مجلة دراسات في سيكولوجية الانحراف
مجلة علمية دولية نصف سنوية ISSN :2602- 554X EISSN :2773-2568
المجلد :08 العدد:01 السنة :2023 ص- ص:360- 377

الجريمة الإلكترونية والآليات الدولية لمكافحتها

Cybercrime and international mechanisms to fight it

بريزة زدام *
مخبر سيكولوجية مستعمل الطريق
جامعة باتنة1 الجزائر
bariza.zedam@univ-batna.dz

سمية بن سماعين
مخبر بنك الاختبارات النفسية والمدرسية والمهنية
جامعة باتنة1 الجزائر
soumia.bensmaine@univ-batna.dz

تاريخ الاستلام: 2023/01/21 تاريخ القبول : 2023/04/22

ملخص:

يعاني العالم اليوم من ظاهرة خطيرة تهدد أمنه نتجت عن تطور تكنولوجيا الاتصال والتي تعرف بالجريمة الالكترونية، الأمر الذي أرق الدول و همها مكافحتها والتصدي لها، رغم الجهود إلا أن أمن وسرية المعلومات مازال في خطر لأن هذا النوع من الجرائم له خصوصية تميزه عن الجرائم العادية من حيث: الآثار والأضرار الناجمة عنها، الحداثة، سرعة الانتشار فهي عابرة للحدود، صعوبة اكتشافها، إثباتها و كشف هوية المجرم الالكتروني. تهدف الدراسة إلى تحديد بعض المفاهيم المتعلقة بالجريمة الالكترونية، أركانها و سمات المجرم الالكتروني. خلصت الدراسة إلى أنه لا يوجد مفهوم موحد للجريمة الالكترونية رغم انتشارها وكونها ظاهرة عالمية خطيرة وصعوبة التعرف على مرتكبيها و كذا عدم وصول الدول إلى اتفاقيات مشتركة لمكافحتها.

الكلمات المفتاحية:

الجريمة الإلكترونية؛ قانون؛ المجرم الالكتروني؛ المعاهدات الدولية.

Abstract:

Today's world suffers from a serious phenomenon that threatens its security because of the development of communication technology, namely cybercrime, which has thinned States to combat and respond to it. Despite efforts, information security is at risk because electronic crimes have a distinctive specificity in terms of: damage caused, modernity, speed of spread, difficulty in detecting and proving the identity of the cybercriminal. The study aims to identify certain concepts of cybercrime, its components, features, and to detect perpetrators of cybercrime .The study showed that, despite its prevalence and being a global phenomenon, there is no standard concept of cybercrime. Also it is difficult to identify its perpetrators and reach common conventions to combat it.

Keywords :

Cybe crime; law; cyber criminal; International treaties.

* المؤلف المرسل .

مقدمة:

يعرف العالم اليوم تطورا سريعا في مجال الإعلام والاتصال وذلك من خلال شبكة الانترنت وما تلعبه من دور محوري في نقل المعلومات، حيث أصبحت قوة لا يستهان بها ولا يمكن الاستغناء عنها لما تقدمه للفرد والمجتمع، وبالرغم مما تتمتع به تكنولوجيا المعلومات من إيجابيات إلا أن المعلومة ليست في مأمن وأصبحت تستخدم كأداة للاعتداء على الأشخاص ماديا ومعنويا فساهمت في تطوير طرق الإجرام، مما نتج عنه نوع جديد من الجرائم ما كانت لتظهر للعيان لولا التقدم الكبير والشامل لأجهزة الحاسوب الآلي والأنظمة المعلوماتية التي لا تخلو مؤسسة أو شركة أو بيت من هذه الأجهزة ، وهذا التطور كما له قيمة مضافة للإنسان إلا أنه لم يخلو من السلبيات وكان نقمة على البعض؛ لاستغلاله في أغراض الابتزاز والتشهير وكسب المال الغير مشروع من ضحايا هذه الخروقات الإلكترونية وساهم بصفة كبيرة في ظهور ما يعرف باسم الجريمة الالكترونية أو الجريمة المعلوماتية والتي انتشرت بشكل سريع وبأدوات جد متطورة فأصبحت تأرق و تهدد أمن المجتمعات والدول دون تمييز بينها.(لخضر. 2021، ص: 188). ونذكر على سبيل المثال التطور العددي للجرائم السيبرانية في الجزائر وكان تطورا تصاعديا مخيفا فقد سجلت البلاد في الفترة الممتدة مابين 2013 و 2016 تقريبا نسبة 86% (سنة 2013سجل عدد الجرائم الإلكترونية 91 جريمة في حين كانت في 2016 2130جريمة الكترونية). وقد عرف عام 2020 تطورا هائلا للجريمة السيبرانية جراء الآثار السلبية لجائحة كورونا والتي ساهمت بشكل كبير في نمائها واستفحالها (جمال، عبد الرحمن، 2022، ص ص 9-10) وذلك جراء تدابير الحجر الصحي التي فرضتها الجائحة ، حيث استغل المتورطون هذه الفترة للقيام بأعمالهم الإجرامية، حيث عرفت عدة ولايات الوسط بالجزائر و التي تضم 11 ولاية إحصاء 2026 قضية تخص المساس بأنظمة المعالجة الآلية للمعطيات تورط فيها 1514 شخص وعولج منها 1264 قضية، في حين تم إحصاء 2618 قضية وتوقيف 3717 شخص بخصوص مكافحة جرائم الاقتصادية والمالية خلال نفس الفترة. وفيا يتعلق بالجرائم المعلوماتية والنصب والاحتيال عبر الأنترنيت وحسب فرقة مكافحة جرائم المعلوماتية التابعة للمديرية العامة للأمن الوطني أحصت 152 قضية التي أضفت إلى توقيف 216 شخصا خلال الفترة الممتدة بين جانفي إلى 30 سبتمبر 2020 . وكما سيعرف العالم بحلول 2025 خسائر الجرائم الإلكترونية بقيمة تقدر بـ 10,50 تريليون دولار بحسب شركة Cybersecurity Ventures حسب موقع العربية نت.

ومن أجل دراسة مدى انتشار واستفحال الظاهرة أجريت عدة دراسات كثيرة ولعل أهمها الدراسة التي قام بها الموقع العالمي comaritech .com في سنة 2019 للتعرف على خطورة الجرائم السيبرانية

في الجزائر وقد شملت الدراسة 60 دولة من بينها دول عربية وأجنبية من بينها الجزائر، احتلت فيها الجزائر المرتبة الأولى من ضمن 60 دولة التي شملتها الدراسة بنسبة 55,75 % والتي تعبر عن أنها تمتلك أضعف أمن إلكتروني، في حين احتلت اليابان المرتبة 60 بنسبة 8,81 % يعني أنها تمتلك أقوى أمن إلكتروني (زينب و مجيد، 2020، ص ص 780-794).

ونظرا لأهمية وحداثة الموضوع تناولت هذه الدراسة تعريف وتحديد المفاهيم الخاصة بالجريمة الالكترونية، الأطر القانونية الخاصة بها، إبراز أهم سمات المجرم الالكتروني، ضبط مفهوم الجريمة الالكترونية ومفهوم المجرم الإلكتروني لمحاولة تحديد وكشف هويته والوصول إليه من أجل التحكم في هذه الظاهرة والتصدي لها؛ من خلال المشاركة الدولية الفعالة والناجعة لبذل المزيد من الجهود من طرف المختصين في المجال الإلكتروني والجريمة الإلكترونية؛ وذلك بسن قوانين رادعة و بناء اتفاقيات ومعاهدات تجرم الأشخاص المتسببين في تطور الجريمة الإلكترونية، ومن خلال هذا العرض نطرح الإشكالية التالية: ما هي الجريمة الإلكترونية والآليات الدولية لمكافحتها؟

وللإجابة على هذه الإشكالية اعتمدنا الخطة التالية: قسم يتحدث عن الجريمة الإلكترونية و سمات المجرم الإلكتروني، وخصائص الجريمة المعلوماتية، وأركانها، والقسم الثاني حاولنا عرض بعض المواثيق الدولية لمكافحة الجريمة الإلكترونية.

1. تعريف الجريمة الإلكترونية (المعلوماتية):

نجد للجريمة الالكترونية عدة تعاريف ولكن لخصوصيتها وطبيعتها المختلفة عن باقي أنواع الجرائم لم يتفق المختصون على وضع تعريف موحد لها، حيث تعددت الآراء والأفكار بشان المفهوم، فهناك من حاول واعتمد في تعريفه على الجانب الفني وهناك من اعتمد على الجانب القانوني وهناك من اعتمد على معايير أخرى مختلفة ومن بين هذه المحاولات التعريف الصادر عن منظمة التعاون الاقتصادي للتنمية حيث عرفت الجريمة الالكترونية "بأنها كل فعل أو امتناع من شأنه الاعتداء على الأموال المادية والمعنوية، يكون ناتجا بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية"(أحمد خليفة. 2006، ص: 96).

كما عرفها الألماني تيدمان بأنها كل أشكال السلوك غير المشروع الذي يرتكب باستخدام الحاسب.

وعرفها أيضا روزنبلات على أنها:" نشاط غير مشروع موجه لنسخ أو الوصول إلى المعلومات المخزنة داخل الحاسوب أو تغييرها أو حذفها"

وقد عرف مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين المنعقد في فيينا عاصمة النمسا سنة 2000 الجريمة المعلوماتية بأنها" أية جريمة يمكن ارتكابها بواسطة نظام حاسوبي او

شبكة حاسوبية أو داخل نظام حاسوب والجريمة تلك تشمل من الناحية المبدئية جميع الجرائم التي كان ارتكبتها في بيئة الكترونية".

وعرفت أيضا بأنها" كل فعل غير مشروع اقترن بالتواصل مع منظومات معلوماتية وشبكات الاتصال الخاصة به، والتي يحميها قانون العقوبات ويفرض عقابا لها".

أما تعريف المشرع الجزائري للجريمة الالكترونية:

فقد حرم المشرع الجزائري الجريمة المعلوماتية نتيجة تأثر الجزائر بالثورة المعلوماتية التي نتج عنها أشكال جديدة من الجرائم، وذلك من خلال التعديل الذي ادخله على قانون العقوبات بموجب القانون 04-15 (الأمر رقم ¬66-156 المؤرخ في 10 جوان 1966 يتضمن قانون العقوبات، الصادرة بتاريخ 11 جوان 1996) (الجريدة الرسمية قانون رقم 04-15، 2004) المتمم لقانون العقوبات، الذي افرد قسما خاصا بها في المواد من 394مكرر إلى 294مكرر 07.

واستعمل القانون 09-04 تسمية " المساس بأنظمة المعالجة الآلية للمعطيات" للدلالة على الجريمة المعلوماتية معتبرا في ذلك أن النظام المعلوماتي في حد ذاته وما يشمله من مكونات غير مادية محلا للجريمة، حيث جاء ذلك في نص المادة 02، فنصت الفقرة "أ" على أن الجرائم المتصلة بتكنولوجيات الإعلام والاتصال هي جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات، وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الالكترونية، وعرفت الفقرة "ب" من نفس المادة المنظومة المعلوماتية بأنها: " مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة فيما بينها، فيما ينوب واحد منها أو أكثر بالمعالجة الآلية للمعطيات تنفيذا لبرنامج معين".

إن الاختلاف في تعريف الجريمة الالكترونية ووضع تعريفا محددا وشاملا لها يعود إلى اختلاف الزوايا التي ينظر منها من حيث موضوع الجريمة، مرتكب الجريمة، أداة الجريمة (محمد حمادة. 2005، ص:201).

من خلال ما سبق يمكن وضع تعريف شامل للجريمة الالكترونية على أنها هي كل فعل إجرامي يقوم به المجرم الالكتروني في العالم الافتراضي لتحقيق مكسب مادي خاصة المال أو معنوي كإثبات قدراته الإجرامية عن طريق السرقة والابتزاز أو إلحاق أضرار مادية ببعض الشركات المالية الكبرى أو مؤسسات وهيئات مؤيدة لقضايا معينة في العالم أو المناهضة لفكر أو تيار معين وكل ذلك باستخدام الحاسب الآلي موصول بالإنترنت وبكبسة أصبع فقط.

2. خصائص الجريمة الالكترونية:

تختلف الجريمة الالكترونية عن الجريمة الكلاسيكية بعدة خصائص نورد بعضها في النقاط التالية:

1.2. جريمة عابرة للحدود والقارات:

ساهمت شبكة المعلومات في توسيع عملية الاتصال وتبادل المعلومات بين الدول والأنظمة التي يفصل بينها آلاف الأميال، ومع القدرة التي يتمتع بها الحاسوب أدى ذلك إلى إمكانية ارتكاب الجريمة الالكترونية في أماكن متعددة من العام وفي وقت واحد، كما يمكن أن يكون المجني عليه في غير الدولة التي يقيم فيها الجاني (القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004 المتتم لقانون العقوبات، العدد 17، الصادرة بتاريخ 10 نوفمبر 2004).

و ما ينذر بزيادتها أنها لا تعترف بعنصر الزمان والمكان ولا بالحدود بين الدول ولا حتى بين القارات، وما يتطلبه الأمر من أجل القيام بأعمال الجريمة الإلكترونية إلا جهاز حاسب آلي ومتصل بشبكة النت و كبسة أصبع وهو جالس في مكانه ويجنى الأموال الكثيرة أو ينشر فيروسا أو يهدد مؤسسة أو شخصا معينا(لخضر. 2021، ص: 189).

2.2 . ارتكاب الجرائم الالكترونية بالحاسب الآلي:

تعتبر هذه الخاصية من أهم الخصائص التي تميز الجرائم الالكترونية عن الجرائم الكلاسيكية، ذلك لان شبكة الانترنت هي إحدى التقنيات الحديثة التي افرزها تطور الحاسوب ولذلك فان ارتباطها بالحاسب الآلي هو أمر لا مفر منه باعتباره النافذة التي تطل بها تلك الشبكة على العالم الخارجي(أمين. 2015، ص: 15).

3.2.خصوصية مرتكبي الجريمة الالكترونية:

الجريمة الالكترونية تتأثر بالمستوى العلمي للمجرم كقاعدة عامة عكس الجريمة التقليدية، حيث لا تتطلب عادة الاختصاص والمعرفة، عكس ما يحدث في مجال تقنية المعلومات وقد يتعدد تصنيف مجرمي الجريمة الالكترونية إلى المحترفين والحاقدين، وذلك نظرا للصفات التي تتمتع بها مثل هذه الجرائم.

4.2. صعوبة إثبات الجريمة الالكترونية:

تكمن الصعوبة في إثبات الجريمة الالكترونية ذلك لأنها تحدث في الخفاء وعدم وجود أي أثر ايجابي لما يجري خلال تنفيذها من أفعال إجرامية، حيث يتم نقل المعلومات الكترونيا فضلا عن إمكانية تدمير المعلومات التي يمكن أن تستخدم كدليل في مدة قد تقل عن الثانية الواحدة، زيادة على ذلك أن

الجريمة المعلوماتية لا عنف فيها وإنما هي أرقام وبيانات تمحى من السجلات المخزنة في ذاكرة الحاسوب، حيث تصبح غير مرئية وبمعنى آخر فالجرائم الالكترونية هي جرائم فنية هادئة، حيث يتم اكتشاف 1% فقط من هذه الجرائم أما المبلغ عنها لا تتعدى 5% وحتى ما طرح أمام القضاء من هذه الجرائم فان أدلة الإدانة فيه لم تكن كافية إلا في حدود الخمس(محمد حمادة. 2005، ص: 210) .

5.2. أسلوب ارتكاب الجريمة الالكترونية:

إن الإجرام الالكتروني هو إجرام الأذكياء بالمقارنة بالإجرام الكلاسيكي الذي يميل إلى العنف، كما أن المجرم الإلكتروني عادة ما يكون ذو مهارات تقنية عالية وإلمام كبير بتكنولوجيا المعلومات والاتصال(أحمد خليفة. 2006، ص: 114).

في حين نجد الجريمة التقليدية تستدعي جهدا عضليا كممارسة العنف اللفظي والعنف البدني خاصة، ونجد عكس ذلك في الجريمة الالكترونية حيث تعرف بأنها جرائم هادئة وتتصف بالنعومة واللباقة اللفظية لأنها تتم بمجرد الضغط على زر معين وكتابة رقم سري وتبدأ الجريمة الالكترونية وتستلزم الذكاء وطول البال كما يستلزم أن يكون متصل بشبكة الانترنيت وتوفر عنصر الإرادة.

6.2.الجريمة الالكترونية تتم عادة بتعاون أكثر من شخص:

تتم الجريمة المعلوماتية عادة بتعاون أكثر من شخص على ارتكابها وإلحاق أضرارا بالمجني عليه، وغالبا ما يشترك في إخراج الجريمة إلى حيز الوجود شخص متخصص في تقنيات الحاسوب والانترنت يقوم بالجانب الفني للمشروع الإجرامي وشخص آخر من المحيط أو من خارج المؤسسة المجني عليها مهمته تغطية عملية التلاعب وتحويل المكاسب إليه، والاشتراك في إخراج الجريمة الالكترونية إلى حيز الوجود قد يكون اشتراكا سلبيا وهو الذي يترجم بالصمت من جانب من يعلم بوقوع الجريمة في محاولة منه لتسهيل إتمامها مقابل مبلغ مادي متفق عليه مسبقا وقد يكون اشتراكا إيجابيا ويتمثل غالبا في المساعدة الفنية أو المادية وتقاسم الأموال بينهم(نهلا. 2008، ص: 58).

3. أركان الجريمة الالكترونية:

أركان الجريمة الالكترونية لها نفس أركان الجريمة الكلاسيكية مع اختلاف بسيط وهذه الأركان هي:

1.3.الركن الشرعي للجريمة الالكترونية:

لقد جرمت وحرمت كل الشرائع والقوانين الدولية الجرائم الالكترونية وشددت العقوبات على المخالفين ومرتكبي هذا النوع من الجرائم، مثلا نجد المشرع الجزائري كان صارما في إصدار وتطبيق قوانين رادعة للمجرم الالكتروني.

ووفقا لأحكام المادة الأولى من قانون العقوبات الجزائري التي تنص على: "لا جريمة ولا عقوبة أو تدابير امن بغير قانون"، جرم القانون رقم 04-15 بعض صور الجريمة الالكترونية ونص على العقوبات المقررة لمرتكبيها في القسم السابع مكرر تحت عنوان "المساس بأنظمة المعالجة الآلية للمعطيات" من الفصل الثالث المعنون "الجنايات والجنح ضد الأموال من الباب الثاني المتعلق " بالجنايات والجنح ضد الأفراد وذلك في المواد من 394 مكرر إلى 394 مكرر 08 من قانون العقوبات المعدل والمتمم.

ولجأ المشرع الجزائري إلى تقنين مثل هكذا جرائم وجعلها في نطاق مبدأ الشرعية حيث يمنع القاضي من اللجوء إلى القياس، بمعنى عدم جواز لجوء القاضي الجنائي إلى قياس فعل لم يرد نص على تجريمه على فعل ورد نص بتجريمه، فيقرر القاضي الجنائي للأول العقوبة للثاني بسبب التشابه بين الفعلين(أحمد خليفة. 2006، ص: 10).

2.3.الركن المادي للجريمة الالكترونية:

قاعدة معروفة في القانون أنه " لا جريمة دون ركن مادي " أو " لا جريمة إلا بفعل"(عبد الرحمن. 2012، ص: 101) إلا أن الركن المادي للجريمة الالكترونية يختلف نوعا ما عن الجرائم التقليدية لأنه يقوم على عدة صور في فعل اعتداء والمتمثلة فيما يلي:

1.2.3إدخال المعطيات عن طريق الغش:

حسب المادة 394مكرر 01 من قانون العقوبات نعنى بفعل الإدخال: إضافة معطيات جديدة إلى نظام المعالجة الآلية أو التعديل من معلومات داخلية كان يتضمنها مسبقا فغير فيها، ومثال ذلك حالة الاستخدام التعسفي لبطاقات السحب والائتمان سواء من صاحبها الشرعي أو عن غيره كحالة السرقة والتزوير(أمال. 2007، ص: 121).

2.2.3 الدخول أو البقاء غير المشروع في نظام المعالجة الآلية للمعطيات أو الشروع في ذلك:

حسب المادة 394 مكرر في قانون العقوبات ينص على أن الدخول والبقاء غير المشروع في نظام المعالجة الآلية للمعطيات أو الشروع في ذلك يشكل فعلا إجراميا، انطلاقا من هذا نحدد صورتين لهذا الفعل وهما:

أ. **الصورة البسيطة**:يتمثل النشاط الإجرامي في:

- **فعل الدخول**: والذي يتحقق بمجرد الوصول إلى المعلومات المخزنة داخل النظام ودون علم ورضا صاحب المعلومات، لأن هذا النظام لا يسمح للدخول فيه إلا لأشخاص معينين أو يسمح بالدخول لكن بمقابل.

- **البقاء:** يعنى التواجد داخل نظام المعالجة الآلية للمعطيات والذي في الحقيقة هو ضد إرادة من له الحق في السيطرة على هذا النظام، أو بتجاوز المدة المسموح له بالبقاء فيها، أو عدم الانسحاب فورا وقطع وجوده في نظام البيانات أو يطبع أو ينسخ معلومات حين يسمح له بالرؤية فقط (أمين، 2015، ص: 32).

ب.الصورة المشددة: نصت المادة السابقة في الفقرتين 1و2 من قانون العقوبات على ظروف تشدد عقوبة فعل الدخول والبقاء غير المشروع عندما ينتج عن هذين الفعلين إما محو أو تحويل المعطيات والمعلومات التي يحتويها النظام، وإما عدم صلاحية النظام لأداء وظائفه من خلال تخريب اشتغال المنظومة المعلوماتية.

3.3.الركن المعنوي للجريمة الالكترونية:

ونعني به القصد الجنائي أو النية الجنائية والذي يتحقق بتوفر إرادة وإصرار على عمل غير شرعي ومخالف للقانون لدى الجاني مع علمه بان القانون يجرمه ويعاقب عليه(عبد الرحمن. 2012، ص: 101) هذا بالنسبة للجرائم التقليدية.

ونفس الأمر ينطبق على الجريمة الالكترونية التي يقوم ركنها المعنوي على توافر الإرادة أو النية الإجرامية لدى الفاعل، ونستدل بذلك على أن المشرع استعمل عبارات "الغش" " العمد "" الإعداد للجريمة" في المواد المشار إليها أعلاه، وهذا دليل على أن الجريمة الالكترونية جريمة عمدية قصدية.

ومثال ذلك جريمة الاحتيال الالكتروني التي بدورها تعد جريمة عمدية يتطلب لقيامها توافر القصد الجنائي لقيام مسؤولية الجاني، والقصد الجنائي المشترط هو القصد الجنائي بنوعيه العام والخاص، فالمجرم يعلم بأنه يخالف القانون بسلوكه مع نيته لتحقيق ربح غير مشروع له أو لغيره وتجريد شخص من ممتلكاته على نحو غير مشروع(أحمد خليفة. 2006، ص: 121) كما أن المجرم الالكتروني يحقق ربح معنوي غير مشروع كالشعور باللذة والمتعة وإشباع غرائزه، لا يمكن لأي هيئة أن تقيم الأضرار التي يخلفها والأذى الذي يلحقه بالآخرين من خلال التشهير بالأشخاص ونشر الإشاعات، مثلا التقاط صور لضحايا حوادث المرور وعرضها على منصات التواصل الاجتماعي مهما كانت حالتهم دون احترام الضحايا أو أهلهم وذويهم أو الأشخاص الذين سيطلعون على هذه الصور المفزعة,

4. سمات المجرم الالكتروني: هناك عدة صفات للمجرم الالكتروني منها:

1.4.إنسان متخصص:

المجرم الالكتروني إنسان متخصص ماهر في مجال الحاسوب وتقنياته، يستغل ما له من مهارات في الاختراق ليحوز المعلومات المختلفة التي تساعده في جرائمه من نصب واعتداء وابتزاز مقابل المال، ثم يخفي كل أثر لجريمته فلا تكشفه أي أنظمة أمنية بتعددها وتخصصها (بشرى. 2014، ص: 59).

2.4.الشخصية الاجتماعية (إنسان اجتماعي):

يعتبر المجرم الالكتروني إنسانا اجتماعيا قادرا على التكيف مع المجتمع ومتوافق معه كونه شديد الذكاء، في معظم الأحيان يكون موثوقا من محيطه وبعيدا عن الشبهات وهو الأمر الذي يجعله يتمادى في جرائمه العسيرة الاكتشاف، ولكنه يقترف هذه الجرائم بدافع اللهو أو لمجرد إظهار تفوقه على الكمبيوتر أو على البرامج التي يتم تشغيلها بها (عبد الفتاح. 1982، ص: 45).

3.4.الاحترافية والذكاء:

يتميز المجرم الالكتروني بالذكاء وعدم الميول لاستعمال العنف والقوة (محمد أمين. 2004، ص: 22) وهذا الأمر بديهي فالمجرم الذكي يسعى لإخفاء جريمته بإحكام وذلك بعدم ترك أدلة ضده فيفضل العمل بهدوء ولا يلجأ للعنف الذي يترك دليلا ماديا واضحا. ولأن الجريمة الالكترونية توافي شروط عمله كونها تتطلب قدرة ذهنية وعقلية عميقة، فهو يستخدم طرقا جديدة لا يعرفها أحد سواه؛ فكلما قلت معرفة الآخرين بالطريقة، كلما صعب اكتشافها من طرف عناصر الأمن المتخصصة.

4.4.تكرار الجريمة نفسها:

كمجرم الكتروني فهو شخص عائد، يرجع إلى الثغرات التي أدت إلى كشفه، وان لم يفلح في سدها فانه سيضبط مجددا بنفس الجريمة ويقاد مرة أخرى إلى المحاكمة.

5.4.السلطة تجاه النظام الالكتروني المعلوماتي:

وهي مجموعة من الحقوق والمزايا التي تميز المجرم الالكتروني وتضمن له ارتكاب جريمته، تتمثل في الشيفرة الخاصة بالدخول إلى النظام الذي يحتوي على المعلومات التي تتيح فتح الملفات ومحو المعلومات أو تعديلها؛ وأيضا استعمال الأنظمة المعلوماتية بشتى الطرق، وتتمثل أيضا السلطة في استعمال الأنظمة المعلوماتية أو إجراء بعض التعاملات، أو بمجرد الدخول إلى الأماكن التي تحتوي على هذه الأنظمة(نهلا. 2008، ص ص:80-81).

5.أصناف المجرم الالكتروني:

إن الجرائم الالكترونية جرائم مستحدثة وجاءت نتيجة الثورة العلمية الحالية والتي تبدأ وتنتهي بالضغط على زر معين من طرف مجرم الكتروني ذكي وهادئ ومختلف عن كل مجرم، وهذا الذي صعب تحديد أنماطه ولكن رغم هذا حدد عدة أنواع وأصناف للمجرم الالكتروني ونذكر منها ما يلي:

1.5.القراصنة:

ويتميزون بالخبرة والكفاءة في مجال الكمبيوتر وهدفهم كسر الحواجز الأمنية للدخول إلى أنظمة غير مسموح الدخول إليها وهم نوعان:

5-1-1القراصنة الهواة العابثون(الهاكرز):

الهاكرز هم مبرمجون يتميزون بالذكاء المعلوماتي بهدف الدخول إلى أنظمة الحاسبات الآلية غير مسموح بالدخول إليها، ليس لتخريب المعطيات الموجودة داخل النظام، لكن لأجل إثبات الذات وإشباع الفضول ودافعهم ليس إجرامي وهم يحتلون مكانة مرموقة في المجتمع.

وهناك قراصنة يتميزون بأخلاقهم (قراصنة أخلاقيون)، هدفهم قرصنة المواقع لحجب ما فيها وما تعرضه من أمور غير أخلاقية، ومنهم من يسعون إلى اكتشاف ثغرات في أنظمة المؤسسات المالية قصد سدها ويسمون أيضا بذوي القبعات البيضاء، ويتعلمون طرق الاختراق من أجل الدفاع والتأمين والحماية لا من أجل إلحاق الأضرار بالآخرين.

وتطلق كلمة هاكرز على الذين يخترقون الأنظمة الالكترونية والبيانات ويستولون على المعلومات بالسطو أو الإتلاف ويسمون في الغالب بذوي القبعات السوداء ويتفرعون إلى ثلاث مجموعات:

أ. القراصنة المحترفون(الكراكرز):

هدفهم الرئيسي هو التخريب، هذا النوع يعتمد على خبرته وقدرته التقنية الواسعة وكفاءته وخبرته في استخدام برامج تقنية معينة للحصول على معلومات وبيانات سرية، والاستيلاء على بطاقات الائتمان، وتدمير وإتلاف وتشفير ملفات مهمة لبيعها أو الاستفادة منها بتغيير كلمات المرور، ويطلق عليهم اسم العناكب لأنهم يعملون في الخفاء وفي الفضاء الالكتروني ولا يتركون أثارا مادية لأفعالهم لذلك فهم خطيرون إلى درجة كبيرة(غنية. 2015، ص: 15)

أخطر نوع من الكراكرز وهم المبتدئون والذين يستخدمون برامج التخريب دون علم، ويقومون في غالب الأحيان بإلحاق أضرار كبيرة دون علم وغالبا ما ينتهي بهم الأمر في قبضة أجهزة الأمن السيبراني لأنهم لا يخفون معالم جرائمهم.

ب. السكامرز:

هم أشخاص غير محترفين ولا يمتلكون مهارات فريدة في مجال البرمجة ولا في مجال الاختراق، ويلجئون إلى استخدام الهندسة العكسية الاجتماعية وإلى الحيل والمخططات من أجل الحصول على مبتغاهم ويكون عادة المال.

ت. السبامرز:

وهذا النوع الذين يعمدون إلى إرسال رسائل غير ذي صلة وغير مرغوب فيها لأكبر عدد من مستخدمي الانترنت قصد الإشهار غير المدفوع، أو نشر البرامج الضارة وغير أخلاقية، وتعد سرقة الأموال هدف هذه الفئة.

2. صغار السن:

هم الأشخاص "الصغار المتحمسين للحاسوب، يتصفون بالشعور بالبهجة والسعادة ودافعهم في ذلك هو التحدي لكسر الرموز السرية لتركيبات الحاسوب"(علي حسن. 2008، ص: 49)، وشاع تسميتهم في نطاق الدراسات الإعلامية والتقنية والدراسات الاستطلاعية بمصطلح (المتلعثمين)، ومن أمثلة جرائمهم ما حدث في ألمانيا حيث تمكن طالب عمره (19 سنة) من نسخ وإفشاء بيانات حاسب آلي على نحو غير مصرح به، مما أدى إلى خسارة هذه الصناعة في ألمانيا بمبلغ (23ألف مارك ألماني) واستفاد الجاني بمبلغ (26 ألف مارك)(عبد الفتاح. 2007، ص: 81)

وتوجد فئة أخرى يطلق عليها صغار نوابغ المعلوماتية ويقصد بهم الشباب البالغ المحب و المفتون بالمعلومات وأنظمتها(محمد سامي. 1994، ص: 39)

3.أصحاب الآراء المتطرفة:

وهم الجماعات الإرهابية المتطرفة ذوي المعتقدات المختلفة والتي يرغبون في فرضها بأي طريقة، وغالبا ما ينتهجون أسلوب العنف، وقد ساعدتهم في الانتشار مواقع التواصل الاجتماعي وضم أشخاص جدد ومتعددي الجنسيات والثقافات والمعتقدات ومن هنا يتم الهجوم على المواقع المخالفة لمعتقداتهم وفكرهم المتطرف والقيام بغلقها وحجبها(غنية. 2015، ص: 16)

4.مجرمو المعلوماتية في إطار الجريمة المنظمة:

وغرضهم من النشاط الإجرامي هو تحقيق ربح مادي بطريقة غير مشروعة، ويعمل المنتمون إلى هذه الفئة في أغلب الأحوال بطرق منظمة،حيث ينطبق على أفعالهم وصف الجريمة المنظمة، أو على الأقل يشترك في تنفيذ النشاط الإجرامي أكثر من فاعل، ويقترب المجرم المعلوماتي المنتمي إلى هذه الطائفة في سماته من المجرم التقليدي.

إن جرائم الحاسبات الآلية بدأت تجذب بشكل كبير اهتمام الجماعات الإجرامية المنظمة نظرا لارتفاع قيمة ما تدره من أرباح مادية مع صعوبة الكشف عنها وإثباتها بالمقارنة بالجرائم التقليدية(نائلة. 2005، ص:62)

ويمكن للمجرم الإلكتروني الانضواء تحت كل الأصناف التي ذكرناها سابقا.

5.الآليات المطبقة والتعاون الدولي لمكافحة الجريمة المعلوماتية:

نظرا للتسارع الكبير في مجال التطور الإلكتروني واختلاف مستعمليه أصبح لزاما على كل الأنظمة باستعمال هذه التقنية الجديدة لأجل مواكبة الثورة الإلكترونية الهائلة وعدم الاستغناء عنها ولكن هذا التطور استغله البعض في ممارسة نشاطاتهم الغير مشروعة للإطاحة بحكم وأنظمة هذه الدول، باعتبار أن الفضاء الإلكتروني لا يملكه أحد ويدخل إليه كل من يمتلك جهاز حاسوب إما بالصلاح أو يعيث الفساد كل شخص ورغبته في استغلال هذا التطور، ولهذا ولأجل التصدي لهذه الظاهرة يجب تضافر الجهود الدولية للحد من انتشارها بزيادة، ويتم ذلك بإنشاء قوانين ومواثيق واتفاقيات دولية مشتركة واستحداث مسارات دولية سلسة وفعالة لتطبيق ما جاء في هذه المواثيق للتصدي لمثل هكذا جرائم.

1.5.التعاون القضائي في مكافحة الجريمة المعلوماتية الدولية:

إن إجراءات التحقيق والملاحقة القضائية في جرائم الإنترنت تقتضي تتبع النشاط الإجرامي الأمر الذي يستوجب تقصي آثار الجريمة من مصدرها إلى غاية تنفيذها وتحديد مواقع الأضرار التي مستها، وهذه الأفعال قد تقع في مختلف البلدان ولهذا يتطلب ملاحقة مرتكبي هذه الجرائم وذلك بالتعاون القضائي الدولي وتمديد صلاحيتها إلى كل البلدان ليكون التعاون دولي وفعال للقضاء على هذه الظاهرة الإجرامية ونستعرض هنا شكلين من أشكال التعاون القضائي وهما:

1-1-5 التعاون الأمني:

بما أن الجريمة الإلكترونية دولية فمن المفروض أن لا تكون الحدود الجغرافية معضلة تقف في وجه الإجراءات الجنائية للتصدي لهذه الجرائم و ملاحقة مجرمي المعلومات المنتشرين في كل مكان، فمثلا يمكننا أن نجد مجرم يحمل جنسية دولة معينة ويقوم بأفعاله ونشاطاته في نطاق وبأجهزة دولة أخرى في حيث تقع آثار و أضرار هذه الجريمة على دولة أخرى، ولذا كانت الحاجة ملحة وضرورية جدا لتوحيد الجهود وتضافر كل الدول بقوانينها ومراسيمها الجنائية أن تتوحد لمتابعة مجرمي المعلومات للكشف عن هوياتهم وشركائهم والمؤسسات التي تساعدهم في ذلك، لأن جهود الدولة الواحدة و بأنظمتها الأمنية لا يكفي للقضاء على الجريمة الإلكترونية؛ لأنها تطارد مجرمين في نطاقها

الجغرافي فقط وفي حالة فرار المجرم إلى دولة أخرى تتوقف على ملاحقته وهو يستمر في أفعاله الغير مشروعة وكبد الدولة التي يتواجد بها أضرار مماثلة للتي قام بها في دولته الأم (مصطفى، القادر، 2022، ص ص:1222-1244) وهناك عدة أشكال للتعاون الأمني لمكافحة الجريمة الإلكترونية وهي:

أ. **إنشاء مكاتب وهيئات متخصصة لجمع المعلومات حول مرتكبي الجرائم الإلكترونية ونشرها:**

الغرض منها هو تنمية تعاون السلطات القضائية الدولية في مجال مكافحة الجريمة، من خلال جمع البيانات والمعلومات الخاصة بالمجرم وتعميمها بين الدول وكذا تبادل الخبرات وتقديم العون لكل الأطراف أن استلزم الأمر ذلك.

ب. **التعاون في إطار المنظمة العالمية للشرطة الجنائية " الأنتربول":**

الهدف من إنشاءها هو تأكيد وتشجيع التعاون الدولي بين أجهزة الشرطة بشكل فعال وسلس في مكافحة الجريمة الإلكترونية والمنتمون إليها سواء أشخاص أو مؤسسات، وذلك بجمع المعلومات والبيانات عن هؤلاء المجرمين من خلال المكاتب المركزية الوطنية للشرطة الدولية المتواجدة في كل دولة منضوية تحتها، وتبادلها فيما بينها، وقد ساهمت هذه المنظمة الدولية في حل الكثير من القضايا المتعلقة بالجريمة الإلكترونية خاصة فيما يتعلق بتبييض الأموال و التجارة الإلكترونية و القبض على عدة مجرمين المبحوث عنهم وتسليمهم للدولة لمقاضاتهم وتسليط العقوبات عليهم.

ت. **القيام بعمليات أمنية مشتركة لمتابعة مجرمي المعلومات:**

ويتم وذلك بتتبع الأدلة والبيانات الرقمية وضبطها والقيام بعمليات التفتيش العابر للحدود لمكونات الأجهزة الإلكترونية منها أجهزة الإعلام الآلي وشبكات الاتصال للبحث عن الأدلة والبراهين، وهذا لا يتأتى إلا بالتعاون الدولي والاشتراك في عمليات نوعية مكثفة ودورية وفي مناسبات خاصة، وما من شأنه أن يصقل المهارات وتبادل الأفكار والخبرات بين المشاركين ذلك لمكافحة للجريمة الإلكترونية والتصدي لها.

5-1-2. المساعدات الدولية القضائية لمكافحة الجريمة الالكترونية:

يمكننا استنتاج المبادئ العامة التي تحكم الالتزام بالمساعدة القضائية المتبادلة في الفقرة 1 من المادة 25 من اتفاقية بودباست بالمجر للإجرام الإلكتروني والالتزام بالمساعدة، يجب أن يتوفر لأقصى حد ممكن وتكون شاملة وممتدة وخالية من الصعوبات و المعوقات(عبد الله. 2007، ص: 327) وتتخذ المساعدة القضائية عدة أشكال نذكر منها:

أ. **تبادل المعلومات حول الجريمة الإلكترونية:**

ويتم ذلك بتبادل البيانات والوثائق والمواد الاستدلالية التي تطلبها السلطة القضائية بصدد النظر في جريمة ما، وتبادل السوابق القضائية للمتابعين وملفاتهم القضائية للجرائم المتابع فيها في دولته الأصل، ونجد لهده الصورة تطبيقات عديدة منها ما ورد في الفقرتين 6و7 من المادة الأولى من معاهدة الأمم المتحدة النموذجية لتبادل المساعدة في القضايا الجنائية وكذلك الفقرات 3و4 من المادة الثامنة من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة.

ب. **نقل الإجراءات الجنائية لجرائم المعلومات:**

يقصد به قيام دولة معينة بموجب اتفاقية معينة باتخاذ جملة من الإجراءات الجنائية بصدد جريمة ارتكبت في حدود دولة أخرى ولمصلحة تلك الدولة بناء على توفر جملة من الشروط من أهمها التجريم المزدوج الذي يعني أن يكون الفعل مجرم في كل من الدولة الطالبة والدولة المطلوب لها نقل الإجراءات بالإضافة إلى مشروعية الإجراءات المطلوب اتخاذها أي أن توافق قانون الدولة المطلوب منها وأن تكون جدية وذات أهمية بالقدر الذي يسهم في الوصول إلى الحقيقة في الكشف عن ملابسات الجريمة، وقد أقرت العديد من المواثيق والمعاهدات على هذا الشكل نذكر مثلا معاهدة الأمم المتحدة النموذجية بشأن نقل الإجراءات في المسائل الجنائية(مصطفى، عبد القادر، 2022، ص ص: 1222-1244)واتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية في مادتها 21 والمادة 23 من اتفاقية بودباست للإجرام الالكتروني.

ت. **الإنابة القضائية الدولية:**

وتعني اتخاذ إجراء قانوني من إجراءات الدعوى الجنائية لأثره المباشر من أجل الفصل في مسألة معروضة على السلطة القضائية التي تعذر على الدولة التي تقدمت بطلب الإنابة القيام به بنفسها، والهدف منها هو تسهيل الإجراءات الجنائية بين الدول لضمان إجراء التحقيقات اللازمة لتقديم المتهمين للمحاكمة. وعادة ما يتم طلب الإنابة عبر قنوات ديبلوماسية تفاديا لتعقيدات الإجراءات وبطئها للتعجيل بتطبيق الإجراءات وغالبا ما تكون الطلبات موجهة إلى وزارة العدل.

وبالرغم من أن التعاون القضائي في مجال مكافحة الجريمة الإلكترونية يشكل أحد أهم الآليات والسياسات لمكافحتها إلا أن الملاحظ أن أغلبية الاتفاقيات والمعاهدات كانت سطحية في تطرقها للجريمة الإلكترونية، ولأن الوضع الدولي العام يوحي بعمق الأضرار والآثار السلبية للجريمة الالكترونية الناجمة عن التطور السريع في هذا المجال فإن هذا الوضع ينذر بخطر كبير على المجموعة الدولية وعلى أمنها الإلكتروني لهذا باتت الحاجة ملحة وضرورية إلى عقد اجتماعات عاجلة وعقد اتفاقيات

تواكب هذا التطور الهائل في المجال الالكتروني و المعلوماتي ويجب أن تتصف هذه الاتفاقيات بالصرامة، الفعالية، الالتزام بتطبيق فحواها بشكل صادق وحقيقي.

2.5تطبيق سياسة تسليم المجرمين كآلية دولية لمكافحة الجرائم الالكترونية:

إن عملية تسليم المجرمين تعتبر شكلا من أشكال مكافحة الجريمة الإلكترونية على الصعيد العالمي والذي اتخذته أغلب الدول للحفاظ على أمنها الإلكتروني وجاءت كنتيجة حتمية للتطور السريع في مجال الاتصالات والمعلوماتية، والذي لا يمر يوم إلا ونسمع عن اكتشافات واختراعات من شأنها تطوير تقنية معينة في هذا الخصوص، وأصبح المجرم الإلكتروني أكثر ذكاء وسريعا في تنفيذه جريمته في عدة دول وفي وقت قصير، كأن يخطط لعملية إجرامية إلكترونية في دولة ما ويطبقها في أخرى لضرب استقرارها وإلحاق الضرر بالأخرى.

1.2.5 أشكال تسليم المجرمين الإلكترونين:

وفقا للممارسات الدولية في مجال مكافحة الجريمة الإلكترونية قد وضعت ثلاث أنظمة لتسليم المجرمين الإلكترونين وهي:

أ. **التسليم القضائي:**

والذي يميزه هو أن الجهة القضائية هي التي تتحمل مسئولية إصدار قرار تسليم المجرمين إلى الدول التي طلبت بذلك وكذا الحفاظ على حقوق الأفراد في دفاعهم عن أنفسهم، ومن سلبيات هذا النوع البطء في إجراءات التسليم وهذا ما ينعكس سلبا على ما تستدعيه سرعة ملاحقة المجرمين لسهولة اندثار أدلة الإثبات عليها.

ب. **التسليم الإداري:**

والجهة المختصة في تسليم المجرمين هي السلطة التنفيذية والتي تملك الصلاحية المطلقة لقرار التسليم من عدمه ويتميز بالسرعة وتجنب الإجراءات التي تعيق من إنهاء عملية التسليم وما يعاب عليها أنها مهدرة لحقوق الأفراد الدفاعية، وكذا خضوع قرار التسليم إلى اعتبارات سياسية، مع جهل الجهة المنفذة للتسليم بالخلفية القانونية(مصطفى، عبد القادر، 2022، ص ص: 1222-1244).

ت. **التسليم المختلط:**

وهو الأكثر انتشارا، وهو مزيج بين مميزات النظامين السابقين وهو يسهل الإجراءات ويقوم على تسريعها ويضمن حق الدفاع للمتهمين.

3.5. قانون الأونيسترال النموذجي:

جاء هذا القانون بعد اقتناع الدول المتضررة من الجرائم الإلكترونية وإيمانا منها بأن الحماية الدولية للأشخاص والمؤسسات العالمية لا تتأتى إلا بتضافر جهودها والعمل بطريقة شاملة وديناميكية لمكافحة ظاهرة الإجرام الالكتروني، وقد صيغ هذا القانون من قانون متعلق بالتجارة الإلكترونية والآخر بشأن التوقيعات الإلكترونية.

5-3-1القانون المتعلق بالتجارة الإلكترونية:

تنطبق نصوصه على أي نوع من المعلومات التي تكون على شكل رسالة بيانات مستخدمة في سياق نشاط تجاري، يتم تسليمها وتخزينها بوسائل إلكترونية، ويتم تبادلها ونقلها إلكترونيا من حاسب آلي إلى أخر باستعمال معيار متعارف ومتفق عليه(محمد. 2006، ص: 92)

5-3-2 القانون المتعلق بالتوقيعات الإلكترونية:

وجاء هذا القانون لتعويض التوقيعات التقليدية بالتوقيعات الإلكترونية لكسر قيود المسافات والأقاليم الدولية لأنه يتسم بالسرعة والسرية، وهو عبارة عن رمز سري أو شفرة سرية التي يتم الحصول عليها بعد عدة إجراءات، واعتمد هذا القانون بتاريخ:05 جويلية 2001(وسام. 2013، ص:253)

ولكن ورغم كل هذه الآليات والجهود الدولية لمكافحة الجريمة الإلكترونية إلا أنها تبقى بعيدة عن المأمول، بسبب العوائق التي تحول دون ذلك، وهذا راجع إلى عدة أسباب نذكر منها ما يلي:

- عدم وجود تنسيق وانسجام الرؤى فيما يتعلق بالإجراءات الجنائية الخاصة بالجريمة الالكترونية كأشكال التحقيق والحصول على الأدلة والبراهين.
- عدم وجود اتفاقيات ومعاهدات حقيقية وصارمة وفعالة تضمن التحقيق الإلكتروني الصارم والمثمر خاصة خارج حدود الدول.
- قصور التشريع الخاص بالجريمة الإلكترونية وعدم مسايرته للتطور السريع لتكنولوجيا الاتصال والمعلومات.
- انعدام الثقة الأمنية فيما يتعلق بالجانب الإلكتروني وعدم السماح للمحققين بولوج أنظمة الأجهزة الإلكترونية للدول خوفا من الاعتداء على سيادة هذه الدول.

خاتمة:

إن الجرائم الالكترونية ظاهرة عالمية خطيرة تهدد كيان كل الدول والمجتمعات على اختلاف ثقافاتها وأيديولوجياتها، في كل المجالات وعلى كل الأصعدة وهذا نظرا لحداثتها واختلافها عن الجرائم التقليدية

الكلاسيكية وخصوصية سرعتها وصعوبة اكتشافها وتحديد مرتكبيها، بالرغم من الجهود التي بذلتها الدول بصفة منفردة وبكل استقلالية وفرض أنظمة وقرارات لمكافحتها داخل حدودها ، وكذا الجهود الدولية المشتركة في إنشاء قوانين ومواثيق دولية والتي اشتركت في وضعها أغلب دول العالم، لكن تبقى هذه الجهود غير كافية وغير ناجعة نظرا للتطور السريع والمفاجئ للجريمة الإلكترونية مما يستدعي التدخل السريع والفعال من قبل الأنظمة الدولية إلى إنشاء مواثيق وقوانين مشتركة و تسهيل التدخلات الفعالة فيما بينها للتخفيف من هذه الظاهرة العالمية العابرة للحدود ولا تحتاج الكثير من الوقت، مما سبق نستخلص ما يلي:

1- بما أن الجريمة الالكترونية مفهوم حديث وجديد، فإن أغلب المهتمين لم يتفقوا على وضع اسم موحد لها.

2- لا يوجد مفهوم موحد وشامل عالميا للجريمة الالكترونية رغم انتشارها وكونها ظاهرة عالمية خطيرة.

3- صعوبة التعرف على مرتكبي الجريمة الالكترونية لاختلافها المتباين عن الجريمة الكلاسيكية وكذا تنوع مرتكبيها.

4- التعامل بالتستر والكتمان مع الجرائم الالكترونية من قبل أغلب الضحايا خاصة الجرائم الالكترونية التي تمس البعد المعنوي.

وللتصدي للجرائم الالكترونية ومحاربتها نقترح من خلال هذه الدراسة ما يلي:

5- ضبط وتحديد المصطلحات والمفاهيم المتعلقة والخاصة بالجريمة الالكترونية.

6- توفير وضمان الأمن التقني لشبكات وأجهزة الاتصال المختلفة الذي من شأنه تحقيق أمن المعلومة وسريتها.

7- متابعة الجرائم الالكترونية وكشف هوية مرتكبيها يكون من طرف مختصين يتمتعون بذكاء وكفاءة عاليين ويتحكمون في مجال العالم الافتراضي بشكل يواكب التطورات السريعة والمتنوعة لحركة هذه الجرائم.

8- سن قوانين واتفاقيات دولية موحدة و صارمة لمحاربة الجرائم الإلكترونية والتي تكفل الحماية الجنائية للجرائم الماسة بسرية المعلومات الإلكترونية.

9- التوعية والتحسيس من خطر الجرائم الالكترونية عند مختلف الفئات العمرية لأن الجهل بمخاطرها يسهل استدراج المجرم الالكتروني لضحاياه لتحقيق هدفه في وقت قياسي ودون أي جهد أو مقابل.

10- تشجيع وتحسين طرق التبليغ على الجرائم الالكترونية مع ضمان الحفاظ على خصوصية المبلغين والمتعرضين لها؛ درءا للانتقام أو التهديد بالتصفية الجسدية وغيرها.

قائمة المراجع:

الأمر رقم ¬66-156 المؤرخ في 10 جوان 1966 يتضمن قانون العقوبات. (الصادرة بتاريخ 11 جوان 1996). الجريدة الرسمية، العدد 49.

القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004 المتتم لقانون العقوبات. (العدد 17، الصادرة بتاريخ 10 نوفمبر 2004). الجريدة الرسمية.

الحمداني بشرى حسين. (2014). القرصنة الالكترونية واسلحة الحرب الحديثة. الاردن. دار اسامة للنشر والتوزيع.

الرومي محمد أمين. (2004). جرائم الكمبيوتر والانترنت. مصر. دار المطبوعات الجامعية.

الشناوي محمد. (2006). استراتيجية مكافحة جرائم النصب المستحدثة(الانترنت،بطاقات إئتمان،الدعاية،التجارة الكاذبة). القاهرة. دار لبيان للطبع والنشر.

الشوا محمد سامي.(1994). ثورة المعلومات وانعكاساتها على قانون العقوبات. مصر . دار النهضة العربية.

الطوابلة علي حسن. (2008). الجرائم الالكنرونية. البحرين. مؤسسة الفخراوي للدراسات والنشر.

الملط أحمد خليفة. (2006). الجرائم المعلوماتية مصر. دار الفكر العربي.

العيتي محمد حمادة مرهج. (2005). جرائم الحاسوب. الأردن. دار المناهج للنشر والتوزيع.

المومني نهلا عبد القادر. (2008). الجرائم المعلوماتية. الأردن. دار الثقافة للنشر والتوزيع.

بالطي غنية. (2015). الجريمة الالكترونية "دراسة مقارنة" . الجزائر. دار الجزائرية للنشر.

حجازي عبد الفتاح بيومي. (2007). الإثبات الجنائي في جرائم الكمبيوتر والانترنت. مصر. دار الكتب القانونية.

خلفي عبد الرحمان. (2012). محاضرات في القانون الجنائي العام. الجزائر. دار الهدى للنشر والطباعة والتوزيع.

دقيش مجيد، جنيدي عبد الرحمن، واقع الجريمة الإلكترونية في الجزائر: دراسة تحليلية خلال الفترة2013-2017،واقع الجريمة الإلكترونية بين مبادئ الحرية والمسؤولية، غليزان، الجزائر، 15جوان2022،9-10.

طايل البشابشة وسام. (2013). دوافع استخدام طلبة الجامعات الأردنية لمواقع التواصل الاجتماعي واشباعاتها (فيس بوك وتويتر- دراسة على طلبة الجامعة الأردنية وجامعة البتراء أنموذجا. الأردن. جامعة البتراء.

طعباش أمين. (2015). الحماية الجنائية للمعاملا الإلكترونية. مصر. مكتبة الوفاء القانونية للنشر والتوزيع.

عبد الفتاح مراد. (1982). شرح جرائم الكمبيوتر والانترنت. مصر. دار الكتب والوثائق المصرية.

قارة أمال. (2007). الحماية الجزائية للمعلوماتية في التشريع الجزائري. الجزائر. دار هومة للطباعة والنشر و التوزيع.

قزران مصطفى، زرقين عبد القادر.(2022). الآليات الدولية لمكافحة الجريمة الإلكترونية، مجلة صوت القانون .العدد (02) 1222-1244.

قورة نائلة عادل محمد فريد. (2005). جرائم الحاسب الآلي الإقتصادية. لبنان. منشورات الحلي الحقوقية.

لخضر سلامي.(2021). ضحايا الجريمة الالكترونية عبر مواقع التواصل - الفايسبوك أنموذجا-،مجلة دراسات في سيكولوجية الانحراف. العدد (01). 136-218.

نافع زينب، شعباني مجيد.(2020).تحديات الحكومة الإلكترونية في الجزائر- الجريمة الإلكترونية نموذجا-، مجلة العلوم الاقتصادية والتسيير والعلوم التجارية. المجلد 13، العدد (01).780-794.

هلالي عبد الله أحمد. (2007). أتفاقية بودباست لمكافحة الجرائم المعلوماتية. القاهرة. دار النهضة العربية.