



التأصيل المفاهيمي للجريمة الإلكترونية في التشريعات الدولية والتحديات التي تواجهها

The conceptual foundation of cybercrime in international legislation and the challenges it faces

قرزو بغداد¹

جامعة عمار ثلجي الأغواط- الجزائر

b.guerzou@lagh-univ.dz

مخبر الحقوق والعلوم السياسية

فرقة بحث تنمية الموارد البشرية في ظل المتغيرات الدولية

تاريخ القبول للنشر: 2025-08-26

تاريخ الاستلام: 2025-05-23

ملخص:

تهدف هذه الدراسة إلى البحث في مفهوم الجرائم الإلكترونية في ظلّ المقاربات العلمية والمبادرات الدولية التي اختلفت في تحديد وضبط المفهوم. من ثم تعددت الآراء والتشريعات الدولية حولها. لكون الجريمة الإلكترونية جرائم ترتكب في البيئة الرقمية وليست جرائم تقليدية، كما تتطرق الدراسة أيضا إلى تشخيص الأسباب الدافعة إلى ارتكاب الجرائم الإلكترونية وإبراز طبيعة هذه الجرائم وخصائصها لأنها جرائم غير تقليدية، ونختم دراستنا بتحديد مختلف التحديات التي من شأنها أن تعرقل جهود الدول والهيئات الأممية في مكافحة هذا النوع من الجرائم. كلمات مفتاحية: الجريمة الإلكترونية، المعلوماتية، الفضاء الإلكتروني، الأمن السيبراني، مكافحة الجريمة.

Abstract:

This study aims to research the concept of cybercrime in light of the scientific approaches and international initiatives that differed in defining and control. Hence the multiplicity of opinions and international legislation around it, because cybercrime is crimes committed in the digital environment and not traditional crimes. The study also addresses the diagnosis of the reasons that motivate the commission of cybercrime and highlight the nature

¹ قرزو بغداد

and characteristics of these crimes because they are non-traditional crimes, and we conclude our study by identifying the various challenges that would hinder the efforts of countries and UN bodies in combating this type of crime.

Keywords: Cybercrime, informatics, cyberspace, cybersecurity, crime control.

مقدمة:

إن التطور الهائل في مجال تقنية المعلومات والاتصالات أحدث ثورة غير مسبوقة في شتى المجالات حيث تغيرت طريقة التعاملات التقليدية وأصبح التعامل إلكترونيا، إلا أنه مع الاستخدام المتزايد لهذه الشبكات والأنظمة المعلوماتية أدى إلى ظهور الكثير من مشاكل ومخاطر هذه التقنية وأساليبها المتطورة، فأصبحنا أمام ظاهرة جديدة هي ظاهرة الجريمة الإلكترونية التي تعتمد في ارتكابها على وسائل التقنية الفنية المتطورة.

إن الجريمة الإلكترونية ظاهرة حديثة نسبياً يقتربها مجموعة من مجرمون يتميزون بالذكاء ويمتلكون مؤهلات من المعرفة الفنية والتقنية، يهددون بها الحياة الخاصة للأفراد كما تكبد الأعمال التجارية الخسائر الفادحة بالإضافة إلى أنها قد تشكل هاجساً يهدد الأمن القومي والسيادة الدولية.

فقد ساهم استخدام هذه التقنيات في نهضة كبرى غير مسبوقة وازدهارا في كافة المجالات الاقتصادية والاجتماعية والسياسية الأمنية لكن سرعان ما صاحب هذه التقدم في مجال تكنولوجيا الاتصال والإعلام مشكلات متعلقة بتجاوزات مستخدميها في حق العديد من المؤسسات والأفراد على المستوى الدولي والوطني حيث وصلت هذا النوع من الانتهاك والتجاوزات المتصلة بتكنولوجيا الاتصال والإعلام إلى مستوى الاجرام وهي تمثل من أبرز وأخطر التحديات الأمنية التي تواجه كل مجتمعات العالم في مجال استخدامات تقنية المعلومات والاتصالات على نطاق مؤسسات القطاع العام والخاص والأفراد حيث أخذت معدلات هذا النوع من الجريمة في تصاعد، فقد بلغ عدد مستخدمي الإنترنت 66,2 % من سكان العالم في عام 2024 م، ولقد شكلت التهديدات الداخلية مصدر قلق دائم. حيث أفادت 83% من الشركات بأنها تعرضت لهجوم داخلي واحد على الأقل في عام 2024.



1- المناهج المستخدمة:

المنهج التحليلي والوصفي: يتم توظيف هذا المنهج من خلال التطرق إلى الجوانب المتعلقة بالجرائم المتصلة بتكنولوجيا الاتصال والاعلام في الفضاء الإلكتروني، وذلك للإجابة على تساؤلات الدراسة المتعلقة بالجريمة الإلكترونية والمفاهيم المرتبطة بها في حدود حقل دراسة الظاهرة بعرض اهم الخصائص والمظاهر للجريمة الإلكترونية وتحليل وربط البيانات للوصول الى احكام معرفية تحدد طبيعتها.

أ- المنهج التاريخي: والذي تم الاستفادة منه في البحث عن التقارير والأبحاث في فترات زمنية مختلفة عن الجهات ذات العلاقة بظاهرة الجريمة الإلكترونية سواء على المستوى المحلي أو الدولي

ب- المنهج المقارن: نستخدم المنهج المقارن لما له من أثر بالغ الاهمية في دراسة الظاهرة المتطورة والمتفاعلة وذلك في دراسة ظواهر متشابهة أو متناظرة في مجتمعات مختلفة، وفي فترات زمنية متباينة ومن هنا يمكن تحليل الاختلافات في موضوع الجريمة الإلكترونية عبر مجتمعين أو أكثر ومقارنتها ايضا بالجرائم التقليدية من حيث الطبيعة والاليات والاثار التي تخلفها واستخراج العلاقات بين المتغيرات التي تتأثر بها بغية تفسير الظاهرة محل الدراسة.

هذا المنطلق طرح التساؤل العام كمشكلة بحثية حول موضوع الدراسة كما

يلي:

ما هو التأصيل النظري والمفاهيمي للجرائم الإلكترونية في ظل تعدد المفاهيم والاتجاهات الدولية وماهي أهم التحديات التي تواجهها؟

- تندرج ضمن هذه الاشكالية المركزية، جملة من التساؤلات الفرعية، وهي كالتالي
ما هو التأصيل النظري والمفاهيمي لجرائم المتصلة بتكنولوجيا المعلومات والاتصال؟

- كيف يمكن فهم وطبيعة وأسباب الجرائم الإلكترونية؟

- ماهي تحديات الجرائم المتصلة بتكنولوجيا المعلومات والاتصال؟
للإجابة على هذه الأسئلة وكشف الغموض حول مختلف جوانب الموضوع
تقدمت هذه الورقة البحثية ضمن المحاور التالية:
المحور الأول: التأصيل النظري والمفاهيمي حول الجريمة الإلكترونية
المحور الثاني: طبيعة وأسباب الجرائم الإلكترونية
المحور الثالث: تحديات وتداعيات الجرائم الإلكترونية.
خاتمة: وتشمل: النتائج-التوصيات. بالإضافة إلى: استراتيجية موحدة لمواجهة جرائم
المتصلة بتكنولوجيا الاتصال والاعلام.

قبل أن نشرع في اعطاء مفهوم الجرائم الإلكترونية ونتعرف على طبيعتها
وآلياتها يجدر بنا أن نحدد حقلها ومصدر تكونها، فهي مرتبطة قبل كل شيء بالتطور
التكنولوجي الحاصل في مجال معالجة المعلومات وتطور وسائل الاتصال التي
شكلت بدورها عالماً جديداً في التواصل بين الأشخاص وبين الدول أو الحكومات
والمؤسسات المالية والخدماتية وهو ما فرض ضرورة تبني منظومة معلوماتية خاصة
بكل قطاع للاستفادة من مزاياها، لكن يبقى الأمر متعلقاً بمدى التحكم في هذه
التقنيات الاتصالية والتعامل معها بحذر من خلال تحديد ضوابطها وإمكانات
المتاحة لمجابهة مخاطرها.

1- التأصيل المفاهيمي والنظري للجرائم الإلكترونية

تعددت التعريفات التي تناولت الجريمة المعلوماتية، وسبب ذلك هو الخلاف
الذي أثير بشأن تعريف هذه الجريمة ذاتها، فالجريمة الإلكترونية تعتبر نوع غير
مألوف من الجرائم ومن الصعب التعامل معه، لأنه يرتبط بتكنولوجيا حديثة.
وعلى هذا الأساس فإعطاء مفهوم واضح حول الجريمة الإلكترونية يكون صعب
نظراً لغموض طبيعته حتى قيل أن هذا النوع من الجريمة ما هو إلا جريمة
مألوفة ترتكب بأسلوب إلكتروني (فهد بن عايد، 2023، ص19).



فمصطلح الجريمة الإلكترونية (Cyber) للدلالة على جزء متصل بالحاسب وهي تدل أيضا على عصر المعلوماتية، أما الجريمة (Crime) فهي السلوكيات والأفعال الخارجة على القانون وبذلك تكون معنى الجريمة الإلكترونية المخالفات التي تُرتكب ضد الأشخاص أو المجموعات أو المؤسسات بدافع الحاق الضرر بالضحية مادية كانت أو معنوية باستخدام شبكات الاتصالات مثل الانترنت.

المعلوماتية: ظهرت المعلوماتية في بداية الستينيات حين بدا الاهتمام بالمعلومة كرهان للتقدم والتوسع في مختلف المجالات خاصة بين الدول المتنافسة ويُقصد بالمعلوماتية ذلك العلم الذي يهتم بالموضوعات والمعارف المتصلة بالبيانات وتجميعها وتنظيمها، ومن ثمة تفسيرها واستخدامها وبالتالي فهي عملية ديناميكية تتم بوسائل أو أوتوماتيكية تتميز بدقتها وبسرعة الفائقة ومن بين التعاريف الشائعة.

كما ورد تعريفا للمعلوماتية في الأكاديمية الفرنسية حيث تصفها على أنها: "علم التعامل العقلاني بواسطة الأجهزة والآلات، مع المعلومات بحكم أنها تدعم المعارف الإنسانية الاتصالات في ميادين تقنية، اقتصادية واجتماعية" (نائلة، 2005، ص.28)، فكلية معلوماتية تعني المعالجة الآلية للمعلومة، ويطلق عليها أيضا تقنية المعلومات فهي أية وسيلة مادية أو معنوية أو مجموعة وسائل لتخزين المعلومات وترتيبها وتنظيمها واسترجاعها ومعالجتها وتطويرها وتبادلها وفقا للأوامر والتعليمات المخزنة بها (مدحت محمد، 2005، ص.28).

1.1 - تعريف الجرائم المتصلة بتكنولوجيا الاتصال والإعلام

الأفعال والسلوكيات في الجرائم الإلكترونية يستوجب وجود بيئة رقمية، ويتطلب أيضا معرفة بداية هذا النشاط والشروع فيه، ونتيجته. فعلى سبيل المثال يقوم المجرم بتجهيز الكمبيوتر لكي يقوم بالجريمة، كما يمكن أن يقوم بجريمة إعداد برامج فيروسات.

بما أنّ مصطلح الجريمة الإلكترونية ارتبط بالمعلوماتية فإنّ التعامل مع هذه الظاهرة يختلف من دولة لأخرى من حيث تحديد مفهومها وتحديد نطاقها بحكم التطور العلمي المستمر في مجال تقنيات الاتصال، مما يعني عدم التمكن من ضبط

الأحكام والتشريعات وفق مراحل زمنية لاحقة، لذا نجد تباين في التعبير عن الجريمة الإلكترونية فمنهم من يُطلق عليها جرائم الحاسب الآلي أو إساءة استخدام الحاسب الآلي، وهناك من يطلق عليها مصطلح جرائم الكمبيوتر، ويوجد من يحددها بجرائم الإنترنت، وهناك من يسميها بالجرائم المعلوماتية، عموماً تصب هذه المنطلقات التعريفية في أنّ كل فعل إجرامي يقع عمداً أياً كانت صلتها بالمعلوماتية ينشأ عنه خسارة تلحق بالمجني عليه أو مكسب يحققه الفاعل (فتوح الشاذلي، 2003، ص.31).

أ. الاتجاه القانوني لمفهوم الجريمة الإلكترونية

يرى أنصار هذا الاتجاه أنّ الجرائم الإلكترونية تتطلب تعريف المفردات الضرورية المتعلقة بارتكاب جرائم الحاسب الآلي وهي الحاسب الآلي، برنامج الحاسب الآلي، البيانات، الممتلكات، الدخول الخدمات (عبد الفتاح، 2006، ص.20) فأنصار الفقه القانوني قد اعتمدوا على مجموعة من التعاريف والتي تعتمد على سمات شخصية المجرم، حيث تعرفها وزارة العدل الأمريكية في دراسة علمية قام بها معهد ستانفورد للأبحاث وأكدتها الوزارة في دليلها لعام 1979 حيث قالت أنّ الجريمة المعلوماتية تعتبر أي جريمة لفاعلها معرفة فنية بالحاسبات تمكن من ارتكابها كما عرفها المفكر "دافيد تومسن" أي جريمة يكون متطلبها لاقترافها أن تتوافر لدى فاعلها المعرفة الإلكترونية (هشام محمد، 2000، ص.20).

ب. تعريف الجرائم الإلكترونية من حيث المنظور التقني

يرى هذا الاتجاه أنّ الجرائم الإلكترونية ما هي إلا سلوك إجرامي تتمتع التعامل فيه بالتقنية الإلكترونية بطريقة مباشرة أو غير مباشرة كوسيلة أو غاية لتنفيذ الجريمة المستهدفة ومن أنصار هذا المنظور المفكر تايدمان "Tiedeman" والذي عرف الجريمة الإلكترونية بأنها: "كل أشكال السلوك الضار بالمجتمع وغير المشروع والذي يرتكب باستخدام الكمبيوتر وعرفها البعض الآخر بأنها "الفعل غير المشروع الذي يتورط في ارتكابه الحاسوب، أو هي الفعل الإجرامي الذي يستخدم في



اقتراه الكمبيوتر كأداة رئيسية"، وعرفت أيضا بأنها: "جريمة يستخدم الكمبيوتر كوسيلة أو أداة لارتكابها أو يمثل إغراء بذلك، أو جريمة يكون الكمبيوتر نفسه ضحيتها"، كما عرفت بأنها: "نشاط إجرامي تستخدم فيه تقنية الحاسب الآلي بطريقة مباشرة أو غير مباشرة كوسيلة أو هدف لتنفيذ الفعل الإجرامي" (محمد الأمين، 2005، ص.6).

ج. تعريف الجرائم الإلكترونية من حيث الموضوع

يرى مفكرو الاتجاه الموضوعي أنّ الجرائم الإلكترونية لا يشترط وصف هذا النوع من الإجرام لمجرد استخدام الحاسب الآلي فيها ولكن الشرط هو وقوع الفعل داخل نظام الحاسب الآلي لكي نعتبرها جريمة إلكترونية، وعلى هذا الأساس تم تعريف الجريمة الإلكترونية على أنها نشاط غير مشروع لتغيير أو لنسخ أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب أو التي ترسل عن طريقه كما تم تعريفها بأنها نوع من الغش المعلوماتي ينصرف إلى كل سلوك غير مشروع يتعلق بالمعلومات المعالجة ونقلها ومعرفة مكنونها (عبد الفتاح بيوم، 2006، ص.25).

ولقد سار في هذا الاتجاه الفقيه "روزنبلات" ROSENBLATT الذي عرف هذه الجريمة بأنها "نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب أو التي تحول عن طريقه" وهو ما ذهب إليه الأستاذ THOMAS J SMEDINGHOFF إلى أن ما يسمى جريمة حاسوب "يجب أن تتضمن تقريبا أي ضرب من ضروب النشاط الموجه ضد أو المنطوي على استخدام نظام الحاسب وعرفت أيضا بأنها "سلوك غير مشروع معاقب عليه قانونا صادر عن إرادة إجرامية، محله معطيات الكمبيوتر. (Thomas, 1986, p.310)

د. تعريف الجرائم الإلكترونية من حيث الجانب المعرفي

يركز أنصار هذا الاتجاه على الجانب المعرفي لا على الوسيلة أو الموضوع المتعلق بهذا النوع من الجرائم إذ يعرفها بأنها كل جريمة يكون متطلباً لاقترافها أن تتوفر لدى فاعلها المعرفة بتقنية الكمبيوتر بمعنى كل سلوك غير أخلاقي أو غير مشروع أو سري يتعلق بالمعالجة الآلية للبيانات أو نقلها (عادل يوسف، 2008، ص.113).

وفي اجتماع عقد بباريس سنة 1983 لبحث الإجرام المرتبط بالمعلوماتية عرّف خبراء لمنظمة التعاون الاقتصادي والتنمية الجرائم المتصلة بتكنولوجيا الاتصال والإعلام على أنّها كل سلوك غير شرعي أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات أو بنقلها (سامي علي، 2007، ص. 20).

بناء على ما تم ذكره فإنّ الجريمة الإلكترونية تشمل كافة أشكال السلوك غير المشروع الذي يُستخدم فيها الحاسوب لاستهداف ممتلكات الغير بغرض الاستحواذ عليها أو اتلافها وإفسادها أو الوصول إلى المعلومات المخزنة في الأجهزة، لأنّ المعلومات تعتبر من حقوق الملكية مهما كانت طبيعتها وعليه تصبح البيانات التكنولوجية والبرامج المعلوماتية جوهر العملية برمتها وعليه يمكن أن يكون الكمبيوتر إما موضع الجريمة كإتلاف المعلومات، أو تخريب لأجزاء الحاسب وبرامجه، وقد يكون الحاسب وسيلة لارتكاب الجريمة عن طريق استخدامه للاحتيال، وإجراء تحويلات من حساب لحساب آخر أو سرقة أرقام بطاقات الائتمان واستخدامها في الشراء عبر شبكة الأنترنت أو التجسس وسرقة الأموال.

2.1- الأطر النظريّة

لم يتفق الفقه الجنائي على تسمية موحدة للجرائم المتصلة بتكنولوجيا الاتصال والإعلام، إذ يسميها البعض الجريمة الإلكترونية وهناك من يسميها الجريمة المعلوماتية، ويذهب البعض الآخر إلى مسمى جرائم الكمبيوتر والإنترنت. وآخرون يطلق عليها جرائم إساءة استخدام تكنولوجيا المعلومات والاتصال.

للتّعرف على ظاهرة الجريمة الإلكترونية وجب الإلمام بالمفاهيم والمقاربات النظريّة التي تناولت الظاهرة وذلك بقصد التحكّم في مفاصل الدّراسة والوصول إلى النتائج والغايات العلمية والحقائق المعرفية في حقل موضوع الدراسة.

أ- الاتجاه التقليدي

يرى هذا الاتجاه أن المعلومة تتميز بطبيعة خاصة، وهو يضيف وصف القيمة على الأشياء المادية فقط ويرتكز هذا المبدأ على بديهية مسلمة مفادها أن للمعلومات



خاصية معنوية تجعلها في حقيقة الامر غير قابلة للاستئثار والاستحواذ المادي إلا عن طريق حقوق الملكية الفكرية أو الذهنية و عليه فإن المعلومات المخزنة والتي لا تتعلق بالحقوق الأدبية أو الذهنية أو الصناعية لا يمكن إدراجها في قائمة القيم المحمية قانونا، لذا تستبعد من قائمة الملكية أو الأموال (سامي علي 2007، ص.27).

ب- الاتجاه الحديث

هذا الاتجاه له نظرة مغايرة اذ يعتبر ويصف ظاهرة المعلوماتية بالشيء المادي، بمعنى أنه يمكن إعتبار المعلومات ثروة مالية، وهذا من منطلق القيمة الاقتصادية، وقد تزيد قيمتها عن الأموال المادية، وبالتالي تتحول القيمة المادية الى قيمة اقتصادية وأن علاقة المعلومة بصاحبها هي علاقة قانونية كعلاقة المالك بالشيء الذي يملكه وعليه تكسب صاحبها خاصيتين في غاية الأهمية، الأولى حق صاحب المعلومة في ضمان سرية المعلومة والخاصية الثانية حق صاحب المعلومة في طلب التعويض عن الأضرار المترتبة على أي عمل غير مشروع يتعلق بالمعلومة (سامي جلال، 2011، ص.46).

3.1- الجرائم الإلكترونية في التشريعات الدولية

جاء في تقرير مؤتمر الامم المتحدة العاشر حول منع الجريمة ومعاينة المجرمين المنعقد في فيينا في نيسان (أفريل) من عام 2000م، إلى أنه لا يوجد تعريف محدد للجريمة المعلوماتية على الصعيد الدولي بسبب الخلاف في عناصرها المكونة لها وإن كان هذا المؤتمر قد تبني التعريف الاتي " الجريمة المعلوماتية هي كل جريمة ترتكب بواسطة نظام حاسوبي أو شبكة كمبيوتر أو داخل نظام الكتروني ، وتشمل تلك الجريمة من الناحية الميدانية كل الجرائم التي ترتكب في الفضاء الكتروني" أما عن المنظمة الأوروبية للتعاون الاقتصادي التنمية فقد أعطت تعريفا للجريمة المعلوماتية من أجل استخدامه خصيصا للدراسات التي تمس المجال التعاوني الاقتصادي منذ عام 1983 " بأن الجريمة المعلوماتية هي كل سلوك غير اخلاقي أو غير مشروع أو لم

يتم التصريح به، مرتبط بالمعالجة الآلية للبيانات الخام أو بنقل هذه البيانات (عمار عباس 2017، ص. 34).

أ- اتفاقية بودابست لمقاومة جرائم المعلوماتية والاتصالات 2001

نظرا لخطورة الجريمة المعلوماتية والتي وصفت بأنها جريمة عابرة للحدود تم إبرام اتفاقية تم التوقيع عليها عدة دول وأبرمت هذه الاتفاقية لهدف تحديد خصائص وطبيعة الجرائم الالكترونية دوليا وبالتالي عقدت في 23 نوفمبر 2001 في بودابست وتضم في عضويتها 45 دولة أوروبية و 17 دولة من خارج أوروبا حتى تاريخ 5/10/2014، وتم الإجماع على تعريف الجريمة الإلكترونية بأنها الجرائم ضد السرية والنزاهة وتوافر البيانات وأنظمة الحاسوب الآلي في مواده من 2 إلى 12 حيث دعت هذه الدول على ضرورة مكافحة هذه النوع من الجريمة والترصد لمرتكبيها و/أو تعقب أعمالهم والبحث عن الدليل على جرائمهم وضبطها، ولذلك تم تصنيف هذه الجريمة ضمن الجرائم المعلوماتية المرتكبة بواسطة النظام المعلوماتي (عمار عباس 2017، ص. 34).

وقد تم ترتيب هذه الجرائم الى خمس فئات: الأولى تعريف الدخول غير المشروع في سلوك الاعتراض غير القانوني، التدخل في البيانات، التدخل في النظام، إساءة استخدام أجهزة والثانية تتمثل في الجرائم المتعلقة بالحاسوب: الجرائم المتعلقة الغش، والجرائم المتعلقة بالتزوير؛ أما بالنسبة للفئة الثالثة بالترتيب فتتجسد في خصائص الجرائم المتعلقة بالمحتوى، كالجرائم المتعلقة بالمواضيع الإباحية عن الأطفال اما الفئة الرابعة الجرائم المتعلقة بانتهاك حقوق الملكية الفكرية والحقوق المجاورة، الجرائم المتعلقة بالتعدي على حقوق المؤلف والحقوق المجاورة. اما خامس هذه الفئات فهي: المسؤولية المؤسسية المحاولة والإعانة على الجريمة والتحرير في المادة 12.

نصت اتفاقية "بودابست" في المادة الثانية تحت عنوان "الدخول غير القانوني" حيث تم الإجماع على ضرورة تبني كل طرف بالإجراءات التشريعية أوكل إجراء يرى أنه يؤدي إلى اعتبار السلوك جريمة جنائية وفقا للقانون الداخلي، فإنتهاك

إجراءات الأمن من أجل الحصول على بيانات الحاسوب أو أية نية إجرامية أخرى يُعدّ جريمة وعليه فإنّ الفكرة التي تضمنتها المادة هي أن الولوج إلى الحاسب يمكن أن يترتب عليه الوصول إلى سرقة المعلومات وتزويرها، التجسس المعلوماتي، الاعتداء على خصوصية للأفراد... الخ (اتفاقية بودابست 2001).

ب- الاتفاقية العربية لمكافحة جرائم تقنية المعلومات

جاء في القانون العربي لمكافحة جرائم تقنية أنظمة المعلومات 2004 في المادة الثالثة " تجريم سلوك كل من دخل عمدا وبطريقة غير شرعية موقعا أو نظاما معلوماتيا يعاقب بالحبس أو الغرامة. أو بكلا العقوبتين "وهو الحكم نفسه نصت عليه المادة 06 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات (المؤرخة في ديسمبر 2010. ص4).

إذا بناء على هذه الاحكام تتبلور لنا القاعدة الفقهية للجريمة الالكترونية مفادها تجريم سلوك الدخول غير المشروع، متى كان ذلك الدخول مخالفا لإرادة صاحب النظام خاصة اذا هذا النظام مقيدا وخرق الجاني هذه القيود وخلاصة هذا الجزء من الدّراسة هو أنّ الدول وصلت الى قناعة بضرورة تجريم الدخول غير المصرح به رغم التباين في صيغة تبني الاحكام واليات التنفيذ نظرا للفوارق بين طبيعة التركيبة الاجتماعية الثقافية لمجتمعاتها من جهة والى طبيعة الانظمة السياسية والأمنية من جهة ثانية (الاتفاقية العربية 2010. ص4).

ج - الجرائم المتصلة بتكنولوجيا الاتصال والإعلام في التشريعات العربية

من التشريعات العربية التي تناولت الجرائم المتصلة بتكنولوجيا الاتصال والإعلام، بعد الاطلاع نصوص لتشريعات والأنظمة العربية نجد اختلافا سواء في التعريف أو في تحديد طبيعة الجريمة، حيث نرى من منها من أعطى تعريفا للجريمة الالكترونية والبعض الآخر لم يتطرق لتعريفها بينما أكتفى بتسمية الأفعال التي يجرمها ووضع العقوبات التي يراها مناسبة لها .

1. التشريع القطري

أعطى تعريفا للجريمة الإلكترونية المعلوماتية في القانون رقم 14 لسنة 2014 م الصادر بتاريخ 15 سبتمبر 2014 وذلك في فقرته العاشرة من المادة الأولى من الباب الأول الذي جعله خصيصا للمفاهيم في تطبيق أحكامه. حيث قال إن الجريمة الإلكترونية هي كل فعل يعتمد على استخدام الشبكة المعلوماتية أو وسيلة تقنية المعلومات أو نظام معلوماتي بطريقة غير مشروعة، بما يخالف أحكام القانون وعليه لم يترك المشرع القطري تعريف الجرم الإلكتروني للاجتهادات الفقهية بل قالها بصراحة في نصوصه منعاً لتلك الاجتهادات التي قد تأول التعريف حسب مرادها بالإضافة أو النقصان من قبل الفقيه (القانون القطري رقم 14، 2014).

2. المشرع السعودي لمكافحة جرائم المعلوماتية

المشرع السعودي أعتمد الصراحة في تعريف الجريمة الإلكترونية في الفقرة الثامنة من المادة التشريع الأولى من النظام الصادر بالمرسوم الملكي رقم 17: بتاريخ 1428/3/8 هـ والتي عرفها بأنها كل فعل يرتكب مستخدماً الشبكة المعلوماتية أو الحاسب الآلي بالمخالفة لأحكام هذا النظام ويتبين لنا من خلال فهذا التعريف الذي نص عليه المشرع السعودي أن الجريمة الإلكترونية هي كل فعل ضار وغير مشروع يرتكبه الفرد أو الجماعة عبر استعماله الأجهزة الإلكترونية، ويكون لهذا السلوك أثر ضار على غيره من الأفراد وبالتالي المشرع السعودي لم يترك تعريف الجريمة المعلوماتية لاجتهاد الفقهاء (القانون القطري رقم 14، 2014).

3. التشريع الجزائري

الذي أطلق عليها بالجرائم المتصلة بتكنولوجيات الاعلام والاتصال وعرف هذا النوع من الجرائم في نص المادة الثانية الفقرة الأولى من قانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها على أنها "الجرائم المتصلة بالمعلوماتية والجرائم التي تمس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو



يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية" ويقصد بأنظمة المعالجة الآلية للمعطيات أي الأنظمة المعلوماتية والتي عرفها المشرع الجزائري في الفقرة (ب) من نفس المادة بأنها " أي مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة أو أي نظام منفصل ، يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذاً لبرنامج معين " وقد عرف المعطيات والتي يقصد بها البيانات في الفقرة (ج) بأنها: "كل عملية تقوم بعرض المعلومات أو للوقائع أو المفاهيم في شكل جاهز للمعالجة داخل منظومة معلوماتية، بما في ذلك البرامج المناسبة التي من شأنها جعل منظومة معلوماتية تؤدي وظيفتها " (القانون رقم 04-09، 2009، ص 5).

نص قانون العقوبات الجزائري على ثلاث أنواع من الجرائم المعلوماتية يمكن أن تقع في قطاع البنوك، وهي جريمة الدخول أو البقاء غير المصرح بهما في أنظمة المعالجة الآلية للمعطيات وجريمة التلاعب بالمعطيات وجريمة التعامل في معطيات غير مشروعة حيث حرص المشرع الجزائري على تجريم كل تواجد عمدي غير مشروع داخل أنظمة المعالجة الآلية للمعطيات سواء أدى إلى نتيجة معينة أو لم يؤدي إلى ذلك.

حيث نصت عليها المادة 394 مكرر من قانون العقوبات تحت القسم السابع مكرر من الفصل الثالث الخاص بالجنايات والجنح ضد الأموال. وتتمثل في جريمة الدخول أو البقاء غير المصرح بهما داخل النظام، جريمة التلاعب غير المصرح به بمعطيات نظام المعالجة الآلية، وجريمة التعامل في معلومات غير مشروعة، ولقد أصدر المشرع الجزائري قانون رقم 07-18 يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

الجريمة مرتبطة بسلوك معين يتضمن إحدى صورتين، إما الولوج أو البقاء، ولم يصدر في المادة 394 مكرر على تعريف للولوج أو البقاء، وهناك من أعطى تعريفاً للولوج غير المصرح به، بأنه الولوج إلى البيانات والمعطيات المخزنة داخل نظام الحاسب الآلي بدون رضا المسؤول عن هذا النظام، أو هو إساءة استخدام الحاسب الآلي ونظامه عن طريق شخص غير مرخص له باستخدامه والولوج إليه، للوصول إلى

الكم الهائل من المعطيات والمعلومات المخزنة بداخله، للإطلاع عليها أو لمجرد التسلية، أو لإشباع الشعور بالنجاح في اختراق الحاسب الآلي، أما البقاء فقد تم تعريفه بأنه التواجد داخل النظام المسؤول عن المعالجة الآلية للمعطيات على حساب صاحب الملكية الحقة لهذا النظام (علي عبد القادر، 2000، ص. 52).

وقد جاء هذا بصراحة في المادة 394 مكرر بالعبرة التالية " كل من يدخل أو يبقى"، دون اشتراط الطريقة أو الكيفية التي يلج بها المجرم، أما فيما يخص النتيجة الإجرامية فلا يشترط تحقق نتيجة معينة حتى تقوم الجريمة، وإنما تقوم هذه الأخيرة بمجرد توافر السلوك الإجرامي أي الدخول أو البقاء، لكن إذا ترتب على الدخول أو البقاء نتائج محددة فإنّ المشرع رتب على ذلك تشديد العقوبة وهذه النتائج هي تغيير أو حذف معطيات نظام المعالجة الآلية للمعطيات أو تخريب هذا النظام. في الأساس (محمد خليفة، 2007 ص 159).

وقد جاء فيما تضمنته المادة السالفة الذكر وجوب التعمد في ارتكاب الجريمة حتى لا يقع هؤلاء تحت طائلة العقاب، فالشرط الأساسي هو ان تكون هذه الجريمة عمدية، وذلك من أجل الموازنة بين حماية حرية الأفراد في استخدام الانترنت وخصوصية الأنظمة المعلوماتية لكن بالنسبة للظروف المشددة لهذه الجريمة، أو النتيجة المشددة فلا بد أن تكون غير عمدية، لأنها لو كانت عمدية ستشكل جريمة أخرى هي جريمة التلاعب بالمعطيات (محمد خليفة، 2007، ص. 159).

2- أسباب وخصائص الجرائم المتصلة بتكنولوجيا الاتصال والإعلام

لقد انتقلت المجتمعات من العالم الواقعي إلى العالم الافتراضي، كذلك انتقلت الجريمة من صورها التقليدية إلى عالمها الافتراضي ومع الحجم الهائل للتفاعلات والتدخلات في الاتصالات بمختلف تقنياتها فقد اوجد أيضا فئات متخصصة تستهدف الأشخاص أو المؤسسات في مجال الخدمات أو الأعمال، ومما لا شك فيه أن أصحاب الجريمة الإلكترونية يختلفون عن مرتكبي الجريمة التقليدية، وذلك راجع إلى الاختلاف بين الأشخاص من حيث السن والجنس والمستوى التعليمي وغير ذلك من المؤثرات الخارجية وعليه فإن الجرم الإلكتروني



يختلف عن الجرم التقليدي، وعلى هذا الأساس تختلف الأسباب والدوافع التي تدفع المجرمين لارتكاب الفعل غير المشروع لها تختلف عن الأسباب والعوامل التي تدفع المجرمين لارتكاب الفعل غير المشروع للجريمة التقليدية ومن جملة هذه الأسباب نذكر الآتي:

1.2- أسباب الجرائم المتصلة بتكنولوجيا الإعلام والاتصال

تعتبر الجرائم المتصلة بتكنولوجيا الإعلام والاتصال بأنها ظاهرة اجتماعية متوافقة مع انتقال المجتمعات إلى المجتمع الرقمي، حيث انتقل نشاط المجتمعات في العالم من الواقع الفعلي (المادي) إلى الواقع الافتراضي، وبهذا الانتقال لم يتأخر فئة المجرمين في الانتقال معها وفق خصائصها وتقنياتها على اختلاف غاياتهم ويمكن تشخيص أسباب انتشار الجرائم الإلكترونية في العوامل التالية:

أ- الحاجة إلى اكتساب المهارات والرغبة في جمع المعلومات

يهدف هؤلاء القراصنة إلى معرفة الجديد من المعلومات والمفيدة على وجه العموم والتي تكون كذلك ليست خاضعة لقيود قانونية أو إلكترونية بمعنى آخر أن تكون متاحة بسهولة ومناسبة مع استخدامات الأشخاص. وكثيراً من الأحيان نجد أن مجرموا الأنظمة يبررون أن هدفهم من الوصول للمعلومات ودخولهم للشبكات والحواسيب الإلكترونية هو من أجل اكتساب المهارات التعلم لا غير (مصطفى سعدون، 2011، ص 35).

ب- الرغبة في تحقيق الثروة غير المشروعة بدون ملاحقات قانونية

هناك بعض الجرائم الإلكترونية التي ترتكب يكون الدافع منها تحقيق أرباح ومكاسب مادية كاستخدام شبكة الإنترنت للإعلان عن صفقات تجارية غير مشروعة كصفقات المخدرات والاتجار بالبشر، يسعى الإنسان إلى المتعة ويتجنب الألم هكذا تقول النظرية العامة في الجريمة لجتفردسون وهيرشي (Gottfredson, 1990, p87) وقد ورد في بحث أعده هشام بشير المستشار الإعلامي للجمعية المصرية مكافحة جرائم الإنترنت أن عصابات الإجرام المنظم استغلت التكنولوجيا الحديثة في

تيسير شئون الاتجار في البشر ويرى الباحث أن الاتجار بالبشر عبر الإنترنت هو تجارة الإلكترونية حيث أن تعريف التجارة الإلكترونية تلك التعاملات التي تتم الكترونيا عبر شبكة المعلومات العالمية.

ج- الحياة الحضرية دافع للجريمة

يعد التحضر أحد الدوافع الى الجريمة الإلكترونية، حيث الهجرة الكبيرة من المناطق الحضرية والمدن الكبيرة. وعادة ما يهاجر الشباب غير المتمكنين من الريف إلى المدينة من مواجهة متطلبات الحياة الحضرية، باهضه التكاليف، والتي تتطلب مهارات عالية أحيانا. مما يجعل شرائح كبيرة من المهاجرين غير قادرين على تلبية متطلبات الحياة الحضرية، مما يجعلهم يلتفتون إلى الاستثمار في الجريمة الإلكترونية (ذياب موسى، 2014، ص.14).

ساهمت عوامل التحضر باستخدام التكنولوجيا اثناء الحاق الضرر بالآخرين، في مقابل غياب التشريعات وضعف أدوات الحماية في بعض الأحيان يكون الدافع وراء ارتكاب هذه الجرائم هو قهر النظام وإثبات قدرة الجاني وتفوقه على تعقيدات وتطور وسائل التقنية الحديثة، حيث يمضي كل وقته أمام شاشات أجهزته لكسر الحواجز الامنية للأنظمة الإلكترونية واختراقها ليثبت براعته في القدرة على تحدي عوامل نفسية واجتماعية كالسعي وراء الشهرة او بدافع الدفاع عن قضايا تتعلق بالوطنية والشعور بالانتماء لها.

د- تهديد الأمن القومي والعسكري للدول

من الدوافع لارتكاب الجرائم الالكترونية التأثير على الدول والحكومات من خلال التهديد الإلكتروني بالاختراق والقرصنة المعلوماتية للأسرار الأمنية والتي قد تكون لها نتائج وخيمة على الأمن القومي و الهوية الوطنية للبلاد، وهذا ما جعل الدول تتصدى لهذا النوع من الجرائم غير المألوفة، بشتى الطرق والوسائل الوقائية من أجل الحفاظ على منظومتها المعلوماتية التي تشكل القاعدة الأساسية لكل التعاملات الاقتصادية والسياسية والأمنية لأن المجرم الإلكتروني يشكل تهديد أمني



صعب التحكم فيه وفي الطرق التي يستعملها في اقترافه للجريمة فأحيانا يصعب التعرف عليه بسهولة وتوقع ما يمكن القيام به الأمر الذي يستدعي من كافة الحكومات والمنظمات الدولية العمل على جعل آليات وقائية للحد من انتشار الجرائم الإلكترونية والتصدي لأي تهديد من خلال وضع جملة من التشريعات القانونية تكون ملزمة لكل الدول.

2.2 - طبيعة وخصائص الجرائم المتصلة بتكنولوجيا الإعلام والاتصال

أوجد الفضاء الإلكتروني فرصا جديدة للمجرمين لارتكاب الجرائم من خلال خصائص فريدة من نوعها في هذا الفضاء مثلت لها مفاتيح تحويلية بدخول متغير العولمة (Globalisation) والتي تمكن الجناة مع وجود فرص جديدة من تجاوز الحدود التقليدية وهذا ما يسمى بالجرائم عبر الإقليمية وتتلخص خصائص الجريمة الإلكترونية فيما يلي:

أ- أنها ترتكب من مجرم غير تقليدي

يختلف مجرم المعطيات كثيرا عن المجرم في الجرائم التقليدية، لأن العوامل التي تدفعه لارتكاب الجريمة مختلفة عنده، فبالنسبة لسمات هذا المجرم فهو إنسان اجتماعي، أي أنه متوافق مع مجتمعه ويمتلك المعرفة والمهارة والوسيلة الخاصة بهذه الجريمة، وهذا الاكتساب يتم عن طريق الدراسة المتخصصة في هذا المجال، أو عن طريق الخبرة والاحتكاك بالآخرين (محمد عبيد الكعبي، 2009، ص.38).

ب- الجرائم الإلكترونية جرائم عابرة للحدود

في عالم اليوم لا يوجد حد من الحدود يقف حائلا أمام نقل المعطيات والمعلومات بين الأجهزة الآلية المنتشرة حول مختلف دول العالم عبر شبكات المعلومات فيمكن في بضع ثواني تحميل و نقل كم لا حصر له من المعطيات، كما يمكن أن تقع الجريمة من مجرم في دولة معينة على شخص ما في دولة أخرى في وقت وجيز جدا مخلفا خسائر لا يستهان بها لاسيما مع الدور الهائل الذي تقدمه شبكة الإنترنت من خدمات، بالخصوص في مجال المعاملات التجارية الإلكترونية

وازدیاد اعتماد البنوك على هذا التعامل مما قد یسبب العديد من المشاكل على المستوى الدولي، كمشكلة السيادة الدولية والاختصاص.

ج - جرائم ناعمة وسريعة التنفيذ

فنقل بيانات من حاسب إلى آخر أو السطو الإلكتروني على أرصدة بنك ما لا يتطلب أي عنف أو تبادل إطلاق نار مع رجال الأمن، وهي لا تحتاج إلى القوة العضلية كما هو الحال في الجريمة الإلكترونية وإنما هي بحاجة إلى قوة علمية وقدر من الذكاء ومهارة في توظيف ذلك، والمجرم في سبيل تنفيذها لا يحتاج من الوقت إلا ثوان أو دقائق معدودات (اسامة احمد المناعسة، وآخرون، 2001، ص. 107).

ولا يحتاج من القوة العضلية غير تحريك الأنامل من علي لوحة مفاتيح وقد يتسبب بذلك في حصول خسائر فادحة رغم أن جريمته قد لا ترى بالعين، كما لا تتطلب الجريمة الإلكترونية في أغلبها وجود الفاعل في مكان الجريمة.

د- صعوبة اكتشاف وإثبات الجرائم الإلكترونية

تتميز الجريمة الإلكترونية عن الجرائم التقليدية بصعوبة إثباتها وهذا راجع إلى افتقاد وجود الآثار التقليدية للجريمة وتبقى جرائم المعطيات بالغ التعقيد في التحقيق نظرا لأنّ الهيئات المختصة لم تصل إلى تلك المعرفة أو الخبرة التي تملكها حيال التحقيق في الجرائم التقليدية (سعيد عبد اللطيف، 1999، ص. 95)، لأن الأمر يتطلب معرفة واسعة وإحاطة كاملة بهذه التكنولوجيا الحديثة.

3 - مظاهر وتحديات الجرائم المتصلة بتكنولوجيا الإعلام والاتصال

كلما تطورت المعلوماتية شيئا إلا وتطورت معها الجريمة بشكل متوازي ومترد فبعد أن كانت الجرائم المتصلة بتكنولوجيا الإعلام والاتصال الأساسية تتمثل في عدد محدود من الأعمال التي تمس بسرية البيانات أو النظم الحاسوبية وسلامتها وتوافرها، فإنه ظهرت أعمال إجرامية أخرى تمثلت في استعمال الحاسوب والنظم المعلوماتية لتنفيذ جرائم أخرى والتي تهدف إلى تحقيق مكاسب شخصية أو مالية أو أحداث أضرار بما في ذلك أشكال الجرائم المتصلة بالهوية وبمحتوى الحواسيب، وهذا



التنامي المتزايد في الجرائم الذي يمس بالنظم المعلوماتية ذاتها أو باستعمال النظم المعلوماتية ذاتها لاقتراف أنواع أخرى من الجرائم، جعل من الصعب حصر هذه الأنواع والأساليب الإجرامية في المجال المعلوماتية مما دفع بالفقهاء إلى محاولة تقسيمها إلى طوائف أو أقسام وفق التشريعات والمنظمات و الاتفاقيات الدولية.

1.3- مظاهر وأنماط الجرائم المتصلة بتكنولوجيا الاعلام والاتصال

أ- جرائم التجسس الإلكتروني

التجسس الإلكتروني عملية سرية غايتها جمع المعلومات عبر الإنترنت عن طريق اختراق أنظمة الحواسيب والشبكات. حيث يعتمد المتجسس الإلكتروني على استخدام التكنولوجيا الرقمية كوسيلة من أجل الوصول إلى البيانات ومن ثم المعلومات بدون إذن من المالكين الشرعيين لها، وفي غالب الامر يتم استخدام هذه البيانات لتحقيق أهداف شخصية او سياسية، اقتصادية، أو. ويعد التجسس الإلكتروني من أخطر التهديدات التي تواجه الأفراد والشركات والدول في العصر الرقمي.

ب- جرائم القرصنة

اتسعت وتطورت صور القرصنة من خلال العثور على مواقع الانترنت لترويج البرامج المقرصنة مجاناً أو بمقابل مبلغ رمزي مما ألحق العديد من الخسائر المادية الباهظة مما أدى بالشركات المتخصصة في صناعة البرامج إلى إنشاء منظمة خاصة لمراقبة وتحليل ما يعرف بسوق البرمجيات ويتم قرصنة البرمجيات أو البيانات ويشمل النسخ غير القانوني واستخدامها أو بيعها مرة أخرى. (سهيل محمد العزام، 2009، ص. 79).

ج- جرائم الإرهاب الإلكتروني

أدى التطور الإلكتروني، وقيام ما يعرف بالحكومات الإلكترونية إلى تغيير أنماط الجريمة الإلكترونية، وظهر ما يعرف بالإرهاب الإلكتروني، حيث تم إنشاء لجنة خاصة لحماية البنية التحتية في الولايات المتحدة الأمريكية، وتم تحديد

الأهداف المحتملة من قبل الإرهابيين وهي مصادر الطاقة الكهربائية، والاتصالات، وشبكات الحاسب الآلي.

د- الجرائم المنظمة

الجريمة المنظمة هي الاقتصاد المنظم مقولة أعجبتني من أستاذي في العلوم السياسية محند برقوق حيث يتم الاعتماد على استغلال الإمكانيات المتاحة والمشروعة والعمل بطرق إجرامية مخطط لها مسبقا من خلال إخفاء المصدر غير المشروع الذي تكتسب منه الأموال تمرير خلال إنشاء مواقع خاصة بها على شبكة الانترنت لمساعدتها في إدارة العمليات والترويج بتجارة المحذرات وكذا جرائم غسل الأموال التي تعتمد على إخفاء المصدر غير المشروع الذي تكتسب منه الأموال ويوجد العديد من الجرائم تندرج في هذا النوع من الجرائم منها سرقة المعلومات بغرض المتاجرة كالبحوث العلمية أو ذات العلاقة بالتطوير التقني، أو الصناعي، أو العسكري، والاستهداف من أجل تخريب قواعد المعلومات أو تحريفها كتحرير السجلات الرسمية (ذياب موسى، 2014، ص.23).

من خلال تعدد الجرائم السالفة الذكر يمكننا فهم وإدراك حجم اثار هذه الجرائم وانتشارها حول العالم حيث المتتبع الأحداث الدولية يشاهد الارتفاع المتزايد للجريمة من خلال المؤشرات العالمية، مع تمكن المجرمين الإلكترونيين من اكتشاف طرق حديثة في الإجرام مكنهم من تنفيذ الجرائم بطرق احترافية تجاوزت الحدود الدولية ولتي تسببت في خسائر وخيمة على المستوى الاقتصادي فاقت أحيانا الجرائم التقليدية، وهناك دراسة أجريت في 2020 أجراها بنك "إتش إس بي سي" بالإشراف مع مجموعة الدراسات العالمية "نيلسن" أشارت إلى أن جرائم الإنترنت تكلف الاقتصاد العالمي نحو 445 مليار دولار كل عام، وأن الأضرار المتعلقة التي لحقت بقطاع الأعمال الأدبية ونتيجة سرقة حقوق الملكية الفكرية تسبب بخسارة الأفراد لحوالي 160 مليار دولار.

بالإضافة الى التقرير الذي أصدره مركز الدراسات الاستراتيجية والدولية CSIS أن الجريمة الإلكترونية تلحق أضرار بالأعمال التجارية والقدرة على التنافس



والابتكار. وتشير دراسة تبنتها شركة البرمجيات الأمنية (مكافي)، أن الخسائر التي تم تقديرها في التخصص السالف الذكر وصلت إلى 450 مليار دولار، في حين التقديرات القصوى التي وصلت لها الخسائر قد تجاوزت 575 مليار دولار كما ذكرت الدراسة أيضاً البلدان اليابان والولايات المتحدة والصين والمانيا أنه بلغ إجمالي خسائرها 200 مليار دولار سنوياً، كما تم تقدير الخسائر المرتبطة بالبيانات الشخصية كبيانات بطاقات الائتمان، 150 مليار دولار. وفيتقرير ذكره لجيم لويس، العامل لدى CSIS إن الجريمة الإلكترونية لها آثار خطيرة على العمالة ولا سيما في الدول المتطورة وهي بالتالي تبطئ وتيرة الابتكار العالمي بتقليل معدل العائد للمبدعين والمستثمرين على حد سواء (عبد الفتاح بيومي، 2002، ص.102).

2.3 - تحديات الجرائم الإلكترونية الوطنية والدولية

- تباين الأنظمة القانونية في الدول حيث لم تتفق على صور محددة يندرج ضمنها ما يسمى بإساءة استخدام نظم المعلومات في ظل غياب تعريف محدد للجريمة الإلكترونية. كما تبرز مشكلة تضارب المصالح وبطء آليات التعاون الدولي بين الدول، بالإضافة إلى صعوبة الموازنة بين مكافحة الجريمة الإلكترونية وحماية حقوق الإنسان. ويعد عدم التبليغ عن الجرائم السيبرانية، والاعتماد على الوسائل التقليدية للتعاون الدولي الرسمي، من العوامل التي تحول دون فعالية جهود المكافحة.

- ضعف المعاهدات الثنائية أو جماعية بين الدول يُرسخ التعاون في مجال مكافحة الجريمة الإلكترونية، وإن وُجد بعضها تبقى محدودة في تحقيق الحماية المطلوبة في ظل تطور الجريمة.

- ضعف الاختصاص في الجرائم الإلكترونية لملاحقة وادانة المجرمين بسبب التداخل والترابط بين شبكات المعلومات لأنّ الجريمة قد تقع في مكان ما وتنتج آثارها في مكان آخر.

- تُعتبر معظم التشريعات الجنائية المطبقة حالياً في معظم دول العالم تركز على الصفة الإقليمية في تطبيق قواعد الإجراءات الجنائية وتواجه تحدي سيادة الدول

امام ملاحقة المجرمين وهذا ما يفرض ضرورة الاتفاقيات الثنائية والجماعية بين الدول تتضمن تشريعات جنائية أكثر مرونة حتى تواكب سرعة التقدم التكنولوجي وعصر المعلوماتية مع تحقق الاندماج الكبير بين الحوسبة والاتصالات وولادة المدلول الشامل لتقنية المعلومات.

إن الجرائم المتصلة بتكنولوجيا الاعلام والاتصال تعتبر من الجرائم المعلوماتية المعاصرة التي ارتبطت بالأنترنت ونتيجة التقدم العلمي في هذا المجال فقد أدى الى انتشار السلوك الإجرامي المصاحب لهذه التقنية و الذي أصبح يهدد حياة لإنسان وخصوصيته والدولة وأمنها القومي ويهدد مختلف المجالات الأخلاقية والاقتصادية والاجتماعية والثقافية، برغم من تواجد الاتفاقيات الدولية المتعلقة بالجريمة الالكترونية إلا أنها تبقى غير كافية في مقابل غياب الإرادة الدولية للحد من هذه الجرائم التي تتميز بطبيعة خاصة تختلف عن الجرائم العادية التقليدية والتي تحتاج الى سن قوانين تجعلها تتوافق وتتماشى مع الواقع الرقمي الذي نعيشه.

الخاتمة:

بما أنّ التعامل بنظام المعلوماتية في مختلف الميادين والقطاعات ضرورة وحتمية مطلقة بحكم التقدم التكنولوجي في مجال الاتصالات، فقد تطورت معه اساليب الجريمة تُستخدم فيها أحدث التقنيات التكنولوجية العالية و المتطورة والسريعة ايضا لذا أُصطلح عليها بالجريمة الالكترونية او المعلوماتية، وتبقى المعادلة قائمة وفي تطور مستمر في كلا الاتجاهين الا أن تُحرز الاليات القانونية والتقنية في حماية البيانات السّرية التي تتضمنها برامج أو محتويات الحواسيب والاجهزة المستخدمة تقدما ومن ثمة قد تتغير المعادلة في صالح الحماية الامنية للنظام المعلوماتي .

هذا لن يتأتى الا من خلال مقارنة دولية واقليمية يكون مصدرها الارادة السياسية لأعلى هيئة أممية من خلال الاتفاقيات الدولية التي تعمل على تجريم الدخول غير المصرح به بمختلف صوره بالإضافة الى التشريعات الوطنية التي



تقوض من فرصة الافلات من المجرمين من العقاب خاصة اذا امتدت الى الملاحقة الدولية والاقليمية من خلال تفعيل هذه الاتفاقيات.

النتائج:

إنّ دراسة موضوع الجريمة الالكترونية تكتسي اهمية بالغة كونها تعالج اخطر الجرائم الحديثة وانطلاقا من اظهار طبيعتها وتحديد المفاهيم المرتبطة بها والتطرق ايضا الى الجهود الدولية والهيئات الأممية التي ابدت اهتمامها بالظاهرة باعتبارها جرائم دائمة التطور يجب تطويقها لضمان امن وممتلكات الاشخاص، الجماعات والمؤسسات حيث توصلت الدراسة الى النتائج التالية:

- تأكد أنّ الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ظاهرة إجرامية حديثة الولادة وهي جريمة يمكن أن ترتكب في أي مكان عبر الشبكة العنكبوتية أي أنها عابرة للحدود، فمن الصعب الكشف عن أدلتها ومن الصعب التحقيق فيها حتى أصبحت مشكلة عالمية تهدد أمن المجتمعات والدول؛
- أنّ مكافحة الجرائم المتصلة بتكنولوجيا الاعلام والاتصال يتطلب مصداقية في التشريعات والقوانين على المستوى الدولي لتعزيز اليات مكافحتها على المستوى المحلي؛
- أنّ نقص الخبراء والمختصين في قطاع أمن المعلومات يُعزز من قدرات المجرمين في الفضاء الالكتروني ويتسبب في حدوث جرائم إلكترونية؛
- أنّ التقصير في الاهتمام بالأجهزة الخاصة بالخبرة الجنائية الرقمية يُساعد على تنامي وانتشار الجرائم المعلوماتية.

التوصيات:

- سن التشريعات الدقيقة الشاملة التي تناسب مقاومة تلك الجرائم، من خلال صياغة قوانين تنظم وتواكب التطورات التكنولوجية المتسارعة للحد من التهديدات والمخاطر المحتملة؛

- عمل منصات ومبادرات رقمية لمكافحة الشائعات والأخبار المضللة ورفع درجة الوعي الاجتماعي بمخاطر التوظيف السيء لوسائل التكنولوجيا لدى الأفراد والمؤسسات.
- اتباع سياسة فعالة وقوية لتشفير البيانات والمعلومات الحساسة والتركيز على أمن التقنية السحابية؛
- تشجيع البحث والتطوير في مجال الحماية من الجريمة الإلكترونية ورصد انتهاكاتهما وضبط أدلتها ومركبها؛
- بناء هياكل تنظيمية فعالة لتقييم وتقويم جاهزية الأمن السيبراني لمواجهة الجريمة الإلكترونية؛
- ضرورة العمل على وضع التدابير اللازمة لحماية المعلومات والبيانات الأصلية الحساسة وتعزيز صمودها في وجه الاختراقات والهجمات الإلكترونية؛
- اختراع شفرات جديدة لاكتشاف الهجمات المفاجئة والمحتملة وتتبعها بدقة، والعمل على وضع آلية لتطوير وإنشاء نظام الإنذار المبكر الذي يرصد الهجمات والتهديدات الأمنية المتوقعة، وذلك من خلال عمل نظام محاكاة لتقنيات الهجوم الرقمية الفعلية لكشف نقاط الضعف الأمنية؛
- استضافة الخبراء والمتخصصين في مجال الرقمنة والأنترنت والاستفادة من خبراتهم وتوجيهاتهم في مختلف وسائل معالجة القضايا الأمنية الاستراتيجية الرقمية؛
- ضرورة استحداث مناهج تعليمية لدى كافة الأطوار التعليمية متعلقة بأنظمة مكافحة جرائم الفضاء السيبراني ضمن لتعزيز الثقافة الرقمية والأمن الرقمي، والتي من شأنها دعم الاستخدام الآمن والأمثل لتكنولوجيا الاتصال والإعلام؛
- تكوين وتدريب الكوادر المختصة في القطاع العام والخاص لتأهيلهم وبناء قدراتهم من أجل إعطاء الدعم للمجتمع والدولة في مجال تحقيق للأمن السيبراني؛



- إنشاء بنيات تحتية علمية منتشرة في كل الدولة بالشراكة مع القطاع الخاص للتدريب على الأمن السيبراني؛
- إنشاء مختبرات لتقييم وتحليل مهددات الأمن السيبراني والتحذير منها، وتنمية وتطوير لمهارات في المجالات الأساسية للأمن السيبراني.

قائمة المصادر والمراجع:

أولاً: المراجع باللغة العربية:

1- الكتب

- أحمد حسبو عمرو، حماية الحريات في مواجهة نظم المعلومات، دراسة مقارنة القاهرة : دار النهضة العربية، 2000
- الحسيني عمار عباس جرائم الحاسوب والانترنت، الجرائم المعلوماتية الطبعة الأولى منشورات زين الحقوقية، بيروت 2017.
- سامي جلال فقي حسين، التفتيش في الجرائم المعلوماتية، دراسة تحليلية، دار شتات للنشر والبرمجيات القاهرة:، 2011.
- سامي علي حامد عياد، الجريمة المعلوماتية وإجرام الانترنت، دار الفكر الجامعي القاهرة : 2007.
- سعدون مصطفى، وآخرون، الجريمة الإلكترونية عبر الانترنت أثرها وسبل مواجهتها الكلية التقنية، "بغداد : 2011
- سهيل محمد العزام، الوجيز في الجرائم الانترنت، الطبعة الأولى دائرة مكتبة الجامعة الأردنية، عمان : 2009
- عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكومبيوتر والانترنت دار الكتب القانونية القاهرة :، 2002.
- عبد اللطيف حسن سعيد، اثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الإنترنت، ط 1 ، دار النهضة العربية القاهرة: ، 1999
- عبد النبي الشكري عادل يوسف الجريمة المعلوماتية وأزمة الشريعة الجزائية، مركز دراسات بغداد الكوفة، 2008.
- عبيد الكعبي محمد، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الأنترنت، دراسة مقارنة الطبعة الثانية ، دار النهضة العربية القاهرة :، (2009) ،

- العزام سهيل محمد، الوجيز في الجرائم الانترنت الطبعة الأولى دائرة مكتبة الجامعة الأردنية، عمان ، 2009.
- فتوح الشاذلي وعفيفي كامل عفيفي، جرائم الكمبيوتر، بيروت، منشورات الحلبي الحقوقية 2003
- محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي، دار الجامعة الجديدة للنشر القاهرة :، 2007
- محمد عبيد الكعبي، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الأنترنت، دراسة مقارنة، الطبعة الثانية، دار النهضة العربية، القاهرة : 2009
- مدحت محمد عبد العزيز ابراهيم، الجرائم المعلوماتية الواقعة على النظام المعلوماتي ط1،، دراسة مقارنة، دار النهضة العربية القاهرة، 2015.
- مصطفى سعدون، سلمان محمود، عبد الرحمن حسن الجريمة الإلكترونية عبر الانترنت أثرها وسبل مواجهتها الكلية التقنية، بغداد :، 2011.
- المناعسة اسامة احمد، جلال محمد الزعبي، صايل فاضل الهواوشة، جرائم الحاسب الآلي والإنترنت، دراسة تحليلية مقارنة،، الطبعة الأولى دار وائل للنشر، عمان، الأردن، 2001.

2- الملتقيات:

- البشري محمد الامين، التحقيق في جرائم الحاسب الآلي، بحث مقدم إلى مؤتمرات القانون والكمبيوتر والانترنت، كلية الحقوق والشرعية جامعة الامارات، الامارات العربية 21 مايو 2005.
- ذياب موسى البدنية، الجرائم الالكترونية – المفهوم والاسباب - الملتقى العلمي حول الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية خلال الفترة من 02-2014/09/04، كلية العلوم الإستراتيجية، عمان، ص.

3- المجلات:

- فهد بن عايد الشمري، الإطار القانوني لحماية البيانات الشخصية في المملكة العربية السعودية، مجلة البحوث الفقهية القانونية كلية الشريعة والقانون، جامعة الأزهر العدد 43، 2023 ص19

4- الاتفاقيات:

- نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية، ط1، منشورات الحلبي، بيروت 2005



- إتفاقية بودابست المبرمة في 8 نوفمبر سنة 2001 والخاصة بحماية المعلوماتية ومنع وقمع الإجرام المعلوماتي.
- الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المؤرخة في ديسمبر 2010.

5- القوانين الدولية:

- قانون رقم 04-09 المؤرخ في 14 شعبان 1430 الموافق لـ 05 أوت 2009م، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.
- نص الفقرة الثامنة من المادة رقم (1) من نظام مكافحة جرائم المعلوماتية السعودي.
- الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المؤرخة في ديسمبر 2010.
- نص الفقرة العاشرة من المادة رقم (1) من القانون القطري رقم 14 لسنة 2014 م.

ثانيا: المراجع باللغة الأجنبية:

- Al Badayneh Human Behavior: When and where virtual Society meets physical Society?. European Journal of Science and Theology, February 2013, Vol.9, No.1, 3-17
- Halder, D., & Jaishankar : Cyber crime and the Victimization of Women: Laws Rights, and Regulations. Hershey, PA, USA: IGI Global. ISBN 978-1-60960-830-9
- Kenneth Laudon, Jane Laudon, " Management Information System- managing The digitalFirm" , seventh edition, prentice-hall, inc ,new jersey ,USA, 2004,p 8.
- Thomas j smedinghoff, the legal guide to developing protecting and