المعهد القومى للملكية الفكرية
The National Institute of Intellectual Property
Helwan University, Egypt

المجلة العلمية للملكية الفكرية وإدارة الابتكار

دورية نصف سنوية محكمة يصدرها

المعهد القومي للملكية الفكرية

جامعة حلوان

العدد الثالث
يوليو٢٠٢٠

الهدف من المجلة:

تهدف المجلة العلمية للملكية الفكرية وإدارة الابتكار إلى نشر البحوث والدراسات النظرية والتطبيقية فى مجال الملكية الفكرية بشقيها الصناعي والأدبي والفني وعلاقتها بإدارة الابتكار والتنمية المستدامة من كافة النواحي القانونية والاقتصادية والادارية والعلمية والأدبية والفنية.

ضوابط عامة:

- تعبر كافة الدراسات والبحوث والمقالات عن رأى مؤلفيها ويأتي ترتيبها بالمجلة وفقا لإعتبارات فنية لا علاقة لها بالقيمة العلمية لأى منها.
- تنشر المقالات غير المحكمة (أوراق العمل) فى زاوية خاصة في المجلة.
- تنشر المجلة مراجعات وعروض الكتب الجديدة والدوريات.
- تنشر المجلة التقارير والبحوث والدراسات الملقاه في مؤتمرات ومنتديات علمية والنشاطات الأكاديمية في مجال تخصصها دونما تحكيم في أعداد خاصة من المجلة.
- يمكن الاقتباس من بعض مواد المجلة بشرط الاشارة إلى المصدر.
- تنشر المجلة الأوراق البحثية للطلاب المسجلين لدرجتى الماجستير والدكتوراه.
- تصدر المجلة محكمة ودورية نصف سنوية.

ألية النشر فى المجلة:

- تقبل المجلة كافة البحوث والدراسات التطبيقية والأكاديمية في مجال حقوق الملكية الفكرية بكافة جوانبها القانونية والتقنية والاقتصادية والادارية والاجتماعية والثقافية والفنية.
- تقبل البحوث باللغات (العربية والانجليزية والفرنسية).
- تنشر المجلة ملخصات الرسائل العلمية الجديدة، وتعامل معاملة أوراق العمل.
- يجب أن يلتزم الباحث بعدم إرسال بحثه إلى جهة أخرى حتى يأتيه رد المجلة.
- يجب أن يلتزم الباحث بإتباع الأسس العلمية السليمة في بحثه.
- يجب أن يرسل الباحث بحثه إلى المجلة من ثلاثة نسخ مطبوعة، وملخص باللغة العربية أو الانجليزية أو الفرنسية، فى حدود ٨ ـ ١٢ سطر، ويجب أن تكون الرسوم البيانية والإيضاحية مطبوعة وواضحة، بالإضافة إلى نسخة إلكترونية Soft Copy، ونوع الخط Romanes Times New ١٤ للعربى، و١٢ للانجليزي على B5 (ورق نصف ثمانيات) على البريد الالكتروني: ymgad@niip.edi.eg
- ترسل البحوث إلى محكمين متخصصين وتحكم بسرية تامة.
- في حالة قبول البحث للنشر، يلتزم الباحث بتعديله ليتناسب مع مقترحات المحكمين، وأسلوب النشر بالمجلة.

مجلس إدارة تحرير المجلة	
أ.د. ياسر محمد جاد الله محمود	أستاذ الاقتصاد والملكية الفكرية وعميد المعهد القومي للملكية الفكرية (بالتكليف) - رئيس تحرير المجلة
أ.د. أحمد عبد الكريم سلامة	أستاذ القانون الدولي الخاص بكلية الحقوق بجامعة حلوان والمستشار العلمي للمعهد - عضو مجلس إدارة تحرير المجلة
أ.د. وكيل المعهد للدراسات العليا والبحوث	سكرتير تحرير المجلة
أ.د. جلال عبد الحميد عبد اللاه	أستاذ الهندسة الانشائية بكلية الهندسة بالمطرية بجامعة حلوان - عضو مجلس إدارة تحرير المجلة
أ.د. هناء محمد الحسيني	أستاذ علوم الأطعمة بكلية الاقتصاد المنزلي بجامعة حلوان - عضو مجلس إدارة تحرير المجلة
أ.د. وزير مفوض/ مها بخيت محمد زكي	مدير إدارة الملكية الفكرية والتنافسية بجامعة الدول العربية - عضو مجلس إدارة تحرير المجلة
اللواء أ.د. عبد القدوس عبد الرزاق العبيدلي	رئيس مجلس إدارة جمعية الامارات للملكية الفكرية - عضو مجلس إدارة تحرير المجلة
Prof Dr. Alexander Peukert	أستاذ القانون المدنى بجامعة جوته فرانكفورت أم ماين – ألمانيا - عضو مجلس إدارة تحرير المجلة
Prof Dr. Andrew Griffiths	أستاذ القانون التجارى بجامعة نيو كاسل - بريطانيا - عضو مجلس إدارة تحرير المجلة

المراسلات

ترسل البحوث إلى رئيس تحرير المجلة العلمية للملكية الفكرية وإدارة الابتكار بجامعة حلوان
جامعة حلوان - ٤ شارع كمال الدين صلاح - أمام السفارة الأمريكية بالقاهرة -جاردن سيتى
ص.ب: ١١٤٦١ جاردن سيتي
ت: ٠٢٠٢ ٢٥٤٨١٠٥٠ + محمول: ٠٢٠١٠٠٠٣٠٠٥٤٨ + ف: ٠٢٠٢ ٢٧٩٤٩٢٣٠ +
http://www.helwan.edu.eg/niip/
ymgad@niip.edu.eg

الجريمة المعلوماتية كإحدى الجرائم المستحدثة في الدول النامية

أحمد السيد سيف

الجريمة المعلوماتية كإحدى الجرائم المستحدثة في الدول النامية

أحمد السيد سيف

مقدمة:

مع ظهور تكنولوجيا المعلومات والاتصالات التي ارتبطت بكل جوانب الحياة تقريبا، ظهر نوع جديد من الجرائم يعرف بجرائم المعلومات، والتي تشير في معناها الواسع إلى: أي سلوك غير قانوني يتصل أو يتعلق بأنظمة الحاسب الآلي أو الشبكات بما في ذلك الحيازة غير القانونية، وعرض أو توزيع المعلومات بواسطة أنظمة الحاسب الآلي أو الشبكات.[1]

برغم حداثة هذا النوع من الجرائم إلا أنها تعد واحدة من أسرع أشكال الجريمة نمواً حيث بلغ عدد المتضررين منها قرابة ٩٧٨مليون فرد في٢٠ دولة عام ٢٠١٧ وتجاوزت الخسائر الناجمة عنها ١٧٢ بليون دولار أمريكي في ذات العام ٢٠١٧[2]، كما أصبحت عملية العثور على مرتكبي هذه الجرائم وإثباتها أصعب، وتضخمت الآثار والمعوقات الناجمة عن هذا النوع من الجرائم في البلدان النامية حيث تحتاج هذه الدول الى تكنولوجيا المعلومات وشبكة الانترنت وما يقدمانه من فرص تساعد على تسريع وتيرة عملية التنمية، مع إفتقارهاللقدرات والامكانيات اللازمة لمكافحة هذه الجرائم غير التقليدية ذات النطاق العالمي.

تزداد حدة هذه الجرائم وتعقيدها في حالة التعامل مع جرائم المعلومات المتعلقة بالملكية الفكرية، حيث يسهل تحويل أغلب المواد المتصلة بحقوق الملكية الفكرية الى شكل رقمي، كما تتصل هذه الحقوق بالأفكار وهي

[1] Gercke, Marko. (2012). Understanding cybercrime: Phenomena, challenges and legal response .First Edition,ITU.P.19
www.itu.int/ITUD/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf

[2] Symantec.(2018). "Norton Cyber Security Insights Report 2017".p.4. https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&cad=rja&uact=8&ved=2ahUKEwjNq4epuvLnAhVxTRUIHV_oBFUQFjABegQIAxAB&url=https%3A%2F%2Fwww.symantec.com%2Fcontent%2Fdam%2Fsymantec%2Fdocs%2Fabout%2F2017-ncsir-global-results-en.pdf&usg=AOvVaw3wY4

عنصر غير مادي يترتب عليها مكاسب مادية عالية، أي أن المشكلة في هذه الحالة أصبحت مركبة.

في هذا البحث سوف يتم القاء الضوء على مفهوم الجريمة المعلوماتية، ونشأتها، وسبل مكافحتها، في الدول النامية، مع القاء الضوء على الجهود الدولية المبذولة لتحقيق هذه الغاية، والتركيز على الجرائم المعلوماتية المتصلة بحقوق الملكية الفكرية من خلال المطلبين التاليان:

المطلب الاول
مفهوم الجريمة المعلوماتية وطبيعتها الخاصة

في هذا المطلب سوف يتم عرض نشأة وظهور الجرائم المعلوماتية، والمفاهيم المختلفة التي تناولت هذا النوع من الجرائم، مع توضيح نقاط القصور والقوة بكل من هذه المفاهيم، ثم استعراض الطبيعة الخاصة لهذه الجرائم التي تميزها عن الجرائم التقليدية من خلال الفروع التالية:

أولاً:النشأة التاريخية للجرائم المعلوماتية.

ثانياً: تعريف الجرائم المعلوماتية.

ثالثاً:أركان الجريمة المعلوماتية

رابعاً: الطبيعة الخاصة لجرائم المعلومات.

المطلب الثاني
أنواع جرائم المعلومات والتشريعات الدولية والمحلية المبذولة لموجهتها في الدول النامية

وفيه سيتم تناول أشكال هذه الجرائم، مع التركيز على الجرائم المعلوماتية المتعلقة بحقوق الملكية الفكرية، والخسائر الناجمة عنها، والجهود المحلية والدولية المبذولة لمواجهة هذه الجرائم، من خلال الفروع التالية:

أولاً: أنواع الجرائم المعلوماتية.

ثانياً: الجريمة المعلوماتية في الدول النامية

ثالثاً: الجرائم المعلوماتية المتصلة بحقوق الملكية الفكرية.

رابعاً: التدابير الاجرائية الواجب اتخاذها لمواجهة الجريمة المعلوماتية.

المطلب الاول
مفهوم الجريمة المعلوماتية وطبيعتها الخاصة

الفرع الأولً: النشأة التاريخية

تزامن ظهور الجريمة المعلوماتية مع ظهور تكنولوجيا المعلومات، وارتبط تطور هذا النوع من الجرائم بالتطور الحادث في هذا المجال، ويمكن اعتبار أن المرحلة الأولى من هذه الجرائم بدأت في ستينيات القرن الماضي عندما تم تطوير أجهزة الحاسب بالاعتماد على أنظمة الترانزستور"transistor-based computer"، بعد أن كانت تعتمد على أنابيب التفريغ " vacuum-tube"، مما أدى إلى صنع أجهزة كمبيوتر أصغر حجما وأقل تكلفة، خلال هذه الفترة تركزت الجرائم على الأضرار المادية للكمبيوتر، على سبيل المثال تسببت أعمال شغب الطلاب التي إندلعت في فبراير من عام ١٩٦٩ بكندا في نشوب حريق دمر أجهزة الكمبيوتر وبلغت الخسائر الناجمة عن هذا الحريق ٢ مليون دولار تقريباً[1].

في السبعينات والثمانينات من القرن الماضي انتشر استخدام تكنولوجيا الكمبيوتر وانخفضت أسعارها ووصل عدد أجهزة الكمبيوتر في الولايات المتحدة وحدها عام ١٩٧٠ الى أكثر من ١٠٠,٠٠٠ حاسوب[2]، وبدأ شكل الجرائم المتعلقة بها يتغير من الأضرار المادية الى اشكال أخرى كالاستخدام غير القانوني لأنظمة الكمبيوتر، والتلاعب بالبيانات.

[1] Kabay , M. (2008). A Brief History of Computer Crime: An Introduction for Students .Norwich University.p.5.
[2] Gercke , Marko. (2012). Ibid.p.21.

مع زيادة عدد أجهزة الكمبيوتر وبداية تكوين شبكات تربط بين هذه الأجهزة في الثمانينيات، ظهرت أشكل جديد من الجرائم التي يمكن لمرتكبها القيام بها دون التواجد في مسرح الجريمة، بل وأتمتة هذه الجرائم، الأمر الذي أدى الى زيادة حجم عمليات القرصنة وظهور تعديات على حقوق الملكية الفكرية الخاصة بالبرمجيات والوسائط المتداولة عبر هذه الشبكات.

مع ظهور الواجهة التفاعلية للانترنت في التسعينات زاد عدد مستخدمي الحاسبات وشبكة الانترنت العالمية بشكل مطرد ليبلغ ١٦ مليون مستخدم تقريباً عام ١٩٩٥، وفي عام ٢٠٠٢ وصلت نسبة مستخدمي الانترنت إلى١٠٪ تقرياً من اجمالي تعداد سكان العالم ، وارتفع هذا العدد في عام ٢٠١٧ ليصل الى ٣.٨٩ بليون مستخدم تقريباً يمثلون أكثر من ٥١٪ من تعداد سكان العالم[١]، صحب هذه الزيادة في اعداد المتعاملين زيادة مقابلة في عدد جرائم المعلومات حيث بلغ عدد الأفراد الذين تعرضو لهذا النوع من الجرائم ٩٧٨ مليون فرد وذلك في ٢٠ دولة عام ٢٠١٧، وبلغ اجمالي الخسائر التي تكبدها المستخدمين خلال هذا العام ١٧٢ بليون دولار[٢]، وهو ما يشير لضرورة دراسة هذه الظاهرة لفهمها والتصدي للمخاطر المترتبة عليها.

[1] Yar, Mojid & Steinmetz, (2019). "Cybercrime and Society".Third Edition – London:SAGE.p.7-9.
https://books.google.com.eg/books?hl=en&lr=&id=gpuHDwAAQBAJ&oi=fnd&pg=PP1&ots=flxTugCwFW&sig=f1K7t0BFvo4je2YGzU2mw2XzMw&redir_esc=y#v=onepage&q&f=false

[2] Symantec .Ibid.p.4.

الفرع الثاني
تعريف الجرائم المعلوماتية

اختلفت المسميات التي تناولت الجريمة المعلوماتية، فالبعض يطلق عليها جرائم الكمبيوتر، ويسميها البعض الآخر جرائم المعلومات، وهي التسمية التي يتفق معها الباحث اذ أنها أشمل وأوسع نطاقاً من جرائم الكمبيوتر التي حصرت هذه الجرائم في الجرائم التي يكون الكمبيوتر جزءاً منها فقط، وهي بهذا لا تغطي الجرائم المتعلقة بالفضاء الالكتروني والهواتف الذكية والعديد من الوسائط الأخرى التي يمكن استخدامها لتنفيذ هذه الجرائم، وتنوعت تعريفات الجريمة المعلوماتية وفق اختلاف طبيعة النظم القانونية والدول، وفيما يلي عرض لبعض من هذه التعريفات:

التعريفات التي أخذت بالمفهوم الضيق للجريمة المعلوماتية:

عرف الفقيه الفرنسي (Mass) الجريمة المعلوماتية بانها:"الاعتداءات القانونية التي ترتكب بواسطة المعلوماتية بغرض تحقيق الربح"[١].

في حين عرف (Merwe) الجريمة المعلوماتية على أنها:"الفعل غير المشروع الذي يتورط في ارتكابه الحاسب الآلي – أو هو الفعل الاجرامى الذي يستخدم في اقترافه الحاسب الآلي كأداة رئيسية"[٢].

وقد حصر أنصار هذا المفهوم الجريمة المعلوماتية في الحالات التي تتطلب قدر كبير من المعرفة الفنية أو تلك التي يكون الحاسب الآلي هو الأداة الرئيسية في ارتكابها، أو التي يكون الدافع الرئيسي من ورائها هو تحقيق الربح.

التعريفات التي أخذت بالمفهوم الواسع للجريمة المعلوماتية:

ذهب الفقيهان (Credo&Michel) إلى أن:

---

[١] عمیار، ریم، (٢٠١٨). تأثیر الجریمة المعلوماتیة على الاقتصاد الوطني العربي(مذكرة مكملة لنيل درجة الماستر في القانون).جنائي أعمال.كلية الحقوق والعلوم السياسية.جامعة العربي بن مهيدي.ص.٩.

[٢] فريال، لعاقل.(٢٠١٥). الجريمة المعلوماتية في ظل التشريع الجزائري(مذكرة مكملة لنيل درجة الماستر في القانون العام).قانون جنائي.كلية الحقوق والعلوم السياسية.جامعة جامعة اكلي محند – البويرة.ص.٨.

"الجريمة المعلوماتية تشمل استخدام الحاسب كأداة لارتكاب الجريمة هذا بالإضافة إلى الحالات المتعلقة بالولوج غير المصرح به لحاسب المجني عليه أو بياناته، كما تمتد جريمة الحاسب لتشمل الاعتداءات المادية سواء على بطاقات الائتمان، وانتهاك ماكينات الحساب الآلي بما تتضمنه من شيكات تحويل الحسابات المالية بطرق إلكترونية وتزييف المكونات المادية والمعنوية للحاسب، بل وسرقة الحاسب في حد ذاته وأي من مكوناته"[١].

عرف مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاقبة الجرمين المنعقد في فيينا عام ٢٠٠٠ الجريمة المعلوماتية بأنها:"أية جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبيةأو داخل نظام حاسوب، وتشمل تلك الجريمة من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في البيئة الإلكترونية[٢]"

ويرى الباحث أن الاتجاه الموسع في تعريف الجريمة المعلوماتية هو الأفضل لأننا نتعامل مع موضوع سريع التغير لارتباطه بتكنولوجيا المعلومات والاتصالات، واسع النطاق حيث يتصل بمختلف نواحي الحياة وشتى المجالات، لذلك كلما كان المفهوم أكثر اتساعاً كلما كان أكثر قدرة على التعامل مع التغيرات السريعةوالمتلاحقة.

تعريف الجريمة المعلوماتية في بعض القوانين المحلية:

يعد وضع تعريف ثابت ومحدد للجريمة المعلوماتية أمراً في منتهى الصعوبة، لذلك لم يقم كل من المشرع المصري والاماراتي بوضع تعريف للجريمة المعلوماتية في قوانينهم فنجد أن القانون المصري رقم ١٧٥ لسنة ٢٠١٨[٣] في شأن مكافحة جرائم تقنية المعلومات اكتفى بذكر الحالات

[١] عمیار، ریم. مصدر سابق.ص.١١.
[٢] مختاري، إكرام. (٢٠١٦). خصوصيةالجريمة المعلوماتية وإشكالية الاختصاص. **منشورات مجلة دفاتر قانونية – سلسلة دفاتر جنائية**.ع١.ص.٢٠٤.
[٣] جمهورية مصر العربية. قانون مكافحة جرائم تقنية المعلومات. قانون رقم١٧٥ (٢٠١٨).(الوقائع المصرية: العدد ٣٢ مكرر(ج) في ١٤ أغسطس ٢٠١٨.

والأفعال التي يعتبر ارتكابها جريمة وتحديد عقوبتها، وهو نفس النهج الذي اتبعه المشرع الاماراتي عند إصدار القانون الاتحادي رقم ٥ لسنة ٢٠١٢[١].

ولعل الداعي الى ذلك هو عدم وجود اتفاق على تعريف محدد لهذا النوع من الجرائم، والرغبة في اتاحة درجة عالية من المرونة لمقابلة أي نوع جديد يظهر من هذه الجرائم.

أما المشرع الجزائري فقد وضع تعريفاً للجرائم المعلوماتية في المادة ٢ من القانون ٠٩-٠٤ الصادر عام ٢٠٠٩ على أنها:

"جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل إرتكابها عن منظومة معلومات أو نظام الاتصالات الالكترونية"[٢]، ونرى أن المشرع الجزائري قد إكتفى في هذا التعريف بالاشارة الى محل الجريمة وهو أنظمة المعالجة الآلية ومحل الجريمة وهو عن منظومة معلومات أو نظام الاتصالات الالكترونية.

بشكل عام لا يوجد تعريف محدد للجريمة المعلوماتية، ساعد على ذلك التطور السريع والمستمر في تكنولوجيا المعلومات، واختلاف الترجمات التي تحاول عرض هذه الظاهرة، ونظراً لأن هذا النوع من الجرائم يتخطى الحدود الجغرافية، وفي سبيل إيجاد مفهوم يحقق درجة من التوافق الدولي على ما يقصد بالجرائم المعلوماتية، شدد فريق الخبراء التابع للأمم المتحدة في مداولات اجتماعه الأول المنعقد في فيينا عام ٢٠١١ على أن وضع تعريف واحد دقيق للجرائم المعلوماتية غير ممكن وأن الأنسب هو اتباع نهج وصفي أو تصنيف يكون أساسه اتفاقية المجلس الأوروبي المتعلقة بالجريمةالمعلوماتية[٣].

---

[١] الإمارات العربية المتحدة.القانون الاتحادي رقم ٥ قانون مكافحة جرائم تقنية المعلومات,(٢٠١٢).

[٢] الجمهورية الجزائرية.القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، قانون رقم ٠٩-٠٤ لسنة ٢٠٠٩.(الجريدة الرسمية للجمهورية الجزائرية:العدد ٤٧.١٦ أغسطس ٢٠٠٩)، مادة ٢.ص.٥.

[٣] الأمم المتحدة (٢٠١١). مداولات الاجتماع الأول لفريق الخبراء المعني باجراء دراسة شاملة عن الجريمة السيبرانية، فيينا.ص.٤.

الفرع الثالث: أركان الجريمة المعلوماتية

تعتبر اركان الجريمة جزء لا يتجزء من طبيعتها، وتخلف أحد هذه الأركان يؤدي الى انتفاء الجريمة، ويتطلب القانون توافر ركن مادي وركن معنوي حتى يتم التجريم ويستحق العقاب.

الركن المادي للجريمة المعلوماتية:

بشكل عام فإن الركن المادي هو علاقة بين ثلاثة عناصر :فعل أو سلوك غير مشروع; نتيجة مجرمة;علاقة سببية بين الفعل الجريمة[1]، وفي حالة جرائم المعلومات قد يأخذ هذا الفعل العديد من الأشكال وفقاً لنوع الجريمة المعلوماتية المرتكبة، فقد يكون في شكل القيام بنشر مواد اباحية، أو التعدي على مواد محمية، ونتيجة هذ الفعل قد تتمثل في وقوع أضرار مادية كما هو الحال في التعدي على حقوق الملكية الفكرية، أو نفسية كما في حالة التشهير والتعدي على الحريات الشخصية، كما قد تضر بالنظام العام كنشر الأخبار الكاذبة والمواد المخلة بالأداب، أما عنصر السببية والذي يربط بين الفعل والنتيجة فيمثل اثباته تحديا كبيرا في الجريمة المعلوماتية نظراً للطبيعة التقنية المتطورة لهذا النوع من الجرائم والطبيعة الفنية لمرتكب الجريمة التي تضع صعوبة في اثبات هذه العلاقة.

الركن المعنوي للجريمة المعلوماتية:

يشير الركن المعنوي إلى العلاقة بين ماديات الجريمة ونفسية الجاني التي دفعته لارتكابها، وهو يقوم على عنصرين رئيسيين; العلم والإرادة[2]، وبتطبيق هذين العنصرين على الجرائم المعلوماتية، فيجب أن يكون الفاعل في حالة الجرائم المعلوماتية على علم بان عملية نسخ المواد المحمية مثلا أمر غير قانوني، وتوفرت لديه النية لإلحاق الخسائر المادية مثلا بصاحب هذا الحق، ونظرا للطبيعة الفنية للجريمة المعلوماتية وطبيعة مرتكبها يصعب تصور عدم توافر هذان الركنان فيها، فقيام شخص تتوافر

[1] الحوامدة.لورنس(٢٠١٧).الجرائم المعلوماتية أركانها وآلية مكافحتها(دراسة تحليلية مقارنة).**مجلة الميزان للدراسات الإسلامية والقانونية**.مج٤.ع١.ص١٩٧-٢٠٠.

[2] المصدر السابق.ص.٢٠٦.

لديه مهارات التعدي على حقوق برنامج أو اختراق نظام بشكل غير قانوني يصعب تصور جهله بعدم قانونية الفعل أو عدم توافر إرادة الحاق الضرر وهو النهج الذي تبناه القضاء الفرنسي في الأخذ بمبدأ سوء النية في شأن جرائم الانترنت[1].

الفرع الرابع: الطبيعة الخاصة للجريمة المعلوماتية

هناك عدد من الخصائص التي تجعل الجريمة المعلوماتية تختلف عن غيرها من الجرائم، ويرى الأستاذ/غانم الشمري أن هذه الخصائص هي:

١- ترتكب في بيئة تكنولوجيا لمعلومات

فبخلاف الجرائم الأخرى أدة هذه الجريمة هي الحاسب الآلي ومحلها هو الفضاء الالكتروني.

٢- لا تتسم بالعنف.

بعكس العديد من الجرائم التقليدية كالقتل والخطف، لا يعتمد هذا النوع من على المجهود العضلي وإنما على المعرفة الفنية والمجهود الذهني، ساعد على ذلك عدم وجود اتصال جسدي مباشر بين الجاني والمجني عليه ووقوع هذه الجرائم في الفضاء الالكتروني.

٣- جرائم عابرة للحدود

حيث أنها من نواتج ثورةالاتصالات والمعلومات التي جعلت الحدود بين الدول تتلاشى وأصبح من السهل على مرتكب هذا النوع من الجرائم تنفيذه من والى أي مكان، بل قد يكون الجاني في مكان والمجني في مكان والضرر الواقع في مكان مختلف عن كليهما.

٤- صعوبة اكتشافها واثباتها

حيث لا يلاحظ المجني عليه في كثير من الأحيان وقوعها إلا بعد مدة، كما أنه من الصعب العثور على أثر مادي لها نظراً لاعتمادها على تكنولوجيا المعلومات، كما أنها في العديد من

[1] النهوي.أحلام(٢٠١٧).جرائم الحاسب الآلي وسبل مكافحتها.**المجلة الليبية العالمية**.ع٢٠.ص.١٢.

الحالات لا تستغرق الكثير من الوقت ويسهل محو الدليل الخاص بها[1].

المطلب الثاني
أنواع جرائم المعلومات والتشريعات الدولية والمحلية المبذولة لموجهتها

الفرع الأول: أنواع جرائم المعلومات

يستخدم مصطلح الجريمة المعلوماتية لتغطية نطاق واسع من الجرائم، ويوجد العديد من التصنيفات والأسس لتصنيف هذا النوع من الجرائم، فصنفها البعض وفقاً لنوع النشاط الضار الذي تسببه في حين صنفها البعض الآخر وفق الأداة المستخدمة في ارتكابها، كما تم التواصل لتقسيم أكثر شمولية وتفصيل وفق اتفاقية بودابست ٢٠٠١، وفيما يلي استعراض لأهم هذه التصنيفات:

تقسيم الجرائم المعلوماتية بناءاً على الأداة المستخدمة في ارتكابها:

١- جرائم على الجهاز "crimes in the device".
وتشير الى الحالات التي يكون محتوى الجهاز فيها غير قانوني كاحتوائه على مواد مقرصنة، أو مواد تدعو للكراهية.
٢- جرائم باستخدام الجهاز "crimes using the device".
وهي الجرائم التي يتم فيها استخدام الأنظمة الرقمية كأداة لتنفيذ الجريمة لخداع الضحايا، كجرائم السرقة الالكترونية للاموال.
٣- جرائم ضد الجهاز "crimes against the device".
وهي الجرائم التي تتعرض لسلامة الأجهزة وسلامة البيانات الموجودة عليها، كهجمات الفيروسات وسرقة البريد اللكتروني[2].

---

[1] الشمري، غانم (٢٠١٦). الجرائم المعلوماتية- ماهيتها - خصائصها - كيفية التصدي لها قانونياً.ط١. دار الثقافة,الدار العلمية الدولية.ص ٦٩-٧٩.

[2] Nurse,Jason. (2019). The OxfordHandbook of Cyberpsycholog -Cybercrime and You: How Criminals Attack and the Human Factors That They Seek to Exploit.First Edition.printed by:GPI Group.UK.p.663-667.
https://books.google.com.eg/books?id=9guXDwAAQBAJ&pg=PR7&source=gbs_selected_pages&cad=2#v=onepage&q&f=false

تصنيف الجرائم المعلوماتية وفقاً لنوع النشاط الضار الذي تسببه:

١- جرائم تعدي

وتشمل التعدي على حقوق الملكية الفكرية، وختراق حسابات ونظم الغير ونشر الفيروسات وخلافه.

٢- جرائم الخداع والسرقات.

وكافة أشكال الاحتيال الأخرى التي تحدث داخل الفضاء الالكتروني كالاستخدام الاحتيالي لبطاقات الائتمان والعملات الرقمية واقتحام الحسابات المصرفية.

٣- نشر المواد الاباحية الخاصة بالأطفال.

٤- نشر المواد العنيفة أو الداعية للعنف[1].

تصنيف الجرائم المعلوماتية وفقاً لاتفاقية بودابست:

وفق اتفاقية بودابست التي تبناها المجلس الأوروبي " Council of Europe (COE)" عام ٢٠٠١ لمواجهة الجريمة المعلوماتية يمكن تقسيم الجرائم المعلوماتية الى أربع مجموعات رئيسية يندرج تحت كل منها عدد من الجرائم هذه المجموعات هي:

١- جرائم ضد سرية وسلامة وتوافر بيانات الكمبيوتر وأنظمته:

- النفاذ غيرالقانوني "Illegal access ".
- الاعتراض غير القانوني"Illegal interception ".
- التلاعب في البيانات"Data interference ".
- التلاعب في النظام"System interference ".
- إساءة استخدام الأجهزة"Misuse of devices ".

٢- الجرائم ذات الصلة بالحاسوب"Computer-related offences":

التزوير المتصل بالكمبيوتر"Computer-related forgery ".

الاحتيال المتصل بالكمبيوتر"Computer-related fraud ".

٣- الجرائم المتعلقة بالمحتوى"Content-related offences":

- الجرائم المتعلقة باستغلال الأطفال في المواد الإباحية" Offences related to child pornography"

٤- المخالفات المتعلقة بانتهاكات حقوق النشر والحقوق المجاورة:

[1] Hosseinian-Far, A., Jahankhani, H., & Al-Nemrat, A. (2014). Cyber crime Classification and Characteristics The University of Northampton. P.154-155.

Offences related to infringements of copyright and related "
rights[1]".

وسوف يتم تناول هذا النوع من الجرائم بشيئ من التفصيل في الفرع التالي.

يلاحظ على هذا التصنيف أنه يركز على موضوع الحماية باستثناء النوع الثاني وهو الحماية ضد الجرائم ذات الصلة بالحاسوب الذي يركز على وسيلة ارتكاب الجريمة، الأمر الذي قد يمثل نوع من التضارب في الأساس المستخدم للتصنيف.

الفرع الثاني
الجرائم المعلوماتية المتعلقة بانتهاكات حقوق النشر والحقوق المجاورة

كما سبق الاشارة عاليه فقد تم تقسيم الجرائم المعلوماتية وفق اتفاقية بودابست، وهي الاتفاقية الأم في هذا الصدد الى أربع أنواع رئيسية، من ضمنها المخالفات المتعلقة بانتهاكات حقوق النشر والحقوق المجاورة، ويواجه أصحاب هذه الحقوق في البيئة الرقمية العديد من المخاطر، حيث يمكن التعدي على علاماتهم التجارية وتصميماتهم لتقديم منتجات مقلدة، يسهل استنساخ المصنفات وتوزيعها عبر الانترنت، وتأخذ الجرائم المعلوماتية المتعلقة بحقوق الملكية الفكرية احد شكلين رئيسيين:

أولاً:الجرائم المتعلقة بحق المؤلف copyright related offences

في ظل ثورة الاتصالات والمعلومات أصبحت حماية حقوق المؤلف والحقوق المجاورة لها عملية بالغة الصعوبة، حيث أصبح من الممكن تحويل معظم الاعمال المحمية الى شكل رقمي ونسخها وتوزيعها الى كل مكان في العالم من خلال شبكة الانترنت، وفي حين كانت عملية نسخ المواد الترفيهية كالأفلام ومقاطع الموسيقى على شرائط الفيديو والكاسيت عملية صعبة من حيث حجم اعادة الانتاج وجودته، فقد اختلف الوضع مع ثورة المعلومات حيث أثبتت اقراص الCD وDVDأنها أكثر استدامة وسرعة بل وحفاظاً على الجودة، ومع التطور المستمر والسريع تزداد القدرة على نسخ وتوزيع هذه المصنفات دون حتى الحاجة الى وسائط مثل هذه الأقراص، بل

[1] Cybercrime (Convention)، Pub. L. No. 185, 3 (2001). https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

ان أكثر أشكال التعدي على حقوق المؤلف شيوعا أصبح تبادل البرامج والأفلام والأغاني المحمية بواسطة برامج المشاركة عبر .

ثانياً:التعدي على العلامات التجارية "Trademark-related offences "

مع زيادة المتعاملين مع شبكة الانترنت تزايدت أهمية التجارة الالكترونية وبالتبعية زادت أهمية العلامات التجارية وأسماء النطاق المستخدمة عبر الانترنت، حيث ترغب الشركات في تسهيل عملية تعرف ووصول المستهلكين الى مواقعهم الالكترونية وبضائعهم وذلك من خلال استخدام اسماء نطاق وعلامات تجارية جذابة ومتصلة بهذه الشركات حيث ترتبط السمعة الجيدة عادة بأسماء شركات معينة. [١]

تأخذ عملية التعدي على العلامات التجاريةالعديد من الأشكال، كتقليد العلاماة التجارية بشكل مباشر أو إرسال رسائل الكترونية تحمل نفس طابع الرسائل المرسلة بواسطة الشركة صاحبة العلامة، بالإضافة إلى التعدي على أسماء النطاق"domain name related offences "، ولعل هذا كان السبب وراء شراء العديد من الشركات لأسماء نطاق التي تعبر عنها أو تمثل عنصر جذب للمستخدمين، فقد تم بيع حقوق اسم نطاق " linux.com " بأكثر من مليون دولار عام ١٩٩٩، كما تم بيع اسم النطاق "eflowers.com"إلى مالك شركة فلاورز دايركتز ومقره فلوريدا مقابل مليون دولارعام ٢٠٠٠.[٢]

تعتبر انتهاكات حقوق الملكية الفكرية، ولا سيما حق التأليف والنشر، من بين أكثر الجرائم التي ترتكب عادة على شبكة الانترنت، وتشمل هذه المصنفات المحمية الأعمال الأدبية والتصويرية والموسيقية والسمعية البصرية وغيرها من المصنفات، وقد بلغت خسائر الجرائم المعلوماتية المتعلقة بالملكية الفكرية عام ٢٠١٢ في الولايات المتحدة وحدهاحوالي ٣٦٠ مليار دولار، وفي عام ٢٠١٥ قفذ هذا المعدل قفذة كبيرة حيث بنسبة

[1] Gercke, Marko. (2012). Ibid.p.27-28.

[2] Settapong.Malisuwan(2007). Conflict of Domain Name and Trademark in Thailand. **International Journal of The Computer**, the Internet and Management Vol. 15.p.63-64.

١٩٪ مقارنة بالعام السابق[١]، ووفق التقرير الذي أعدته منظمة "WIPO"، بلغت نسبة الشركات التي تعرضت لجرائم معلوماتية متعلقة بالملكية الفكرية عبر الانترنت ٣٪ من حجم العينة وكان حجم السرقات وفق طبيعة حق الملكية الفكرية كالتالي:

- الأسرار التجارية (٧٠ ٪ من الحالات).
- والمواد المحمية بموجب حقوق الطبع والنشر (٤٧ ٪).
- والمواد المشتملة على براءة اختراع (١٤ ٪).
- والعلامات التجارية (٨ ٪).

على الرغم من أن نسبة الجرائم المعلوماتية المتعلقة بالملكية الفكرية صغيرة "٣٪"مقارنة بباقي أنوا الجرائم المعلوماتية، الا أنها صاحبة اكبر قدر من الخسائر المالية حيث بلغ إجمالي الخسائر المالية الناتجة عنها قرابة ١٦٠ مليون دولار امريكي في مفردات العينة.[٢]

الفرع الثالث:الجريمة المعلوماتية في الدول النامية

من العرض السابق لظاهرة الجرائم المعلوماتية يبدو جليا ارتباطها بتكنولوجيا المعلومات وشبكة الانترت، ولعل تأخر انتشار هذه التكنولوجيا في العالم النامي قد أدى الى تأخر ظهور تأثيرات هذا النوع من الجرائم في دول العالم النامي، وتوضح الخريطة رقم (١)[٣] أن نسبة السكان الذين يستخدمون الانترنت في جميع دول العالم خلال العام ١٩٩٤لم تكن تتجاوز ال٢٠٪ في حين أن جزء كبير من دول أفريقيا وأسيا، وهي الدول النامية لم تكن هذه النسبة تتخطى ١٠٪، وفي معظم الدول الأفريقية كانت هذه النسبة منعدمة.

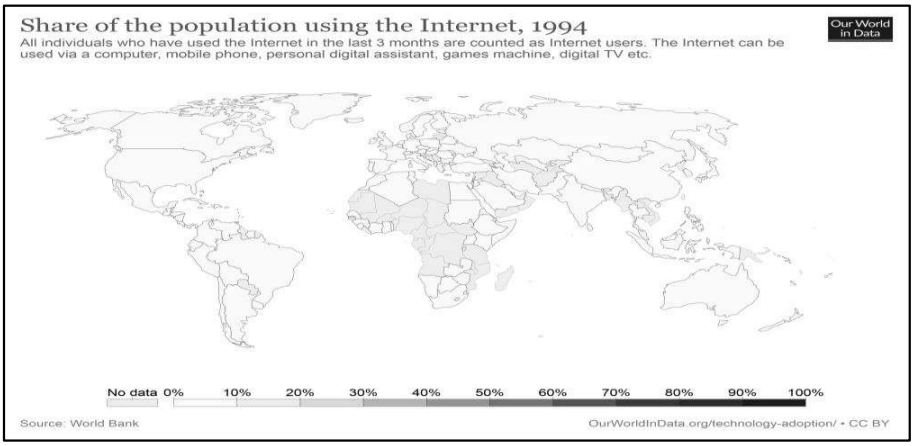
خريطة رقم(١)نسبة السكان الذين يستخدمون الانترنت عام ١٩٩٤

---

[1] Siles. Emile. (2015). Cybersecurity and Cybercrime: Intellectual Property and Innovation. **SSRN Electronic Journal.** Vol. 8, No2.p2-3.

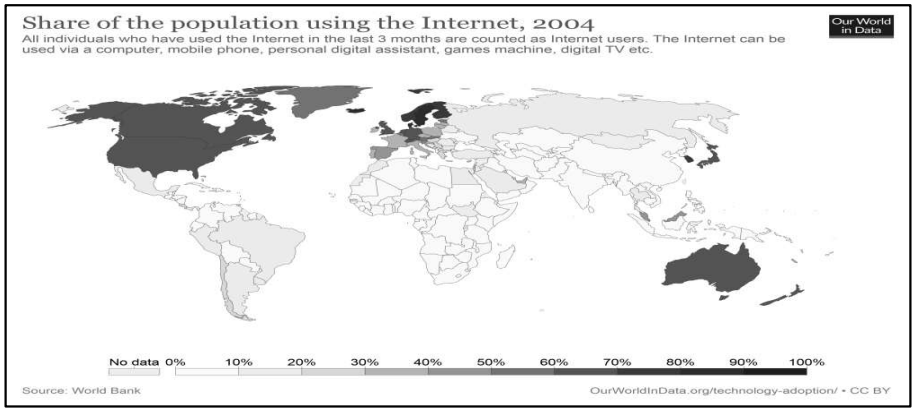
2 Rantala, Rantal. (2018). Cybercrime against Businesses, 2005. U.S. Department of Justice.p.5.

[3] The World Bank. (2019). Individuals using the Internet (% of population).14/4/2020.
https://data.worldbank.org/indicator/IT.NET.USER.ZS?view=map



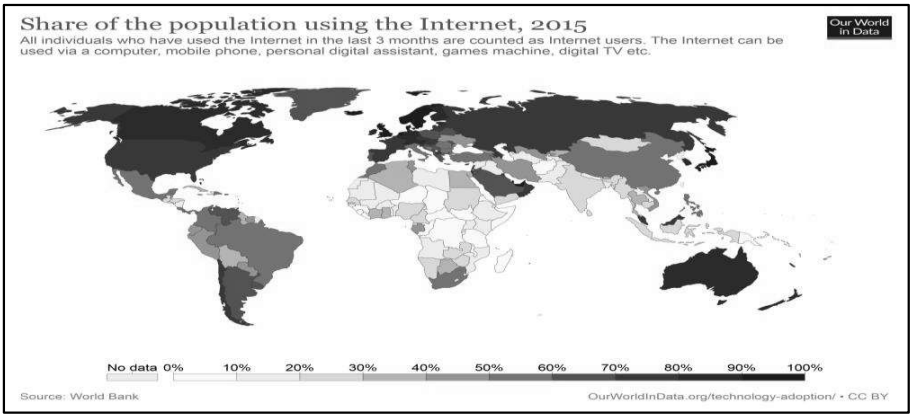
خلال ١٠ سنوات تضاعفت هذه النسبة كما توضح الخريطة رقم (٢)[1] فأصبحت في معظم الدول المتقدمة بأوروبا وأستراليا وأمريكا الشمالية واليابان تتجاوز ٨٠٪ن أما الدول النامية في أفريقيا وأسيا وأمريكا الجنوبية فقد تراوحت هذه النسبة بين ١٠٪، و٢٠٪، وكانت هذه النسبة في مصر والمملكة العربية السعودية والمغرب ٢٠٪.

خريطة رقم(٢)نسبة السكان الذين يستخدمون الانترنت عام ٢٠٠٤



[1] Ibid

خريطة رقم(٣)نسبة السكان الذين يستخدمون الانترنت عام ٢٠١٥



وخلال العشرة أعوام التالية وبالوصول الى عام ٢٠١٥ تغير شكل الخريطة العالمية لاستخدام الانترنت كما توضح خريطة رقم(٣)[1] لتتراوح في الدول المتقدمة ما بين ٩٠٪ و١٠٠٪، وتتراوح في دول العالم النامي بين ٣٠٪ و٦٠٪، وكانت هذه النسبة في مصر والجزائر ٤٠٪ وفي المغرب وجنوب أفريقيا ٦٠٪ وارتفعت هذه النسبة في المملكة العربية السعودية لتصل الى ٧٠٪، وتبلغ أقصاها في الدول العربية في الامارات العربية المتحدة ٩٠٪ وقطر ١٠٠٪.

تصاحب مع هذا الانتشار والتوسع في استخدام الانترنت زيادة حجم الأعمال المتعلقة به كالتجارة الالكترونية والتي يوضح الجدول رقم(١)ترتيب أكبر ١٠ إقتصادات نامية فيها"Developing Economics" وترتيب أكبر عشر دول أفريقية من حيث حجم التجارة اللكترونية بها عام ٢٠١٤[2].

جدول رقم (١) ترتيب أكبر عشر دول نامية وأفريقية من حيث حجم التجارة الاكترونية بها عام٢٠١٤

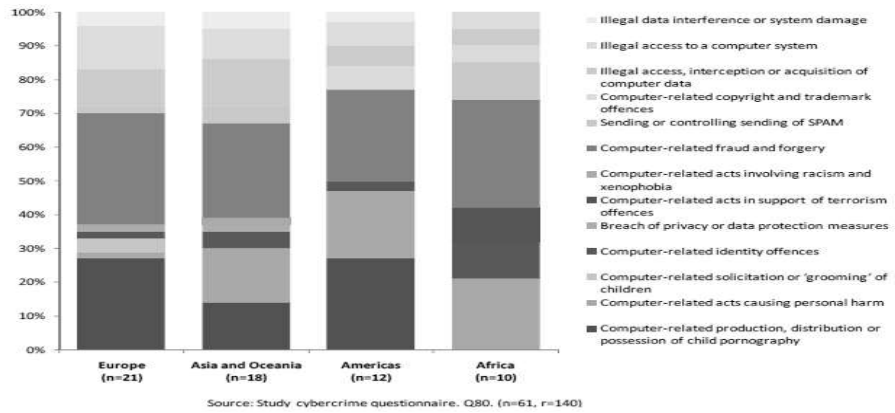
الترتيب	الدول النامية	الدول الافريقية
١	كوريا الشمالية	موريشيوس
٢	هونج كونج"الصين"	جنوب أفريقيا
٣	سنغافورة	مصر

[1] Ibid.
[2] United Nations. (2015). INFORMATION ECONOMY REPORT- Unlocking the Potential of E-commerce for Developing Countries.Switzerland.p.4.

٤	البحرين	تونس
٥	تركيا	المغرب
٦	شيلي	سيراليون
٧	أورجواي	زامبيا
٨	ترنيداد وتوباجو	مدغشقر
٩	ماليزيا	زمبابوي
١٠	البرازيل	مالي

وفيما يتعلق بالجرائم المعلوماتية في الدول النامية فإن حداثة هذا النوع من الجرائم وضعف البنية المعلوماتية في الدول النامية تجعل من الصعب تتبع الاحصاءات الخاصة به ، ولكن بالنظر الى معدلات الجرائم المعلوماتية التي تم تسجيلها بواسطة نلاحظ أن النسبة الاكبر من هذه الجرائم في جميع دول العالم هي جرائم الغش والتزوير المتعلقة بالحاسب" Computer related fraud and forgery "، وتتقارب نسبة الانتهاكات المتعلقة بحقوق الملكية الفكرية مقارنة بباقي الجرائم المعلوماتية في دول الأفريقية مع نظيرتها في باقي القارات كما يوضح الشكل رقم (١)[1].

شكل رقم(١) التوزيع النسبي للجرائم المعلوماتية وفق للقارات

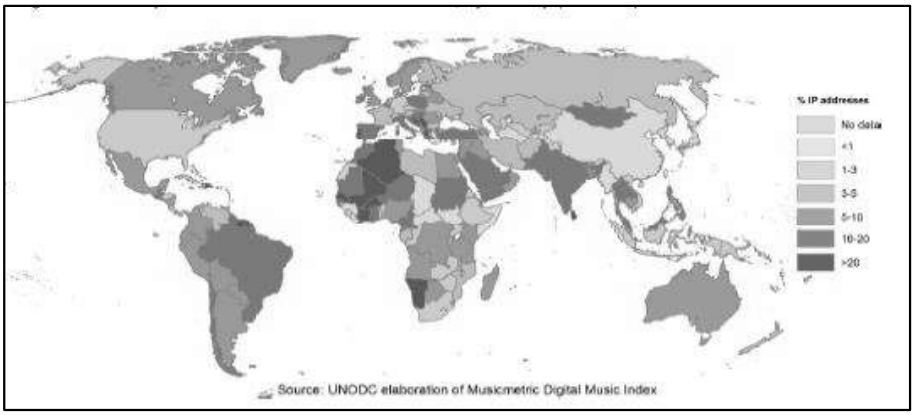


Source: Study cybercrime questionnaire. Q80. (n=61, r=140)

[1]UNITED NATIONS OFFICE ON DRUGS AND CRIME.(2013).Comprehensive Study on Cybercrime. Vienna.p.26. http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf

ورغم صعوبة الحصول على بيانات حول حجم جرائم المعلومات في الدول النامية الى أن التعرض لتوزيع أحد هذه الجرائم وهو حجم التحميلات غير القانونية للملفات الموسيقية باستخدام برنامج تحميل واحد والذي بلغ [1] ٤٠٥ مليون تحميل تركز معظمها في الدول النامية في أفريقيا وأسيا وأمريكا الجنوبية كما توضحه الخريطة رقم (٤) يمكن أن يعطينا تصور عن حجم هذه الظاهرة في الدول النامية.

خريطة رقم (٤) حجم التحميلات غير القانونية للملفات الموسيقية باستخدام أحد برامج التورنت



الفرع الرابع: التدابير الاجرائية الواجب اتخاذها لمواجهة الجريمة المعلوماتية:

تؤدي التدابير القانونية دورًا رئيسيًا في منع ومكافحة الجريمة المعلوماتية. وهذه التدابير ضرورية في جميع المجالات، بما في ذلك التجريم والصلاحيات الإجرائية والولاية القضائية والتعاون الدولي ومسؤولية مقدّمي خدمات الإنترنت، وعلى الصعيد الوطني، كثيرًا ما تتعلق قوانين الجريمة المعلوماتية، القائمة والجديدة (أو المخطط لها) على حدٍّ سواء، بالتجريم، مما يدّل على التركيز بصفة رئيسية على تجريم الأفعال التي تغطي الجرائم السيبرانية الأساسية وتحديد الاجراءات اللازمة لمكافحتها وضبطها.

[1] Ibid.p.38.

التدابير الاجرائية الواجب اتخاذها للتعامل مع الجرائم المعلوماتية وفقاً لاتفاقية بودابست:

تناول القسم الثاني من اتفاقية بودابست التدابير الاجرائية الواجب اتخاذها على الصعيد الوطني لأغراض التحقيق الجنائي في الجرائم المعلوماتية، والتي تمثل الحد الأدنى الذي ينبغي الالتزام به، وهو ما أوضحته الاتفاقية في الفقرة الثالثة من المادة ٣٩، وتم تناول هذه التدابير في خمسة أبواب:

الباب الأول:الأحكام العامة:

وفي هذا الباب ألزمت الاتفاقية جميع الأطراف بتضمين قوانينها ما يلزم من تدابير وتشريعات تسمح للسلطات المختصة باجراء التحقيقات والاجراءات الجنائية اللازمة في الجرائم بالاضافة الى وضع الشروط والضمانات اللازم توفيرها للتأكد من تطبيق هذه الاجراءات بشكل سليم لا يتعارض مع الحريات وفقا لمبدأ التناسب والذي يشير الى ضرورة تناسب السلطة والاجراء مع طبيعة الجريمة وظروفها.

الباب الثاني:تعجيل حفظ بيانات الكمبيوتر المخزنة:

تشير عملية حفظ بيانات الكمبيوتر الى ابقاء البيانات المخزنة من قبل أصحاب البيانات كمقدمي الخدمة مثلاً بحالة سليمة ومناسبة، وهي بهذا تتعلق بابقاء بيانات موجودة بالفعل في شكل مخزن وحمايتها من أي شيئ من شئنه أن يتسبب في تغيير جودتها أو وضعها الراهن، وهذايختلف عن عملية الاحتفاظ بالبيانات والتي تشير الى الابقاء على بيانات يتم توليدها حاليا لاستخدامها في المستقبل وقد تناوت الاتفاقية هذا الأمر من خلال حكمين:

١- التعجيل في حفظ بيانات الكمبيوتر المخزنة:

" Expedited preservation of stored computer data"

كما سبق الاشارة عاليه فإن عملية الحفظ تقتضي بأن تكون البيانات موجودة بالفعل ومخزنة، وتهدف عملية التعجيل الى ضمان قدرة السلطات

المختصة من الوصول الى البيانات قبل أن يتم تعديلها أو حذفها، وليس معنى حفظ البيانات هنا تجميدها إذ يمكن للمستخدمين الشرعيين لهذه البيانات الحصول على نسخ منها أو الولوج اليها ما لم ترى السلطات المحلية المختصة ضرورة لتجميد التعامل مع هذه البيانات، ولا يجوز أن تتجاوز مدة التجميد ٩٠ يوماً.

٢- التعجيل في الحفظ والكشف الجزئي عن بيانات الحركة
"data partial disclosure of traffic& Expedited preservation "

تم تعريف بيانات الحركة في الفقرة الرابعة من المادة الأولى لتشير الى: فئة من بيانات الكمبيوتر الخاضعة لنظام قانوني خاص يتم توليدها في اطار من الاتصالات بغرض توجيه الاتصال من مصدره الاصلي الى متلقيه المستهدف، ويعد الحصول على بيانات الحركة أمراً حاسماً في تحديد جهات الاتصال وبالتالي تحديد هوية متصل قد يكون مسئولا عن إحدى الجرائم المعلوماتية كتوزيع نسخ غير قانونية أو نشر مواد إباحية متصلة بالاطفال، وترجع أهمية التعجيل في حفظ هذه البيانات الى أن هذه البيانات تخزن عادة لمدد قصيرة جدا وقد تعرقل قوانين حماية الحرية الشخصية أو تحظر تخزين مثل هذه البيانات بالاضافة الى أنها تكون عادة مرتبطة بأكثر من متصل أو مقدم للخدمة يمتلك كل منهم جزء من اللوحة ولا يمكن استيضاح ما تم فعلا الا بجمع هذه الأجزاء مع بعضها البعض.

الباب الثالث: أمر التقديم:

يشير أمر التقديم الى قيام السلطات المختصة باصدار أمر يلزم شخص يحوز على بيانات أو يمتلك إمكانية الوصول اليها"كمقدمي الخدمة" بتقديم بيانات حاسوبية مخزنة لديه بالفعل أو يمكنه الوصول اليها للسلطة المختصة، وهو يعد إجراء مرن حيث قد يكون لدى هذا الشخص الحائز للبيانات الرغبة في مساعدة السلطة المختصة في الحصول على هذه البيانات مع حاجته لاطار قانوني مناسب يساعده على ذلك، كما أن أمر التقديم قد يكون خطوة أولية تتبعه أجراءات أكثر قوة كالتحفظ على بيانات أو اعتراضها.

الباب الرابع: البحث عن بيانات الكمبيوتر المخزنة ومصادرتها:

تتيح القوانين الإجرائية للسلطات المختصة البحث عن الأدلة الملموسة ومصادرتها لأغراض التحقيق وجمع الأدلة، الأمر الذي يمثل تحدياً في حالة التعامل مع المعلومات كدليل حيث أن المعلومات والبيانات المخزنة عناصر غير ملموسة وبالتالي لا يمكن التحفظ عليها وتأمينها بنفس الطريقة المتبعة مع الأدلة المادية الأخرى، وفي سبيل ذلك يمكن التحفظ على الوسيط المادي الذي خزنت عليه هذه البيانات، كما يمكن الحصول على نسخة منها على وسيط مادي "كطابعتها أو نسخها على CD" مع تحديد امكانية السماح بالوصول واستخدام هذه المعلومات من عدمه، ولا شك أن الطبيعة الخاصة للمعلومات والجريمة المعلوماتية تستدعي في الكثير من الأحيان توفير إجراءات إضافية تسمح للسلطة المختصة بالحصول على نسخة منها كحالة أن تكون المعلومات المرجو الحصول عليها غير مخزنة على جهاز الحاسب الآلي المستخدم وانما مخزنة بواسطة الشبكة العنكبوتية على وسيط آخر يقع خارج الحدود الجغرافية للدولة، وكحالة رسائل البريد الالكتروني العابرة التي تحتاج الى استصدار أوامر لاعتراضها.

الباب الخامس: جمع بيانات الكمبيوتر في الوقت الحقيقي:

تناول هذا الباب الأحكام الخاصة بجمع واعتراض بيانات الكمبيوتر في الوقت الحقيقي والتزامات السرية الواجب مراعاتها، ويوجد نوعان من بيانات الكمبيوتر التي يمكن جمعهما وفق هذا الباب هما;بيانات الحركة وبيانات المحتوى، تشير بيانات الحركة الى بيانات الكمبيوتر التي توضح منشأ والوجهة والمسار والزمن وتاريخ وحجم ومدة ونوع الاتصال، في حين تشير بيانات المحتوى الى مضمون هذا الاتصال كاحتوائه على صور معينة أو نصوص كتابية أو تسجيلات صوتية مثلاً، ويلاحظ أن عملية

جمع البيانات لا تأثر على عملية تدفق البيانات، فالاتصال يكون مستمراً أثناء تتبعك لبيانات الحركة الخاصة به أو نسخك لمحتواه على أي وسيط[1].

وترجع أهمية جمع هذه البيانات الى أنها في العادة لا يتم الاحتفاظ بها وبالتالي اذا لم تجمع في أثناء حدوثها فقد لا يكون هناك امكانية للوصول اليها، كما أن الشخص الذي يقوم بهذا النوع من الاتصالات قد يكون على دراية فنية تسمح له بتغيير مسار الاتصال عبر عدد من الشبكات الأمر الذي يشكل تحديا في تتبع بياناته خاصة اذا لم يتم جمعها في وقت حدوث الاتصال.

التدابير الاجرائية للتعامل مع الجرائم المعلوماتية في القانون المصري:

تناول المشرع المصري الاحكام والقواعد الاجرائية الواجب اتباعها للتعامل مع الجرائم المعلوماتية في الباب الثاني من القانون رقم ١٧٥ لسنة ٢٠١٨ والتي جاءت متسقة مع ما أقرته اتفاقية بودابست.

ففي البداية أوضحت المادة الخامسة السلطات التي يجوز لها منح صفة الضبطية القضائية وكيفية منحها ومن تمنح لهم، ثم أوضحت المادة السادسة جواز اصدار أمراً مسبباً لمأموري الضبط القضائي يسمح لهم بضبط أو سحب أو جمع أو التحفظ على البيانات والمعلومات وأنظمة المعلومات وتتبعها في أي مكان أو نظام أو برنامج أو دعامة الكترونية أو حاسب، كما يمكن أن يجيز له هذا الأمر البحث والتفتيش والدخول والنفاذ الى برامج الحاسب وقواعد البيانات وغيرها من الأجهزة والنظم المعلوماتية، ويجوز للسلطة المختصة وفق نفس المادة أن تصدر أمرا لمقدم الخدمة بتسليم ما لديه من بيانات أو معلومات تتعلق بنظام معلومات أو مستخدمين أو بيانات حركة لمأمور الضبطية القضائية الذي يحمل هذا الأمر وهو ما يتفق مع الدور الذي يؤديه أمر التقديم من ناحية ويوضح نطاق الصلاحيات التي يتيحها القانون من جهة أخرى ، وفي جميع الأحوال السابقة لا بد أن

[1] Council of Europe.European Treaty Series - No. 185(2001).Convention on Cybercrime. Budapest.p.7-11.

يكون الأمر مسبب وهو ما يحافظ على قدر مناسب من الحرية الشخصية ويضمن عدم التعدي عليها الا بسبب.

كماأقر هذا القانون لجهة التحقيق المختصة أن تأمر بحجب المواقع التي قد تمثل خطرا على أمنها القومي، أو تقوم بعرض أو بث أو أرتكاب أفعال تعد جرائم معلوماتية وفق أحكام هذاا لقانون، وذلك من خلال عرض أمر حجب على المحكمة المختصة خلال ٢٤ ساعة وألزم القانون المحكمة باصدار أمرها بالقبول أو الرفض خلال مدة لا تتجاوز ٧٢ ساعة من وقت اللعرض، وفي الحالات الطارئة التي لا تحتمل مثل هذا الوقت أجاز القانون اخطار والزام مقدم الخدمة مباشرة بالحجب المؤقت مع تحرير محضراً بذلك وبعدها تصدر المحكمة أمراً اما بتأييد هذا الأمر أو وقفه.

نظراً للطبيعة الفنية الخاصة للجرائم المعلوماتية التي تقتضي نوع خاص من المعرفة الفنية فقد سمح هذا القانون وفق مادته العاشرة بانشاء سجلان لقيد الخبراء العاملون بالجهاز وغير العاملون بالجهاز وذلك للاستعانة بهم مع تحديد قواعد عملهم، كما أقرت المادة الحادية عشر التساوي في الحجية بين الأدلة الالكترونية وغيرها من الأدلة الجنائية متى ما توافرت فيها الشروط الفنية اللازمة[١].

التدابير الاجرائية للتعامل مع الجرائم المعلوماتية في القانون الجزائري:

حدد المشرع الجزائري في المادة الرابعة من القانون رقم ٩-٤ لسنة ٢٠٠٩ الحالات التي تسمح بالمراقبة الالكترونية مع التأكيد على عدم جواز القيام بهذه المراقبة دون الحصول على اذن كتابي من السلطة القضائية المختصة، وذلك للحفاظ على الحريات الشخصية وضمان عدم التدخل فيها الا في حدود الضرورة، وهو نفس السبب الذي دعا المشرع في المادة التاسعة من ذات القانون لايضاح أنه لا يجوز استخدام المعلومات المتحصل عليها عن طريق عمليات المراقبة المنصوص عليها في هذا القانون الا في الحدود الضرورية للتحريات أو التحقيقات القضائية.

[١] جمهورية مصر العربية.قانون مكافحة جرائم تقنية المعلومات.مصدر سابق.الباب الثاني- الأحكام والقواعد الاجرائية – مأمورو الضبط القضائي.

تدرج المشرع في تحديد الخطوات التي يتم اتخاذها للحصول على الأدلة الرقمية حيث تبدأ بالتفتيش في النظام الأساسي، وحال الاعتقاد بارتباط الأدلة اللكترونية المراد جمعها بنظام اخر يكون من حق ضابط الشرطة القضائية المختصة أو السلطة القضائية المختصة تمديد عملية التفتيش لهذا النظام، ويتبع عملية التفتيش اذا ما وجدت معلومات مفيدة اعطاء الصلاحية بالحجز على هذه البيانات مع امكانية تخزينها على اي وسيط مادي يمكن التعامل معه، وفي حال استحال الحجز على المعلومات المراد الحصول عليها مع الحاجة الماسة لها أجاز المشرع في المادة السابعة من القانون للسلطة القائمة بعملية التفتيش أن تستخدم التقنيات المناسبة لمنع الوصول الى هذه المعلومات، وهو ما يتوافق مع الباب الرابع من القسم الثاني في اتفاقية بودابست الخاص بالبحث عن بيانات الكمبيوتر المخزنة ومصادرتها، ونظرا للطبيعة الفنية الخاصة لمثل هذه الجرائم فقد أجاز المشرع الجزائري للسلطة المختصة الاستعانة بشخص له دراية بكيفية عمل المنظومة المعلوماتية محل التفتيش بغرض مساعدتها في انجاز عملها.

أفرد المشرع الجزائري الفصل الرابع من هذا القانون لتنظيم التزامات مقدمي الخدمة، وحفظ بيانات الحركة نظرا لطبيعة بيانات الحركة التي لا تسمح في العادة بتخذينها الأمر الذي يترتب عليه ضياعها اذا لم يتم الاحتفاظ بها حال وقوعها، بالاضافة الى قدرة مقدم الخدمة على الوصول السريع الى الكثيرمن البيانات، مما يترتب عليه تسهيل مهمة فرق العمل حال تعاونه معها[١].

الخاتمة:

١- تتمتع ظاهرة الجريمة المعلوماتية بالحداثة النسبية، فلم تبدأ في الظهور الى في الستينات من القرن الماضي، وتأخر ظهورها في الدول النامية بشكل نسبي نظراً لارتباطها بتكنولوجيا المعلومات التي لم تنتشر في دول العالم النامي الا في وقت متأخر، ولكن مع

[١] الجمهورية الجزائرية.القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحته.مصدر سابق.الفصل الثالث – القواعد الاجرائية.

بداية القرن الحادي والعشرين أخذ انتشارها سواء في الدول النامية أو المتقدمة قفزة كبيرة.

٢- لا يوجد تعريف محدد للجريمة المعلوماتية وان كان هناك فهم عام للأفعال التي يوقع ارتكابها فاعلها تحت طائلة هذا النوع من الجرائم، كم يوجد العديد من التصنيفات الرئيسية والفرعية لتوضيح ما يمكن اعتباره جريمة معلوماتية.

٣- يتمتع هذا النوع من الجرائم بالعديد من الخصائص والسمات التي تميزه عن غيره من الجرائم لعل أبرزها هوا اتساع نطاقه الجغرافي وحاجته الى دراية فنية عالية وصعوبة اثباته وارتفاع الخسائر الاقتصادية الناجمة عنه خاصة فيما يتعلق بمجال انتهاكات حقوق الملكية الفكرية الأمر الذي يستلزم تضافر الجهود على المستوى الدولي لمجابهة هذاالنوع من الجرائم.

٤- على الرغم من انخفاض نسبة الجرائم المعلوماتية المتعلقة بالملكية الفكرية مقارنة بباقي أنواع الجرائم المعلوماتية، الا أن الخسائر الاقتصادية المترتبة عليها تفوق الخسائر الاتصادية المترتبة على باقي أنواع هذه الجرائم.

٥- هناك العديد من المحاولات على المستويان الدولي والمحلي للتعامل مع هذه الظاهرة والحد منها وان كان ضعف الامكانات المادية والبنى التحتية في الدول النامية يحول دون رصدها والتعامل معها بالشكل المطلوب.

قائمة المراجع

أولاً: المراجع العربية:

- الأمم المتحدة (٢٠١١). مداولات الاجتماع الأول لفريق الخبراء المعني باجراء دراسة شاملة عن الجريمة السيبرانية، فيينا.
- الحوامدة.لورنس(٢٠١٧).الجرائم المعلوماتية أركانها وآلية مكافحتها(دراسة تحليلية مقارنة).**مجلة الميزان للدراسات الإسلامية والقانونية**.مج٤.ع١.ص١٩٧-٢٠٠.
- الشمري، غانم (٢٠١٦). الجرائم المعلوماتية- ماهيتها - خصائصها - كيفية التصدي لها قانونياً.ط١. دار الثقافة,الدار العلمية الدولية.
- النهوي.أحلام(٢٠١٧).جرائم الحاسب الآلي وسبل مكافحتها.**المجلة الليبية العالمية**.ع٢٠.ص.١٢.
- عمیار، ریم، (٢٠١٨). تأثير الجريمة المعلوماتية على الاقتصاد الوطني العربي(مذكرة مكملة لنيل درجة الماستر في القانون).جنائي أعمال.كلية الحقوق والعلوم السياسية.جامعة العربي بن مهيدي.
- [1] فريال، لعاقل.(٢٠١٥). الجريمة المعلوماتية في ظل التشريع الجزائري(مذكرة مكملة لنيل درجة الماستر في القانون العام).قانون جنائي.كلية الحقوق والعلوم السياسية.جامعة جامعة اكلي محند - البويرة.
- مختاري، إكرام. (٢٠١٦). خصوصيةالجريمة المعلوماتية وإشكاليةالاختصاص.**منشورات مجلة دفاتر قانونية – سلسلة دفاتر جنائية**.ع١.ص.

ثانياً:المراجع الأجنبية

- Gercke, Marko. (2012). Understanding cybercrime: Phenomena, challenges and legal response.First Edition,ITU.

www.itu.int/ITUD/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf

- Hosseinian-Far, A., Jahankhani, H., & Al-Nemrat, A. (2014). Cyber crime Classification and Characteristics.The University of Northampton.
- Settapong.Malisuwan(2007). Conflict of Domain Name and Trademark in Thailand. **International Journal of The Computer**, the Internet and Management Vol. 15.p.63-64.
- Nurse,Jason. (2019). The OxfordHandbook of Cyberpsycholog - Cybercrime and You: How Criminals Attack and the Human Factors That They Seek to Exploit.First Edition.printed by:GPI Group.UK. https://books.google.com.eg/books?id=9guXDwAAQBAJ&pg=PR7&source=gbs_selected_pages&cad=2#v=onepage&q&f=false
- Rantala,Ramona. (2018). Cybercrime against Businesses, 2005. U.S. Department of Justice.
- Siles. Emile. (2015). Cybersecurity and Cybercrime: Intellectual Property and Innovation. **SSRN Electronic Journal.** Vol. 8, No2.p2-3.
- Symantec.(2018). Norton Cyber Security Insights Report 2017.
- The World Bank. (2019). Individuals using the Internet (% of population) .14/4/2020. https://data.worldbank.org/indicator/IT.NET.USER.ZS?view=map
- UNITED NATIONS OFFICE ON DRUGS AND CRIME.(2013).Comprehensive Study on Cybercrime. Vienna.http://www.unodc.org/documents/organizedcrime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf
- United Nations. (2015). INFORMATION ECONOMY REPORT- Unlocking the Potential of E-commerce for Developing Countries.Switzerland
- Yar, Mojid & Steinmetz, (2019). Cybercrime and Society.Third Edition . London:SAGE. https://books.google.com.eg/books?hl=en&lr=&id=gpuHDwAAQBAJ&oi=fnd&pg=PP1&ots=flxTugCwFW&sig=f1K7t0BFvo4je2YGzU2mw2XzMw&redir_esc=y#v=onepage&q&f=false