معهد الكويت للدراسات القضائية والقانونية
Kuwait Institute for Judicial & Legal Studies

كويت جديدة
NEWKUWAIT

وزارة العدل

الجرائم الإلكترونية

2019-2018

الجرائم الإلكترونية

إعداد

اللجنة العلمية

معهد الكويت للدراسات القضائية والقانونية

2019-2018

مقدمــة

اتسعت في العصر الحديث دائرة استخدام الشبكات الدولية للمعلومات كوسيلة للاتصال في شتى مجالات الحياة لتحقيق ما تصبو إليه الانسانية من اختصار للوقت والمسافات والجهد البدني والذهني، وأصبحت هذه الشبكات تحوي معلومات لا حصر لها تتعلق بكافة ميادين الحياة الشخصية والاقتصادية والعلمية وغيرها.

إلا أنه على الجانب المقابل فقد أدى الاستخدام المتزايد لهذه الشبكات والأنظمة المعلوماتية والحاسب الآلي[1] إلى كثير من المخاطر، إذ أفرز أنواعا جديدة من الجرائم يطلق عليها الجرائم المعلوماتية[2] كجرائم الاختلاس والتزوير التي تتم بالوسائل الإلكترونية، والجرائم الماسة بالأخلاق والآداب العامة، والإرهاب وتجارة المخدرات، والاتجار بالسلاح، والدعارة المنظمة باستخدام الإنترنت والاعتداء على حرمة الحياة الخاصة، وعلى البيانات الشخصية، والتجسس وسرقة المعلومات، واختراق النظم السرية، وارتكبت العديد من الجرائم التقليدية كالسرقة والنصب وخيانة الأمانة، وظهرت جرائم ملازمة لهذه المستحدثات، مثل الغش الإلكتروني، والنسخ غير المشروع للبرامج، والعديد من الجرائم المتعلقة بالتجارة الإلكترونية، وإتلاف الأجهزة الإلكترونية، وإتلاف السجلات المدونة على الحاسب الآلي، وبث الصور أو الأفلام الجنسية من خلال الأجهزة، والقذف أو السب عن طريق الإيميل، وغسل الأموال باستخدام النقود الإلكترونية.

وإذ كانت النصوص الجزائية التقليدية لا تسعف لمواجهة هذه الجرائم المستحدثة التي تعتمد في ارتكابها على وسائل التقنية المتطورة، وحماية لحريات الأشخاص وشرفهم وسمعتهم، ودَرْءًا للعدوان على الأموال والممتلكات العامة والخاصة، وسعياً من المشرع، وفي سياق دعم التوجهات الدولية الخاصة بمكافحة هذه الجرائم، والتزاما بأحكام الإتفاقية العربية لمكافحة جرائم تقنية المعلومات التي صادقت عليها دولة الكويت بموجب القانون رقم 60 لسنة 2013 .

لذا فقد أصدر المشرع القانون رقم 63 لسنة 2015 بشان مكافحة جرائم تقنية

1 عرف الحاسب الآلي بأنه « مجموعة من الأجهزة التي تعمل متكاملة مع بعضها البعض بهدف تشغيل مجموعة البيانات الداخلة طبقا لبرنامج تم وضعه مسبقا للحصول على نتائج معينة . د هدى حامد قشقوش، جرائم الحاسب الإلكتروني في التشريع المقارن، دار النهضة العربية، القاهرة، 1992، ص6

2 د احمد خليفة الملط – الجرائم المعلوماتية – دار الفكر الجامعي – ط الثانية 2006- ص67

المعلومات .

ودراسة الجرائم الالكترونية تتطلب معرفة مفهومها لبيان التعريفات المختلفة لها، والخصائص التي تتميز بها عن غيرها من الجرائم فضلا عن بيان اركانها ثم توضيح الاحكام الاجرائية الخاصة بها.

تقسيم :

المبحث الأول: ماهية الجرائم الإلكترونية .

المبحث الثاني: صور الجرائم الإلكترونية .

المبحث الثالث: الاحكام الاجرائية للجرائم الإلكترونية .

المبحث الأول

ماهية الجرائم الالكترونية

تمهيد وتقسيم:

الجريمة ظاهرة اجتماعية ظهرت بظهور الإنسان وارتبطت ارتباطاً وثيقاً به، فأصبحت بذلك الوجه السلبي الذي يتنقل عبر العصور التي يتطور فيها الإنسان، فكان من البديهي أن تظهر أنماط جديدة من الجرائم لم تكن معهودة من قبل، ومجرم الأمس ليس بمجرم اليوم، حقيقة أن الإجرام في تقدم مستمر ومتواصل، خاصة في عصرنا الحالي عصر تفجرت فيه ثورة المعلومات والتكنولوجيا المتقدمة نتيجة تطور وسائل الاتصال والحوسبة التي جعلت العالم قرية إلكترونية مفتوحة للعموم، ألغت معها الحدود الجغرافية والسياسية للدول. ولكنها سلاح ذو حدين فيمكن أن تُسَخر للخير والمنفعة، كما يمكن أن تُسَخر للشر والمضرة نتيجة لسوء استخدامها من قبل بعض المجرمين لارتكاب جرائمهم. تبعاً لذلك اعتبرت الجرائم الإلكترونية أثراً من الآثار السلبية التي خلفتها التقنية العالية، كونها تطال في اعتداءاتها قيماً جوهرية تخص الأفراد والمؤسسات والدول في كافة نواحي الحياة الاقتصادية، الثقافية والأمنية، كما أن هذه الجرائم تركت في النفوس شعوراً بعدم الأمان وغياب الثقة، الأمر الذي يؤدي إلى تهديد هذه التقنية لحياة الأفراد وأمنهم.

انطلاقاً مما سبق عرضه، يتضح أن الجريمة الإلكترونية أصبحت تحدياً كبيراً للفقه والتشريع والقضاء، الأمر الذى بات معه ضرورياً مواكبة هذا التطور الملحوظ في تلك الجرائم ومواجهتها تشريعياً بقواعد قانونية غير تقليدية لهذا النوع من الجرائم المستحدثة.

وعلى ذلك نتناول مفهوم الجريمة الإلكترونية، وأركانها. على النحو التالي:

المطلب الأول: مفهوم الجريمة الإلكترونية .

المطلب الثاني: أركان الجريمة الالكترونية .

المطلب الأول

مفهوم الجريمة الإلكترونية

تمهيد:

يرجع وجود الجريمة – بوجه عام – ونشأتها وتطورها إلى الدراسة المعروفة بعلم الإجرام «ذلك العلم الذي يدرس الأسباب الدافعة إلى الإجرام الظاهر والأشكال المختلفة للجريمة والأنماط المتباينة للمجرمين، بما يستتبعه ذلك من تلمس سبل الوقاية من الإجرام»[1].

وبيان مفهوم الجريمة الالكترونية يتطلب التعريف بها وبيان خصائصها المميزة لها.

الفرع الاول

تعريف الجريمة الإلكترونية

تمثل الجريمة – آيا كانت – اعتداء على مصلحة يرى المشرع أنها جديرة بالحماية ويجرم الاعتداء عليها. فليس التجريم غاية في ذاته، وإنما هو مقرر حماية لأغراض وغايات أخرى، هذه الأغراض وتلك الغايات تحقق مصلحة للمجتمع في إبقائه بعيداً عن الجريمة، أو السعي إلى احتواء الجريمة.

وتعتبر 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].

هذا وقد تعددت تعريفات الجريمة الإلكترونية وتباينت فيما بينها ضيقاً واتساعاً، ولعل

---

1 د. أحمد عوض بلال، علم الإجرام، النظرية العامة والتطبيقات، دار النهضة العربية، القاهرة، الطبعة الأولى، 1985، ص8، وفي شق الوقاية من الجريمة: انظر ذات المرجع، ص 149.

2 د. هلالي عبداللاه أحمد، التزام الشاهد بالإعلام في الجرائم المعلوماتية، دراسة مقارنة، دار النهضة العربية، القاهرة، 1997، ص13.

سبب ذلك هو عدم وجود تعريف مُجمع عليه لهذه الجريمة[3]

فهى «كل سلوك غير مشروع، أو غير أخلاقي، أو غير مصرح به، يتعلق بالمعالجة الآلية للبيانات أو نقلها»[4]

وهى الجريمة التي تلعب فيها البيانات الحاسوبية، والبرامج المعلوماتية دورا رئيسيا[5] وبناء على ما سبق، وأياً ما كان الخلاف حول تعريف الجريمة الإلكترونية، فإن المحاولات التي بذلت من أجل تعريف الجريمة الإلكترونية متعددة، وإن كانت لا تخرج عن أحد اتجاهين:

الاتجاه الأول: اتجاه يضيق من مفهوم الجريمة الإلكترونية، ووفقاً لهذا الاتجاه فالجريمة الإلكترونية هي « نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب الآلي أو تلك التي يتم تحويلها عن طريقه»[6].

الاتجاه الثاني: وعلى عكس الاتجاه السابق يذهب فريق آخر من الفقهاء إلى توسيع مفهوم هذه الجريمة فيعرفها بأنها « كل فعل إجرامي يستخدم الحاسب الآلي في ارتكابه كأداة رئيسية »[7].

كما تمتد جريمة الحاسب لتشمل الاعتداءات المادية على جهاز الحاسب ذاته أو المعدات المتصلة به، وكذلك الاستخدام غير المشروع لبطاقات الائتمان وانتهاك ماكينات الحساب الآلية بما تتضمنه من شبكات تحويل الحسابات المالية بطرق إلكترونية وتزييف المكونات المادية والمعنوية للحاسب بل وسرقة جهاز الحاسب في حد ذاته أو أي مكون من مكوناته[8].

وهناك تعريف في الفقه يجمع بين الاتجاهين السابقين، فيعرف الجريمة الإلكترونية

---

3 بينما استعمل بعض الفقهاء تعبيرات أخرى مثل الجرائم المرتبطة بالحاسب الآلي Computer Related Crimes، جرائم الحاسب الآلي Computer Crimes، وأخيرا يستخدم البعض تعريف جرائم المعلوماتية نظراً لارتباط هذه الجرائم بالمعلومات بصفة أساسية «information crime». انظر: د. هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة، أسيوط، 1992، ص31. ونود أن نشير إلى أننا سوف نستخدم في هذه الورقة العلمية مصطلح الجرائم الإلكترونية وجرائم المعلوماتية كمترادفين.

4 تعريف منظمة التعاون الاقتصادي والتنمية (OCDE) للجريمة المعلوماتية

5 محمد عبيد الكعبي: الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الانترنت، دار النهضة العربية،القاهرة، – ط 2، 2009، ص 33

6 د. هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات **الحديثة، أسيوط، ١٩٩٢، ص ٣١.**

7 راجع:
Le sile D. Ball, computer crime, in «the information technology revolution», Edited and Introduced by .Tom Forester, The Mit press, Cambridge, 1985, pp. 543-544
مشار إليه لدى د. هشام محمد فريد رستم، الجرائم المعلوماتية، أصول التحقيق الجنائي الفني وآلية التدريب التخصصي للمحققين، مجلة الأمن والقانون، تصدر عن أكاديمية شرطة دبى، السنة السابعة، العدد الثاني، يوليو 1999، ص 78.

8 د. هلالي عبد اللاه أحمد، التزام الشاهد بالإعلام في الجرائم المعلوماتية، دراسة مقارنة، المرجع السابق، ص14.

بأنها « كل نشاط إجرامي يؤدي فيه نظام الحاسب الآلي دور على قدر من الأهمية لإتمامه، سواء أكان الحاسب أداة لإتمام النشاط الإجرامي أم كان محلاً له، ففي كلتا الحالتين ينبغي أن يكون دور الحاسب الآلي مؤثر لإتمام النشاط الإجرامي[9].

كما عرفت هذه الجريمة بأنها «سلوك غير مشروع معاقب عليه قانونا صادر عن ارادة أجرامية محله معطيات الحاسوب» [10]

وتُعرف الجريمة الالكترونية ايضا بانها «النشاط الاجرامي الذي تستخدم فيه التقنية الالكترونية الرقمية بصورة مباشرة أو غير مباشرة، كوسيلة لتنفيذ الفعل الاجرامي المستهدف»[11]

أما بالنسبة للتشريع فقد عرف القانون رقم 63 لسنة 2015 في شأن مكافحة جرائم تقنية المعلومات الجريمة المعلوماتية بأنها: «كل فعل يرتكب من خلال استخدام الحاسب الآلي أو الشبكة المعلوماتية أو غير ذلك من وسائل تقنية المعلومات بالمخالفة لأحكام هذا القانون».

الفرع الثاني

خصائص الجريمة الإلكترونية

تتميز الجريمة الإلكترونية بطبيعة خاصة تميزها عن غيرها من الجرائم التقليدية وذلك نتيجة ارتباطها بالحاسب الآلي، وتعد الجرائم الإلكترونية إفرازاً ونتاجاً لتقنية المعلومات، وقد استدعت السياسة الجنائية الحديثة محاولة حصر خصائص الجريمة الإلكترونية والتي تتسم بلوناً وطابعاً قانونياً خاصاً يميزها عن غيرها من الجرائم – سواء التقليدية منها أو المستحدثة – بمجموعة من الخصائص، قد يتطابق بعضها مع خصائص طوائف أخرى من تلك الجرائم، ولعل أبرز خصائص الجرائم الإلكترونية ما يلي:

9 د. نائلة عادل فريد قورة، جرائم الحاسب الآلي الاقتصادية،، دراسة نظرية وتطبيقية، منشورات الحلبي الحقوقية، بيروت، لبنان، 2005، ص 32-33.

10 د محمود محمد المرزوقي – جرائم الحاسب الالى – المجلة العربية للفقه والقضاء – العدد 28 – الامانة العامة لجامعة الدول العربية – ص53

11 د. مصطفي محمد موسى – اساليب اجرامية للتقنية الرقمية – ماهيتها ومكافحتها – القاهرة 2003 دارالنهضة العربية – ص 56

1- خطورة الجرائم الإلكترونية :

وذلك لمساسها بالإنسان في فكره وحياته الخاصة، وتمس المؤسسات في اقتصادها، والبلاد في أمنها القومي والسياسي والاقتصادي. ومن شأن ذلك أن يضفي أبعاداً خطيرة غير مسبوقة على حجم الأضرار والخسائر التي تنجم عن ارتكاب هذه الجرائم على مختلف القطاعات والمعاملات.

وتعتبر البنوك الهدف الرئيسي للجيل الجديد من مجرمي تقنية المعلومات، وذلك لاعتمادها كلياً على أنظمة نقل التمويل إلكترونياً.

2- جرائم ناعمة :

اذا كانت الجريمة بصورتها التقليدية تحتاج في الاغلب الى مجهود عضلي من الجاني كجرائم القتل، السرقة، الاغتصاب، فان الجريمة الالكترونية على العكس لا تحتاج الى ادنى مجهود عضلي، بل تعتمد على الدراية الذهنية والتفكير العلمي المدروس القائم على معرفة بتقنيات الحاسب الالي، والية تشغيله، بالإضافة الى الاحاطة ببعض البرامج التشغيلية[12].

3-جرائم مغرية للمجرمين :

من الاغراءات التي تجذب المجرمين نحو هذه الجرائم انها جرائم سريعة التنفيذ، اذ غالبا ما يتمثل الركن المادي فيها باستعمال جهاز الحاسب الالي، مع امكانية تنفيذ ذلك عن بعد، دون اشتراط الوجود على مسرح الجريمة، فضلا عن ضخامة الفوائد والمكاسب التي يستطيع الجاني تحقيقها[13] .

4- صعوبة اكتشاف الجرائم الإلكترونية :

ويرجع السبب في صعوبة اكتشاف ارتكاب الجريمة الإلكترونية – ذات الطابع التقني – إلى أنه من السهل إخفاء معالم تلك الجريمة وصعوبة تتبع مرتكبيها، كما أن هذه الجرائم

12 د مصطفى سليمان ابكر – جرائم الحاسوب واساليب مواجهتها – مجلة الامن والحياة – العدد 210 السنة 19 – 1420هـ الرياض- ص47

13 د مصطفى سليمان ابكر – جرائم الحاسوب واساليب مواجهتها – مجلة الامن والحياة – العدد 210 السنة 19 – 1420هـ الرياض- ص47

لا تترك أثراً لها بعد ارتكابها، علاوة على صعوبة الاحتفاظ الفني بآثارها إن وجدت، فليست هناك أموال أو مجوهرات مفقودة، وإنما هي أرقام تتغير في السجلات، ولذا فإن معظم الجرائم الإلكترونية تم اكتشافها بالمصادفة وبعد وقت طويل من ارتكابها، كما لا يتم في الغالب الأعم الإبلاغ عن الجرائم الإلكترونية إما لعدم اكتشاف الضحية لها وإما خشيته من التشهير، وفى الواقع، فإن من أهم الأسباب وراء صعوبة اكتشاف هذه الجرائم يرجع إلى أنها لا يشوب ارتكابها أي عمل من أعمال العنف، وإلى الطابع التقني الذي يضفي عليها غالباً الكثير من التعقيد. [14].

5- صعوبة إثبات الجريمة الالكترونية :

يعد الاثبات من اهم التحديات التي تواجه الاجهزة الامنية، ويزداد الاثبات صعوبة في الجريمة الالكترونية، حيث ان اكتشاف الجريمة الالكترونية امر ليس بالسهل، فالجريمة الالكترونية تتم في بيئة غير تقليدية حيث تقع خارج اطار الواقع المادي الملموس، مما يجعل الامور تزداد تعقيدا لدى سلطات الامن واجهزة التحقيق والملاحقة، ففي هذه البيئة تكون البيانات والمعلومات عبارة عن نبضات الكترونية غير مرئية تنساب عبر النظام المعلوماتي[15] .

كما ان وسائل المعاينة وطرقها التقليدية لا تفلح غالبا في اثبات هذه الجريمة نظرا لطبيعتها الخاصة التي تختلف عن الجريمة التقليدية، فالأخيرة لها مسرح تجري عليه الاحداث، حيث تخلف اثارا مادية تقوم عليها الادلة وهذا المسرح يعطي المجال امام سلطات الاستدلال والتحقيق الجنائي في الكشف عن الجريمة وذلك عن طريق المعاينة والتحفظ على الاثار المادية التي خلفتها الجريمة، لكن فكرة مسرح الجريمة في الجريمة الالكترونية يتضاءل دورها في الافصاح عن الحقائق المؤدية للأدلة المطلوبة وذلك لسببين[16] :

الاول : ان الجريمة الالكترونية لا تخلف اثارا مادية .

الثاني :ان العديد من الاشخاص يترددون على مسرح الجريمة خلال الفترة من زمان

---

١٤ () د. جميل عبد الباقي الصغير، القانون الجنائي والتكنولوجيا الحديثة، الكتاب الأول، الجرائم الناشئة عن استخدام الحاسب الآلي، دار النهضة العربية، القاهرة، الطبعة الأولى، ١٩٩٢، ص١٧.

١٥ هشام محمد فريد رستم - الجوانب الاجرامية للجوانب المعلوماتية - ط١٩٩٤ - ص ٢٣

١٦ عبدالفتاح حجازي - الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنت - القاهرة ٢٠٠٢ - دار الكتب القانونية - ص ٥٩

وقوع الجريمة وحتى اكتشافها او التحقيق فيها، وهي فترة طويلة نسبيا، الامر الذي يعطي مجالا للجاني او للآخرين ان يغيروا او يتلفوا ويعبثوا بالآثار المادية ان وجدت، الامر الذي يورث الشك في دلالة الادلة المستقاة من المعاينة في الجريمة الالكترونية .

بالإضافة الى ذلك فان نقص الخبرة الفنية والتقنية لدى الشرطة وجهات الادعاء والقضاء يشكل عائقا اساسيا امام اثبات الجريمة الالكترونية[17] .

6- خصوصية مجرمي المعلومات :

المجرم الذي يقترف الجريمة الالكترونية، والذي يطلق عليه لقب المجرم المعلوماتي يتسم بخصائص معينة تميزه عن المجرم الذي يقترف الجرائم التقليدية، فاذا كانت الجرائم التقليدية لا اثر فيها للمستويين العلمي والمعرفي للمجرم في عملية ارتكابها باعتبارها قاعدة عامة، فان الامر يختلف بالنسبة للجرائم المعلوماتية، فهي جرائم فنية تقنية في الغالب الاعم، ومن يرتكبها عادة يكون من ذوي الاختصاص في مجال تقنية المعلومات او على الاقل شخص لدية حد ادني من المعرفة والقدرة على استعمال جهاز الحاسوب والتعامل مع شبكة الانترنت[18] .

ومن أهم ما يميز المجرم الإلكتروني أنه مجرم يتمتع بذكاء حاد، لا نجد هذا الذكاء في المجرمين التقليديين الذين في الغالب ما يتركوا أثراً ليدل عليهم بخلاف المجرم الإلكتروني فقد ألم بجميع الجوانب الفنية والتقنية لجريمته مما يساعده في التخلص من أدلة إدانته في وقت سريع وبدون جهد يذكر[19]

7- جرائم عابرة للدول:

إن من أهم الخصائص التي تميز الجريمة الإلكترونية هي تخطيها للحدود الجغرافية، ومن ثم اكتسابها طبيعة دولية أو كما يطلق عليها البعض أنها جرائم ذات طبيعة متعدية الحدود.

فبعد ظهور شبكات المعلومات، لم يعد هناك حدود مرئية أو ملموسة تقف أمام نقل المعلومات عبر الدول المختلفة. فالقدرة التي تتمتع بها الحاسبات الآلية في نقل وتبادل كميات

17 عبدالفتاح حجازي – الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنت – القاهرة 2002 – دار الكتب القانونية – ص 60
18 تركي بن عبدالرحمن المويشير – النموذج الامني لمكافحة الجرائم المعلوماتية وقياس فاعليته – ط 2009 – ص 25
19 خالد ممدوح إبراهيم ، الجرائم المعلوماتية، الطبعة الأولى، دار الفكر الجامعي- الإسكندرية، 2009 ص 134

كبيرة من المعلومات بين أنظمة يفصل بينها آلاف الأميال، قد أدت إلى نتيجة مؤداها أن أماكن متعددة في دول مختلفة قد تتأثر بالجريمة الإلكترونية الواحدة في آن واحد.

فالجرائم لم تعد تقتصر على إقليم ولا تتعداه، بل أصبح بالإمكان ارتكاب الجرائم عن طريق الكمبيوتر باختراقه لكمبيوتر آخر في بلد آخر أو إتلاف معطياته، فالتعدي في بلد وأثره في بلد آخر وهكذا[20].

ولقد أدى هذا التباعد إلى تشتت الجهود في مواجهة الجريمة الإلكترونية، فعلى سبيل المثال وجود الجاني في بلاد والمتضرر في بلاد أخرى جعل مواجهة هذا النوع من الإجرام بالأمر العسير، وذلك لاختلاف الإجراءات الجنائية أو النزاع حول القانون الواجب التطبيق، فالتطور السريع فى مجال المعلومات والتكنولوجيا وما يسببه ذلك من آثار هامة فى مجال انتقال هذه الأموال عبر الدول أو المصارف المختلفة كان له أكبر الأثر فى انتشار جريمة غسل الأموال، تلك الجريمة التى تتميز بتشعبها بالإضافة إلى الصعوبات التى تواجه عملية التغلب عليها لمنعها ومراقبتها على نحو فعال[21].

المطلب الثاني

أركان الجريمة الإلكترونية

تمهيد:

وفقاً للقواعد الراسخة في القانون الجزائى فإن القول بوجود جريمة يتطلب كأصل عام ركن مادي وركن معنوي، وبغير هذين الركنين لا يمكن القول بوجود الجريمة، وعلى ذلك نتناول كل ركن في فرع مستقل.

20 د. عبدالله حسين علي محمود، سرقة المعلومات المخزنة في الحاسب الآلي، دار النهضة العربية، القاهرة، 2002، ص351.

21 د. محمود كبيش، السياسة الجنائية فى مواجهة غسيل الأموال، دار النهضة العربية، القاهرة، 2001، ص 12 وما بعدها؛ د. عادل محمد أحمد السيوى، المسئولية الجنائية عن جريمة غسل الأموال فى التشريع المصرى، دراسة مقارنة، رسالة دكتوراه، كلية الحقوق- جامعة القاهرة، 2007، ص 33.

الفرع الاول

الركن المادي

إن الفعل الإيجابي هو حركة عضوية إرادية صادرة عن إنسان[22]، فجوهر الفعل الإيجابي هو تلك الحركة التي تصدر عن طريق أحد أعضاء الجسم ولا يهم العضو المستخدم في إتيان هذه الحركة، ونظراً لما تتسم به الجرائم الإلكترونية من طبيعة خاصة فقد اتجه الفقه الحديث إلى تعريف الركن المادى فى تلك الجرائم بالنشاط التقنى.

النشاط التقني:

إن الركن المادي في الجرائم الإلكترونية ينبني على العلاقة التقنية بين مرتكب جريمة ضد المستندات الإلكترونية مثلاً وبين الآلة وهى الحاسب الآلي كما في جريمة تزوير مستند إلكتروني، ومثل هذه العلاقة يجب أن تؤخذ في الاعتبار عند بناء الركن المادي في مثل هذه الجرائم.

ولعل أهم مثال على ذلك، هو النشاط الإيجابي في جريمة إتلاف المستندات الإلكترونية فالفعل أو النشاط الإيجابي من الجاني المتمثل في بث فيروسات كحصان طروادة[23] أو من خلال برامج ضغط يأتي عن طريق قيامه ببث هذه الفيروسات عن طريق جهاز حاسب آلي من خلال شبكة الإنترنت، وهو ما يمثل أهمية النشاط التقني كفعل إيجابي في الجرائم الإلكترونية[24].

كما أن النشاط أو السلوك المادي في جرائم الانترنت يتطلب وجود بيئة رقمية واتصال

---

22 د. عمر سالم، شرح قانون العقوبات المصري القسم العام، طبعة 2010، دار النهضة العربية، القاهرة، رقم 181، ص 295.

23 فيروس حصان طرواده: Trojan horse وهو عبارة عن برنامج فيروسى لديه القدرة على الاختفاء فى البرنامج الاصلى. وعندما يتم تشغيل البرنامج الاصلى ينشط الفيروس وينتشر ليبدأ نشاطه التدميرى الذى قد يؤدى الى تعديل فى البرنامج الاصلى او تزوير المعلومات أو محو بعضها بل قد يصل الى تدمير النظام المعلوماتى بأسره . نظراً للقدرة الفائقة لهذا الفيروس على الاختباء والاختفاء عن أعين المستخدم والتمويه عليه فقد شبه بحصان طرواده الذى استخدمه الإغريق حوالى عام 1200 ق.م. اذ تحكى ملحمة الالياذة لهوميروس : قصة حصار طروادة الذى استمر تسع سنوات دون أن يظفر اليونانيون بها وغلبهم اليأس والحنين إلى الوطن. فلجأو إلى الخدعة وقاموا بصنع هيكل حصان كبير ووضعوا فى داخله مجموعة من جنودهم وانسحبوا وتركوا الحصان خلفهم وعندما وجدت قوات طروادة الحصان فرحوا به وأدخلوه داخل الحصن، وفى الليل تسلل الجنود المختفون داخل الحصان وهاجموا الحصن وفتحوا أبوابه لإدخال القوات الإغريقية. راجع فى قصة حصار طروادة : د. نازلى اسماعيل حسين، تاريخ الفلسفة اليونانية، المكتبة القومية، القاهرة، 1981، ص 41 وما بعدها.

24 د. عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الإنترنت، رسالة دكتوراه، كلية الحقوق – جامعة عين شمس، 2004، ص263

بالإنترنت ويتطلب أيضًا معرفة بداية هذا النشاط والشروع فيه ونتيجته. فمثلاً يقوم مرتكب الجريمة بتجهيز الحاسب لكي يحقق له حدوث الجريمة.

بداية النشاط :

الجرائم الإلكترونية ليست مثل أي جريمة تستلزم وجود أعمال تحضيرية، إذ أنه يصعب الفصل بين العمل التحضيري والبدء في التنفيذ - حتى ولو كان القانون لا يعاقب على الأعمال التحضيرية - إلا أنه في مجال تكنولوجيا المعلومات الأمر يختلف بعض الشيء، فشراء برامج اختراق، ومعدات لفك الشفرات وكلمات المرور، وحيازة صور دعارة للأطفال أو حتى بعض الفيروسات التي لم يتم إطلاقها على الشبكة الإلكترونية، كل هذه الأفعال تمثل جريمة في حد ذاتها[25] .

الفرع الثاني

الركن المعنوي

الركن المعنوي في الجرائم الإلكترونية في كل التشريعات التي تناولتها يتخذ صورة القصد الجنائي العام[26]، باعتبارها من الجرائم العمدية، فلكي يتوافر لهذه الجرائم ركنها المعنوي يجب أن تتحقق عناصر القصد الجنائي من علم وإرادة ولذا قيل أن هذا الركن يعني في الحقيقة الجاني أو المجرم تحديداً[27].

وبتطبيق هذه المبادئ العامة على الجرائم الإلكترونية، ينبغي أولاً أن يحيط علم الجاني بكل واقعة ذات أهمية قانونية تدخل في تكوين هذه الجريمة، فلكي يتوافر القصد الجنائي يجب أن يحيط علم الجاني بعناصر الركن المادي للجريمة. ولعل أول هذه العناصر هو موضوع الحق المعتدى عليه، فعلى سبيل المثال يتعين توافر علم الجاني أن فعله ينصب على مستند إلكتروني محمي جنائياً بما يتضمنه من معلومات وبيانات باعتباره محل الحق الذي يحميه المشرع.

25 الدكتور/ وليد طه رئيس محكمة عضو قطاع التشريع بوزارة العدل جمهورية مصر العربية التنظيم التشريعي للجرائم الإلكترونية في اتفاقية بودابست -

26 ولمزيد من التفصيل حول مدلول القصد الجنائي وعناصره. انظر : د. عبدالمهيمن بكر، القصد الجنائي في القانون المصري والمقارن، رسالة دكتوراه، كلية الحقوق- جامعة عين شمس، 1959، المستشار الدكتور عمر الشريف على الشريف، درجات القصد الجنائي، دار النهضة العربية، القاهرة، الطبعة الأولى، 2002.

27 د. علي راشد، عن الإرادة والعمد والخطأ والسببية في نطاق المسئولية الجنائية، مجلة العلوم القانونية والاقتصادية، السنة الثامنة، العدد الأول، يناير 1966، ص15.

فإذا اعتقد الفاعل بناء على أسباب معقولة أنه يقوم على سبيل المثال بإجراء بعض العمليات الحسابية عن طريق الحاسب الآلي دون أن يتجه علمه إلى أنه يقوم بالدخول إلى نظام الحاسب بما يحتوي عليه من مستندات إلكترونية، فإن قصد الدخول لا يتوافر لديه. والحقيقة أن هذا الفرض على الرغم من أهميته القانونية إلا أنه يفتقر إلى هذه الأهمية من الناحية العملية، ونادراً ما يدخل الفاعل إلى نظام الحاسب الآلي وهو على غير علم بذلك. ويرجع ذلك إلى الخبرة التي يتمتع بها المجرم المعلوماتي في أغلب الأحوال والتي تحول دون إمكانية التسليم بهذا الفرض، وعلى الرغم من ذلك فإنه إذا ثبت انتفاء هذا العلم انتفى القصد الجنائي بدوره.

دوافع ارتكاب الجرائم الإلكترونية

للمجرم المعلوماتى في مجال الجرائم الإلكترونية دوافع خاصه تدفعه لارتكاب هذا النوع من الجرائم، من أهمها :

1- تحقيق الربح المادي:

قد يكون الدافع لارتكاب الجرائم الإلكترونية الطمع الذي يشبعه الاستيلاء على المال، فالثابت أن حوالى 43% من حالات الغش المعلوماتى المعلن عنها قد بوشرت من أجل الحصول على المال. ووفقاً للدراسات، فإن القطاع المالي يعد أكثر القطاعات استهدافا من قبل جرائم الحاسب الآلي[28].

فحب الفرد للمال والثراء السريع قد يدفعه للقرصنة والسرقة والنصب عن طريق الحاسب الآلي للحصول على المال لتلبية حاجاته الأساسية والرغبة في الثراء السريع الغير مكلف، فالرغبة في تحقيق الربح المادي بطريق غير مشروع قد يدفع بعض المجرمين بالاعتداء على بطاقات الدفع الإلكتروني مثلاً بتزويرها والتلاعب فيها من أجل الحصول على المال وهو ما يعد تزويراً في مستند إلكتروني كما سيلي بيانه في موضعه لاحقاً .

2- إثبات التفوق العلمي:

تدفع الرغبة في قهر نظام الحاسب[29] وإثبات التفوق العلمي في مجال الحاسب الآلي

28 Donn Parker, Fighting Computer Crime: A New Framework for Protecting Information, Wiley 1998.., p. 142.

29 د. هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، المرجع السابق، ص38.

بعض المجرمين إلى التحدي الفكري أثناء استخدامه الحاسب الآلي بإثبات قدرته على اختراق أنظمة الحاسب الآلي والدخول غير المشروع إليها، وأغلب من يقومون بتلك الأفعال هم صبية صغار أو المعروفون باسم صغار نوابغ المعلوماتية لأن هدفهم هو المنافسة في إثبات اكتشاف كل ما هو جديد في عالم المعلوماتية، ويكون ذلك بتخطي حاجز الحماية لبرامج الحاسب الآلي غير عابئين بما يحدث من مشاكل بسبب ذلك[30].

3- الرغبة في الانتقام:

الانتقام موجود داخل النفس البشرية، ويعتبر دافع الانتقام من أهم الدوافع التي تدفع المجرم المعلوماتي لارتكاب جريمته، فغالباً ما يصدر من شخص يملك معلومات كبيرة عن مؤسسة أو شركة أو بنك كان يعمل به لأنه غالباً ما يكون أحد موظفيها والذي يملك المعلومات الكافية عنها، ويقوم بهذا الدافع وهو غرض الانتقام نتيجة فصله تعسفياً أو تخطيه في الحوافز أو الترقية أو وقوع ظلم عليه في عمله، فيقدم بدافع الانتقام إلى ارتكاب جريمته ليجعل الشركة أو المؤسسة تتكبد الخسائر المالية الكبيرة[31]. كقيام أحد المحاسبين بالتلاعب بالبرامج المحاسبية بالشركة بعد أن يتم إبلاغه برغبة رب العمل بفصله بحيث تختفي هذه البرامج وتتآكل رغبة في الانتقام.

كما قد ترتكب هذه الأفعال خدمة لمصالح الغير، فقد تقوم بعض الشركات والمصانع والمنشآت الأخرى باستئجار محترفي التقنية بهدف التجسس على منشآت أخرى بقصد الإطلاع على أسرار المهنة أو آخر ما تم التوصل إليه من علوم لاختصار الوقت في البحث، أو لأجل المنافسة التجارية.

4- الشعور بالنقص:

قد يدفع الشعور بالنقص إلى إقدام المجرم المعلوماتي على ارتكاب الجريمة الإلكترونية سواء تعلق ذلك بالناحية الفسيولوجية أم النفسية أم العلمية، فيشعر الفرد بأنه أقل من الآخرين مما يؤدي إلى محاولة إثبات ذاته وتغلبه على هذا النقص وتعويضاً عن هذا العجز يقدم على ارتكاب الجريمة الإلكترونية .

---

30 د. محمد الشناوي، جرائم الإنترنت وبطاقات الإئتمان والجريمة المنظمة، تقديم د. مأمون سلامة، دار الكتاب الحديث، 2007، ص 46.

31 الاستاذة نسرين عبد الحميد نبيه، الجريمة المعلوماتية والمجرم المعلوماتي، منشأة المعارف، الإسكندرية، 2008، ص 44.

وأياً ما كان الباعث وراء إرتكاب الجرائم الإلكترونية فإنه يوجد شعور دائماً لدى مرتكب الفعل في تلك الجرائم بأن ما يقوم به لا يدخل في عداد الجرائم أو بقول آخر لا يتسم بالا أخلاقية.

5- حرية التعبير وتداول المعلومات:

قد تدفع حرية التعبير وتداول المعلومات وإطلاق الإعلام الإلكتروني بلا قيود بعض الأفراد والمنظمات وبدافع من الرغبة في إشاعة الحرية الإعلامية والفكرية والتواصل بين الأفراد إلى ارتكاب الجريمة الإلكترونية باختراق سرية بعض المواقع ونشر المستندات الإلكترونية السرية بين طرفين، وقد رأينا ما قام به جوليان آسانج[32] مؤسس موقع ويكيليكس الشهير وصاحب تسريبات ويكيليكس لخفايا و أسرار السياسة العالمية، ولا شك أن تلك المستندات الإلكترونية التي قام بالكشف عنها وتلك الوثائق تعد محررات إلكترونية سرية. ونرى أن الدافع لارتكاب تلك الجريمة الإلكترونية وما صاحبها من اختراق أمني للمعلومات كان دافعه الأكبر هو حرية تداول المعلومات حيث يزعم مؤسسه إلى «نشر الأخبار والمعلومات المهمة إلى الجمهور» من خلال نشر وثائق سرية، لاسيما وأن هذا الموقع الذى أسسه آسانج لا يهدف إلى الربح.

32 جوليان أسانج: مؤسس موقع ويكيليكس من مواليد 1971 بتاونسفيل بولاية كوينزلاند الاسترالية. وهو صحفي وناشط في الإنترنت ومبرمج استرالي، معروف بمشاركته في موقع ويكيليكس. حصل على جائزة من منظمة العفو الدولية في 2009. ولد أسانج – 39 عاما – لأبوين عملا في صناعة الترفيه، أدين أسانج بتهمة قرصنة الكمبيوتر في عام 1995، ويقال أنه كان يسمى نفسه «ميندا كس» عندما ارتكب تلك المخالفات واستمر ولعه بأجهزة الكمبيوتر حتى أواخر عقد التسعينيات، حيث عمل على تطوير نظم التشفير، وفي عام 1999 سجل أسانج موقعه الأول « ليكس دوت كوم» وبقيت صفحاته غير مفعلة، وفي عام 2006 أسس أسانج موقع «ويكيليكس» والذي يزعم أنه يهدف إلى نشر الأخبار والمعلومات المهمة إلى الجمهور من خلال نشر وثائق سرية، لاسيما حول الحرب الأمريكية في أفغانستان والعراق. ويقبل الموقع غير الهادف للربح «إخباريات من مصادر مختلفة»، لمزيد من التفاصيل حول هذا الموقع انظر: www.wilkileaks-a.blogspot.com

المبحث الثاني

صور الجرائم الإلكترونية

تتعدد صور الجرائم الالكترونية وتختلف باختلاف محل الجريمة والوسيلة، وهناك عدة تصنيفات لها، اهمها هي: تصنيف الجرائم الالكترونية تبعا لدور الكمبيوتر فيها :

1-جرائم تستهدف عناصر السرية والسلامة وتضم:

الدخول غير القانوني، تدمير المعطيات، اعتراض النظم، اساءة استخدام الاجهزة.

2- جرائم مرتبطة بالأجهزة الرقمية وتضم :

التزوير المرتبط بالأجهزة الرقمية، الاحتيال المرتبط بالأجهزة الرقمية .

3- الجرائم المرتبطة بالمحتوى وتضم :

الجرائم المتعلقة بالأفعال الاباحية، الجرائم اللاأخلاقية، الجرائم الماسة بحق المؤلف .

هذا ونستعرض اهم الصور التي وردت بالقانون ومواجهة المشرع لها.

المطلب الاول

صور الجرائم الإلكترونية

اولا : تزوير المستندات والتوقيعات الإلكترونية :

لقد اجتهد الفقه والقضاء في وضع تعريف عام للتزوير، حيث يتفق معظم الفقه[33] على تعريف التزوير بأنه هو تغيير الحقيقة في محرر يمكن أن يستخدم في إثبات حق أو واقعة يترتب عليها نتائج قانونية غشاً وإضراراً بالغير بواسطة إحدى الوسائل المحددة قانوناً، وهناك من يعرف التزوير في محرر بأنه هو «إظهار الكذب فيه بمظهر الحقيقة غشاً لعقيدة الغير» [34]. ولكن مع صدور قانون العقوبات الفرنسي الجديد الذي بدأ العمل به في الأول

33 انظر في تعريف التزوير، د. محمود نجيب حسني، شرح قانون العقوبات، القسم الخاص، دار النهضة العربية، القاهرة، 2012، رقم 315، ص 242.

34 د. رمسيس بهنام، القسم الخاص في قانون العقوبات، الجرائم المضرة بالمصلحة العمومية وجرائم الاعتداء على الأشخاص، دار المعارف بمصر، الطبعة الأولى، 1958، ص 88.

من مارس سنة 1994 فقد استحدث المشرع الفرنسي في باب التزوير نصاً جديداً هو نص المادة (141-1)[35] التي عرفت التزوير بأنه «كل تغيير للحقيقة في محرر أو أي نوعاً آخر بأي طريقة». وقد عرف جانب من الفقه[36] التزوير في المستند الإلكتروني بأنه تغيير الحقيقة في المحررات المعالجة آلياً والمحررات المعلوماتية وذلك بنية استعمالها.

علة تجريم التزوير في المستندات الإلكترونية:

لا شك أن تطور تكنولوجيا الحاسبات الآلية[37]، ومع زيادة الاعتماد عليها في تخزين ومعالجة الكثير من المعلومات الهامة التي تحويها المستندات الإلكترونية كالبيانات المتعلقة بالميلاد والوفاة وجوازات السفر ورخص القيادة وملفات الحكومة الإلكترونية وغيرها من البيانات المؤثرة في المعاملات القانونية بوجه عام، كان دافعاً إلى حماية هذه المستندات من التلاعب بها، حتى يدفع الأفراد إلى عدم التشكيك بها واحترامها وبث الثقة فيها.

فالثقة العامة في المستندات الإلكترونية هي المصلحة المحمية بالعقاب على التزوير فيها. والثقة العامة في المحررات عامة[38] هو شعور مشترك لدى أفراد الجماعة بالاطمئنان إلى سلامة المحررات أي صدورها ممن نسب إليه وصدق ما تحويه من تصرفات أو وقائع وذلك بمطابقتها للحقيقة الواقعة. فمجرد الاستناد إلى المحرر دون إظهاره لا يعد استعمالاً له، فلا يرتكب الجريمة من يقدم ورقة مزورة دون أن يتمسك بها، ولكنه يرتكبها إذا أبدى رغبته في الاحتجاج بالورقة المزورة بعد تقديمها. فتقوم جريمة استعمال المستند الإلكتروني المزور باستعماله فيما زور من أجله، مع علم من استعمله بتزويره[39].

---

35 Article 441-1 du Code pénal : Constitue un faux toute altération fraudul - use de la vérité, de nature à causer un préjudice et accomplie par quelque moyen que ce soit, dans un écrit ou tout autre support d'expression de la pensée qui a pour objet ou qui peut avoir pour effet d'établir la preuve d'un droit ou d'un fait ayant des conséquences juridiques. Le faux et l'usage de faux sont punis de trois ans d'emprisonnement et de 45000 euros d'amende.

36 د. علي عبدالقادر القهوجي، الحماية الجنائية للبيانات المعالجة إلكترونياً، دراسة مقدمة إلى مؤتمر «القانون والكمبيوتر والإنترنت»، الذي عقدته كلية الشريعة والقانون بجامعة الإمارات العربية المتحدة، بمدينة العين في الفترة من 1-3 مايو سنة 2000، ص 63.

37 د. نائلة عادل فريد قورة، جرائم الحاسب الآلي الاقتصادية، دراسة نظرية وتطبيقية، منشورات الحلبي الحقوقية، بيروت، لبنان، 2005، ص 270.

38 د. أحمد شوقي الشلقاني، الضرر في تزوير المحررات، رسالة دكتوراه، كلية الحقوق- جامعة القاهرة، 1980، ص45.

39 تمييز جزائي الطعن رقم 9 لسنة 2002 - جلسة 18/ 3 /2003 س31 ق23 ص445 .

ثانيا : جريمة إتلاف أنظمة معالجة البيانات

إن السمة الغالبة في إتلاف المعلومات الإلكترونية، أن يتم الإتلاف داخل النظام المعلوماتي أثناء تشغيل جهاز الحاسب الآلي وذلك بأحد أساليب الإتلاف التي سيأتي بيانها، وهذه الصورة تستلزم في مرتكبيها صفات خاصة مثل الذكاء واحتراف التعامل مع الأنظمة المعلوماتية.

فهو إتلاف لا ينشأ بأسلوب العنف والتحطيم أو التكسير التقليدي ولكن عن طريق ما يسمى بتقنيات التدمير الناعمة[40]. ونظراً للطبيعة الخاصة التي تتسم بها المكونات غير المادية للمعلومات والبيانات الإلكترونية والتي يغلب عليها الطابع المعنوي فقد أطلق عليها بعض الفقه مصطلح «تدمير نظم المعلومات» وذلك على الإتلاف الحاصل للمكونات المعنوية للنظم المعلوماتية[41].

وسائل إتلاف أنظمة معالجة البيانات:

الركن المادي في جرائم إتلاف أنظمة المعلومات يتمثل في قيام الجاني بارتكاب فعل عن طريق وسيلة معينة، وقد تكون هذه الوسيلة هي الفيروسات أو وسائل أخرى، والاتلاف بواسطة الفيروسات يؤدي إلى إحداث خلل في السير الطبيعي للمعلومات أو في شكل المستند الإلكتروني ومحتواه وذلك بتعديل في مضمونه بحيث تصبح البيانات على المستند الإلكتروني غير صحيحة عند استدعائها.

الإتلاف بواسطة الفيروسات:

الفيروسات من وسائل إتلاف أنظمة المعلومات، وهى تختلف من حيث أنواعها وقوتها التدميرية.

مفهوم الفيروس Virus :

فيروس الحاسب الآلي هو وسيلة تكنيكية حديثة تستخدم لارتكاب جرائم معينة[42]، والفيروسات هي برامج مشفرة مصممة بقدرة على التكاثر والإنتشار من نظام إلى آخر

---

40 د. عمر أبوالفتوح عبد العظيم الحمامي، الحماية الجنائية للمعلومات المسجلة إلكترونياً، رسالة دكتوراه، كلية الحقوق -جامعة القاهرة 2009، ص 539.

41 د. محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات،، دار النهضة العربية، القاهرة، 1994، ص197.

42 tions. J.C.P. 1988.I. étude n° 3321. مشار إليه لدى د. رشدي محمد على عيد، الحماية الجنائية للمعلومات عبر الإنترنت، رسالة دكتوراه، كلية الحقوق– جامعة القاهرة، 2009، ص 250.

بواسطة قرص ممغنط أو عبر شبكة الاتصالات، بحيث يمكن أن تنتقل عبر الحدود من أي مكان إلى آخر في العالم[43]، وبرامج الفيروسات لها القدرة على الاختفاء داخل برنامج سليم بحيث يصعب اكتشافها، وقد تكون مصممة لتدمير برامج أخرى أو تغيير معلومات ثم تقوم بتدمير نفسها ذاتياً دون أن تترك أثراً يدل عليها، وعلى الرغم من قدرتها على تدمير البرامج والمعلومات، إلا أنها لا تسبب عادة تدميراً لمكونات النظام المادي[44]. والفيروس المعلوماتي له من خصائص المجرم الكثير فهو يختفي كخطوة أولى ثم يبدأ في التطور كخطوة ثانية ليدمر في خطوة ثالثة، كالمجرم الذي يضع خطته لارتكاب الجريمة[45].

صفوة القول، أن الركن المادي لجريمة إتلاف أنظمة معالجة البيانات يتمثل في التعديل غير المشروع للبيانات التي يحويها المستند الإلكتروني أو تدميرها بمحوها كلياً أو جزئياً أو إخفاءها بحيث لا يمكن الوصول إليها باستخدام الفيروسات المختلفة كما بينا. أو إعاقة سير النظام الذي يحتوي على المستند الإلكتروني.

ثالثا: الإرهاب الإلكتروني (Cyber terrorism)[46]

هي اختراقاتٌ للأنظمةِ الأمنيّة الحيوية على مواقع الإنترنت، تكونُ جُزءاً من مجهودٍ مُنظّم لمجموعةٍ من الإرهابيين الإلكترونيين أو وكالات مخابراتٍ دوليّة، أو أيّ جماعات تَسعى للاستفادة من ثغرات هذه المواقع والأنظمة.

ويعتمد الإرهاب الإلكتروني على استخدام إمكانيات أو مقدرات الحاسب الآلي في ترويع أو إكراه الآخرين، وعلى سبيل المثال الدخول بصورة غير مشروعة إلى نظام الكمبيوتر في أحد المستشفيات بغرض تغيير مقادير ومكونات وصفة طبية لمريض ما لتكون جرعة قاتلة تؤدي إلى وفاة المريض على سبيل الانتقام.

---

43 مثل فيروس الفدية الخبيثة وهو برنامج خبيث يقيد الوصول إلى نظام الحاسب الذي يصيبه، ويطالب بدفع فدية لصانع البرنامج من أجل إمكانية الوصول للملفات، وفيروس «بيتيا»، فيروس الدودة worm virus، انظر: د. هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، المرجع السابق، ص 161 وما بعدها، وايضا فيروس القنبلة المنطقية : Logic Bomb هو اصطلاح يطلق على أنواع من الفيروسات المعلوماتية التي تهدف إلى تدمير المعلومات والبرامج كوسيلة لإرتكاب جريمة الإتلاف

44 د. عزة محمود أحمد خليل، مشكلات المسئولية المدنية في مواجهة فيروس الحاسب، دراسة مقارنة في القانون المدني والشريعة الإسلامية، رسالة دكتوراه، كلية الحقوق - جامعة القاهرة، 1994، ص 37 وما بعدها.

45 د. ماجد عمار، المسئولية القانونية الناشئة عن استخدام فيروس برامج الكمبيوتر ووسائل حمايتها، دار النهضة العربية، القاهرة، 1989، ص76.

46 الارهاب الالكتروني هو العدوان أو التخويف أو التهديد ماديًا أو معنويًا باستخدام الوسائل الإلكترونية الصادر من الدول أو الجماعات أو الأفراد على الإنسان دينه، أو نفسه، أو عرضه، أو عقله، أو ماله، بغير حق بشتى صنوفه وصور الإفساد في الأرض.

رابعا: التشهيروتشويه السمعة: (الابتزاز الإلكتروني)

حيث يقوم المجرم بنشر معلومات قد تكون سرية أو مضللة أو مغلوطة عن ضحيته، والذي قد يكون فرداً أو مؤسسة تجارية أو سياسية، وتتعدد الوسائل المستخدمة في هذا النوع من الجرائم، لكن في مقدمة هذه الوسائل إنشاء موقع على الشبكة يحوي المعلومات المطلوب نشرها أو إرسال هذه المعلومات عبر القوائم البريدية إلى أعداد كبيرة من المستخدمين، و يُضم لهذه الجرائم كذلك تشويه السمعة، الشائعات و الأخبار الكاذبة لمحاربة الرموز السياسية و الفكرية و حتى الدينية من أجل تشكيك الناس في مصداقية هؤلاء الأفراد، و قد يكون الهدف من ذلك هو الابتزاز.

المطلب الثانى

المواجهة التشريعية للجرائم الإلكترونية في دولة الكويت

يكفُل القانون رقم 20 لسنة 2014[47] فى شأن المعاملات الالكترونية ولائحته التنفيذية حماية جنائية للمعاملات الإلكترونية وكذلك القانون رقم 63 لسنة 2015 فى شأن مكافحة جرائم تقنية المعلومات من خلال ما هو مقرر من عقوبات وأحكام رادعة تكفل الحماية لتلك المعاملات وتفرض عقوبات على الجرائم الماسة بالمستند والسجل الإلكترونى وغيره من وسائط التعامل فى البيئة الإلكترونية والتى باتت من الأهمية بمكان لتسهيل سبل الحياة . وعلى هدي من ذلك، سوف نخصص هذا المطلب لعرض استراتيجية مواجهة الجرائم الإلكترونية من خلال النصوص الواردة فى هذين القانونين، على النحو التالى :

الفرع الاول

القانون رقم 20 لسنة 2014 فى شأن المعاملات الالكترونية

يشهد العالم تطوراً هائلاً فى مجال الاتصالات التى تعتمد على تبادل المعلومات عبر شبكات الاتصال الحديثة سواء من خلال شبكة الإنترنت أو غيرها من وسائل الاتصال والنظم الإلكترونية كوسيلة لتبادل ونشر المعلومات وبثها وحفظها واسترجاعها، ولما

47 القانون رقم 20 لسنة 2014 فى شأن المعاملات الإلكترونية الصادر فى 2/11 /2014، والمنشور فى الجريدة الرسمية (الكويت اليوم) بالعدد 1172 السنة الستون بتاريخ 2/23 /2014 .

كانت الكويت من الدول العربية السباقة فى الأخذ بالنظم الحديثة لتطوير أوجه النشاط الاقتصادى فيها[48]، ومن ثم فقد بات من الضرورى إعداد تشريع ينظم هذه المعاملات ويضع القواعد المنظمة لها وكذا العقوبات على الجرائم الماسة بالأفعال التى تهز الثقة فى تلك المعاملات وتضع الحماية الجزائية لها. ويتكون القانون رقم 20 لسنة 2014 فى شأن المعاملات الإلكترونية من 46 مادة موزعة على ثمانية فصول وقد جاء القانون رقم 20 لسنة 2014 فى شأن المعاملات الإلكترونية الكويتى دعماً لمسيرة البلاد في التنمية الشاملة ودفعاً للتطوير والتحديث لكل مجالات الحياة فيها على أن تواكب هذا التطور المتعاظم في وسائل الاتصالات الإلكترونية للاستفادة في المعاملات التجارية وغيرها الأمر الذي اقتضى إعداد تشريع ينظم هذه المعاملات ويضع لها القواعد والضوابط المناسبة. كما يضع صور التجريم والعقوبات للجرائم الماسة بنظم المعالجة الإلكترونية للبيانات والمعلومات لحماية المعاملات الإلكترونية.

الجرائم الإلكترونية الواردة فيه

بداية نشير إلى نص المادة 40 من القانون والتى ناطت بالنيابة العامة دون غيرها بالتحقيق والتصرف والإدعاء فى جميع الجرائم المنصوص عليها فى هذا القانون والجرائم المرتبطة بها.

أما الجرائم المنصوص عليها فى هذا القانون فهى :

1- جريمة تعمد الدخول بغير وجه حق إلى نظام المعالجة الإلكترونية، أو تعطيل الوصول إلى هذا النظام أو التسبب فى إتلافه، أو الحصول على أرقام أو بيانات بطاقات ائتمانية وغيرها من البطاقات الالكترونية للحصول على أموال الغير (المادة 37/أ).

2- جريمة إصدار شهادة تصديق إلكترونية أو مزاولة أى خدمه من خدمات التصديق الإلكترونى دون الحصول على ترخيص بذلك من الجهة المختصة (المادة 37/ب).

3- جريمة إتلاف أو تعييب توقيع أو نظام أو أداة توقيع أو مستند أو سجل إلكترونى أو تزوير شىء من ذلك بطريق الاصطناع أو التعديل أو التحوير بأى طريقة أخرى.(المادة 37/ج)

48 المذكرة الإيضاحية للقانون رقم 20 لسنة 2014 فى شأن المعاملات الإلكترونية .

جريمة استعمال توقيع أو نظام أو أداة توقيع أو مستند أو سجل إلكترونى معيب أو مزور مع العلم بذلك (المادة 37/د).

4- جريمة التوصل بأى وسيلة دون وجه حق على توقيع أو نظام أو مستند أو سجل إلكترونى أو اختراق هذا النظام أو اعتراضه أو تعطيله عن أداء خدمته (المادة 37/هـ) .

5- جريمة الاطلاع دون وجه حق على، أو إفشاء، أو نشر أية بيانات أو معلومات شخصية مسجلة فى سجلات أو أنظمة معالجة إلكترونية تتعلق بالشئون الوظيفية أو السيرة الاجتماعية أو الحالة الصحية أو عناصر الذمة المالية للأشخاص أو غير ذلك من البيانات الشخصية المسجلة لدى الجهات الحكومية أو الهيئات أو المؤسسات العامة أو الشركات أو الجهات غير الحكومية أو العاملين بها، دون موافقة الشخص المتعلقة به هذه البيانات أو المعلومات أو من ينوب عنه قانوناً، ودون قرار قضائى مسبب، ودون بيان الغرض من جمع هذه البيانات أو المعلومات ودون جمعها فى حدود هذا الغرض(عملاً بالمادتين 32، 37/و من القانون).

6- جريمة جمع أو تسجيل أو تجهيز البيانات والمعلومات الشخصية – المشار إليها فى البند السابق – بأساليب أو طرق غير مشروعة أو بغير رضاء الشخص الذى تتعلق به هذه البيانات أو رضاء من ينوب عنه قانوناً (المواد 32، 35/أ، 37/و).

7- جريمة استخدام البيانات أو المعلومات الشخصية – المشار إليها فى البند السابق – والمسجلة لدى سجلات الجهات المشار إليها أو بأنظمة معلوماتها فى غير الأغراض التى جمعت من أجلها (المواد 32، 35/ب، 37/و).

8- جريمة تقديم بيانات غير صحيحه فى طلب التسجيل المقدم ممن رخص له فى إصدار خدمات التصديق الإلكترونى إلى الجهة المختصة أو بالمخالفة لشروط الترخيص (المادة 38).

تشديد العقوبة فى حالة العود:

نصت الفقرة الأولى من المادة 37 من هذا القانون على أن يعاقب كل من يرتكب إحدى الجرائم المنصوص عليها فى تلك المادة بالحبس مدة لا تزيد عن ثلاث سنوات وبغرامة لا

تقل عن خمسة آلاف دينار ولا تزيد على عشرين ألف دينار أو بإحدى هاتين العقوبتين.

كما نصت الفقرة الأخيرة من هذه المادة على أن « تضاعف العقوبة فى حالة العود إلى ارتكاب أى من هذه الجرائم».

مسئولية الشخص المعنوى:

نصت المادة (1/39) من قانون المعاملات الإلكترونية على معاقبة المسئول عن الإدارة الفعلية للشخص المعنوى بذات العقوبات المقررة عن الأفعال التى ترتكب بالمخالفة لأحكام القانون إذا كان إهماله أو إخلاله بالواجبات التى تفرضها عليه إدارته للشخص المعنوى قد أسهم فى وقوع الجريمة مع علمه بذلك.

التصالح :

نصت المادة 42 من القانون على جواز التصالح لمن ارتكب إحدى الجرائم المنصوص عليها فى هذا القانون لأول مرة، على أن يقدم طلب الصلح إلى النيابة العامة مع دفع ألف دينار لخزينة المحكمة قبل إحالة الدعوى إلى المحكمة المختصة، وأجازت للنيابة العامة قبول طلب الصلح بما يرتبه ذلك من انقضاء الدعوى الجزائية قبل المتهم هى وجميع آثارها.

الفرع الثاني

القانون رقم 63 لسنة 2015 فى شأن مكافحة جرائم تقنية المعلومات[49]:

أصبحت الجرائم الإلكترونية واحداً من التحديات التي تحرص الأجهزة الأمنية والشرطية في الدولة على مواجهتها والتصدّي لها بكل حزم، بعد أن تزايدت بصورة واضحة في الآونة الأخيرة، نتيجة تزايد استخدام التكنولوجيا الحديثة في مجال الاتصالات والإدارة والأعمال المصرفية والمالية، وهي المعطيات التي تشكل بيئة خصبة لعمل عصابات الإجرام الإلكتروني. وتتعلق بتأثير الجرائم الإلكترونية في الوضع الاقتصادي العام، خاصة أن نسبة كبيرة من هذه الجرائم بدأت تستهدف بصورة أساسية المؤسسات المالية والشركات العاملة

49 القانون رقم 63 لسنة 2015 فى شأن مكافحة جرائم تقنية المعلومات الصادر فى 7/7 /2015، والمنشور فى الجريدة الرسمية (الكويت اليوم) بالعدد 1244 السنة الالحادية و الستون بتاريخ 12/7 /2015 .

في الدولة، كمحاولات الاحتيال على البنوك باستخدام وسائل تقنية متطورة تستهدف سحب الأموال بطريقة غير شرعية، من خلال تزوير بعض المستندات والأوراق، أو من خلال سرقة الرموز البنكية، أو الأرقام السرية لحسابات العملاء، وبيانات البطاقات الائتمانية لاستغلالها في أغراض إجرامية.

جاء القانون رقم 63 لسنة 2015 فى شأن مكافحة جرائم تقنية المعلومات و تناول في الفصل الأول في المادة الأولى منه التعريفات التي تبين المقصود بالمصطلحات الفنية الواردة فيه . وشمل الفصل الثاني الجرائم والعقوبات، ومن أهم المواد الواردة فيه :

1- جريمة الدخول الغير مشروع

الدخول غير مشروع إلى جهاز حاسب آلي أو إلى نظامه أو إلى نظام معالجة إلكترونية للبيانات أو إلى نظام إلكتروني مؤتمت أو إلى شبكة معلوماتية.

الظرف المشدد:

فإذا ترتب على هذا الدخول إلغاء أو حذف أو إتلاف أو تدمير أو إفشاء أو تغيير أو إعادة نشر بيانات أو معلومات.

او كانت تلك البيانات أو المعلومات شخصية.

2- جريمة الدخول الغير مشروع إلى موقع أو نظام معلوماتي مباشرة أو عن طريق الشبكة المعلوماتية أو بإحدى وسائل تقنية المعلومات بقصد الحصول على بيانات أو معلومات حكومية سرية بحكم القانون.

وتشدد العقوبة :

– فإذا ترتب على ذلك الدخول إلغاء تلك البيانات أو المعلومات أو إتلافها أو تدميرها أو نشرها أو تعديلها

– او كانت البيانات والمعلومات متعلقة بحسابات عملاء المنشآت المصرفية.

3- جريمة تغييّر أو أتلاف مستنداً إلكترونياً عمداً يتعلق بالفحوصات الطبية أو

التشخيص الطبي أو العلاج الطبي أو الرعاية الطبية أو سهل للغير فعل ذلك أو مكنه منه، وذلك باستعمال الشبكة المعلوماتية أو باستخدام وسيلة من وسائل تقنية المعلومات.

4- جريمة تعمد أعاقة أو تعطيل الوصول إلى موقع خدمة إلكترونية أو الدخول إلى الأجهزة أو البرامج أو مصادر البيانات أو المعلومات الإلكترونية بأي وسيلة كانت وذلك عن طريق الشبكة المعلوماتية أو باستخدام وسيلة من وسائل تقنية المعلومات.

5- جريمة تعمد أدخال – عن طريق الشبكة المعلوماتية أو باستخدام وسيلة من وسائل تقنية المعلومات – ما من شأنه إيقاف الشبكة المعلوماتية عن العمل أو تعطيلها، أو دخل موقعاً في الشبكة المعلوماتية لتغيير تصاميم هذا الموقع أو إلغائه أو إتلافه أو تعديله أو شغل عنوانه أو إيقافه أو تعطيله . وتشدد العقوبة اذا ارتكب أياً من هذه الجرائم أو سهل ذلك للغير وكان ذلك أثناء أو بسبب تأدية وظيفته.

6- جريمة تعمد التنصت أو الالتقاط أو اعتراض دون وجه حق، ما هو مرسل عن طريق الشبكة المعلوماتية أو وسيلة من وسائل تقنية المعلومات.

7- جريمة استخدام الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات للوصول دون وجه حق إلى أرقام أو بيانات بطاقة إئتمانية أو ما في حكمها من البطاقات الإلكترونية.

وتشدد العقوبة إذا ترتب على استخدامها الحصول على أموال الغير، أو على ما تتيحه هذه البطاقة من خدمات

8- جريمة انشاء موقعاً أو نشر معلومات باستخدام الشبكة المعلوماتية أو بأي وسيلة من وسائل تقنية المعلومات المنصوص عليها في هذا القانون، بقصد الإتجار بالبشر أو تسهيل التعامل فيهم، أو ترويج المخدرات أو المؤثرات العقلية وما في حكمها، أو تسهيل ذلك في غير الأحوال المصرح بها قانوناً .

9- جريمة القيام – عن طريق الشبكة المعلوماتية أو باستخدام وسيلة من وسائل تقنية المعلومات – بغسل أموال أو بتحويل أموال غير مشروعة أو بنقلها أو بتمويه أو بإخفاء

مصدرها غير المشروع، أو قام باستخدامها أو اكتسابها أو حيازتها مع علمه بأنها مستمدة من مصدر غير مشروع أو بتحويل الموارد أو الممتلكات مع علمه بمصدرها غير المشروع، وذلك بقصد إضفاء الصفة المشروعة على تلك الأموال.

10- جريمة أنشاء موقعاً لمنظمة إرهابية أو لشخص إرهابي أو نشر عن أيهما معلومات على الشبكة المعلوماتية أو بإحدى وسائل تقنية المعلومات ولو تحت مسميات تمويهية، لتسهيل الاتصالات بأحد قياداتها أو أعضائها، أو ترويج أفكارها، أو تمويلها، أو نشر كيفية تصنيع الأجهزة الحارقة، أو المتفجرة، أو أية أدوات تستخدم في الأعمال الإرهابية .

المبحث الثالث

الاحكام الاجرائية للجرائم الإلكترونية

اختصاص النيابة العامة :

نصت المادة 17 من القانون رقم 63 لسنة 2015 فى شأن مكافحة جرائم تقنية المعلومات على أن تختص النيابة العامة – دون غيرها – بالتحقيق والتصرف والادعاء في جميع الجرائم المنصوص عليها في هذا القانون.

ومن ثم فقد اناط المشرع بالنيابة العامة وحدها دون غيرها سلطة التحقيق والتصرف والادعاء .

ويقصد بالتحقيق استجواب المتهم وسماع الشهود وتحقيق الواقعة أما التصرف فيقصد به اتخاذ قرار بشأن التحقيق الذي تم إجراؤه بشأن الواقعة بالإحالة إلى المحكمة أو حفظ الأوراق، أما الادعاء فيقصد به مباشرة الدعوى الجزائية أمام المحكمة وفقا لنص المادة 105 من قانون الإجراءات والمحاكمات الجزائية والتي جرى نصها على أن « تتولى النيابة العامة مباشرة الدعوى الجزائية بطلب توقيع العقوبة على المتهمين بالجنايات وفقا للإجراءات وطبقا للشروط المنصوص عليها في هذا القانون » ومن ثم فلا يجوز لمحققي وزارة الداخلية إجراءات تحقيق أو التصرف في الدعوى الجزائية، ولا يجد لها من ثم إحالتها للمحكمة، فاختصاص النيابة العامة بالتحقيق والتصرف والادعاء في جنح الصحافة هو اختصاص أصيل مقرر لها باعتبارها سلطة الادعاء العام أمام محكمة الجنايات .

المحكمة المختصة :

نظرا لخلو القانون رقم 63 لسنة 2015 بشان مكافحة جرائم تقنية المعلومات من نصوص خاصة في تحديد اختصاص المحاكم، فتطبق القواعد العامة في الاختصاص النوعي.

فتختص محكمة الجنح بنظر الجرائم التي يعاقب عليه بالحبس مدة لا تجاوز ثلاث

سنوات والغرامة أو بإحدى هاتين العقوبتين[50]، في حين تختص محكمة الجنايات بنظر الجرائم المعاقب عليها بالإعدام أو بالحبس المؤبد أو بالحبس المؤقت مدة تزيد على ثلاث سنوات[51].

الاعفاء من العقاب:

للمحكمة أن تعفي من العقوبة كل من بادر من الجناة بإبلاغ السلطات المختصة بالجريمة قبل علمها بها وقبل البدء في تنفيذ الجريمة، فإن كان الإبلاغ بعد العلم بالجريمة وقبل البدء في التحقيق تعيّن للإعفاء من العقوبة أن يكون من شأن الإبلاغ ضبط باقي الجناة في حالة تعددهم[52]

المصادرة :

يجوز الحكم بمصادرة الأجهزة أو البرامج أو الوسائل المستخدمة في ارتكاب أي من الجرائم المنصوص عليها في هذا القانون أو الأموال المتحصلة منها. ويجوز الحكم بإغلاق المحل أو الموقع الذي أُرتكب فيه أي من هذه الجرائم إذا كان ارتكابها قد تم بعلم مالكها لمدة لا تزيد على سنة بحسب الأحوال، مع عدم الإخلال بحقوق الغير حسن النية أو بحق المضرور في التعويض المناسب . ويكون الحكم بإغلاق المحل أو الموقع وجوبياً إذا تكرر ارتكاب أياً من هذه الجرائم بعلم مالكها [53].

ويلاحظ ان المصادرة جوازيه .

مسئولية الشخص المعنوي:

مع عدم الإخلال بالمسئولية الجزائية الشخصية لمرتكب الجريمة، يعاقب الممثل القانوني للشخص الاعتباري بذات العقوبات المالية المقررة عن الأفعال التي تُرتكب بالمخالفة لأحكام هذا القانون، إذا ثبت أن إخلاله بواجبات وظيفته أسهم في وقوع الجريمة مع علمه بذلك. ويكون الشخص الاعتباري مسئولاً عما يحكم به من عقوبات مالية أو تعويضات إذا

50 مادة 5 من قانون الجزاء
51 مادة 3 من قانون الجزاء
52 مادة 12 من القانون رقم 63 لسنة 2015 فى شأن مكافحة جرائم تقنية المعلومات
53 مادة 13 من القانون رقم 63 لسنة 2015 فى شأن مكافحة جرائم تقنية المعلومات

أُرتكبت الجريمة لحسابه أو باسمه أو لصالحه[54] .

انقضاء الدعوى الجزائية :

تسقط الدعوى الجزائية المنصوص عليها في هذا القانون بحسب مدة العقوبة، فإن كانت بحدود الثلاث(جنحة) سنوات فتسقط خلال سنتين .

وإن كانت تتجاوز الثلاث سنوات (جناية) فتسقط خلال خمس سنوات من يوم وقوع الجريمة.

انقضاء دعوى التعويض :

لا تسُمع دعوى التعويض إذا لم يتم رفعها خلال ثلاث سنوات من تاريخ علم المضرور، ما لم تكن الدعوى الجزائية قائمة فيبدأ ميعاد عدم السماع من تاريخ انقضائها أو صدور حكم نهائي فيها.

54 مادة 14 من القانون رقم 63 لسنة 2015 فى شأن مكافحة جرائم تقنية المعلومات

خاتمة :

تناولنا فيما سبق الجريمة الالكترونية وتعريفاتها واركانها وما تتميز به من خصائص وما يتميز به المجرم المعلوماتي، كما عرضنا لاهم صور الجرائم الالكترونية في التشريعات ومما 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 مما حدا بالمشرع بمواجهتها للحد من خطورتها .

ملخص الجرائم والعقوبات

في القانون رقم 63 لسنة 2015 بشأن مكافحة جرائم تقنية المعلومات

مادة 2

الجريمة : الدخول غير المشروع إلى جهاز حاسب آلي او نظام معلوماتي أو شبكة معلوماتية

العقوبة: الحبس مدة لاتجاوز ستة أشهر + غرامة (500 - 2000) دينارأو أحداهما.

الجريمة : إذا ترتب على الدخول إلغاء أو حذف أو تدمير أو تغير أو إعادة نشر بيانات أو معلومات

العقوبة: الحبس مدة لا تتجاوز سنتين + الغرامة (2 - 5) ألف دينار أو إحدى هاتين العقوبتين

إذا كانت البيانات او المعلومات شخصية تكون العقوبة ثلاث سنوات حبس + غرامة (3 - 10) الف دينار او احدهما

مادة 3

الجريمة : الدخول غير المشروع بقصد الحصول على بيانات أو معلومات حكومية سرية

العقوبة : الحبس مدة لاتتجاوز (3) سنوات + الغرامة (3 - 10) آلاف دينار أو إحدى هاتين العقوبتين

إذا ترتب على الدخول الغاء تلك البيانات او إتلافها أو تدميرها أو نشرها أو تعديلها تكون العقوبة (الحبس مدة لاتتجاوز (10) سنوات + الغرامة (5 - 20) ألف دينار أو إحدى هاتين العقوبتين

مادة 2/3

الجريمة : تزوير أو إتلاف مستند،أو سجل أو توقيع إلكتروني أو نظام إلكتروني أو موقع.

العقوبة : الحبس مدة لاتتجاوز (3) سنوات + الغرامة (3 -10) آلاف دينار أو إحدى هاتين العقوبتين

اذا وقع التزوير على مستند رسمي أو بنكي أو بيانات حكومية أو بنكية تكون العقوبة: (الحبس مدة لاتتجاوز (7) سنوات + الغرامة (5 - 20) آلاف دينار أو إحدى هاتين العقوبتين

مادة 3/3

الجريمة: تغيير أو اتلاف مستند الكتروني يتعلق بالفحوصات الطبية أو التشخيص أو العلاج الطبي

العقوبة : الحبس مدة لاتجاوز (3) سنوات + الغرامة (3 - 10) ألف دينار أو إحدى هاتين العقوبتين

مادة 4/3

الجريمة : تهديد او ابتزاز شخص طبيعي أو اعتباري لحملة على فعل أو الامتناع عنه

العقوبة : الحبس مدة لاتتجاوز (3) سنوات + الغرامة (3 - 10) ألف دينار أو إحدى هاتين العقوبتين

اذا كان التهديد بارتكاب جناية أو بما يعد مساساً بكرامة الشخص أو خدش للشرف أو الاعتبار تكون العقوبة الحبس مدة لا تتجاوز (5) سنوات + الغرامة (5 - 20) ألف دينار أو أحدهما

الجريمة: الاستيلاء على منفعة أو مال أو مستند أو توقيع على مستند باستعمال طرق احتيالية

العقوبة: الحبس مدة لاتتجاوز (3) سنوات +غرامة (3 - 10) الف أو إحدى هاتين العقوبتين

المادة 4

الجريمة: إعاقة أو تعطيل الوصول إلى موقع أو الدخول إلى الاجهزة أو البرامج أو مصادر البيانات عمداً

العقوبة: الحبس مدة لاتجاوز سنتين + غرامة (2 - 5) ألف دينار أو إحدى هاتين العقوبتين

المادة 4/2

الجريمة: الادخال العمدي عن طريق الشبكة المعلوماتية أو باستخدام وسيلة من وسائل تقنية المعلومات ما من شانه تعطيلها أو ايقافها عن العمل، او دخول موقع لتغيير تصميمه او الغاء او تعديل أوايقافة

العقوبة: الحبس مدة لاتتجاوز سنتين + الغرامة (2-5) ألف دينار أو إحدى هاتين العقوبتين

ويعاقب بالحبس مدة لا تجاوز ثلاث سنوات وبغرامة لا تقل عن ثلاثة آلاف دينار ولا تجاوز عشرة آلاف دينار أو بإحدى هاتين العقوبتين، كل من ارتكب أياً من هذه الجرائم أو سهل ذلك للغير وكان ذلك أثناء أو بسبب تأدية وظيفته

المادة 4/3

الجريمة : التنصت او الالتقاط اوالاعتراض عمدا ماهو مرسل عن طريق الشبكة المعلوماتية او وسيلة تقنية المعلومات

العقوبة : الحبس مدة لاتجاوز سنتين + غرامة (2 - 5) الف دينار أو إحدى هاتين العقوبتين

فإذا أفشى ما توصل إليه يعاقب بالحبس مدة لا تجاوز ثلاث سنوات وبغرامة لا تقل عن ثلاثة آلاف دينار ولا تجاوز عشرة آلاف دينار أو بإحدى هاتين العقوبتين .

المادة 4/4

الجريمة: إنشاء موقع او نشر او انتاج او اعداد او ارسال او تخزين معلومات او بيانات بقصد الاستغلال او التوزيع او العرض على الغير وكان ذلك من شانه المساس بالآداب العامة أو إداره مكان لهذا الغرض.

العقوبة: الحبس مدة لاتتجاوز سنتين + غرامة (2 - 5) الف دينار أو إحدى هاتين العقوبتين

المادة 5/4

الجريمة : التحريض على ارتكاب اعمال الدعارة والفجور أو المساعدة على ذلك

العقوبة : الحبس مدة لاتتجاوز سنتين + غرامة (2 - 5) الف دينار اواحدهم

فإذا كان الفعل موجهاً إلى حدث فتكون العقوبة الحبس مدة لا تجاوز ثلاث سنوات والغرامة التي لا تقل عن ثلاثة آلاف دينار ولا تجاوز عشرة آلاف دينار أو بإحدى هاتين العقوبتين

المادة 5

الجريمة: استخدام شبكة المعلومات أو وسيلة من وسائل تقنية المعلومات للوصول دون وجة حق إلى أرقام أو بيانات بطاقة ائتمانية أو مافي حكمه

العقوبة : الحبس مدة لاتتجاوز سنة + غرامة (1- 3) ألف دينار

وتكون العقوبة الحبس لمدة لاتتجاوز (3) سنوات + غرامة (3-10) الف دينار أو احدهما إذا ترتب على ذلك الحصول على أموال الغير أو على ما تنتجة من خدمات

المادة 6

الجريمة: استخدام شبكة المعلومات أو وسيلة من وسائل تقنية المعلومات فى المساس بالذات الالهية أو القرآن الكريم...أو التعرض لشخص أمير البلاد أو تحقير وإزدراء دستور الدولة...

العقوبة: العقوبة المنصوص عليها في البنود (1، 2، 3) من المادة 27 من قانون المطبوعات والنشر

المادة 7

الجريمة: من ارتكب أحد الأفعال المنصوص عليها بالمادة (28) من قانون المطبوعات والنشر المشار إليه عن طريق الشبكة المعلوماتية أو باستخدام وسيلة من وسائل تقنية المعلومات

العقوبة : العقوبة المقررة بالمادة (29) فقرة أولى من القانون رقم (31) لسنة 1970 بتعديل بعض أحكام قانون الجزاء رقم (16) لسنة 1960

المادة 8

الجريمة: إنشاء موقع أو نشر معلومات بقصد الاتجار بالبشر أوتسهيل التعامل فيهم أو ترويج المخدرات أومافي حكمها أو تسهيل ذلك في غير الأحوال المصرح به

العقوبة : الحبس مدة لا تجاوز (7) سنوات + غرامة (10- 30) الف دينار أو إحدى هاتين العقوبتين

المادة 9

الجريمة: غسيل الأموال أو تحويل أموال غير مشروعة أو نقلها أو تمويه أو اخفاء مصدرها أو اكتسابها عن طريق الشبكة المعلوماتية أو باستخدام وسيلة من وسائل تقنية المعلومات

العقوبة : الحبس مدة لاتتجاوز (10) سنوات + غرامة (20 - 50) ألف دينار أو إحدى هاتين العقوبتين

المادة 10

الجريمة: إنشاء موقع لمنظمة إرهابية أو لشخص ارهابي أو نشر معلومات على الشبكة بأي وسيلة من تقنية المعلومات، لتسهيل الاتصالات بأحد قياداتها او اعضائها أو افكارها أو تمويلها أو نشر كيفية تصنيع الاجهزة الحارقة أو المتفجرة

العقوبة: الحبس مدة لاتجاوز (10) سنوات + غرامة (20 - 50) الف دينار أو إحدى هاتين العقوبتين.

اهم المراجع:

د. أحمد عوض بلال، علم الإجرام، النظرية العامة والتطبيقات، دار النهضة العربية، القاهرة، الطبعة الأولى، 1985.

د احمد خليفة الملط – الجرائم المعلوماتية – دار الفكر الجامعي – ط الثانية 2006-

د تركي بن عبدالرحمن المويشير – النموذج الامني لمكافحة الجرائم المعلوماتية وقياس فاعليته – ط 2009

د. جميل عبد الباقي الصغير، القانون الجنائي والتكنولوجيا الحديثة، الكتاب الأول،

الجرائم الناشئة عن استخدام الحاسب الآلي، دار النهضة العربية، القاهرة، الطبعة الأولى، 1992

د خالد ممدوح إبراهيم ، الجرائم المعلوماتية، الطبعة الأولى، دار الفكر الجامعي- الإسكندرية، 2009

د. عادل محمد أحمد السيوى، المسئولية الجنائية عن جريمة غسل الأموال فى التشريع المصرى، دراسة مقارنة، رسالة دكتوراه، كلية الحقوق- جامعة القاهرة، 2007

د. عبدالله حسين علي محمود، سرقة المعلومات المخزنة في الحاسب الآلي، دار النهضة العربية، القاهرة، 2002

د. عمر سالم، شرح قانون العقوبات المصري القسم العام، طبعة 2010، دار النهضة العربية، القاهرة

د عبدالفتاح حجازي – الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنت – القاهرة 2002 – دار الكتب القانونية

د. مصطفي محمد موسى – اساليب اجرامية للتقنية الرقمية – ماهيتها ومكافحتها – القاهرة 2003 دار النهضة العربية

د مصطفى سليمان ابكر – جرائم الحاسوب واساليب مواجهتها – مجلة الامن والحياة – العدد 210 السنة 19 – 1420 هـ الرياض

د. محمود كبيش، السياسة الجنائية فى مواجهة غسيل الأموال، دار النهضة العربية، القاهرة، 2001

د محمود محمد المرزوقي – جرائم الحاسب الالى – المجلة العربية للفقه والقضاء – العدد 28 – الامانة العامة لجامعة الدول العربية –

د. هلالي عبداللاه أحمد، التزام الشاهد بالإعلام في الجرائم المعلوماتية، دراسة مقارنة، دار النهضة العربية، القاهرة، 1997

د. هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة، أسيوط، 1992

د هدى حامد قشقوش، جرائم الحاسب الإلكتروني في التشريع المقارن، دار النهضة العربية، القاهرة، 1992

د. نائلة عادل فريد قورة، جرائم الحاسب الآلي الاقتصادية، دراسة نظرية وتطبيقية، منشورات الحلبي الحقوقية، بيروت، لبنان، 2005

الفهـرس

تم بحمد الله

معهد الكويت للدراسات القضائية والقانونية
KUWAIT INSTITUTE FOR JUDICIAL & LEGAL STUDIES

www.kijs.gov.kw.com Kijs_gov_kw kijs.kw kijs.kw kijs.gov.kw@gmail.com