الجريمة الإلكترونية

أ/ياسمينة بونعارة

جامعة الأمير عبد القادر للعلوم الإسلامية

ملخص

تعد الجريمة الإلكترونية، من الجرائم التي استحضرتها الممارسة السيئة لثورة التكنولوجيا المعلوماتية، تختلف كثيرا عن الجريمة التقليدية، في طبيعتها، ومضمونها، ونطاقها، وتأثيراتها، وأنواعها، ووسائلها وأدواتها، وحتى في خصوصية وتميز مرتكبيها، وقد ساهمت عوامل التحضر السريع، والرغبة بتحقيق الثراء، وتوافر الفرص لارتكابها في انتشارها، وارتفاع نسبة ضحاياها، خاصة مع قصور وسائل الرقابة، وضعف التشريعات القانونية، وفرض العقوبات لتحجيم تأثيرات هذا النوع من الجرائم المستحدثة، التي تستهدف الأفراد والبيانات والدول، وترهق كاهلها بالخسائر الفادحة في مختلف قطاعات الحياة، فهي تمثل حقيقة "الاستعمار الإلكتروني" في أبشع صوره.

Summary

The cyber-crime, crimes that Asthoudrtha bad practice for a revolution of information technology, are very different from conventional crime, the nature, content, scope, and its effects, and types, and means and tools, and even in the privacy and distinguish the perpetrators, has been rapid urbanization factors have contributed, and the desire to achieve wealth, and the availability of opportunities to commit in the spread, the higher the proportion of the victims, especially with the palaces and media censorship, and the weakness of legislation, and the imposition of sanctions to curtail the effects of this type of innovative crimes, which target individuals, data and states, and are overburdened losses heavy in the various sectors of life, they represent the fact "colonization e "in its worst form.

مقدمة

يعيش العالم اليوم أزهى عصوره العلمية والتكنولوجية، والتي يعود الفضل فيها للثورة المعلوماتية، التي حققت طفرة ملحوظة في مستويات التقدم التقني والعلمي شملت معظم نواحي الحياة، خاصة التطور الهائل في مجال الاتصالات وأنظمة المعلومات، وأضحى العصر عصر المعلومات بامتياز، لا سيما وقد أصبحت سلعة تباع وتشترى، ترتبط بمختلف نواحي الحياة ومصدر قوة اقتصادية وسياسية وعسكرية، تسعى البلدان للتنافس في امتلاكها، وصار الوعي بأهميتها وقيمتها مظهرا من مظاهر رقي الشعوب والأمم وتحضرها.

لقد أصبحت المعلومات وصناعتها ضرورة من ضروريات العصر الحديث، والمحرك الأساسي لأي تقدم إنساني في مختلف مجالات الحياة، ومنذ أن لبس العصر لباس التقانة والآلية، الذي تفننت الثورة التكنولوجية في صناعته، أصبح التعامل مع منجزاتها يحتاج من الفرد مجهودا ضخما ووقتا كبيرا لفهم أسرار منتجاتها الجديدة وتسخيرها لتسهيل وتسيير شؤون حياته.

فهناك شواهد كثيرة على إيجابية التسهيلات التي أتاحها التقدم العلمي والتكنولوجي، والتي فتحت آفاقا جديدة، وفرصا متزايدة لتحسين أحوال معيشة الشعوب والأفراد، وتيسير حياتهم وممارستهم لمهام الحياة المختلفة، وقد ظهرت العديد من الاختراعات والابتكارات التي تخدم الإنسان وتقدم له الرفاهية، وتوفر الجهد والوقت والأمان والسلامة وتضيف راحة وبهجة وقيمة لحياته، غير أن انحراف هذه الوسائل والصناعات التكنولوجية الحديثة عن مسارها، تجعل الإنسان يدفع ضريبتها.

لم يكن أحد من مخترعي الإنترنت يعلم أنه في يوم من الأيام سوف تستغل هذه الوسيلة الاتصالية في الإجرام، لكن مع مرور الزمن وتزايد عدد المرتبطين بهذه الشبكة، ظهر هذا النوع الجديد من الإجرام "جرائم الكمبيوتر والانترنت"، أو ما يسمى "Cyber Crimes "، الذي يرجعه المختصون إلى التباين الموجود بين مستويات المشتركين في خدماتها.

هذه الظواهر الإجرامية المتزايدة تدق ناقوس الخطر لتنبيه مجتمعاتنا عن حجم المخاطر والخسائر التي يمكن أن تخلفها، خاصة أنها جرائم ذكية تنشأ وتحدث في بيئة خاصة (إلكترونية رقمية)، ويقترفها أشخاص متميزون (أذكياء ويمتلكون أدوات المعرفة التقنية)، مما يسبب خسائر كبيرة على جميع المستويات الاقتصادية والاجتماعية والثقافية والأمنية.

وفي هذا المقال سنبدأ بالتعرف على "**ماهية الجريمة الإلكترونية**" وذلك بالتعرض لمفهومها، التطور التاريخي الذي مرت به، خصائصها، ثم نتعرف على "**دوافع مرتكبي هذا النوع من الجرائم**"، ثم على"**مرتكبيها**" وأصنافهم، بعدها نتعرض "**لتصنيف هذه الجرائم**" وأنواعها، لنصل في الأخير إلى

الإجابة على إشكالية فرضت نفسها على الواجهة مؤخرا والمتمثلة في الاطلاع على "**واقع الجريمة الإلكترونية في الجزائر**" هذه الآفة الخطيرة والمتنامية يوما بعد يوم.

أولا: ماهية الجريمة الإلكترونية

لقد تغيرت أنماط الجريمة، فلم تعد الاعتداءات تستهدف النفس والمال فقط، بل طالت المعلومات، وهو ما أصبح يعرف على الساحة الدولية بإجرام ذوي"**الياقات البيضاء White Collar crime** "، حيث يستطيع المجرمون العصريون ارتكاب أبشع الجرائم، ليس فقط دون إراقة دماء، ولكن أيضا بدون الانتقال من أماكنهم، بل ترتكب الجريمة في أمن وهدوء، وهو ما جعل البعض يصفها **بالجرائم الناعمة (Soft Crime)**، فبمجرد لمس لوحة المفاتيح يحدث دمارا وخرابا في اقتصاديات كبرى الشركات، وهذا النوع من الجرائم ليس مقصورا على منطقة، أو دولة معينة، لكنها مشكلة عالمية [1].

1- مفهوم الجريمة الإلكترونية

تعتبر الجريمة المعلوماتية من بين الجرائم التي تباينت تسمياتها عبر المراحل الزمنية لتطورها التي ارتبطت بتقنية المعلومات، فقد اصطلح على تسميتها بداية "بإساءة استخدام الكمبيوتر"، ثم "احتيال الكمبيوتر"، "فالجريمة المعلوماتية"، بعدها "جرائم الكمبيوتر"، و"الجريمة المرتبطة بالكمبيوتر"، ثم "جرائم التقنية العالية"، إلى "جرائم الهاكرز"، "فجرائم الانترنت"، وأخيرا "السيبر كرايم"[2].

وقد حاولت العديد من الأعمال الأكاديمية تعريف" الجريمة الإلكترونية"، ومع ذلك فلا تبدو التشريعات الوطنية، مهتمة بتعريف دقيق للمصطلح، فمن أصل حوالي 200 مكون منبثقة من التشريعات الوطنية التي استشهدت بها البلدان في الرد على الاستبيان الدولي في تحديد معنى الجريمة الإلكترونية، استخدم أقل من خمسة في المائة كلمة "**الجرائم الإلكترونية**" في العنوان أو في السياق التشريعي وبدلا من ذلك فالاستخدام الأكثر شيوعا في التشريعات هو مصطلح "**جرائم الكمبيوتر**"، و"**الاتصالات الإلكترونية**"، و"**تكنولوجيا المعلومات**"، أو "**الجريمة ذات التقنية العالية**"، وفي الممارسة العملية فإن العديد من هذه المفردات من التشريعات التي تم إنشاؤها للجرائم الجنائية والتي هي المدرجة في مفهوم الجريمة الإلكترونية، مثل الدخول غير المصرح به لنظام الكمبيوتر، أو التدخل في نظام

---

[1] -سميرة معاشي: **ماهية الجريمة المعلوماتية**، مجلة المنتدى القانوني، ع 07، جامعة محمد خيضر، بسكرة، أفريل 2010، ص 275، 276.

[2] -مليكة عطوي: **الجريمة المعلوماتية**، حوليات جامعة الجزائر، ع 21، جوان 2012، ص 08.

الكمبيوتر أو البيانات، حيث لم تستخدم التشريعات الوطنية على وجه التحديد مصطلح "**الجريمة الإلكترونية**" في عنوان فعل أو قانون مثل: " **قانون الجرائم الإلكترونية**"[1].

وتعرف الجريمة بأنها: "الارتكاب المتعمد لفعل ضار من الناحية الاجتماعية أو فعل خطير محظور يعاقب عليه القانون"، وتمثل الجرائم الإلكترونية مجموعة الأفعال والأعمال غير القانونية التي تتم عبر معدات أو أجهزة إلكترونية أو شبكة الانترنت أو تبث عبرها محتوياتها، وهي ذلك النوع من الجرائم التي تتطلب الإلمام الخاص بتقنيات الحاسب الآلي ونظم المعلومات لارتكابها أو التحقيق فيها ومقاضاة فاعليها [2]، يقول الدكتور محمد صالح العادلي*: "الجريمة الالكترونية هي الابن غير الشرعي الذي جاء نتيجة للتزاوج بين ثورة تكنولوجيا المعلومات مع العولمة، أو هي المارد الذي خرج من القمقم ولا تستطيع العولمة أن تصرفه بعد أن أحضرته الممارسة السيئة لثورة تكنولوجيا المعلومات".

ويعرفها مكتب تقييم التقنية بالولايات المتحدة الأمريكية بأنها: "الجريمة التي تلعب فيها البيانات الحاسوبية، والبرامج المعلوماتية دورا رئيسيا" [3]، وقد اتجه جانب كبير من الفقهاء إلى اعتماد التعريف الذي تبنته منظمة التعاون الاقتصادي والتنمية (OCDE) للجريمة المعلوماتية في اجتماع باريس عام 1983، من أنها: "**كل سلوك غير مشروع، أو غير أخلاقي، أو غير مصرح به، يتعلق بالمعالجة الآلية للبيانات أو نقلها**"، وهو تعريف تبنى أكثر من معيار، يتعلق الأول بوصف السلوك، أما الثاني فاتصال السلوك بالمعالجة الآلية للبيانات أو نقلها[4].

ويمكن تعريف الجريمة الإلكترونية بأنها كل أشكال السلوك غير المشروع، والمتعمد الذي يرتكب باستخدام الحاسب الآلي المرتبط بالانترنت، والتي تمس به أو بمحتوياته أو بالعمليات التي تتم بواسطته، بغرض إلحاق الضرر بالضحية أو الكسب المادي أو غير ذلك من الأغراض، من طرف أفراد على دراية كاملة بتقنيات التكنولوجيا المعلوماتية وأسرارها.

2- التطور التاريخي للجريمة الإلكترونية

---

(1) -ذياب موسى البداينة: **الجرائم الإلكترونية : المفهوم والأسباب**، ورقة علمية مقدمة في الملتقى العلمي: الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية، خلال الفترة من 02-04 سبتمبر 2014، كلية العلوم الإستراتيجية، الأردن، ص 05.

* أستاذ القانون الجنائي بكلية الحقوق بمسقط، وجامعة الأزهر بمصر ، ومحامي بالمحكمة العليا الدستورية بمصر.

(2) - عبد الفتاح مراد: **شرح جرائم الكمبيوتر والإنترنت**، دار الكتب والوثائق المصرية، دط، دت، ص 38.

(3) - محمد عبيد الكعبي: **الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الانترنت**، دار النهضة العربية،القاهرة، ط2، 2009، ص 33.

(4) -سميرة معاشي: مرجع سابق، ص 278.

يتجلى صراع الإنسان من أجل حاضره ومستقبله في حاجته الدائمة إلى اتخاذ القرارات السليمة، وتتوقف صحة القرارات على مدى توافر المعلومات المتصلة بالمشكلة المطروحة، ومن هنا يكمن الدافع الأساسي وراء حرص الإنسان على تجميع المعلومات المرتبطة بالإنجازات السابقة وأهمية تنظيمها[1]، ومفهوم جريمة الكمبيوتر مر بتطور تاريخي تبعا لتطور التقنية واستخداماتها ويمكن تقسيمها إلى ثلاثة مراحل:

المرحلة الأولى: من شيوع استخدام الكمبيوتر في الستينات ومن ثم السبعينات:

بظهور استخدام الكمبيوتر وربطه بالشبكة في الستينات إلى السبعينيات، ظهرت أول معالجة لجرائم الكمبيوتر في شكل مقالات صحفية تناقش التلاعب بالبيانات المخزنة وتدمير أنظمة الكمبيوتر و التجسس المعلوماتي، وشكلت موضوع التساؤل إذا ما كانت هذه الجرائم مجرد حالة عابرة أم ظاهرة إجرامية مستجدة ؟ وهل هي جرائم بالمعنى القانوني أم مجرد سلوكيات غير أخلاقية في مجال المعلوماتية؟ ، فبقيت محصورة في إطار السلوك اللاأخلاقي دون النطاق القانوني ومع توسع الدراسات تدريجيا و خلال السبعينات بدأ الحديث عنها كظاهرة إجرامية جديدة [2].

المرحلة الثانية: في الثمانينات

وفي الثمانينات ظهر نوع جديد من الجرائم ارتبط بعمليات اقتحام نظم الحاسوب عن بعد ونشر الفيروسات عبر شبكات الكمبيوتر ،الذي سبب تدمير الملفات و البرامج أين شاع اصطلاح "الهاكرز"، المعبر عن مقتحمي النظم، وبقي دائما الحديث عن دوافع هذه الجرائم محصور في اختراق أمن المعلومات وإظهار التفوق التقني من قبل مرتكبي هذه الأفعال الذين لم يتعدوا فئة صغار السن العباقرة في هذا المجال، لكن بتزايد خطورة هذه الممارسات أصبح من الضروري إعادة تصنيف الفاعلين وتحديد طوائفهم خاصة بعد تحول الجريمة من مجرد مغامرة و إبداء التفوق إلى أفعال تستهدف التجسس والاستيلاء على البيانات الاقتصادية والاجتماعية والسياسية والعسكرية [3].

المرحلة الثالثة: في التسعينات

---

[1] – حسن عماد مكاوي: **تكنولوجيا الاتصال الحديثة في عصر المعلومات**، الدار المصرية اللبنانية، القاهرة، ط4، 2005، ص 28.

[2] – يونس عرب: **جرائم الكمبيوتر والانترنت– إيجاز في المفهوم والنطاق والخصائص والصور والقواعد الإجرائية للملاحقة والإثبات**، ورقة عمل مقدمة إلى مؤتمر الأمن العربي 2002 – تنظيم المركز العربي للدراسات والبحوث الجنائية، أبو ظبي 10-12 /2002/2، ص 08.

[3] – المرجع نفسه، ص 08.

شهدت التسعينات تناميا هائلا في حقل الجرائم التقنية وتغيرا في نطاقها ومفهومها، وكان ذلك بفعل ما أحدثته شبكة الإنترنت من تسهيل لعمليات دخول الأنظمة واقتحام شبكات المعلومات، فظهرت أنماط جديدة كأنشطة إنكار الخدمة، التي تقوم على فكرة تعطيل نظام تقني ومنعه من القيام بعمله المعتاد، وأكثر ما مورست ضد مواقع الإنترنت التسويقية الناشطة والهامة التي يعني انقطاعها عن الخدمة لساعات خسائر مالية بالملايين، ونشطت جرائم نشر الفيروسات عبر مواقع الإنترنت لما تسهله من انتقالها إلى ملايين المستخدمين في ذات الوقت، وظهرت أنشطة الرسائل والمواد الكتابية المنشورة على الإنترنت أو المرسلة عبر البريد الإلكتروني، المنطوية على إثارة الأحقاد أو المساس بكرامة واعتبار الأشخاص أو المستهدفة الترويج لمواد أو أفعال غير قانونية وغير مشروعة (جرائم المحتوى الضار) [1].

3- خصائص الجريمة الإلكترونية

تعد جرائم المعلوماتية إفرازا ونتاجاً لتقنية المعلومات، فهي ترتبط بها وتقوم عليها، وهذا ما أكسبها لونا وطابعا قانونيا خاصا يميزها عن غيرها من الجرائم التقليدية أو المستحدثة بمجموعة من السمات، قد يتطابق بعضها مع صفات أنواع أخرى من الجرائم هذا من ناحية، ومن ناحية أخرى فإن اختلاف الجرائم المعلوماتية عن الجرائم التقليدية من حيث الأفعال الإجرامية أكسبها خصوصية غير عادية.

إن متابعة جرائم الحاسب الآلي والإنترنت والكشف عنها من الصعوبة بمكان حيث أن هذه الجرائم لا تترك أثرا، فليست هناك أموال أو مجوهرات مفقودة وإنما هي أرقام تتغير في السجلات ومعظم جرائم الحاسب الآلي تم اكتشافها بالصدفة وبعد وقت طويل من ارتكابها،كما أن الجرائم التي لم تكتشف هي أكثر بكثير من تلك التي كشف الستر عنها، وتعود أسباب صعوبة إثبات جرائم الحاسب الآلي إلى خمسة أمور هي:

أولا: أنها كجريمة لا تترك أثرا لها بعد ارتكابها.

ثانيا: صعوبة الاحتفاظ الفني بآثارها إن وجدت.

ثالثا: أنها تحتاج إلى خبرة فنية ويصعب على المحقق التقليدي التعامل معها.

رابعا: أنها تعتمد على الخداع في ارتكابها، والتضليل في التعرف على مرتكبيها.

خامسا: أنها تعتمد على قمة الذكاء في ارتكابها [2].

كما أن ارتباط الجريمة المعلوماتية بجهاز الحاسوب وشبكة الانترنت، أضفى عليها مجموعة من الخصائص والسمات التي ميزتها عن الجرائم التقليدية ولعل من أهمها ما يلي:

---

[1] – المرجع نفسه، ص 08.

[2] –محمد عبدالله منشاوي: **جرائم الانترنت من منظور شرعي وقانوني**، ص 11، الجمعية الدولية للمترجمين www.wata.cc تاريخ التصفح (2015/02/12).

- ❖ الجرائم المعلوماتية جرائم ترتكب عبر شبكة الانترنت فهي حلقة الوصل الرئيسية بين كافة الأهداف المحتملة لتلك الجرائم، كالبنوك والشركات وغيرها من الأهداف التي تكون غالبا الضحية لتلك الجرائم.
- ❖ الجريمة المعلوماتية جريمة عابرة للحدود فالمجتمع المعلوماتي لا يعترف بالحدود الجغرافية، فهو مجتمع منفتح عبر شبكات تخترق الزمان والمكان دون أن تخضع لحرس الحدود، وهو ما يعني أن مساحة مسرح الجريمة المعلوماتية لم تعد محلية، بل أصبحت عالمية، الأمر الذي خلق العديد من المشاكل حول تحديد الدولة صاحبة الاختصاص القضائي بهذه الجريمة، وكذلك حول تحديد القانون الواجب تطبيقه بالإضافة إلى إشكاليات تتعلق بإجراءات الملاحقة القضائية، وغير ذلك من النقاط التي تثيرها الجرائم العابرة للحدود بشكل عام[1].
- ❖ صعوبة إثبات الجريمة الإلكترونية نظرا لارتكابها في الخفاء، وعدم وجود أي أثر إيجابي لما يجري خلال تنفيذها من أفعال إجرامية، حيث يتم نقل المعلومات إلكترونيا، أضف إلى ذلك إحجام مجتمع الأعمال عن الإبلاغ عنها تجنبا للإساءة إلى السمعة وهز الثقة في كفاءة المنظمات والمؤسسات المجني عليها، فضلا عن إمكانية تدمير المعلومات التي يمكن أن تستخدم كدليل في الإثبات في مدة قد تقل عن الثانية الواحدة[2].
- ❖ ارتفاع الخسارة الناجمة عن الجرائم المعلوماتية مقارنة بالجرائم التقليدية، فقد أكدت "انتل سكيوريتي"، الشركة العالمية المتخصصة في تقنيات حماية وأمن المعلومات، أن قطاعات الأعمال العالمية تتكبد خسائر سنوية تصل إلى 400 مليار دولار أمريكي، وأوضحت الشركة أن الهجمات الإلكترونية أصبحت اقتصاداً متناميا قائما بذاته تبلغ قيمته ما بين 2 إلى 3 ترليون دولار سنوياً، أو ما يشكل 15 إلى 20% من القيمة الاقتصادية الناتجة عبر الإنترنت [3]، وقد تكبدت شركة بريطانية خسائر بلغت 1.3 مليار دولار بسبب هجوم إلكتروني واحد، وخسر مصرفين في الخليج 45 مليون دولار في ساعات قليلة، وأعلنت الهند عن تعرض 308371 موقعًا إلكترونيًا للاختراق بين العامين 2011 و2013 [4].

---

(1) – رصاع فتيحة: **الحماية الجنائية للمعلومات على شبكة الانترنت**، مذكرة ماجستير منشورة. تخصص القانون العام، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد، تلمسان، 2011-2012، ص 43.

(2) –محمد علي العريان: **الجرائم المعلوماتية**، دار الجامعة الجديدة للنشر، 2004 ،ص 53.

(3) – إنتل سكيوريتي: **خسائر قطاعات الأعمال من الهجمات الإلكترونية تصل إلى 400 مليار دولار سنوياً**، البوابة العربية للأخبار التقنية، www.aitnews.com، تاريخ التصفح (2015/03/19).

(4) –عبد الإله مجيد: القراصنة يفضلون استهداف الدول الغنية: **الجريمة الالكترونية تكلف العالم 400 مليار دولار سنويا**، http://elaph.com/Web/News/10/06/2014/، تاريخ التصفح، (2015/03/28).

- ❖ الصورة التقليدية للمجرم تكاد تختفي في هاته الجرائم بل وعلى العكس من ذلك فالمجرم المعلوماتي عادة ما ينتمي إلى مستوى اجتماعي مرتفع عن غيره من المجرمين، ونادرا ما يكون محترفا للإجرام أو عائدا، كما أنه لا ينظر إليه كمجرم بالمعنى المتعارف عليه لهذه الكلمة وذلك لكون الأسباب والعوامل التي تقف وراء ارتكاب الجريمة المعلوماتية تختلف بالمقارنة بالجريمة التقليدية [1].
- ❖ قلة الإبلاغ عن وقوع الجريمة المعلوماتية وذلك راجع لسببين، أولهما: هو الخشية والخوف من التشهير، لذلك نجد أن معظم جرائم الانترنت تم اكتشافها بالصدفة، أو بعد فترة طويلة من ارتكابها، والسبب الثاني: هو عدم اكتشاف الضحية للجريمة، مما يعني أن الجرائم التي حدثت ولم يتم اكتشافها هي أكثر بكثير من الجرائم التي تم كشف الستار عنها[2].

إذا فالجريمة الإلكترونية من أحدث أنواع الجرائم، مسرحها العالم الافتراضي غير الملموس، بعيدة عن أي مظهر من مظاهر الجريمة التقليدية، هي جريمة معولمة عابرة للحدود، ينفذها مجرمون من الطراز العالي، أذكياء ومتميزون تقنيا، مما يؤدي إلى تشتيت الجهود الدولية في محاولة تعقبها أو التحري عنها، أو الوصول إلى مرتكبيها.

ثانيا: مرتكبو الجريمة الإلكترونية

ليس ثمة أصدقاء في العالم الإلكتروني، وصغير المجرمين ككبيرهم، والمازح من بينهم كالحاقد، وضمان أمن المعلومات وضمان عدم التعرض للمسؤوليات يوجب التعامل مع الكل على أنهم مصدر للخطر، وليست المسألة إهدار لفكرة حسن النية أو الثقة بالآخرين، إنها الضمان الوحيد للحماية من مصادر خطر بالغة قد تؤدي إلى مسؤوليات وخسائر لا يمكن تقديرها أو تجاوزها[3].

وقد أسفرت الدراسات المختلفة في هذا المجال عن وجود سبعة أنماط من مجرمي المعلوماتية، ويمكن أن يكون المجرم الواحد مزيجا من أكثر من طائفة وتتمثل هذه الطوائف فيما يأتي:

---

(1) –سوير سفيان: **جرائم المعلوماتية**، مذكرة ماجستير منشورة، تخصص العلوم الجنائية وعلم الإجرام، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد، تلمسان، 2010-2011، ص 18،19.

(2) –خالد ممدوح إبراهيم: **أمن الجريمة الالكترونية**، الدار الجامعية، ط1، 2008 ، ص 51.

(3) – محمد دباس الحميد وماركو إبراهيم نينو: **حماية أنظمة المعلومات**، دار الحامد للنشر والتوزيع، الأردن، عمان، ط1، 2007، ص 70.

الطائفة الأولى: (Pranksters) المخادعون: وتضم الأشخاص الذين يرتكبون جرائم المعلوماتية بغرض التسلية والمزاح مع الآخرين، بدون أن يكون في نيتهم إحداث أي ضرر بالمجني عليهم، ويندرج تحت هذه الطائفة بصفة خاصة صغار مجرمي المعلوماتية (الأحداث)[1].

الطائفة الثانية (Hackers) القراصنة: ويقصد "بالهاكر " الشباب البالغ المفتون بالمعلوماتية والحاسب الآلي، الذين لديهم قدرة فائقة على اختراق الشبكات والإبحار في عالم البيانات، دون أهمية لحواجز كلمات المرور أو الشفرات، ولكن أهم ما يميز هذه الفئة أو الطائفة هو عدم وجود نية أو قصد لإتلاف المعلومات أو تخريب أنظمة الحاسب وشبكات الاتصال، ولكن هدفهم هو الاستكشاف والبحث عن الجديد في هذا العالم الخيالي، والميل إلى المغامرة والتحدي، ونادراً ما تكون أفعالهم المحظورة غير شريفة [2].

الطائفة الثالثة (Malicious Hackers) القراصنة الخبيثون أو (Crackers): أشخاص هدفهم إلحاق خسائر بالمجني عليهم دون أن يكون الحصول على مكاسب مالية من ضمن هذه الأهداف، ويندرج تحت هذه الطائفة الكثيرون من مخترعي فيروسات الحاسبات الآلية و موزعيها.

الطائفة الرابعة (Personnel Problem Solvers) أفراد يحلون مشكلة: فهم الطائفة الأكثر شيوعا بين مجرمي المعلوماتية، فهم يقومون بارتكاب جرائم المعلوماتية التي تلحق بالمجني عليهم خسائر ويكون الهدف من ورائها إيجاد حلول لمشكلات مادية تواجههم، ولا يستطيع حلها بالوسائل الأخرى بما فيها اللجوء إلى الجريمة التقليدية وغالبا ما يكون المجني عليه مؤسسة مالية.

الطائفة الخامسة (Career Criminals) المجرمون الموظفون: مجرمي المعلوماتية الذين يبتغون تحقيق الربح المادي بطريقة غير مشروعة، بحيث ينطبق على أفعالهم وصف الجريمة المنظمة، أو على الأقل يشترك في تنفيذ النشاط الإجرامي أكثر من فاعل، و يقترب المجرم المعلوماتي المنتمي إلى هذه الطائفة في سماته من المجرم التقليدي.

أما الطائفة السادسة (Extreme Advocates) دعاة متطرفون: فتدخل في عدادها الجماعات الإرهابية أو المتطرفة، والتي تتكون بدورها من مجموعة من الأشخاص لديهم معتقدات وأفكار اجتماعية أو سياسية أو دينية ويرغبون في فرض هذه المعتقدات باللجوء أحيانا إلى النشاط الإجرامي، ويركز نشاطهم بصفة عامة في استخدام العنف ضد الأشخاص والممتلكات من أجل لفت الأنظار إلى ما يدعون إليه، وإن اعتماد المؤسسات المختلفة داخل الدول على أنظمة الحاسبات الآلية في إنجاز

---

[1] – نائلة عادل محمد فريد قورة: **جرائم الحاسب الآلي الاقتصادية– دراسة نظرية وتطبيقية–**، منشورات الحاتي الحقوقية، ط1، 2005، ص 30.

[2] – رصاع فتيحة: مرجع سابق، ص 56.

أعمالها والأهمية القصوى للمعلومات التي تحتويها في أغلب الحالات قد جعل من هذه الأنظمة هدفا جذابا لهذه الجماعات، ومن الأمثلة الشهيرة في هذا الخصوص قيام إحدى الجماعات الإرهابية المعروفة في أوربا باسم **"الألوية الحمراء" "The Red Brigades"** بتدمير ما يزيد عن 60 مركزا للحاسبات الآلية خلال الثمانينات لتلفت النظر إلى أفكارها ومعتقداتها[1].

وأخيرا تأتي الطائفة السابعة: (The Criminally Negligent) المقصرون جنائيا: والتي تضم واحدة من أهم المشكلات التي تتصل بإساءة استخدام الحاسبات الآلية، ألا وهي الإهمال الذي يترتب عليه في مجال الحاسبات الآلية في أغلب الأحيان نتائج خطيرة قد تصل إلى حد إزهاق الروح، ففي نيوزلندا على سبيل المثال قام اثنان من مبرمجي الحاسبات الآلية بتغيير في أحد البرامج التي تحدد خط سير إحدى الطائرات ولم يتمكنوا من إبلاغ قائد الطائرة بهذا التغيير، مما ترتب عليه تحطم الطائرة لاصطدامها بأحد الجبال وقتل 60 راكبا على متنها، ولقد تمت محاكمة المتهمين بتهمة القتل الخطأ[2].

وهكذا يتميز المجرم الإلكتروني بجميع تصنيفاته على المجرم التقليدي، فلا يكفيه الاحتيال والسرقة فقط، ولكن علاوة على ذلك فهو مستخدم ذكي فطن، قادر على ارتداء قفازات إلكترونية لإخفاء هويته وبصماته الافتراضية لتضليل الوصول إليه.

ثالثا: دوافع ارتكاب الجريمة الإلكترونية

تسبق الحاجات عادة الدوافع، فالحاجة تنشأ من الشعور بالنقص أو الحرمان من شيء ما لدى الفرد، مما يؤدي إلى التأثير في القوى الداخلية لديه (الدوافع)، بغرض إشباع هذه الحاجات التي يحقق تواجدها حالة من الرضا النفسي، وتتنوع دوافع الإقدام على الجريمة الإلكترونية باختلاف منفذيها، وتبعا لطبيعة ودرجة خبرته في مجال المعلوماتية، ويمكن تصنيف هذه الدوافع إلى صنفين دوافع شخصية ودوافع خارجية.

1-الدوافع الشخصية: ويمكن رد الدوافع الشخصية لدى المجرم المعلوماتي إلى دوافع مادية وأخرى ذهنية.

أ/ الدوافع المادية (تحقيق الربح وكسب المال):

يعد الدافع المادي من أكثر الدوافع التي تحرك الجاني لاقتراف الجريمة المعلوماتية، وذلك أن الربح الكبير والممكن تحقيقه من خلالها يدفع بالمجرم المعلوماتي إلى تطوير نفسه حتى يواكب كل حديث يطرأ على التقنية المعلوماتية ويقتنص الفرص ويسعى إلى الاحتراف حتى يحقق أعلى المكاسب وبأقل جهد

---

(1) – سوير سفيان: مرجع سابق، ص 31.

(2) –نائلة عادل محمد فريد قورة: مرجع سابق، ص 63.

دون أن يترك أثرا وراءه، ولقد أشارت في هذا الإطار مجلة (Sécurité informatique) وهي مجلة متخصصة في الأمن المعلوماتي أن 43 % من حالات الغش المعلن عنها قد تمت من أجل اختلاس أموال، و 23% من أجل سرقة معلومات و 19% أفعال إتلاف و15% الاستعمال غير المشروع للحاسوب لأجل تحقيق منافع شخصية[1].

فالرغبة في الثراء والربح المادي عادة ما تواجهها صعوبات بالغة لتحقيقها بالطرق القانونية والمقبولة اجتماعيا، لذا يلجأ بعض الأفراد إلى الجرائم الإلكترونية حيث المستهدف مجتمع أكبر، وسهولة التنفيذ ووفرة المردود وقلة الخطورة، إضافة إلى إمكانية محو الدليل، وتوفر الوسائل التقنية التي تعرقل الوصول إليه مع ضمان التستر وعدم التشهير.

ب/ الدوافع الذهنية: (المتعة والتحدي والرغبة في فهم النظام المعلوماتي وإثبات الذات)

غالبا ما يكون الدافع لدى مرتكبي الجرائم عبر الانترنت الرغبة في إثبات الذات، وتحقيق انتصار على تقنية الأنظمة المعلوماتية، دون أن تكون لهم نوايا آثمة، فيتسابقون لخرق هذه الأنظمة وإظهار تفوقهم عليها، ويعتبر دافع المزاح والتسلية من الدوافع التي تجعل الشخص يقوم بتصرفات، وإن كان لا يقصد من ورائها إحداث جرائم، وإنما بغرض المزاح فقط، ولكن قد تنتج عنها نتائج ترقى إلى درجة الجريمة[2].

2–الدوافع الخارجية: يمكن أن يتأثر المجرم المعلوماتي ببعض المواقف قد تكون دافعة له على اقتراف الإجرام المعلوماتي ولا يسعى في ذلك حينها لا للمتعة والتسلية ولا لكسب المال، ويمكن إبراز أهم هذه الدوافع فيما يلي:

1/الانتقام من رب العمل وإلحاق الضرر به

لوحظ أن العاملين في قطاع التقنية أو المستخدمين لها في نطاق قطاعات العمل الأخرى، يتعرضون لضغوطات نفسية كبيرة، ناجمة عن ضغط العمل والمشكلات المالية ومن طبيعة علاقات العمل المنفرة في حالات معينة، هذه الأمور مثلت في حالات كثيرة قوة محركة لبعض العاملين لارتكاب جرائم الحاسوب، باعثها الانتقام من المنشأة أو رب العمل، وتحديدا جرائم إتلاف البيانات، والبرامج، أمثلة كثيرة كان دافع

---

(1) - سعيداني نعيم: **آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري**، مذكرة ماجستير منشورة، تخصص علوم جنائية، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة باتنة، 2013، ص **60،61**

(2) –يوسف صغيري: **الجريمة المرتكبة عبر الانترنت**، مذكرة ماجستير منشورة، تخصص القانون الدولي للأعمال، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، 2013، ص 40،41.

الجناة فيها إشباع الرغبة بالانتقام، وربما تحتل أنشطة زرع الفيروسات في نظم الكمبيوتر النشاط الرئيس، والتكنيك الغالب للفئة التي تمثل الأحقاد على رب العمل الدافع المحرك لارتكاب جرائمها[1].

ب/دافع التعاون والتواطؤ

هذا النوع كثير التكرار في الجرائم المعلوماتية وغالبا ما يحدث من متخصص في الأنظمة المعلوماتية، أين يقوم بالجانب الفني من المشروع الإجرامي وآخر من المحيط أو خارج المؤسسة المجني عليها يقوم بتغطية عمليات التلاعب وتحويل المكاسب المادية، وعادة ما يمارسون التلصص على الأنظمة وتبادل المعلومات بصفة منتظمة حول أنشطتهم[2].

رابعا: تصنيف الجرائم الإلكترونية

من الصعب تصنيف الجرائم الالكترونية نظرا لاختلافها من مجتمع لآخر من حيث تطوره، ومدى استخدامه للحاسوب، ودرجة اعتماده عليه في مختلف جوانب الحياة، وقد أوجد مشروع الاتفاقية الأوروبية لعام 2001 تقسيما جديدا نسبيا لجرائم الكمبيوتر والانترنت يقسمها إلى أربع طوائف، مع ملاحظة أنها تستثني الجرائم المتعلقة بالخصوصية لوجود اتفاقية أوروبية مستقلة.

1- الجرائم التي تستهدف سلامة وسرية عناصر المعطيات والنظم: وتضم (الدخول غير القانوني، الاعتراض غير القانوني، تدمير المعطيات، اعتراض النظم).

2-الجرائم المرتبطة بالكمبيوتر وتضم: (التزوير المرتبط بالكمبيوتر، الاحتيال المرتبط بالكمبيوتر).

3-الجرائم المرتبطة بالمحتوى: وتضم (طائفة واحدة وفق هذه الاتفاقية، وهي الجرائم المتعلقة بالأفعال الإباحية وغير الأخلاقية).

4- الجرائم المرتبطة بالأشخاص والأموال: وتضم (السرقة والاحتيال والتزوير، والإطلاع على البيانات الشخصية، المعلومات المضللة والزائفة، أنشطة الاعتداء على الخصوصية، إساءة استخدام المعلومات، القرصنة، بث البيانات من مصادر مجهولة، الإرهاب الالكتروني... وغيرها من الجرائم[3].

ويصنف الفقهاء والباحثون جرائم الحاسوب والانترنت ضمن فئات عديدة، ولكن على العموم يمكن تقسيمها إلى مجموعتين أساسيتين:

المجموعة الأولى: جرائم تقع على الانترنت

---

(1) - يونس عرب: **جرائم الكمبيوتر والانترنت- المعنى والخصائص والصور وإستراتيجية المواجهة القانونية**، www.arablaw.org ، تاريخ التصفح (2015/03/23)، ص 92.

(2) - سعيداني نعيم: مرجع سابق، ص 62.

(3) - جعفر حسن جاسم الطائي: **جرائم تكنولوجيا المعلومات-رؤية جديدة للجريمة الحديثة-**، دار البداية، الأردن، عمان، ط1، 2012، ص134.

المجموعة الثانية: جرائم تقع بواسطة الانترنت

المجموعة الأولى: الجرائم التي تقع على الانترنت

أي أن الشبكة تكون عنصر سلبي في الجريمة أي محل للجريمة فقط، فإن هدف المجرم ينصب حول البيانات والمعلومات المخزنة والمنقولة عبر قنوات الانترنت الخاصة أو العامة واختراق الحواجز الأمنية إن وجدت والاعتداء على الأموال...الخ.

1- سرقة المال المعلوماتي

أصبح لبرامج المعلومات قيمه غير تقليديه لاستخداماتها المتعددة في كافة المجالات الاجتماعية، والاقتصادية فهذه القيمة المميزة لبرامج المعلومات تجعلها محلا للتداول، وهنا تبدو أهمية الإنترنت بصفته مصدرا للمعلوماتية، مما أدى إلى ظهور قيمة اقتصاديه جديدة وأموال جديدة، عرفت بالأموال المعلوماتية، وصاحب ظهور هذا المال المعلوماتي جرائم جديدة عرفت بالجرائم المعلوماتية وهذه الجرائم يمكن تصورها من زاويتين:

الأولى: تكون المعلوماتية أداة أو وسيلة للاعتداء

الثانية: تكون المعلوماتية موضوعا للاعتداء (أي سرقة تلك المعلومات).

فالزاوية الأولى يستخدم الجاني المعلوماتية لتنفيذ جرائم سواء ما تعلق منها بجرائم الاعتداء على الأشخاص أو الأموال كالسرقة والنصب وخيانة الأمانة، أما الجرائم من الزاوية الثانية يكون المال المعلوماتي موضوعا لها [1].

كما تتضمن جرائم نظم المعلومات كذلك جريمة إساءة استخدام المعلومات، والمقصود بها الأذى الذي يتم تحقيقه باستخدام هذه المعلومات، مثل عدم تمكين المستفيد من الوصول إليها، أو كشفها، أو استغلالها في إلحاق الضرر بمصالح صاحب المعلومات[2].

وتشمل جرائم الملكية الفكرية نسخ البرامج غير القانوني، والسرقة والاتجار بالأسرار التجارية، كما تشمل جرائم النسخ غير القانوني للمعلومات أو حيازة المعلومات بطريقة غير قانونية، وتوزيع المواد ذات حقوق النشر بما في ذلك الصور في الصيغة الإلكترونية والمطبوعة، والمواد المرئية والسمعية والمخزنة على شرائط أو أقراص مرنة، أو أقراص مدمجة أو على الحاسب...الخ[3].

---

[1] – مديرية تكنولوجيا المعلومات: **أنواع الجريمة الإلكترونية وأهدافها**، قسم نظم المعلومات، شعبة أمنية المعلومات، العراق، ص 5، 6، www.ictmoi.com/elibrary/crime.pdf ، تاريخ التصفح (2015/03/03).

[2] – منال هلال المزاهرة: **تكنولوجيا الاتصال والمعلومات**، دار المسيرة، عمان، الأردن، ط1، 2014، ص 376.

[3] –ذياب البداينة: **الأمن وحرب المعلومات**، دار الشروق، عمان، الأردن، ط1، 2006، ص136.

2- الدخول على المواقع المحجوبة باستخدام (البروكسي):

"البروكسي" هو برنامج وسيط يقوم بحصر ارتباط جميع مستخدمي الإنترنت في جهة واحدة ضمن جهاز موحد، والمعنى المتعارف عليه لدى مستخدمي الانترنت "للبروكسي" هو ما يستخدم لتجاوز المواقع المحجوبة، والتي عادة ما تكون إما مواقع جنسية أو سياسية معادية للدولة، وقد يتم حجب بعض المواقع التي لا يفترض حجبها كبعض المواقع العلمية والتي تنشر إحصائيات عن الجرائم، أو حتى بعض المواقع العادية ويعود ذلك للآلية التي تتم بها عملية ترشيح المواقع، وربما لخطأ بشري في حجب موقع غير مطلوب حجبه، ولذلك فقد تجد من يستخدم البروكسي للدخول إلى موقع علمي أو موقع عادي حجب خطأ، وهذا في حكم النادر والشاذ، في حين أن الغالبية العظمى تستخدم البروكسي للدخول إلى المواقع الجنسية أو المواقع السياسية ولكن بدرجة أقل [1].

3-جرائم الاختراق:

هي عملية اقتحام الأنظمة أو الشبكات الخاصة بأفراد أو منظمات خاصة أو حكومية بمساعدة بعض البرامج المتخصصة في فك وسرقة كلمات السر، وتصريحات الدخول بهدف الاطلاع على المعلومات أو تخريبها أو سرقتها[2]، حيث يتسبب الاختراق في مشاكل مزعجة مثل تبطئ حركة التصفح وانقطاعه على فترات منتظمة، ويمكن أن يتعذر الدخول إلى البيانات، وفي أسوء الأحوال يمكن اختراق المعلومات الشخصية للمستخدم[3].

ويقوم المستخدمون المخولون بفتح حسابات الشركات أو المؤسسات للأغراض غير الشرعية، مثل اللعب بالحسابات الشخصية ومزاولة بعض أنواع الألعاب في الحاسوب للوصول إلى الأسرار الخاصة بالمؤسسة عن طريق كسر كلمات السر الخاصة بالأنظمة خلال خطوط شبكات الهاتف [4]. أما الأهداف الأكثر مباشرة للاختراق هي المعلومات التي يطالها المخترق بالتغيير أو السرقة أو الإزالة، وقد يكون الهدف الثاني الأجهزة وتخريبها وتعطيلها.

---

(1) -محمد عبدالله منشاوي: مرجع سابق، ص 32.

(2) - منصور بن سعيد القحطاني: **مهددات الأمن المعلوماتي وسبل مواجهتها-دراسة مسحية على منسوبي مركز الحاسب الآلي بالقوات البحرية الملكية السعودية بالرياض**، مذكرة ماجستير منشورة، قسم العلوم الإدارية، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، ص 34.

(3) - علوطي لمين: **تحديات الأمن الإلكتروني في المؤسسة**، مجلة أبحاث اقتصادية، ع 06، ديسمبر 2009، جامعة محمد خيضر، بسكرة، كلية العلوم الاقتصادية والتجارية وعلوم التسيير، ص ص 160، 179.

(4) - علاء عبد الرزاق السالمي: **تكنولوجيا المعلومات**، دار المناهج للنشر والتوزيع، الأردن، عمان، ط2، 2007، ص 432.

كما أن أبرز ضحايا الاختراق هي مواقع الانترنت التي يقوم المخترقون بتحريف تصاميمها ومعلوماتها، وهذه العملية تسمى"تغيير وجه الموقع Defacing"، ولا يطال الاختراق الأجهزة إلا إذا كانت موصولة بشبكة الانترنت التي توصل الجهاز بالمحترف[1].

وفيما يلي بعض الأساليب المستخدمة في عمليات الاختراق:

أ– الاقتحام أو التسلل:

يشمل الاختراقات سواء للمواقع الرسمية أو الشخصية، أو اختراق الأجهزة الشخصية واختراق البريد الإلكتروني، أو الاستيلاء عليه، والاستيلاء على اشتراكات الآخرين وأرقامهم السرية، وهي أفعال أصبحت تنشر يوميا في الصحف والأخبار، فكثيرا ما تتداول الصحف والدوريات العلمية الآن أنباء كثيرة عن الاختراقات الأمنية المتعددة في أماكن كثيرة من العالم، ليس آخرها اختراق أجهزة الحاسب الآلي في البنتاغون (وزارة الدفاع الأمريكية) [2].

وفي دراسة للأمم المتحدة عن الجريمة الإلكترونية أجراها مجموعة من الخبراء، أبلغت مؤسسات القطاع الخاص في أوروبا عن معدلات تأذي تراوحت بين 2 و16 في المائة، وكانت تتعلق بانتهاك البيانات بسبب الاقتحام أو التصيد الاحتيالي، والساحة التي تُستخدم فيها هذه الأدوات المختارة لارتكاب الجرائم، مثل:"اعتداءات البوت نت*"، هي ساحة عالمية، فقد كان أكثر من مليون عنوان فريد من عناوين بروتوكول الإنترنت يعمل على الصعيد العالمي كخادم"بوت نت" للتحكُّم في شبكات الحواسيب ومراقبتها في عام 2012 [3].

---

(1) – محمد دباس الحميد وماركو إبراهيم نينو: مرجع سابق، ص 66.

(2)-محمد بن عبد الله بن علي المنشاوي: **جرائم الانترنت في المجتمع السعودي**، مذكرة ماجستير منشورة، قسم العلوم الشرطية، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، ص 57، 58 .

(3)-**Comprehensive Study on Cybercrime** :UNITED NATIONS OFFICE ON DRUGS AND CRIME, Vienna, Draft—February 2013, Uuited Nations, New York, 2013, p 25.

* شبكة الروبوت بالإنكليزية (Botnet): هي مجموعة ضخمة (يبلغ تعدادها بالآلاف وقد يصل للملايين) من الأجهزة التي تم اختراقها عن طريق الإنترنت كل واحد منها يسمى بوت تخدم مكون "البوت نت" أو ما يسمى بسيد البوت Bot)

ب– الإغراق بالرسائل:

يستمد البريد الإلكتروني تعريفه من تعريف الوسائل الإلكترونية وهي: "تكنولوجيا تفاعلية تعمل من خلال أجهزة الكمبيوتر، وتسهل الاتصال الشخصي بنوعيه الفردي والجماعي سواء للمعلومات النصية text، أو الصوتية voice، أو الصور المرئية photos" [1].

وقد ظهر البريد الإلكتروني في الأصل كوسيلة لتبادل الأفكار والمعلومات والتقارير بين العلماء والمسؤولين عن تطوير الشبكة، واستمر في التطور حتى أصبح الآن أكثر تطبيقات الانترنت شيوعا[2]،

ووفقا لدراسة توصلت إليها مجلة "انترنت العالم العربي"، فإن وظيفة البريد الإلكتروني تعد أهم أهداف مستخدمي الانترنت، حيث بلغت نسبة متصفحي البريد الإلكتروني 71٪ من إجمالي مستخدمي الشبكة[3].

فسرعة وسهولة إرسال المعلومات والبيانات بواسطة الشبكة العنكبوتية إلى عدد هائل من المستقبلين سهل كثيرا من أنواع الاحتيال، وأصبح البريد الإلكتروني أكبر وسيلة لانتشار الشائعات في الانترنت عن طريق ما يسمى بالرسائل المتسلسلة، حيث يغرر بقارئ الرسالة لتمريرها إلى عدد معين أو أكبر عدد ممكن من الأشخاص[4].

ج–الفيروسات:

الفيروسات هي في الأصل برامج أعدها شخص أو أشخاص بهدف تخريب وشطب البيانات من ذاكرة الحاسوب، وهي مبرمجة بحيث تعمل من خلال برامج أو برنامج آخر ولها القدرة على نسخ ذاتها، وأبرز طرق انتشارها البريد الإلكتروني أو البرامج التي يتم تحميلها من الانترنت[5].

.(Master)، يستخدم سيد البوت قناة أوامر وتحكم لإدارة شبكته وتنفيذ هجماته، وتسمية "البوت نت" هذه مشتقة من كلمة (Robot Network) أي شبكات الروبوت حيث أن الأجهزة تخدم سيد البوت دون اختيارها، تمامًا مثل أجهزة الروبوت، وبمجرد أن ينضم الجهاز لشبكة الروبوت فإن سيد البوت يستطيع التجسس على صاحب الجهاز دون أن يشعر بذلك.(أنظر الموسوعة الحرة ويكيبيديا) .

(1)-صلاح محمد عبد الحميد: **الإعلام الجديد**، مؤسسة طيبة للنشر والتوزيع، القاهرة، ط1، 2012، ص 95.

(2) – السعيد مبروك إبراهيم: **الاتصال وتداول المعلومات في العالم الرقمي**، دار إمدكو للطباعة والنشر، الدقهلية، مصر، ط1، 2012، ص 227.

(3) – فارس حسن الخطاب: **الفضائيات الرقمية وتطبيقاتها الإعلامية**، دار أسامة للنشر والتوزيع، الأردن، عمان، ط1، 2012، ص 40.

(4) – هباس الحربي: **الشائعات ودور وسائل الإعلام في عصر المعلومات**، دار أسامة للنشر والتوزيع، الأردن، عمان، ط1، 2015، ص 115.

(5) – بسام عبد الرحمن المشاقبة: **الأمن الإعلامي**، دار أسامة للنشر والتوزيع، الأردن، عمان، ط1،2014، ص 101.

ويمكن أن يتعمد أشخاص معينون نشر الفيروسات بإضافتها مع ملفات ترسل بالبريد الإلكتروني، وعندما يقوم المرسل إليه بفتح البريد تفتح هذه الملفات وينتشر الفيروس ويبدأ عمله في التخريب[1].

تم إطلاق اسم "فيروسات الحاسبات" على عائلة متنوعة من البرامج الماكرة MALWARE وهي مشتقة من عبارة "Malicious-logic software"، ويمكننا تصنيف البرمجيات الماكرة إلى أربعة أنواع رئيسية هي: الفيروسات (Viruses)، والدود (Worms)، وأحصنة طروادة (Trojan horses)، وبرامج الإنزال (Droppers) [2].

الفيروس: هو برنامج كمبيوتر مصمم عمدا ليقترن ببرنامج آخر، بحيث يعمل الفيروس عندما يعمل ذلك البرنامج، ومن ثم يعيد إنتاج نفسه باقترانه ببرامج أخرى.

الدودة: تختلف عن الفيروس بنقطة مهمة جدا، فبينما يكرر الفيروس نفسه بوساطة تنفيذ برنامج مصاب، تستغل الدودة فجوات في نظام التشغيل للقيام بهجوم مباشر، وتعتبر الدودة المصممة من قبل روبرت موريس في عام 1988، من أشهر أنواع الدود حيث قامت بشل مئات الحاسبات، والمخدمات التعليمية والحكومية المرتبطة على الانترنت.

حصان طروادة: كما اعتمد حصان طروادة بمظهره الخارجي المسالم وغير المسلح بينما احتوى بداخله على أسلحة فتاكة، تعتمد برامج أحصنة طروادة على المبدأ ذاته، فهي تختبئ ضمن برامج يبدو مظهرها بريئا، وعندما يشغل المستخدم واحدا من هذه البرامج ينشط الجزء الماكر ويقوم بعمل معين مصمم له.

برامج الإنزال: صممت لمراوغة برامج مكافحة الفيروسات، وتعتمد على التشفير غالبا لمنع اكتشافها، ووظيفة هذه البرامج عادة نقل وتركيب الفيروسات، فهي تنتظر لحظة حدوث أمر معين على الحاسب لكي تنطلق وتلوثه بالفيروس المحمول في طياتها [3].

4-المواقع المعادية:

أ-المواقع السياسية المعادية

قد ينظر البعض إلى إنشاء تلك المواقع كظاهرة حضاريه تتماشى مع الديمقراطية والحرية الشخصية، ولكن الواقع غالبا ما يكون الغرض من وراء إنشائها هو معارضة النظام السياسي القائم

---

[1] - علي خليل شقرة: **الإعلام الجديد-شبكات التواصل الاجتماعي-**، دار أسامة للنشر والتوزيع، الأردن، عمان، ط1،2012، ص 165.

[2] - دلال صادق وحميد ناصر الفتال: **أمن المعلومات**، دار اليازوري العلمية للنشر والتوزيع، الأردن، عمان، ط1، 2008، ص 74.

[3] - المرجع نفسه، ص 75، 76.

في بلد ما، فيحاولون من خلال تلك المواقع نشر الأخبار الفاسدة التي تسبب الفرقة بين أفراد الشعب ونظامه السياسي القائم [1].

ويتم غالبا تلفيق الأخبار والمعلومات ولو زورا وبهتانا أو حتى الاستناد إلى جزيء بسيط جدا من الحقيقة، ومن ثم نسج الأخبار الملفقة حولها، وغالبا ما يعمد أصحاب تلك المواقع إلى إنشاء قاعدة بيانات بعناوين أشخاص، يحصلون عليها من الشركات التي تبيع قواعد البيانات تلك أو بطرق أخرى، ومن ثم يضيفون تلك العناوين قسرا إلى قائمتهم البريدية، ويشرعون في إغراق تلك العناوين بمنشوراتهم، وهم عادة يلجئون إلى هذه الطريقة رغبة في تجاوز الحجب الذي قد يتعرضون له ولإيصال أصواتهم إلى أكبر قدر ممكن[2].

ب–المواقع الدينية المعادية

بعض المواقع التي تدعي أنها مواقع دينية إسلامية للدعوة، أو يشرف عليها متخصصون في الدين، أو باحثون في مجالات شرعية، وما إن يدخل المستخدم إلى الموقع حتى يفاجأ بأنه موقع إباحي، أو موقع تنصيري ويبث أفكارا هدامة مخالفة للشريعة وتسيء للدين[3].

ولعل أشهر تلك الوقائع قيام بعض الهواة بوضع بعض البيانات في شكل صور من القرآن الكريم، وبدؤوا في الإعلان عنها من خلال إحدى مواقع البث المجاني الشهيرة وهو موقع شركة "ياهو" yahoo، الأمر الذي استدعى الأزهر الشريف والمجلس الأعلى للشؤون الإسلامية، والكثير من الجهات الإسلامية الأخرى في شتى بقاع الأرض إلى مخاطبة المسؤولين عن الموقع، وتم بالفعل إزالة تلك الصفحات ووضع اعتذار رقيق بدلا منها[4].

---

(1) – مديرية تكنولوجيا المعلومات: **أنواع الجريمة الإلكترونية وأهدافها**، مرجع سابق، ص7.
www.ictmoi.com/elibrary/**crime**.**pdf**، تاريخ التصفح (2015/03/03).

(2) – عبد الحميد إبراهيم محمد العريان: **العلاقة بين الإرهاب المعلوماتي والجرائم المنظمة–ما هو رد فعل القطاع الخاص؟**، الدورة التدريبية: مكافحة الجرائم الإرهابية المعلوماتية، خلال الفترة من 09 إلى 13 أفريل 2006،كلية التدريب، قسم البرامج التدريبية، المغرب، القنيطرة، ص 35.

(3) – مهران زهير المصري: **الخداع باستعمال الانترنت**، مجلة المعلوماتية، ع 72، السنة 07، فيفري 2012 ، ص 13.
www.infomag.news.sy، تاريخ التصفح (2015/03/04).

(4) – محمد حجازي: **جرائم الحاسبات والانترنت (الجرائم المعلوماتية)**، المركز المصري للملكية الفردية، مارس 2005، ص 17.

وقد قامت بعض المنظمات المشبوهة بإخراج فيلم بعنوان "محمد نبي الإسلام"والذي عرض جزء منه عبر موقع اليوتيوب في العاشر من سبتمبر 2012، وقد تصاعدت حدة ردود فعل المسلمين في أنحاء العالم على هذا الفيلم المسيء للرسول الكريم (صلى الله عليه وسلم) [1].

ج–المواقع المعادية للأشخاص أو الجهات

مع انتشار الشائعات والأخبار الكاذبة والتي تطول وتمس رموز الشعوب سواء كانت تلك الرموز فكرية أو سياسية، حتى أنها طالت الرموز الدينية أيضا، ظهرت على شبكة الانترنت بعض المواقع المشبوهة، والتي جندت نفسها لهدف واحد هو خدمة تلك الشائعات والأخبار الكاذبة، وذلك بهدف قذف وسب وتشويه سمعة تلك الرموز السياسية والفكرية، وحتى الدينية، وتشكيك الناس في مدى مصداقية هؤلاء الأفراد، ومحاولة فض الناس من حولهم، وتسميم أفكارهم[2].

فلما شاع استخدام الحاسب الآلي والانترنت وجدنا أن المتعاملين معهما قد استسهلوا الاعتداء على الناس، بالتشهير والسب والقذف، مرورا بجريمة التصنت والتقاط الصور لبعض المستخدمين، ومن ثم التصرف بها وربما تغييرها بما يهدف ليس فقط للنيل منهم، ولكن لتحقيق مصلحة للفاعلين غالبا [3].

فقد أصبحت الإنترنت متنفسا لأحقاد الحاقدين ومرتعا لشهوات المرضى والمعتوهين، من ذوي النفوس المريضة، يعمدون فيها للتشهير والقذف والسب والشتم للأشخاص والهيئات من مختلف القطاعات الاجتماعية، والفكرية والدينية، دون رادع أو خوف من حسيب أو رقيب، "**فمن أمن العقوبة أساء الأدب**".

5- جرائم القرصنة

تواجه شبكة الانترنت ما يسمى "بالقرصنة" من قبل بعض الجماعات التي تؤمن بالحرية المطلقة في الرأي والتعبير والاستخدام أيضا، وهي جماعات تستطيع أن تدخل عبر طرق خاصة تخترق أجهزة الحاسوب، الأرقام السرية للأشخاص وإلى بريدهم الإلكتروني، ما يؤدي إلى معرفة أسرار الناس

---

[1] – عبير شفيق الرحباني: **الاستعمار الإلكتروني والإعلام**، دار أسامة للنشر والتوزيع، الأردن، عمان، ط1، 2015، ص 153.

[2] – منير محمد الجنبيهي وممدوح محمد الجنبيهي: جرائم **الانترنت والحاسب الآلي ووسائل مكافحتها**، دار الفكر الجامعي، الإسكندرية، ط1، 2004، ص 34.

[3] –عبير علي محمد النجار: **جرائم الحاسب الآلي في الفقه الإسلامي**، مذكرة ماجستير منشورة، قسم الفقه المقارن، كلية الشريعة والقانون، الجامعة الإسلامية، غزة، ص 81.

وخصوصيات أعمالهم وحياتهم الشخصية، وهذه أيضا مسألة هامة أثارت أخلاقيات الالتزام في استخدام الانترنت[1].

وقد شهد عام 2010 أخطر قضايا القرصنة المعلوماتية في القرن الحالي متمثلة في الزلزال الرهيب والإعصار الجامح في العلاقات الدولية، وكذا العلاقات الشخصية بين قادة ورؤساء دول العالم جراء ما أقدم عليه الموقع الإلكتروني (ويكيليكس) من نشر ما يقرب من ربع مليون وثيقة رسمية خاصة بالدبلوماسيين الأمريكيين، متبادلة بين البعثات الدبلوماسية الأمريكية بالخارج، ووزارة الخارجية الأمريكية بالولايات المتحدة الأمريكية، وقد تم نشر ما يقرب من ألف وثيقة حتى ديسمبر 2010، مما أحدث تسونامي معلوماتي غير مسبوق في العلاقات الدولية والعلاقات الشخصية للعديد من أجهزة المخابرات العالمية ورؤساء وقادة دول العالم، مما سبب الكثير من الحرج في تلك العلاقات والأنشطة، قد تمتد آثارها السلبية لسنوات عديدة قادمة [2].

6-جرائم التجسس الإلكتروني

إن التجسس الإلكتروني هو أشبه "بالشيطان"، وهذا الشيطان الإلكتروني يخترق الأجهزة ويقوم بعمليات التجسس على المستخدم بطرق غير شرعية ولأغراض غير سوية كي يسرق معلومات تتعلق به سواء على الصعيد الشخصي أو السياسي، أو العملي أو الاجتماعي، أو لسرقة حسابه، أو بهدف التخريب، أو بهدف معرفة معلومات تتعلق بالجانب المادي، وغيرها من الجوانب الأخرى، حيث لم يعد هناك سرية يمكن الاحتفاظ بها من دون أن يقوم الشخص بعمليات كثيرة لتجنب عمليات التجسس أو "الهاكرز" [3]، وكشفت الوثائق أن وكالة الأمن القومي الأمريكية تجسست على حوالي 125 مليار اتصال هاتفي، ورسائل نصية في فترة شهر جانفي من العام 2013، وكانت غالبيتها من دول شرق أوسطية[4].

كما أن التجسس الصناعي جريمة تقليدية وتم تجريمه طبقا للقوانين الجنائية القائمة، ومع ذلك تفتح أجهزة الكمبيوتر أبعادا جديدة لهذه الجريمة، فعلى سبيل المثال قد يتم تنزيل الأسرار الصناعية من كمبيوتر في إحدى الشركات وإرسالها بالبريد الإلكتروني مباشرة إلى منافستها، بل وقد تكون تكنولوجيا

---

[1] – مهران زهير المصري: **الخداع باستعمال الانترنت**، مجلة المعلوماتية، ع 72، السنة 07، فيفري 2012 ، ص 13. www.infomag.news.sy، تاريخ التصفح (2015/03/04).

[2] – محمود الرشيدي: **العنف في جرائم الانترنت–أهم القضايا: الحماية والتأمين–**، الدار المصرية اللبنانية، القاهرة، ط1، 2011، ص 88.

[3] – عبير شفيق الرحباني: **الاستعمار الإلكتروني والإعلام**، مرجع سابق، ص 126.

[4] – المرجع نفسه، ص 129.

المعلومات نفسها هدفا مهما لهذه الجريمة، فقد تتم سرقة اختراع جديد في تكنولوجيا الكمبيوتر وبيعه بمبلغ كبير من المال، يعادل ملايين الدولارات[1].

7-الإرهاب الإلكتروني

يعرف الإرهاب الإلكتروني بأنه العدوان أو التخويف أو التهديد ماديا أو معنويا باستخدام الوسائل الإلكترونية الصادر من الدول أو الجماعات أو الأفراد على الإنسان في دينه أو عرضه أو عقله أو ماله، بغير حق بشتى صنوف وصور الإفساد في الأرض[2].

وإن مرونة التكنولوجيا الحديثة والحاسب والانترنت هي التي ساعدت الأصابع الخبيثة لكي تنشر العنف والخوف، ولكي تخطط وتنفذ الهجمات الإرهابية، فتكنولوجيا المعلومات أفادت الجماعات الإرهابية من ناحيتين:

الأولى: يمكن لهم أن يستخدموا أجهزة الحاسوب والانترنت بوصفها أداة مفيدة لتعزيز النشاط الإرهابي التقليدي مثل استخدام الانترنت في التجنيد والتدريب وتبادل المعلومات بين المنظمات الإرهابية المختلفة.

الثانية: البنية التحتية للمعلومات يمكن أن تشكل هدفا جذابا للأعمال الإرهابية التي يمكن من خلالها التأثير على الرأي العام العالمي[3].

يقوم الإرهابيون بإنشاء وتصميم مواقع لهم على شبكة المعلومات العالمية الإنترنت لنشر أفكارهم والدعوة إلى مبادئهم، بل تعليم الطرق والوسائل التي تساعد على القيام بالعمليات الإرهابية، فقد أنشئت مواقع لتعليم صناعة المتفجرات، وكيفية اختراق وتدمير المواقع، وطرق اختراق البريد الإلكتروني، وكيفية الدخول إلى المواقع المحجوبة، وطريقة نشر الفيروسات وغير ذلك[4].

وخطورة الإرهاب الإليكتروني تزداد في الدول المتقدمة التي تضار بنيتها التحتية بالحواسب الآلية والشبكات المعلوماتية، مما يجعلها هدفا سهل المنال، فبدلا من استخدام المتفجرات، تستطيع الجماعات الإرهابية، من خلال الضغط على لوحة المفاتيح، تدمير البنية المعلوماتية وإغلاق المواقع

---

(1) -إيهاب ماهر السنباطي: **الجرائم الإلكترونية(الجرائم السيبيرية) قضية جديدة أم فئة مختلفة؟ التناغم القانوني هو السبيل الوحيد!** ، أعمل الندوة الإقليمية حول "الجرائم المتصلة بالكمبيوتر"، المملكة المغربية، 19-20 جوان 2007، ص 21.

(2) - محسن العبودي: **المواجهة الأمنية لجرائم الإنترنت**، www.eastlaws.com ، ص 12.

(3) - عبير الرحباني: **الإعلام الرقمي(الإلكتروني)**، دار أسامة، للنشر والتوزيع، الأردن، عمان، ط1 ،2012، ص 190.

(4) - أيسر محمد عطية: **دور الآليات الحديثة للحد من الجرائم المستحدثة (الإرهاب الإلكتروني وطرق موجهته)**، ورقة علمية مقدمة في الملتقى العلمي: الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية خلال الفترة 2-4 سبتمبر 2014، عمان، الأردن، ص 16.

الحيوية وشل أنظمة القيادة والاتصالات، أو قطع شبكات الاتصال بين الوحدات والقيادات المركزية، أو تعطيل أنظمة الدفاع الجوي، أو إخراج الصواريخ عن مسارها، أو التحكم في خطوط الملاحة الجوية والبرية والبحرية، أو شل محطات إمداد الطاقة والماء، أو اختراق النظام المصرفي، مما يضر بأعمال البنوك والأسواق المالية العالمية[1].

فمن خلال توظيف تكنولوجيا الاتصال الحديثة، وتقنية المعلومات يمكن إحراج دول متقدمة وتدمير بنيتها المعلوماتية، ومهاجمتها إلكترونيا وإصابتها في أهداف قاتلة، وتكليفها خسائر فادحة دون أن تتمكن السلطات المخولة من معرفة الجناة، وهذا ما ينبئ بأن الإرهاب الإلكتروني هو إرهاب المستقبل، والذي يفرض تحديات صعبة خاصة على الدول المتطورة، نظرا لتعدد أشكاله، واختلاف أساليبه واتساع مجال نشاطه.

المجموعة الثانية: جرائم تقع بواسطة الانترنت

أي أن الشبكة تكون أداة إيجابية لارتكاب الجريمة فتسهل للمجرم المعلوماتي تحقيق غايته، ويلاحظ أن أغلب صورها في هذه الحالة تشكل جرائم الواقعة على الأشخاص.

1-الجرائم الجنسية والممارسات غير الأخلاقية

أما الخطورة الأخلاقية؛ فإن جلّ جرائم الإنترنت تستهدف فضح الأسرار الشخصيّة أو القذف أو التشهير بشركات أو أشخاص بقصد الإضرار بالسمعة الشخصية أو المالية، إمّا بسبب المنافسة، أو بداعي الانتقام، ونحو ذلك، وأيضًا على شبكة الإنترنت تنشط تجارة الدعارة والصور الخليعة التي تُعدّ أكبر صناعة نشطة على شبكة الإنترنت بحجم عائدات كبير يقُدر بنسبة 58% من مجمل عائدات الخدمات المدفوعة على الشبكة لعام 2003، وعبر آلاف المواقع تُنشَر صور فاحشة، وتقُدم خدمات جنسيّة مدفوعة، وتُستغل صور الأطفال والمشاهير في أوضاع شائنة، دون أن تنال كثيرا من هذه الأنشطة يد القوانين المحليّة أو الدولية [2].

وحاول العالم مع انتشار الانترنت وظهور مخاطر عديدة من بينها المخاطر الأخلاقية، وضع قوانين منظمة لعمله فقامت الولايات المتحدة بسن أول قانون باسم "**القانون الفيدرالي للياقة الاتصالات**"، الذي تم إقراره في فبراير 1997، وفي 15 ديسمبر 2000، أقر الكونغرس قانون حماية الأطفال من

---

[1] – جميل عبد الباقي الصغير: **مدى كفاية نصوص قانون العقوبات والإجراءات الجنائي لمواجهة الإرهاب عبر الانترنت**، الحلقة العلمية الانترنت والإرهاب من 15 إلى 19 نوفمبر 2008، القاهرة، جامعة نايف العربية بالتعاون مع جامعة عين شمس، ص 06.

[2] – أمين سعيد عبد الغني: **وسائل الإعلام الجديدة والموجة الرقمية الثانية**، إيتراك للطباعة والنشر والتوزيع ، القاهرة، ط1، 2008، ص 110.

الانترنت، وبعد هجمات سبتمبر أصدرت الولايات المتحدة قانون تقديم الوسائل المناسبة المطلوبة لاعتراض وإعاقة الإرهاب، والذي تم إقراره في 27 أكتوبر 2001 [1].

وهناك تسليم من الجميع أنه لا يمكن السيطرة على الانترنت بقوانين من قبل الدول، "ويبقى أمامها حل مهم يتمثل في تعزيز خط دفاعها الأمتن: جهاز المناعة الذاتية المعتمد على تقوية مؤسسات التنشئة الاجتماعية بغية التمكن من إنشاء أجيال أكثر نضجا وقدرة على التصدي لسلبيات الانترنت، بالإضافة طبعا إلى مواجهتها تكنولوجيا، ورفع تحدي المنحرفين عبر الانترنت، مع تنشيط التعاون الدولي الحكومي وغير الحكومي"[2].

2-الجرائم المالية

أ-جرائم السطو على أرقام البطاقات الائتمانية

ومن الجرائم التي ترتكب باستخدام تكنولوجيا المعلومات سرقة الأقراص الصلبة والمرنة، بغرض الحصول على المعلومات التي تحويها، ويتولى قراصنة المعلومات بيعها بعد الحصول عليها، نظير الحصول على عائد مادي، مثال ذلك: الوصول إلى أجهزة الحاسب الخاصة بمكاتب الائتمان الرئيسية وسرقة المعلومات الائتمانية، ثم استخدامها بإعادة بيعها لأشخاص آخرين، وتدمر المشروعات المهمة للشركات بغرض ابتزازهم[3].

وتعد عمليات السطو على بطاقات الائتمان أحدث أنماط السلوك الإجرامي التي ارتبطت بشبكة الانترنت من بنوك أو مؤسسات مالية وأفراد، وقد زاد خطر انتشار هذا النوع من الجرائم لصعوبة التوصل إلى مرتكبيها، ففي كثير من الأحيان يكتشف حامل بطاقة الفيزا في دولة ما أن بطاقته قد استخدمت في شراء سلعة من أحد المحلات في دولة ثانية، ويكون الفاعل في دولة ثالثة، وقد تمت الواقعة من خلال موقع المحل البائع على شبكة الانترنت[4].

ب-القمار عبر الانترنت

في الماضي كان لعب القمار يستلزم وجود اللاعبين معا على طاولة اللعب ليتمكنوا من اللعب، إلا أنه مع الانتشار الواسع والتطور الكبير لشبكة الانترنت على مستوى العالم، ظهر إلى الوجود آخر

---

(1) - أحمد بن عبد الرحمن البعادي: **دعاوى الجرائم الإلكترونية وأدلة إثباتها في التشريعات العربية بين الواقع والمأمول**، المؤتمر الثالث لرؤساء المحاكم العليا بالدول العربية ، من 23 إلى 25 سبتمبر 2012، الخرطوم، ص 09.

(2) - فضيل دليو: **تكنولوجيا الإعلام والاتصال الجديدة-بعض تطبيقاتها التقنية-**، دار هومة للطباعة والنشر والتوزيع، الجزائر، ط1، 2014، ص 247.

(3) - السعيد مبروك إبراهيم: **المكتبة الجامعية وتحديات مجتمع المعلومات**، دار الوفاء للطباعة والنشر، الإسكندرية، ط1، 2009، ص 88.

(4) - جعفر حسن جاسم الطائي: مرجع سابق، ص192.

صيحات القمار يتمثل في (الكازينوهات الافتراضية) (virtual casino)، التي ما فتئت تظهر هنا وهناك في فضاء الانترنت، وهي عبارة عن مواقع ويب تم تصميمها على طراز كازينوهات"لاس فيغاس" الأمريكية، وتوفر كل أنواع القمار وألعابه ابتداء من ألعاب الورق، وانتهاء بآلات المقامرة، وهي موجودة على الشبكة المعلوماتية[1]، وتشير التقديرات إلى ارتفاع عائدات القمار على الانترنت بالنسبة للولايات المتحدة الأمريكية، من 3.1 مليار دولار أمريكي في عام 2001، إلى 24 مليار دولار أمريكي في عام 2010 [2].

ويوجد على الإنترنت أكثر من ألف موقع للقمار يسمح لمرتاديه من مستخدمي الإنترنت ممارسة جميع أنواع القمار التي توفرها المواقع الحقيقية، ومن المتوقع أن ينفق الأمريكيون ما يزيد عن (600 مليار)دولار سنويا في أندية القمار ويكون نصيب مواقع الإنترنت منها حوالي مليار دولار.

وقد حاول المشرعون الأمريكيون تحريك مشروع قانون يمنع المقامرة عبر الانترنت ويسمح بملاحقة اللذين يستخدمون المقامرة السلكية أو اللذين يروجون لها سواء كانت هذه المواقع في أمريكا أو خارجها[3].

ج–تزوير البيانات

ربما كانت جريمة تزوير بيانات الحاسب هي أكثر جرائم نظم المعلومات انتشارا على الإطلاق، فلا تكاد تخلو جريمة منها من عملية تزوير للبيانات بشكل أو بآخر ويتم تزوير بيانات الحاسب إما بإدخال بيانات مغلوطة إلى قواعد البيانات أو بتعديل البيانات الموجودة عمدا، وللأسف فإن الموظفين المسموح لهم بإدخال البيانات، ثبت أنه كان لهم ضلع كبير في الكثير من جرائم نظم المعلومات، مثل تغيير أرصدة الحسابات، وتزوير المعاملات، والتخريب، وسرقة المخزون، وتزوير المرتبات، باستخدام بعض البرامج المساعدة الجاهزة المصممة خصيصا لتعديل البيانات في أماكنها مباشرة، وهذا النوع من البرامج خطير لأنه لا يترك أثرا يدل على التعديل أو القائم بالتعديل[4].

د–الجرائم المنظمة

"الجريمة المنظمة هي عنف منظم قصد الحصول على مكاسب مالية، بطرق وأساليب غير مشروعة"، وتمارس الجريمة المنظمة على شكل نصب واحتيال وتزوير وسطو وخطف من أجل الابتزاز والقتل...الخ،

---

(1) –محمد علي قطب: **موقف الشريعة الإسلامية من جرائم الأخلاق عبر الانترنت**، مركز الإعلام الأمني، جامعة نايف العربية للعلوم الأمنية، ص04، www.nauss.edu.sa

(2) – **Understanding cybercrime: Phenomena, challenges and legal response**, September 2012, ITU 2012, www.itu.int/ITU-D/cyb/cybersecurity/legislation, p 25.

(3) –عبد الحميد إبراهيم محمد العريان: مرجع سابق، ص 40، 41.

(4) – منال هلال المزاهرة: **تكنولوجيا الاتصال والمعلومات**، مرجع سابق، ص 380.

إلا أنها تختلف عن الجرائم المعروفة كونها تنفذ بعد تدبير وتنظيم، لذا سميت ب"الجريمة المنظمة"، ويشير مصطلح"الجريمة المنظمة "إلى جماعات ترتكب أفعالا تخترق بها القانون للحصول على
مساعدات مادية، كما تهتم بالابتزاز والخداع والإنتاج والتوزيع غير القانوني لإدمان المخدرات، والتعامل مع السلع الممنوعة مثل الأسلحة غير القانونية [1].

من خلال التعريف يتبين أن الجريمة المنظمة تمتاز بخاصيتين أساسيتين أولاهما: التنظيم، وثانيتهما: الكسب المادي.

ولقد أضافت الجريمة المنظمة عبر الحدود الوطنية بعدا سلبيا للعولمة مع غيرها من السلبيات الاقتصادية التي كان لها آثارها السلبية على الدول النامية، فلقد أصبح الفساد أداة من الأدوات المفضلة للجريمة المنظمة بل جزء لا يتجزأ من استراتيجياتها، وذلك باعتبار أن المال الفاسد نوع من الاستثمار الناجح للجماعات الإجرامية المنظمة حيث يزيد من فرص نجاح جرائمهم ويقلل من ملاحقتهم والقبض عليهم ومحاكمتهم[2].

ومن المعروف أن الحالة الراهنة لإنفاذ القانون يجب أن تخضع لتغييرات كبيرة للتعامل مع خطر الجريمة الإلكترونية، فكثير من العلماء والممارسين يحاولون إقامة نجاحات جديدة في التعامل مع الجريمة، تشير إلى أن أكبر تحد للقانون الدولي هو تنفيذ الجريمة الإلكترونية العابرة للوطنية "فكر عالميا واعمل محليا"[3].

هـ–تجارة المخدرات عبر الانترنت

تمثل الانترنت أحدث ما أنتجته ثورة المعلومات وثورة الاتصالات، وتم استخدامها في مختلف المجالات ومنها المجال الأمني، وكذلك سعت جماعات الإجرام المنظم عبر العالم لاستغلال الانترنت في مختلف أنشطتها، حيث تم الإعلان عن المخدرات والعقاقير غير المشروعة، والاتجار بها عبر الانترنت[4].

و–غسيل الأموال

إن أول ما استعمل هذا المصطلح كان في الولايات المتحدة الأمريكية سنة 1931، نسبة إلى شركة الغسل التي تمتلكها المافيا، وذلك خلال محاكمة أحد زعماء تلك المافيا، وقد شملت تلك المحاكمة مصادرة جميع الأموال التي ثبت بأنها متأتية من التجارة غير المشروعة في المخدرات[1].

---

(1) – نصيرة تامي: **الإعلام الفضائي والإرهاب**، دار أسامة للنشر والتوزيع، الأردن، عمان، ط1، 2015، ص 87.

(2) – السيد عوض: **التطور التكنولوجي والجريمة**، ، أعمال المؤتمر السنوي الرابع والثلاثون: قضايا السكان والتنمية من 19- 22 ديسمبر 2004م، المركز الديمغرافي بالقاهرة، ص 10.

(3)-CHRIS E. MARSHALL et des autre: Handbook of: Transnational Crime & Justice-Computer Crime in a Brave New World, Sage publication,2005, p11.

(4) – عادل عبد الجواد محمد: **الإنترنت والإجرام المنظم**، مجلة الأمن والحياة، ع 303، السنة 26، سبتمبر 2007، ص ص (30، 32).

ويعد غسيل الأموال إحدى صور الجرائم الاقتصادية وهو ظاهرة ترتبط بالجريمة العالمية المنظمة وعلى الأخص جرائم المتاجرة بالمخدرات، الإرهاب الدولي، تهريب الأسلحة، الغش والتزييف، الفساد السياسي والفساد الإداري والمالي، وتعد جريمة غسيل الأموال اليوم من المشاكل العالمية التي تحظى باهتمام معظم الدول المتقدمة والنامية على حد سواء وإن كان بدرجات متباينة في الأهمية.

ويقدر خبراء صندوق النقد الدولي حجم الأموال التي يتم غسيلها سنوياً ما بين 620 مليار دولار إلى 1600 مليار دولار، ولأن الجهاز المصرفي هو الوسيلة الأكثر فعالية لإضفاء صفة المشروعية على الأموال القذرة، فانه من الطبيعي أن توجه أنشطة غاسلي الأموال إلى المصارف على أمل إجراء سلسلة من العمليات المصرفية عليها، لتحقيق هذا الهدف مثل عمليات الصرف والتحويل النقدي بواسطة أنماط عديدة من العمليات المصرفية المتطورة في هذا المجال، خاصة في ظل التطور الالكتروني في أنظمة المعلومات[2].

3-قيادة الجماعات الإرهابية عن بعد

إن من أهم دوافع الجرائم المعلوماتية التي برزت بشكل كبير في العصر الحديث هي الدوافع الإرهابية، نظرا لسهولة استخدام التقنيات الحديثة، وخدمتها للمنظمات الإرهابية عن طريق تسهيل الاتصال والتواصل بين قياداتها وأعضائها، ونقل الأفكار والمعتقدات والآراء، وتلقي الأوامر وتمرير المعلومات والتعليمات، والوسائل الأخرى التي تساعد على ارتكاب الجرائم الإرهابية [3].

كما استغلت مواقع التواصل الاجتماعي لتمرير بعض الرسائل والخطابات، تويتر مثلا كانت أداة فعالة في يد الإرهابيين استخدموه كوسيلة للحصول على معلومات حول ما تم إعداده لهم من طرف القوات الأمنية، ووسائل التواصل الاجتماعي الجديدة يمكن أن تستغل من طرف الإرهابيين في التخطيط لهجماتهم الإرهابية[4].

4-السطو على أموال البنوك

---

(1) – أحمد بورزام: **جرائم المعلوماتية**، وكيل جمهورية لدى محكمة باتنة، المجلس القضائي بباتنة، يوم 2006/06/20، ص 24.

(2) –طه أحمد عبد السلام: **مفهوم غسيل الأموال ودور الجهاز المصرفي في مكافحته**، صحيفة المدى العراقية، الأحد 2015/03/22، ع 3317، www.almadapaper.net

(3) –عبد الله بن حسين آل حجراف القحطاني: **تطوير مهارات التحقيق الجنائي في مواجهة الجرائم المعلوماتية–دراسة تطبيقية عل المحققين في هيئة التحقيق والادعاء العام بمدينة الرياض**، مذكرة ماجستير منشورة، قسم العلوم الشرطية، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، ص 37.

(4) –Paul Levinson: New New Media, international edition, 2nd edition, New York, 2013, p 167.

إن الأشخاص الذين يقومون بالتحايل واستخدام الحاسب الإلكتروني للسرقة تنقصهم الأمانة، حيث يعمدون إلى استخدام الحاسبات العائدة لأصحاب العمل لارتكاب جرائمهم، فقد يقومون مثلا بتغيير أرقام سجلات الحسابات بحيث تصبح أقل من المجموع الفعلي للحسابات الموجودة، ثم يتم الاستيلاء على المبلغ الذي يتم طرحه من هذه الحسابات، أو استخدام بطاقات مزورة يتم عند استخدامها نقل الأموال من حسابات الزبائن الآخرين إلى حساب سارق الأموال، عمليات الاحتيال هذه لا تكون مقصورة على المصارف أو مؤسسات الأعمال، وإنما يمكن أن تحصل في أية جهة تعتمد في عملها على الحاسب[1].

خامسا: واقع الجريمة الإلكترونية في الجزائر

1-نظرة عامة عن الجرائم الالكترونية بالجزائر

أضحت الجزائر من بين اهتمامات قوائم وتقارير المنظمات والهيئات الدولية حول الجرائم الإلكترونية وحماية الانترنت، بحكم أن التقارير الأخيرة كشفت أن الجزائر في المراتب الأولى إفريقيا وعربيا بنسبة 85 بالمائة في مجال القرصنة [2].

وتمكنت مصالح المديرية العامة للأمن الوطني، من معالجة أكثر من 380 قضية تتعلق بالجريمة الإلكترونية خلال السداسي الأول من سنة 2013 حسبما علم من السلك الأمني، وقد تم خلال السداسي الأول من سنة 2013 معالجة ما مجموعه 383 قضية تتعلق بالجريمة الإلكترونية في حين تمت معالجة 515 قضية خلال سنة 2012، ويتعلق الأمر بـ126 قضية خاصة بالاستغلال غير القانوني للأداة المعلوماتية و154 تتعلق بالهاتف النقال و103 تخص الصور الفوتوغرافية والفيديو.

وفي هذا الصدد عالجت الخلية المركزية لمكافحة الجريمة الإلكترونية خلال السداسي الأول 15 قضية تتعلق بانتهاك خصوصية الحياة الشخصية، وأربعة خاصة بالتشهير، وإحدى عشرة قضية بسبب الابتزاز، وواحدة خاصة بانتحال الشخصية، وأربعة وعشرون تتعلق بالقرصنة، ويشير القسم المختص في استغلال

---

[1] – دلال صادق وحميد ناصر الفتال: **أمن المعلومات**، مرجع سابق، ص 138.

[2] – **الجزائر معنية بالمشروع الدولي لمكافحة الجرائم الإلكترونية**، قسم التكنولوجيا، الشروق أون لاين ليوم 2012/02/23، www.echoroukonline.com/ara/articles

الأدلة المعلوماتية أن غالبية المخالفات تتعلق بالتكنولوجيات الجديدة سيما بواسطة الحواسيب والانترنت والهواتف النقالة [1].

وتمكنت الفرق المتخصصة في مكافحة الجرائم المعلوماتية للأمن الوطني سنة 2014 وبناء على شكاوي، من معالجة 211 قضية تتعلق بجرائم الانترنت، قُدّم من خلالها الدليل المادي عن تورط 205 مشتبها فيه، منهم 28 امرأة، ومن بين هاته القضايا ما يلي:

- 75 قضية تمس بأنظمة المعالجة الآلية للمعطيات
- 59 قضية لها علاقة بالقذف وبالمساس بحرمة الحياة الخاصة
- 28 قضية متعلقة بالتهديد بالتشهير
- 26 قضية انتحال هوية الغير
- 09 قضايا لها علاقة بنشر الصور المخلة بالحياء
- 03 قضايا متعلقة بالنصب والاحتيال عن طريق الانترنت
- 06 قضايا متعلقة بالإهانة والسب عن طريق الانترنيت
- قضيتان متعلقتان بالاستعمال غير الشرعي للبطاقات الالكترونية [2].

وتبقى الحالات المسكوت عنها أكبر من ذلك إذا عرفنا أن 75 بالمائة من هذه الجرائم متعلقة بالشرف.. الأمر الذي يحول دون الإبلاغ، تفاديا للإعلان والتشهير لما فيه من إساءة للعائلات.

2-آفاق مستقبلية لمكافحة الجريمة الالكترونية في الجزائر

أكد فاروق قسنطيني، رئيس اللجنة الوطنية لترقية وحماية حقوق الإنسان، صعوبة تطبيق القوانين المعاقبة على الجريمة الإلكترونية في الجزائر، لقلّة خبرتها في هذا الشق، وغياب المختصين والخبراء القادرين على تشخيص الجريمة قبل عرضها على المحكمة للفصل فيها، وقال قسنطيني في تصريح لـ"السلام": "إن استصدار الجزائر قوانين لمعاقبة مرتكبي الجرائم الإلكترونية غير كاف، مع عدم تهيئة الأسس التقنية الكفيلة بتصنيف درجات هذه الجرائم وحدّة أضرارها قبل إصدار العقوبة، هذا فضلا عن غياب التواصل

---

[1] - **الجريمة الالكترونية**: المديرية العامة للأمن الوطني تعالج أكثر من 380 قضية خلال السداسي الأول 2013، قسم أخبار الجزائر، النهار الإلكترونية ليوم 2013/10/02، www.ennaharonline.com/ar/algeria

[2] - الموقع الرسمي للشرطة الجزائرية: www.dgsn.dz

الدائم بين القضاء والمختصين في الاتصالات، ما أفرز شبه تذبذب وغموض في شأن العقوبات الدقيقة في مثل هذه الجرائم".

وفي السياق ذاته أوضح أن القانون الجزائري، يعاقب في الغالب مرتكبي هذه الجرائم بالسجن القصير المدى أو بالغرامة المالية، "بحكم أن جل الجرائم الإلكترونية المرتكبة في الجزائر تصب أو تصنّف قانونيا كسرقة"، مبرزا أن المعدل العام لهذه الجرائم في الجزائر متوسط مقارنة بباقي دول العالم، محذّرا من تنامي هذه الجرائم في السنوات الأخيرة على المستوى الوطني، مع بداية مرحلة إدمان الجزائري على الإنترنت، وما يصاحبها من خدمات إلكترونية، ودعا الحكومة إلى ضرورة استحداث إستراتيجيات عقابية وتقنية لحماية ضحايا هذه الجرائم، خاصة فئة الأطفال ورجال المال كونهم الأكثر عرضة لها [1].

وكانت الجزائر ضمن مجموعة الدول المدرجة في مشروع إعداد بحث لتحديد آلية تطور الهجمات الإلكترونية خلال السنوات الثمانية المقبلة من طرف منظمة "**التحالف الدولي لحماية أمن الانترنت**"، والذي يتضمن تقديم إرشادات لحكومات الدول والسلطات المحلية حول أفضل السبل المتاحة لمواجهة هذه الهجمات [2].

خاتمة

مما سبق يمكن أن نصل إلى نتيجة مفادها أن الجريمة الإلكترونية هي آفة العصر، والأخطبوط الذي أنتجته الحضارة التقنية والثورة التكنولوجية، الذي تمتد أذرعه في جميع أنحاء العالم، ولم تفلت من قبضته لا الدول الضعيفة ولا المتطورة، واستشرى خطره المدمر على مختلف القطاعات الحياتية الاقتصادية منها والاجتماعية والسياسية، وحتى الشخصية، وأن جميع الأفراد في العالم مستهدفون بجميع فئاتهم وأعمارهم ومرجعياتهم الفكرية والدينية والثقافية، فنحن نعيش زمن "الاستعمار الإلكتروني" بكل أشكاله ومظاهره، الذي يستهدف التأثير بشكل مباشر وغير مباشر على سلوكيات الناس وأفكارهم وثقافاتهم وحياتهم.

فجرائم الكمبيوتر ليست مجرد جرائم تقليدية بثوب جديد أو أنها طبعة جديدة لجرائم قديمة، باستخدام وسائل جديدة، فهذا قد ينطبق على الجريمة الإلكترونية في بعض صورها والتي يكون الكمبيوتر فيها وسيلة لارتكاب الجريمة، وهي ليست "مجرد نبيذ قديم في زجاجة جديدة" كما وصفها جملة من

---

[1] – 160 مليار دولار سنويا مكاسب عصابات الجريمة المنظمة عبر الإنترنت: **قسنطيني: تطبيق العقوبات في قضايا الجريمة الإلكترونية صعب في الجزائر**، صحيفة السلام الإلكترونية ليوم 2014/01/24، http://essalamonline.com/ara/permalink

[2] – **الجزائر معنية بالمشروع الدولي لمكافحة الجرائم الإلكترونية**، قسم التكنولوجيا، الشروق أون لاين، مرجع سابق.

الإعلاميين الغربيين في المراحل الأولى لظهورها، ولكنها بحق جرائم جديدة في طبيعتها، ومضمونها، ونطاقها وتأثيراتها وأدواتها، وحتى في خصوصية وتميز وطبيعة مرتكبيها.

والمشكلة الكبيرة تكمن في قصور أدوات الرقابة، وتشريع القوانين، وفرض العقوبات، والدول الغربية تسعى وباستمرار إلى اكتشاف أدوات رقابة جديدة أكثر فاعلية، وفرض قوانين وعقوبات أكثر صرامة، لكن ماذا عن الدول العالمثالثية؟ وماذا عن الدول العربية على وجه الخصوص المستخدمة لشبكة الانترنت؟ هل تسعى للحد من الجريمة الإلكترونية؟ وهل استنفرت منظوماتها التشريعية والتنفيذية لإصدار قوانين جديدة وعقوبات حازمة تتأقلم والوضع العالمي الجديد؟.