المسؤولية الجنائية في القانون السيبراني

(cyber law)"دراسة تشريعية مقارنة"

Criminal liability in cyber law
Comparative legislative study

إعداد

د. /أحمد عبدالله عبدالعزيز الحبيب

استاذ مساعد بأكاديمية سعد العبدالله للعلوم الأمنية- قسم القانون العام - دولة الكويت

Dr. Ahmad Abdullah Abdullaziz Alhabib

Assistant Professor at the Saad Al-Abdullah Academy for Security Sciences - Public Law Department, State of Kuwait.

Bo7bib@gmail.com

المسؤولية الجنائية في القانون السيبراني (cyber law)
"دراسة تشريعية مقارنة"

الملخص

نظرا لازدياد الجرائم السيبرانية Cyber Crimes شرعت الدول بوضع تشريعات جنائية خاصة لمكافحة جرائم الحاسوب الآلي التي تعتبر ظاهرة مستحدثة علي علم الإجرام، ويثير موضوع المسئولية الجنائية في القانون السيبراني Cyber Law العديد من الإشكاليات خاصة في بيئة الإنترنت والتي يوجد بها العديد من التعقيدات التشريعية نظرا لطبيعة تلك الجرائم التي تتسم بخصائص السعولة وصغوبة العثور على الدليل المؤدي للإثبات الى جانب مكان تلك الجرائم عبر مناطق العالم المختلفة وكلها أمور أدت الى البحث الدولي عن قوانين وتشريعات تتماشي وطبيعة الجرائم السيبرانية وفي ضوء ما سبق يمكن بلورة مشكلة البحث على هيئة تساؤل رئيس وهو: **ما هي الآليات المختلفة للجوانب الإجرائية والتشريعية للمسؤولية الجنائية في القانون السيبراني (cyber law)؟**

نتائج الدراسة

أولا: من المشكلات التي ظهرت على الساحة التشريعية هي فكرة المسؤولية القانونية للجرائم السيبرانية المزودة بتطبيقات الذكاء الاصطناعي والقادرة على القيام بالأخطاء وارتكاب الجرائم والإضرار بالغير دون أي تدخل من المستعمل أو المبرمج.

ثانيا: إنّ الهجوم السيبراني وقت السلم من الأمور التي يُوجد اختلاف حولها، من خلال تحليل المبادئ العامة للقانون الدولي العام نجد أنّ للدولة التي تعرضت للهجوم السيبراني إذا كانت آثاره تُشبه آثار الهجوم المسلّح يكون لها حق الدفاع عن النفس، سواء أكان بهجمة سيبرانية أم بهجوم مسلح.

ثالثا: إنّ هناك جهودًا دولية وإقليمية لمكافحة الجرائم السيبرانية Cyber Crimes وتحديد المسئولية الجنائية وذلك من خلال المؤتمرات والاتفاقيات الدولية لمنع الجريمة السيبرانية، ومعاملة المجرمين السيبرانيين.

الكلمات الدالة: المسئولية الجنائية-القانون السيبراني-دراسة مقارنة

Summary

Due to the increase in cybercrime, States have introduced special criminal legislation to combat computer crime, which is a new phenomenon in criminology. The issue of criminal liability in cyber law raises many problems, especially in the Internet environment, which has many legislative complexities due to the nature of those crimes, which are characterized by the characteristics of sovereignty and the difficulty of finding evidence leading to proof as well as the location of those crimes across different regions of the world, all of which led to the international search for laws and legislation consistent with the nature of cybercrime The search in the form of a prime question is: What are the different mechanisms for the procedural and legislative aspects of criminal responsibility in cyber law?

Study results

First: One of the problems that have emerged in the legislative arena is the idea of legal responsibility for cybercrime equipped with artificial intelligence applications and able to make mistakes and commit crimes and harm others without any interference from the user or programmer.

Second: A peacetime cyberattack is one of the things about which there is disagreement, through an analysis of the general principles of general international law, we find that a State that has been subjected to a cyberattack if its effects resemble those of an armed attack has the right to self-defense, whether by a cyberattack or an armed attack.

Third, there are international and regional efforts to combat cybercrime and establish criminal responsibility through international conferences and conventions for the prevention of cybercrime and the treatment of cybercriminals.

KeyWords: Criminal liability - Cyber law - Comparative study

الإطار العام للدراسة

مقدمـــة

تعتبر الجرائم السيبرانية Cyber Crimes من الجرائم الحديثة التي ما زال هناك خلاف كبير حول مفهومها خاصة أنها تتطور بتطور تكنولوجيات الاتصال وتتخذ كل يوم صورة ومظهرا جديدا، إلى جانب كونها جريمة واسعة النطاق توسع معها مفهوم الجريمة وبالضرورة مفهوم العقاب خاصة أنها أصبحت تهدد إلى جانب الأفراد العديد من المؤسسات والهيئات العمومية والخاصة وتهدد استقرار الدول وأمنها(١).

ونظرا لازدياد الجرائم السيبرانية Cyber Crimes شرعت الدول بوضع تشريعات جنائية خاصة لمكافحة جرائم الحاسوب الآلي التي تعتبر ظاهرة مستحدثة علي علم الإجرام ومن هذه الدول، الولايات المتحدة الأمريكية وفرنسا وباقى دول الاتحاد الأوروبي الذي وضع اتفاقية حول جرائم الحاسوب الآلي سنة ٢٠٠١م، والتي أوصت فيها الدول الأعضاء باتخاذ كافة الإجراءات التشريعية أو غيرها حسب الضرورة لجعل الدخول إلى جميع نظم الحاسوب الآلي أو أي من أجزائه بدون وجه حق جريمة جنائية بحسب القانون المحلي، كما أوصت هذه الاتفاقية على مجموعة من المبادئ العامة المتعلقة بالتعاون الدولي في مجال الشئون الجنائية، وحددت كذلك الإجراءات المتعلقة بطلبات المساعدة المتبادلة بين الدول الأعضاء في غياب الاتفاقيات الدولية(٢).

---

(١) سمية بهلول ، دور الإدارة الإلكترونية في تفعيل أداء الجماعات الإقليمية في الجزائر، أطروحة مقدمة لنيل شهادة الدكتوراه في الحقوق، تخصص : إدارة محلية كلية الحقوق والعلوم السياسية، جامعة باتنة ١ الحاج لخضر ٢٠١٧/٢٠١٨، ص ٢٨٠.

(٢) د. محمد صادق اسماعيل، جرائم شبكات التواصل الإجتماعي والإنترنت، المنامة، مركز معلومات المرأة والطفل، ٢٠١٤، ص. ٣٤

ولقد سعى المجتمع الدولي للتعاطي مع مسألة المسئولية الجنائية للجرائم السيبرانية حيث تم تدشين إعلان إيريتشي بشأن مبادئ الاستقرار السيبراني والسلام السيبراني بواسطة فريق الرصد الدائم المعني بأمن المعلومات التابع للاتحاد العالمي للعلماء (WFS [1])، حيث اعتمدته الجلسة العامة للاتحاد العالمي للعلماء في الدورة الثانية والأربعين للحلقات الدراسية الدولية بشأن الطوارئ العالمية وفي إيريتشي (صقلية) في ٢٠ أغسطس ٢٠٠٩؛ وقد نشر فريق الرصد ورقات عديدة بشأن الأمن السيبراني والحرب السيبرانية، ويتناول بانتظام قضايا أمن المعلومات باعتبارها موضوعًا من موضوعات الطوارئ الحرجة أثناء الدورات العامة للاتحاد العالمي للعلماء التي تنعقد في شهر أغسطس من كل عام في إيريتشي. ويُبين هذا الإعلان أن تحقيق الاستقرار السيبراني وتحقيق السلام السيبراني أمران متداخلان تداخلا وثيقا، ويتسم الإعلان بالإيجاز ويُركز على العناصر التشغيلية الأساسية للسلام السيبراني([2]). وقد دعا الاتحاد العالمي للعلماء منذ سنة ٢٠٠٢ إلى العمل على وضع قانون عالمي للفضاء السيبراني -

(١) في عام ١٩٧٣ قامت مجموعة من العلماء البارزين بإنشاء الاتحاد العالمي للعلماء في إيرتشه بجزيرة صقلية، ومنذ ذلك الحين انضم كثير من العلماء الآخرين إلى الاتحاد ، والاتحاد تجمع حر أخذ ينمو حتى أصبح يضم أكثر من ١٠٠٠ عالم من ١١٠ دولة. ويتقاسم جميع الأعضاء نفس الأهداف والمثل العليا، ويُساهمون طواعية في الدفاع عن مبادئ الاتحاد ، ويُشجع الاتحاد على التعاون الدولي في العلم والتكنولوجيا بين العلماء والباحثين من كل أنحاء العالم، ويسعى الاتحاد وأعضاؤه إلى تحقيق حرية تبادل المعلومات كهدف مثالي بحيث لا تكون الاكتشافات والتقدمات العلمية قاصرة على قلة مختارة. والهدف هو تقاسم هذه المعارف بين شعوب كل الدول ؛ ليتمتع كل شخص بفوائد تقدم العلم.

وكان إنشاء الاتحاد العالمي للعلماء ممكنا بفضل وجود مركز للثقافة العلمية أقيم في إيرتشه ؛ لتخليد ذكرى عالم الفيزياء إيتوري مايورانا باسم مؤسسة إيتوري مايورانا ومركز الثقافة العلمية (المركز). وأصبح هذا المركز الذي أطلق عليه تسمية ، جامعة الألفية الثالثة قوة تعليمية عالمية، وقام هذا المركز منذ إنشائه في عام ١٩٦٣ بتنظيم ١٢٣ مدرسة و ١٤٩٧ دورة دراسية حضرها أكثر من ٤٨٤ ألف مشاركا منهم ١٢٥) من الحاصلين على جائزة نوبل) من ٩٢٣ جامعة ومختبرا في ١٤٠ دولة.

(٢) هاني محمد العزازي، النظام القانوني الدولي لمكافحة المخاطر السيبرانية، القاهرة، ص.٥٢٣

وأنّه من الأفضل أن يكون تحت رعاية الأمم المتحدة [١] - خاصة في مجال الاستخدامات العدوانية والعسكرية للفضاء السيبراني.

مشكلة الدراسة

يثير موضوع المسئولية الجنائية في القانون السيبراني Cyber Law العديد من الإشكاليات خاصة في بيئة الإنترنت والتي يوجد بها العديد من التعقيدات التشريعية نظرا لطبيعة تلك الجرائم التي تتسم بخصائص السعولة وصغوبة العثور على الدليل المؤدي للإثبات الى جانب مكان تلك الجرائم عبر مناطق العالم المختلفة وكلها أمور أدت الى البحث الدولي عن قوانين وتشريعات تتماشي وطبيعة الجرائم السيبراني وكذلك تحديد أركان المسئولية والتي تزداد تعقيدا يوما بعد يوم. وفي ضوء ما سبق يمكن بلورة مشكلة البحث على هيئة تساؤل رئيس وهو:

ما هي الآليات المختلفة للجوانب الإجرائية والتشريعية للمسؤولية الجنائية في القانون السيبراني (cyber law)؟

تساؤلات الدراسة

تطرح الدراسة الحالية مجموعة من التساؤلات الفرعية التالية:

١) ما مفهوم الجريمة السيبرانية وما أبرز خصائصها المختلفة في البيئة الرقمية؟

٢) كيف تبدو الأبعاد المتعلقة بالمسئولية الجنائية للجريمة السيبرانية؟

---

(١) انظر:

Toward a Universal order of Cyberspace managing Threats from Cybercrime of Cyberya

تقرير وتوصيات، فريق الرصد الدائم المعني بمجتمع المعلومات والتابع لاتحاد العلماء العالمي، ١٩ نوفمبر ٢٠٠٣، تقرير مقدم إلى القمة العالمية لمجتمع المعلومات http://www.itu.int/dms_pub/itu-s/md./pdf

٣) ما هي تدابير الضبط القانوني الدولي تجاه المسئولية الجنائية للجرائم السيبرانية؟

أهمية الدراسة

يمكن تحديد أهمية هذه الدراسة في ضوء الاعتبارات التالية:

أولا: يكتسب البحث أهميته من حداثة تلك الجرائم والبحث في أبعاد المسئولية الجنائية في ظل تفاقم تلك الجرائم نتيجة الثورة التكنولوجية الهائلة في كافة أرجاء العالم.

ثانيا: يمثل مبدأ المسئولية الجنائية للجرائم السيبرانية أحد ركائز الإطار التشريعي للضبط القانوني من خلال تحديد ابعاد تلك المسئولية والبحث عن اليات تشريعية لطرفي المشكلة "الجريمة/القوانين الحاكمة ".

ثالثا: تتبلور الأهمية التطبيقية لتلك الدراسة في طرح اليات تشريعية داخل الدول العربية والأجنبية تجاه المسئولية الجنائية سواء من خلال تحديد عناصر الجريمة ودور الشرطة والإدعاء العام تجاه الجرائم السيبرانية Cyber Crimes.

منهاجية الدراسة

سعى الباحث إلى الاستفادة من بعض المناهج في دراسة موضوع البحث وذلك على النحو التالي :

١- **المنهج القانوني"** يتم استخدام هذا المنهج وذلك من خلال معالجة وتحليل الأساليب والطرق والإجراءات المرتبطة بالمسئولية الجنائية تجاه الجرائم السيبرانية Cyber Crimes في التشريعات العربية والأجنبية.

٢- **المنهج المقارن"** تعتمد الدراسة على المنهج التحليلى المقارن في سبيل تحديد الأطر المختلفة للمسئولية الجنائية تجاه الجريمة السيبرانية عربيا وعالميا سعيا لتحديد اركان تلك المسئولية واليات المكافحة التشريعية.

بنية الدراسة

تم تقسيم الدراسة الحالية الى ثلاثة مباحث رئيسة وذلك كما يلي:

المبحث الاول: ماهية وخصائص المسئولية الجنائية في القانون السيبراني وتطبيقاته المعاصرة

المبحث الثاني: تطبيقات المسئولية الجنائية في القانون السيبراني المقارن

المبحث الثالث: آليات تعاطي المجتمع الدولي مع المسئولية الجنائية للجرائم السيبرانية

المبحث الاول

ماهية وخصائص المسئولية الجنائية في القانون السيبراني وتطبيقاته المعاصرة

تعتبر الجرائم السيبرانية Cyber Crimes من الجرائم الجديدة التي لم تظهر إلا مع الانتشار الواسع للتقنيات الرقمية المعاصرة وتزايد استخدامها وما ترتب عنه من تجاوزات من طرف الأفراد والمؤسسات في استغلال واستعمال هذه التكنولوجيات الأمر الذي استوجب إعادة النظر في الجرائم التقليدية والعمل على بذل إجراءات وقائية، وتجريمية لهذا النوع من الجرائم الذي أصبح يثبت يوميا مدى خطورته بالنسبة للأفراد والمؤسسات التي تطورت إلى درجة أنها أصبحت تهدد حتى الأمن القومي للدول وسيادتها واستقرارها وتعرف الجريمة في صورتها التقليدية بأنها "كل عمل غير مشروع يقع على الإنسان في نفسه أو ماله أو عرضه أو على المجتمع ومؤسساته ونظمه السياسية والاقتصادية"[1].

أولا: ماهية المسئولية الجنائية

يمكن التأكيد أن المسؤولية القانونية تتوزع بين مسؤوليتين أساسيتين: جزائية ومدنية والمسؤولية المدنية ليست موحدة؛ إذ إنها تنقسم إلى مسؤولية عقدية ومسؤولية تقصيرية تترتب عن عمل غير مشروع يصدر عن شخص وينجم عنه ضرر مما يلقي على المسؤول عنه واجب إصلاح الضرر.

(١) أحسن بوسقيعة، الوجيز في القانون الجزائي العام، دار هومة للنشر والتوزيع، الجزائر، الطبعة العاشرة، ٢٠١١، ص٢٧.

أما المسؤولية الجزائية فيكون مرتكب الفعل الضار مسؤولا تجاه الدولة باعتبارها حامية للمجتمع ويكون الجزاء عقوبة توقع عليه باسم المجتمع زجرًا له وردعًا لغيره وتتولى النيابة العامة إقامة الدعوى عليه أمام المحاكم الجزائية وتقوم الدولة بتنفيذ العقوبة بمالها من عمال تابعين لسلطتها التنفيذية. أما في المسؤولية المدنية فيكون الفاعل قد أخل بالتزام مقرر في ذمته ويترتب على هذا الإخلال ضرر للغير، ويكون للمتضرر وحده حق المطالبة بالتعويض ويعتبر هذا الحق حقًا مدنيًا خالصًا له وتختص بها المحاكم المدنية، ذلك أن دائرة المسؤولية المدنية أوسع من دائرة المسؤولية الجزائية؛ لأن المسؤولية الجزائية مقصورة على حالات الإخلال بأوامر أو نواه منصوص عليها صراحة في القوانين الجزائية. أما المسؤولية المدنية فيكفي في قيامها الإخلال بأي واجب قانوني. وبما أن الواجبات القانونية لا حصر لها فإن دائرة المسؤولية المدنية تكون لا حد لها(١).

ولفظ "المسؤولية" إذا أطلق دون وصف أو إضافة فالمراد به "حالة الشخص الذي ارتكب أمرًا يوجب المؤاخذة" (٢)، وهو بهذا المعنى يتنوع بحسب القاعدة التي خالفها الشخص من جهة، ومن حيث الأمر المرتكب من جهة أخرى؛ فعلى الاعتبار الأول تنقسم المسؤولية إلى مسؤولية أدبية، ومسؤولية قانونية.

---

(١) بندر عساف الخالدي، الضمان ضد المسؤولية المدنية في القانونين الكويتي واللبناني. نموذج ضمان السيارات، رسالة دكتوراه غير منشورة، الجامعة اللبنانية، المعهد العالي للدكتوراة في الحقوق والعلوم السياسية والإدارية والاقتصادية،٢٠١٢،ص.١١٧

(٢) راجع الأستاذ مصطفى مرعي، المسؤولية المدنية في القانون المصري ط- مطبعة نورى – القاهرة – الأولى – ١٩٣٥ – ١٩٣٦ ص ١، الأستاذ حسن عكوش، المسؤولية المدنية في القانون المدني الجديد، نشر مكتبة القاهرة الحديثة – ط – أولى – ١٩٥٧ – ص ١٠، د. سليمان مرقس الوافي في شرح القانون المدني، الطبعة الخامسة – ١٩٨٨ – الالتزامات – المجلد الثاني ص ١، الأستاذان حسين وعبد الرحيم عامر المسؤولية المدنية ط دار المعارف – مصر – الثانية – ١٩٧٩ ص ٣.

ومن هنا يمكن التأكيد أن المسؤولية هي الالتزام بالتعويض المادي عن الأضرار التي تلحق بالغير نتيجة خطأ. وعلى هذا الأساس تتحقق المسؤولية بتوفر ثلاثة عناصر هي الخطأ والضرر والعلاقة السببية بينهما. وعلى الرغم من تعدد أنواع المسؤوليات ما بين مسؤولية أدبية وجنائية ومدنية، فإن التأمين عمومًا يركز على تغطية المسؤولية المدنية. وتقوم تلك المسؤولية عند وجود ضرر يصيب الآخرين نتيجة خطأ أو إهمال غير متعمد ويترتب على المتسبب ضرورة جبر هذا الضرر. وفي هذا الصدد يمكن التأكيد أن المسؤولية تجاه الغير تشمل المسؤولية عن أعمال شخصية وهي تتمثل في كل خطأ سبَّب ضررًا للغير ويلزم من ارتكبه بالتعويض، وتشمل أيضًا المسؤولية عن أعمال الغير مثل المسؤولية عن أعمال من تجب الرقابة عليهم كمسؤولية الأب عن تصرفات أبنائه أو مسؤولية المتبوع عن أعمال تابعيه مثل مسؤولية رب العمل عن أعمال موظفيه، بالإضافة إلى المسؤولية الناتجة عن الأشياء مثل مسؤولية صاحب السيارة عما تسببه سيارته من أضرار للغير(١).

ثانيا: ماهية الجريمة التقنية

يمكن تحديد ماهية الجرائم التقنية Cyber Crimes وأبرز خصتئصها كما يلي:

١- **التعريف الضيق للجريمة السيبرانية :** ذهب جانب كبير من الفقه إلى التضييق من نطاق التعريف الموضوع لمفهوم الجريمة السيبرانية وركز بذلك على جانب معين في سبيل وضع هذا التعريف كما يلي:

أ - تعريف الجريمة السيبرانية استنادا إلى وسيلة ارتكابها يذهب الفقه انطلاقا من هذا المعيار إلى التركيز على الحاسب الآلي على اعتباره أساس الجريمة السيبرانية

(١) راجع د. أحمد عبد المعطي أحمد، مقدمة في القانون المدني، القاهرة، دار المطبوعات القانونية، ٢٠٠٨، ص ٦٦.

ونقطة التمييز بينها وبين الصور التقليدية وحتى الحديثة للجرائم المعروفة في مجال القانون[١]. وبالتالي تعد الجريمة السيبرانية هى "الاعتداءات القانونية التي ترتكب بواسطة المعلوماتية بهدف تحقيق الربح وعرفها البعض الآخر بأنها "فعل إجرامي يستخدم الحاسب في ارتكابه كأداة رئيسية".

كما ذهب جانب إلى أن الجريمة السيبرانية هي "كل نشاط إجرامي تستخدم فيه التقنية الإلكترونية المتمثلة في الحاسوب الآلي الرقمي وشبكة الإنترنت بطريقة مباشرة أو غير مباشرة كوسيلة لتنفيذ الفعل الإجرامي المستهدف"[٢]. وهناك من ذهب إلى التفصيل نوعا ما في هذا المعيار وعرفها على أنها "جرائم" الشبكة العالمية التي يستخدم فيها الحاسب وشبكاته العالمية كوسيلة مساعدة لارتكاب جريمة، كاستخدامه في النصب والاحتيال وغسل الأموال وتشويه السمعة والسب"[٣].

ب- **تعريف الجريمة التقنية استنادا إلى** الوسيلة المستخدمة في ارتكابها ذهب جانب آخر من الفقه إلى تعريف الجريمة السيبرانية استنادا إلى مستوى معرفة المجرم للتقنيات الحديثة للحاسوب وتكنولوجيات الإعلام والاتصال على اعتبار أن هذه التقنيات والوسائل هي المحل الأساسي لارتكاب هذا النوع من الجرائم وتنفيذها يستحيل دون علم المجرم بهذه التقنيات ومعرفة طريقة استخدامها لارتكاب الفعل

(١) غنية باطلي، الجريمة الإلكترونية (دراسة مقارنة)، منشورات الدار الجزائرية، الجزائر، ٢٠١٥، ص١٥.

(٢) كحلوش علي، "جرائم الحاسوب الآلي وأساليب مواجهتها"، مجلة الشرطة، العدد ٨٤، يوليو ٢٠٠٧، المديرية العامة للأمن الوطني، الجزائر،ص٥١.

(٣) مصطفى محمد موسى، التحقيق الجنائي في الجرائم الإلكترونية، مطابع الشرطة، القاهرة، الطبعة الأولى، ٢٠٠٩، ص١١٢.

الاجرامي، وانطلاقا من هذا المعيار يعرف الفقه الجريمة السيبرانية بالقول إنها "جرائم" يكون متطلبا لاقترافها أن تتوافر لدى فاعلها معرفة بتقنية الحاسب"[١]. كما أنها "كل فعل غير مشروع تكون المعرفة بتقنية المعلوماتية أساسية لمرتكبه وللتحقيق فيه وملاحقته قضائيا" وعرفها جانب آخر بأنها كل فعل غير مشروع يكون العلم بتكنولوجيا الحاسبات الآلية بقدر كبير لازما لارتكابه من ناحية، والملاحقته وتحقيقه من ناحية أخرى"[٢].

ج- **تعريف الجريمة الرقمية استنادا إلى موضوعها :** حيث عرفت بأنها نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب الإلكتروني أو التي تحول عن طريقه"[٣].

٢- **التعريف الموسع للجريمة السيبرانية :** حيث تعرف بأنها "كل فعل أو امتناع عن فعل يأتيه الإنسان إضرارا بمكونات الحاسب الآلي المادية والمعنوية وشبكات الاتصال الخاصة به باعتبارها من المصالح والقيم المتطورة التي تمتد تحت مظلة قانون العقوبات لحمايتها"[٤]، **كما** عرفها البعض بأنها "كل سلوك غير مشروع أو

(١) سمية سليمان بهلول، اعتماد المسئولية القانونية للروبوتات الذكية للحماية من مخاطر الجرائم السيبرانية، مرجع سابق، ص. ٨٩

(٢) نائلة عادل محمد فريد، جرائم الحاسب الاقتصادية، رسالة مقدمة لنيل درجة الدكتوراه، كلية الحقوق جامعة القاهرة، ٢٠٠٣، ص٢١.

(٣) أشرف جمال محمود عبد العاطي، الإدارة الإلكترونية للمرافق العامة، دار النهضة العربية، مصر، ٢٠١٦، ص ٣٥٩

(٤) هلالي عبد الله أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم في جرائم المعلومات (دراسة مقارنة)، دار النهضة العربية، القاهرة، ٢٠٠٠، ص ٠٧.

غير أخلاقي أو غير مصرح به، يتعلق بالمعالجة الآلية للبيانات أو بنقلها"[١] وتم تعريفها بأنها "كل استخدام في صورة فعل أو امتناع من شأنه الاعتداء على أي مصلحة مشروعة، سواء كانت مادية أو معنوية يكون ناتجا بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية ومعاقب عليه قانونا أيا كان غرض الجاني"[٢]..

ومن هنا يتبنى الباحث التعريف التالي: " كل جريمة أو سلوك غير مشروع يستخدم بالحاسب الآلي أو محاولة نسخ أو حذف أو إتلاف لبرامج الحاسب الآلي أو أي جريمة يكون لتنفيذها صلة بالقواعد والعلوم المعلوماتية أو أي سلوك غير مشروع متعلق بالمعالجة الآلية للبيانات"[٣].

ثالثا: خصائص المسئولية الجنائية في القانون التقني

يمكن توضيح خصائص الجريمة التقنية كما يلي:

١- **صعوبة اكتشاف الجريمة التقنية** يذهب كثير من الفقه إلى أن الجريمة السيبرانية ما إلا أداة محايدة في حين أن مصدر الانتهاك الأساسي هو الإنسان ذاته، لكونه غالبا ما يهيئ الفرصة لاستغلالها، وبناء عليه فإن جوهر الجريمة السيبرانية

(١) هشام محمد فريد رستم ، الجرائم المعلوماتية أصول التحقيق الجنائي الفني واقتراح إنشاء آلية عربية للتدريب التخصصي"، ورقة بحث مقدمة ضمن فعاليات مؤتمر القانون والكمبيوتر والإنترنت كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، من ٠١ إلى ٠٣ ماي ٢٠٠٠، منشور ضمن مجلة "الشريعة والقانون"، المجلد الثاني، الطبعة الثالثة، ٢٠٠٤، ص٤٠٧.

(٢) أسماء حسين رويعي، الحق في حرمة الحياة الخاصة في مواجهة الجرائم المعلوماتية، رسالة مقدمة لنيل درجة الدكتوراه في الحقوق، كلية الحقوق، جامعة القاهرة، ٢٠١٣، ص٦٤.

(٣) نايل نبيل عمر، الحماية الجنائية للعمل الإلكتروني في جرائم المعلوماتية، دار الجامعة الجديدة، القاهرة، ٢٠١٢، ص٢٣.

يرتبط بالجاني وشخصيته ودوافعه، أما فيما يخص المجني عليهم فغالبا ما يفضلون عدم إفشاء الجرم الواقع عليهم والمرتكب ضدهم، خاصة أنها جرائم لا تحتاج إلى العنف ولا إلى استخدام وسائل الجريمة التقليدية، كما أنها لا تترك أي آثار ملموسة في الغالب، الأمر الذي يجعل من الصعب اكتشافها مع غياب آثارها المادية الخارجية، وتنقسم صعوبات اكتشاف الجريمة السيبرانية إلى قسمين منها ما يتعلق بالجاني أو المجرم مرتكب الجريمة السيبرانية ومنها ما تنصرف أو تتعلق بالمجني عليه أو الضحية المتضرر من هذه الجريمة.

٢- **الصعوبات المتعلقة بالجاني:** ثبت أن المجرم في جميع الحالات شخص طبيعي لكن المتغير أنه يهدف من خلال قيامه بالجريمة إلى تحقيق مصلحة شخصية له أو لحساب أحد الأشخاص المعنوية العامة أو الخاصة التي تعمل في مجال المعلوماتية وتستند في عملها علي التكنولوجيا بهدف التعدي علي الأنظمة المعلوماتية أو الإضرار بالغير، علاوة علي كون العوامل التي تدفع لارتكاب هذا النوع من الجرائم ليس الهدف منها الاضرار بالأشخاص إنما في العادة المساس بالمؤسسات والإضرار بالأمن العام للبلاد ، خاصة ان المتورطين في هاته الجرائم لديهم قدر كبير من الذكاء والتفوق الذي يجعلهم يباشرون جرائمهم بدقة متناهية خشية افتضاح أمرهم وضبطهم(١).

وفيما يلى عرضا لبعض السمات العديدة للمجرم المعلوماتى والتي في الغالب تميزه عن غيره من المجرمين العاديين:

(١) محمد حماد مهرج الهيتى، التكنولوجيا الحديثة والقانون الجنائي ، دار الثقافة للنشر ، الأردن ، الطبعة الأولي ، ٢٠٠٤، ص ١٢٤.

أ- المجرم التقني، مجرم متخصص حيث تبين في عديد من القضايا أن عددا من المجرمين لا يرتكبون سوى جرائم الحاسوب الآلي أي أنهم يتخصصون في هذا النوع من الجرائم، دون أن يكون لهم أي صلة بأي نوع من الجرائم التقليدية الأخرى، مما يعكس أن المجرم الذي يرتكب إلا جرام المعلوماتى هو مجرم في الغالب متخصص في هذا النوع من الإجرام[١].

ب- المجرم التقني يتسم بقدرات معلوماتية كبيرة حيث يتمتع المجرم المعلوماتى باحترافية كبيرة في تنفيذ جرائمة، حيث أنه يرتكب هذة الجرائم عن طريق الحاسوب الآلي الأمر يقتضى الكثير من الدقة والتخصص والاحترافية في هذا المجال للتوصل إلى التغلب على العقبات التي أوجدها المتخصصون لحماية أنظمة الحاسوب الآلي كما في حالة البنوك والمؤسسات العسكرية.

٣- **الصعوبات التقنية للجرائم ذات البعد الرقمي** مثل سرعة التنفيذ حيث لا يتطلب تنفيذ الجريمة عبر جهاز الكمبيوتر الوقت الكبير، وبضغطة واحدة على لوحة المفاتيح يمكن أن تنتقل ملايين الدولارات من مكان إلى آخر. وهذا لا يعني إنها لا تتطلب الإعداد قبل التنفيذ أو استخدام معدات وبرامج معينة. الى جانب التنفيذ عن بعد خيث لا تتطلب جرائم الحاسوب الآلي في أغلبها (إلا جرائم سرقة معدات الحاسوب الآلي) وجود الفاعل في مكان الجريمة.بل يمكن للفاعل تنفيذ جريمته وهو في دولة بعيدة كل البعد عن الفاعل سواء كان من خلال الدخول للشبكة

---

(١) يمكن الرجوع الى:

- Vonderau, Patrick. (December 30, 2009),The YouTube Reader, Sweden: National Library of Sweden.
- Wittkower, D:E. (October 1, 2010), Face book and Philosophy: What's on Y::our Mind?. USA: Open Court.

المعنية أو اعترض عملية تحويل مالية أو سرقة معلومات هامة أو تخريب...الخ. هذا الى جانب صعوبة إثباتها، وهذا راجع إلى افتقاد وجود الآثار التقليدية للجريمة، وغياب الدليل الفيزيقي(بصمات، تخريب، شواهد مادية) وسهولة محو الدليل أو تدميره في زمن متناه القصر، يضاف إلى ذلك نقص خبرة الشرطة والنظام العدلي، وعدم كفاية القوانين القائمة.

رابعا: المسؤولية الجنائية تجاه التطبيقات السيبرانية المتطورة " الروبوت الذكي نموذجا"

في سبيل قيام المسؤولية القانونية للروبوتات الذكي، ظهرت العديد من الآراء الفقهية التي حاولت وض تكييف قانوني للروبوت الذكي بين من يعتبر الروبوت شيء ويرى وفق هذا التكييف أن الروبوت عبارة عن شيء تقليدي أصم ما يجعل المسؤولية الناجمة عن أخطاء الروبوت في هذه الحالة تؤسس انطلاقا من قواعد مسؤولية حارس الشيء[١]. وبالتالي فإن الإشكالات الناجمة عن تعويض الأضرار التي تسببها الروبوتات في هذه الحالة تفصل فيها من خلال إقرار نظام تأمين إلزامي عن حوادث الروبوت، إضافة إلى إلزامية إنشاء صناديق خاصة لتغطية أضرارها كنظام مكمل للتأمين في حال عدم وجود غطاء تأميني، إلا أن التسليم بهذا الاتجاه يعني أن الذكاء الاصطناعي بنظر القانون هو والعدم سواء، فهذا الذكاء لا يرقى قانونيا بمنزلة شخصية الآلة الإلكترونية التي تتمتع بالذكاء، ولا حتى يغير جذريا من القواعد التي تحكم أنشطتها بصدد المسؤولية المدنية سواء أكانت ضد الروبوت أو لمصلحته[٢].

(١) فطيمة نساخ " الشخصية القانونية للكائن الجديد: الشخص الافتراضي الروبوت"، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، مجلد ٥ عدد ١، ٢٠٢٠.

(٢) كوثر منسل، وفاء شناتلية، "إثبات الخطأ الطبي في مجال الجراحة الروبوتية مداخلة مقدمة ضمن فعاليات الملتقى الوطني حول عبء إثبات الخطأ الطبي المرفقي في المؤسسات العمومية للصحة وتطبيقاته القضائية في الجزائر ، المنظم بتاريخ ٠٣ يونيو ٢٠٢١.

لتظهر في المقابل على الساحة الفقهية نظرية النائب الإنساني التي تذهب للقول بأن الروبوت هو صناعة تقنية ذكية يمكن استخدامه من قبل البشر لتحقيق منافع كثيرة، وعلى هذا الأساس برزت فكرة النائب الإنساني المسؤول عن الروبوت التي تختلف عن فكرة حارس الأشياء وتختلف أيضا عن فكرة القيم أو الوصي، وبناء على ذلك ابتكر البرلمان الأوروبي نظرية النائب الإنساني المسؤول وفقا لقواعد القانون المدني الأوروبي الخاص بالروبوتات الصادر في ١٦ فيفري ٢٠١٧ ، وذلك حتى يفرض المسؤولية عن تشغيل الروبوت على الأشخاص المعنيين وفقا لمدى تقصيرهم في تصنيعه أو استغلاله ومدى سلبيتهم في تفادي التصرفات المتوقعة من الروبوت دون افتراض الخطأ(١).

١- **الطبيعة القانونية للروبوتات الذكية :** لاشك أن الروبوتات الذكية أصبحت متطورة لدرجة أنها تنزل منزلة الأشخاص فإن هذا يعني بأننا سنجعلها تتحمل المسؤولية عن ارتكابها لأخطاء في حال وقعت، أما إذا ذهبنا مع الاتجاه الذي يعتبرها أشياء فهذا يسقط عنها تلك المسؤولية ، وبالتالي نخلص إلى أن تكييف الطبيعة القانونية للروبوتات الإلكترونية يقوم على أساسين(٢): حيث يذهب في الأساس الأول جانب من الفقه إلى اعتبار الروبوتات أشياء، وأن مالكها عبارة عن حارس لهذه الأشياء ويقع عليه عبء تحمل الخطأ المفترض وهو رأي منتقد لكون الروبوت الذكي المزود بتقنيات الذكاء الاصطناعي حاليا ليس كالآلة الصماء التي لا بد من أن

(١) محمد عرفان الخطيب، «المسؤولية المدنية والذكاء الاصطناعي... إمكانية المساءلة؟ دراسة تحليلية معمقة لقواعد المسؤولية المدنية في القانون المدني الفرنسي»، مجلة كلية القانون الكويتية العالمية، العدد الأول، ٢٠٢٠.

(٢) حسن محمد عمر الحمراوي، "أساس المسؤولية المدنية عن الروبوتات بين القواعد التقليدية والاتجاه الحديث"، مجلة كلية الشريعة والقانون، العدد ٢٣، الإصدار ٠٢، الجزء الرابع ٢٠٢١، ص ٣٠٦٦.

تكون تحت قيادة وتصرف صاحبها، فهو يمكنه التفكير وإصدار قرارات بنفسه وبنفس درجة ذكاء الشخص الطبيعي وأكثر.

ويذهب في الأساس الثاني جانب آخر من الفقه إلى إمكانية اعتبار الروبوت وكيلا عن مالكه في القيام بالأعمال والتصرفات الموكلة إليه، وأي ضرر ينتج عنه يمكن الرجوع به إلى الموكل الإنسان وهو رأي منتقد كذلك لأن الوكالة لا تتم إلا بين شخصين قانونيين، فكيف يكون الروبوت وكيلا وهو لا يتمتع بالشخصية القانونية.

٢- **طبيعة المسئولية القانونية للروبوتات الإلكترونية :** جاء في قرار البرلمان الأوروبي أن يتم التعامل مع وفق قواعد القانون المدني وتوجيهة المفوضية الأوروبية باستحداث شخصية قانونية للروبوت[١] إلا أنه لم يتم الاتفاق على السير في هذا الاتجاه وفق ما أصدره البرلمان الأوروبي، إذ وجهت له العديد من الانتقادات منها أن التفرقة في القانون المدني بين الأشخاص والأشياء تفرقة واضحة من حيث الأساس ومن حيث الآثار، فهناك من الدول من هذا القرار كالمملكة العربية السعودية مثلا وكثير من الدول الأجنبية، فدولة السعودية وكمثال واضح حينما منحت اسما وجنسية للروبوت "صوفيا" كانت مؤيدة بذلك لفكرة منح الشخصية القانونية للروبوتات الإلكترونية كونها حتمية قانونية في نظرها، كما أن العديد من الدول الأجنبية أصبحت تتعامل مع هذه الروبوتات بطريق أكثر من كونها روبوتات، فهي تتجه شيئا فشيئا للاعتراف بالشخصية القانونية لها،

(١) تهاني حامد أبو طالب، الروبوت من منظور القانون المدني المصري الشخصية والمسؤولية)، مجلة البحوث الفقهية والقانونية، العدد ٣٧، إصدار أبريل ٢٠٢٢م/١٤٤٣هـ ، ص١٦١.

إضافة إلى ذلك، ففي نظر مؤيدي هذا الاتجاه أنه لا مشكلة في منح الشخصية القانونية لهذا الروبوت الذكي(١).

إلا أن معارضي هذا الرأي، أقروا أنه في حال الاعتراف بالشخصية المعنوية للروبوتات، فإن ذلك يسقط المسؤولية عن صانعها أو مطورها أو الشركة التابعة لها، وسندخل في مشاكل جديدة كالتقاضي، حتى أن الروبوتات ليست كلها على درجة واحدة من الذكاء والقدرات، وبالتالي منحها جميعها الشخصية القانونية سيؤدي لظهور العديد من المشاكل، في حين اتجه البعض الآخر، إلى أنه تمنح للروبوتات الإلكترونية الشخصية الإلكترونية القانونية، وهي وجهة النظر التي أيدها المشرع الأوروبي، غير أن السير في هذا الاتجاه دون إنشاء آلية تنظيمية وأخلاقية تحكم عمل الروبوتات أمر له تبعاته على الإنسان والمنظومة التشريعية(٢).

٣- صور قيام المسؤولية التشريعية للروبوتات الذكية.

تأخذ المسئولية القانونية للروبوت الالكتروني عدة صور كما يلي:

أ- الجانب المتعلق بالمسؤولية المدنية: وهو ما يرتبط الجوانب التالية:

أهلية الوجوب: وهي التي تمنح الشخص الصفة القانونية التي تجعله يكتسب حقوقا،وتثبت أهلية الوجوب لكل شخص سواء كان عاقلا أم غير عاقل، وبالتالي فإن كل شخص حي له أهلية الوجوب.

(١) محمد عرفان الخطيب المسؤولية المدنية والذكاء الاصطناعي ... إمكانية المساءلة؟، دراسة تحليلية معمقة لقواعد المسؤولية المدنية في القانون المدني الفرنسي، مجلة كلية القانون الكويتية العالمية، السنة الثامنة، العدد ٠١ ، العدد التسلسلي ،٢٩ ، قطر ، مارس ٢٠٢٠، ص ١١٦.

(٢) حسن عمر محمد الحمراوي، مرجع سابق، ص ٣٠٦٧.

أهليــة التــصرف: وهــي مرتبطــة بــسلامة العقــل، فالــشخص العاقــل الــذي يمكنـه التفكير بـشكل سليم وحـده الـذي تمنح لـه أهليـة الأداء، أي إمكانيـة قيامـه بالأعمـال والتصرف فيها، وتقوم مسؤوليته في هذه الحالة في حـال قيامـه بتـصرفات غير قانونيـة أو أخل بها.

ب- **الجوانــب المتعلقــة بالمــسؤولية الجزائيــة**: فـرض الاسـتخدام الواسـع للروبوتـات الإلكترونيـة فـي العديـد مـن مجـالات الحيـاة وزيـادة توجهـات الفقـه للحـديث عـن فكـرة مـنح الشخـصية القانونيـة لهـذه الروبوتـات وفـق مـا يتناسـب وطبيعتهـا[١]. فالجرائم التـي يرتكبها الروبوت نتيجـة عدم تـوفر أحد العناصـر التـي تـوفر السلامة والأمــان عنـد اسـتعمال الروبـوت، هـذا الأمـر يكـون الـصانع هـو المـسؤول عنـه ويعاقـب علـى ذلـك، أمـا الجـرائم التـي يكـون سـببها إهمـال أو سـوء اسـتعمال هـذا الروبوت، فيعاقب عليها مستعمل ذلك الروبوت، فـي حين يقع الإشكال فـي الجرائم التـي ترتكـب مـن طـرف هـذه الروبوتـات وبإرادتهـا دون تـدخل البـشر فيهـا وكيفيـة معاقبتها عليها[٢].

ومـا يفهـم مـن كـل مـا سـبق أن قواعـد المـسؤولية الجزائيـة لـم تعـد مـستمدة مـن مفـاهيم تتـصل بمـا وراء الحـس والطبيعـة، وإنمـا مـن اعتبـارات نفـسية واجتماعيـة ونفعية، ففي منظور الفلسفة المعاصرة للتشريع الجنائي يظل الهدف من تقرير المسؤولية الجزائيـة مقاومـة الجريمـة التـي ترتكـب ومنـع ارتكـاب جـرائم أخـرى باتبـاع سياسـة جزائيــة موضــوعية يكــون هــدفها حمايــة المجتمــع حتــى يجــد كــل إنــسان الأمــان

(١) بن عودة حسكر مراد، إشكالية تطبيق أحكام المسؤولية الجنائية على جرائم الذكاء الاصطناعي، مجلة الحقوق والعلوم الإنسانية، جامعة تلمسان، المجلد ١٥ ، العدد ٠١ ٢٠٢٢، ص ٢٠٠.

(٢) سمية سليمان بهلول، اعتماد المسئولية القانونية للروبوتات الذكية للحماية من مخاطر الجرائم السيبرانية، مرجع سابق، ص.٩٧

والسكينة[١] فالإنسآلة (الروبوت) كمبدأ قانوني معمول به حديثا له شخصية قانونية اعترفت بها صراحة الكثير من النصوص القانونية الدولية خاصة على مستوى الاتحاد الدولي كما سبق ووضحنا ، وهو الأمر الذي يضفي على الروبوت الذكي مجموعة من الحقوق وكذلك الواجبات طالما يتم نمذجته من قبل البشر ليؤدي أدوارا ومصالح عديدة[٢].

وختاما، مما لا شك فيه أن الوضع التشريعي الحالي بات لا يواكب التطور المتلاحق في نظم الذكاء الاصطناعي، ويتضح ذلك في الفرضية التي تقول إنه على فرض أن الروبوت ارتكب إحدى الجرائم المعاقب عليها بعقوبة سالبة للحرية وهذا فرض لا محالة ،له، فإن هناك تساؤلات عديدة حول كيفية التحقيق مع الروبوت، بما في ذلك سؤاله واستجوابه، والحصول على الدليل الجنائي الذي هو محور اهتمام العدالة الجنائية، وكذلك حضور الجلسات والحبس المؤقت والكفالة، وعناصر الركن المادي للجريمة المتمثلة في السلوك الإجرامي للروبوت والنتيجة الإجرامية، والركن المعنوي للجريمة بما في ذلك إرادة ارتكاب الجريمة السيبرانية[٣].

(١) ممدوح حسن مانع العدوان، «المسؤولية الجنائية عن أفعال كيانات الذكاء الاصطناعي غير المشروعة»، مجلة دراسات علوم الشريعة والقانون، المجلد ٤٨ عدد ٤ ٢٠٢١، ص ١٥٧.

(٢) سمية سليمان بهلول، اعتماد المسئولية القانونية للروبوتات الذكية للحماية من مخاطر الجرائم السيبرانية، مرجع سابق، ص.٩٨

(٣) مراد بن عودة عسكر، إشكالية تطبيق أحكام المسؤولية الجنائية على جرائم الذكاء الاصطناعي"، مجلة الحقوق والعلوم الإنسانية، مجلد ١٥،عدد ١، ٢٠٢٢، ص ١٩٥.

المبحث الثاني

تطبيقات المسئولية الجنائية في القانون السيبراني المقارن

يمكن تناول التطبيقات المتعلقة بالمسئولية الجنائية للجرائم السيبرانية على النحو التالي:

أولا: الاحكام الاجرائية للجرائم التقنية الحديثة في التشريع الكويتي

لقد نصت المادة ١٧ من القانون رقم ٦٣ لسنة ٢٠١٥ في شأن مكافحة جرائم تقنية المعلومات على أن تختص النيابة العامة - دون غيرها - بالتحقيق والتصرف والادعاء في جميع الجرائم المنصوص عليها في هذا القانون. ومن ثم فقد اناط المشرع بالنيابة العامة وحدها دون غيرها سلطة التحقيق والتصرف والادعاء. ويقصد بالتحقيق استجواب المتهم وسماع الشهود وتحقيق الواقعة أما التصرف فيقصد به اتخاذ قرار بشأن التحقيق الذي تم إجراؤه بشأن الواقعة بالإحالة إلى المحكمة أو حفظ الأوراق، أما الادعاء فيقصد به مباشرة الدعوى الجزائية أمام المحكمة وفقا لنص المادة ١٠٥ من قانون الإجراءات والمحاكمات الجزائية والتي جرى نصها على أن « تتولى النيابة العامة مباشرة الدعوى الجزائية بطلب توقيع العقوبة على المتهمين بالجنايات وفقا للإجراءات وطبقا للشروط المنصوص عليها في هذا القانون» ومن ثم فلا يجوز لمحققي وزارة الداخلية إجراءات تحقيق أو التصرف في الدعوى الجزائية، ولا يجد لها من ثم إحالتها للمحكمة، فاختصاص النيابة العامة بالتحقيق والتصرف والادعاء في جنح الصحافة هو اختصاص أصيل مقرر لها باعتبارها سلطة الادعاء العام أمام محكمة الجنايات [1].

(١) وزارة العدل الكويتية، الجرائم الإلكترونية، الكويت: معهد الكويت للدراسات القانونية والقضائية، ٢٠١٩، ص. ٣١

ونظرا لخلو القانون رقم ٦٣ لسنة ٢٠١٥ بشان مكافحة جرائم تقنية المعلومات من نصوص خاصة في تحديد اختصاص المحاكم، فتطبق القواعد العامة في الاختصاص النوعي. فتختص محكمة الجنح بنظر الجرائم التي يعاقب عليه بالحبس مدة لا تجاوز ثلاث سنوات والغرامة أو بإحدى هاتين العقوبتين[١]، في حين تختص محكمة الجنايات بنظر الجرائم المعاقب عليها بالإعدام أو بالحبس المؤبد أو بالحبس المؤقت مدة تزيد على ثلاث سنوات[٢].

وللمحكمة أن تعفي من العقوبة كل من بادر من الجناة بإبلاغ السلطات المختصة بالجريمة قبل علمها بها وقبل البدء في تنفيذ الجريمة، فإن كان الإبلاغ بعد العلم بالجريمة وقبل البدء في التحقيق تعيّن للإعفاء من العقوبة أن يكون من شأن الإبلاغ ضبط باقي الجناة في حالة تعددهم[٣]. ويجوز الحكم بمصادرة الأجهزة أو البرامج أو الوسائل المستخدمة في ارتكاب أي من الجرائم المنصوص عليها في هذا القانون أو الأموال المتحصلة منها. ويجوز الحكم بإغلاق المحل أو الموقع الذي ارتكب فيه أي من هذه الجرائم إذا كان ارتكابها قد تم بعلم مالكها لمدة لا تزيد على سنة بحسب الأحوال، مع عدم الإخلال بحقوق الغير حسن النية أو بحق المضرور في التعويض المناسب . ويكون الحكم بإغلاق المحل أو الموقع وجوبياً إذا تكرر ارتكاب أياً من هذه الجرائم بعلم مالكها[٤] .ويلاحظ ان المصادرة جوازيه .

(١) مادة ٥ من قانون الجزاء
(٢) مادة ٣ من قانون الجزاء
(٣) مادة ١٢ من القانون رقم ٦٣ لسنة ٢٠١٥ في شأن مكافحة جرائم تقنية المعلومات
(٤) مادة ١٣ من القانون رقم ٦٣ لسنة ٢٠١٥ في شأن مكافحة جرائم تقنية المعلومات

ثانيا: المسئولية الجنائية في الجريمة التقنية الحديثة في التشريع السعودي

إن **الاستدلال هو** "مجموعة الإجراءات الأولية السابقة على تحريك الدعوى الجنائية والتس تستهدف التحري عن الجرائم والتثبت من وقوعها وجمع معلومات كافية بشأنها، وإثبات الآثار التي تولدت عنها على وجه يتيح لسلطة التحقيق التصرف في التهمة ، سواء بتحريك الدعوى الجنائية الناشئة عنها ، أو بحفظ أوراقها وصرف النظر عنها ، فهو إجمالا بمثابة إعداد العناصر الازمة للتحقيق في الجريمة "[١]. وعلى رجال الضبط الجنائي بحسب المهمات الموكلة إليهم وحسب اختصاصاتهم بأن يستقبلوا جميع البلاغات والشكاوى التي تردهم في الجرائم، ولقد حدد نظام الإجراءات الجزائية السعودي في المادة السادسة والعشرون رجال الضبط الذين خولهم النظام بالقيام بأعمال الضبط.[٢]

وعادة لا تظهر الجريمة حتى يتم الكشف عنها أمام جهات القضاء والشرطة، ، و أي إخبار أو بلاغ عن الجريمة لابد وأن يتضمن على الأقل معلومات أولية عن الجريمة مثل محل الجريمة ومكان وقوعها ونوعها ، ويتم الكشف عن الجرائم السيبرانية Cyber Crimes بوضع برمجيات حاسوبية معينة خصوصا فيما يخص جرائم القرصنة أو نشر المواد الإباحية. وللحصول على البيانات المتعلقة بارتكاب الجريمة من نظام الحاسب الآلي[٣] .

(١) د. محمد حميد المزمومي ، الوسيط في شرح نظام الإجراءات الجزائية السعودي ، مركز النشر العلمي بجامعة الملك عبد العزيز ، جدة ، الطبعة الثانية ، ٢٠١٩ ، ص ٩٨ .

(٢) روان بنت عطية الله الصحفي، الجرائم السيبرانية، المملكة العربية السعودية، المجلة الإلكترونية الشاملة متعددة التخصصات، العدد الرابع والعشرون، مايو ٢٠٢٠، ص. ٣٢

(٣) روان بنت عطية الله الصحفي، الجرائم السيبرانية، المملكة العربية السعودية، مرجع سابق، ص. ٣٤

وفي الواقع نادرا ما نجد شاهدا على وقائع الجريمة السيبرانية ، وذلك لعدة أسباب أهمها أن الجرائم السيبرانية Cyber Crimes تتطلب دراية كافية بالجوانب الفنية والتقنية للحاسب الآلي ، كما أن الجرائم التقنية ترتكب في هدوء أي أن الجاني يرتكبها وحده دون وجود أحد معه ، وكما انها لاتترك أي آثار خارجية يشهد بها أحد كما هو المعتاد في الجرائم التقليدية . وليس لمأمور الضبط الجنائي أن يأمر بإحضار متهم او شاهد ، بل له استدعاء من يشاء لسماع أقواله ، وإذا رفض الحضور فليس له إكراه في ذلك ، أو احضاره بمذكرة قبض ، لأن هذا من اختصاص النيابة العامة [١].

وتقوم النيابة العامة من ضبط الكيانات المعنوية السيبرانية باكتشافها من بعد ضبط الكيان المنطقي للحاسب الآلي مثل البرامج والفيروسات والبيانات والمعلومات المسروقة وكل المواد المعنوية التي تتعلق بالجريمة وتم ارتباطها بالحاسب الالي . وتعد حالة التلبس من الحالات التي يباح فيها مأمور الضبط الجنائي أن يتخذ إجراءات لم يكن باستطاعته مباشرتها في الظروف العادية وذلك مراعاة لظروف الاستعجال التي تتطلب كشف الحقيقة وجمع الأدلة. وكون حالة التلبس حالة استثنائية فقد منح لرجل الضبط الجنائي مجموعة من الإجراءات التي يجب عليه اتخاذها إذا توافرت حالة التلبس[٢] . وتكون بجمع الأدلة من المعاينة وندب الخبراء والتفتيش وضبط الأشياء ومراقبة المحادثات وتسجيلها وسماع الشهود والاستجواب والمواجهة ، ولا يلزم المحقق ترتيب معين عند مباشرة هذه الإجراءات .

المعـــاينـــة والمطابقة: على المحقق ضبط كل ماله علاقة بتلك الجرائم التقنية ، وإثبات حالة الأشخاص والأماكن والأشياء ذات الصلة بالجريمة ، وقد يكون إثبات

(١) خالد حسن أحمد لطفي، مرجع سابق ، ص ١٠٢ خالد حسن أحمد لطفي ، مرجع سابق ، ص ١٠٢.
(٢) خالد حسن أحمد لطفي مرجع سابق ، ص ١٠٨ .

المعاينة مع الجرائم السيبرانية Cyber Crimes أمرا صعبا للفترة الزمنية التي قد تطول ما بين وقوعها واكتشافها مما يؤدي بها إلى تلف البيانات أو نقلها أو إخفائها . وهنا نلاحظ بان المعاينة قد تكون إجراء تحقيق أو استدلال ، و لا تتوقف طبيعتها على صفة من يجريها ، بل على مدى ما يقتضيه إجراؤها من مساس بحقوق الأفراد وحرياتهم ، فإذا جرت المعاينة في مكان عام كانت إجراء استدلال ، وإذا اقتضت دخول مسكن أو مكان له حرمة خاصة كانت إجراء تحقيق[١] .

ندب الخبير وللمحقق أن يستعين بالخبراء المختصين لاستكمال إجراءات التحقيق ، وهذا بالفعل ما تتطلبه طبيعة الجرائم السيبرانية Cyber Crimes الذي تقتضي معرفة تامة بنظم الحاسبات و مهارة وتقنية فنية عالية تمكنهم من مباشرة التحقيق في مجال الجرائم السيبرانية Cyber Crimes .

التفتيش: وهو إجراء من إجراءات التحقيق التي تؤدي إلى ضبط أدلة الجريمة بعد اكتشافها، وللتفتيش شروط موضوعية تتعلق بسببه وقوع الجريمة بالفعل وأن يوجه اتهام إلى الشخص المراد تفتيشه والغاية منه من ضبط أشياء تفيد في كشف الحقيقة، وهناك ضرورة خاصة بأن يكون أمر التفتيش مسببا وذات علة محددة، ومحل التفتيش في الجرائم السيبرانية Cyber Crimes هو المكونات المادية للحاسب الآلي وكذلك البرامج أو الكيانات المنطقية وهي المكونات الغير مادية [٢].

والإثبات الجنائي هي تلك الأدلة الجنائية الرقمية التي تضاف إلى وسائل الإثبات، لإثباتها في المحاكمة الجنائية السيبرانية ، فالدليل الرقمي هو " الدليل المأخوذ من أي جهاز يعتمد في تشغيله على التقنية الرقمية ، وهو يكون في شكل مجموعة

(١) محمد حميد المزمومى، مرجع سابق ، ص ١٦٥.
(٢) خالد حسن أحمد لطفى ، مرجع ، ص١١٣.

المجـالات أو النبـضات المغناطيـسية أو الكهربائيـة التـي يمكـن تجميعهـا وتخليلهـا باسـتخدام بـرامج وتطبيقـات خاصـة لتظهـر فـي شـكل صـور أو تـسجيلات صـوتية أو مرئية[١].

كما تتميز الأدلة الجنائية التقنية بعدة مميزات لتكون حجة قوية في الإثبات أمام القضاء :

١ - يمكن استخراج نسخ منها مماثلة ومطابقة للأصل ولها ذات الحجية . كما يمكن بالأساليب العلمية الملائمة تحديد وتأكيد ما إذا كانت الأدلة الرقمية قد تعرضت لتعديل أو تحريف . ومن الصعب إتلاف الأدلة الجنائية الرقمية ، وفي حالة محوها أو إتلافها يمكن استرجاعها من ذاكرة الحاسوب

٢- إذا حاول المتهمون إتلاف الأدلة الرقمية يمكن الاحتفاظ بنسخ منها في أماكن عامة، علما بان للنسخ قيمة الأصل [٢].

ثالثا: المسئولية الجنائية في القانون التقني الغربي

يمكن التعرض للجوانب التشريعية المتعلقة بالمسئولية الجنائية التقنية في التشريعات الأجنبية المقارنة على النحو التالي:

١- المسئولية الجنائية التقنية في إنجلترا

استحدث المشرع الانجليزى عام ١٩٩٠ قانونا يعالج فيه إساءة استخدام نظم المعلومات وقد تم بموجب هذا التشريع تجريم عملية دخول أى فرد على البيانات

(١) خالد حسن أحمد لطفى مرجع سابق ، ص ١٢٨.
(٢) د. محمد الأمين البشري، مرجع سابق ، ص ٩٩

المختزنة بالحاسب الآلى أو البرامج وكذلك عملية تعديلها بصورة غير مشروعة أو أى محاولة لفعل ذلك [١]. وقد نص القانون على ثلاثة جرائم محددة وهى [٢]:

١ـ الدخول المتعمد غير المشروع:

Access is deliberate and unauthorized

٢ـ الدخول غير المشروع والذى يتم بنية ارتكاب العديد من الجرائم.

٣ـ قيام الفرد بأى فعل متعمد ينشأ عنه إجراء تعديل غير مشروع لمحتويات أجهزة الحاسوب الآلي.

ويلاحظ من صياغة هذا القانون ما يأتى:

أن المشرع الانجليزى يعاقب على التآمر والشروع والتحريض.

- لا تلزم جهة الادعاء أن تقدم دليل يستفاد منه أن الأفعال المقترفة قد استهدفت بيانات أو برامج معينة.

---

(١) راجع فى ذلك:

Rapport de Mr. Andre au nom de la commission delois constitu- tiannelles de LA legistation et de l" administration generale de la republique sur la Proposition de m.Godfrain relative a la fraude informatique no. 744.P. 13. DOC. Ass .nat(1986/87) lly aura acces Frauduleux des lorsqu on cherchera a sintrodiure indumenta dans un systeme prcetege par un disposetif de Securite.

(٢) وقد أدرج القانون بعضا لتعريفات الآتية:

- البيانات: هى تلك المعلومات الكائنة فى صيغة قابلة للمعالجة.
- البيانات الشخصية: هى البيانات المتعلقة بأفراد أحياء يمكن تحديد هويتهم.
- الأشخاص المسند إليهم العمل فى مجال البيانات: هم الأفراد المعينون بها.

- لم يشترط القانون المشار إليه سلفا تواجد المتهم وقت ارتكاب الجريمة ولا بيانات الحاسب الآلى المستهدفة فى بريطانيا.

وتنص المادة ١٦ من نفس القانون على أنه " يعاقب كل من حصل بطريق غير مشروع وبأى وسيلة خداع سواء لنفسه أو للغير على منفعة مالية"[١].

وقد قدر اتحاد الصناعات الإنجليزية الخسائر الناشئة عن الغش المعلوماتي بمبلغ يتراوح ما بين ٢٥ إلى ٣٠ مليون جنيه إسترليني في السنة. وتوضح الدراسة التي قام بها K. Wong على ٩٥ حالة غش معلوماتي أن متوسط الخسارة فيها بلغ ٣٠,٠٠٠ جنيها إسترلينياً. كما أبانت عن أن سرقة المعدات المادية ولاسيما "الحاسبات الآلية الميكروية" والحرائق العمدية والإتلاف لا تمثل كل منها سوي ٣٠% من الحالات محل الدراسة. ومع ذلك فإن خسائرها كانت مرتفعة جداً.

وبالنسبة لسرقة المعلومات والبرامج "وتمثل ١٥% من الحالات"، فهي تباشر بصفة أساسية عندما يحل المستخدمون محل الإجراء، وأن إتلاف التجهيزات غالباً ما يتسبب عنه الطاقم المسئول عن تشغيل وتخزين الدعائم الممغنطة، ولكن بالنسبة لإتلاف وظيفة النظام bombes logiques " ٨%" فهو من صنع المبرمجين أو أصحاب البرامج. ويمثل انتهاك الأنظمة المعلوماتية بغرض الحصول على معلومات أو خدمات مجانية نسبة تقدر بحوالي العشر، ولكن هذا النمط من الإجرام سيتضاعف بسبب انتشار الحاسبات الميكروية المنزلية[٢].

---

(١) انظر فى ذلك:

M. BRAIT,la fraude informatiqu.. une .Approche de droit compare REV. dr.pen.cirm.p.290.

(٢) راجع في ذلك:

=

٢- الميئولية الجنائية السيبرانية في فرنسا

استحدث القانون الفرنسى الصادر فى ٥ يناير ١٩٨٨ بموجب المادة ٢/٤٦٢ عقوبات، جريمة الولوج غير المشروع فى نظم المعلومات والتى تنص على" يعاقب .... كل من ولج أو تواجد بطريق الغش فى كل أو جزء من نظام مبرمج للبيانات". وتشدد العقوبة إذا ما ترتب على ذلك إلغاء أو تعديل للبيانات التى يحتويها النظام أو إتلاف لوظيفة هذا النظام".

ويستهدف هذا النص فى المقام الأول حماية الولوج فى نظم المعلومات لا حماية حق الملكية ذاته وهو بذلك سد فراغا تشريعيا هائلا فى القانون الفرنسى، ومن جهة أخرى استجاب لرغبة ملاك الأنظمة المعلوماتية [١].

وتفترض هذه الجريمة توافر عنصرين أحدهما مادى والآخر معنوى.

أ- **العنصر المادى:** يتحقق العنصر المادى لهذه الجريمة بمجرد شروع أى شخص- ليس له الحق – فى الدخول، أو تدخل بالفعل فى نظام مبرمج للبيانات. ولكن هل يشترط لنشوء الجريمة أن يكون النظام محميا بواسطة جهاز أمن dispositif de securite! تمسك مجلس الشيوخ الفرنسى بهذا الشرط، وحجته فى ذلك جذب انتباه أصحاب الأنظمة إلى هذه النقطة الأساسية كى يدعموا أنظمتهم بأجهزة الأمن [٢].

=

Christakis, Nicholas A. Fowler, James H. (January 12, 2011), Connected: The Surprising Power of Our Social Networks and How They Shape Our Lives - How Your Friends' Friends' Friends Affect Everything You Feel, Think, and Do, USA: Back Bay Books; Reprint edition

(١) راجع فى ذلك:

J.P.Buffelan,art.Prec.P.99.

(٢) راجع فى ذلك:

=

بينما رأت الجمعية الوطنية الفرنسية، أنه من غير المناسب التمسك بهذا الشرط، لأنه سوف يترتب عليه قصر الحماية الجنائية على الأنظمة المحمية بواسطة أجهزة الأمن ومن ثم يستبعد من مجال تطبيق النص أفعال الولوج التى ترتكب ضد الأنظمة المفتوحة للعامة [١] كالدليل الالكتروني أو الخدمات التى تقدم على رقم ٣٦-١٥. وكتب لهذا الرأي الأخير النجاح، وتم التصويت على النص بدون حاجة إلى اقتضاء هذا الشرط.

ويتحقق التواجد غير المشروع، بمجرد علم الشخص بأنه تدخل بمحض الصدفة أو عن طريق الخطأ- وعلى نحو غير مشروع – فى نظام مبرمج للبيانات، ويستمر فى حال الاتصال به بدلا من الانفصال عنه فى الحال.

وهذه جريمة من جرائم الامتناع التى يصعب تقديم دليل أثبات فيها حيث يزعم المتهم دائما حال القبض عليه أنه كان على وشك الانفصال عن النظام المعتدى عليه [٢] ويستوى أن يكون الولوج فى النظام المعتدى عليه كليا أو جزئيا حيث يستطيع المعتدى فى حالة التدخل المقترن بالغش، أن يدعى بسهولة بأن تحوله كان محدودا بجزء ضيق جداً من النظام، ولا يمكن التحقق من مثل هذا الإدعاء من الناحية العلمية[٣].

=

J.Pradel,art prec,P.827, Lucas de leyssac, OP.CIT.P.21.

(١) انظر:

Rapport de r.Andre, Assemble Nationale,no.1078 "1987, 1988"P.5.

(٢) راجع فى ذلك:

J.P.Buffelan,art. Prec,P.100.

(٣) راجع فى ذلك:

F.Chamoux ,art prec ,H..Croze ,ART,PREC V. ROULET ,art prec.

ب-لعنصر المعنوى:

يجب أن يتوافر لدى الفاعل قصد خلاص علاوة على القصد العام " أى اتيان الفعل غير المشروع عن علم وإرادة". والذى يتمثل فى نية الغش Fraudulcuscmcnt. ويقصد بالغش أن يباشر الفاعل سلوكه عن طريق الخديعة وبسوء نية وبغرض خداع الغير (١).

ويتمثل قصد الغش فى معرفة المتهم بأنه قد ولج أو تواجد فى نظام البيانات المبرمج ضد رغبة صاحب النظام وأيا كان الدافع إلى ذلك.

وقد ارتفع معدل الخسائر الناتجة عن المعلوماتية في فرنسا حيث بلغت وفقاً لإحصاء الجمعية العمومية لشركات التأمين ضد الحرائق والمخاطر المختلفة APSAIRO حوالي ٧,٣ مليار فرنك فرنسي، ويرجع ٤٦% منها إلى الأفعال الإجرامية و ٣٠% إلى المخاطر العارضة و٢٤% إلى الأخطاء. ويتبين من تحليل الخسائر المرتبطة بجرائم المعلومات في فرنسا أن ٦٠% منها يتعلق بالبرامج، ويتركز الغش في معظم هذه الحالات في اتفاقات غير مشروعة (٣٥%) واستغلال الأعطال القائمة ١٠% وتضليل البرامج ٩% ومن ناحية التشغيل فإن ٢٥% من الخسائر ترجع إلى تعديل الإجراءات والملفات والسهو المتعمد ونقل البيانات.

وقد تضاعفت خسائر سرقة البرامج المنطقية ذو النمط الواحد وفقاً لتقدير وكالة حماية البرامج لتصل إلى ١,١٢ مليار فرنك ويرجع ٤٣% من هذه الخسائر إلى سرقة أدوات البرامج المنطقة ذو النمط الواحد "كبرامج الفائدة الخاصة بالتصنيف والمعاونة في

(١) أنظر فى ذلك:

Lucas de Leyssac,OP.CIT.,P.20.

تصميم برامج وإدارات البيانات والأمن وصيانة البرامج، و ٣٠% للبرامج المنطقية التطبيقية ذو النمط الواحد الخاصة بالسداد والمحاسبة وإدارة الوثائق، ١٧% للبرامج المنطقية الأساسية ذو النمط الواحد الخاصة بأنظمة التشغيل، وقدرت خسائر الألعاب بحوالي ١٠%. ويشهد معدل الخسائر في مجال صفقات الإنتاج وشركات الخدمات والمنشآت الناشرة للبرامج ارتفاعاً ملحوظاً حيث وصلت الخسائر إلى ١٩% في عام ١٩٨٥، ٥٠% منها للحاسب الآلي الميكروي، ١١% للأنظمة المتوسطة والكبيرة[١].

(١) انظر في ذلك

Christakis, Nicholas A. Fowler, James H. (January 12, 2011), Connected: The Surprising Power of Our Social Networks and How They Shape Our Lives - How Your Friends' Friends' Friends Affect Everything You Feel, Think, and DoOp, Cit

المبحث الثالث

آليات تعاطي المجتمع الدولي مع المسئولية الجنائية للجرائم السيبرانية

لقد أدى انتشار الجرائم السيبرانية Cyber Crimes الى البحث عن آليات فاعلة لتحديد المسئولية الجنائية وكذلك الأركان المرتبطة لتلك الجرائم المستحدثة وهو ما تبين من خلال المحاور التالية:

أولا: معاهدة بودابست لمكافحة الجرائم السيبرانية Cyber Crimes

تُعد معاهدة بودابست لمكافحة جرائم الإنترنت أولى المعاهدات المتعلقة بتلك الجرائم، والتي تمت فى العاصمة المجرية بودابست فى ٢٠٠١/١١/٢٣، والتي تبرز التعاون والتضامن الدولي في محاربة الجرائم السيبرانية Cyber Crimes، ويُعد التوقيع على تلك المعاهدة الدولية الخطوة الأولى فى مجال تكوين التضامن الدولي ضد تلك الجرائم التي تتم عبر شبكة الإنترنت والاستخدام السيء لها(١).

وقد وقعت على تلك المعاهدة ٢٦ دولة أوروبية بالإضافة إلى كندا واليابان، وجنوب أفريقيا والولايات المتحدة الأمريكية، وتُوفّر المعاهدة أسس الأمن العام. وعلى الرغم من أنّ هذه الاتفاقية أوروبية المنشأ، إلا أنها مفتوحة للدول الأخرى لطلب الانضمام إليها لتعم الفائدة. وتتضمن الاتفاقية التعاون والعمل المشترك ما بين الدول

(١) د. منير محمد الجهيني، د. ممدوح محمد الجهيني، جرائم الإنترنت والحاسب الآلي ووسائل مكافحتها، دار الفكر العربي الإسكندرية، ط ٢٠٠٤ ، ص: ٩٦ .

الأعضاء وأعضاء القطاعات وأصحاب المصلحة ذوي الصلة، وهما ضروريان لبناء ثقافة للأمن السيبراني وفي الحفاظ عليها، وسبل مكافحة الجرائم السيبرانية Cyber Crimes، إذ تقرر(١):

١- مواصلة اعتبار الأمن السيبراني فى صدارة أنشطة الاتحاد ذات الأولوية والاستمرار في إطار مجالات اختصاصاته الرئيسية بدراسة مسألة توفير الأمن وبناء الثقة فى استعمال الاتصالات تكنولوجيا المعلومات والاتصالات؛ من خلال إذكاء الوعي، وتحديد أفضل الممارسات وتطوير مواد التدريس المناسبة لتعزيز ثقافة الأمن الإلكتروني.

٢- تعزيز العمل والتعاون وتبادل المعلومات مع جميع المنظمات الدولية والإقليمية ذات الصلة فيما يتعلّق بالمبادرات المتصلة بالأمن السيبراني في مجالات اختصاصاتها، مع مراعاة احتياجات مساعدة البلدان النامية.

٣- تعيين نظام سريع وفعّال للتعاون الدولي، والحفاظ بشكل سريع على البيانات المخزنة على أجهزة الحاسوب الآلي وحفظها والإفصاح الجزئي عن حركة هذه البيانات المخزنة على الحاسوب الآلي(١) .

(١) وتعود أهمية توقيع هذه الاتفاقية إلى رغبة المجتمع الدولي لإيجاد صيغة دولية لمكافحة ومواجهة هذا الإجرام المستحدث وعلى ذلك بذلت الجهود الدولية لتحقيق هذه الرغبة، فبتاريخ ٢٠ نوفمبر تقدمت اللجنة الأوروبية لمشكلات الجريمة CDBC ولجنة الخبراء في حقل جرائم التقنية (-CU-PC -CYBERCRIME)) بمشروع اتفاقية جرائم الكمبيوتر، وخضعت مواد الاتفاقية المقترحة للمناقشة وتبادل الآراء خلال الفترة من إصدار مشروعها الأول وحتى إعداد مسودتها النهائية التي أقرت لاحقا في بودابست ٢٠٠١، وتعرف باتفاقية بودابست ٢٠٠١) اتفاقية الجرائم السيبرانية - سايبر كرايم) ، ولا شك في أن الاتفاقية قد بذل فيها جهد واسع ومميز يذكر للاتحاد الأوروبي ومجلس أوروبا ولا سيما في المسائل المتعلقة بجرائم الكمبيوتر وأغراضها منذ أواخر القرن الواحد والعشرين. للمزيد انظر: د. هلالي عبد اللاه أحمد، اتفاقية بودابست لمكافحة جرائم المعلوماتية (معقبا عليها) ، دار النهضة العربية ، ط ٢ ، ٢٠١١

هذا وقد تناولت المعاهدة الجرائم التي تُعتبر من أكثر الجرائم شيوعًا على مستوى العالم مثل الإرهاب السيبراني وعمليات تزوير بطاقات الائتمان ودعارة الأطفال. كما حددت المعاهدة الطرق الواجب اتباعها فى التحقيق في جرائم الإنترنت، وتعهدت الدول الموقعة بالتعاون من أجل محاربتها، كما حاولت المعاهدة إقامة التوازن بين الاقتراحات التي تقدمت بها أجهزة الشرطة، وما عبرت عنه المنظمات المدافعة عن حقوق الإنسان ومزودي خدمات الإنترنت من قلق، حيث تخشى منظمات حقوق الإنسان من أن تحدّ المعاهدة من حرية الأفراد، وأن تُؤدِّي الرقابة إلى انتهاك حقوق مستخدمي الإنترنت [٢].

وفي عام ٢٠١٦ أصدرت لجنة اتفاقية الجرائم السيبرانية Cyber Crimes مذكرة توجيهية تتعلّق بجوانب الإرهاب السيبراني بموجب اتفاقية بودابست، تُعلن فيها أنّ «الجرائم الموضوعية في الاتفاقية قد تكون أيضًا أعمالا إرهابية على النحو المحدد في القانون المعمول به « . وجاءت هذه المذكرة الإضافية بموجب الاتفاقية في الوقت المناسب؛ لتُسلّط المذكرة الضوء على أنّ هذه الاتفاقية ليست معاهدة مختصة بالإرهاب، إلا إنّه يمكن القول: أنّ الجرائم الموضوعية في الاتفاقية يمكن أن تُنفّذ على أنّها أعمال إرهابية، لتسهيل الإرهاب ولدعم الإرهاب، ومن ذلك الجانب التمويلي، أو الأعمال التحضيرية[٣] .

=

(١) هاني محمد العزازي، النظام القانوني الدولي لمكافحة المخاطر السيبرانية، مجلة مصر المعاصرة، القاهرة، العدد رقم ٥٤٩، يناير ٢٠٢٣، ص. ٥٠٧

(٢) د. هلالي عبد اللاه أحمد ، الجوانب الموضوعية والإجرائية للجرائم المعلوماتية، المرجع السابق، ص: ٣٠ وما بعدها.

(٣) د. منير محمد الجهيني ، د . ممدوح محمد الجهيني، جرائم الإنترنت والحاسب الآلي ووسائل مكافحتها ، المرجع السابق، ص: ٩٦.

ثانيا: التوصيات التشريعية المجلس الأوروبي تجاه الجرائم السيبرانية Cyber Crimes[١]

من أهم ما ورد بتوصية المجلس الأوروبي ما يلي:[٢]

١- أهمية استجلاء التشريعات المرتبطة بإجراءات تفتيش أجهزة الحاسب الآلي وضبط المعلومات التي تحويها ومراقبة المعلومات أثناء انتقالها.

٢- أن تسمح الإجراءات الجنائية الوطنية لجهات التفتيش بضبط برامج الحاسوب الآلي والمعلومات الموجودة بالأجهزة وفقا لذات الشروط الخاصة بإجراءات التفتيش العادية، ويتعين إخطار الشخص القائم على الأجهزة بأنّ النظام كان محلا للتفتيش مع بيان المعلومات التي تم ضبطها، ويُسمح باتخاذ إجراءات الطعن العادية في قرارات الضبط والتفتيش.

٣- أن يُسمح أثناء عملية التفتيش للجهات القائمة بالتنفيذ ومع احترام الضمانات المقرّرة بمد التفتيش إلى أنظمة الحاسوب الآلي الأخرى في دائرة اختصاصهم، والتي تكون متصلة بالنظام محل التفتيش وضبط ما بها من معلومات، بشرط أن يكون هذا الإجراء ضروريًا. كما أنه يتعين على العاملين بالمؤسسات الحكومية والخاصة التي توفر خدمات الاتصال بالتعاون مع سلطة التحقيق لإجراء المراقبة والتسجيل.

(١) د. مدحت رمضان، جرائم الاعتداء على الأشخاص والإنترنت، دار النهضة العربية، ط ٢٠٠٠، ص: ٨٠ وما بعدها.

(٢) هاني محمد العزازي، النظام القانوني الدولي لمكافحة المخاطر السيبرانية، مرجع سابق،ص. ٥١١

٤- هناك أهمية كبيرة لمنح سُلطات التحقيق صلاحيات كبيرة لإصدار أوامر لمن يكون لديه معلومات خاصّة للدخول على نظام من أنظمة المعلومات أو الدخول على ما يحويه من معلومات باتخاذ اللازم؛ للسماح لرجال التحقيق بالاطلاع عليها . وأن تخول سلطات التحقيق بإصدار أوامر مماثلة لأي شخص لديه معلومات عن طريق التشغيل والمحافظة على المعلومات.

ثالثا: السياسات الجنائية للاتحاد الدولي للاتصالات

من المهام التي يضطلع بها الإتحاد تعزيز التعاون الدولي للخدمات الهاتفية والسلكية واللاسلكية وتوسيع استخدامها بواسطة الجمهور وتطوير إمكانات الاتصالات السلكية واللاسلكية، وتوزيع الموجات اللاسلكية، ويعمل الاتحاد بصورة وثيقة مع المنظمات الأخرى المعنية على (وضع المعايير المتعلقة بالأمن المعلوماتي؛ إذ يقوم الاتحاد بالاشتراك مع الوكالة الأوروبية لأمن الشبكات والمعلومات بنشر خريطة الطريق المتعلقة بمعايير الأمن فى مجال تكنولوجيا المعلومات والاتصالات، كما تعاون الاتحاد الدولي مع مجلس أوروبا لإنجاز الاتفاقية الأوروبية حول الجريمة الإلكترونية؛ من أجل الاستعانة بها في عملية وضع إطار قانوني دولي[١].

وبغية معالجة مسألة الأمن السيبراني المتنامية، قام الاتحاد الدولي للاتصالات بإنشاء فريق متخصص معني بالشبكات الإلكترونية؛ من أجل جمع وتوثيق المعلومات والمفاهيم التي ستكون مفيدة من أجل إعداد توصيات لدعم تلك الشبكات من منظور

(١) د. خالد محمد نور عبد الحميد الطباخ المواجهة القانونية للإرهاب الإلكتروني الدولي، مجلة الدراسات القانونية والاقتصادية، جامعة مدينة السادات - كلية الحقوق، مج ٣، ١٦ ، ٢٠١٧، ص: ٣٣.

الاتصالات[١] ، وكان أحد الأدوار الأساسية التي أنيطت بالاتحاد الدولي للاتصالات في أعقاب القمة العالمية لمجتمع المعلومات ومؤتمر المندوبين المفوضين لعام ٢٠٠٦ يتمثل في بناء الثقة والأمن فى استعمال تكنولوجيا المعلومات والاتصالات؛ فقد قام رؤساء الدول والحكومات وغيرهم من قادة العالم المشاركين في القمة العالمية لمجتمع المعلومات، وكذلك الدول الأعضاء في الاتحاد ، بتكليف الاتحاد باتخاذ خطوات ملموسة للحد من التهديدات وانعدام الأمن فيما يتصل بمجتمع المعلومات، ولتحقيق هذه الولاية أطلق الأمين العام للاتحاد برنامج الأمن السيبراني العالمي في عام ٢٠٠٧؛ ليكون إطارا للتعاون الدولي[٢].

وهكذا أعلن الأمين العام للاتحاد الدولي للاتصالات عام ٢٠٠٧ إطلاق مبادرة أجندة شاملة بشأن الأمن السيبراني، تتضمن التوصل إلى إطار أو بروتوكول لتنسيق جهود مكافحة الجرائم السيبرانية Cyber Crimes، وبما يشمل تدابير قانونية، وتقنية، وإجرائية وتنظيمية، وتعاون دولي[٣]. وتنصُّ هذه المبادئ على ما يلي[٤] .

(١) الفرق المتخصصة : هي أداة من أدوات الاتحاد التي تُعزّز برنامج عمل لجان الدراسات من خلال توفير بيئة عمل بديلة لتطوير المواصفات بسرعة في مجالات عملها، مما يجعلها مثالية للتكنولوجيات المتغيرة والمتطورة بسرعة مثل الشبكات الذكية، ويتألف الفريق المتخصص بالشبكة الذكية من ممثلين من مختلف الدول الأعضاء، وسيقوم بالتعاون مع مجتمعات الشبكة الذكية في جميع أنحاء العالم (مثل: معاهد البحوث والمنديات والأوساط الأكاديمية).

(٢) د. أميرة عبد العظيم محمد عبد الجواد ، المخاطر السيبرانية وسبل مواجهتها في القانون الدولي العام، المرجع السابق، ص: ٤٩٣ .

(٣) د. محمد عادل محمد عسكر، وضع العمليات السيبرانية في القانون الدولي مع التطبيق على ممارسة التجسس وقت السلم، دراسة على ضوء دليل تالين » بشأن القانون الدولي المطبق على العمليات السيبرانية ٢٠١٧-٢٠١٣ ، ٢٠٢٠م، ص: ٣٠٨.

(٤) قرارات المؤتمر العالمي لتنمية الاتصالات لعام ٢٠١٧ (wtdc١٧) المرفوعة إلى عناية مؤتمر المندوبين المفوضين، مؤتمر المندوبين المفوضين (١٨ -pp) دبي ، ٢٩ اكتوبر - ١٦ نوفمبر ٢٠١٨ ، الاتحاد الدولي للاتصالات.

١- أهمية اتاحة الخدمات التقنية والرقمية لكافة المواطنين.

٢- الحاجة لتحقيق الأمن الرقمي للشعوب وعدم تمكين الارهابيين من الاستيلاء والقرصنة على مواقع الانترنت الحكومية.

٤- أن يلتزم كلُ بلد بألا يكون الطرف الذي يبدأ شنّ هجوم سيبراني على غيره من البلدان.

٥- أن يلتزم كل بلد بالتعاون مع غيره ضمن إطار دولي للتعاون لضمان السلام في الفضاء السيبراني[١].

رابعا: السياسات الجنائية للمنظمة العالمية للملكية الفكرية

إبان عام ١٩٦٧ تم التوقيع في ستوكهولم بالسويد على اتفاقية المنظمة العالمية للملكية الفكرية، وأصبحت هذه المنظمة إحدى الوكالات المتخصصة التابعة للأمم المتحدة اعتبارًا من السابع عشر من ديسمبر عام ١٩٧٤، والتي من أهدافها حماية الملكية الفكرية في شتّى أنحاء العالم عن طريق التعاون بين الدول الأعضاء والمنظمات الدولية الأخرى، وتعمل المنظمة على متابعة تنفيذ الاتفاقيات المتعلقة بالتصميمات الصناعية وتصنيف السلع التجارية وحماية الأعمال الإدارية والفنية وحقوق الإنتاج. كما تشجع المنظمة كذلك على توقيع معاهدات دولية جديدة، وتقوم بالتنسيق بين التشريعات الوطنية، وتقديم المساعدات القانونية والفنية للدول النامية؛ بهدف حماية الملكية الفكرية وتنميتها وتغطية بعض أوجه القصور في مجال التوثيق العلمي ونقل التقنية الحديثة[٢].

(١) هاني محمد العزازي، النظام القانوني الدولي لمكافحة المخاطر السيبرانية، مرجع سابق،ص.٥١٦

(٢) د. طارق عزت رخا، المنظمات الدولية المعاصرة، دار النهضة العربية، القاهرة، ٢٠٠٦ ، ص: ٢١٤.

خامسا: السياسات الحنائية لمنظمة حلف شمال الأطلسي

لقد نفّذت الناتو السياسة الخاصة بها فى مجال الدفاع السيبراني في ٢٠٠٨؛ من أجل حماية مواردها التكنولوجية وتلك الخاصة بالدول الأعضاء[١]، وكجزء من هذه السياسة، أنشأ الحلف هيئة معيّنة بإدارة الدفاع السيبراني، وفريقًا للاستجابة للحوادث الحاسوبية، يكفل إرسال فِرق الدعم السريع إلى فرادى البلدان الأعضاء، ومركزا للتميز من أجل الدفاع السيبراني التعاوني[٢]، ويضم هذا المركز الذي يُوجد مقره في إستونيا خبراء يضطلعون بالبحث والتدريب في مجال الأمن السيبراني. وتضم البلدان التي ترعى هذا المركز : إستونيا ولاتفيا وليتوانيا وألمانيا وإيطاليا والجمهورية السلوفاكية وإسبانيا [٣]. ووقعت الناتو مذكرة تفاهم بشأن الأمن السيبراني مع إستونيا والولايات المتحدة الأمريكية والمملكة المتحدة وتركيا وسلوفاكيا [٤].

سادسا: السياسات التشريعية لدليل تالين تجاه الجريمة السيبرانية

تبنى (NATO) إعداد دليل «تالين»، بشأن القانون الدولي المطبق على الحرب السيبرانية، بإصداريه لعامي ٢٠١٣، ٢٠١٧، وهو توجيه غير ملزم بشأن القواعد الدولية التي تحكم العمليات السيبرانية، حيث استضاف المركز التعاوني للدفاع السيبراني، التابع للحلف بمقره فى مدينة « تالين» عاصمة » إستونيا »، وصياغة هذا الدليل فى الفترة من

---

(١) الدفاع ضد الهجمات السيبرانية ، الناتو
https://www.nato.int/cps/en/natohq/

(٢) انظر: https://www.nato.int/cps/en/natolive/official_texts

(٣) مركز التميز للدفاع السيبراني التعاوني WWW.ccdcoe.org

(٤) أبرمت الناتو وإستونيا اتفاقا بشأن الدفاع السيبراني nato-news ، أبريل ٢٠١٠
https://www.nato.int/cps/en/natolive/news_62894.htm

عـام ٢٠٠٩ وحتـى ٢٠١٧ ، بجهـود فريـق خبـراء قـانونيين دوليـين (IGE) برئاسـة البروفيسور « Michael N.Schmitt) [١].

وقـد عـرّف خُبـراء تـالين العمليـات الـسيبرانية علـى أنّهـا: «تلـك التـي تتـضمن استخدام القوة أو التهديد بهـا ضـد سـلامة الأراضـي أو الاسـتقلال السياسي لأي دولـة، أو على وجه آخر لا يتفق ومقاصد الأمم المتحدة » [٢] ؛ وذكروا أن العملية السيبرانية تُشكّل استخدامًا للقوّة عندما يكون حجمها وأثرها قابلا للمقارنة مع العمليات غير السيبرانية التـي تصل لمستوى استخدام القوة[٣].

وقد ظهر الإصدار الأوّل من الدليل عام ٢٠١٣ ، وتضمّن (٩٥) قاعدة لسلوك الدول في سياق الحرب السيبرانية، مع تعليقات على كل قاعدة، وفي عام ٢٠١٧ ظهر الإصدار الثاني، وتضمّن (١٥٤) قاعدة، تشكل مستوى أكثر عمقا بشأن معالجة العمليات السيبرانية، مع تعليقات على كل قاعدة، تُبين النقاش الذي دار بشأنها ، وأنّ أي وجهة نظر قبلت بالأغلبية، وموقف الأقلية إن وجد، وكذلك حالات الإجماع. وانتهى الدليل إلى أنّ القواعد الدولية السارية فاعلة إلى حدٍّ كبير، ويمكن تطبيقها على العمليات السيبرانية، وتعرّض الدليل لبعض الإشكاليات القانونية في المجال السيبراني، كسيادة الدول، وقواعد ممارسة الاختصاص، وقانون مسئولية الدول، إضافة إلى قانون حقوق الإنسان، وقانون البحار، والقانون الدبلوماسي والقنصلي[٤].

---

(١) د. محمد عادل محمد عسكر، وضع العمليات السيبرانية في القانون الدولي مع التطبيق على ممارسة وقت السلم، المرجع السابق، ص: ٦٩.

(٢) القاعدة (١٠) من دليل تالين والمعنونة ب حظر التهديد أو استخدام القوة .

Tallinn Mnnual on the International Law Applicable to Cyber Warfare (Michael N. Schmitt ed., 2013) , pp. 106-107.

(٣) القاعدة (١١) من دليل تالين والمعنونة بـ تعريف استخدام القوة ..

(٤) د. محمد عادل محمد عسكر ، وضع العمليات السيبرانية في القانون الدولي مع التطبيق على ممارسة التجسس وقت السلم المرجع السابق، ص: ٧٠.

ووفقا لدليل تالين فإنّ العمليات السيبرانية تُعتبر استخدامًا للقوّة عندما يكون مستواها وتأثيرها متقاربين مع العمليات غير السيبرانية، وذلك اعتمادًا على معيار النطاق والأثر فى تحديد الدرجة التي يجب أن يصل إليها الهجوم السيبراني كاستخدام للقوّة أو هجوم مسلّح، وعليه يمكن اعتبار هجوم سيراني كهجوم مسلح إذا أحدث ضررًا، أو يصل إلى درجة الشدّة ، والمقصود بذلك أن يُحدث أضرارا مادية جسيمة، واستند خبراء تالين فى اعتماد هذا الاختبار على رأي محكمة العدل الدولية في قضية « نيكاراجوا » ، على أساس أنّه الأنسب لتحديد الدرجة المناسبة للأعمال التي تصل إلى حد استخدام القوّة والهجمات المسلّحة، وبالقياس على الهجمات السيبرانية، اتّفَق خبراء دليل تالين في الإصدار الثاني، على أنّ قيام دولة بتزويد قوات أو أفراد بأجهزة وتدريبهم لشن هجمات سيبرانية ضد دولة أخرى يُعدُّ ذلك استخدامًا غير مشروع للقوة(١).

وطبق هذا المعنى بصورة واضحة فى عملية استخدام الهجمات السيبرانية في الحرب بين جورجيا وروسيا فى أغسطس ٢٠٠٨ ، وفي الهجمة السيبرانية العالمية - فيروس الفدية - التي طالت أكثر من ٦٠ دولة على مستوى العالم في ٢٧ يونيو ٢٠١٧ منهم بريطانيا ومصر وروسيا وأوكرانيا وألمانيا والمكسيك وإسبانيا، إلى ظهور الفضاء السيبراني على الساحة الدولية على نحو مباشر وعلني فى الصراع الدولي، وكأداة ووسيلة في الصراع المسلّح، لذلك ثار الجدل حول مدى اعتبار تلك الهجمات عملا من أعمال الحرب، وتُقارب الهجمات السيبرانية الهجمات التقليدية في النتائج مع اختلاف الوسائل وإستراتيجيات التنفيذ، مما أدى إلى خلق حرب مفتوحة يمكن أن تكون هناك

(١) انظر:

Michael N. Schmitt, "Peacetime Cyber Responses and wartime Cyber Operations inder International Law: An Analytical Vade Mecum", Harvard National Security Journal, Vol.8, 2017, p.245.

صعوبة فى تحديد أطرافها، لذا تسعى الدول إلى تطوير أساليب جديدة في الحروب المستقبلية. وقد وضعت اللجنة مجموعة من الصفات التي يجب أن تتسم بها الهجمات السيبرانية؛ حتى ترقى إلى درجة الهجوم المسلح ، وبالتالي تعطي الدولة المعتدى عليها حق الدفاع الشرعي وتفعيل المادة ٥١ من الميثاق[١]:

وتجدر الإشارة إلى أنّ هذا الدليل ليس صكًا دوليًا رسميًا أو مُلزمًا، أو يُمثل وجهة نظر (NATO)، أو الدول التي شارك خبراء من جنسيتها في وضع الدليل، وإنّما هو رؤية الخبراء المستقلين الذين صاغوه بصفاتهم الشخصية، ومع ذلك، فإنّ أهميّته كبيرة، كوثيقة رائدة في مجال العمليات السيبرانية، وخطوة مهمة لتنظيم الفضاء السيبراني [٢].

(١) هاني محمد العزازي، النظام القانوني الدولي لمكافحة المخاطر السيبرانية، مرجع سابق،ص.٥٢١

(٢) د. محمد عادل محمد عسكر، وضع العمليات السيبرانية في القانون الدولي مع التطبيق على ممارسة التجسس وقت السلم، المرجع السابق، ص: ٧٠.

خاتمة الدراسة

في ختام هذه الدراسة، يمكن القول أن الجرائم السيبرانية Cyber Crimes هى نمط مستحدث من الجرائم والذي تطلب تفاعل النظم التشريعية المحلية والدولية معه خاصة أن تلك الجرائم تزداد في الإنتشار يوما بعد الآخر وذلك في ظل التوسع الهائل في تطبيقات الإنترنت وتمكن الجميع من استخدام تلك التقنيات الامر الذي تطلب التعاطي التشريعي مع مبادىء المسئولية الجنائية لتلك الجرائم السيبرانية Cyber Crimes.

ولقد أصبحت التكنولوجيا هي المسيطر الرئيسي عليه، وأمام التطور الهائل والسريع الذي يشهده العالم في هذا المجال أصبحنا اليوم نقف أمام حقيقة أن التكنولوجيا في مقابل أنها أسهمت كثيرا في تطوير الحياة وتسهيلها وخلقت الكثير من الجوانب الإيجابية في جميع المجالات إلا أن هذا لا يمنع من وجود الكثير من الجوانب السلبية والمظلمة لهذه التكنولوجيا التي أصبحت تتطور وتظهر أكثر مع اقتحام الذكاء الاصطناعي لمختلف جوانب الحياة من أبسطها إلى أكثرها تعقيدا وازداد الأمر سوءا مع ظهور الروبوتات الإلكترونية التي أصبحت تعمل وفق خوارزميات الذكاء الاصطناعي وتنافس الإنسان في الكثير من المهام والوظائف اليومية وتقوم بها بسرعة وأكثر دقة وصلت إلى درجة إقدام هذه الروبوتات على القيام بالجرائم السيبرانية Cyber Crimes دون أي تدخل إنساني مما خلق الكثير من التخوف لدى المختصين من خروج هذه الروبوتات الإلكترونية عن السيطرة، وهذا ما طرح الكثير من الإشكاليات على الساحة القانونية على رأسها إشكالية المسؤولية القانونية لها ودورها في الحد من مخاطر ارتكاب هذه الروبوتات للجرائم السيبرانية، وهو الأمر الذي أصبح يفرض استحداث نصوص قانونية تعترف بالشخصية القانونية للروبوتات الإلكترونية وفق الخصائص التي تتمتع

بها، وتعمل هذه المسؤولية على الحد من خطر ارتكابها للجرائم السيبرانية ضد الأفراد والمؤسسات وحتى الدول سواء العربية أو الغربية.

نتائج الدراسة

أولا: من المشكلات التي ظهرت على الساحة التشريعية هي فكرة المسؤولية القانونية للجرائم ذات البعد التكنولولجي والقادرة على القيام بالأخطاء وارتكاب الجرائم والإضرار بالغير دون أي تدخل من المستعمل أو المبرمج.

ثانيا: بالرغم من كل الخلافات القائمة بشأن فكرة الشخصية القانونية وقيام المسؤولية القانونية للجرائم السيبرانية إلا أن أغلب التوجهات التشريعية في العالم تسير نحو ضرورة النظر جديا في الطبيعة الخاصة للتطبيقات التقنية الإلكترونية والعمل على منحها شخصية قانونية بما يتماشى وطبيعتها القانونية وبالتالي وضعها أمام حقيقة المساءلة القانونية تجنبا لأي فراغ قانوني في هذا المجال من شأنها المساس بسلامة الأفراد وحتى الدول.

ثالثا: إن الفضاء الرقمي أصبح واقعا علميا ، ذا تأثيرات اجتماعية وسياسية واقتصادية، وتبدو الحاجة واضحة إلى آليات شاملة للأمن السيبراني، عن ضمان أمن شبكات اتصالاتها وبنيتها التحتية، واعتماد المعايير والمقاييس الدولية الخاصة بالحماية والأمن المعلوماتي، وأصبح ساحة جديدة للصراع بشكله التقليدي، ولكنّه ذو طابع إلكتروني يعكس النزاعات التي تخوضها الدول أو الفاعلون من غير الدول على خلفيات دينية أو عِرقية أو أيدلوجية أو اقتصادية أو سياسية، ويتمدد الصراع الإلكتروني بداخل شبكات الاتصالات والمعلومات متجاوزا الحدود التقليدية وسيادة الدول.

رابعا: إنّ الهجوم التقني وقت السلم من الأمور التي يُوجد اختلاف حولها، من خلال تحليل المبادئ العامة للقانون الدولي العام نجد أنّ للدولة التي تعرضت للهجوم السيبراني إذا كانت آثاره تُشبه آثار الهجوم المسلّح يكون لها حق الدفاع عن النفس، سواء أكان بهجمة سيبرانية أم بهجوم مسلح.

خامسا: إنّ هناك جهودًا دولية وإقليمية لمكافحة الجرائم السيبرانية Cyber Crimes وتحديد المسئولية الجنائية وذلك من خلال المؤتمرات والاتفاقيات الدولية لمنع الجريمة السيبرانية، ومعاملة المجرمين السيبرانيين. حيث انتقلت جهود المنظمات الدولية التي تُقدِّمها منظمة الأمم المتحدة في مجال مجابهة المخاطر السيبرانية من مرحلة الشجب والتحذير غير المنتظم بنسق وإطار محدد إلى مرحلة التأطير القانوني ووضع الإستراتيجيات النظامية لمواجهة هذا التهديد.

توصيات الدراسة

أولا: ضرورة توجه التشريعات إلى تأطير مسألة المسؤولية الجنائية للجرائم ذات البعد التقني باستحداث تشريع ينظم مسائل المسئولية الجنائية وفق أنظمة الذكاء الاصطناعي للانسجام مع التطورات التكنولوجية.

ثانيا: أهمية الاعتراف التشريعي بالشخصية القانونية للتطبيقات الرقميو وجعلها منفصلة عن الشخصية القانونية لمالكها، مع ضرورة الانتباه للاختلاف بين طبيعة الشخصيتين لكون شخصية تلك التطبيقات التقنية ناقصة وليست كاملة، وبالتالي تكون مساءلته في الحدود الممكنة في التصرف التي يتمتع بها.

ثالثا: ينبغي لجميع الحكومات الاعتراف بأنّ القانون يضمن للأفراد التدفق الحر للمعلومات والأفكار؛ وتنطبق هذه الضمانات أيضًا على الفضاء السيبراني،

وينبغي عدم فرض القيود إلا عند الاقتضاء، على أن تخضع لعملية مراجعة قانونية.

رابعا: ينبغي لجميع البلدان العمل لوضع تشريعات جنائية مشتركة للسلوك السيبراني وإطار قانوني عالمي منسق، بما فى ذلك أحكام إجرائية تتعلق بالمساعدة في التحقيق والتعاون بما يكفل احترام الخصوصية.

خامسا: لا بد من تكاتف الجهود الداخلية والدولية لإنشاء منظمات دولية وإقليمية وإبرام اتفاقات ثنائية وجماعية، وتكون متخصصة، مهمتها الأساسية التنسيق بشأن مواجهة الجرائم التقنية واحتوائها ، ومحاولة التخفيف منها.

قائمة المراجع

أولا: المراجع العربية

الكتب :

١. ٤-سعيد عبد اللطيف حسن إثبات جرائم الحاسوب الآلي والجرائم المرتكبة عبر الإنترنت، دار النهضة العربية، القاهرة، ١٩٩٩.

٢. أحسن بوسقيعة، الوجيز في القانون الجزائي العام، دار هومة للنشر والتوزيع، الجزائر، الطبعة العاشرة،2011.

٣. إسماعيل صبري مقلد أصول العلاقات الدولية فى إطار عام، دار النهضة العربية، الطبعة الأولى، ٢٠٠٧.

٤. أشرف جمال محمود عبد العاطي، الإدارة الإلكترونية للمرافق العامة، دار النهضة العربية، مصر، ٢٠١٦.

٥. تيري ديبيل، إستراتيجية الشئون الخارجية منطق الحكم الأمريكي، ترجمة وليد شحادة، دار الكتب العربية، مؤسسة محمد بن راشد آل مكتوم، بيروت ٢٠٠٩م.

٦. جمال محمد غيطاس، الحرب وتكنولوجيا المعلومات، الطبعة الأولى، دار النهضة العربية، ٢٠٠٦.

٧. خالد ممدوح إبراهيم الجرائم المعلوماتية، دار الفكر الجامعي، مصر، ٢٠٠٩.

٨. د. أحمد الأنور، قواعد وسلوك القتال، دراسات فى القانون الدولي الإنساني دار المستقبل العربي، القاهرة، ٢٠٠٠.

٩. د. حسين المحمدي بوادي، الإرهاب الدولي بين التجريم والمكافحة، دار الفكر العربي، ٢٠٠٦.

١٠. د. عادل عبد الصادق الفضاء الإلكتروني والرأي العام، تغير المجتمع والأدوات والتأثير المركز العربي لبحوث الفضاء الإلكتروني : قضايا إستراتيجية ٢٠١٣م.

١١. صالح بن علي بن عبد الرحمن الربيعة، الأمن الرقمي وحماية المستخدم من مخاطر الإنترنت هيئة الاتصالات وتقنية المعلومات المملكة العربية السعودية، ٢٠١٨م.

١٢. طارق إبراهيم الدسوقي، الأمن المعلوماتي، دار الجامعة الجديدة، مصر، 2009.

١٣. طارق عزت رخا، المنظمات الدولية المعاصرة، دار النهضة العربية، القاهرة ٢٠٠٦.

١٤. عباس بدران الحروب الإلكترونية، الاشتباك فى عالم متغير مركز

١٥. عبد الصبور عبد القوي، الجريمة الإلكترونية، دار العلوم للنشر والتوزيع، القاهرة، ٢٠٠٨.

١٦. غنية باطلي، الجريمة الإلكترونية (دراسة مقارنة، منشورات الدار الجزائرية، الجزائر، ٢٠١٥.

١٧. كلاوس شواب الثورة الصناعية الرابعة، ملخصات لكتب عالمية، تصدر عن مؤسسة محمد بن زايد للمعرفة، دبي، الإمارات، ٢٠٢٠ م.

١٨. محمد الأمين، د. محسن عبد الحميد أحمد، معايير الأمم المتحدة في مجال العدالة لجنائية ومنع الجريمة، أكاديمية نايف للعلوم الأمنية، الرياض، الطبعة الأولى، ١٩٩٨.

١٩. محمد حماد مهرج الهيتي، التكنولوجيا الحديثة والقانون الجنائي، دار الثقافة للنشر، الأردن، الطبعة الأولى، 2004.

٢٠. محمد فهاد الشلالدة، القانون الدولي الإنساني، منشأة المعارف، الإسكندرية، ٢٠٠٥.

٢١. محمود حجازي محمود ، العنف الجنسي ضد المرأة في أوقات النزاعات المسلحة، دار النهضة العربية، القاهرة، ٢٠٠٧.

٢٢. مدحت رمضان، جرائم الاعتداء على الأشخاص والإنترنت، دار النهضة العربية، ط ٢٠٠٠.

٢٣. مصطفى محمد موسى الإرهاب الإلكتروني، بدون دار نشر، الطبعة الأولى، ٢٠٠٩.

٢٤. مصطفى محمد موسى، التحقيق الجنائي في الجرائم الإلكترونية، مطابع الشرطة، القاهرة، الطبعة الأولى، 2009.

٢٥. منير البعلبكي المورد : قاموس إنكليزي - عربي » ، دار العلم للملايين، بيروت

٢٦. منير محمد الجهيني، د. ممدوح محمد الجهيني جرائم الإنترنت والحاسب الآلي ووسائل مكافحتها ، دار الفكر العربي، الإسكندرية، ط ٢٠٠٤.

٢٧. نايل نبيل عمر، الحماية الجنائية للعمل الإلكتروني في جرائم المعلوماتية، دار الجامعة الجديدة، القاهرة، 2012.

٢٨. نزار العنبكي، القانون الدولي الإنساني، الطبعة الأولى، ٢٠١٠.

٢٩. هاني محمد خليل العزازي - النظام القانوني الدولي لمكافحة المخاطر السيبرانية دراسات الحكومة الإلكترونية، بيروت، لبنان، ٢٠١٠م.

٣٠. هلالي عبد اللاه أحمد، اتفاقية بودابست لمكافحة جرائم المعلوماتية (معلقا عليها) ، دار النهضة العربية، ط٢، ٢٠١١.

٣١. هلالي عبد اللاه أحمد، الجوانب الموضوعية والإجرائية للجرائم المعلوماتية (على ضوء اتفاقية بودابست (٢٠٠١) دار النهضة العربية، ط ٢٠٠١.

٣٢. هلالي عبد الله أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم في جرائم المعلومات (دراسة مقارنة)، دار النهضة العربية، القاهرة، ٢٠٠٠ .

الرسائل العلمية:

١. أسماء حسين رويعي، الحق في حرمة الحياة الخاصة في مواجهة الجرائم المعلوماتية، رسالة مقدمة لنيل درجة الدكتوراه في الحقوق كلية الحقوق جامعة القاهرة، ٢٠١٣.

٢. أميرة عبد العظيم محمد عبد الجواد، المخاطر السيبرانية وسبل مواجهتها في القانون الدولي العام، مجلة الشريعة والقانون، العدد الخامس والثلاثون، الجزء الثالث، ٢٠٢٠م.

٣. سمية بهلول ، دور الإدارة الإلكترونية في تفعيل أداء الجماعات الإقليمية في الجزائر، أطروحة مقدمة لنيل شهادة الدكتوراه في الحقوق تخصص إدارة محلية كلية الحقوق والعلوم السياسية جامعة باتنة ١ الحاج لخضر، ٢٠١٨

٤. عمر بن محمد العتيبي، الأمن المعلوماتي في المواقع الإلكترونية ومدى توافقه مع المعايير الدولية والمحلية، أطروحة مقدمة استكمالا لمتطلبات الحصول على درجة دكتوراه الفلسفة في العلوم الأمنية، كلية الدراسات العليا جامعة نايف العربية للعلوم الأمنية، الرياض، ٢٠١٠.

٥. نائلة عادل محمد فريد، جرائم الحاسب الاقتصادية، رسالة مقدمة لنيل درجة الدكتوراه، كلية الحقوق، جامعة القاهرة، ٢٠٠٣.

الدوريات العلمية

١. تهاني حامد أبو طالب، الروبوت من منظور القانون المدني المصري الشخصية والمسؤولية)، مجلة البحوث الفقهية والقانونية العدد ٣٧ إصدار أبريل ٢٠٢٢م/١٤٤٣هـ.

٢. حكيم سياب السمات المميزة للجرائم المعلوماتية عن الجرائم التقليدية ، مجلة دراسات وأبحاث، جامعة زيان عاشور، الجلفة ، المجلد الأول، العدد الأول.

٣. روان بنت عطية الله الصحفي، الجرائم السيبرانية Cyber Crimes، المملكة العربية السعودية، المجلة الإلكترونية الشاملة متعددة التخصصات، العدد الرابع والعشرون، مايو ٢٠٢٠

٤. سمية بهلول ، دمان ذبيح عماد الآليات العقابية لمكافحة الجريمة الإلكترونية في الجزائر"، مجلة الحقوق والعلوم السياسية، جامعة عباس لغرور خنشلة ، المجلد السابع، العدد ١٣، جانفي ٢٠٢٠.

٥. عسكر مراد، إشكالية تطبيق أحكام المسؤولية الجنائية على جرائم الذكاء الاص الحقوق والعلوم الإنسانية جامعة تلمسان، المجلد ١٥، العدد ٠١، ٢٠٢٢.

٦. فطيمة نساخ، " الشخصية القانونية للكائن الجديد : الشخص الافتراضي الروبوت"، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، مجلد ٥، عدد ١، ٢٠٢٠.

٧. محمد عرفان الخطيب المسؤولية المدنية والذكاء الاصطناعي... إمكانية المساءلة، دراسة تحليلية معمقة لقواعد المسؤولية المدنية في القانون المدني الفرنسي، مجلة كلية القانون الكويتية العالمية، السنة الثامنة، العدد ٠١، العدد التسلسلي ،٢٩، قطر، مارس ٢٠٢٠.

٨. محمد عرفان الخطيب، «المسؤولية المدنية والذكاء الاصطناعي...إمكانية المساءلة؟ دراسة تحليلية معمقة لقواعد المسؤولية المدنية في القانون المدني الفرنسي»، مجلة كلية القانون الكويتية العالمية، العدد الأول، ٢٠٢٠.

٩. مراد بن عودة حسكر، إشكالية تطبيق أحكام المسؤولية الجنائية على جرائم الذكاء الاصطناعي"، مجلة الحقوق والعلوم الإنسانية، مجلد ١٥، عدد ١، ٢٠٢٢.

١٠. ممدوح حسن مانع العدوان، «المسؤولية الجنائية عن أفعال كيانات الذكاء الاصطناعي غير المشروعة»، مجلة دراسات علوم الشريعة والقانون، المجلد ٤٨، عدد ٤، ٢٠٢١.

ثانيا: المراجع باللغة الإنجليزية

1. Blimding weapons: Reports of the meetings of experts convened by the international committee of the red cross on battlefield laser weapons, 1989- 1991, ICRC, 1993.
2. Christian Agrum, Words for Understanding Cyber Security: Enjoying a Calm Internet, Edition, October, 1, 2010.
3. Dorothy E. Denning, Activism, Hacktivism and cyber terrorism, the internet as a tool for influencing Foreign policy in Arquilla & D. Ronfold (eds), Networks and net wars, the future of terror crime and miletences, National Defense Research Institute, 2001.
4. Doswald- Beck "international humanitarian law and the advisory opinion of international court of justice on the threat or use of nuclear weapons" ICRC Vol.316, 1997.
5. Ebert Hannes and Maurer Tim. "Cyber Security" oxford bibliographies, Last Modified: 11 January,2017.
6. Fahad Ullah Khan, States rather than criminals pose a greater threat to global cyber security: a critical analysis, the Institute of Strategic Islamabad ISSI ..olume xxxi, no3, Autumm 2011, p.93,

7. Hall William Edward, A Treatise on international law, Fourth edition Oxford, London, 1895.

8. Harvard, Joseph S. Nye: The future of power .press realise, Belfer center for Science and international Affairs, Kennedy Scholl, 31 january 2011.

9. in The Charter of the United Nations Article 51, A. Randelzhofer .664 (B.Simma ed.) 1995, A Commentary 661.

10. Jack L. Brock, Computer Security: Hackers Penetrate DOD Computer System (Washington DC: General Accounting Office, 1991)

11. Jeffrey T. G Kalsey, Hacking in to international humanitarian law: The principles of distinction and neutrality in the age of cyber warfare, Michigan law review, 2008, vol.106, issue 7.

12. Jennie M. Williamson "Information Operations: computer U.S.Army, PA, Carlisle Barracks, Network Attack in the 21 st century" war college, 2002. Joseph. S. Nye, Cyberpower Haward Kennedy School, Belfer center for science and International Affairs 2010

13. Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion, 2004, JCJ Rep 136, para 35, Separate opinion of Judge Higgins.

14. Maura Conway, Terrorism and new media: the cyber-battl espace in: Forest, James F., (eds.), Countering terrorism and insurgency in the 21st century, Greenwood Publishing Group, Inc., Westport. CT, 2007,PP.363-384.

15. Michael N Schmitt, Computer Network Attack and The Use of Force in International Law: Thoughts on a normative framework, Co;ombia Journal of transnation law, 1998-1999.

16. Michael N. Schmitt, "Peacetime Cyber Responses and wartime Cyber Operations inder International Law: An Analytical Vade Mecum", Harvard National Security Journal, Vol.8, 2017.

17. Michael N.Schmitt & Liis Vihul, Tallinn Manual 2.0 on the International Law Applicable to Cyber, pretations, Cambridge University Press, 2017, note 13, Rule 32.

18. N.TSAGOURLAS, Cyber Attacks, Self-defence and the Problem of Artibution, J.Conflict & Sec L.Vol.17, no 2, 2012,.

19. Rohas Nagpal, Cyber terrorism in the context of globalization, Paper presented at II World Congress on Informatics and Law, Madrid, Spain, September 2002, p.4,

20. Ruseell Buchan, "Cyber espionage and international law", In: Nicholas Tsagourias and Russell Buchan (eds), Research.

Handbook on International law Cyberspace, (Edward Elgar Publishing 2015).

21. S.SCHJOLBERG, The History of Global Harmonication on Cybercrime Legislation, 2008,

22. Tallinn Mnnual on the International Law Applicable to Cyber Warfare (Michael N. Schmitt ed., 2013), pp.106-107.

23. Toward a Universal order of Cyberspace :managing Threats from Cybercrime of Cyberya The International Telecommunication Union, ITU Toolkit for Cybercrime Legislation, Geneva, 2010.

ثالثا: المراجع باللغة الفرنسية

1-Al Azouzi Ali, La Cybercriminalité au Maroc, Edition Bishops solution, Casablanca, 2010.

2-Jean François Casile, Le Code pénal à l'épreuve de la délinquance informatique, Presse Universitaire d'Aix, Marseille, 2002.