جامعة المنصورة
كلية الحقوق
قسم القانون العام

بحث بعنـوان
الإطار التجريمي للهجوم السيبراني

إعـــداد

الباحث / خالد سلامة أسعد الزينات

تحت إشراف

أ.د/ أحمد لطفي السيد مرعي

أستاذ ورئيس قسم القانون الجنائي
كلية الحقوق - جامعة المنصورة

العام الجامعي ١٤٤٥هـ - ٢٠٢٥ م

(إِنَّهُ مَنْ يَأْتِي رَبَّهُ مُجْرِمًا فَإِنَّ لَهُ جَهَنَّمَ لَا يَمُوتُ فِيهَا وَلَا يَحْيَى) [1].

" صدق الله العظيم"

---

(1) سورة طه، آية ٧٤.

المقدمة

أولًا: موضوع البحث:

تُعَدّ الجرائم الإلكترونية من أبرز التحديات الملحّة التي تواجه دول العالم اليوم، إذ تُثير قلق الحكومات والمتخصصين والأفراد على حدّ سواء. وقد برزت هذه الجرائم كنتيجة مباشرة لظهور شبكة الإنترنت وما رافقها من تطورات متسارعة في تكنولوجيا المعلومات والاتصالات، فضلاً عن الانتشار الواسع للتقنيات الحديثة، الأمر الذي جعلها تُشكّل تهديداً حقيقيًا للأمن القومي وللنظام الدولي برمّته.

تُعدّ التكنولوجيا الحديثة أساسيةً في جوانب عديدة من حياتنا اليومية. وينتشر تطبيق تكنولوجيا المعلومات والاتصالات الآن في التعليم والترفيه والنقل والاتصالات. وقد ساهم هذا الانتشار الواسع في إدخال تقنيات مبتكرة غذّت نموّ وتطور الجرائم الإلكترونية.

يُعدّ رسم خرائط البيانات، وإدخال البيانات، وغيرها من التقنيات المعاصرة أمثلةً على هذه التقنيات. فبمساعدة هذه التقنيات، يُمكن للجناة تنفيذ جرائمهم الإلكترونية بدقة وبساطة. وتشمل هذه التقنيات رسم خرائط لمصادر جمع البيانات، مثل بيانات نظام تحديد المواقع العالمي (GPS)، وكاميرات المراقبة، ومنشورات مواقع التواصل الاجتماعي، لتحديد مواقع الضحايا ومتابعتهم. وبالتالي، تنطوي الجريمة الإلكترونية على بيئة رقمية واتصال بالإنترنت لممارسة الأنشطة أو السلوكيات الجسدية. هذا يستلزم الإلمام ببداية هذه الممارسة وبدايتها ونهايتها. إن موقع وتوقيت الجريمة الإلكترونية ليسا سوى اثنين من القضايا العديدة التي يثيرها سؤال نهايتها الجنائية.

لم تتخذ الحكومات حول العالم إجراءات كافية لحماية الأمن السيبراني، حتى مع الارتفاع المطرد في عدد مستخدمي الإنترنت منذ بداية الألفية الثالثة. من المهم ملاحظة أن أجهزة الكمبيوتر تُستخدم على نطاق واسع في جميع دول العالم، سواء في المجال العام أو التجاري أو الشخصي. ومع ذلك، في السنوات القليلة الماضية، أعطت سياسات العديد من الدول الأولوية لحماية المعلومات والاتصالات وأمن الشبكات، بالإضافة إلى مكافحة الجريمة الإلكترونية.

جعل التقدم العلمي والتكنولوجي في مجالات البرمجيات والحواسيب الهجمات الإلكترونية سلوكًا غير قانوني. هذه جرائم لا يمكن لأحد ارتكابها إلا إذا كان لديه فهم شامل للقرصنة الإلكترونية، نظريًا

وعمليًا. ونتيجة لذلك، فهي تختلف عن الجرائم التقليدية التي لا تتطلب مستوى عاليًا من الكفاءة في هذا المجال.

ثانيًا: أهمية البحث:-

يُسهم موضوع هذا البحث في التأثير على التكتيكات المعاصرة، لا سيما في مجال الجرائم الإلكترونية، يُعدّ موضوع الدراسة أساسياً في القانون الجنائي. تُعدّ الجرائم الإلكترونية فئةً جديدةً من الجرائم التي يجب على المؤسسات الحكومية والمجتمع الدولي بأسره مكافحتها بحزم، نظراً لنموها بالتزامن مع ثورة المعلومات والاتصالات، وارتباطها بالتكنولوجيا الحديثة.

ثالثًا: مشكلة البحث:

يُشكّل تزايد الجرائم الإلكترونية والجريمة المنظمة، وتنوع أشكالها، وتزايد عدد ضحاياها وخسائرها، تحديًا بحثيًا. فهي تُشكّل الآن تهديداً خطيراً لأمن المعلومات في جميع القطاعات الأساسية والعامة. في الواقع، يُشكّل استخدام الإنترنت والشبكات الإلكترونية تهديداً للسلم والأمن العالميين، فضلًا عن الأمن السيبراني. وتتمثل مشكلة الدراسة فيما يلي:

١. تزايد الجرائم الإلكترونية.

٢. الحصول على البيانات المحفوظة على أجهزة الكمبيوتر أو المُرسلة عبر الإنترنت.

٣. الإضرار بالأفراد أو المنظمات الشرعية والأخلاقية.

٤. يكمن تحدي مكافحة الجرائم الإلكترونية في سهولة إخفائها وصعوبة الحصول على الأدلة المادية.

رابعًا: منهج البحث:

يهدف هذا البحث إلى تسليط الضوء على أهم جرائم الهجمات الإلكترونية التي تهدد الأمن القومي، اعتمدت هذه الدراسة على المنهج الوصفي التحليلي المقارن للإطار الموضوعي لجريمة الهجمات الإلكترونية من أجل توضيحها والوصول إلى النتائج.

المبحث الأول

ماهية الجريمة السيبرانية

تُعتبر الجرائم الإلكترونية من أكثر أشكال الجريمة انتشاراً نظراً للنمو المتواصل لها، والذي يتجلى في استخدام الشبكات الإلكترونية والمعلوماتية. لذا، لا بد من تعريف الجريمة الإلكترونية وخصائصها.

المطلب الأول

مفهوم الجريمة السيبرانية

يُواجِه أمنُ المعلومات في عالمنا المعاصر تهديداً خطيراً ومتنامياً ناجماً عن الهجمات الإلكترونية. ونتيجةً لهذا النوع من السلوك، يتمكن مرتكب الجريمة من الوصول إلى أنظمة المعلومات وإتلافها وإعاقة تشغيلها. يشير مصطلح "الهجمات الإلكترونية" إلى مجموعة متنوعة من الإجراءات التي تهدف إلى اختراق أنظمة وشبكات الحاسوب من خلال اكتشاف أو توليد ثغرات أمنية واستغلالها لتدمير الشبكة الإلكترونية. وبناءً على ذلك، سيركز هذا الفصل على مجالين دراسيين. نستكشف في القسم الأول التعريف التشريعي لجريمة القرصنة الإلكترونية، ثم نتناول التعريف الفقهي لها في القسم الثاني، على النحو التالي:-

أولًا : التعريف التشريعي للهجمات السيبرانية:

يركز التحليل المقدم في هذا القسم على نقطتين رئيسيتين. يناقش الفصل الأول مفهوم جريمة القرصنة الإلكترونية في القانون الدولي، بينما يقدم الفصل الثاني مفهوم جريمة القرصنة الإلكترونية في القانون الوطني، على النحو التالي:

١- مفهوم جريمة الإختراق السيبراني في التشريعات الدولية.

بدايةً، يمكن القول إن المشرع الدولي كان أول من أدرك خطورة الجرائم الإلكترونية، بما في ذلك اتساع نطاق السلوك الإجرامي الذي تنطوي عليه. وقد مثّل مؤتمر الأمم المتحدة الثامن لمنع الجريمة ومعاملة المجرمين، الذي عُقد في هافانا، كوبا، عام ١٩٩٠، بداية اهتمام المجتمع الدولي بهذا الحدث الإجرامي. وشجع المؤتمر في قراراته الدول الأعضاء على تكثيف جهودها لمكافحة إساءة

استخدام الحاسوب وتجريم السلوكيات التي تعكس هذه الإساءة، مثل انتهاك الخصوصية الإلكترونية، والانخراط في القرصنة الإلكترونية، واختراق الفضاء الإلكتروني للآخرين.[٢].

وعلاوة على ذلك، وافق المؤتمر الخامس عشر للجمعية الدولية للقانون الجنائي، الذي عقد في البرازيل عام ١٩٩٤، على جعل عدد من الجرائم المتعلقة بالكمبيوتر غير قانونية، مثل الاحتيال والتزوير المرتكبين عبر أجهزة الكمبيوتر، فضلاً عن الوصول غير القانوني إلى أنظمة المعلومات من خلال انتهاكات الضمانات الأمنية الإلكترونية الموضوعة لحماية هذه الأنظمة.[٣] .

ميّز الفقه المقارن بين الجريمة الإلكترونية والجريمة الافتراضية، حيث لاحظ أنه في حين أن هناك رابط بين شكلي الجريمة، إلا أن هناك فرق بينهما يؤدي إلى الاستنتاج بأن النوع الأخير من الجريمة، الافتراضي، يتطلب اتصالاً مستمراً بالشبكات، في حين أن الوضع مختلف تماماً مع الجريمة الإلكترونية، والتي يمكن أن تحدث بعيداً عن اتصالات الشبكات، بما في ذلك الإنترنت، مثل جريمة الاعتداء على حقوق الطبع والنشر.[٤].

تُعرّف اتفاقية منظمة شنغهاي للتعاون "جرائم المعلومات" بشكل أوسع بأنها استخدام موارد المعلومات في المجال المعلوماتي والتلاعب بها لأغراض غير مشروعة [٤] ,إلا أن الجريمة المتعلقة بمعلومات الحاسوب تُصنّف كفعل إجرامي يستهدف هذه المعلومات. وحتى مع تعريفها لمصطلحاتها، فإن اتفاقية مجلس أوروبا تستخدم فئات جنائية عامة، مثل "الجرائم المرتكبة ضد سرية البيانات والمعلومات والأنظمة الإلكترونية وسلامتها وتوافرها". [١] .

---

(٢) د . وفاء محمد صافي ، الحماية الجنائية لجريمة القرصنة الإلكترونية لحقوق الملكية الفكرية الإلكترونية ، مركز الدراسات العربية للنشر والتوزيع ، القاهرة ، ٢٠٢٢ ، ص١٦.

(٣) د . محمد عبدالله أبو بكر سلامة ، موسوعة جرائم المعلوماتية – جرائم الكمبيوتر والإنترنت ، المكتب العربي الحديث، القاهرة ، ٢٠١٥ ، ص٢٥.

(4) E.cesay: digital evidence and Computer Crim " londer, academic press", 2000, p.9 et s. & D.parker: Combattre la Criminalite informatique (paris, oros), 1985, j, p.18. & M. Chawki, Combattre LaCybercriminalite, Universite Lyon III, France, 2008, p. 42.

٢- مفهوم جريمة الإختراق السيبراني في القانون.

سنّت العديد من الدول قوانين لمواجهة هذه الجرائم الإلكترونية، نتيجةً للتطورات في تكنولوجيا المعلومات وظهور أساليب إلكترونية معاصرة، ما أدى إلى ظهور جرائم جديدة تُعرف بمعناها الواسع بالجرائم الإلكترونية، وبمعناها الخاص بالجرائم السيبرانية. ومن هذه التشريعات القانون المصري لمكافحة جرائم تقنية المعلومات رقم ٧٥ لسنة ٢٠١٨.(٥).

يُظهر استعراض نصوص هذا القانون أنه في حين لم يُحدد المشرع تعريفًا صريحًا للهجمات الإلكترونية أو الجرائم الإلكترونية عمومًا، فقد حدد في المادة الأولى منه أن الاختراق يُعدّ أحد أشكال الهجمات الإلكترونية، وهو الوسيلة الأساسية لإبراز هذه الجريمة. وعُرِّف الاختراق بأنه "الدخول غير المصرح به، أو الدخول بالمخالفة لشروط الترخيص، أو الدخول بأي طريقة غير مشروعة إلى نظام معلوماتي، أو حاسوب، أو شبكة معلوماتية، أو ما شابه"(٦).

تمثل الجرائم الإلكترونية مختلفة، لأن المصطلحات المرتبطة بتكنولوجيا المعلومات والتكنولوجيا واسعة النطاق وتحتاج إلى تعريف لمنع استخدامها بشكل تعسفي أو غير لائق بطريقة لا تتفق مع نية المشرع.(٧).

يتخذ المشرع الأردني نهجًا مختلفًا عن المشرعين المصريين والإماراتيين، مستخدمًا قانون الأمن السيبراني الأردني. فقد وضع القانون رقم ١٦ لسنة ٢٠١٩ تعريفًا واضحًا للهجمات السيبرانية، مُشيرًا إليها بحوادث الأمن السيبراني، ومُعرّفًا إياها بأنها "فعل أو هجوم يُشكّل تهديدًا للبيانات أو المعلومات أو شبكة المعلومات أو البنية التحتية المرتبطة بها، ويستدعي ردًا لوقفه أو التخفيف من عواقبه أو آثاره"(٨).

---

(٥) منشور في الجريدة الرسمية العدد ٣٢ مكرر (ج) في ١٤ أغسطس ٢٠١٨.

(٦) المادة الأولى من قانون مكافحة جرام تقنية المعلومات المصري رقم ١٧٥ لسنه ٢٠١٨.

(٧) د. علي حمزة عسل الخفاجي ، فاعلية السياسية الجنائية لحماية الأمن السيبراني ، دار مصر النشر والتوزيع، ٢٠٢٥، ص٦٣.

(٨) نص المادة (٢) من قانون الأمن السيبراني الأردني رقم ١٦ لسنة ٢٠١٩.

ويبدو أن المبرر التشريعي لتجريم حتى الدخول غير المشروع البسيط، حتى لو لم يتحقق أي من القصد الجنائي أو الآثار الجنائية المرتبطة بالاختراق، هو توفير أكبر قدر من الحماية لأنظمة وبرامج المعلومات مما قد تتعرض له من اختراق أو تسلل أو أي دخول غير مشروع إلى نظام المعلومات، سواء كان هذا الدخول إلى جزء من نظام المعلومات أو إلى نظام المعلومات بأكمله، خاصة في ظل هذا التطور التقني والتكنولوجي المعاصر.[٩].

ثانيا : التعريف الفقهى لجريمة الإختراق السيبرانى.

يقتضي البدء التأكيد على أن مصطلح قانون الإنترنت تصف القانون الذي يحكم كل فعل يحدث في الفضاء الإلكتروني، حيث يتعايش الإنترنت والقانون في قاعة واحدة.[١٠].

---

(٩) د. إبراهيم رمضان عطايا ، الجريمة الإلكترونية وسبل مواجهتها في الشريعة الإسلامية والأنظمة الدولية ، مكتبة الوفاء القانونية ، القاهرة ، ٢٠٢٢ ، ص٦٣.

(١٠) الأنترنت هو عبارة عن شبكة تتألف من مئات الحاسبات الألية المرتبطة ببعضها بعضاً عن طريق الأقمار الصناعية، وتمتد عبر العالم لتؤلف في النهاية شبكة هائلة وكبيرة. وتعود بداية الأنترنت إلى ٢/١/١٩٦٩ وذلك عندما قامت وزارة الدفاع الأمريكية بإنشاء وكالة مشاريع للأبحاث المتقدمة، وقد كان الهدف من إيجاد شبكة الأنترنت في بداية الأمر هو الحاجة إلى وجود شبكة اتصال تصمد أثناء فترة الحرب وكانت بداية شبكة الأنترنت على هذا الأساس للخدمات العسكرية، ومع بداية سنة ١٩٨٣ تحول الأمر إلى الاستعمال في المجال السلمي، وأجريت تطورات تقنية على شبكة الأنترنت من بداية سنة ١٩٩٣ وأدت هذه التطورات إلى زيادة إمكانية شبكة الأنترنت مما أدى ذلك إلى تمكين مستخدمي الشبكة العنكبوتية الدخول إليها في أي وقت ومن أي مكان يتواجدون فيه. ينظر في ذلك كل من : د.علي سعيد الحيان الغامدي: الحماية الجنائية للمراهقين من المؤثرات الجنسية دراسة مقارنة، الطبعة الأولى، مركز الدراسات العربية، مصر ، ٢٠١٥ ، ص ٤٩؛ د. علي جبار الحسيناوي، جرائم الحاسوب والإنترنت، مطابع اليازوري الأردن ، ٢٠٠٩، ص ١٧ ، و عماد محمد سلامة، الحماية القانونية لبرامج الحاسب الآلي ومشكلة قرصنة البرامج ، دار وائل للنشر، عمان، الطبعة الأولى، ٢٠٠٥، ص ٢٥؛ و د . ، فتحي محمد انور عزت، تفتيش شبكة الإنترنت لضبط جرائم الاعتداء على الآداب العامة والشرف والاعتبارات التي تقع بواسطتها المركز القومي للإصدارات القانونية، القاهرة، الطبعة الأولى، ٢٠١٢، ص ٢٥؛ ود. ذياب موسى البيداني الشباب والأنترنت والمخدرات، الطبعة الأولى، أكاديمية نايف العربية، الرياض السعودية، ٢٠١٢، ص٣١؛ د. عبد الفتاح بيومي حجازي: الأحداث والأنترنت دراسة متعمقة عن أثر الأنترنت في أنحراف الأحداث، دار الكتب القانونية ، مصر، ٢٠٠٧، ص ١٢٤.

نتيجةً لذلك، تُشير الجريمة الإلكترونية إلى نشاط إجرامي يخضع للقانون الجنائي ويحدث في المجال الرقمي. ومن بين المشكلات التي يُواجهها الفقهاء في تحليلهم للجرائم الإلكترونية عدم قدرتهم على الاتفاق على مصطلح واحد لوصف الجريمة المرتكبة عبر الإنترن. ورغم الاهتمام المحلي والعلمي الواسع بمعالجة قضية الجرائم التقنية والتكنولوجية المُتزايدة، إلا أنهم لم يتوصلوا إلى تعريف واضح ومُعترف به عالمياً لمفهوم الهجمات الإلكترونية [١١]، وبالإضافة إلى التفاوت بين النظم القانونية والثقافية للدول، فإن حداثة هذه الأخيرة ساهمت في عدم وجود تعريف متناسق لهذه الظاهرة الإجرامية بسبب المخاوف من حصرها في منطقة صغيرة من شأنها أن تضر بها.[١٢].

ونتيجةً لذلك، تعددت التعريفات القانونية، وتختلف في نطاقها وخصوصيتها. وتُعدّ الجريمة من جرائم الإنترنت إذا كانت وسيلة ارتكابها هي الحاسوب أو إحدى الوسائل التقنية الحديثة المرتبطة به، بغض النظر عن خصوصية الوسيلة.[١٣]، يقتصر نطاق هذه الجريمة، من وجهة نظر مؤيديها، على الحالات التي تؤثر على العناصر غير المادية للحاسوب، مثل بياناته وبرامجه والمعلومات المخزنة. ويُعرّفها مكتب تقييم التكنولوجيا في الولايات المتحدة الأمريكية بأنها "الجرائم التي تلعب فيها بيانات الحاسوب وبرامج المعلومات دوراً رئيسياً". وفي هذه الجريمة، يُستخدم الحاسوب كأداة رئيسية لتنفيذها [١٤].

وعرفها آخرون بشكل مختلف، بأنها الجرائم التي تقع عند استخدام التكنولوجيا الحديثة مثل الكمبيوتر والإنترنت للقيام بأعمال وأنشطة إجرامية بهدف تحقيق أرباح ضخمة من أنشطة غير مشروعة يتم إعادة إدخالها إلى الاقتصاد العالمي عبر الإنترنت من خلال الأموال الإلكترونية، وبطاقات

---

(١١) وهو ما أكدته قمة برلين :-

- Le sommet de Berlin, relative à la cybercriminalité n' aura permis de dégager qu' une seule certitude, une définition universelle de la cybercriminalité et l'on peut même se demander si une entente sera un jour possible» L'impossible définition universel de la cybercriminalité, http:// www.vilage -justice.com

(١٢) د . أحمد خليفة الملط، "الجرائم المعلوماتية"، الطبعة الثانية، دار الفكر الجامعي، الإسكندرية، ٢٠٠٦، ص٨٣.

(١٣) د. يوسف صغير، "الجريمة المرتكبة عبر الإنترنت"، المرجع السابق ، ص٨.

(١٤)TOM Forester, Essential problèmes to High-tech Society First MIT Prés édition, Cambridge, Massachusetts, 1989, P. 105.

الخصم التي تحمل أرقاماً سرية للشراء عبر الإنترنت، أو تداول الأسهم والأنشطة التجارية التي تتم عبر هذه الشبكة.[١٥].

يُعرّف نجاح الجاني في استخدام اختراقه، الذي يتضمن جمع المعلومات والبيانات، لتحقيق نتيجة معينة، بالقرصنة الإلكترونية. ويمكن القول إن الاختراق في هذه الحالة يُعدّ جريمةً مُخالفةً للقانون، كما يتضح من خلال الوصول غير المصرح به إلى نظام البيانات أو الموقع الإلكتروني أو الحساب الإلكتروني، بالإضافة إلى ارتكاب فعل إجرامي يتجاوز مجرد وجود الجاني دون سلطة قانونية للحصول على المعلومات والبيانات الموجودة في الموقع الذي وقعت فيه الجريمة.[١٦].

يستخدم أنصار هذا الاتجاه معياراً ذاتياً، إذ يجب أن يكون مرتكب هذه الجرائم على دراية بتكنولوجيا المعلومات ومتمكناً منها. ومن هذه التعريفات تعريف الجريمة المرتكبة عبر الإنترنت، والتي يصفها البروفيسور ديفيد تومبسون بأنها "أي جريمة تتطلب من مرتكبها معرفة بتكنولوجيا الحاسوب". قدّم المحامي شتاين شيولبيرج تعريفه لجرائم الحاسوب، موضحاً أنها تشمل "أي فعل غير قانوني تُعد معرفة تكنولوجيا المعلومات أساسية لمرتكبه والتحقيق فيه وملاحقته قضائياً"[١٧]، ولقد أخذت وزارة العدل الأمريكية بهذا التعريف في التقرير الصادر عنها سنة ١٩٨٩ والمتعلق بجرائم الإنترنت[١٨]،يُجادل مُؤيدو هذا التعريف بأن مرتكب هذه الجريمة يجب أن يتمتع بصفات فردية مُحددة، تتمحور في الغالب حول الكفاءة والمعرفة التقنية. ووفقًا لما سبق، يُمكن تعريف الهجمات الإلكترونية بأنها هجمات تسعى إلى تعديل أو تعطيل أو تدمير أنظمة الكمبيوتر أو الشبكات أو البيانات أو البرامج الموجودة داخلها. يُعد الاختراق الإلكتروني نوعاً من الاعتداء على الخصوصية الإلكترونية يرتكبه شخص يتمتع بخبرة تقنية وتكنولوجية كبيرة. ينطوي هذا الاختراق على اقتحام المُتسلل للمجال الرقمي الشخصي للضحية دون إذن ودون الحق القانوني للقيام بذلك. وينتج وجودهم غير القانوني على موقع

---

(١٥) د. عبدالله عبد الكريم عبدالله، "جرائم المعلوماتية والإنترنت"، منشورات الحلبي الحقوقية، بيروت، ٢٠٠٧، ص١٥.

(16) Madhava Soma Sundaram, Cyber Crime and Digital Disorder, K. Jaishankar, London 2011, p 66

(١٧) د. عبد اللطيف معتوق، "الإطار القانوني لمكافحة جرائم المعلوماتية في التشريع الجزائري والتشريع المقارن"، مذكرة ماجستير، جامعة العقيد الحاج لخضر بباتنة، كلية الحقوق والعلوم السياسية، قسم الحقوق، ٢٠١١-٢٠١٢، ص٧.

(١٨) د. سفيان سوير، "جرائم المعلوماتية"، مذكرة ماجستير، جامعة أبو بكر بلقايد بتلمسان، كلية الحقوق والعلوم السياسية، قسم الحقوق، ٢٠١٠-٢٠١١، ص١٢.

الضحية الإلكتروني أو حسابه الإلكتروني أو نظامه أو شبكة معلوماته عن هذا الاختراق، إما لأنهم غير مُصرّح لهم بشكل صحيح أو لأنهم يستخدمون تفويضهم بما يتجاوز حدوده.[١٩].

تجدر الإشارة إلى أن الضرر الناجم عن هذه الهجمات قد يستهدف الأشخاص أو البنية التحتية المادية أو شبكات الكمبيوتر. يمكن أن تؤدي الهجمات الإلكترونية إلى مجموعة واسعة من الأضرار، بدءًا من تشويه مواقع الويب والقرصنة الخبيثة وصولًا إلى تدمير واسع النطاق وحتى الانهيار الكامل للبنية التحتية. باختصار، إنه هجوم يستخدم الاختراق، ثم التحكم، وفي النهاية التحكم عن بُعد لتحويل التعليمات الرقمية إلى إجراء مادي من أجل التسبب في الدمار والتعطيل. تنطبق اللوائح الجنائية على الجاني نتيجة لفعل القرصنة نفسه. بغض النظر عن الغرض المقصود منه، فإن أي فعل أو امتناع عن فعل غير قانوني يُعتبر قرصنة. القرصنة الإلكترونية جريمة مستقلة لا يلزم ربطها بأي سلوك غير قانوني آخر [٢٠].

(19) International Journal Of Engineering And Computer Science ISSN:2319- 7242 Volume 6 Issue 4 April 2017, Page No. 21042-21050 Index Copernicus value (2015): 58.10 DOI: 10.18535/ijecs/v6i4.42 Aman Gupta, IJECS Volume 6 Issue 4 April, 2017 Page No. 21042-21050 Page 21042 Ethical Hacking and Hacking Attacks Aman Gupta, Abhineet Anand.

(٢٠) Study Of Ethical Hacking Bhawana Sahare1, Ankit Naik2, Shashikala Khandey, International Journal of Computer Science Trends and Technology (IJCST) Volume 2 Issue 4, Nov-Dec 2014

المطلب الثاني

خصائص جريمة الإختراق السيبرانى

تتسم الجرائم الإلكترونية بسمات وخصائص معينة ضرورية لاعتبار الجريمة الإلكترونية جريمةً مشروعة. ولأن الجريمة الإلكترونية جريمةٌ خفية يصعب إثباتها في كثير من الأحيان، فقد تكون هذه السمات موضوعية، أي أنها تتعلق بالجريمة نفسها. وقد تشمل أيضاً سماتٍ وصفاتٍ فريدةً تخص مجرم الإنترنت نفسه، إذ يجب أن يتمتع بخبرةٍ واحترافيةٍ وذكاءٍ عالٍ لارتكاب جريمته. مع وضع ذلك في الاعتبار، سنناقش سمات الجريمة الإلكترونية على النحو التالي:

تتميز جريمة الهجوم الإلكتروني أو القرصنة عن غيرها من الجرائم الشائعة بامتلاكها مجموعةً فريدةً من السمات والخصائص، منها:

١- جرائم ترتكب بواسطة الأجهزة الالكترونية كالحاسب الآلي والهواتف الخلوية.

يُسلّم الفقه بأن الجرائم الإلكترونية تمثّل تحدياً قانونياً وأمنياً متنامياً، كالهجمات الإلكترونية، تُنفّذ باستخدام أجهزة الحاسوب أو غيرها من وسائل التكنولوجيا الحديثة، حيث يلعب الإنترنت والحاسوب دوراً هاماً في ارتكاب هذه الجرائم. قد تُرتكب الجرائم الإلكترونية ضد الأجهزة الإلكترونية أو تنطوي عليها. يحدث هذا عندما يتمكن شخص ما من الوصول غير المُصرّح به إلى موقع إلكتروني، أو يخترق أنظمة الحاسوب، أو يُدمِّر أو يُتلف أو يُغيِّر أو يُعدِّل البيانات أو المعلومات أو البيانات المُخزّنة عليه. يُعرف هذا باسم قرصنة المعلومات، وهو انتهاك للخصوصية والسرية، أو عندما يُزرع شخص ما فيروسات أو يستولي على البيانات المُرسَلة عبر الأنظمة.[٢١].

علاوة على ذلك، يمكن استخدام الأجهزة الإلكترونية لارتكاب جرائم محددة، مثل سرقة الأموال بإساءة استخدام بطاقات الائتمان عبر استخدام أجهزة الكمبيوتر والإنترنت. وقد تُستخدم أحياناً لارتكاب

---

(٢١) د . محمد أمين الرومى ، جرائم الكمبيوتر والإنترنت ، دار المطبوعات الجامعية ، الاسكندرية ، ٢٠٠٤، ص١٥

جرائم قتل من خلال اختراق البيانات المحفوظة وتغيير برامجها. ومن الأمثلة الواقعية على ذلك قـدرة لص إلكتروني على السيطرة على سفينة أو طائرة، أو تفجيرها، أو قتل ركابها، أو تعديل بيانات تتعلق بملفات المرضى أو تشخيصات الأمراض. وأخيراً، يمكن أن تُشكل أجهزة الكمبيوتر والإنترنت منصـةً للجرائم الإلكترونية، كما هو الحال عند استخدامها لنشر محتوى غير مشروع، مثل إنشاء مواقع إباحية، وللتشجيع على أنواع مختلفة من الجرائم، مثل الاتجار بالأسلحة والمخدرات.(٢٢).

٢ ـ جرائم الهجوم السيبرانى جرائم خفية

يصعب تحديد الجرائم الإلكترونية بسبب نقص الكفاءة التقنية لدى الضحية نسبياً مقارنة بالمجرم الإلكتروني الذي أتقن التكنولوجيا واستغل خبرته لتنفيذ مثل هذه الجرائم وإخفائها. وقد يخفي الضـحية أيضاً هذا النوع من الجرائم خوفاً من إبلاغ الشرطة والإضرار بسمعته.(٢٣).

٣- ـجرائم الهجوم السيبرانى جرائم عابرة للحدود .

تُعرف الهجمات الإلكترونية بامتدادها العالمي، إذ تتجاوز الحدود الزمانية والمكانية للدول. فمن خلال الأقمار الصناعية والقنوات الفضائية والإنترنت، ارتبط العالم بأسره بشبكة واحدة، مما يُسهّل نشر الثقافة وعولمتها ومنع الجريمة، متجاهلاً الحدود الوطنية. ونتيجةً لذلك، لا تعترف الهجمات الإلكترونيـة بالحدود بين الدول والقارات، إذ تربط دولاً لا تحدها حدود طبيعية أو سياسية، وتُمكّن مستخدميها مـن التنقل بين الدول والقارات دون أي عوائق.(٢٤).

تُضاف إلى ذلك المسائل المتعلقة بالملاحقة القضائية، فإن التعامل مـع الهجمـات الإلكترونيـة كهجمات عابرة للحدود يطرح تحديات عملية عديدة فيما يتعلق بتحديد الدولة المختصة بهذا النوع مـن

---

(٢٢) د . يونس عرب ، الخصوصية وأمن المعلومات فى الأعمال الاسلكية بواسطة الهاتف الخلوى ، ورقة مقدمة إلى منتدى العمل الإلكترونى بواسطة الهاتف الخلوى ، إتحاد المصارف العربية ، عمان ، الآردن ٢٠٠١ ، ص ١٩ ، د . عبد الله حسين على محمود ، سرقة المعلومات المخزنة فى الحاسب الآلى ، الطبعة الأولى ، دار النهضة العربية ، القاهرة ، ٢٠٠١ ، ص ٦٧ .

(٢٣) محمود أحمد القرعان، "الجرائم الإلكترونية"، دار وائل للنشر والتوزيع، عمان، الطبعة الأولى، ٢٠١٧، ص٣٩.

(٢٤) د .على حمزة عسل خفاجى الجرائم الناشئة عن إختراق الأمن السيبرانى وآليات مكافحتها ، دار مصر للنشر والتوزيع، ٢٠٢٥ ، ص ٤٤ .

الجرائم والقوانين المنطبقة. وهذا يتطلب تعاون المشرّعين الـوطنيين والأجانـب لإصـدار تشـريعات وقوانين تعالج هذا النشاط الإجرامي وتضع آليات قانونية لمواجهته.[٢٥]

٤- جرائم الهجوم السيبرانى يصعب إكتشافها وإثباتها.

لا تتطلب الهجمات الإلكترونية أي عنف أو أفعال بدنية صريحة. وتشمل هذه الهجمات سـرقة البيانات والمعلومات من الملفات المحفوظة في ذاكرة الحاسوب، أو اختراقها، أو تغييرهـا، أو حـذفها. ونتيجةً لذلك، يصعب تحديدها وملاحقة مرتكبيها. كما أن سرعة ارتكابها – فقد تحدث في جـزء مـن الثانية، وقد لا تتطلب أي تحضير مسبق – تزيد من صعوبتها. ويكمن التحدي في إثبات هذا النوع مـن الجرائم في اكتشافها وتتبعها دون قصد. ونظراً لعدم تركها أي دليل مادي أو رؤيتها بالعين المجـردة، يصعب تحديد موقعها بدقة. فهي مجرد أرقام تطفو في الوثائق والمواقع الإلكترونية. إضافةً إلى ذلـك، فإن عدد الجرائم التي لم تُحل يفوق بكثير عدد الجرائم التي تم حلها. وهناك عدد مـن العوامـل التـي تُسهم في هذا التحدي.[٢٦] :

أ. إنها كجريمة لا تترك أثراً بعد ارتكابها. صعوبة الاحتفاظ الفني بآثارها إن وجدت.

ب. تحتاج لخبرة فنية يصعب على المحقق التقليدي التعامل معها.

ج .تعتمد على الخداع في ارتكابها، والتضبيب في التعريف على مرتكبيها.

---

(٢٥) د . حازم حسن الجمل ، الحماية الجنائية للأمن الإلكترونى ، دار الفكر والقانون ، المنصورة ، ٢٠٢٢ ، ص١٤

(٢٦) د . حسين بن سعيد الغافرى ، السياسة الجنائية فى مواجهة جرائم الإنترنت ، دار النهضة العربية ، القاهرة ، ٢٠٠٩ ، ص٥٦ ؛ د . على حمزة عسل الخفاجى ، القواعد الموضوعية والإجرائية فى مواجهة الجريمة السيبرانية ، المرجع السابق ، ص٢٤، د . محمد حسين ، المسئولية القانونية فى مجال شبكات الإنترنت ، الطبعة الاولى ، دار النهضة العربية ، ٢٠٠٢ ، ص٨ .

المبحث الثاني

أركان جريمة الهجوم السيبرانى.

تشترط جريمة الهجوم الإلكتروني توافر أركانها. وكما هو الحال في أي جريمة أخرى، تشترط الجريمة الإلكترونية توافر الركن المادي، وهو الجانب الظاهر للجريمة، والذي من خلاله يتم الاعتداء على المصلحة المحمية قانوناً. أما الركن المادي فهو الجانب الظاهر للجريمة، والذي من خلاله يستخدم الجاني مهاراته الحاسوبية لتحقيق هدف غير مشروع.

المطلب الأول

الركن المادي لجريمة الهجوم السيبراني

يُعرّف الركن المادي للجريمة بأنه فعل خارجي ذو طابع مادي ملموس يُدرك بالحواس. يُعدّ الركن المادي ضرورياً لوجود جريمة. والسبب في ذلك هو أن المشرعين لا يأخذون في الاعتبار إلا السلوك المادي الملموس الذي يرقى إلى مستوى الاعتداء على الحقوق والمصالح التي يحاولون حمايتها عندما يتدخلون في عملية التجريم والعقاب. ومع ذلك، فإن الأفكار والمواقف والدوافع غير ضارة طالما بقيت كامنة في العقل ولم تتجسد في الواقع. وبالتالي، فإن الركن المادي لجريمة الهجوم الإلكتروني هو فعل الوصول إلى موقع ويب أو حساب إلكتروني أو نظام أو شبكة معلومات، بغض النظر عما إذا كان هذا ينطوي على الدخول غير القانوني أو البقاء غير القانوني داخل الموقع. وهذا يعني جعل مجرد الوصول غير القانوني أمراً غير قانوني، بغض النظر عن الغرض من الوصول أو إمكانية حدوث عواقب جنائية غير مقصودة [٢٧].

ولما كانت الجريمة السيبرانية شانها شان الجرائم العاديه، لهذا فان المشرع لا يعاقب على الاعمال التحضيرية لهذه الجريمة، فالجريمة السيبرانية قبل أن يرتكبها الجاني وتتخذ مظهرها الخارجي

([٢٧]) د. إسلام هديب ، الأمن السيبراني ، المرجع السابق ، ص١٠٦

نظراً لأنه يفكر ويتأمل باستمرار في الجريمة، فإن الخطوة الأولى للجريمة تكون في ذهنه. على سبيل المثال، لا يُعاقب الجاني إذا غير رأيه قبل تطبيق البرامج التي أعدها وثبتها لكسر الرموز الخاصة المستخدمة للوصول إلى مواقع الويب من أجل سرقة المعلومات الشخصية والحساسة للأشخاص. لا يعاقب المشرع مجرد التفكير في ارتكاب جريمة. يُلغى العنصر المادي للجريمة، وبالتالي تُلغى العقوبة أيضًا، إذا لم يتم تطبيق هذه النية. على الرغم من ذلك، غالبًا ما يكون من المستحيل التمييز بين مرحلة التخطيط وبداية النشاط الإجرامي، لأن غالبية الجرائم الإلكترونية، بما في ذلك الهجمات الإلكترونية، لا تتطلب ذلك. تُعتبر جرائم الهجوم الإلكتروني جرائم خطيرة لأنها تُرتكب عند إثبات العنصر المادي. تُعرف الجريمة الإلكترونية بأنها شراء كلمات مرور وأدوات فك التشفير وبرامج القرصنة، من بين أمور أخرى. يرتكز الركن المادي لأي جريمة، وخاصةً الجرائم الإلكترونية، على ثلاثة عناصر: السلوك الإجرامي الإيجابي أو السلبي، والنتيجة الإجرامية، وهي الأثر القانوني للسلوك، وأخيراً، العلاقة السببية بين السلوك والنتيجة الإجرامية. وسيتم استخدام هذا الركن في البحث المتعلق بجريمة الهجوم الإلكتروني، على النحو التالي:-

أولًا :- السلوك الإجرامي في جريمة الهجوم السيبراني.

إن الفعل المادي الخارجي الذي يُشكل جريمة هو ما يُحدد السلوك الإجرامي في المقام الأول. ونتيجةً لذلك، لا يمكن أن تكون هناك جريمة ما لم تُبدِ هذه النوايا نفسها، لأن القانون لا يُعاقب على النوايا أو الرغبات أو الشهوات البسيطة. إن المصالح التي يحميها القانون معرضة للخطر من النشاط الإجرامي في مجال الجرائم الإلكترونية. عندما يُحقق الجاني النتيجة المقصودة، يُظهر هذا السلوك نفسه. وباعتباره أحد مكونات الركن المادي للجريمة، فإن للسلوك الإجرامي تعريفًا واسعًا يشمل السلوك الجيد والسيئ على حد سواء، أو ما يُشار إليه بالامتناع. يتميز الأخير بعدم رغبة الشخص في القيام بعمل إيجابي مُعين كان القانون يتوقعه منه في ظروف معينة، بافتراض أن القانون يُلزم بهذا السلوك. ومع ذلك، فإن الفرد لا يقوم بهذا العمل [٢٨].

والسؤال الذي يثور في هذا الصدد هل يمكن أن تتحقق الجريمة السيبرانية بسلوك سلبي؟

([٢٨]) د. محمود نجيب حسني ، شرح قانون العقوبات ، المرجع السابق ، ص٢٧

الرأي السائد في الفقه الإسلامي هو أن السلوك الإجرامي في الهجوم الإلكتروني لا يمكن أن يتحقق من خلال السلوك السلبي لأن الجريمة الإلكترونية تلزم الجاني باستخدام برامج وأدوات تسمح له باختراق جهاز كمبيوتر، وهو ما لا يمكن القيام به إلا من خلال السلوك الإيجابي. يمكن استخدام هذا لمعالجة هذه المشكلة. من ناحية أخرى، يمكن أن يتخذ السلوك الإجرامي في الهجوم الإلكتروني شكلاً سلبيًا، كما هو الحال إذا فشل الموظف الذي تتمثل وظيفته في حماية المعلومات الإلكترونية في مؤسسة حكومية أو شركة عمدًا في حماية البيانات والمعلومات بطريقة تردع الاختراق. إما أنهم متواطئون مع مرتكب الهجوم الإلكتروني أو أن سوء سلوكهم يهدف إلى الإضرار بالشركة التي يعملون بها. الشخص المسؤول عن حماية البيانات الإلكترونية هو الوصي على تلك البيانات، ونتيجة لذلك، فإن فشله في اتخاذ التدابير الأساسية للحفاظ على البيانات الإلكترونية وتأمينها قد يجعلها عرضة للاختراق. إن جريمة الهجوم الإلكتروني يمكن أن ترتكب بفعل سلبي، ولكن من الأرجح أن ترتكب بفعل إيجابي، إذ لا بد أن يستخدم الجاني برامج وأدوات حتى يتمكن من اختراق الحاسوب والدخول إلى المواقع الإلكترونية، سواء بقصد أو بغير قصد، ومن ثم لا بد أن يقوم الجاني باختراق موقع إلكتروني، أو نظام معلومات إلكتروني، أو شبكة معلوماتية، أو وسيلة من وسائل تكنولوجيا المعلومات.[٢٩].

في الجرائم الإلكترونية، يتجلى السلوك الإجرامي في القرصنة، وهي الوصول غير المصرح به أو غير القانوني إلى نظام معلومات أو حاسوب أو جهاز أو نظام تشغيل أو مركبة أو آلة أو شبكة معلومات أو ما شابه ذلك أو البقاء فيه. تتجلى الجرائم الإلكترونية بأشكال متنوعة. في بعض الحالات، يتم تنفيذ النشاط الإجرامي من خلال اختراق غير قانوني لحياة الأفراد وخصوصيتهم بهدف الوصول إلى بياناتهم الحساسة، ثم التهديد بالكشف عن هذه الخصوصية ما لم يدفعوا مبلغًا محددًا من المال. يؤدي انتهاك حرمة الحياة الاجتماعية للأفراد إلى سلوك إجرامي. في كل مرحلة من مراحل المعاملات الإلكترونية، توجد عدة طرق قد يحاول بها الأشخاص الوصول إلى المعلومات الشخصية لشخص ما. وتشمل هذه الطرق استخدام بيانات شخصية غير دقيقة لتحقيق الهدف المنشود، وهو المعلومات

---

(٢٩) د. علي حمزه عسل الخفاجي ، القواعد الموضوعية والإجرائية في مواجهة الجريمة السيبرانية ، المرجع السابق ، ص٣٢.

الخاصة، أو استخدام برامج وفيروسات معينة تساعد في عملية القرصنة، أو الاستيلاء المتعمد على الرمز السري للفرد دون علمه.[٣٠] .

ولكن هو موقف المشرع من تحديد السلوك الإجرامي في جريمة الإختراق السيبراني؟

وقد تناول المشرع المصري أنواع السلوك الإجرامي المتضمن في الهجمات الإلكترونية من خلال نصوص قانون مكافحة تقنية المعلومات المصري رقم (١٧٥) لسنة ٢٠١٨، والتي يمكن الاستعانة بها للإجابة على هذا التساؤل. وبنص المادة الأولى من هذا القانون، أرسى المشرع مفهوم جريمة الاختراق، التي عرّفها بأنها الدخول غير المصرح به، أو الدخول بالمخالفة لشروط الترخيص، أو الدخول بأية وسيلة غير مشروعة إلى نظام معلوماتي أو جهاز حاسوب أو شبكة معلوماتية أو ما شابه. ونتيجة لذلك، فإن السلوك الإجرامي في جريمة الهجوم الإلكتروني يرتكب عندما ينجح الجاني في الوصول غير المصرح به إلى وسيط إلكتروني، سواء كان ذلك بصورة قانونية أو من خلال عقد. وترتكب هذه الجريمة ضد الأشخاص الذين ليس لديهم الحق في الدخول أصلاً، أو ضد حاملي التراخيص إذا تجاوزوا القيود التي يفرضها ترخيصهم.[٣١].

تُحدد المادة (١٤) من قانون مكافحة تكنولوجيا المعلومات المصري أنواع السلوك الإجرامي الذي يُشكل جريمة الدخول غير المشروع. ووفقًا لهذه الوثيقة، يُعاقب بالسجن المؤبد كل من دخل، عمدًا أو بغير قصد، موقعًا إلكترونيًا أو حسابًا خاصًا أو نظام معلومات مُحظور الدخول إليه، أو أقام فيه بشكل غير قانوني، إذا أدى هذا الدخول إلى إتلاف أو حذف أو تعديل أو نسخ أو إعادة نشر البيانات أو المعلومات المخزنة على ذلك الموقع الإلكتروني أو الحساب الخاص أو نظام المعلومات. كما يُحدد التشريع نفسه أنواع النشاط الإجرامي الذي يُشكل جريمة الإخلال بسلامة البيانات والمعلومات وأنظمة المعلومات بموجب المادة (١٧). كل من قام عمداً وبغير وجه حق بإتلاف أو تعطيل أو تغيير مسار أو إلغاء كل أو جزء من البرامج أو البيانات أو المعلومات المخزنة أو المعالجة أو المنتجة أو المنشئة على أي نظام معلومات أو نظام مماثل، أياً كانت الطريقة المستخدمة في الجريمة، يعاقب

---

(٣٠) د. علي عبود جعفر، جرائم تكنلوجيا المعلومات الحديثة الواقعة على الأشخاصوالحكومة – دراسة مقارنة ، مصدر سابق، ص٤١٣ .

(٣١) د. إسلام هديب ، الأمن السيبراني ، المرجع السابق ، ص١٠٦

بالسجن مدة لا تقل عن سنتين وبغرامة لا تقل عن مائة ألف جنيه مصري ولا تزيد على خمسمائة ألف جنيه مصري أو بإحدى هاتين العقوبتين وفقاً لهذه المادة."

كما تناول القانون ذاته صور السلوك الإجرامي في جريمة مهاجمة البريد الإلكتروني أو المواقع الإلكترونية أو الحسابات الخاصة في المادة (١٨)، والتي تنص على أن كل من دمر أو عطل أو أبطأ أو اخترق بريدًا إلكترونيًا أو موقعًا إلكترونيًا أو حسابًا تابعًا لشخص آخر بشكل غير قانوني يكون مذنبًا بارتكاب الجريمة. كل من دمر أو تداخل أو أبطأ أو شوه أو أخفى أو عدّل تصميم موقع إلكتروني تابع لشركة أو مؤسسة أو منشأة أو شخص طبيعي بشكل غير قانوني يرتكب جريمة بموجب المادة (١٩) من التشريع نفسه، والتي تحدد أيضًا أنواع السلوك الإجرامي في جريمة مهاجمة تصميم موقع ويب. يميز المشرع الفرنسي بين الدخول المتعمد وغير المتعمد. ترتكب جريمة إلكترونية في المقام الأول إذا دخل شخص ما عمدًا إلى أي بريد إلكتروني أو موقع ويب. ومع ذلك، إذا زار موقعًا إلكترونيًا عن غير قصد، فيجب عليه التوقف فوراً. ويعتبر هذا جريمة إذا استمر في ذلك. وبموجب هذا تنص المادة (١/٣٢٣) من قانون العقوبات الفرنسي على أن "كل من يدخل أو يبقى كليا أو جزئيا داخل نظام معالجة المعلومات يعاقب بالسجن لمدة ثلاث سنوات وبغرامة قدرها ١٠٠ ألف يورو "[٣٢].

يوضح ما سبق أن جريمة الهجوم الإلكتروني تخضع لتمييزات تشريعية في أنواع السلوك الإجرامي. فخلافًا للمشرع الإماراتي الذي فرّق بين الاختراق الإلكتروني البسيط والاختراق الإلكتروني الذي يُلحق الضرر بحاوية المعلومات أو محتواها، رأى المشرع المصري أن الركن المادي لهذه الجريمة متحقق بغض النظر عما إذا كان الدخول إلى المواقع الإلكترونية متعمداً أم غير متعمد مع إقامة غير مشروعة. أما المشرع الإنجليزي، فقد رأى أن السلوك الإجرامي ينشأ بمجرد وصول الجاني إلى البيانات المخزنة، بغض النظر عما إذا كان ذلك يُسبب ضرراً، مما يعني أنه أخذ الاختراق البسيط في الاعتبار. أما المشرع الفرنسي، فقد فرّق بين الدخول المتعمد والغير متعمد. فلا تتحقق الجريمة الإلكترونية إذا كان الدخول غير متعمد واختار الفرد المغادرة فوراً.

([32])Article 323-1- Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de trois ans d'emprisonnement et de 100 000 € d'amende.

ثانيا :- النتيجة الإجرامية في جريمة الهجوم السيبراني.

بعد الفعل الإجرامي، فإن الجانب الثاني للعنصر المادي هو النتيجة الإجرامية. وبغض النظر عما إذا كان السلوك الإجرامي جيداً أم سيئًا، فإنه يستلزم تحولًا في العالم الخارجي. والنتيجة الإجرامية هي اسم هذا التعديل. وهذه النتيجة هي نتيجة للسلوك غير القانوني، والذي يتضمن العدوان الذي ينتهك حق أو مصلحة يحميها القانون جنائيًا. وفي الواقع، فإن النتيجة الإجرامية لها معنيان متميزان. المعنى المادي، الذي يشير إلى التغيير في العالم الخارجي الناتج عن السلوك الإجرامي، هو المعنى الأول. ونتيجة لذلك، يجب أن تكون هناك علاقة سببية مادية بين النتيجة والفعل الذي تسبب فيها. والجرائم المادية أو جرائم الإيذاء هي الأسماء التي تُطلق على هذا النوع من السلوك. وينص المشرع على تحقيق نتيجة في هذه الجرائم. وهذا يشير إلى أن العنصر المادي لهذه الجرائم يتكون من نتائج ملموسة لا لبس فيها يفرضها القانون. وكعنصر من عناصر الجريمة، لا يُرتكب هذا النوع من الجرائم بشكل كامل إلا بعد حدوث النتيجة المحددة مسبقًا.[١].

اما المدلول الثاني المعنى القانوني للنتيجة هو أنها تشكل اعتداءً على مصلحة يحميها القانون، بغض النظر عما إذا كان الاعتداء يسبب ضررًا للمصلحة المحمية أو يعرضها للخطر. تُعرف هذه الجريمة بأنها مجرد سلوك، وتُعرف بغياب نتيجة إجرامية وتركيزها على السلوك نفسه. بمعنى آخر، يتكون مكونها المادي من عنصر واحد فقط: السلوك الإجرامي. وقد قُسِّمت الجريمة إلى فئتين من خلال الفقه الجنائي: جرائم الإيذاء وجرائم الخطر. جريمة الإيذاء هي جريمة يشترط فيها القانون حدوث ضرر فعلي وانتهاك واضح للمصلحة التي يحميها القانون الجنائي. إن الضرر الفعلي الذي يلحق بالمصلحة التي سعى المشرع إلى حمايتها هو نتيجة هذه الجرائم. وعلى النقيض من ذلك، فإن جرائم الخطر تعني فقط تهديدًا للمصلحة المحمية، أي أنها تشكل خطرًا عليها فقط ولا تسبب ضررًا حقيقيًا[٢].

حقيقيًا[٢].

---

(١) د. عمر السعيد رمضان ، فكرة النتيجة في قانون العقوبات ، مجله القانون والاقتصاد ، عدد مارس عام ١٩٦١ ، ص١٠٤

(٢) د. مدحت محمد عبد العزيز ابراهيم ، قانون العقوبات ، القسم العام ، المرجع السابق ، ص٧٥

والسؤال الذي يثور في هذا الصدد هل تعد الجرائم السيبرانية من جرائم الضرر أم انها من جرائم الخطر؟

يمكن وصف أصل الجريمة الإلكترونية بأنها جريمة خطرة، إذ يُفهم النشاط الإجرامي فيها بمجرد تعريض البيانات والمعلومات المخزنة على الحاسوب أو شبكة المعلومات للخطر، إذ تُعتبر من القيم الاجتماعية التي تستوجب من المشرع توفير الحماية الجنائية لها. مع ذلك، تجدر الإشارة إلى أنه يمكن تشديد عقوبة المخترق إذا أدى سلوكه الإجرامي إلى ضرر. ونتيجة لذلك، تنص المادة رقم (١٤) من قانون مكافحة تقنية المعلومات المصري رقم (١٧٥) لسنة ٢٠١٨ على أن "كل من دخل عمداً، أو دخل بخطأ غير مقصود وظل بغير حق، على موقع إلكتروني أو حساب خاص أو نظام معلومات محظور الدخول إليه، يعاقب بالحبس مدة لا تقل عن سنة، وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائة ألف جنيه، أو بإحدى هاتين العقوبتين. وتكون عقوبة هذا الدخول الحبس مدة لا تقل عن سنتين، وغرامة لا تقل عن مائة ألف جنيه ولا تجاوز مائتي ألف جنيه، أو بإحدى هاتين العقوبتين، إذا أدى ذلك إلى إتلاف أو حذف أو تعديل أو نسخ أو إعادة نشر البيانات أو المعلومات الموجودة على ذلك الموقع الإلكتروني أو الحساب الخاص أو نظام المعلومات"[١].

وسوف نعرف فيما يلي لموقف كل من المشرع المصري والفرنسي وإتفاقية بودابست من تجريم الشروع في جرائم الهجوم السيبرانى ، وذلك على النحو الاتي :-

١- موقف المشرع المصري من تجريم الشروع في الجرائم السيبرانية.

بدايةً، جرّم المشرع المصري جميع أنواع محاولات ارتكاب الجرائم الإلكترونية، ولا سيما الجريمة الإلكترونية نفسها. وقد أوضحت المادة (٧٤) من القانون ذلك بوضوح تام. يُعاقب بالحبس مدة

---

(١) كما نصت المادة رقم (٢٣) من ذات القانون على انه " يعاقب بالحبس مدة لا تقل عن ثلاثة أشهر والغرامة التى لا تقل عن ثلاثين ألف جنيه ولا تجاوز خمسين ألف جنيه، أو بإحدى هاتين العقوبتين، كل من استخدم الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات، فى الوصول بدون وجه حق إلى أرقام أو بيانات أو بطاقات البنوك والخدمات أو غيرها من أدوات الدفع الالكترونية ، فإن قصد من ذلك استخدامها فى الحصول على أموال الغير أو ما تتيحه من خدمات، يعاقب بالحبس مدة لا تقل عن خمسين ألف جنيه ولا تجاوز مائة ألف جنيه، أو بإحدى هاتين العقوبتين ، وتكون العقوبة الحبس مدة لا تقل عن سنة، والغرامة التى لا تقل عن مائة ألف جنيه ولا تجاوز مائتى ألف، أو إحدى هاتين العقوبتين، إذا توصل من ذلك إلى الاستيلاء لنفسه أو لغيره على تلك الخدمات أو مال الغير"

لا تزيد على ستة أشهر وبغرامة لا تجاوز خمسمائة جنيه أو بإحدى هاتين العقوبتين، كل من دخل أو حاول الدخول أو حصل أو حاول الحصول على بيانات أو معلومات واردة في سجلات أو حاسب آلي أو وسائط تخزين متصلة بها، أو غيّرها بأية طريقة كانت بإضافة أو حذف أو إلغاء أو إتلاف أو عبث بها، أو أذاعها أو أفصح عنها في غير الأحوال المبينة في القانون ووفقًا للإجراءات المنصوص عليها فيه، وذلك دون الإخلال بأي عقوبة أشد ينص عليها قانون العقوبات أو غيره من القوانين. وقد نص على ذلك قانون الأحوال المدنية رقم ١٤٣ لسنة ١٩٩٤. وتكون عقوبة ارتكاب جريمة ضد البيانات أو المعلومات أو الإحصاءات الحبس. بتحليل هذه المادة، نكتشف أنها تتناول الحماية الجنائية للبيانات والمعلومات المحفوظة في الوثائق أو أجهزة الحاسوب أو وسائط التخزين المتصلة بها، وأن العقوبة واحدة سواءً تم ارتكاب الجريمة أو مجرد الشروع فيها. وتشير المادة إلى أن عقوبة الشروع في هذه الجريمة هي السجن لمدة لا تتجاوز ستة أشهر، أما إذا ارتُكبت الجريمة بالفعل بناءً على البيانات أو المعلومات أو الإحصاءات المجمعة، فإن العقوبة هي السجن.

بالإضافة إلى ذلك، يُعاقب بالأشغال الشاقة المؤقتة كل من انتهك أو شرع في انتهاك سرية البيانات أو المعلومات أو الإحصائيات المتحصل عليها بأية طريقة، وذلك وفقًا للمادة (٧٦) من القانون نفسه. وإذا وقعت الجريمة في زمن الحرب، تكون العقوبة الأشغال الشاقة المؤقتة. وبناءً على ذلك، عاقب المشرع الشروع في انتهاك السرية بالأشغال الشاقة المؤقتة، وعاملها معاملة المخالفات الحقيقية. أما الجريمة المرتكبة في زمن الحرب، فعقوبتها الأشغال الشاقة المؤبدة.

وعلاوة على ذلك، نص المشرع في المادة (٤٠) من قانون مكافحة تقنية المعلومات رقم (١٧٥) لسنة ٢٠١٨ على معاقبة كل من حاول ارتكاب الأذى المنصوص عليه في هذا القانون بعقوبة لا تزيد على الحد الأقصى للعقوبة المقررة للجريمة.

ولذلك، عاقب المشرع الجنائي مجرد الشروع في ارتكاب الجريمة، دون الإصرار على تنفيذها التام واكتمال جميع أركانها. فنصف العقوبة المقررة للجريمة التامة هي العقوبة المنصوص عليها في هذه الحالة.

في الواقع، أخطأ المشرع في صياغة المادة (٤٠) من قانون مكافحة تقنية المعلومات، التي نصت على الشروع في ارتكاب الجنح المنصوص عليها في هذا القانون دون الإشارة إلى الشروع في

ارتكاب الجنايات، مثل جريمة الشروع في التجسس الإلكتروني، التي تناولها الفصل الأول من هذا التشريع، والذي يتناول الجرائم والجنح التي تهدد أمن الحكومة من الخارج. ويبدو أن المشرع قد استند في تحريم محاولة التجسس الإلكتروني إلى الصياغة الفضفاضة للمادة (٤٦) من قانون العقوبات ( ). وفي رأيي، كان من الأنسب للمشرع أن يضع نصاً عاماً يجرم كل من يحاول ارتكاب أي من الجرائم المنصوص عليها في هذا القانون، بغض النظر عما إذا كانت الجريمة جناية أو جنحة. ومن ثم فإننا نقترح تعديل نص المادة (٤٠) من قانون مكافحة جرائم تقنية المعلومات المصري لتقرأ على النحو التالي: كل من حاول ارتكاب أي من الجرائم المنصوص عليها في هذا القانون يعاقب بعقوبة لا تجاوز نصف الحد الأقصى للعقوبة المقررة له"[١] .

٢- موقف المشرع الفرنسي من تجريم الشروع في الجرائم السيبرانية.

في قانون العقوبات الفرنسي، أدرج المشرع الفرنسي بنوداً فريدة تُجرّم محاولة ارتكاب جرائم إلكترونية. ويُجرّم الآن ارتكاب جرائم الاتصال الاحتيالي بنظام معالجة آلي، أو التدخل في تشغيل النظام أو إفساده، أو استخدام مستند مزور، أو حذف البيانات أو تغييرها. ويُعدّ مجرد محاولة ارتكاب هذه الجرائم جريمة يُعاقَب عليها ( ). وبالنظر إلى نص المادة (٤/٣٢٣) من قانون العقوبات الفرنسي الصادر بالقانون رقم (٦٨٣) بتاريخ ٢٢ يوليو ١٩٩٢ والمعدل بالقانون رقم (٢٢) بتاريخ ٢٤ يناير ٢٠٢٣ في المادة رقم (٦) منه، يتبين أنه "يعاقب بالعقوبة المنصوص عليها في الجريمة نفسها أو بعقوبة الجريمة الأشد في حالة تعدد الجرائم كل من اشترك في جماعة مشكلة أو في اتفاق بغرض الإعداد مصحوباً بفعل أو عدة أفعال بدنية بقصد ارتكاب جريمة أو عدة جرائم من الجرائم المنصوص عليها في المواد من (١/٣٢٣) إلى المادة (٣/٣٢٣)."[٢].

([١]) وحسنا ما فعله المشرع السعودي في هذا الشان حيث نصت الماده رقم (٩) من النظام السعودي رقم (١٧) لسنة ٢٠٠٧ بشان مكافحه جرائم المعلوماتية بالمملكه العربية السعوديه على " يعاقب كل من حرّض غيره، أو ساعده، أو اتفق معه على ارتكاب أيٍّ من الجرائم المنصوصعليها في هذا النظام ؛ إذا وقعت الجريمة بناء على هذا التحريض، أو المساعدة، أو الاتفاق، بما لا يتجاوز الحد الأعلى للعقوبة المقررة لها ، ويعاقب بما لا يتجاوز نصف الحد الأعلى للعقوبة المقررة لها إذا لم تقع الجريمة الأصلية". كما نصت المادة العاشرة " عاقب كل من شرع في القيام بأي من الجرائم المنصوصعليها في هذا النظام بما لا يتجاوز نصف الحد الأعلى للعقوبة المقررة. "

([2]) Article 323-4 La participation à un groupement formé ou à une entente établie en vue de la préparation, caractérisée par un ou plusieurs faits matériels, d'une ou de plusieurs des

علاوة على ذلك، تنص المادة (٧/٣٢٣) من قانون العقوبات الفرنسي على أن "محاولة ارتكاب أي جريمة من الجرائم المذكورة في الفصل الثالث من الباب الثاني من الباب الثالث من قانون العقوبات، أو المتعلقة بالاعتداءات على نظام معالجة معلومات آلي، مع الجرائم المنصوص عليها في المواد من (١/٣٢٣) إلى (٣/٣٢٣) يعاقب عليها بالعقوبة المقررة للجريمة بأكملها ( ). وبالنظر إلى نص المادة (٩/٤٤١) من قانون العقوبات الفرنسي ( )، نجد أنها تعاقب على محاولة ارتكاب جريمة استعمال مستند مزور، حيث نصت هذه المادة على عقوبة محاولة الاستخدام المنصوص عليها في المواد (١/٤٤١، ٢)، التي تجرم تزوير مستند رسمي أو عرفي واستعمال مثل هذه المستندات المزورة، وفي المواد من (٤/٤٤١) إلى المادة (٨/٤٤١)، نص المشرع على عقوبة محاولة ارتكاب هذه المواد مع عقوبة الجريمة نفسها.

ثالثا :- رابطه السببيه بين السلوك الإجرامي والنتيجه الإجرامية.

لا يكفي وجود السلوك الإجرامي والنتيجة المعاقب عليها لإثبات العنصر المادي للجريمة. يجب أن يكون العنصر الثالث للعنصر المادي، وهو وجوب وجود علاقة سببية بين الجريمة ونتيجتها، موجوداً. وهذا يعني أن النتيجة غير القانونية يجب أن تكون نتيجة الفعل غير القانوني. إذا ارتُكبت الجريمة عن عمد، فإن الجاني يكون مسؤولاً فقط عن المحاولة؛ وإلا، فهو غير مسؤول عن الفعل بأكمله. ومع ذلك، لا يكون الشخص مسؤولاً عن جريمة غير مقصودة لأنه لا يوجد أي نية متضمنة ( ). وعلى الرغم من وجود العديد من الفرضيات المقترحة فيما يتعلق بالرابط السببي ( )، فإن الرأي السائد في الأوساط القانونية والقضائية هو أن نظرية السببية الصحيحة قيد الاستخدام.[1]، وفقًا لتسلسل الأحداث النموذجي، يكون الجاني مسؤولاً عن الآثار المحتملة أو المتوقعة لأفعاله ما لم يُكسر هذا الرابط

---

infractions prévues par les articles 323-1 à 323-3-1 est punie des peines prévues pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée.

La participation à un groupement formé ou à une entente établie en vue de la préparation, caractérisée par un ou plusieurs faits matériels, d'une ou de plusieurs des infractions prévues par les articles 323-1 à 323-3-1 est punie des peines prévues pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée.

([1]) د. محمد زكي ابو عامر ، قانون العقوبات ، القسم العام ، منشأة المعارف ، الإسكندرية ، ١٩٩٣. ص٧.

سببٌ غير متوقع أو غريب. تُدحض العلاقة السببية في هذه الحالة. في هذه الحالة، يكون الجاني هو السبب المباشر للضرر الذي لحق بالضحية، لأن الفيروس الذي ينقله إلى بريد الضحية الإلكتروني يُسبب إصابة الجهاز بالكامل. ونتيجةً لذلك، يكون هو المسؤول الوحيد عن أفعاله ويتحمل المسؤولية الكاملة. ووفقًا لنظرية السببية المناسبة، تُلغى جريمة إتلاف موقع إلكتروني في هذه الحالة، ويُحاسب الجاني فقط على جريمة الوصول غير القانوني إلى الموقع، بافتراض أن الموقع قد تعرض للتلف أو التدمير سابقًا لسببٍ يتعلق بنظام شبكة المعلومات، مما يُشير إلى عدم ضلوع الجاني في ذلك التدمير أو التدمير. وبالمثل، إذا اخترق شخصٌ موقع الشركة القابضة لتوزيع الكهرباء، وقام شخصٌ آخر في الوقت نفسه باختراقه، مما أدى إلى تلف النظام وانقطاع التيار الكهربائي، فإن الشخص الأول مسؤولٌ فقط عن الاختراق، بينما يكون الشخص الثاني مسؤولًا عن كلٍّ من الاختراق والضرر. بما أن الجريمة الإلكترونية تُعتبر جريمةً جسيمة، فمن البديهي أن الجريمة تُرتكب لمجرد انخراط الجاني في نشاط إجرامي، بغض النظر عما إذا كان قد تسبب في أي ضرر. ولا يُبرر تشديد العقوبة إلا عند حدوث ضرر. ونتيجةً لذلك، غالبًا ما تكون الجريمة الإلكترونية غير مرتبطة بالسببية.

المطلب الثاني

الركن المعنوى لجريمة الهجوم السيبرانى

إن وجود العناصر المادية للجريمة لا يكفي لإثبات المسؤولية الجنائية. ومع ذلك، يجب أن يكون الفرد قد ارتكب خطأ. ومن الممكن أن يكون هذا الخطأ قد حدث عن عمد أو عن طريق الصدفة. ونتيجة لذلك، قد تُرتكب الجريمة عمدًا، وفي هذه الحالة يتمثل العنصر الأخلاقي في القصد، أو عن غير قصد، وفي هذه الحالة يتمثل العنصر الأخلاقي في خطأ غير مقصود ()). وعندما يتعلق الأمر بالجرائم الإلكترونية، فإن هذه الجرائم هي أفعال متعمدة تتطلب نية إجرامية واسعة ( )، مما يعني وجود عنصري المعرفة والإرادة، وهما ضروريان لارتكابها. وإذا كان أحد هذين العنصرين مفقودًا، فلن

تحدث الجريمة الإلكترونية. وهذه هي المكونات الأساسية للجريمة الإلكترونية، بغض النظر عما إذا كانت موجودة أم غائبة.[١].

مع وضع هذا في الاعتبار، فإن عنصري المعرفة والإرادة هما أساس هذه الجريمة. إن فهم الجاني لجوهر الجريمة هو كيفية اكتساب المعرفة بالجرائم الإلكترونية. يجب أن يدركوا أن الفعل الذي يقومون به هو هجوم أو وصول غير قانوني إلى معلومات وبيانات يحميها القانون. سواء كانت البيانات تتعلق بالأفراد، أو الدولة، أو إحدى وكالاتها، أو الجوانب الاجتماعية أو الاقتصادية لحياة الناس، أو حياتهم الخاصة، فهذا لا يزال صحيحاً. علاوة على ذلك، يجب أن يكون الجاني على دراية بتداعيات سلوكه، مما يعني أنه يجب أن يفهم أنه سيؤدي إلى انتهاك البيانات المحمية التي لا يمكن للجمهور الوصول إليها. هذه المعلومات ليست متاحة للجميع، ولا يُسمح لهم بالاطلاع عليها أو الوصول إليها. كما يُحظر عليهم استخدام أي طرق إلكترونية للوصول إلى هذه المعلومات أو إفشائها أو تسريبها لأي شخص آخر. باختصار، تشبه الجريمة الإلكترونية الجريمة التقليدية من حيث أنها تتطلب من مجرم الإنترنت أن يكون على دراية بما يفعله. وفي هذه الحالة لا تقوم المسئولية إذا كان الجاني معرضاً لموانع المسئولية أو لموانع العقاب وفقاً لما هو محدد في المواد (٦٠ إلى ٦٣) من قانون العقوبات المصري.

الجريمة الإلكترونية مميزة وذاتية بطبيعتها، وتعتمد على ذكاء الجاني ومهارته. ولهذا السبب، أعتقد أن مجرمي الإنترنت يدركون دائمًا طبيعة الفعل الذي يقومون به مسبقًا، ومع ذلك يواصلون تنفيذه مرارًا وتكرارًا. وهذا أكثر شيوعًا في الدول التي لا تزال تعاني من فجوة تشريعية تجعل هذه الجريمة غير قانونية. الإرادة هي العنصر الثاني من الركن الأخلاقي للجريمة الإلكترونية، وتشير إلى قدرة الشخص على اختيار الانخراط في سلوك معين أو الامتناع عنه. بمعنى آخر، يجب على الجاني القيام بأفعال نفسية معينة بقصد تحقيق النتيجة الإجرامية المقصودة. الغرض من الإرادة ليس مجرد التحريض على السلوك الإجرامي؛ بل يهدف أيضًا إلى تحقيق النتيجة المقصودة. أي بيان آخر من شأنه

([١]) د. هشام محمد فريد رستم ، قانون العقوبات ومخاطر تقنية المعلومات، الطبعة الثانية، مكتبة الآلات الحديثة، مصر، ١٩٩٢ ، ص٦٣.

أن يقوض الطبيعة النفسية والواقعية للإرادة. عندما يكون الفعل الإجرامي والرغبة في تحقيق النتيجة موجودين معًا، يتم إثبات القصد الإجرامي.[١].

هذا يعني أنه في الجرائم الإلكترونية، يتوافر ركن الإرادة بتوجيه إرادة الجاني نحو الجوانب المادية للجريمة، أي إرادة ارتكاب الفعل والنتيجة الإجرامية المترتبة عليه. ويجب أن تكون إدارة الجاني موجهة نحو تنفيذ الفعل أو السلوك الذي يُشكل الجريمة الإلكترونية، كالدخول غير المصرح به أو المخالف لشروط الترخيص، أو أي اقتحام غير مشروع لنظام معلوماتي أو حاسوب أو شبكة معلوماتية أو ما شابه. كما يجب أن يكون لسلوكه النتيجة الإجرامية المحددة في إرادته.[٢].

الخاتمة

بدأتُ موضوع دراستي، "الإطار الموضوعي لجريمة الهجوم الإلكتروني"، بعون الله وتوجيهه. تُعرّف اتفاقية منظمة شنغهاي للتعاون الجريمة الإلكترونية بأنها أي جريمة تستهدف المعلومات الحاسوبية، بينما تعريفنا هو أي جريمة تتعلق بالمعلومات الحاسوبية. وبشكل أعم، تُعرّف اتفاقية منظمة شنغهاي للتعاون جرائم المعلومات بأنها استخدام موارد المعلومات في الفضاء الإلكتروني والتلاعب بها لأغراض غير مشروعة. نعتقد أن الإنترنت يلعب دوراً هاماً في تحول الجرائم الإلكترونية إلى جرائم عابرة للحدود الوطنية وعابرة للقارات، إذ تُرتكب الجريمة في بلد واحد وتمتد آثارها إلى بلدان أخرى. لذا، فإن التعاون الدولي المشترك ضروري لمعالجة القضايا الفريدة التي تطرحها هذه الجرائم وتذليل أكبر العوائق أمام التعاون على نطاق عالمي. وفيما يلي أهم الاستنتاجات والاقتراحات التي توصلت إليها دراستنا:

أولا: النتائج:

---

(١) د. أحمد فتحى سرور ، الوسيط فى قانون العقوبات ، القسم العام ، دار النهضة العربية ، القاهرة ، ١٩٩٦ ، بند رقم ٢٢٩ ، ص٣٤٩ ، د. محمد عبد اللطيف فرج ، شرح قانون العقوبات – القسم العام – دار النهضة العربية ، القاهرة ، ٢٠١٢ ، ص٢٥٠.

(٢) د. على حمزة عسل الخفاجي ، فاعلية السياسة الجنائية لحماية الأمن السيبرانى ، المرجع السابق ، ص٨٢.

١. ١. واكبت التطورات التكنولوجية في أنظمة الاتصالات والمعلومات المعاصرة نمو الجرائم الإلكترونية بجميع مظاهرها.

٢. ٢. على الرغم من أن السياسة الجنائية الحديثة قد أحرزت تقدماً ملحوظًا في معالجة الجرائم الإلكترونية بشكل عام، على الصعيدين المحلي والدولي، إلا أن فعالية هذه الجهود قد تضاءلت إلى حد ما بسبب ضعف التنسيق والتعاون بين الدول.

٣. ٣. وفيما يتعلق بمكافحة جرائم تكنولوجيا المعلومات، صدر القانون المصري رقم ١٧٥ لسنة ٢٠١٨ ولائحته التنفيذية رقم ١٦٩٩ لسنة ٢٠٢٠. ووفقًا لمبدأ المعاملة بالمثل أو في إطار الاتفاقيات الدولية والإقليمية والثنائية المصدق عليها، تلتزم الجهات المصرية المختصة بتسهيل التعاون مع نظيراتها في الدول الأجنبية من خلال تبادل المعلومات لضمان منع جرائم تكنولوجيا المعلومات والمساعدة في التحقيق فيها وتعقب مرتكبيها، وذلك وفقًا لما ورد في المادة (٤) من القانون، المتعلقة بالتعاون الدولي في مكافحة جرائم تكنولوجيا المعلومات. وفي هذا الصدد، ستكون الجهة الفنية المعتمدة هي المركز الوطني للاستعداد لطوارئ الحاسبات والشبكات التابع للجهاز القومي لتنظيم الاتصالات.

ثانيًا: التوصيات:

من خلال تحليل هذا البحث ونتائجه كما هو موضح أعلاه، يُمكننا استخلاص عدد من المقترحات حول كيفية مكافحة الجرائم الإلكترونية، وخاصةً الجرائم الإلكترونية العابرة للحدود الوطنية. وبناءً على ذلك، أقترح ما يلي:

١. الدعوة إلى وضع اتفاقية دولية موحدة في إطار الأمم المتحدة لمكافحة الجرائم الإلكترونية، تُنظّم هذا النوع من الجرائم بما يحمي حقوق الأطراف الموقعة دون المساس بمبدأ السيادة.

٢. وفقًا لمبدأ العالمية، ينبغي التعامل مع الجرائم الإلكترونية كجريمة تخضع للولاية القضائية الكاملة للتشريعات الجنائية، وينبغي تسهيل عمل المنظمات الدولية.

٣. ضرورة قيام الدول بإنشاء منظمات ذات خبرة جنائية في مجال الأمن السيبراني.

٤. التركيز على زيادة وعي المستخدمين من خلال نشر المعلومات، وخاصةً المعلومات الشخصية والحساسة.

تم بحمد الله وعونه،،

قائمة المراجع

أولًا: الكتب القانونية العامة:

١. أحمد شوقي ابو خطوة، شرح الاحكام العامة لقانون العقوبات، دار النهضة العربية، ٢٠٠٣.

٢. أحمد فتحى سرور، الوسيط فى قانون العقوبات، القسم العام، دار النهضة العربية، القاهرة، ١٩٩٦ م.

٣. أحمد فتحي سرور: الوسيط في قانون العقوبات، القسم العام، الطبعة السادسة، مطورة ومحديثة، ٢٠١٥م.

٤. أمين مصطفي محمد السيد، علم الجزاء الجنائي، الجازء الجنائي بين النظرية والتطبيق، دار الجامعة الجديدة، الإسكندرية، ١٩٩٠م.
٥. جميل عبدالباقي الصغير، علم العقاب، دار النهضة العربية، القاهرة، ط١، ١٩٩٨م.
٦. عبد العظيم مرسي وزير، شرح قانون العقوبات، القسم العام، الجزء الاول، الطبعه الخامسة
٧. فوزية عبد الستار، مبادئ علم الإجرام والعقاب، دار النهضة العربية، القاهرة، ١٩٨٥م.
٨. مامون محمد سلامة، قانون العقوبات، القسم العام، دار الفكر العربي، طبعه ١٩٧٩.
٩. محمد زكي ابو عامر، قانون العقوبات، القسم العام، منشأة المعارف، الإسكندرية، ١٩٩٣.
١٠. محمد صبحي نجم، قانون العقوبات، القسم العام، النظرية العامة للجريمة، مكتبه دار الثقافه، عمان، الاردن، ١٩٩٦م.
١١. محمد عبد اللطيف فرج، شرح قانون العقوبات – القسم العام – دار النهضة العربية، القاهرة، ٢٠١٢م.
١٢. محمود محمود مصطفى، شرح قانون العقوبات، القسم العام، الطبعه العاشره، مطبعه جامعه القاهرة، ١٩٨٣م.
١٣. محمود نجيب حسني، شرح قانون العقوبات، القسم العام، دار النهضة العربية، الطبعة السادسة، ١٩٨٩م.
١٤. محمود نجيب حسني، شرح قانون العقوبات، القسم العام، النظرية العامة للجريمة والنظرية العامة للعقوبة والتدبير الاحترازي، دار النهضة العربية، القاهرة، نادي القضاة، ط ٨، ٢٠١٨.
١٥. مدحت محمد عبد العزيز ابراهيم، قانون العقوبات، القسم العام، النظرية العامة للجريمة والمساهمة الجنائية، الجزء الثاني، دار النهضة العربية، ٢٠٠٩.

ثانيًا: الكتب القانونية المتخصصة:

١. إبراهيم رمضان عطايا، الجريمة الإلكترونية وسبل مواجهتها في الشريعة الإسلامية والأنظمة الدولية، مكتبة الوفاء القانونية، القاهرة، ٢٠٢٢م.

٢. أحمد خليفة الملط، "الجرائم المعلوماتية"، الطبعة الثانية، دار الفكر الجامعي، الإسكندرية، ٢٠٠٦م.
٣. أشرف شوقي عبد الوهاب عطية، الحماية الجنائية للسجين، دراسة مقارنة بين القانون الوضعي والشريعة الإسلامية، دار النهضة العربية، القاهرة، ٢٠١٥م .
٤. تميم عبد الله سيف التميمي، "الجرائم المعلوماتية في الاعتداء على الأشخاص"، مكتبة القانون والاقتصاد، الرياض، الطبعة الأولى، ٢٠١٦م.
٥. حازم حسن الجمل، الحماية الجنائية للأمن الإلكترونى، دار الفكر والقانون، المنصورة، ٢٠٢٢.
٦. حسام الدين محمد أحمد، النظرية العامة للعقوبة والتدابير الاحترازية، دار النهضة العربية، القاهرة، ١٩٧٧م.
٧. حسين بن سعيد الغافرى، السياسة الجنائية فى مواجهة جرائم الإنترنت، دار النهضة العربية، القاهرة، ٢٠٠٩ م.
٨. دحان حزام القريطى، الجرائم السيبرانية والتحديات الإجرائية لحماية الأمن السيبرانى، دار الفكر الجامعى، الاسكندرية، ٢٠٢٥ م.
٩. ذياب موسى البيداني الشباب والأنترنت والمخدرات، الطبعة الأولى، أكاديمية نايف العربية، الرياض السعودية، ٢٠١٢م.
١٠. رؤوف عبيد، السببية في القانون الجنائي، الطبعه الثانيه، مطبعه نهضة مصر، ١٩٦٦.
١١. سفيان سوير، "جرائم المعلوماتية"، مذكرة ماجستير، جامعة أبو بكر بلقايد بتلمسان، كلية الحقوق والعلوم السياسية، قسم الحقوق، ٢٠١٠-٢٠١١.
١٢. الشحات ابراهيم محمد منصور، الجرائم الإلكترونية في الشريعة الاسلامية والقوانين الوضعية، دار الفكر العربي، مصر، ٢٠١١ .
١٣. طارق ابراهيم الدسوقي عطية، الأمن المعلوماتي، نظام قانون الحماية المعلوماتية، دار الجامعة الجديدة للنشر، الإسكندرية، ٢٠٠٩.

١٤. عبد العال الدريبي، د .محمد صادق إسماعيل، "الجريمة الإلكترونية"، الطبعة الأولى، المركز القومي للإصدارات القانونية، القاهرة، ٢٠١٢.
١٥. عبد الفتاح بيومى حجازى، جرائم الكمبيوتر والانترنت في التشريعات العربية، الطبعة الاولي، دارالنهضة العربية، ٢٠٠٩.
١٦. عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، طبعه ٢٠٠٩.
١٧. عبد الفتاح بيومي حجازي: الأحداث والأنترنت دراسة متعمقة عن أثر الأنترنت في أنحراف الأحداث، دار الكتب القانونية، مصر، ٢٠٠٧م.
١٨. عبد الله حسين على محمود، سرقة المعلومات المخزنة فى الحاسب الآلى، الطبعة الأولى، دار النهضة العربية، القاهرة، ٢٠٠١ .
١٩. عبد المنعم درويش، رؤية تحليلية لوظيفة العقوبة في القانون الروماني، فكرتي الردع العام والخاص، مع الإشارة للوضع في الفقه الإسلامي، دار النهضة العربية، القاهرة، ٢٠٠٥م.
٢٠. عفيفى كامل عفيفى، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، دراسة مقارنة، منشأة المعارف، الإسكندرية ٢٠٠٣م.
٢١. على حسن عبدالحسن، الحماية الجزائية للأمن الأسرى من التطور التكنولوجى دراسة مقارنة، دار مصر للنشر، القاهرة، ٢٠٢١.
٢٢. على حمزة عسل خفاجى الجرائم الناشئة عن إختراق الأمن السيبرانى وآليات مكافحتها، دار مصر للنشر والتوزيع، ٢٠٢٥ .
٢٣. علي جبار الحسيناوي، جرائم الحاسب الآلي ومشكلة قرصنة البرامج، دار وائل للنشر، عمان، الطبعة الأولى، ٢٠٠٥.
٢٤. علي حمزة عسل الخفاجي، فاعلية السياسية الجنائية لحماية الأمن السيبراني، دار مصر النشر والتوزيع، ٢٠٢٥ م.

٢٥. علي سعيد الحيان الغامدي: الحماية الجنائية للمراهقين من المؤثرات الجنسية دراسة مقارنة، الطبعة الأولى، مركز الدراسات العربية، مصر، ٢٠١٥.
٢٦. عماد محمد سلامة، الحماية القانونية لبرامج الحاسوب والإنترنت، مطابع اليازوري الأردن، ٢٠٠٩.
٢٧. عمر ابو الفتوح عبد العظيم الحمامي، الحماية الجنائية للمعلومات المسجله الكترونيا، دراسة مقارنة، دار النهضة العربية، القاهرة، ٢٠١٠ .
٢٨. فتحي محمد انور عزت، تفتيش شبكة الإنترنت لضبط جرائم الاعتداء على الآداب العامة والشرف والاعتبارات التي تقع بواسطتها المركز القومي للإصدارات القانونية، القاهرة، الطبعة الأولى، ٢٠١٢م.
٢٩. محمد أبو العلا عقيدة، النظرية العامة للعقوبة والتدابير الاحترازية، دار النهضة العربية، القاهرة، ٢٠٠٩م.
٣٠. محمد أمين الرومى، جرائم الكمبيوتر والإنترنت، دار المطبوعات الجامعية، الاسكندرية، ٢٠٠٤.
٣١. محمد حسين، المسئولية القانونية فى مجال شبكات الإنترنت، الطبعة الاولى، دار النهضة العربية ٢٠٠٢.
٣٢. محمد زكي أبو عامر، دراسة في علم الإجرام والعقاب – القسم الثاني– علم العقاب، ١٩٨٧
٣٣. محمد سامى الشوا، ثورة المعلومات وإنعكاساتها على قانون العقوبات، دار النهضة العربية، القاهرة ١٩٩٤م.
٣٤. محمد عبدالله أبو بكر سلامة، موسوعة جرائم المعلوماتية – جرائم الكمبيوتر والإنترنت، المكتب العربي الحديث، القاهرة، ٢٠١٥م.
٣٥. محمود أحمد القرعان، "الجرائم الإلكترونية"، دار وائل للنشر والتوزيع، عمان، الطبعة الأولى، ٢٠١٧.

٣٦. هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، الطبعة الثانية، مكتبة الآلات الحديثة، مصر، ١٩٩٢.
٣٧. وفاء محمد صافي، الحماية الجنائية لجريمة القرصنة الإلكترونية لحقوق الملكية الفكرية الإلكترونية، مركز الدراسات العربية للنشر والتوزيع، القاهرة، ٢٠٢٢م.
٣٨. ولنفس المؤلف: الامتناع عن النطق بالعقاب في القانون الكويتي، دراسة مقارنة بنظام الاختبار القضائي في القانونين المصري والفرنسي، دار الجامعة الجديدة، الإسكندرية، ط٢، ٢٠١٢م.

ثالثًا: الدوريات والمجلات العلمية:

١. أحمد عبد الكريم سلامه، الإنترنت والقانون الدولي الخاص بالتعاون مع مركز الامارات للدراسات والبحوث الاستراتيجية، مركز تقنية المعلومات بدولة الامارات العربية المتحده في الفترة من ٣١ مايو ٢٠٠٠.
٢. رحيمة نميلي، "خصوصية الجريمة الإلكترونية في القانون الجزائري والقوانين المقارنة"، مداخلة مقدمة في أعمال المؤتمر الدولي الرابع عشر، طرابلس، الموسوم بعنوان: "الجرائم الإلكترونية"، طرابلس، يومي ٢٤ و٢٥ مارس .
٣. سعد عاطف عبد المطلب حسنين، احكام المسئوليه الجنائية عن الجرائم المعلوماتية، دراسة مقارنة، بحث منشور بمجله الدراسات القانونيه والاقتصاديه، مجله كليه الحقوق جامعه مدينه السادات، ٢٠٢٣ م
٤. عبدالله عبد الكريم عبدالله، "جرائم المعلوماتية والإنترنت"، منشورات الحلبي الحقوقية، بيروت، ٢٠٠٧،.
٥. عمر السعيد رمضان، فكرة النتيجة في قانون العقوبات، مجله القانون والاقتصاد، عدد مارس عام ١٩٦١م.

٦. موسى مسعود ارحومة،السياسة الجنائية فى مواجهة جرائم الإنترنت، بحث منشور بمجلة الدراسات القانونية، كلية القانون، جامعة قاريونس، العدد ١٧، منشور في الجريده الرسميه العدد ٢٣ (تابع) في ٩ يونيو ١٩٩٤

٧. هدى حامد قشقوش، جرائم الحاسب اللي في التشريع المقارن، دار النهضة العربية، القاهرة، ١٩٩٢.

٨. هشام محمد فريد رستم، "الجرائم المعلوماتية أصول التحقيق الجنائي الفني واقتراح إنشاء آلية حربية موحدة للتدريب التخصصي"، بحوث مؤتمر القانون والكمبيوتر والإنترنت، جامعة الإمارات المتحدة، كلية الشريعة والقانون، الطبعة الثالثة، المجلد الثاني، ٢٠٠٤.

٩. يونس عرب، الخصوصية وأمن المعلومات فى الأعمال الاسلكية بواسطة الهاتف الخلوى، ورقة مقدمة إلى منتدى العمل الإلكترونى بواسطة الهاتف الخلوى، إتحاد المصارف العربية ، عمان، الآردن ٢٠٠١.

ثانيًا: المراجع باللغة الفرنسية:

1. Bauman : Problèmes réels et faux problèmes de la réforme du droit pénal en République fédérale d'Allemagne, Rev. Sc. Crime, 1970, .
2. E.cesay : preuves numériques et criminalité informatique "Londres, Academic Press", 2000,. & D.parker : Combattre la Criminalité informatique (paris, oros), 1985, & M. Chawki, Combattre LaCybercriminalite, Université Lyon III, France, 2008.
3. Riza Azmi et Kautsarina, Revisting cyber definition, Conférence européenne sur la cyberguerre et la sécurité, juillet 2019.
4. TOM Forester, Essential problèmes to High-tech Society First MIT Prés édition, Cambridge, Massachusetts, 1989.
5. Madhava Soma Sundaram, Cyber Crime and Digital Disorder, K. Jaishankar, Londres 2011,
6. Étude sur le piratage éthique Bhawana Sahare1, Ankit Naik2, Shashikala Khandey, International Journal of Computer Science Trends and Technology (IJCST) Volume 2 Numéro 4, novembre-décembre 2014
7. Voir : Dr. Mohammed Buzubar : "La Criminalité Informatique sur L'internet", Journal of Law, (Kwait University), No. 1,.26, mars 2002.

8. Roger Merle et André ViTu : Traité de Droit criminel, Droit pénal, Troisième édition, 1979, n° 467 ; Frédéric DESPORTES et Francis LE GMNEHEC, le nouveau Droit pénal, tome 1, Droit pénal général, sixième édition, no 460.
9. Jonathan Herring M.A., Marise Cremona B.A. : Criminal Law, deuxième édition, Macmillan, Londres, 1998, .
10. International Journal Of Engineering And Computer Science ISSN : 2319-7242 Volume 6 Numéro 4 avril 2017

ثالثًا: المواقع الالكترونية:

- Le sommet de Berlin, relative à la cybercriminalité n' aura permis de dégager qu' une seule certitude, une définition universelle de la cybercriminalité et l'on peut même se demander si une entente sera un jour possible» L'impossible définition universel de la cybercriminalité,

http:// www.vilage -justice.com