلومات سرية.

حدث أحد الأمثلة الشهيرة لعمليات التصيد الاحتيالي أثناء كأس العالم 2018. وفقًا لتقريرنا احتيال كأس العالم 2018، تضمنت هذه العملية رسائل بريد إلكتروني تم إرسالها إلى مشجعي كرة القدم عن كأس العالم 2018. حاولت رسائل البريد الإلكتروني العشوائية هذه إغراء المشجعين برحلات مجانية

[1] VICKY NGO-LAM ،"Cyber Crime: Types, Examples, and What Your Business Can Do" ، www.exabeam.com, up loaded : 24-12-2019, Retrieved 13-2-2021.

مزيّفة إلى موسكو حيث تمت استضافة كأس العالم، وتمت سرقة البيانات الشخصية الخاصة بالأشخاص الذين فتحوا رسائل البريد الإلكتروني هذه والضغط على الروابط الواردة فيها.

هناك نوع آخر من حملات التصيد الاحتيالي معروف باسم التصيد بالحربة. هذه هي حملات التصيد الاحتيالي المستهدفة التي تحاول خداع أفراد معيّنين لتعريض أمن المؤسسة التي يعملون فيها للخطر.

على عكس حملات التصيد الاحتيالي العادية التي تعتبر عامة جدًا من حيث الأسلوب، يتم في العادة تصميم رسائل التصيد بالحربة لتبدو وكأنها رسائل من مصدر موثوق. على سبيل المثال: يتم تصميمها لتبدو كأنها من المدير التنفيذي أو مدير تكنولوجيا المعلومات، وقد لا تحتوي على أي دلالة بصرية على كونها زائفة.[1]

3. هجمات الحرمان من الخدمات الموزَّعة

هجمات الحرمان من الخدمات الموزَّعة (DDoS) هي إحدى أنواع هجمات الجرائم الإلكترونية التي يستخدمها المجرمون الإلكترونيون في إسقاط نظام أو شبكة. يتم أحيانًا استخدام أجهزة إنترنت الأشياء المتصلة (IoT) في شن هجمات الحرمان من الخدمات.

يتسبب هجوم الحرمان من الخدمات في إرباك النظام باستخدام أحد بروتوكولات الاتصال القياسية التي يستخدمها لإرسال البريد العشوائي إلى النظام بطلبات الاتصال. وقد يستخدم المجرمون الإلكترونيون الذين ينفّذون الابتزاز الإلكتروني التهديد بهجوم الحرمان من الخدمات للمطالبة بالمال. بدلاً من ذلك، يمكن استخدام هجوم الحرمان من الخدمات كأسلوب إلهاء أثناء وقوع نوع آخر من الجرائم الإلكترونية.

من الأمثلة الشهيرة لهذا النوع من الهجمات هو هجوم الحرمان من الخدمات لعام 2017 على موقع UK National Lottery. أدى هذا الهجوم إلى قطع اتصال موقع اليانصيب على الإنترنت وتطبيق الجوال بالإنترنت، مما منع مواطني المملكة المتحدة من اللعب. لا يزال سبب الهجوم غير معروف، إلا أنه يُشتبه في أن الهجوم كان محاولة لابتزاز اليانصيب الوطني.[2]

4. الاحتيال المالي عبر الإنترنت: اختراق

[1] VICKY NGO–LAM, op.cit.

[2] VICKY NGO–LAM, op.cit.

في يوليو 2017، أعلنت شركة "Equifax"، إحدى أكبر شركات الائتمان في الولايات المتحدة، عن تعرضها لاختراق ضخم أدى إلى تسريب بيانات شخصية حساسة لحوالي 147 مليون شخص. تضمنت البيانات المسربة أسماء، تواريخ ميلاد، أرقام ضمان اجتماعي، وعناوين. هذا الاختراق أثار موجة من الانتقادات للشركة بسبب تأخرها في الإعلان عن الحادث وبسبب ضعف أنظمتها الأمنية. الحادثة كشفت عن حجم المخاطر المرتبطة بحفظ المعلومات الحساسة على الأنظمة الرقمية وأكدت الحاجة الماسة لتطبيق معايير أمنية صارمة لحماية البيانات الشخصية.[1]

5. الهجمات على البنية التحتية الحيوية:

في مايو 2021، تعرضت شركة "Colonial Pipeline"، التي تدير أكبر شبكة أنابيب لنقل الوقود في الولايات المتحدة، لهجوم سيبراني ببرنامج الفدية نفذته مجموعة قراصنة معروفة باسم "DarkSide". أدى الهجوم إلى شلّ عمليات الشركة وتوقف نقل الوقود على طول الساحل الشرقي للولايات المتحدة، مما أثار ذعرًا واسعًا ونقصًا في الوقود في عدة مناطق. الشركة اضطرت لدفع فدية تقارب 4.4 مليون دولار لاستعادة السيطرة على أنظمتها. هذه الحادثة أظهرت كيف يمكن للهجمات السيبرانية على البنية التحتية الحيوية أن تؤدي إلى تأثيرات كبيرة على الاقتصاد والأمن القومي، مؤكدة على ضرورة تعزيز الدفاعات السيبرانية لهذه المنشآت الحيوية.[2]

[1] VICKY NGO–LAM, ibdem.

[2] idim

خلاصة الفصل:

في هذا الفصل، تم استعراض الجوانب العملية لمكافحة الجريمة الإلكترونية من خلال تحليل آليات القانون المقارن والإجراءات التطبيقية المعتمدة في مختلف الدول. بدأنا بدراسة وسائل الكشف عن الجرائم الإلكترونية وأهمية تطوير تقنيات متقدمة للكشف المبكر عن هذه الجرائم. تناولنا دور بعض التشريعات المقارنة في توفير الحماية الجزائية وتعزيز العقوبات الرادعة للمجرمين الإلكترونيين. كما تم التركيز على أهمية التعاون التشريعي الدولي والإقليمي، حيث يُعَد التعاون بين الدول أمرًا حيويًا لمواجهة التهديدات العابرة للحدود.

وتم التعمق في الجانب الإجرائي والتطبيقي لكشف الجريمة الإلكترونية، بدءًا من التسرب الإلكتروني واعتراض المراسلات والمراقبة الإلكترونية، وصولاً إلى كشف الجريمة المعلوماتية من خلال تحليل المعطيات. كما تم تناول وسائل إثبات الجريمة الإلكترونية من خلال المعاينة، التفتيش، والشهادة، مما يوضح الإجراءات العملية المتبعة لتقديم الأدلة القاطعة أمام القضاء.

أخيرًا، تطرقنا الى بعض النماذج التطبيقية للجريمة الإلكترونية، مما يسلط الضوء على التحديات العملية التي تواجه الجهات المعنية في مواجهة هذه الجرائم. من خلال هذه الدراسة، تبين أن مكافحة الجريمة الإلكترونية تتطلب تكاملًا بين التكنولوجيا الحديثة والتشريعات الفعالة، بالإضافة إلى تعاون دولي وثيق لضمان بيئة رقمية آمنة.

خاتمة

و في ختام هذا الموضوع توصلنا الى مجموعة من النتائج و التوصيات مع تزايد استخدام شبكة الإنترنت وتطورها، ومع وجود اختلافات في الفهم والمستوى العلمي بين المستخدمين، ظهرت ممارسات غير مشروعة على هذه الشبكة. فأصبحت الإنترنت وسيلة لارتكاب أو مكانًا لتلك الممارسات غير القانونية، حسب الحالة. وهذا أدى إلى ظهور طائفة جديدة من الجرائم تعبر الحدود، تختلف عن الجرائم التقليدية، وأطلق عليها اسم "الجرائم الإلكترونية". وبالتالي، أصبح واضحًا لنا مدى خطورة تحول الإنترنت إلى منصة لممارسة أعمال تتعارض مع القيم والأخلاقيات العامة.

لقد تطرقنا في هذه الدراسة إلى آليات مكافحة الجريمة الإلكترونية في القانون المقارن، يمكن القول إن التحديات الناجمة عن الجرائم الإلكترونية تتزايد بسرعة مع تقدم التكنولوجيا وتعمق الانتشار الرقمي. حيث تضمنت الدراسة استعراضًا شاملاً لوسائل الكشف عن الجرائم الإلكترونية، ودور التشريعات المقارنة في الحماية الجزائية، وأهمية التعاون التشريعي الدولي والإقليمي، إلى جانب التحليل العملي والإجرائي لمعالجة هذه الجرائم. كما استعرضت الدراسة نماذج عملية لتطبيق القوانين وسبل إثبات الجرائم الإلكترونية والتقنيات المستخدمة في التحقيق والمحاكمة.

النتائج:

- يعتبر المجتمع الجزائري كغيره من المجتمعات من المتضررين من شيوع الجرائم الإلكترونية؛
- اصطلح المشرع الجزائري على تسمية الجرائم الإلكترونية بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال وعرفها بموجب القانون 04-09 المؤرخ في 05 أوت 2009 على أنها جرائم المساس بأنظمة المعالجة الآلية للمعطيات الآلية المحددة في قانون العقوبات وأية جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام الاتصالات الإلكترونية؛
- لا تختلف الجريمة الإلكترونية رغم ارتكابها على الفضاء الافتراضي عن الجريمة العادية في اشتراط توفر أركان لقيامها. فلها ركن معنوي وركن مادي وركن تشريعي وكل نوع منها يختص بميزة عن جريمة أخرى؛
- تأخذ الجرائم الإلكترونية صورا متعددة وكل صورة من هذه الصور تثير مشكلات موضوعية وإجرائية؛
- آليات المكافحة الحالية غير كافية لمجابهة الجريمة الإلكترونية، فلا يمكن لأي دولة مهما بلغ تطورها التكنولوجي والمعلوماتي أن تتصدى لهذه الجريمة العالمية بمفردها، فالمجرم الإلكتروني قد يكون في دولة ما وينفذ جريمته الإلكترونية في دولة ثانية، وبالإمكان أن تتحقق نتيجتها في دولة ثالثة، أو حتى في عدة دول، مما يُصعب عملية متابعته خاصة في حالة عدم وجود اتفاقية بين

الدولة التي يتواجد على أرضها والدولة المطالبة به، وعليه فإن آليات المكافحة المخصصة من طرف بعض الدول تعد غير كافية للتصدي للجريمة الإلكترونية؛

- شكلت الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها محور اهتمام العديد من السلطات، مما أدى إلى تعاقب السلطات على ترأسها؛ بداية من وزارة العدل سنة 2015 ، ثم وزارة الدفاع الوطني سنة 2019 ، لتوضع تحت سلطة رئيس الجمهورية.

الاقتراحات

ومما سبق يمكن أن نخرج بمجموعة من التوصيات نذكرها فيما يلي:

- نناشد المشرع الجزائري بإصدار قانون خاص بمكافحة الجرائم الإلكترونية، وإرفاقه بالآليات الإجرائية والمؤسساتية الكفيلة التي تسهل تلك المكافحة.
- فقد كشفت الدراسة عن ضرورة ملحة لتحسين التشريعات والسياسات الجنائية في مختلف الدول لمواكبة هذا التطور السريع ومكافحة الجرائم الإلكترونية بفعالية.
- لا بد من تفعيل آليات التعاون الدولي التي تتسم بسرعة التنفيذ حتى لا يترك للمجرم الإلكتروني ملاذاً آمناً يلتجئ إليه، وتوسيع الاتفاقيات الدولية الثنائية والجماعية لمكافحة الجرائم الإلكترونية.
- يتعين على الدولة حجب المواقع المخالفة للقوانين والأخلاق، وخاصة تلك التي تستهدف الأطفال، لأنه ورغم كثرة البرامج المخصصة لهذا الشأن إلا أنها لم تجْد نفعاً، ذلك أن تلك البرامج قد تصعب عملية التحميل العادية، وتبطئ من سرعة الانترنت، إضافة إلى قيام أصحاب تلك المواقع بتغيير عنوان الويب الخاص بها بشكل مستمر، مما يحول دون ملاحقة تلك المواقع وحجبها.
- نظراً لكثرة الجرائم الإلكترونية وتنوعها، يستحسن إنشاء شرطة متخصصة بهذه الجرائم، تكون مهمتها الوحيدة متابعة مثل هذا النوع من الجرائم.
- إنشاء محكمة جنائية دولية تحت مظلة الأمم المتحدة يكون لها صلاحية النظر في القضايا التي تعنى بالجرائم الإلكترونية الخطيرة ذات الطابع الدولي.

قائمة المصادر والمراجع

مراجع باللغة العربية

أولا: الكتب

أحمد خليفة الملط، الجرائم المعلوماتية: دراسة مقارنة، دار الفكر الجامعى،الإسكندرية، 2005

أحمد فتحي سرور، الوسيط في قانون العقوبات / القسم العام، الطبعة الخامسة دار النهضة العربية، القاهرة، 1991.

أيمن عبد الحفيظ الاتجاهات الفنية والأمنية لمواجهة الجرائم المعلوماتية، دون ذكر دار النشر، دون ذكر بلد النشر.

البشري، محمد الأمين، التحقيق في جرائم الحاسب الآلي، دار الكتب القانونية، مصر،2009.

الجبور محمد، الوسيط في قانون العقوبات، القسم العام، دار وائل، عمان، ط1، 2012.

جعفر حسن حاسم الطالبي، جرائم تكنولوجيا المعلومات، رواية جديدة للحريقة المعلوماتية، دار البداية، عمان، 2007.

جمال نجيمي، إثبات الجريمة على ضوء الإجتهاد (دراسة مقارنة)، دار هومة، الجزائر، 2011.

جميل عبد الباقي الصغير، القانون الجنائي والتكنولوجيا الحديثة، الكتاب الأول، الجرائم الناشئة عن استخدام الحاسب الآلي، الطبعة الأولى، منشورات دار النهضة العربية، القاهرة، 1992.

حسني، محمود نجيب، النظرية العامة للقصد الجنائي، دار النهضة العربية، ط2، 1971.

حنان ريحان مبارك المضحكي، الجرائم المعلوماتية دراسة مقارنة، منشورات الحلبي الحقوقية، بيروت،2014

خالد حسن أحمد لطفي، جرائم الأنترنت بين القرصنة الالكترونية وجرائم الابتزاز الالكتروني، دار الفكر الجامعي الإسكندرية، د ذ ط ، 2019.

خالد ممدوح ابراهيم، الجرائم المعلوماتية، ط1، دار الفكر الجامعي، الإسكندرية، 2009

رشيدة بوكر، جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري والمقارن، منشورات الحلبي الحقوقية، بيروت، لبنان، 2012.

ريان محمد عادل، جرائم الحاسب الآلي وأمن البيانات، بيروت، 2002

سلامى جلال، ففي حسين الأدلة المتحصلة من الحاسوب وحجيتها في الإثبات الجنائي درط دار الكتب القانونية مصر 2012.

شيخ ناجية، أساليب البحث والتحري المتخذة في القانون رقم ،22/06، المعدل والمتمم لقانون الإجراءات الجزائية الجزائري، المجلة النقدية، 2017.

طارق إبراهيم الدسوقي عطية، الأمن المعلوماتي النظام القانوني لحماية المعلوماتية، دار الجامعة الجديدة للنشر، الإسكندرية ، 2009.

عامر محمود الكسواني، التزويز المعلوماتي للعلامة التجارية، دار الثقافة للنشر والتوزيع، الأردن،2014.

عائشة بن قارة مصطفى حجية الدليل الالكتروني في مجال الإثبات الجنائي دار الجامعة الإسكندرية – 2010.

عبد الفتاح بيومي حجازي، نحو صياغة نظرية عامة في علم الجريمة والمجرم المعلوماتي، دار بهجات للطباعة والتجليد، مصر، ط 1 2009.

عبد الفتاح بيومي حجازي، نحو صياغة نظرية عامة في علم الجريمة والمجرم المعلوماتي، دار بهجات للطباعة والتجليد، مصر، ط 1 2009

عبد الفتاح مراد شرح جرائم الكمبيوتر والانترنت دار الكتب والوثائق المصرية – 2005.

عبد الله عبد الله عبد الكريم، الملكية الفكرية على شبكة الانترنت، دار الجامعة الجديدة للنشر، لاسكندرية ، 2008.

عوض، محمد محيي الدين، مشكلات السياسة الجنائية المعاصرة في جرائم نظم المعلومات، دار الفكر العربي القاهرة، ط1، 2011.

غائم مرضي الشمري، الجرائم المعلوماتية، ماهيتها خصائصها، كيفية التصدي لها قانونا، د.د.ن ، د.ط.

فايز الظفيري، الأحكام العامة للجريمة الإلكترونية، مجلة العلوم القانونية والاقتصادية، كلية الحقوق، جامعة عين شمس، مصر،العدد 2، 2002.

الفتاح بيومي حجازي، الإثبات الجنائي في جرائم الكومبيوتر والانترنت دار الكتب القانونية، 2007.

الفتاح بيومي حجازي، الإثبات الجنائي في جرائم الكومبيوتر والانترنت دار الكتب القانونية، 2007.

فدوي عمارة، ،2010 اعتراض المراسلات وتسجيل الأصوات كإجراء قضائي في المواد الجنائية، مقال منشور بمجلة العلوم الإنسانية، العدد 33.

كامل السعيد ، شرح الأحكام العامة في قانون العقوبات الأردني والقانون المقارن، الطبعة الثانية، دار الفكر للنشر والتوزيع ، عمان، 1983.

محمد عبيد الكعبي، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الإنترنت: دراسة مقارنة، دار النهضة العربية،القاهرة، 2009.

محمود نجيب حسني، شرح قانون العقوبات / القسم العام، الطبعة السادسة، دار النهضة العربية، القاهرة.

محمود نجيب حسني، شرح قانون العقوبات / القسم العام، الطبعة السادسة، دار النهضة العربية، القاهرة.

مصطفى يوسف كافي، جرائم الفساد غسيل الأموال السياحة الارهاب الالكتروني المعلوماتية، مكتبة المجتمع العربي للنشر والتوزيع، الأردن ، ط1، 2014.

منى الأشقر، القانون والانترنت " تحدي التكيف والضبط " ، بيروت ، الناشر ش م م، مصر، 2008.

موسى، مصطفى محمد (2010) دليل التحري عبر شبكة الإنترنت، دار الكتب القانونية، مصر.

نائلة عادل فريد قورة ، جرائم الحاسب الاقتصادية، دراسة نظرية تطبيقية، دار النهضة العربية الإسكندرية، 2004.

نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية، منشورات الحلبي الحقوقية، بيروت، لبنان، ط1، 2005.

نهلا عبد القادر المومني، الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، الطبعة الثانية، 2001.

هشام فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة، أسيوط، 1994.

ثانيا: رسائل دكتوراه ومذكرات ماستر

بعرة سعيد، الجريمة الإلكترونية في التشريع الجزائري، رسالة لنيل الماستر في الحقوق، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، 2015-2016.

عمر محمد أبو بكر يونس، الجرائم الناشئة عن استخدام الانترنت، الأحكام الموضوعية والجوانب الإجرائية، رسالة دكتوراه، جامعة عين شمس، دار النهضة العربية، القاهرة، 2004.

ثالثا: مداخلات ومقالات

أميرة حوالف، معالم الجريمة المعلوماتية في القانون الجزائري. مجلة البحوث القانونية والسياسية، المجلد 03 ، العدد 16، 12 فيفري 2021.

حسين صالح دويب، القوانين العربية وتشريعات تجريم الجرائم الإلكترونية وحماية المجتمع، المؤتمر السادس الجمعية المكتبات والمعلومات السعودية، 06 أفريل 2010.

ذباب البدايئة ، جرائم الحاسب والانترنت، أبحاث الندوة العلمية لدراسة الظواهر الإجرامية المستحدثة وسبل مواجهتها، أكاديمية نايف العربية للعلوم الأمنية 2009.

الرواشدة سامي، الهياجنة أحمد، مكافحة الجريمة المعلوماتية بالتجريم والعقاب، المجلة الأردنية في القانون والعلوم السياسية، جامعة مؤتة – الأردن، المجلد (1)، العدد (3)، 2009.

سميحة بلقاسم، حميد بوشوشة، الجريمة الإلكترونية بعد جديد للإجرام في الجزائر.واقعها وآليات مجابهتها، مجلة العلوم الإنسانية لجامعة أم بواقي، 2023/01/18.

سمير بارة، الأمن السيبراني Cyper Security في الجزائر : السياسات والمؤسسات المجلة الجزائرية للأمن الإنساني، جويلية 2017.

م ش، المصلحة المركزية للجريمة الإلكترونية في مواجهة مجرمي العالم الإفتراضي، تاريخ الإسترداد 2021/02/08، بتاريخ 2016/02/13، تم الاطلاع عليه بتاريخ 2024/06/24 على الساعة: 21:06.

معاشي، سميرة، ماهية الجريمة المعلوماتية، بحث منشور في مجلة المنتدى القانوني، العدد السابع، جامعة محمد خيضر بسكرة، الجزائر، 2011.

معزيز أمينة، التسرب في قانون الإجراءات الجزائية الجزائري، مقال منشور في مجلة القانون والمجتمع، العدد11، 2019.

يونس عرب صور الجرائم الإلكترونية واتجاهات تبويبها، ورقة عمل مقدمة ضمن ورشة عمل تطوير التشريعات في مجال مكافحة الجرائم الإلكترونية، هيئة تنظيم الاتصالات، مسقط، سلطة عمان يومي 2 و 4 أفريل، 2006.

رابعا: دورات وإتفاقيات:

الدورة التاسعة عشرة لمجلس وزراء العدل العرب بالقرار رقم 495 – 19 8/10/2003.

الدورة الحادية والعشرين لمجلس وزراء الداخلية العرب بالقرار رقم 417 – د 21/2004.

الاتفاقية الأوربية لجرائم الانترنت في بودابست بدولة المجر بتاريخ 2001/11/23.

خامسا: أوامر قوانين ومراسيم

الأمر رقم ،155/66 المؤرخ في 08جوان ،1966، المتضمن قانون الإجراءات الجزائية المعدل والمتمم.

قانون الجزاء الكويتي.

قانون العقوبات الأردني.

قانون العقوبات الفرنسي.

قانون المعالجة الإلكترونية والحريات الفرنسي.

قانون جرائم أنظمة المعلومات الأردني رقم (30) لسنة 2010م.

القانون رقم ،01/06 المؤرخ في 20 فبراير ،2006 المتعلق بالوقاية من الفساد ومكافحته، الجريدة الرسمية للجمهورية الجزائرية، العدد،14، الصادرة في 08 مارس 2006.

القانون رقم 09/04 المؤرخ في 05 أوت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

القانون رقم 20/05، المتعلق بالوقاية من التمييز وخطاب الكراهية، المؤرخ في 28 أبريل ،2020 الجريدة الرسمية للجمهورية الجزائرية، العدد 25، الصادرة في 29 أبريل 2020.

القانون رقم 09 – 04 مؤرخ في 5 أوت سنة 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

القانون الاسترشادي العربي الموحدالمقرر سنة 2003،المتضمن مكافحة سوء استخدام تكنولوجيا المعلومات والاتصال.

المرسوم الرئاسي رقم ،261/15، المؤرخ في 08 أكتوبر 2015، المحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، الجريدة الرسمية للجمهورية الجزائرية، العدد 53، الصادرة في 08 أكتوبر 2015.

المرسوم الرئاسي رقم 442/20، المؤرخ في 30 ديسمبر 2020، المتعلق بإصدار التعديل الدستوري المصادق عليه في استفتاء 01 نوفمبر 2020، الجريدة الرسمية للجمهورية الجزائرية، العدد 82، الصادرة في 30 ديسمبر 2020.

مراجع باللغة الفرنسية

Alain Bensoussan, L'informatique et le droit. Memento Guide. édition Hermes, Paris, France, Tome 1, 1994.

Mascala corinne, Travaux de l'association «criminalité et contrat électronique», journées national Henir CAPITANT, paris, 2000.

Nidal El Chaer, La Criminalité Informatique Devant La Justice Pénale, édition juridique sader, Beyrouth, Liban, 2004.

Redouane Semlali, art-Cit,p.40, voir aussi. Frédérique Chopin, Les politiques publiques de lutte contre la cybercriminalité. Actualité Juridique Pénal, Editions Dalloz, 2009.

قائمة المحتويات

ملخص:

تهدف هذه الدراسة إلى فهم ظاهرة الجرائم الإلكترونية فهمًا معمقًا وتعريفها في القانون الجزائري والتشريعات المقارنة، ومن ثم الوقوف على خصائصها وأركانها وأنواعها. تتناول الدراسة سبل مكافحة الجريمة الإلكترونية على المستوى الوطني،عبر استعراض الأجهزة والتشريعات المسخرة من قبل الجزائر وبعض الدول للحد من هذه الظاهرة.

كما تتطرق إلى الجهود الدولية من خلال المؤتمرات والاتفاقيات الدولية المخصصة لمكافحة الجرائم الإلكترونية.

وقد جاءت نتائج الدراسة لتشير لضرورة تفعيل آليات التعاون الدولي حتى لا يترك للمجرم الإلكتروني ملاذاً آمناً يلتجئ إليه، وحجب المواقع المخالفة للقوانين والأخلاق، وبالأخص إنشاء شرطة متخصصة بهذه الجرائم.

كلمات مفتاحية:

الجريمة الإلكترونية، القانون المقارن، التشريعات الوطنية، مكافحة الجريمة الإلكترونية

Abstract:

This study aims to deeply understand the phenomenon of cybercrime and define it within Algerian law and comparative legislation. It then examines its characteristics, elements, and types. The study explores methods of combating cybercrime on a national level by reviewing the mechanisms and legislation employed by Algeria and other countries to curb this phenomenon. It also addresses international efforts through conferences and international agreements dedicated to combating cybercrime.

The study's findings indicate the necessity of activating international cooperation mechanisms to ensure that cybercriminals have no safe haven to retreat to, blocking websites that violate laws and ethics, and specifically establishing specialized police forces for these crimes.

Key words:

Cybercrime, Comparative law, National legislation, Combating cybercrime.