الحماية الجنائية لمستخدمي تطبيقات إنترنت الأشياء

"دراسة مقارنة"

Criminal protection for users of Internet of Things applications "A comparative study"

إعداد

د/ محمد عبد الرحمن عبدالمحسن

أستاذ القانون الجنائي المساعد

كليات عنيزة الاهلية - المملكة العربية السعودية

الحماية الجنائية لمستخدمي تطبيقات إنترنت الأشياء
"دراسة مقارنة"

محمد عبد الرحمن عبدالمحسن
قسم القانون الجنائي – كليات عنيزة الاهلية – المملكة العربية السعودية
البريد الإلكتروني : mohammed.a@oc.edu.sa

الملخص

يعد نظام انترنت الأشياء نظام تقنى حديث يتخطى أسلوب تواصل الأشخاص مع الأجهزة الذكية عبر شبكة الانترنت بحيث يتيح للأشخاص التواصل مع الأجهزة الذكية دون تدخل الانسان برز حديثا هذا النوع من التقنيات التكنولوجية الحديثة بحيث يعتمد على الجيل الجديد من الانترنت (الشبكة) الذى يهي التفاهم بين الأجهزة المترابطة مع بعضها (عبر بروتوكول الانترنت) من بينها الأجهزة والأدوات والمستشعرات والحساسات وكافة أدوات الذكاء الاصطناعي المختلفة وغيرها ، حيث تتخاطب وتتفاهم الأشياء عبر شبكة الانترنت دون تدخل البشر فيها ، كما تهدف هذه الدراسة إلى بيان أوجه الحماية الجنائية لمستخدمي برامج انترنت الأشياء حيث تم تقسيم الدراسة الى عدة مباحث رئيسة تناولنا في المبحث الأول : مفهوم انترنت الأشياء ،تناولنا في المطلب الأول : مفهوم الامن السيبراني وعلاقته انترنت الأشياء ،أما عن المطلب الثاني : الحماية الجنائية من الهجمات السيبرانية على انترنت الأشياء، في حين تناول المطلب الثالث: الحماية الجنائية في التشريعات العربية أما عن المطلب الرابع : التكييف القانوني للهجمات السيبرانية وعلاقته انترنت الأشياء ، وتناولنا في المبحث الثاني: الجهود الدولية لمواجهة الجرائم السيبرانية وحماية انترنت الأشياء ،وتناول المطلب الأول: النماذج العملية للجرائم السيبرانية وحماية تطبيقات انترنت الأشياء ، والمطلب الثاني: التعاون الدولي وحماية انترنت ، المبحث الثالث : المواجهة الجنائية لمخترقي تطبيقات انترنت الأشياء، المطلب الأول:. صور المواجهة الجنائية لجرائم انترنت الأشياء .

الكلمات المفتاحية : الحماية الجنائية، انترنت الأشياء، الجرائم السيبرانية، التطبيقات القضائية، الجهود الدولية .

Criminal protection for users of Internet of Things applications
"A comparative study"

Muhammad Abdel Rahman Abdel Mohsen
Department of Criminal Law - Unayzah Private Colleges - Kingdom of Saudi Arabia
Email: mohammed.a@oc.edu.sa

Abstract :
This study aims to explain the aspects of criminal protection for users of Internet of Things programs. This topic was divided into several main sections. In the first section, we discussed the concept of the Internet of Things. As for the second section, we discussed international efforts to confront cybercrimes and protect the Internet of Things, while in the third section, we discussed applications Judicial case for cybercrimes.
Criminal protection in Arab legislation. As for the fourth requirement: the legal adaptation of cyberattacks and its relationship to the Internet of Things, we discussed in the second section: international efforts to confront cybercrimes and protect the Internet of Things. The first requirement dealt with: practical models for cybercrimes and the protection of Internet of Things applications, and the second requirement: cooperation. International and Internet Protection, Third Section: Criminal Confrontation of Hackers of Internet of Things Applications, First Requirement:. Pictures of criminal confrontation for Internet of Things crimes.

Keywords: Criminal Protection, Internet Of Things, Cybercrime, Judicial Applications, International Efforts.

بسم الله الرحمن الرحيم

مقدمة :

نتيجة لتطور الانترنت وتوسع استخداماته في كافة نواحي الحياة اصبح مجالاً خصباً للتفكير وارتكاب الجرائم من خلاله خصوصاً مع ظهور ما يعرف بأنترنت الأشياء من خلال اختراق الأجهزة الحاسوبية والبريد الالكتروني واختراق الشفرات وغيرها من وسائل الهجوم المعلوماتي الذى اصبح ثمة العصر وواحد من الأنواع الجديدة من الجرائم في العصر الحديث ، ويعد إنترنت الأشياء أسلوب متطور لشبكة الانترنت ظهر عام ١٩٩٩ من اختراع العالم البريطاني(كيفن اشتون)ويشار اليه (IOT)كما يشير انترنت الأشياء إلى المجموعة من الكيانات والاشياء التي يتم استخدامها يومياً ومتلازمة من خلال شبكة واحدة وهو بمثابة حلقة وصل بين أجهزة الحوسبة المضمنة الفريدة القابلة للتعرف داخل بنية تحتية موجودة [١].

وعلى ذلك فان انترنت الأشياء يعد نظام تقنى حديث يتخطى أسلوب تواصل الأشخاص مع الأجهزة الذكية عبر شبكة الانترنت بحيث يتيح للأشخاص التواصل مع الأجهزة الذكية دون تدخل الانسان برز حديثا ، بحيث يعتمد على الجيل الجديد من الانترنت (الشبكة) الذى يهي التفاهم بين الأجهزة المترابطة مع بعضها (عبر بروتوكول الانترنت) من بينها الأجهزة والأدوات والمستشعرات والحساسات وكافة أدوات الذكاء الاصطناعي المختلفة وغيرها ، حيث تتخاطب وتتفاهم الأشياء عبر شبكة الانترنت دون تدخل البشر فيها .

1) Brian and oters ,2014.p18

مشكلة البحث : -

أصبح من الضروري التدخل لحماية مستخدمي برامج انترنت الأشياء من خلال بسط الحماية الجنائية لمستخدمي مثل هذه التطبيقات الحديثة من الاختراق أو أي اعتداء خصوصاً مع عدم تدخل الانسان .

أهداف البحث : -

١-التعرف على أنواع الجرائم التي تتم على برامج اختراق انترنت الأشياء.

٢-التعرف على الوسائل البديلة التي تضمن حفظ المعلومة المنشورة الالكتروني .

٣-التوعية من مخاطر هذه الجرائم على المجتمع .

أهمية الموضوع : -

أولا : الأهداف العلمية تتحقق من خلال زيادة وانتشار استخدام انترنت الأشياء في العالم فأصبح من الضروري والمحتم بسط الحماية الجنائية الكاملة لمستخدمي مثل هذه البرامج .

ثانيا : **الأهداف العملية** : حيث ارتكز هذا البحث على استعراض الأنظمة المحدثة وطرق الحماية الجنائية ،فضلا عن كون هذا الموضوع من الموضوعات الهامة نظراً لان الجرائم الالكترونية من الجرائم المستحدثة لذلك فان المعالجة القانونية يجب ان تتم في إطار شمولي وذلك لان اعتماد المحاور الرئيسية للحماية الجنائية في ضوء الدراسة يتطلب بالضرورة استخدام المنهج التحليلي المقارن بين كافة التشريعات الجنائية .

خطة الدراسة

المبحث الاول: مفهوم انترنت الأشياء .

المطلب الأول : مفهوم الامن السيبراني وعلاقته انترنت الأشياء .

المطلب الثاني : الحماية الجنائية من الهجمات السيبرانية على انترنت الأشياء .

المطلب الثالث: الحماية الجنائية في التشريعات العربية .

المطلب الرابع : التكييف القانوني للهجمات السيبرانية وعلاقته انترنت الأشياء .

المبحث الثاني: الجهود الدولية لمواجهة الجرائم السيبرانية وحماية انترنت الأشياء

المطلب الأول: النماذج العملية للجرائم السيبرانية وحماية تطبيقات انترنت الأشياء .

المطلب الثاني: التعاون الدولي وحماية انترنت

المبحث الثالث : المواجهة الجنائية لمخترقي تطبيقات انترنت الأشياء .

المطلب الأول:. صور المواجهة الجنائية لجرائم انترنت الأشياء

المبحث الأول

مفهوم انترنت الأشياء

تمهيد وتقسيم :

يعد نظام انترنت الأشياء "Internet of things "أو ما يعرف (IOT)بحيث يشار اليه باسم الأجهزة المتصلة والأجهزة الذكية) والمباني وغيرها من المواد المحسوسة التي تمثل جزاء لا يتجزأ من الالكترونيات والبرمجيات الحديثة أي ان يتم العمل بها دون تدخل بشرى فضلاً على وجود عدد هائل من الأجهزة المعرضة للاختراق والقرصنة ما يشكل تهديدا وضحاً للبيانات وخطر على خصوصية المستخدم من الدراسات الحديثة في هذا الشأن ان زيادة إنترنت الأشياء زادت من ٥٠٠ مليون جهاز في عام ٢٠٠٣ إلى ٥.١٢ بليون جهاز في عام ٢٠١٠ وبلغ عددهم عام ٢٠١٥ أكثر من ٢٥ بليوناً ، وتضاعفت عام ٢٠٢١ الى ٥٠ بليون جهاز ومما جعلها كثيرة مما يستوجب أكثر أمان وفاعلية خاصة بعد صدور العديد من المجرمين المحترفين في هذا المجال[١] .

كما يعرفه بعض الفقه بأنه " مجموعة من الأجهزة القابلة للعنونة في بروتوكول الانترنت التي تتفاعل مع البيئة المادية ، والتي تحتوى على عناصر للاستشعار والتواصل والمعالجة والتشغيل . وهو جميع الأشياء والأجهزة والمعدات والبرمجيات والتطبيقات والتي منها انترنت الأشياء وأيضا أجهزة المراقبة والتحكم وأجهزة ووسائل معالجة وتخزين البيانات وأجهزة المراسلات والمستقبلات وأية معدات مساعدة ولعل من الملاحظ ان أول من قدم عرضاً تقديماً عن انترنت الأشياء هو الباحث في التقنية

١) ادهم طارق الحماية الجنائية للحياة الخاصة عبر الانترنت دراسة مقارنة ٢٠٠٧ ص٨٠

البريطـاني Ashton kevin لشـركة Gamble. proctor فـي عام ١٩٩٩م[١]

وعرفه جانب أخر من الفقه بأنه " جيل متطور من الانترنت لجعل الأشـياء المتصـلة بالشـبكة بشـكل مسـتمر قـادرة علـى إرسـال البيانـات واستقبالها "[٢]

ويعد تطبيق انترنت الأشياء جزء لا يتجزأ من الذكاء الاصطناعي كما أنـه يجمـع بـين بـين إدارة البيانـات والتحليلات الزاخرة بالمعلومـات للتصـميم خدمات سهلة الاستخدام مصممة لبيانات إنترنت الأشياء كبيرة الحجم[٣].

هناك فارق جوهري بين إنترنت الأشياء والذكاء الاصطناعي الأول مهمتـه جمـع البيانـات فـي حـين الثـاني يقـوم بتحليـل البيانـات حتـي اصـبح المتعاملين يخلطون بين المصطلحين في كثير من الأحيان .

ويعتبـر تطبيـق انترنـت الأشـياء مـن الخـدمات والبـرامج التـي تـدمج البيانات المستلمة من أجهزة إنترنت الأشياء المختلفة وهى تستغل تكنولوجيا الـتعلم الالـي أو الـذكاء الاصـطناعي لتحليـل هـذه البيانـات واتخـاذ قـرارات مدروسة علـى أن تعاد هذه القرارات إلـى جهاز إنترنت الأشياء ثم يستجيب جهاز إنترنت الأشياء بعد ذلك بذكاء للمدخلات .

وفـى عـام (٢٠١١) تـم الاسـتعانة بآليـة مسـتندة الـى نظـام اقتحـام انترنت الأشياء ومعرفة مجرمين وجرائم اقتحام انترنت الأشياء .

---

١) أ . عارف بن خميس الفزاري مقالة منشورة عام ٢٠٢٢ م

٢) د . عبد الرحيم نـادر عبد الرحيم ، دور إنترنت الأشياء في إدارة معرفة العمـلاء ، المجلة العلمية للدراسات التجارية والبيئية ٢٠٢١ ص٢٥٥

3) cyber-crimes: a review, op, cit, P. 28 Selma Dilek, applications of artificial intelligence techniques to combatin

مزايا استخدام تطبيقات انترنت الأشياء : –

- سرعة وسهولة الاتصال بالإنترنت .
- استخدام التقنيات الحديثة المدمجة والتطبيقات الحديثة وأجهزة الاستشعار .
- استخدام انترنت الأشياء وفى تنفيذ التحريات في مجال التحقيقات الجنائية الرقمية [1] .
- إتمام كافة المهام بطريقة يومية أوتوماتيكيا والتحكم بها والحفاظ عليها أيضا .
- توفير الجهد والمال لمستخدم لإنترنت الأشياء .
- الحد من التدخل البشري من شأنه ان يقلل نسبة الأخطاء .
- زيادة الإنتاج .
- استغلال الموارد المتاحة بشكل فعال .
- استخدامه في علم التحقيقات الجنائية الرقمية ، كما انه تجدر الإشارة الى ان التحقيق الجنائي الرقمي يستخدم للحفاظ على الأدلة الرقمية وتوثيقها وذلك لاستخدامها في المحاكم كدليل من ادلة الاثبات كما ان هذا النظام يوفر الكثير من الوقت والجهد خاصة في جميع التحقيقات ، كما انه يوفر كثير من المصادر الجنائية الجديدة .
- تتم الإجراءات الخاصة بالتحقيق الجاني الرقمي من خلال جمع بيانات وذلك يتم من خلال إشارات من خلال السجلات المخزنة ، كما انها تتم

---

١) أ . فرج عامر الرويلي ، هيكلة التحقيق الجنائي الرقمي لإنترنت الأشياء ٤ /١١ / ٢٠٢٢ م مقال منشور

– د . عبد الرحيم نادر عبد الرحيم ، دور إنترنت الأشياء في إدارة معرفة العملاء ص ٥٠ مرجع سابق

من خلال جمعها من أنظمة إنترنت الأشياء واثبات الوقائع القانونية المحددة لها كما يمكن جمع ذلك أجهزة الاستشعار الثابتة الموجودة في المنازل أو المباني ، وأجهزة الاستشعار المتحركة في التكنولوجيا أو المركبات القابلة للارتداء ، وكذلك أجهزة الاتصال الجديدة ، ولعل الملاحظ ان هذه الأجهزة تجعل من الافراد تدريب عالي الجودة على الأشياء الحديثة في مجال الاثبات الجنائي .[١]

اذن ينبغي ان نعلم مكونات النظام البيئي لإنترنت الأشياء بعد التعرض لمزايا التطبيق يتكون النظام من خمسة مكونات رئيسية :

-الشبكة : هي الوسيلة التي يحافظ النظام البيئي من خلالها على اتصال مستمر من الجهاز إلى المستخدم .

- الخدمة : من خلال مكون البرنامج .
- الجهاز : المكون المادي المتحكم في الجهاز .
- المستخدم : المالك المفترض للنظام البيئي .
- السحابة : حيث تتم معالجة البيانات وتخزينها .
- برنامج تقنى لمعالجة البيانات .

من الأمثلة على ذلك اختراق الأجهزة الإنذار الأمنية أثناء تواجد أصحاب المنازل بعيداً عنهم للسماح بعمليات اقتحام سلسلة وذلك لتحقيق الأغراض الشخصية اليومية من خلال تهديد خطير لمستخدمي مثل هذه البرامج .

1(M .Stoyanova ,y .Nicolaides ,s .Panagiotaki's ,E .Pallis and E.K, Markis , A Survey on the Internet of Things (IOT) Forensics: Challenges ,Approaches ,and Open issues ,in LEEE Communications ,Surveys , Tutorials , vol,22 ,no2,pp.1191-1221,Secondquter 2020 ,doil; 10.1109/ COMST . 2019 .2962586

مجالات استخدام إنترنت الأشياء :

يسمح تطبيق نظام انترنت الأشياء (IOT) بالاتصال بالإنترنت بما يتجاوز الأجهزة التقليدية مثل أجهزة الحاسوب والهواتف الذكية **حيث يستخدم التطبيق في مجالات واسعة منها :**

- **إنترنت الأشياء في المنزل الذكي .**
- **أنترنت الأشياء الرياضية .**
- **إنترنت الأشياء الطبية .**
- **إنترنت الأشياء في الصناعة .**
- **إنترنت الأشياء في الزارعة .**
- **إنترنت الأشياء في التعليم .**
- **إنترنت الأشياء في البناء .**
- **التعريف بالأنترنت : هو عبارة عن شبكة الكترونية ضخمة تضم الملايين من الشبكات الداخلية و أجهزة الحاسوب المرتبطة مع بعضها البعض عن طريق الاتصال السلكي واللاسلكي والمنتشرة في ارجاء العالم وتزود المستخدمين على مدار الساعة بمجموعة كبيرة من الخدمات المتنوعة[1] .**
- **عن طريق مجموعة من الوحدات منها ١- وحدة إدارة المراقبة الكترونية وهى تراقب أي بيانات آو حركة مروتذهب أو تاتى من جهاز الاستشعار**

١) د . عبد الفتاح بيومي حجازي ، الجرائم المتحدثة ، مرجع سابق ص٣٥.- فرج عامر الرويلي ، هيكلة التحقيق الجنائي الرقمي لإنترنت الأشياء ٤ /١١ / ٢٠٢٢

. تتم إجراءات التحقيق الجنائي الرقمي لأنترنت الأشياء من خلال تسع مراحل :

- **التحديد**
- **التحضير**
- **النهج**
- **الحفظ**
- **التجمع**
- **الفحص**
- **التحليل**
- **العرض التقديمي**
- **إعادة الأدلة**

المطلب الأول

مفهوم الامن السيبراني وعلاقته بأنترنت الأشياء

شهد العالم نموذجا جديداً في سباق التسلح يتمثل في الهجمات الالكترونية (السيبرانية) وهذه الهجمات اما ان تكون ذات طبيعة عسكرية تتمثل في اتساع نطاق التدمير لقوات الدولة او لمدنيين توقع الهجوم ضدها أو يستهدف البنية التحتية للدولة كمحطات الطاقة او الخدمات المالية او يستهدف المؤسسات الأمنية او العسكرية وذلك باختراق هذه الشبكات الخاصة بالمؤسسات بهدف سرقة هذه المعلومات او تدميرها الكترونيا[١] .

تعريف الامن : عرفه بعض الفقهاء بأنه القدرة التي تتمكن بها الدولة التي تستعرض فيها الدولة قدرتها العسكرية والاقتصادية و الداخلية والخارجية لمواجهة الاخطار الداخلية والخارجية وقت السلم والحرب على حدا سواء .

كما عرفه جانب أخر من الفقه بأنه " شعور الانسان بالطمأنينة على نفسه وما يتصل به من عرض ومال ومسكن وملبس وطعام [٢] .

عرفته وزارة الدفاع الامريكية " البنتاغون " تعريفاً دقيقاً لمصطلح الأمن السيبراني ، فاعتبرته جميع الإجراءات التي تحول لضمان حماية المعلومات بجميع أشكالها المادية والمعنوية من مختلف الاعتداءات[٣] .

---

١) ،د. ايهاب خليفة : ما هو موقف ميثاق الامم المتحدة من استخدام القوة السيبرانية في التفاعلات الدولية – مقال صادر عن مركز المستقبل للأبحاث والدراسات المتقدمة – ابوظبي – الامارات العربية المتحدة ، ٢٠١٩م ، ص ٢ ، ٣ .

٢) عبد الله يحيى سعيد الزهراني ، استراتيجيات الامن السيبراني في ضوء التقنيات والتحديات الحديثة ، دراسة مقارنة ، رسالة قدمت لنيل درجة الماجستير في العلوم الاستراتيجية ، جامعة نايف العربية للعلوم الأمنية ، كلية العلوم الاستراتيجية قسم الدراسات ، المملكة العربية السعودية ، عام ٢٠١٠ م ص ١١

(٣) انظر الموقع hh//political-encyclopedia.org

وكنتيجة طبيعة للتقدم التكنولوجي في كافة المجلات ظهر ما يسمى بأنترنت الأشياء والتي يستخدم فيه الأجهزة والشبكة ويعنى انترنت الأشياء هو شبكة عملاقة يتم من خلالها اتصال ملايين من الأجهزة والسيارات بشبكة الانترنت ليتم من خلاله تمرير البيانات ، والامثلة عديدة على ذلك في استخدامات انترنت الأشياء مثل شراء الاحتجاجات من المحلات والمتاجر دون الاعتماد على الانسان ومن أمثلة ذلك أيضا استخدام انترنت الأشياء في إدارة قطاع الطاقة ويتم من خلال ذلك التحكم في العدد الذكي .

ويوجد اختلاف واضح بين الحرب السيبرانية والحرب التقليدية باعتبار أن الحرب التقليدية تقوم على استخدام الجيوش النظامية في الاعلان المسبق لهدا الحرب بخلاف الحرب السيبرانية فهي حرب غامضة وغير محددة الاهداف باعتبارها تتحرك عبر شبكة المعلومات الالكترونية[١] .

وإما ان تكون ذات طبيعة غير عسكرية بمعنى أن تكون تداعياتها ذات طبيعة اقتصادية او اجتماعية كالإرهاب السيبراني وذلك من خلال تنفيذ هجمات الكترونية ضد اهداف ومؤسسات الدولة او تشويه الرموز السياسية لمواقع التواصل باستخدام الهاش تاج في التشويه لهذه الرموز أو الاساءة لها[٢] .

وعندما تشكل الهجمات السيبرانية نزاعا مسلحا فإننا نكون أمام مصطلح الحرب السيبرانية أو ما يسمى بالهجوم السيبراني طبقا لقواعد القانون الدولي الانساني سواء كانت هذه الهجمات هجومية أم دفاعية يمكن أن يترتب عليها ضحايا أو اصابة أو قتل أشخاص ، وبالتالي فإن هذه

(٣) الرائد / حسن فياض : الهجمات السيبرانية من منظور القانون الدولي الانساني ، مجلة الدفاع الوطني ، لبنان ، العدد 14 ، ٢٠٢٠ ، ص ١ .

(٤) د. ايهاب خليفة : ما هو موقف ميثاق الامم المتحدة من استخدام القوة السيبرانية في التفاعلات الدولية ، مرجع سابق ، ص ٢ ، ٣ .

الهجمات يمكن أن تكون أوسع نطاقا من الحرب السيبرانية الامر الذي يمكن أن يترتب عليه قيام الحرب[١] ويتضح لنا علاقة الامن السيبراني بإنترنت الأشياء من خلال طبيعة انترنت الأشياء تتطلب ان يتم كل شي دون تدخل الانسان ويتم الاعتداء على التطبيق بواسطة الهجمات السيبرانية المتقنة من أجل اختراق التطبيق والدخول فيه أما بإعطاء معلومات خاطئة غير حقيقة مخالفة للحقيقة أو لتضليل الاخرين المتعاملين مع مثل هذه التقنية الحديثة .

(١) د. يحي ياسين سعود : الحرب السيبرانية في ضوء قواعد القانون الدولي الانساني ، بحث منشور في المجلة القانونية بكلية الحقوق ، جامعة القاهرة ، المقالة ٣، المجلد ٤، العدد ٤، 2018م ، ص ٨٤ . انظر الموقع التالي:
https://jlaw.journals.ekb.eg/article_45192_52d735c1a23cca2bf7dbbe56c4eb6846.pdf

المطلب الثاني

الحماية الجنائية من الهجمات السيبرانية على انترنت الأشياء

يعني مصطلح السيبرانية في اللغة أنه مشتق من الكلمة اليونانية (kybemetes) وقد ورد في مؤلفات الخيال العلمي بمعنى القادة والتحكم عن بعد كما ورد فى قاموس المورد ويعني علم الضبط ، وفى اللغة العربية نجد أن مصطلح السيبرانية هو مصطلح مستخدم فى اللغة الانجليزية فى اللغة الانجليزية (cyber) وليس له مصطلح مماثل فى اللغة العربية للك نجد صعوبة فى فى اختيار مصطلح يقارب مصطلح (cyber) فى اللغة الانجليزية ، كما أن أغلب الترجمات لهذا المصطلح كانت غير صائبة وأن كل ما نجده فى هذه الترجمة عنوان (اتفاقية أوربا المتعلقة بالجريمة السيبرانية) وتم ترجمتها للغة العربية الى الاتفاقية المتعلقة بالجريمة الالكترونية[١] .

مفهوم الحماية الجنائية :سعى المشرع للحافظ على المجتمع من خلال حماية المصالح الضرورية والقيم الأساسية في المجتمع ولذلك الحماية الجنائية المتحققة بشقيها لحماية المراكز الشخصية والمعنوية على حدا سواء من تهديد أمن وطمأنينة المجتمع ككل ويقصد بالحماية الدولية كمصطلح أعم و أشمل حماية الدول من الاعتداء عليها من حق الانسان في المحافظة على حياته الخاصة من عدم العبث بها أو الدخول فيها ، وذلك فمن الفقهاء من يراي ان الحماية الجنائية هي أحد أنواع الحماية القانونية

٢) د. يحي ياسين سعود : الحرب السيبرانية في ضوء قواعد القانون الدولي الانساني ، مرجع سابق ، ص ٨٣ .

بل أهمها قاطبة واخطرها اثرا على الكيان الانسان وحرياته ووسيلتها القانون الجنائي[١]

وفى الاصطلاح تعددت التعريفات في هذا الشأن ويشير مصطلح السيبرانية الى أشياء كثيرة كالإشارة الى تنوع وسائل القتال التي يمكن في النهاية أن يصل الى حد النزاع المسلح[٢] .

كما عرفت أيضا بأنها "هي التي تتم بواسطة الكمبيوتر أو أحد الوسائل التقنية الحديثة على كومبيوتر أخر أو أحد وسائل التقنية الحديثة ، مع ضرورة توفر شبكة أتصال فيما بينها[٣].

وعرفها الفقه الالماني بأنها " هي كل أشكال السلوك غير المشروع أو الضار بالمجتمع والذى يرتكب باستخدام الحاسب الألي .

وعرفت أيضا بأنها " نشاط أجرامي تستخدم فيه تقنية الحاسب الألى بطريقة مباشرة أو غير مباشرة كوسيلة أو هدف للتنفيذ الفعل الاجرامي المقصود "[٤]

---

١) د . عبد العظيم مرسى وزير : الشروط المفترضة في الجريمة ، دار النهضة العربية، مصر ١٩٨٣ ص ١٣٣ .

٢) د . أحمد فتحي سرور: شرح قانون العقوبات القسم العام ، دار النهضة العربية ، ٢٠٠٥ ص ٩٠

(3) د. طلال ياسين العيسى ، عدي محمد غياب : المسئولية الدولية الناشئة عن الهجمات السيبرانية في ضوء القانون الدولي المعاصر ، مجلة الزرقاء للبحوث والدراسات الإنسانية ، الأردن ، المجلد التاسع عشر ، العدد الأول ، ٢٠١٩م ، ص ٨٣ .

(٤) أ. أسامة مهمل : الاجرام السيبراني ، رسالة ماجستير ، كلية الحقوق والعلوم السياسية ، جامعة

(٥) د. محمد الامين البشرى – التحقيق في جرائم الحاسب الألي كلية الحقوق والشريعة جامعة الامارات ص ٦

وفي تعريف أخر " كل عمل أو أمتناع يأتيه الانسان إضرار بمكونات الحاسوب المادية و المعنوية وشبكات الاتصال الخاصة باعتبار من المصالح والقيم المتطورة التي تمتد مظلة القانون لحماتيها [١]

تعد الجرائم السيبرانية من الجرائم من الجرائم الحديثة من حيث الكم والكيف لما لها من خطورة على الفرد والمجتمع على حد سواء حيث يتفنن الجناة باستخدام أحدث الأجهزة والتقنيات في تنفيذ هاجمتهم السيبرانية على القطاع العام أو الخاص والافراد وتعد صور الاعتداء من خلال الجرائم ضد جهاز الحاسب الألي أو أنظمة تقنية المعلومات والاتصالات من صورها جرائم الاحتيال وسرقة الهركس على والابتزاز الكتروني والسلوك المنحرف والاستغلال الجنسي للأطفال ، إضافة إلى الترويج للأفكار المتطرفة عبر الانترنت:

ومن احدث الدراسات التي اجيرت على في هذا الشأن في الفترة من ٢٠٠٠ حتى ٢٠١٤م تبين أن هناك زيادة كبيرة في ارتكاب الجرائم السيبرانية نظراً لكثرة استعمال أجهزة الحاسب الألي وارتفاع معدلات الجرائم وخاصة مع اصدار مجلس أوربا الاتفاقية الخاصة بالحد من الجرائم والهجمات السيبرانية council Europe convention on cybercrimes

ولعل من الملاحظ ما تم رصده عام ٢٠١٤ م حيث تبين ارتفاع في معدل ارتكاب الجرائم الإلكترونية مما نتج عنه خسائر كبيرة على المستوى العالمي حيث قدرت بحوالي ٤٤٥ مليار دولارو في ذات السياق وذلك في

١) أ . محمد أمين الشوابكة : جرائم الحاسوب والانترنت (الجريمة المعلوماتية) – دار الثقافة للنشر والتوزيع ، عمان ، الأردن ٢٠٠٩ ص ٦

دراسة اجريت عام ٢٠١١ م إلى زيادة نسبة انتهاك البيانات الخاصة بمؤسسات القطاع الخاص ..:[١]

وتختلف الحرب السيبرانية عن الحرب التقليدية باعتبار أن الحرب السيبرانية غير محددة المجال وهي حرب غامضة الأهداف لأنها تقوم عبر شبكة المعلومات ولاتصالات المتعدية للحدود الدولية ، كما أنها يمكن أن توصف بأنها أسلحة الكترونية جديدة تستخدم لضرب المنشآت الحيوية للعدو ، كما يمكن توجيهها أو دسها للعدو عن طريق عملاء لأجهزة الاستخبارات[٢] .

ويهدف الهجوم السيبراني الى ضرب أو تعطيل أو تدمير أو سرقة البيانات والمعلومات للعدو أو الحصول على البيانات بالطرق غير المشروعة ، كما تستهدف أيضا أنظمة المعلومات أو البنية التحتية أو الشبكات ، كما يمكن أن تكون أو تتحقق هذه الهجمات عن طريق تثبيت برامج التجسس وذلك من خلال وسائل مختلفة من الاعمال الخبيثة وغالبا ترتكب هذه الاعمال أو يكون مصدر هذه الاعمال مجهولا[٣] .

---

(1) Number of Internet Users (2014) Internet live stats

٢) د. يحي ياسين سعود : الحرب السيبرانية في ضوء قواعد القانون الدولي الانساني ، مرجع سابق ، ص ٨٤ .

٣)) د. محمد أحمد: الجريمة الكترونية في المجتمع الخليجي وكيفية مواجهتها ، ٢٠١٦م ، ص ٧

٤) الجريمة الإلكترونية في المجتمع الخليجي وكيفية مواجهتها ٢٠١٦، م ص48

١) د. شريف نسيم قتلة : دليل "تالين" الهجمات الالكترونية وخطر استخدام القوة في القانون الدولي ' المركز العربي للأبحاث الفضاء الإلكتروني ، مصر ، ٢٠١٧م ، ص ١ .

تعد المملكة العربية السعودية من الدول الأوائل في مكافحة الامن السيبراني حصلت على المركز الأول عربياً في مؤتمر الامن السيبراني للاتحاد الدولي وحصلت على المركز الثالث عشر دولياً ، وتقدمت بثلاثة وثلاثون مرتبة عن المؤتمر العالمي للأمن السيبراني عام ٢٠١٦[١]

كما أن طبيعة السلاح المستخدم في الهجوم السيبراني واسع النطاق في تدمير المنشآت الحيوية العامة للدولة المستهدفة والتي قد تصيب مفاصل الدولة بشلل عند وقوع هذا الهجوم ، ونظرا لخطورته فقد نال اهتماما كبيرا لدى الأمم المتحدة ، ووفق للجنة الأسلحة التابعة للأمم المتحدة صدر تعريف للأسلحة غير التقليدية ١٩٦٨م وهو " أسلحة الانفجارات الذرية والأسلحة المصنوعة من مادة ذات نشاط إشعاعي وأسلحة الفتك الكيمائية البيولوجية وأي نوع من الأسلحة الأخرى التي يتم تصنيعها في المستقبل والتي تتشابه خصائصها في الأثر التدميري مع القنبلة الذرية أو الأسلحة الأخرى [٢] .

وتضمنت المادة (٣٦) من البروتوكول الإضافي الأول ١٩٧٧ الملحق باتفاقية جنيف المؤرخة في ١٢ آب ١٩٤٩م بخصوص الأسلحة الجديدة على أنه عند تطوير أو اقناء سلاح جديد يجب التحقق من هذا السلاح عما إذا كان محظورا من عدمه ، كما يستفاد أيضا من هذه المادة على قابلية القانون الدولي الانساني في أن يطبق على الحرب الفضائية باعتبار أن القانون الدولي الإنساني لم يبن تعريف موحدا لفكرة النزاع

---

١) صحيفة الشرق الأوسط الالكترونية (hh//psaawsat.com) منشور في ٢٩ /٣ / ٢٠١٩ م

(٢) د. يحي ياسين سعود : الحرب السيبرانية في ضوء قواعد القانون الدولي الانساني ، مرجع سابق ، ص ٨٤ .

المسلح ولكنه فرق بين النزاع المسلح الدولي والنزاعات المسلحة الداخلية[١] .

ويري البعض أن التقدم التكنولوجي والانترنت والهجوم الذي يمكن أن يتم من خلاله لم يكن متصورا عند التوقيع على الاتفاقيات التي تنظم حالة الحرب سواء قواعد اللجوء الى استخدام القوة أو قواعد ادارة المعارك خلال حالة الحرب لأن هذه الاتفاقيات كانت تنظم حالة الحرب من حيث الزمان والمكان[٢].

ومما يجب ملاحظته أن الهجمات الإلكترونية التي تكون صادرة عن الدولة أو أحد مؤسساتها بقصد إضعاف أو عدم قيام أجهزة الحاسب الآلي بوظائفها لتحقيق اهداف السياسة ، كما تهدف الى الحاق ضرر شامل بالنسبة للأشخاص أو الممتلكات للدولة المقصودة في حين أن الجريمة الإلكترونية يقت صر ضررها على مستخدمين معينين[٣]

٤) د. عمر محمودا عمر الحرب الإلكترونية في القانون الدولي الإنساني ، دراسات علوم الشريعة والقانون ، المجلد ٤٦ ، العدد ٣ ٢٠١٩م ، ص ١٣٩ .

١) د . جميل عبد الباقي الصغير ، الانترنت والقانون الجنائي ، دار النهضة العربية – القاهرة ٢٠٠٢ ص ١٠٠

(٢) د. رزق أحمد سمودي: حق الدفاع عن النفس نتيجة الهجمات الإلكترونية في ضوء قواعد القانون الدولي العام ، بحث منشور في مجلة جامعة الشارقة لعلوم القانونية ، المجلد ١٥ ، العدد ٢ ، ٢٠١٨ ، ص ١٤٦ .

وبعد هذا العرض الموجز يمكن تعريف الحرب السيبرانية بأنها : عبارة عن وسيلة قتالية تستخدم بذاتها للتسلل الى أنظمة الكترونية معدة لسير عمل منشآت حيوية مثل محطات توليد الطاقة النووية ، وسائل النقل وأهمها المطارات ويمكن أن يقال هجوم يتم عبر الانترنت يقوم على التسلل الى مواقع الكترونية مرخص الدخول اليها بقصد إتلاف هذه البيانات أو تعطيلها أو السيطرة عليها[١] .

ولعل الهدف الرئيسي هو الحصول على الربح جراء ارتكاب هذه الجرائم التي ترتكب تمثل قرصنة حقيقة على الحسابات الشخصية فضلا على الاعتداء على البيانات الشخصية وأيضا على استهداف مجموعة من الافراد وحثهم على الكراهية والعدوان على الاخرين[٢].

١) د . رزق أحمد سمودي : مرجع سابق ص ٥٠

٢) محمد أمين الشوابكة المرجع السابق ص ٣١

المطلب الثالث

الحماية الجنائية في التشريعات العربية

في التشريع المصري :

نص قانون مكافحة جرائم تقنية المعلومات الخاصة ، من القوانين الهامة التي تصدت لجرائم الاختراق والقرصنة والاعتداء على شبكات الإنترنت التي تخص الدولة أو الأشخاص الاعتبارية العامة ، كما حمي المشرع الحياة الخاصة التي كفلها الدستور للمراسلات الإلكترونية وعد م افشائها أو التصنت عليها الا بأمر قضائي مسبب .ونصت على ذلك المادة ١٤ على " بعاقب بالحبس مدة لا تقل عن سنة وبغرامة لا تقل عن خمسين الف جنيه ولا تجاوز مائة الف جنيه ، أو بإحدى هاتين العقوبتين ، كل من دخل عمدا ، أو دخل بخطأ غير عمدى وبقى بدون وجه حق ، على موقع أو حساب خاص أو نظام معلوماتي محظور الدخول عليه .

فاذا نتج عن ذلك الدخول إتلاف أو محو أو تغيير أو نسخ أو أعادة نشر للبيانات أو المعلومات الموجودة على ذلك الموقع أو الحساب الخاص أو النظام المعلوماتي ، تكون العقوبة الحبس مدة لا تقل عن مائة جنيه ولا تجاوز مائتي ألف جنيه ، أو بإحدى هاتين العقوبتين " ووفقا للقانون يجوز للمحكمة الاعفاء من العقوبة أو التخفيف منها اذا حصل البلاغ بعد كشف الجريمة وقبل التصرف في التحقيق السلطات المختصة من القبض على مرتكبي الجريمة الاخرين ، أو على ضبط الأموال موضوع الجريمة أو أهان أثناء البحث والتحقيق على كشف الحقيقة فيها ، أو أعان أثناء البحث والتحقيق على كشف الحقيقة فيها ، أو على القبض على مرتكبي جريمة أخرى مماثلة لهذا النوع والخطورة ووفقا لمادة رقم ٤١ من قانون الجريمة الالكترونية فلا يخل حكم هذه المادة ، بوجوب الحكم برد المال المتحصل من الجرائم المنصوص عليها بالقانون .

ولم يكتفى بذلك فقط بل أنشأت مصر بناء على قرار رئيس مجلس الوزراء رقم ٢٢٥٩ لسنة ٢٠١٤ م مجلس أعلي للأمن السيبراني تكون مهمة المجلس التصدي للهجمات السيبرانية وكل ما يخص الانتهاكات الانترنت .[١]

دولــة الامــارات العربيــة المتحــدة : حيث صدر القانون رقم ٢ لسنة ٢٠٠٦ الخاص بمكافحة جرائم تقنية المعلومات حتى صدر في عام ٢٠١٨ المرسوم الاتحادي رقم ٢ لسنة ٢٠١٨ الخاص بتعديل المرسوم الاتحادي رقم ٥ لسنة ٢٠١٢ م وتنص المادة ٣٤ من التشريع الاماراتي على " يعاقب بالحبس مدة لا تقل عن سنة واحدة والغرامة التي لا تقل عن مائيتين وخمسين الف درهم و لا تجاوز مليون درهم ، أو بإحدى هاتين العقوبتين كل من انتفع أو سهل للغير بغير وجه حق الانتفاع بخدمات الاتصالات أو قنوات البث المسموعة أو المرئية وذلك عن طريق الشبكة المعلوماتية أو وسيلة تقنية معلومات " .

دولــة الكويــت : تبنت دولة الكويت حزمة من التشريعات هدفها الرئيسي استخدام وسائل التقنية الحديثة وتجريم كافة الانتهاكات من أمثلة ذلك القانون رقم ٣٧ لسنة ٢٠١٤ م بإنشاء هيئة الاتصالات وتقنية المعلومات ، قانون مكافحة جرائم تقنية المعلومات رقم ٦٣ لسنة ٢٠١٥ م ، كما جرمت المادة الأولى من نظام مكافحة جرائم تقنية المعلومات الكويتي على تجريم جميع أشكال الاعتداء على أدوات التواصل وما يخص الاعتداء المعلوماتي .

١) نشر القرار في الجريدة الرسمية في ديسمبر ٢٠١٤ م العدد الخمسون ١٥ / ١٢ / ٢٠١٤ م

سلطنة عمان : صدر القانون رقم ٧٢ لسنة ٢٠٠١ متضمناً جرائم الحاسب الألى وذلك بإضافة فصل في الباب السابع من قانون الجزاء العماني بعنوان جرائم الحاسب الألي وحماية المتعاملين على شبكات الأنترنت .

المملكة العربية السعودية :

صدر عام ٢٠٠٧ أول نظام خاص حماية أمن المعلومات تحت عنوان " نظام مكافحة الجرائم المعلوماتية وأقره مجلس الوزراء حيث الهدف الرئيسي من النظام هو حماية المجتمع والاقتصاد الوطني والحافظ على الحقوق المترتبة على الاستخدام المشروع للحاسبات الألية و الشبكات المعلوماتية ، المساعدة علي تحقيق الامن المعلوماتي ، المحافظة على الآداب العامة وجرمت المادة الأولى من نظام مكافحة جرائم المعلوماتية السعودي من الأمثلة على ذلك أيضا الاختراق الذى أصاب شركة (SONY) الامريكية عام ٢٠١٤ وكان الهدف من ذلك لمنع الاختراق على برامج الشركة من الملاحظ ان الدول خصصت مبالغ طائلة لأنشاء هيئات و أقسام متخصصة لمعالجة مسائل الاختراق السيبراني ومن أمثلة هذه الدول (الولايات المتحدة الامريكية و استراليا والمملكة المتحدة)[١]

١) عبد الله صادق دحلان، الامن السيبراني علم ينبغي أن يدرس ، تقرير عبر قناة العربية ، ٢٠١٨ .

المطلب الرابع

التكييف القانوني للهجمات الالكترونية على انترنت الأشياء

تعددت اراء الفقهاء حول بيان التكييف القانوني للهجمات الالكترونية

الجريمة السيبرانية لها طبيعة خاصة بها نظرا لصعوبة اكتشافها فضلا على طبيعة ارتكاب الجريمة والسلوك الاجرامي فيها يجعلها من الضرورة ان يتم التركيز عليها لبيان طبيعتها القانونية وكذلك التكييف القانوني لها وقيام الجريمة من خلال شبكات الانترنت .

أولا : صعوبة اكتشاف الجريمة الالكترونية :

نظرا لأنها جريمة مستترة وغير ظاهرة مما يجعل من الصعوبة اكتشافها معرفة الجاني ويتم الجاني بالحرفية الكاملة والاتقان والتمكن من أداء الجريمة من أمثلتها ارسال الفيروسات الى أجهزة الحاسب الالي [١].

فضلا على سهولة التنفيذ من خلال الجهاز بحيث يتم الضغط على زر الفارة أو من خلال لوحة المفاتيح مع الاعداد الكامل من الجاني قبل ارتكاب الجريمة فضلا على طبيعتها ان تتم عن بعد ولا تتطلب وجود الجاني في مكان وقع الجريمة بحيث يستطيع الجاني ارتكابها وهو متواجد في بلد أخرى .

---

١) أ . بشرى عواطة : حجية الدليل الالكتروني في الإثبات الجنائي دار الجامعة الجزائر ص ١٩

ثانيا : الجريمة الالكترونية من الجرائم الحديثة : –

ينظر هذا الاتجاه من الفقه ان الجريمة الالكترونية من الجرائم الحديثة وكنتيجة حقيقية لتقدم التكنولوجي والتطور في أساليب ارتكاب الجرائم فضلا عن ان طبيعة الجريمة تتم من خلال على شبكات الانترنت والبرامج الالكترونية والواصل الالكترونية بصفة عامة فضلا على تنوعها وتطور الأداء الاجرامي من قبل المجرم المعلوماتي[١].

ثالثا : – الجريمة الالكترونية جريمة هادئة: –

أي أنها من الجرائم التي لا تتطلب العنف واستخدام القوة من جانب الجاني ولكنها من الجرائم الهادئة البسيطة سهلة التنفيذ من خلال الجاني نفسه من أمثلتها القراصنة الدخول على أجهزة الحاسب الالي واختراق الحاسبات الشخصية والدخول على بطاقات الائتمان ولا يتطلب الجاني مجهود عضلي لارتكاب الجريمة .

رابعا : الجريمة الالكترونية من الجرائم عابرة الحدود :

وهذه الاتجاه يراى ان الجريمة الالكترونية من السهولة في تحقيقها فهي بحسب طبيعتها تتم من خلال الأقمار الصناعية فهي جريمة تتم من خلال من دولة أخرى وهى بذلك على تعترف بالحدود الإقليمية للدول مما جعل الامر اكثر عولمة الجريمة أمر أكثر ارتكاباً من أقليم دولة أخرى فضلا على الخسائر الكبيرة التي تتسبب فيها هذه الجرائم من أجل التعاون الدولي للحد من هذه الجرائم[٢].

---

١) د .عبد الحى صالح عبد الله مغرب: الأدلة المستخدمة في ارتكاب الجريمة الالكترونية ، مجلة العدل العدد السابع والثلاثون السنة الرابعة عشرة، ص ٢٥

٢) د . عبد العال الدريبي – الجرائم الالكترونية – دراسة قانونية قضائية مقارنة مع أحدث التشريعات العربية في مجال مكافحة جرائم المعلوماتية والانترنت ، المركز القومى للإصدارات القانونية ، القاهرة مصر ٢٠١٢ ص ٥٥

المبحث الثاني

الجهود الدولية لمواجهة الجرائم السيبرانية وحماية انترنت الأشياء

تمهيد وتقسيم :

حظيت الجرائم السيبرانية باهتمام عالمياً حيث عقدت المؤتمرات والندوات لمواجهة هذه المشكلة ، وصدرت في ذلك تشريعات وقوانين لمواجهة هذه الجرائم من أمثلة ذلك مجموعة من الدولة منها السويد حيث تعتبر من أول الدول التي سنت تشريعات لمواجهة هذه الجرائم ونصت على تجريم الاحتيال الكتروني عن طريق الحاسب الألى ، وكذلك جرائم الدخول غير المشروع على البيانات في الحاسوبية أو تزويرها أو تحويلها أو الحصول غير المشروع عليها [١]

المطلب الأول

النماذج العملية للجرائم السيبرانية وحماية تطبيقات انترنت الأشياء

من أمثلة مكافحة الجرائم السيبرانية في الاتي ما تقوم بين الدول على الصعيد الداخلي للحد من انتشار الجرائم السيبرانية وأيضا ما تقوم به الدول من جهود لمكافحة الجرائم السيبرانية من خلال التعاون الدولي سواء على الوطني أو العالمي .[٢]

ومن الدول التي اعتمدت على مصطلحات عديدة لتجريم الجرائم السيبرانية منها جرائم الفضاء الإلكتروني من أمثلتها جرائم التزوير

---

١) د. ابراهيم رمضان عطا : الجريمة الإلكترونية وسبل مواجهتها في الشريعة الاسلامية والانظمة الدولية دراسة تحليلية تطبيقية ، العدد الثلاثون ، الجزء الثاني ، ٢٠١٥م، ص ٣٨٩ ، ٣٩٠ .

٢١) مكتب الأمم المتحدة المعني بالمخدرات والجريمة دراسة شاملة عن الجريمة السيبرانية ص ٣٥ .

الإلكتروني والاحتيال والهكر على الحاسب الآلي من أجل التطبيق القانوني على مستوي أوسع والتدابير الوقائية وتشديد العقوبات من الدول وتكمن أساليب منع الجريمة السيبرانية في مجموعة الاستراتيجيات يعتمد عليها الدول وتنسيق مع بعضها البعض الاخر من خلال الاتي[١] :-

- نشر الثقافة القانونية وخطر على المجتمع .
- تطبيق القانون على تشكيل واسع .
- نشر ثقافة الأمن السيبراني خطورة على المجتمع .

من أمثلة الدول التي أهتمت بمواجهة الجرائم السيبرانية الولايات المتحدة الامريكية حيث شرعت قانونا خاصا لمواجهة الجرائم الإلكترونية في الفترة بين ١٩٧٦ – ١٩٨٥م وحدد أيضا معهد العدالة ١٩٨٥ م على خمسة أنواع رئيسة للجرائم المعلوماتية وهي جرائم الحاسب الآلي داخل الدول ، وجرائم الاستخدام غير المشروع التي تتم عن بعد ،وجرائم التلاعب بالحاسب الآلي ، وجرائم دعم التعاملات الاجرامية وكذا سرقة البرامج والمعلومات المادية للحاسب الآلي[٢] .

وفى عام ١٩٨٥ قامت الولايات المتحدة الامريكية بتعديل تشريعي تضمن اضافة الجرائم السيبرانية منها جرائم التدمير حيث اعطت جهات التحقيق صلاحيات واسعة لمواجهة هذه الجرائم[٣] .

---

١)أ. روان بنت عطية الله : الجرائم السيبرانية ، المجلة الإلكترونية الشاملة ٢٠٢٠ ص ٥ .

(٢) د. ابراهيم رمضان عطا : مرجع سابق ص ٣٩٠

٣) شيخة حسين الزهراني " التعاون الدول في مواجهه الهجوم السيبراني " المجلد ١٧ العدد ٢٠٢٠ مجلة الشارقة للعلوم القانونية ، ص ٧٥١ .

كما ان الهدف لإنترنت الأشياء هو جمع الشبكات في شبكة واحدة عالمية حيث يمكن للسيارة أن تحتوى على عدة أنظمة مستقلة لإدارة والتحكم بالمحرك والأمان ونظام الاتصالات فإن توحيدها كلها في نظام واحد يمكن أن يقلل المعدات والأدوات المستخدمة لذلك ، كما يمكن الاستفادة من تطبيقات انترنت الأشياء في الصيانة الوقائية ومراقبة خطوط الإنتاج وتحسين التغليف والتوريد وأيضا يمكن ان تحسن من مستوي جودة الحياة [١]

-**فرنسا** : تصدت فرنسا لظاهرة الامن المعلوماتي وحماية الانترنت من خلال القانون الفرنسي رقم ١٩ لسنة ١٩٨٨ م الخاص بالتصدي للتزوير المعلوماتي .

-**بريطانيا** : أصدرت قانون مكافحة التزوير والتزييف عام ١٩٨٦ وعالج القانون وعرف ادة التزوير بأنها وسائط تخزين الحاسوبية المتنوعة ، أو أي أداة أخرى يتم التسجيل عليها ، سواء بالطرق التقليدية أو الالكترونية أو بأي طريق من الطرق التقليدية أو الالكترونية أو بأي طريقة أخرى .

الولايات المتحدة الامريكية :

أهمت الولايات المتحدة الامريكية بمكافحة الجرائم الخاصة بالمعلومات والانترنت حيث صدر قانون تقنية المعلومات رقم ٤٧٤ – ٩٩ – ١٠٠ الخاص بجرائم الحاسوب إلى ان تطورت التشريعات

١) أ . عارف بن خميس الفزازى انرنت الأشياء مقالة منشور ٢٠٢٢ م

وقد عقدت عده اتفاقيات دولية لمواجهه هذه الجرائم أهمها :-

اتفاقية المجلس الأوربي :

من نتائج التقدم التكنولوجي في كافة المجالات الحديثة في مجال الانترنت مما جعله سببا رئيسياً في اعادة العقوبات المشددة لمواجهة هذه الجرائم [١]

معاهدة بودابيست لمكافحة الجرائم السيبرانية

في ٢٣/ ١١/ ٢٠٠١م تم توقيع معاهدة التعاون " بودابست "لمكافحة الجرائم الإلكترونية وتعتبر معاهدة بودابست من اهم المعاهدات المتعلقة لمكافحة جرائم الانترنت وهذه على التعاون والتضامن الدولي لمرتكبي هذه الجرائم ، وقعت (٢٦) دولة على هذه المعاهدة بالإضافة إلى كندا واليابان والولايات المتحدة الامريكية وتضمنت (٤٨) مادة لمعاقبة مرتكبي هذه الجرائم ، وبالرغم من أن هذه المعاهدة أوربية المنشأ الا أنها متاحة للدول غير الاوربية للانضمام اليها [٢]

وتعتبر الجرائم السيبرانية من أكثر الجرائم شيوعياً علي المستوي الدولي من أمثلتها جرائم الارهاب الإلكتروني ، كما نصت هذه المعاهدة على كيفية التحقيق في الجرائم الإلكترونية ، كما تعهدت الدول الموقعة على هذه المعاهدة أن تعاون لمكافحة هذه الجرائم ، وليس هذا فحسب بل حاولت هذه المعاهدة إقامة التوزان بين المقترحات التي نفذتها أجهزة الشرطة وما

١)شيخة حسين الزهراني " التعاون الدول في مواجهه الهجوم السيبراني " المجلد ١٧ العدد ٢٠٢٠ مجلة الشارقة للعلوم القانونية ، ص ٧٥٤ .

٢) د . محمد عبد الحميد السيد " حماية المجتمع من الجرائم المعلوماتية " دراسة مقارنة دار النهضة العربية ٢٠١٠ ص٥٠

عبرت عنه المنظمات المدافعة عن حقوق الانسان وخدمات الأنترنت حيث أهتمت منظمات حقوق الانسان من المساس بحقوق الانسان أو أن يرتب على الرقابة على انتهاك لحقوق الافراد مستخدمي الانترنت[١]

المطلب الثاني

التعاون الدولي وحماية انترنت الأشياء

يتحقق ذلك من خلال ما تضمنته الاتفاقية الاوربية لمكافحة جرائم الانترنت بوجه عام ونموذج الاتحاد الأوروبي وتضمن الاتحاد اليات وإجراءات مكافحة الجرائم السيبرانية وذلك في عام ٢٠٠٠ من خلال تجريم كافة الجرائم الخاصة بالسرقات ومنع جرائم السرقة الكترونية من خلال رابطها أجهزة الحاسب الالي من خلال لجنة خاصة لمكافحة القرصنة وللجنة صلاحيات واسعة لاتخاذ ما تراه مناسباً للحد من هذه الجرائم[٢]

ومن أهم الأمثلة في ذات السياق مؤتمر الإنتربول واليورو بول الثامن لمكافحة الجريمة السيبرانية الذى عقد في أكتوبر ٢٠٢٠ بحضور أكثر من ٤٠٠ خبير دولي في مجال مكافحة الجرائم السبيرانية وتضمن ذلك تقرير الأمين العام للإنتربول السيد يورغن شتوك " إن عالما يتجاوز فيه عدد مستخدمي الانترنت ٤,٥ مليارات شخص يعني أن أكثر من نصف البشرية معرض للخطر الوقوع ضحية الجريمة السيبرانية في أي وقت [٣].

---

١) د. شيخة حسين زهراني: التعاون الدول في مواجهه الهجوم السيبراني ، مرجع سابق ص ٧٥٥ .

(2) Dommages : -inerets a payer par les members mineurs du forum Utopi-Board; jeudi 10 janvier, 2019. P .50

٣) مؤتمر الإنتربول واليورو بول الثامن لمكافحة الجريمة السيبرانية : نصف البشرية معرض للخطر ٦ أكتوبر ٢٠٢٠

وصف المؤتمر الجريمة الإلكترونية هي جريمة فعلية التي تركز علي ستة من تهديدات الجريمة الالكترونية كما ركز المؤتمر أيضا على التحديات المستقبلية التي يتعين مواجهتها ودعا أجهزة إنفاذ القانون والحكومات وكذلك المنظمات غير الحكومية إلى أتباع نهج مرن واستباقي في مجال الأمن السيبيري .

كما يساعد الانتربول البلدان الأعضاء على مكافحة الجرائم السيبرانية من خلال اجراء تحقيقات في الجرائم السيبرانية وذلك لحد منها والتنسيق الكامل بين الدول الأعضاء في اجراء المعلومات عن التهديدات لتوجيه أعمالها لمكافحة مثل هذه الجرائم ومن أهم الجهود التي يقدمها الانتربول تكمن في نشر تقارير لتنبيه البلدان إلى تهديدات سيبريه جديدة وشيكة أو متطورة ، وتشمل هذه التوعية للدول الأعضاء من البرامج الخبيثة ورسائل التصيد الاحتيالي والمواقع الالكترونية الحكومية المخترقة والاحتيال باستخدام الوسائل الحديثة[1].

وأيضا ما نصت عليه المادة (١٤) من الاتفاقية العربية لمكافحة الجرائم المعلوماتية جريمة الاعتداء على حرمة الحياة الخاصة باعتبارها جريمة معلوماتية بأنها " الاعتداء على حرمة الحياة الخاصة بواسطة تقنية المعلومات " .

وأيضا ما نصت عليه المادة (٢١) من الاتفاقية العربية لمكافحة الجريمة المنظمة عبر الحدود الوطنية على " تتعهد كل دولة طرف أن تتخذ ما يلزم من تدابير في إطار قانونها الداخلي لتجريم ارتكاب أو المشاركة في ارتكاب أو المشاركة في ارتكاب الأفعال الاتية التي تقوم بها جماعة إجرامية منظمة في نطاق الاستعمال غير المشروع لقنية أنظمة المعلومات الاختراق

١) الانتربول السعودي وكيفية مواجهة الجرائم الالكترونية تقرير وزارة الداخلية

غير المشروع أو تسهيل الاختراق غير المشروع على نحو كلي أو جزئي لأحد نظم المعلومات – تعطيل أو تعريف تشغيل أحد نظم المعلومات – إدخال بيانات بطرق غير مشروعة في أحد نظم المعلومات أو مسح وتعديل أو نسخ أو نشر البيانات التي يحتويها هذا النظام بطريق غير مشروع – استيراد أو حيازة أو عرض أو ترك أو إتاحة إحدى المعدات أو الأدوات أو برامج تقنية بدون سبب مشروع بهدف ارتكاب احدى الجرائم المنصوص عليها في

الفقرات الثلاث السابقة – أي جريمة من الجرائم التقليدية ترتكب بإحدى وسائل تقنية أنظمة المعلومات(١).

وفى ذات السياق تضمن البروتوكول الإضافي لاتفاقية الجريمة الالكترونية المنعقدة في فرنسا ستراسبورغ ٢٠٠٨ بشأن تجريم الأفعال ذات الطبيعة العنصرية ، التي تحرض على الكراهية والتي يتم ارتكابها عن طريق الحاسب الالي حيث نصت في المادة الخامسة منها تجريم الاتي :

- نشر المواد التي تتعلق بالعنصرية وكراهية الأجانب عبر أجهزة الحاسب الالي .
- التهديد الذى تحركه دوافع التمييز العنصرية وكراهية الأجانب .
- الإهانة التي تحركها دوافع التمييز العنصري وكراهية الأجانب .
- الانكار أو التقليل أو الموافقة أو تبرير جرائم الإبادة الجماعية وجرائم ضد الإنسانية(٢).

---

١)الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المحررة بالقاهرة بتاريخ ٢١ / ١٢ / ٢٠١٠ م

(٢) د. نهلا عبد القادر المومني : جرائم المعلوماتية ، دار الثقافة للنشر والتوزيع ، عمان ، الأردن ، ط١ ٢٠٠٨ ص ١٧٣ ، ١٧٤

وتعد الاتفاقيات والمعاهدات الثنائية خير دليل على الحد من هذه الجرائم على الصعيد الدولي حيث تنص على ذلك المادة ٤ من اتفاقية الجريمة المنظمة " تودي الدول الأطراف التزاماتها بمقتضي هذه الاتفاقية علي نحو يتفق مع مبادى المساواة والسيادة والسلامة الإقليمية للدول من خلال ذلك يتم التعاون الدولي وتسليم المجرمين ، فضلا عن ذلك التعاون الدولي وتقديم(المساعدات القانونية المتبادلة)[١].

ومن الصعوبات التي تواجه الدول على الصعيد الدولي تكمن في صعوبة الحد من هذه الجرائم على الرغم من الجهود الدولية المبذولة الا ان ذلك يتطلب بالضرورة مواجهة مجموعة من الصعوبات التي تواجها الدول لمحاولة التصدي لمثل هذا النوع من الجرائم ومن أهم هذه الصعوبات :

-عدم كفاية التشريعات في مكافحة مثل هذا النوع من الجرائم والتصدي له بشكل فعال .

-عدم قيام الجهات المعتدى عليها بتبليغ السلطات عند حدوث مثل هذا من الجرائم مما يكون له الأثر الكبير في عدم اكتشاف مثل هذه الجرائم والحد منها .

- سهولة ارتكاب مثل هذه الجرائم بصفة مستمرة [٢].

- عدم التنسيق مع الدول في القوانين الإجرائية في مجال التحري والتحقيق الجنائي للحد من هذه الجرائم وعدم التعاون الدولي .

- عدم التدريب الجاد والخبرة الكافية من أجل الحد من هذه الجرائم على المستوى الدولي .

1) Brownlie: Public International Law ,6, ed Oxford University press I,2003,.p. 306 (٢

٢) الجريمة الكترونية وسبل مكافحتها مرجع سابق ص ٥٠

- عدم اتخاذ التدابير المانعة والوقائية من الدول قبل وقوع الجريمة بشكل كافي[١] .
- سهولة ارتكاب الجريمة وعدم اكتشافها في وقت قصير .
- تعدد وتنوع المجرمين واستخدام وسائل وتكنولوجية جديدة من أجل تحقيق هذه الجرائم .
- عدم وجود تشريع دولي موحد للتامين الحماية للبيانات على المستوي القومي للحد من هذه الجرائم في المستقبل[٢] .

ومن ابرز الجهود الدولية لمحاربة الجرائم السيبرانية ما قامت به كوريا حيث اسفرت الجهود الى محاربة البرامج الخبيثة مما اسفر عن اعتقال أشخاص كثيرين ، وفى نيجريا بتاريخ ١٩ يناير ٢٠٢٢ م القت الشرطة النيجيرية تم القبض على ١١ شخصا يشتبه في انتمائهم إلى شبكة جريمة السيبرانية ناشطة جدا تم ذلك بمعرفة الإنتربول وذلك بمعرفة وحدة مكافحة الجريمة السيبرانية التابعة للقوات النيجرية من ابراز ما قامت به هذه الوحدة تم التواصل إلى رصد جرائم احتيال BEC التي ارتكبها المشتبه فيهم بشكل جامعي قد تكون مرتبطة بأكثر من ٥٠٠٠٠ جهة مستهدفة[٣].

وفى ذات السياق يعد ما قامت به سنغافورة على قيادة عمليةFalcon لمكافحة الجرائم السيبرانية وذلك على سبيل الاحتيال بإصدار أومر غير حقيقة من أجل الابتزاز الالكتروني لتحويل الأموال وتعد جهود الانتربول

---

١) د. وقائي بغدادي : حماية وتأمين الانترنت التحدي القادم وأساليب المواجهة ، سلسلة العلوم والتكنولوجيا ، الهيئة المصرية العامة للكتاب ، القاهرة ، ٢٠١٠ م ص ١٥٦

٢) د . أحمد الشربجي المرجع السابق ص ٥٠

٣) صفحة الانتربول الدولي ١٩ يناير ٢٠٢٢ م تقرير منشور مجلة العدالة ص ٢٠

لمكافحة هذه الهجمات وذلك بعد الانضمام وتفعيل مبادرة Gateway حيث تم التواصل القبض على العصابات المنظمة وذلك من خلال تحقيق الشراكات بين أجهزة إنفاذ القانون والقطاع الخاص بهدف جمع البيانات المتعلقة بالتهديدات التي تقع على الجهات المختلفة وقيام أجهزة الشرطة من التصدي لمثل هذه الهجمات ، ومن الجهود التي يقوم بها الانتربول لمكافحة الجريمة السيبرانية القضاء على عمليات القرصنة على العملات المشفرة حيث قام الانتربول ونسق عملية Goldfish Alphas في جنوب شرق اسيا التي كشفت بداية عن أكثر من ٢٠٠٠٠ موجه مقرصن وتعاون محققون وخبراء في مكافحة الجريمة السيبرانية من أجهزة الشرطة للحد من هذه الجرائم في المستقبل وأيضا من خلال جرائم المواقع الالكترونية المخترقة وذلك للحد من القراصنة على المواقع ومن ضمن العمليات التي قام بها الانتربول للحد من هذه الجرائم عمليات cyber surge وفى الولايات المتحدة الامريكية اتخذت البلدان المشاركة إجراءات ميدانية لتعطيل انتشار مثل هذه الجرائم حيث دلت الإحصاءات الى الحد من ٤٠ حالة تصيد احتيالي وكشف ٢٦ موقعا الكترونيا حكوميا متضررا [١].

١) صفحة الانتربول interpol.int arn4 62

المبحث الثالث

المواجهة الجنائية لمخترقي تطبيقات انترنت الأشياء

هو ما يظهر جلياً لنا من خلال توفر المسؤولية الجنائية وعن ذلك أصدرت محكمة باريس حكما قضت فيه " أن مساهمة مقدم خدمات الأنترنت في بث معلومات غير مشروعة حيث اعتبرته المحكمة تدخل في ارتكاب الجريمة يستوجب العقاب الامر الذى يتم من خلاله ادانته إلى جانب الفاعل الأصلي للجريمة .

وفى هذا الشأن نجد ان القانون الأمريكي (DMCA)حدد مساءلة مقدمي خدمات الإنترنت جنائيا في حدود الاعتداء على حقوق الملكية الفكرية في نطاق الإنترنت، فأقام مسؤوليتهم فقط في حال علمهم بعدم مشروعية المضمون المعلوماتي الإلكتروني الذي يقومون بنقله أو تخزينه. ويثبت علمهم هذا في حالتين: الأولى: أن تكون عدم المشروعية ظاهرة إلى حدٍّ لا يُمكن تجاهلها، والثانية: قيام السلطات الأمريكية المختصة أو الشخص المتضرر من نشر المضمون المعلوماتي بإبلاغ مقدم الخدمة بوجه عدم المشروعية. فإذا ما تحقق علمه بعدم المشروعية، وعلى وجه الخصوص بالعمل المقلَّد أو المنسوخ بصورة غير شرعية، توجب عليه المبادرة إلى اتخاذ موقف إيجابي بشطب المضمون الإلكتروني غير المشروع، أو على الأقل منع وصوله لجمهور مستخدمي الشبكة. وبخلاف ذلك، يُعدُّ مقدم الخدمة مُخلاً بالتزاماته، مما يستوجب قيام مسؤوليته[١].

ولكي تنتفي مسؤولية مقدمي خدمات الإنترنت الجنائية ، بشكلٍ كُلِّي، وفي إطار مساعدتهم للسلطات العامة في الدولة في مُحاربة جرائم انتهاك

١) إبراهيم رمضان إبراهيم عطايا ، الجريمة الالكترونية وسبل مواجهتها في الشريعة الإسلامية والأنظمة الدولية كلية الشريعة والقانون ٢٠١٤ م مرجع سابق ص ٦٠

حقوق الملكية الفكرية، وحرمات الحياة الخاصة وقداسة الأديان وجرائم الحث على المشاعر العنصرية، والاعتداء الجنسي على الأطفال، فإنهم مُطالبون، أيضاً، وفقاً لنص الفقرة الثالثة من المادة ٦-٧/٢ من القانون الفرنسي حول "الثقة في الاقتصاد الرقمي"، والتي جاءت متفقةً مع الاتجاه العام للمواد ١٣ و١٤ من التوجيه الأُوروبي حول "التجارة الإلكترونية"، ومع المادة ٣/g/٥١٢ من القانون الأمريكي (DMCA)، والخاصة بالتعدي على حقوق الملكية الفكرية في نطاق الإنترنت، بأن يضعوا تحت تصرُّف عملائهم الوسائل اللازمة لتسهيل عملية التبليغ عن أيٍّ مخالفات قد تتم عبر الشبكة. وبعد تحقق مقدم الخدمات من صحة موضوع التبليغ ومن عدم مشروعية المضمون الإلكتروني عليه أن يُبادر فوراً إلى إبلاغ السلطات العامة في الدولة عن هذه الواقعة، وذلك من أجل استصدار أمرٍ إداريٍّ أو قضائيٍّ بشطب هذا المضمون، أو منع وصوله لمستخدمي الشبكة.

المطلب الأول

صور المواجهة الجنائية لجرائم انترنت الأشياء

- جريمة اختراق انترنت الأشياء

من احدث الإحصاءات التي تدل عليها الجهات ان حوالى ما يقرب من ١١.٦ مليار جهاز إنترنت الأشياء في عام ٢٠٢١ م لابد ان تكون مؤمنة تماما ضد أي محاولة اختراق [١].

- القرصنة : وهى عبارة عن أعمال من شأنها الوصول الى البيانات بطريقة غير مشروعة والدخول عليها باي طريقة كانت من اجل الحصول على المعلومات وذلك من خلال استغلال الثغرات من بعض الأنظمة[٢].
- الجرائم الالكترونية ضد الافراد : هي الجرائم التي تهدد الحياة الخاصة للأفراد وتشمل أيضا التشهير والاساء على مواقع التواصل الاجتماعي .
- الجرائم الالكترونية على الممتلكات : من خلال الدخول على أجهزة الحاسب الالي وسرقة ما بها من معلومات وانتهاك خصوصية حقوق النشر والملكية .
- الجرائم الالكترونية ضد الحكومات : وهى الجرائم التي تمثل انتهاك لسيادة الدول والوصول الى معلومات سرية ويمكن من خلالها الى شن الحروب والاعمال الإرهابية [٣].

-تزوير المعلومات من خلال اختراق النظام التعليمي وتغير المعلومات المدونة به[٤].

1(https//www.jigsawacademy.com

2) Types of Cyber Crime: HOW Cybersecurity professionals prevent Attacks 6-5-2020 ,Retrieved 13-2-2021

3(WWW.Pandasecurtiy .com,retrieved13-12-2021

٤) إبراهيم رمضان إبراهيم عطايا ، الجريمة الالكترونية وسبل مواجهتها في الشريعة الإسلامية والأنظمة الدولية كلية الشريعة والقانون ٢٠١٤ م ص ٣٢ .

من أحدث الإحصاءات التي تدل على زيادة الجرائم الالكترونية حيث وصلت تكلفة الهجمات الى ما يقارب ٦ ترليون دولار عام ٢٠٢١ م وان تكلفة خسائر الشركات العاملة في هذا المجال من شركات تحليل البيانات نتيجة الخرق الواحد ما يقارب ٤ مليون دولار ونرى انها تكلفة كبيرة جدا وهذه الدارسة قام بها معهد بونيمون في عام ٢٠١٦ م[١].

بعض الأمثلة على استخدام الجرائم الالكترونية الاعتداء والقرصنة على شركة ياهو عام ٢٠١٦ م من سرقة مستخدم والحصول على ملايين المعلومات الخاصة وكلمات المرور من هذه الحسابات وتمكن المهاجمون من الوصول الى حسابات المستخدمين في خدمات عبر مواقع التواصل الاجتماعي ، وأيضا الاعتداء على سرقة متاجر التجزئة الامريكية حيث اخترقت أنظمة نقاط البيع وسرقة المهاجمون ٥٠ مليون بطاقة ائتمانية شخصية وحصلوا على تفاصيلها ، ومن الأمثلة الأخرى عام ٢٠١٧ م أغلقت خلال هذا الهجوم محتوى ٣٠٠٠٠ جهاز كمبيوتر حول العالم ، وطلب من المستخدمين دفع مبالغ مالية مقابل فك التشفير وإتاحة وصولهم لبياناتهم مرة أخرى [٢].

ويعد من صور الاحتيال عبر البريد الالكتروني والانترنت .

- تزويد الهوية (حيث تتم سرقة المعلومات الشخصية واستخدامها)
- سرقة البيانات المالية أو بيانات الدفع بالبطاقة .
- سرقة بيانات الشركة وبيعها .
- الابتزاز الالكتروني (طلب المال لمنع هجوم مهدد) والتهديد به .
- هجمات برامج الفدية كنوع من (الابتزاز الالكتروني).

1 (WWW.Pandasecurtiy .com,retrieved13-12-2021

2 (types ;EXaples ,and what your Buiness can Do ,www.exabeam.com,Retieved13-2-2021

- الهجمات والقراصنة من جانب التشكيلات العصابية الدولية .
- الهجرس على المواقع الرسمية و الخاصة والفردية من خلال الابتزاز على المواقع .
- من صورها أيضا سرقة مبالغ كبيرة واختراق حسابات البنوك .
- تدمير الأنظمة العسكرية لبعض الدول عن طريق الحرب الالكترونية المنظمة .
- سرقة الملكية الفكرية وحقوق النشر والطباعة وغيرها .
- سرقة الحسابات عن طريق الهجوم الإلكتروني المنظم على الحسابات الجارية للأفراد [١].
- جرائم الفيروسات والبرامج الخبيثة من أشهر هذه الفيروسات عام ٢٠١٧م ما يعرف فيروس الفدية ودمر أجهزة كبيرة في دول كثيرة .
- الجرائم الالكترونية تتم بشكل يومي كل يوم تحصل مع الافراد والجماعات والمؤسسات والشركات والبنوك الدول الأخرى فهي ظاهرة تهدد المجتمعات بصفة مباشرة .
- جرائم استغلال الثغرات الأمنية : وهى جرائم الكترونية تهدف الى استغلال ثغرات امنية موجودة في الأنظمة الالكترونية للحصول على معلومات كثيرة وذلك بواسطة محترفين في هذا المجال وذلك من خلال برامج متقدمة في هذا المجال مع الاحترافية العالية في نظام الدخول واستغلال الثغرات الأمنية [٢].

من أحدث التطبيقات على الجرائم الالكترونية ما قامت به النيابة العامة المصرية بتقديم ٥ أشخاص الى المحاكمة الجنائية في اتهامهم بتهديد

1 (info@cyberone.com
2(m https ;llcyberone.co

طفلتين شقيقتين ونشر صور خادشه منسوبة لإحداهما التي أقدمت على الانتحار وان الجناة يواجهون اتهامات بتهديد المجنى عليها الطفلة هايدي وشقيقتها عبر تطبيق للتواصل الاجتماعي وافشائهم صورا تكشف حياتها الخاصة وعلى المبادئ والقيم الأسرية في المجتمع المصري [1] التصنت والتجسس والتشهير وانتهاك الخصوصية و السرقة العلمية و افشاء الاسرار الإرهاب الالكتروني [2].

١) جريدة الشرق الأوسط الاحد ٦ فبراير ٢٠٢٢

٢) رفد عبادة الهاشمي ، الإرهاب الالكتروني القانوني ، دار أمجد للنشر والتوزيع العراق ، ٢٠٢٠ ص ١٤٠ .

الخاتمة

بعد أن تناولنا موضوع البحث من خلال تناول في **المبحث الاول: مفهوم انترنت الأشياء** .

المطلب الأول مفهوم الامن السيبراني أما عن المطلب الثاني تناولنا فيه تعريف الحماية الجنائية من الهجمات السيبرانية على انترنت الأشياء ، في حين تناولنا في المطلب الثالث أنواع الهجمات السيبرانية ، أما عن المطلب الرابع تناولت فيه التكييف القانوني للهجمات السيبرانية ، كما تم تقسيم **المبحث الثاني** وتناول **الجهود الدولية لمواجهة الجرائم السيبرانية وحماية انترنت الأشياء** ، المطلب الأول النماذج العملية للجرائم السيبرانية في حين تناول

المطلب الثاني التعاون الدولي في مواجهة الجرائم السيبرانية ، وتناولت في المطلب الثالث صور جرائم انترنت الأشياء ، وتناولنا في **المبحث الثالث** المواجهة الجنائية لمخترقي تطبيقات انترنت الأشياء ، **أما عن** المطلب الأول صور المواجهة الجنائية لجرائم انترنت الأشياء .

أولا : النتائج

- يتضح لنا من العرض السابق في ثنايا البحث مجموعة من النتائج :
- زيادة انتشار جرائم شبكة الانترنت من خلال برامج اختراق انترنت الأشياء .
- أغلب الدول تولى اهتماماً بمفاهيم تكنولوجيا انترنت الأشياء .
- يمكن استخدام انترنت الأشياء في المواقع البعيدة حيث يكون الوصول المادي مكلفاً .
- يستخدم انترنت الأشياء في حل المشكلات الخاصة بالتواصل الاجتماعي المعرضة للاختراق من قبل محترفي هذه الجرائم .
- هناك حلولا تشريعية وعمليه يمكن من خلالها مواجهة جرائم انترنت الأشياء .
- تبين لنا من خلال العرض السابق ان الجهود الدولية في مواجهة جرائم انترنت الأشياء لم تعد كافية نتيجة لتطور الجرائم والاعتداء بصورة متكررة واختراق شبكات الانترنت .

التوصيات :

-نوصى المشرع ان يتدخل بالنص صراحة على الجرائم الواقعة على اختراق تطبيقات انترنت الأشياء وزيادة الحماية الفاعلة .
- تنشأ بمقر وزارة العدل والداخلية إدارة خاصة تكون مهمتها الاهتمام بجرائم انترنت الأشياء لضمان الفاعلية الكاملة لها والتصدي لكافة محاولات التهديد المعلوماتي .
- تدريب القضاة على كل ما هو جديد فيما يخص جرائم انترنت الاشياء مع النص صراحة في القوانين المنظمة للإثبات الجنائي بما يسمح للقضاة من الاستناد إلى الأدلة المستخرجة من الحاسب الالي والانترنت في الاثبات .

- نشر الوعى والثقافة بين المتعاملين مع انترنت الأشياء وخاصة مع ما يتعلق بالاختراق المعلوماتي لشبكات بطريقة خاطئة .
- الاهتمام بطريقة اكثر فاعلية من خلال تحقيق استراتيجية موحدة في أطار التعاون الدولي للحد من جرائم اختراق انترنت الأشياء .
- زيادة الندوات والمؤتمرات التي تنادى باستخدام انترنت الأشياء من المخاطر التي تهدد تطبيقات انترنت الأشياء .
- عدم الاحتفاظ بأية معلومات شخصية في داخل جهازك كالرسائل والصور الخاصة أو الملفات المهمة وغيرها من معلومات بنكية .
- عدم أعطاء أي بيانات أو معلومات شخصية ، مثل أرقام الحسابات ، عبر الهاتف أو الإفصاح عنها ما لم تكن الخطوات امنة .
- تعديل قواعد وإجراءات المحاكمة الجنائية في مثل هذه الجرائم .
- النص صراحة على تجريم الدخول غير المصرح به الى البريد الإلكتروني لإتلاف محتوياته أو إرسال رسائل وتغيرها عبر الانترنت .
- ادخال مادة دراسية تدرس ضمن صفوف المناهج الدراسية تسمي " اخلاقيات استخدام الانترنت "

قائمة المراجع

أولاً: – مراجع باللغة العربية:

أ–الكتب الرئيسية :

a-alktb alr2ysya :

– د. ادهم طارق الحماية الجنائية للحياة الخاصة عبر الانترنت دراسة مقارنة ٢٠٠٧م.

- d. adhm 6ar8 al7maya algna2ya ll7yaa al5asa 3br alantrnt drasa m8arna 2007m.

– رفد عبادة الهاشمي ، الإرهاب الالكتروني القانوني ، دار أمجد للنشر والتوزيع العراق ، ٢٠٢٠ م

- rfd 3bada alhashmy ،al erhab alalktrony al8anony ،dar amgd llnshrwaltozy3 al3ra8 ، 2020 m

- روان بنت عطية الله : الجرائم السيبرانية ، المجلة الإلكترونية الشاملة ٢٠٢٠ .

- roan bnt 36ya allh : algra2m alsybranya ،almgla al elktronya alshamla 2020 .

- د. شريف نسيم قتلة : دليل "تالين" الهجمات الالكترونية وخطر استخدام القوة في القانون الدولي ، المركز العربي للأبحاث الفضاء الإلكتروني ، مصر ، ٢٠١٧م .

- d. shryf nsym 8tla : dlyl "talyn" alhgmat alalktronyaw56r ast5dam al8oa fy al8anon aldoly , almrkz al3rby llab7ath alfda2 al elktrony , msr , 2017m .

- د. محمد أحمد: الجريمة الكترونية في المجتمع الخليجي وكيفية مواجهتها ، ٢٠١٦م .

- d. m7md a7md: algryma alktronya fy almgtm3 al5lygywkyfya moaghtha , 2016m .

- أ . محمد –أمين الشوابكة : جرائم الحاسوب والانترنت (الجريمة المعلوماتية) – دار الثقافة للنشر والتوزيع ، عمان ، الأردن ٢٠٠٩ ص ٦
- a . m7md -amyn alshoabka : gra2m al7asobwalantrnt (algryma alm3lomatya) – dar alth8afa llnshrwaltozy3 ، 3man ،alardn 2009 s 6
- أ. أحمد عبد الحميد ،الجريمة الإلكترونية في المجتمع الخليجي وكيفية مواجهتها ، ٢٠١٦، م .
- a. a7md 3bd al7myd ،algryma al elktronya fy almgtm3 al5lygywkyfya moaghtha , 2016 ،m .
- شيخة حسين الزهراني " التعاون الدول في مواجهه الهجوم السيبراني " المجلد ١٧ العدد ٢٠٢٠ مجلة الشارقة للعلوم القانونية .
- shy5a 7syn alzhrany " alt3aon aldol fy moaghh alhgom alsybrany " almgld 17 al3dd 2020 mgla alshar8a ll3lom al8anonya .
- د. يحيى بن سعود : الحرب السيبرانية في ضوء قواعد القانون الدولي الإنساني .
- d. y7yy bn s3od : al7rb alsybranya fy do2 8oa3d al8anon aldoly al ensany .
- د. وقائي بغدادي : حماية وتأمين الانترنت التحدي القادم وأساليب المواجهة ، سلسلة العلوم والتكنولوجيا ، الهيئة المصرية العامة للكتاب ، القاهرة ، ٢٠١٠ م .
- d.w8a2y bghdady : 7mayawtamyn alantrnt alt7dy al8admwasalyb almoagha ،slsla al3lomwaltknologya ،alhy2a almsrya al3ama llktab ،al8ahra ،2010 m .
- د . عبد العظيم مرسى وزير : الشروط المفترضة في الجريمة ، دار النهضة العربية ، مصر ١٩٨٣ .

- d . 3bd al3zym mrsywzyr : alshro6 almftrda fy algryma ،dar alnhda al3rbya ،msr 1983 .
- د . جميل عبد الباقي الصغير ، الانترنت والقانون الجنائي ، دار النهضة العربية – القاهرة ٢٠٠٢ .
- d . gmyl 3bd alba8y alsghyr ،alantrntwal8anon algna2y ،dar alnhda al3rbya – al8ahra 2002 .
- هلالي عبد اللاه أحمد : اتفاقية وأدبست لمكافحة جرائم المعلوماتية " معلقا عليها ، دار النهضة العربية القاهرة ، ٢٠١١ .
- hlaly 3bd allah a7md : atfa8yawadbst lmkaf7a gra2m alm3lomatya " m3l8a 3lyha ،dar alnhda al3rbya al8ahra ،2011 .
- د . مأمون محمد سلامة شرح قانون العقوبات القسم الخاص ، دار النهضة العربية ٢٠٠٠
- d . mamon m7md slama shr7 8anon al38obat al8sm al5as ،dar alnhda al3rbya 2000
- نهلا عبد القادر المومني : جرائم المعلوماتية ، دار الثقافة للنشر والتوزيع، عمان ، الأردن ٢٠٠٨ .
- nhla 3bd al8adr almomny : gra2m alm3lomatya ،dar alth8afa llnshrwaltozy3 ،3man ،alardn 2008 .

ب– الرسائل العلمية المقالات والدوريات

b- alrsa2l al3lmya alm8alatwaldoryat

- أ . بشرى عواطة : حجية الدليل الالكتروني في الإثبات الجنائي دار الجامعة الجزائر ٢٠١٧ م
- a . bshry 3oa6a : 7gya aldlyl alalktrony fy al ethbat algna2y dar algam3a algza2r2017 m
-) أ . عارف بن خميس الفزاري مقالة منشورة عام ٢٠٢٢ م
-) a . 3arf bn 5mys alfzary m8ala mnshora 3am 2022 m

- د. ابـراهيم رمضـان عطـا : الجريمـة الإلكترونيـة وسـبل مواجهتهـا فـي الشـريعة الاسـلامية والانظمـة الدوليـة دراسـة تحليليـة تطبيقيـة ، العـدد الثلاثون ، الجزء الثاني ، ٢٠١٥م .
- d. abrahym rmdan 36a : algryma al elktronyawsbl moaghtha fy alshry3a alaslamyawalanzma aldolya drasa t7lylya t6by8ya ، al3dd althlathon ،algz2 althany , 2015m .
- د. ايهاب خليفة : ما هو موقف ميثاق الامم المتحدة من استخدام القوة السـيبرانية فـي التفـاعلات الدوليـة – مقـال صـادر عـن مركـز المسـتقبل للأبحـاث والدراسـات المتقدمـة – ابـوظبي – الامـارات العربيـة المتحـدة ، ٢٠١٩م ، ص ٢ ، ٣ .
- d. ayhab 5lyfa : ma ho mo8f mytha8 alamm almt7da mn ast5dam al8oa alsybranya fy altfa3lat aldolya – m8al sadr 3n mrkz almst8bl llab7athwaldrasat almt8dma – abozby – alamarat al3rbya almt7da , 2019m , s 2 , 3 .
- الرائـد / حسـن فيـاض : الهجمـات السـيبرانية مـن منظـور القـانون الـدولي الانساني ، مجلة الدفاع الوطني ، لبنان ، العدد 14 ، ٢٠٢٠م .
- alra2d / 7sn fyad : alhgmat alsybranya mn mnzor al8anon aldoly alansany ،mgla aldfa3 alo6ny ،lbnan ،al3dd 14 ، 2020m .
- د. رزق أحمـد سـمودي : حـق الـدفاع عـن الـنفس نتيجـة الهجمـات الإلكترونية في ضوء قواعد القانون الدولي العام ، بحث منشور في مجلة جامعة الشارقة لعلوم القانونية ، المجلد ١٥ ، العدد ٢ ٢٠١٨م
- d. rz8 a7md smody : 78 aldfa3 3n alnfs ntyga alhgmat al elktronya fy do2 8oa3d al8anon aldoly al3am , b7th mnshor fy mgla gam3a alshar8a l3lom al8anonya , almgld 15 , al3dd 2 2018m
- د. طلال ياسين العيسى ، عدي محمد غياب : المسئولية الدولية الناشئة عن الهجمات السيبرانية في ضوء القانون الدولي المعاصر، مجلة الزرقاء

للبحوث والدراسات الإنسانية ، الأردن ، المجلد التاسع عشر ، العدد الأول ، ٢٠١٩م .

- d. 6lal yasyn al3ysy , 3dy m7md ghyab : alms2olya aldolya alnash2a 3n alhgmat alsybranya fy do2 al8anon aldoly alm3asr, mgla alzr8a2 llb7othwaldrasat al ensanya , alardn , almgld altas3 3shr , al3dd alaol , 2019m .

- د. يحي ياسين سعود : الحرب السيبرانية في ضوء قواعد القانون الدولي الانساني ، بحث منشور في المجلة القانونية بكلية الحقوق ، جامعة القاهرة ، المقالة ٣، المجلد ٤، العدد ٤، 2018م .

- d. y7y yasyn s3od : al7rb alsybranya fy do2 8oa3d al8anon aldoly alansany ،b7th mnshor fy almgla al8anonya bklya al78o8 , gam3a al8ahra , alm8ala 3 ،almgld 4 ،al3dd 4 ،2018m .

- د .عبد الحى صالح عبد الله مغرب: الأدلة المستخدمة في ارتكاب الجريمة الالكترونية ، مجلة العدل العدد السابع والثلاثون السنة الرابعة عشرة.

- d .3bd al7y sal7 3bd allh mghrb: aladla almst5dma fy artkab algryma alalktronya ،mgla al3dl al3dd alsab3walthlathon alsna alrab3a 3shra.

- – د . عبد العال الدريبي – الجرائم الالكترونية – دراسة قانونية قضائية مقارنة مع أحدث التشريعات العربية في مجال مكافحة جرائم المعلوماتية والانترنت ، المركز القومي للإصدارات القانونية ، القاهرة مصر ٢٠١٢م.

- d . 3bd al3al aldryby – algra2m alalktronya – drasa 8anonya 8da2ya m8arna m3 a7dth altshry3at al3rbya fy mgal mkaf7a gra2m alm3lomatyawalantrnt ،almrkz al8omy ll esdarat al8anonya ،al8ahra msr 2012m.

- د . عبد الرحيم نادر عبد الرحيم ، دور إنترنت الأشياء في إدارة معرفة العملاء ، المجلة العلمية للدراسات التجارية والبيئية

- d . 3bd alr7ym nadr 3bd alr7ym ،dor entrnt alashya2 fy edara m3rfa al3mla2 ، almgla al3lmya lldrasat altgaryawalby2ya

د- الوثائق والقرارات:

- ثانياً: - مراجع باللغة الأجنبية:

- Types of Cyber Crime: HOW Cybersecurity professionals prevent Attacks 6-5-2020 ,Retrieved 13-2-2021
- Selma Dilek, applications of artificial intelligence techniques to combatingcyber-crimes: a review, op, cit, P. 28
- M .Stoyanova ,y .Nicolaides ,s .Panagiotaki's ,E .Pallis and E.K, Markis , A Survey on the Internet of Things (IOT) Forensics: Challenges ,Approaches ,and Open issues ,in LEEE Communications ,Surveys , Tutorials , vol,22 ,no2,pp.1191-1221,Secondquter 2020 ,doil; 10.1109/ COMST . 2019 .2962586

Al- Masr ,EYhab Bai, yan . li ,guan.(2018).A fog – Based Digital forensics Investigation framework for IOT S YSTEMS. 196-201 10 .1109/Smart Cloud 2018 .00040

[1] Types of Cyber Crime: HOW Cybersecurity professionals prevent Attacks 6-5-2020 ,Retrieved 13-2-2021)

- WWW.Pandasecurtiy .com,retrieved13-12-2021

types;EXaples,and what your Buiness can Do ,www.exabeam.com,Retieved13-2-2021

- info@cyberone.co
- m https ;llcyberone.co
- info@cyberone.com

WWW.Pandasecurtiy .com,retrieved13-12-2021-

WWW.Pandasecurtiy .com,retrieved13-12-2021-

https//www.jigsawacademy.com-