الجريمة الإلكترونية

وحجية الدليل الرقمي في الإثبات الجنائي

HRDO
هردو

مركز هردو
لدعم التعبير الرقمي
HRDO CENTER
To Support the Digital Expression

الجريمة الالكترونية

وحجية الدليل الرقمي في الإثبات الجنائي

مركز هردو لدعم التعبير الرقمي
القاهرة ٢٠١٤

الناشر

مركز هردو

لدعم التعبير الرقمي

www.hrdoegypt.org
info@hrdoegypt.org

المتحويات

تمهيد

تعتبر الجريمة الالكترونية الآن هي أكبر تحدي يواجه رجال القانون والتشريع ليس في مصر فقط ولكن في العالم اجمع، نظرًا لان تلك الجريمة مرتبطة بالتطور التكنولوجي الهائل الذي تشهده علوم الكمبيوتر في الآونة الأخيرة كذلك المجرم المعلوماتي الذي يختلف عن المجرم الطبيعي من حيث قدرات الذكاء والإحتيال التي تتطلب قدرات موازية ومماثلة لدى القائمين على وضع القوانين والتشريعات الخاصة بمكافحة الجريمة الالكترونية ومعاقبة مرتكبيها.

ولما كانت الجريمة الالكترونية أصبحت واقعًا ملموسًا تواجهه مصر الآن، في ظل قصور تشريعي واضح في مواجهة تلك الجرائم، يُصدر مركز هردو لدعم التعبير الرقمي ذلك التقرير للتعرف على ماهية الجريمة الالكترونية، وتعريفها وخصائصها وأسبابها ووسائل مكافحتها وكيف تناولتها المواثيق الدولية والدستور والقانون المصري، كذلك نتعرف على سمات المجرم المعلوماتي ودوافعه لارتكاب الجريمة.

ويستعرض التقرير دراسة مقارنة حول كيفية التصدي للجريمة الالكترونية في بعض البلدان في أوروبا والولايات المتحدة والمنطقة العربية من حيث التشريعات التي وضعتها تلك البلدان وآلية تنفيذها بما يضمن ولا يخل بحق مواطنيها في تداول المعلومات وسرية مراسلتهم الالكترونية وحقهم في حرية التعبير عن رأيهم بشتى الوسائل.

وفي هذا الإطار يطرح التقرير تساؤلًا هامًا حول حجية الدليل الرقمي في الإثبات الجنائي سواء من حيث كونه دليل براءة أو دليل إدانة ومدى تكييف ذلك من الناحية القانونية.

وأخيرًا يتناول التقرير نظرة تحليلية حول حجية الدليل الرقمي أمام القضاء المصري، من حيث كونه دليل إثبات قائم بذاته وكيفية تعديل القوانين المصرية المنظمة لحرية الاتصالات والمعلومات وما يتوافق مع حقيقة وجود الدليل الرقمي واعتماده كدليل إثبات جنائي شأنه شأن كافة أدلة الإثبات المتعارف عليها من شهادة الشهود والقرائن والبينة والاعتراف ودليل الثبوت الكتابي وغيرها، كذلك يبدي التقرير بعض التوصيات التي رأيناها كفيلة لمواجهة الجريمة الالكترونية والحد من انتشارها.

الجريمة الالكترونية:[1]

التعريف الضيق للجريمة الالكترونية

ذهب الفقيه (merwe) إلى أن الجريمة الالكترونية هي فعل غير مشروع يتورط في ارتكابه الحاسب الآلي – أو هو الفعل الإجرامي الذي يُستخدم في اقترافه الحاسب الآلي كأداة رئيسية، فيما عرفها الفقية (ros blat) بأنها كل نشاط غير مشروع موجة لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب الآلي وإلى تحويل طريقه.

وعرفها كلاوس تايدومان بأنها كافة أشكال السلوك غير المشروع الذي يُرتكب باسم الحاسب الآلي.

ويرى البعض أن تعريف كلا من (marwe) و(ros blat) مقصورين على الإحاطة بأوجه الظاهرة الإجرامية أما تعريف كلاوس تايدومان فيؤخذ عليه أنه بالغ في العمومية والاتساع؛ لأنه يدخل فيه كل سلوك غير مشروع أو ضار بالمجتمع.

ويدخل في نطاق تعريفات مفهوم الجريمة المعلوماتية الضيقة، تعريف مكتب تقييم التقنية بالولايات المتحدة الأمريكية، حيث يعرف الجريمة المعلوماتية من خلال تحديد مفهوم جريمة الحاسب بأنها الجرائم التي تلعب فيها البيانات الكمبيوترية والبرامج المعلوماتية دورًا رئيسيًا.

[1] – المركز العربي لأبحاث الفضاء الالكتروني – دوريات– العدد١٩١١.

التعريفات الموسعة لمفهوم الجريمة الالكترونية

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

وذهب رأى أخر من الفقة إلى تعريف الجريمة الالكترونية بأنها عمل أو امتناع يأتيه الإنسان، إضرارًا بمكونات الحاسب وشبكات الاتصال الخاصة به التي يحميها قانون العقوبات ويفرض لها عقاب.

ويرى جانب من الفقه من أنصار هذا الاتجاه الموسع بأنها كل سلوك إجرامي يتم بمساعدة الكمبيوتر أو كل جريمة تتم في محيط أجهزة الكمبيوتر.

ويذهب البعض إلى أنه عند وضع تعريف محدد للجريمة الالكترونية يجب مراعاة عدة إعتبارات مهمة منها:-

١- أن يكون هذا التعريف مقبول ومفهوم على المستوى العالمي.
٢- أن يراعى هذا التعريف التطور السريع والمتلاحق في تكنولوجيا المعلومات.
٣- أن يحدد التعريف الدور الذي يقوم به جهاز الكمبيوتر في إتمام النشاط الإجرامي.
٤- أن يفرق هذا التعريف بين الجريمة العادية والجريمة المعلوماتية وذلك عن طريق إيضاح الخصائص المميزة للجريمة المعلوماتية.

- موقف بعض التشريعات والهيئات الدولية من تعريف الجريمة المعلوماتية:
أشارت الأمم المتحدة في المدونة الصادرة عنها بشأن الجريمة المعلوماتية، إلى الخلاف الواقع بين الخبراء حول ماهية العناصر المكونة لجرائم الكمبيوتر أو حتى المتعلقة بالكمبيوتر ولعل ذلك ما يفسر عدم التوصل إلى تعريف متفق علية دوليًا لهذه المصطلحات وإن كان هؤلاء قد اتفقوا ضمنا على وجود ظاهرة تتزايد بمعدلات عالمية لتلك الجرائم.

وإن كان مكتب تقييم التقنية في الولايات المتحدة الأمريكية، قد عرف الجريمة المعلوماتية بأنها الجرائم التي تلعب فيها البيانات الكمبيوترية والبرامج المعلوماتية دورًا رئيسيًا.

المفهوم القانوني للمعلومات

تعتبر المعلومات في الوقت الراهن سلعة تباع وتشترى ومصدر قوة اقتصادية وسياسية وعسكرية، وذلك لارتباطها بمختلف مجالات النشاط الإنساني وتداخلها في كافة جوانب الحياة العصرية، وبات الوعي بأهميتها مظهرا لتقدم الأمم والشعوب.

تعريف المعلومات

لم تعد المعلومات الآن مجرد نوع من الرفاهية والترف تتباهى به الشعوب أو المنظمات وإنما أصبحت ركيزة أساسية في تقدم وتطور المجتمع وتحقيق تقدمة ورفاهيته المنشودة، وفى سبيل ذلك وضع عدد غير قليل من التشريعات الوطنية المختلفة تعريفًا للمعلومة.

وقد عرف المشرع الأمريكي، المعلومات في قانون المعاملات التجارية الإلكتروني لعام ١٩٩٩ بالفقرة العاشرة من المادة الثانية بأنها تشمل (البيانات والكلمات والصور والأصوات والوسائل وبرامج الكمبيوتر والبرامج المضغوطة والموضوعة على الأقراص المرنة وقواعد البيانات أو ما شابة ذلك).

والتعريف السابق نجد انه قد وسع من مفهوم المعلومة، ووضع تقريبًا كل ما يتعلق بها بل أكثر من ذلك أنة تحسب ما قد يظهر من تتطور تكنولوجي جديد.

والمشرع الفرنسي ووفقًا للقانون رقم ٨٢-٦٥٢ الصادر في ٢٦ يوليو لسنة ١٩٨٢، تُعرّف المعلومة على أنها صور أو مستندات أو معطيات أو خطابات أيًا كانت طبيعتها.

أما قانون البحرين رقم ٨٣ لسنة ٢٠٠٢ بشأن المعاملات الإلكترونية فقد عرف المعلومات بأنها (البيانات والنصوص والصور والأصوات والرموز وبرامج الحاسوب والبرمجيات ويمكن أن تكون قواعد البيانات والكلام)

كما عرف قانون إمارة دبي بشأن المعاملات والتجارة الإلكترونية رقم ٢ لسنة ٢٠٠٢، المعلومات الإلكترونية بأنها(معلومات ذات خصائص إلكترونية في شكل نصوص أو رموز أو أصوات أو رسوم أو صور أو برامج حاسب إلى أو غيرها من قواعد البيانات).

هذه مجموعة من التشريعات التي وضعت تعريف واضح للمعلومة والمعلومات كان أغلبها كما رأينا يدور حول الأشكال المختلفة للمعلومات وصورها التي تظهر فيها سواء تعلق الأمر برموز أو صور أو بيانات الخ.

وقد ذهب البعض إلى ضرورة التفرقة بين المعلومات والبيانات، فالبيانات تعبر عن مجموعة من الأرقام والرموز والحقائق التي لا علاقة بين بعضها البعض أما المعلومات فهي المعنى الذي يستخلص من هذه البيانات.

أنواع المعلومات

تقسم المعلومات إلى ثلاث طوائف هي، المعلومات الاسمية والمعلومات المتعلقة بالمصنفات الفكرية والمعلومات المباحة.

أما الطائفة الأولي وهى المعلومات الاسمية، فتتقسم إلي مجموعتين هما:
١-المعلومات الموضوعية وهى تلك المعلومات المرتبطة بشخص المخاطب بها مثل اسمه وموطنه وحالته الاجتماعية وهى معلومات لا يجوز الإطلاع عليها إلا بموافقة الشخص نفسه،
٢- المعلومات الشخصية ويقصد بها تلك المعلومات المنسوبة لآخر مما يستدعى إدلاء الغير برأيه الشخصي فيها وهى مثل المقالات الصحفية والملفات الإدارية للعاملين لدى جهة معينة.

الطائفة الثانية: هى المعلومات الخاصة بالمصنفات الفكرية، فهذه المصنفات محمية بموجب قوانين الملكية الفكرية مثل الاختراعات والابتكارات المختلفة والتسجيلات الفنية والمؤلفات الأدبية.

والطائفة الثالثة: هى المعلومات المباحة، فيقصد بها أن تلك المعلومات مباح أن يحصل عليها الجميع، لأنها بدون مالك مثل تقارير البورصة والنشرات الجوية هذه المعلومات مباحة للكافة وغير محمية بأي من وسائل الحماية.

الشروط التي يجب توافرها في المعلومة محل الحماية

بصفة عامة هناك شروط يجب توافرها في المعلومة حتى تتمتع بالحماية القانونية وتتمثل هذه الشروط في الآتي:

أولًا: أن يتوافر في المعلومة التحديد والابتكار
المعلومة التي تفتقد لصفة التحديد لا يمكن أن تكون معلومة حقيقية فإذا كانت المعلومة هي تعبير وصياغة محددة تجعل رسالة ما قابلة للتبليغ عن طريق علامات أو إشارات معينة.
وهذا يتطلب أن تكون محدده تحديداً دقيقًا، خاصة في مجال الاعتداء على الأموال فهذه الاعتداءات تتطلب أن يكون هناك شيء محدد ومبتكر أما الشيء الشائع فلا يتمتع بأي حماية قانونية.

ثانيًا: أن يتوافر في المعلومة السرية والاستئثار.
السرية صفة لازمة للمعلومة محل الحماية القانونية، ولا يتصور في جرائم مثل جرائم السرقة والنصب وخيانة الأمانة إذا انعدم هذا الحصر وذلك لأن المعلومة العامة الشائعة تكون بمنأى عن أي حيازة، وتكتسب المعلومة وصفها إما بالنظر إلى طبيعتها أو بالنظر إلا إرادة الشخص أو إلى الأمرين معا مثل الرقم السري(password).

إذن حتى تتمتع المعلومة بالحماية القانونية، فلابد أن يتوافر فيها الشرطان السابقان، فإذا فقدتهما أصبحت معلومة غير محمية ولا يملكها أحد وغير قابلة لأن يستأثر بها أي شخص بل أصبحت عامة لكل من يريد استخدامها.

أسباب الجريمة الإلكترونية وخصائصها[2]

لاشك أن فئات مرتكبي الجريمة المعلوماتية تختلف عن مرتكبي الأفعال الإجرامية التقليدية، لذا من الطبيعي أن نجد نفس الاختلاف في الأسباب والعوامل التي تدفع في ارتكاب الفعل غير المشروع فضلًا عن ذلك، تتمتع جرائم الكمبيوتر والمعلوماتية بعدد من الخصائص التي تختلف تمامًا عن الخصائص التي تتمتع بها الجرائم التقليدية، كما أن الجاني الالكتروني (أو المجرم الالكتروني) يختلف أيضا عن المجرم العادي.

---

[2]- Dr. Linda volonino.cyber terrorism. Op. cit.

ويأتي في مقدمة أسباب الجريمة المعلوماتية، غاية التعلم والتي تتمثل في استخدام الكمبيوتر والإمكانيات المستحدثة لنظم المعلومات وهناك أمل الربح وروح الكسب التي كثيراً ما تدفع إلى التعدي على نظم المعلومات بالإضافة إلى الدوافع الشخصية والمؤثرات الخارجية التي قد تكون سبباً في ارتكاب الجريمة المعلوماتية.

- غاية التعلم[٣]

يشير الأستاذ ليفي مؤلف كتاب قراصنة الأنظمة HACKERS إلى أخلاقيات هؤلاء القراصنة والتي ترتكز على مبدأين أساسيين:

١- أن الدخول إلى أنظمة الكمبيوتر يمكن أن يعلمك كيف يسير العالم.

٢- أن جمع المعلومات يجب أن تكون غير خاضعة للقيود.

وبناء على هذين المبدأين فإن أجهزة الكمبيوتر المعنية ما هي إلا آلات للبحث، والمعلومات بدورها ما هي إلا برامج وأنظمة معلومات.

ومن وجهة نظر هؤلاء القراصنة فإن جميع المعلومات المفيدة بوجه عام يجب أن تكون غير خاضعة للقيود وبعبارة أخرى أن تتاح حرية نسخها وجعلها تتناسب مع استخدامات الأشخاص.

ويرى هؤلاء القراصنة إغلاق بعض نظم المعلومات وعدم السماح بالوصول إلى بعض المعلومات وخاصة بعض المعلومات السرية التي تخص الأفراد.

ويعلق قراصنة الأنظمة أنهم يرغبون في الوصول إلى مصادر المعلومات والحاسبات الإلكترونية والشبكات بغرض التعلم.

وقد لاحظ كل من "ليفي" و "لاندريس" أن قراصنة الأنظمة لديهم الاهتمام الشديد بأجهزة الكمبيوتر وبالتعلم ويدخل العديد منهم في أجهزة الكمبيوتر على أنهم محترفين ويختار بعض القراصنة الأنظمة لتعلم المزيد عن كيفية عمل الأنظمة.

---

[3] - قراصنة أنظمة الكمبيوتر إعداد: دورثي إي. دينغ ورقة مقدمة للمؤتمر القومي الثالث عشر لأمن الكمبيوتر، واشنطن، ترجمة: آمنة علي يوسف، ديسمبر ١٩٩٨، ص ٨.

ويقول "لاندريس" أن هؤلاء القراصنة يرغبون في البقاء مجهولين حتى يتمكنوا من الاستمرار في التواجد داخل الأنظمة لأطول وقت ممكن، ويكرّس البعض منهم كل وقته في تعلم كيفية اختراق المواقع الممنوعة والتقنيات الأمنية للأنظمة حيث تتفاوت معرفتهم عن الأنظمة والبرمجة إلى حد بعيد.

وكتب أحد قراصنة الأنظمة يقول: يكتشف قراصنة الأنظمة نقطة ضعف أمنية فيحاولون استغلالها لأنها موجودة بهدف عدم تخريب المعلومات أو سرقتها، أعتقد أن ما نقوم به يشبه قيام شخص باستكشاف أساليب جديدة للحصول على المعلومات من المكتبة فيصبح في غاية الإثارة والانهماك.
وينبغي ألا نستهين بكفاءة الشبكات التي يتعلم من خلالها القراصنة حرفتهم.

وهم يقومون بالفعل بالبحث واكتشاف الأنظمة، والعمل من خلال الجماعة وتعليم بعضهم البعض، حيث ذكر الكتاب أن قراصنة الأنظمة أنه ينتمي إلى مجموعة بحث مهمتها استخراج كميات كبيرة من المعلومات وتعلم أكبر قدر منها.

ويسعى أعضاء القرصنة إلى التخصص والتعاون في المشاريع البحثية وتقاسم البرامج والأخبار وكتابة المقالات وتعريف الآخرين بمجالات اختصاصهم ويدع قراصنة الأنظمة نظامًا خاصًا لمجال المعرفة الذي يجذبهم ويعلهم التفكير ويسمح لهم بتطبيق ما تعلموه في أنشطة هادفة وإن لم تكن قانونية دائمة.

- السعي إلى الربح

أشارت إحدى المجلات المتخصصة في الأمن المعلوماتي securite informatique إلى الرغبة في تحقيق الثراء من بين العوامل الأساسية لارتكاب الجريمة المعلوماتية حيث أشارت:

- أن ٤٣% من حالات الغش المعلن عنها في كتيبات من أجل اختلاس الأموال.
- ٢٣% من أجل سرقة المعلومات.
- ١٩% أفعال إتلاف.
- ١٥ % سرقة وقت الآلة؛ أي الاستعمال غير المشروع للحاسب الآلي لأجل تحقيق أغراض شخصية.

لذا نجد أن الدافع لارتكاب الجريمة المعلوماتية يمكن أن تكون سببه مجرد سداد الديون المستحقة أو مشاكل عائلية راجعة للنقود أو إدمان ألعاب القمار أو المخدرات لذا فإن بيع المعلومات المختلسة هو نشاط متسع للغاية ويمكن أن نبين في هذا المجال واقعة استيلاء مبرمج يعمل لدى إحدى الشركات الألمانية على ٢٢ شريطًا ممغنطًا تحتوي على معلومات هامة بخصوص عملاء وإنتاج هذه الشركة حيث هدد السارق ببيعها للشركات المنافسة ما لم تدفع له فدية مقدارها ٢٠٠,٠٠٠ دولار.

وبعد أن قامت الشركة بتحليل الموقف وقدرت الخسائر التي يمكن أن تنشأ عن إفشاء محتواها تفوق بكثيرالمبلغ المطلوب فقد فضلت دفع المبلغ من أجل استرداد الشرائط المسروقة.

كذلك أيضاً دفعت الرغبة بمستخدم يعمل بشركة التأمين كي يحتفظ بوظيفته التي سبق وأن فصل منها إلى احتجاز الذاكرة المركزية الخاصة بالشركة كرهينة لديه، حيث هدد المختلس رئيسه في العمل بأنه إذا حاول أن يلغي بطاقة أجرته من ذاكرة الحاسب الآلي فإن هذه الأخيرة سوف تدمر تلقائيًا عن طريق ما يعرف بالقنابل المنطقية.

- الإثارة والمتعة والتحدي[٤]

يدرك القراصنة شيئاً عن أساسيات الكمبيوتر وأن هذا الأمر يمكن أن يكون ممتعاً، حيث جاء على لسان أحد القراصنة ما يأتي "كانت القرصنة هي النداء الأخير الذي يبعثه دماغي فقد كنت أعود إلى البيت بعد يوم ممل آخر في المدرسة، وأدير تشغيل جهاز الكمبيوتر، وأصبح عضوًا في نخبة قراصنة الأنظمة، كان الأمر مختلفاً برمته حيث لا وجود لعطف الكبار، وحيث الحكم هو موهبتك فقط، في البدء كنت أسجل أسمي في لوحة النشرات Bulletin Borard الخاصة حيث يقوم الأشخاص الآخرين الذين يفعلون مثلي بالتردد على هذا الموقع، ثم أتصفح أخبار المجتمع وأتبادل المعلومات مع الآخرين في جميع أنحاء البلاد.

وبعد ذلك أبدأ عملية القرصنة الفعلية، وخلال ساعة واحدة يبدأ عقلي بقطع مليون ميل في الساعة وأنسى جسدي تماماً بينما أتنقل من جهاز كمبيوتر إلى

[4] - حول قراصنة أنظمة الكمبيوتر، راجع: دروثي إي. دينغ، ورقة مقدمة للمؤتمر القومي الثالث عشر لأمن الكمبيوتر، مرجع سابق، ص ١١.

آخر محاولًا العثور على سبيل للوصول إلى هدفي، لقد كان الأمر يشبه سرعة العمل في متاهة إلى جانب الاكتشاف الكبير لأعداد ضخمة من المعلومات.

وكان يرافق تزايد سرعة الأدرينالين الإثارة المحظورة بفعل شيء غير قانوني، وكل خطوة أخطوها كان يمكن أن تسقطني بيد السلطات، كنت على حافة التكنولوجيا واكتشاف ما وراءها، واكتشاف الكهوف الإلكترونية التي لم يكن من المفترض وجودي بها".

وذكرت Jutian Dibbell بأنها تعتقد بأن المتعة تكمن في المخاطر التي ترتبط بعملية القرصنة وذكرت قائلة "أن التكنولوجيا تستلم من الدراما المليئة بالمغامرات وأن قراصنة الأنظمة يعيشون في عالم لا يعتبرون فيه العمل السري سوى لعبة يلهو بها الأطفال.

– الدوافع الشخصية

إن الدافع لارتكاب جرائم الكمبيوتر يغلب عليه الرغبة في قهر النظام أكثر من شهوة الحصول على الربح، ويميل مرتكبوا جرائم نظم المعلومات إلى إظهار تفوقهم ومستوي ارتقاء براعتهم لدرجة أنه إزاء ظهور أي تقنية مستحدثة فإن مرتكبوا هذه الجرائم لديهم شغف الآلة يحاولون إيجاد – وغالباً ما يجدون – الوسيلة إلى تحطيمها بل والتفوق عليها.

ويتزايد شيوع هذا الدافع لدى فئات صغار السن الذين يمضون وقتاً طويلًا أمام حواسبهم الشخصية في محاولة لكسر حواجز الأمن لأنظمة الكمبيوتر وشبكات المعلومات وإظهار تفوقهم على وسائل التكنولوجيا، الأمر الذي دفع بالعديد من الفقهاء إلى المناداة بعدم مساءلة مرتكبي جرائم الحاسب الآلي الذي يتمثل باعثهم في إظهار تفوقهم، واعتبار أعمالهم غير منطوية على نوايا آثمة.

وقد أمكن الكشف في بعض الأحوال عن أن مجرد إظهار شعور جنون العظمة هو الدافع لارتكاب فعل الجريمة المعلوماتية، وفي هذا الشأن نجد المحلل أو المبرمج المعلوماتي هو مفتاح سر كل نظام قد ينتابه إحساس بالإهمال أو النقص داخل المنشأة التي يعمل بها، وقد يندفع تحت تأثير الرغبة القوية من أجل تأكيد قدراته الفنية لإدارة المنشأة إلى ارتكاب الجريمة المعلوماتية، ومن ثم يجد ترضية من خلال الإفصاح عن شخصيه أمام العامة.

– جريمة سرقة المعلومات[5]

تتميز جرائم الحاسب بالصعوبات البالغة في اكتشافها والعجز في حالات كثيرة عن أمكان إثباتها في حالة اكتشافها.

وذلك الأسباب التالية:

أولًا: لا تخلف جرائم الحاسب آثارًا ظاهرة خارجيًا، فهي تنصب على البيانات والمعلومات المختزنة في نظم المعلومات والبرامج مما ينفي وجود أي أثر مادي يمكن الاستعانة به في إثباتها، فالجرائم المعلوماتية ينتفي فيها العنف وسفك الدماء ولا توجد فيها آثار لاقتحام سرقة الأموال، وإنما هي أرقام ودلالات تتغير أو تُمحي من السجلات ومما يزيد من هذه الصعوبة ارتكابها في الخفاء، وعدم وجود أثر كتابي مما يجري من خلال تنفيذها من عمليات حيث يتم نقل المعلومات بواسطة النبضات الإلكترونية.

ثانيًا: يتم ارتكاب جريمة الحاسب عادة عن بعد فلا يتواجد الفاعل في مسرح الجريمة حيث تتباعد المسافات بين الفاعل والنتيجة، وهذه المسافات لا تقف عند حدود الدولة بل تمتد إلى النطاق الإقليمي لدول أخرى مما يضاعف صعوبة كشفها أو ملاحقتها.

ثالثًا: تبدو أكثر المشاكل جسامة في صعوبة اكتشاف وإثبات جرائم الحاسب بل وفي دراسة هذه الظاهرة في مجملها هي مشكلة امتناع المجني عليهم عن التبليغ عن الجرائم المرتكبة ضد نظام الحاسب وهو ما يعرف بالرقم الأسود Chiffrenoir[6] حيث لا يعلم ضحايا هذه الجرائم شيئاً عنها إلا عندما تكون أنظمتهم المعلوماتية هدفاً لفعل الغش أو حتى عندما يعلمون فهم يفضلون عدم إفشاء الفعل.

[5] – يونس خالد عرب مصطفي، جرائم الحاسوب، دراسة مقارنة، رسالة ماجستير مقدمة إلى الجامعة الأردنية ١٩٩٤، ص ٧٢.

[6]– Dr. Francillon, Les crimes inormatiques et d'autres crimes dans le domaine de la technologie informatique en france Rev. int. pén, 1990, vol 64, p. 293

خصائص الجرائم المتصلة بالكمبيوتر والمعلوماتية:

تتميز الجرائم المرتكبة بواسطة الكمبيوتر كأداة أو كهدف للجريمة بالخصائص التالية:

١. سرعة التنفيذ: لا يتطلب تنفيذ الجريمة عبر الهاتف الوقت الكبير، وبضغطة واحدة على لوحة المفاتيح يمكن أن تنتقل ملايين الدولارات من مكان إلى آخر. وهذا لا يعني إنها لا تتطلب الإعداد قبل التنفيذ أو استخدام معدات وبرامج معينة.

٢. التنفيذ عن بعد: لا تتطلب جرائم الكمبيوتر في أغلبها (إلا جرائم سرقة معدات الكمبيوتر) وجود الفاعل في مكان الجريمة.بل يمكن للفاعل تنفيذ جريمته وهو في دولة بعيدة كل البعد عن الفاعل سواء كان من خلال الدخول للشبكة المعنية أو اعترض عملية تحويل مالية أو سرقة معلومات هامة أو تخريب...الخ.

٣. إخفاء الجريمة:أن الجرائم التي تقع على الكمبيوتر أو بواسطته كجرائم (الإنترنت) جرائم مخفية، إلا انه يمكن أن تلاحظ آثارها، والتخمين بوقوعها.

٤. الجاذبية: نظرًا لما يمثله سوق الكمبيوتر والإنترنت من ثروة كبيرة للمجرمين أو الأجرام المنظم، فقد غدت أكثر جذبًا لاستثمار الأموال وغسلها وتوظيف الكثير منها في تطوير تقنيات وأساليب تمكن الدخول إلى الشبكات وسرقة المعلومات وبيعها أو سرقة البنوك أو اعتراض العمليات المالية وتحويل مسارها أو استخدام أرقام البطاقات...الخ.

٥. عابرة للدول:إن ربط العالم بشبكة من الاتصالات من خلال الأقمار الصناعية والفضائيات والإنترنت جعل الانتشار الثقافي وعولمة الثقافة والجريمة أمرًا ممكنًا وشائعًا، لا يعترف بالحدود الإقليمية للدول، ولا بالمكان، ولا بالزمان، وأصبحت ساحتها العالم أجمع.

ففي مجتمع المعلومات تذوب الحدود الجغرافية بين الدول، لارتباط العالم بشبكة واحدة، حيث أن أغلب الجرائم المرتكبة عبر شبكة الإنترنت، يكون الجاني فيها في دولة ما والمجني عليه في دولة أخرى، وقد يكون الضرر المترتب عن الجريمة ليس واقعًا على المجني عليه داخل إقليم دولة الجاني، وتعارض المواد المعروضة مع الثقافات المتلقية لها خاصة إذا كانت تتعارض في الدين والعرف والاجتماعي والنظام الأخلاقي والسياسي للدولة.

٦. جرائم ناعمة: تتطلب الجريمة التقليدية استخدام الأدوات والعنف أحيانا كما في جرائم الإرهاب والمخدرات، والسرقة والسطو المسلح.إلا أن الجرائم المتصلة بالكمبيوتر تمتاز بأنها جرائم ناعمة لا تتطلب عنفا،فنقل بيانات من كمبيوتر إلى أخر أو السطو الإلكتروني على أرصدة بنك ما لا يتطلب أي عنف أو تبادل إطلاق نار مع رجال الأمن.

٧. صعوبة إثباتها:تتميز جرائم الإنترنت عن الجرائم التقليدية بأنها صعبة الإثبات، وهذا راجع إلى افتقاد وجود الآثار التقليدية للجريمة، وغياب الدليل الفيزيقي(بصمات، تخريب، شواهد مادية) وسهولة محو الدليل أو تدميره في زمن متناه القصر، يضاف إلى ذلك نقص خبرة الشرطة والنظام العدلي، وعدم كفاية القوانين القائمة.

٨. التلوث الثقافي: لا يتوقف تأثير الجرائم المتصلة بالكمبيوتر عند الأثر المادي الناجم عنها وإنما يتعدى ذلك ليهدد نظام القيم والنظام الأخلاقي خاصة في المجتمعات المحافظة والمغلقة.

٩. عالمية الجريمة والنظام العدلي: نظرا لارتباط المجتمع الدولي إلكترونيا، فقد أصبح مجتمعنا تخيليا مما أدى إلى أن تكون ساحة المجتمع الدولي بكافة دوله ومجتمعاته مكانا لارتكاب الجريمة من كل مكان، مما أن تطلب أن تمارس الدول المتطورة وخاصة الصناعية على الدول النامية من أجل سن تشريعات جديدة لمكافحة الجرائم المتصلة بالكمبيوتر مما استدعى أن تكون القوانين ذات صبغة عالمية.

١٠. لا يتم – في الغالب الأعم – الإبلاغ عن جرائم الانترنت إما لعدم اكتشاف الضحية لها وإما خشيته من التشهير. لذا نجد أن معظم جرائم الانترنت تم اكتشافها بالمصادفة؛ بل وبعد وقت طويل من ارتكابها، زد على ذلك أن الجرائم التي لم تكتشف هي أكثر بكثير من تلك التي كشف الستار عنها. فالرقم المظلم بين حقيقة عدد هذه الجرائم المرتكبة؛ والعدد الذي تم اكتشافه؛ هو رقم خطير. فالفجوة بين عدد هذه الجرائم الحقيقي؛ وما تم اكتشافه: فجوة كبيرة.

١١. من الناحية النظرية يسهل ارتكاب الجريمة ذات الطابع التقني؛ كما أنه من السهل إخفاء معالم الجريمة وصعوبة تتبع مرتكبيها.

١٢. لذا فهذه الجرائم لا تترك أثرًا لها بعد ارتكابها؛ علاوة على صعوبة الاحتفاظ الفني بآثارها إن وجدت. فهذه الجرائم لا تترك أثرا، فليست هناك أموال أو مجوهرات مفقودة، وإنما هي أرقام تتغير في السجلات، ولذا فإن معظم جرائم الانترنت تم اكتشافها بالمصادفة وبعد وقت طويل من ارتكابها.

١٣. تعتمد هذه الجرائم على قمة الذكاء في ارتكابها؛ ويصعب على المحقق التقليدي التعامل مع هذه الجرائم. إذ يصعب عليه متابعة جرائم الانترنت والكشف عنها وإقامة الدليل عليها. فهي جرائم تتسم بالغموض؛ وإثباتها بالصعوبة بمكان والتحقيق فيها يختلف عن التحقيق في الجرائم التقليدية.

١٤. الوصول للحقيقة بشأنها تستوجب الاستعانة بخبرة فنية عالية المستوى.

١٥. عولمة هذه الجرائم يؤدي إلى تشتيت جهود التحري والتنسيق الدولي لتعقب مثل هذه الجرائم؛ فهذه الجرائم هي صورة صادقة من صور العولمة؛ فمن حيث المكان يمكن ارتكاب هذه الجرائم عن بعد وقد يتعدد هذا المكان بين أكثر من دولة؛ ومن الناحية الزمنية تختلف المواقيت بين الدول؛ الأمر الذي يثير التساؤل حول : تحديد القانون الواجب التطبيق على هذه الجريمة.

١٦. صعوبة المطالبة بالتعويض المدني بخصوص جرائم الانترنت.

المجرم المعلوماتى

لم يكن لارتباط الجريمة المعلوماتية بالحاسب الآلي أثره على تمييز الجريمة المعلوماتية عن غيرها من الجرائم التقليدية فحسب، وإنما كان له أثره في تمييز المجرم المعلوماتى عن غيره من المجرمين العاديين الذين جنحوا إلى السلوك الإجرامي النمطي. وهذا ماسوف نعرض له موضحين أهم سمات المجرم المعلوماتى ثم خصائصه المميزة وأخيرا لأنماط هذا المجرم وذلك على النحو التالي.

سمات المجرم المعلوماتي

يمكن أن نستخلص مجموعة من السمات التي يتميز بها المجرم المعلوماتى، والتي يساعد التعرف عليها مواجهة هذا النمط الجديد من المجرمين، ويعد الأستاذ (parker) واحد من أهم الباحثين الذين عنوا بالجريمة المعلوماتية بصفة عامه والمجرم المعلوماتى بصفة خاصة، ويرى (parker) أن المجرم المعلوماتى وإن كان يتميز ببعض السمات الخاصة إلا انه في النهاية لا يخرج عن كونه مرتكبا لفعل إجرامي يتطلب توقيع العقاب علية.

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

أولا: المجرم المعلوماتى، مجرم متخصص

تبين في عديد من القضايا أن عدداً من المجرمين لا يرتكبون سوى جرائم الكمبيوتر أي أنهم يتخصصون في هذا النوع من الجرائم، دون أن يكون لهم أي صلة بأي نوع من الجرائم التقليدية الأخرى، مما يعكس أن المجرم الذي يرتكب إلا جرام المعلوماتى هو مجرم في الغالب متخصص في هذا النوع من الإجرام.

ثانيا: المجرم المعلوماتى، مجرم عائد إلى الإجرام

يعود كثير من مجرمي المعلومات إلى ارتكاب جرائم أخرى في مجال الكمبيوتر انطلاقًا من الرغبة في سد الثغرات التي أدت إلى التعرف عليهم وأدت إلى تقديمهم إلى المحاكمة في المرة السابقة، ويؤدى ذلك إلى العودة إلى الإجرام، وقد ينتهي بهم الأمر كذلك في المرة التالية إلى تقديمهم إلى المحاكمة.

ثالثا: المجرم المعلوماتى، مجرم محترف

يتمتع المجرم المعلوماتى بإحترافية كبيرة في تنفيذ جرائمه، حيث أنه يرتكب هذه الجرائم عن طريق الكمبيوتر الأمر يقتضى الكثير من الدقة والتخصص والاحترافية في هذا المجال للتوصل إلى التغلب على العقبات التي أوجدها المتخصصون لحماية أنظمة الكمبيوتر كما في حالة البنوك والمؤسسات العسكرية.

رابعا: المجرم المعلوماتى، مجرم غير عنيف

المجرم المعلوماتى من المجرمين الذين لا يلجئون إلى العنف بتاتا في تنفيذ جرائمهم وذلك لأنه ينتمي إلى إجرام – الحيلة – فهو لا يلجا إلى العنف في ارتكاب جرائمة، وهذا النوع من الجرائم لا يستلزم أي قدرا من العناء للقيام به.

فضلا عما تقدم ، فالمجرم المعلوماتى مجرم ذكى، ويتمتع بالتكيف الاجتماعي، أي لا يناصب أحد العداء وأيضا يتمتع بالمهارة والمعرفة وأحيانا كثيرة على درجة عالية من الثقافة.

خصائص المجرم المعلوماتى

يتميز المجرم المعلوماتى كذلك بمجموعة من الخصائص التي تميزه بصفة عامة عن غيرة من المجرمين، وهى:

أولا: المهارة

يتطلب تنفيذ الجريمة المعلوماتية قدرًا من المهارة يتمتع بها الفاعل، والتي قد يكتسبها عن طريق الدراسة المتخصصة في هذا المجال، أو عن طريق الخبرة المكتسبة في مجال التكنولوجي، أو بمجرد التفاعل الاجتماعي مع الآخرين، وهذه ليست قاعدة في أن يكون المجرم المعلوماتى على هذا القدر من العلم ، وهذا ما أثبته الواقع العملي أن جانب من انجح مجرمي المعلوماتية، لم يتلقوا المهارة اللازمة لارتكاب هذا النوع من الإجرام.

ثانيا: المعرفة

تميز المعرفة مجرمي المعلوماتية، حيث يستطيع المجرم المعلوماتى أن يكون تصور كامل لجريمته، ويرجع ذلك إلى أن المسرح الذي تمارس فيه الجريمة المعلوماتية هو نظام الحاسب الأولى، فالفاعل يستطيع أن يطبق جريمته على أنظمة مماثلة وذلك قبل تنفيذ الجريمة

ثالثا: الوسيلة

ويراد بها الإمكانيات التي يحتاجها المجرم المعلوماتى لإتمام جريمته.
وهذه الوسائل قد تكون في غالب الأحيان، وسائل بسيطة وسهلة الحصول عليها خصوصا إذا كان النظام الذي يعمل به الكمبيوتر من الأنظمة الشائعة أما إذا كان النظام من الأنظمة غير المألوفة، فتكون هذه الوسائل معقدة وعلى قدر من الصعوبة.

رابعا: السلطة

يقصد بالسلطة، الحقوق والمزايا التي يتمتع بها المجرم المعلوماتى والتي تمكنه من ارتكاب جريمته، فكثير من مجرمي المعلوماتية لديهم سلطة مباشرة أو غير مباشرة في مواجهة المعلومات محل الجريمة.

وقد تتمثل هذه السلطة في الشفرة الخاصة بالدخول إلى النظام الذي يحتوى على المعلومات وأيضًا قد تكون السلطة عبارة عن حق الجاني في الدخول إلى الحاسب الآلي وإجراء المعاملات، كما أن السلطة قد تكون شرعية من الممكن أن تكون غير شرعية كما في حالة سرقة شفرة الدخول الخاصة بشخص آخر.

خامسا: الباعث
وهو الرغبة في تحقيق الربح المادي بطريقة غير مشروعة ويظل هو الباعث الأول وراء ارتكاب الجريمة المعلوماتية، ويرى البعض أيضًا ما يخالف ذلك في أن الربح المادي لا يعد هو الباعث في أغلب الأحيان على ارتكاب جرائم المعلوماتية وإنما هناك أمور عديدة أخرى.

في الغالب تكون هي الباعث مثل الانتقام من رب العمل، وأيضا مجرد الرغبة في قهر نظام الحاسب واختراق حاجزه الأمني.

الأنماط المختلفة للمجرم المعلوماتى

يتم تقسيم مجرمي المعلوماتية (criminals cyber) إلى مجموعة من الطوائف المختلفة، حيث أسفرت الدراسات المختلفة في هذا المجال إلى وجود عدد من الأنماط المختلفة لمجرمي المعلومات، نرصدها فيما يلي:

الطائفة الأولي (pranksters):
وهم الأشخاص الذين يرتكبون جرائم المعلوماتية بغرض التسلية والمزاح مع الآخرين دون أن يكون في نيتهم إحداث أي ضرر بالمجني عليهم. ومن أمثلة هذة الطائفة صغار مجرمي المعلوماتية.

الطائفة الثانية (hackers):
وتضم الأشخاص الذين يستهدفوا من الدخول إلى أنظمة الحاسبات الآلية الغير مصرح لهم بالدخول إليها كسر الحواجز الأمنية الموضوعة لهذا الغرض وذلك بهدف اكتساب الخبرة وبدافع الفضول، أو لمجرد إثبات القدرة على اختراق هذه الأنظمة.

الطائفة الثالثة (malicious hackers):
وهم أشخاص هدفهم إلحاق خسائر بالمجني عليهم، دون أن يكون الحصول على مكاسب مالية ضمن هذه الأهداف، ويندرج تحت هذه الطائفة الكثير من مخترعي فيروسات الحاسبات الآلية وموزعيها.

الطائفة الرابعة (personal problem solvers):
وهم الطائفة الأكثر شيوعا من مجرمي المعلوماتية فهم يقومون بارتكاب جرائم المعلوماتية بحيث يترتب عليها في كثير من الأحيان خسائر كبيرة تلحق بالمجني عليه، ويكون الباعث في هذه الجريمة إيجاد حلول لمشاكل مادية تواجة الجاني لا يستطيع حلها بالطرق العادية.

الطائفة الخامسة (career criminals):

وهم مجرمي المعلوماتية الذين يهدفون من وراء نشاطهم الاجرامى تحقيق ربح مادي بطريق غير مشروع، ويقترب المجرم المعلوماتى من هذه الطائفة في سماته إلى المجرم التقليدي.

ومن جانب آخر، أكدت بعض الدراسات والأبحاث العلمية على أن فئات المجرمين (أو الجناة) تنحدر من:

١- مستخدمو الحاسب بالمنازل.

٢- الموظفون الساخطون على منظماتهم.

٣- المتسللون ومنهم الهواة أو العابثون بقصد التسلية.

٤- المحترفون الذين يتسللون إلى مواقع مختارة بعناية ويعبثون أو يتلفون النظام أو يسرقون محتوياته وتقع أغلب جرائم الانترنت حاليا تحت هذه الفئة بتقسيمها.

٥- العاملون في الجريمة المنظمة.

ويتمتع هؤلاء الجناة بصفات أخرى غير متوفرة فى الجناة العاديين نذكر منها:

١- أعمارهم تتراوح عادة بين ١٨ إلى ٤٦ سنة والمتوسط العمري لهم ٢٥ عاما.

٢- المعرفة والقدرة الفنية الهائلة.

٣- الحرص الشديد وخشية الضبط وافتضاح الأمر.

٤- ارتفاع مستوى الذكاء ومحاولة التخفي.

ومن الجدير بالذكر في هذا الصدد أن هناك اتفاق بين الخبراء والمتخصصين على أن جرائم الانترنت تمثل تحديا جديدا في عالم الجريمة، وذلك للأسباب التالية:

- صعوبة التعرف على هوية الجاني، فهو لا يترك أثرا لجريمته، وان وجد فقد لا تدل عليه.

- وجود بعض العقبات في محاكمة الجاني حال اكتشاف هويته إذا كان من بلد لا يعتبر ما قام به جرما.

- اتساع شريحة الجناة لتشمل صغار مستخدمي الانترنت، بسبب توفر الوسائل والبرامج المستخدمة في التخريب لصغار مستخدمي الانترنت، مما يجعل جرائم الانترنت لا تتطلب خبرة عالية.

- نقص الوعي بسلبية الاستخدام السيئ للانترنت، مما يجعل البعض ينظر للأعمال التخريبية على الانترنت – كاختراق المواقع – عمل بطولى.

حجية الدليل الرقمي في الإثبات الجنائي:

تعريف الدليل الرقمي:[٧]

هو الدليل المأخوذ من أجهزة الكمبيوتر وهو يكون في شكل مجالات أو نبضات مغناطيسية أو كهربائية ممكن تجميعها وتحليلها باستخدام برامج تطبيقات وتكنولوجيا وهى مكون رقمي لتقديم معلومات في أشكال متنوعة مثل النصوص المكتوبة أو الصور أو الأصوات أو الأشكال والرسوم وذلك من أجل اعتماده أمام أجهزة أنفاذ و تطبيق القانون.

مجموعة المجالات أو النبضات المغناطيسية أو الكهربائية التي يمكن تجميعها وتحليلها باستخدام برامج وتطبيقات خاصة لتظهر في شكل صور أو تسجيلات صوتية أو مرئية.

خصائص الدليل الرقمي[٩٨]:

١-يعتبر الدليل الرقمي دليلاً غير ملموس أي هو ليس دليلاً مادياً، فهو- أي الدليل الرقمي – تلك المجالات المغناطيسية أو الكهربائية، ومن ثم فإن ترجمة الدليل الرقمي وإخراجه في شكل مادي ملموس لا يعني أن هذا التجمع يعتبر هو الدليل، بل أن هذه العملية لا تعدو كونها عمليه نقل لتلك المجالات من طبيعتها الرقمية إلى الهيأة التي يمكن الاستدلال بها على معلومة معينة.
٢-يعتبر الدليل الرقمي من قبيل الأدلة الفنية أو العلمية، وهو من طائفة ما يعرف بالأدلة المستمدة في الآلة.
٣- إن فهم مضمون الدليل الرقمي يعتمد على استخدام أجهزة خاصة بتجميع وتحليل محتواه، و لذلك فكل ما لا يمكن تحديد وتحليل محتواه بواسطة تلك الأجهزة لا يمكن اعتباره دليلاً رقمياً، وذلك لعدم إمكانية الاستدلال به على معلومة معينة، ما يعدم قيمته التدليلية في إثبات الجريمة ونسبها إلى الجاني.

---

[7] – د.خالد ممدوح إبراهيم،الدليل الالكتروني في جرائم المعلوماتية ص ٢.

[9] – د. علي محمود علي حمودة، الأدلة المتحصلة من الوسائل الالكترونية في أطار نظرية الإثبات الجنائي، مقدم ضمن أعمال المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الالكترونية ونظمته أكاديمية شرطة دبي، في الفترة من ٢٦-٤ إلى ٤٨-٤-٢٠٠٣- دبي ص ٢٢-f www. law.comتاريخ الزيارة ٢٠٠٩/٨/٢٠

مميزات الدليل الرقمي:[10]

١. يتميز الدليل الرقمي بصعوبة محوه أو تحطيمه، حتى في حالة محاولة إصدار أمر بإزالة ذلك الدليل فمن الممكن إعادة إظهاره من خلال ذاكرة الآلة التي تحتوى ذلك الدليل.
٢ . إن محاولة الجاني محو الدليل الرقمي بذاتها تسجل عليه كدليل، حيث إن قيامه بذلك يتم تسجيله في ذاكرة الآلة وهو ما يمكن استخراجه واستخدامه كدليل ضده.
٣. إن الطبيعة الفنية للدليل الرقمي تمكّن من إخضاعه لبعض البرامج والتطبيقات للتعرف على ما إذا كان قد تعرض للعبث والتحريف كما سنرى لاحقا.

أنواع الدليل الرقمي:[11]

أ . أدلة أعدت لتكون وسيلة إثبات:
وهذا النوع من الأدلة الرقمية يمكن إجماله فيما يلي:
١ .السجلات التي تم إنشاؤها بواسطة الآلة تلقائياً، وتعتبر هذه السجلات من مخرجات الآلة التي لم يساهم الإنسان في إنشائها مثل سجلات الهاتف وفواتير أجهزة الحاسب الآلي.
٢ .السجلات التي جزء منها تم حفظه بالإدخال وجزء تم إنشاؤه بواسطة الآلة ومن أمثلة ذلك البيانات التي يتم إدخالها إلى الآلة و تتمّ معالجتها من خلال برنامج خاص، كإجراء العمليات الحسابية على تلك البيانات.

ب . أدلة لم تعد لتكون وسيلة إثبات:
وهذا النوع من الأدلة الرقمية نشأ دون إرادة الشخص، أي أنها أثر يتركه الجاني دون أن يكون راغباً في وجوده، ويسمى هذا النوع من الأدلة بالبصمة الرقمية، وهى ما يمكن تسميه أيضاً بالآثار المعلوماتية الرقمية، وهى تتجسد في الآثار التي يتركها مستخدم الشبكة المعلوماتية بسبب تسجيل الرسائل المرسلة منه أو التي يستقبلها وكافه الاتصالات التي تمت من خلال الآلة أو شبكة المعلومات العالمية.

والواقع أن هذا النوع من الأدلة لم يُعد أساسا للحفظ من قبل من صدر عنه، غير أن الوسائل الفنية الخاصة تمكن من ضبط هذه الأدلة ولو بعد فترة زمنية من

---

[10] – 1 د. ممدوح عبد الحميد عبد المطلب، زبيده محمد قاسم، عبد الله عبد العزيز، مرجع سبق ذكره، ص ٢٢٤٠

[11] – د. خالد ممدوح إبراهيم، مرجع سابق، ص٢.

_ د. ممدوح عبد الحميد عبد المطلب، زبيده محمد قاسم، عبد الله عبد العزيز، مرجع سبق ذكره ، ص٢٢٣٨.

نشوئها، فالاتصالات التي تجرى عبر الانترنت والمراسلات الصادر عن الشخص أو التي يتلقاها، كلها يمكن ضبطها بواسطة تقنية خاصة بذلك.

أشكال الدليل الرقمي:[12]

أ .الصور الرقمية: وهي عبارة عن تجسيد الحقائق المرئية حول الجريمة، وفى العادة تقدم الصورة إما في شكل ورقي أو في شكل مرئي باستخدام الشاشة المرئية، والواقع أن الصورة الرقمية تمثل تكنولوجيا بديلة للصورة الفوتوغرافية التقليدية و هي قد تبدو أكثر تطوراً ولكنها ليست بالصورة أفضل من الصور التقليدية.
ب .التسجيلات الصوتية: وهى التسجيلات التي يتم ضبط وتخزينها بواسطة الآلة الرقمية، وتشمل المحادثات الصوتية على الانترنت والهاتف.... الخ.

ج- النصوص المكتوبة: وتشمل النصوص التي يتم كتابها بواسطة الآلة الرقمية، ومنها الرسائل عبر البريد الالكتروني، والهاتف المحمول، والبيانات المسجلة بأجهزة الحاسب الآلي،.... الخ .

مشروعية الدليل الرقمي:[13]

يقصد بمشروعية الوجود أن يكون الدليل معترف به، بمعنى أن يكون القانون يجيز للقاضي الاستناد إليه لتكوين عقيدته للحكم بالإدانة، ويمكن القول إن النظم القانونية تختلف في موقفها من الأدلة التي تُقبل كأساس للحكم بالإدانة بحسب الاتجاه الذي تتبناه، فهناك اتجاهان رئيسان؛ الأول نظام الأدلة القانونية ، والثاني نظام الإثبات الحر .

أولا نظام الأدلة القانونية:
فوفقاً لهذا النظام فإن المشرع هو الذي يحدد حصراً الأدلة التي يجوز للقاضي اللجوء إليها في الإثبات، كما يحدد القيمة الاقناعية لكل دليل، بحيث يقتصر دور القاضي على مجرد فحص الدليل للتأكد من توافر الشروط التي حددها القانون، فلا سبيل للاستناد إلى أي دليل لم ينص القانون عليه صراحة ضمن أدلة الإثبات، كما أنه لا دور للقاضي في تقدير القيمة الإقناعية للدليل، ولذا يسمى هذا النظام

12 – د. ممدوح عبد الحميد عبد المطلب،-أدلة الصور الرقمية في الجرائم عبر الكمبيوتر.

13 –. د هلالي عبد الإله احمد، حجية المخرجات الكمبيوترية في المواد الجنائية، دراسة مقارنة، بدون رقم طبعة او دار نشر ، ١٩٩٩ ، ص ٤٩.

_ د هلالي عبد الإله احمد، مرجع سبق ذكره. ص ٩١

_ د. علي محمود علي حمودة، الأدلة المتحصلة من الوسائل الالكترونية في أطار نظرية الإثبات الجنائي.

بنظام الإثبات القانوني أو المقيد، حيث إن القانون قيد القاضي بقائمة من الأدلة التي حددت قيمتها الاثباتية، وهذا النظام ينتمي للنظم ذات الثقافة الأنجلوسكسونية، مثل المملكة المتحدة " بريطانيا " والولايات المتحدة الأمريكية، ولذا فإن النظم التي تتبنى هذا النظام لا يمكن في ظلها الاعتراف للدليل الرقمي بأية قيمة إثباتية ما لم ينص القانون عليه صراحة ضمن قائمة أدلة الإثبات، ومن ثم فإن خلو القانون من النص عليه سيهدر قيمته الاثباتية مهما توافرت فيه شروط اليقين، فلا يجوز للقاضي أن يستند إليه لتكوين عقيدته.

وتطبيقاً لهذا الفهم نصَّ قانون الإثبات في المواد الجنائية البريطاني على قبول الدليل الرقمي وحدد قيمته الاثباتية اتفاقاً وطبيعة النظام القانوني في بريطانيا .

ويمكن أن يعاب على نظام الإثبات القانوني أن من شأنه تقييد القاضي على نحو يفقده سلطته في الحكم بما يتفق مع الواقع، فيحكم في كثير من الأحيان بما يخالف قناعته التي تكونت لديه من أدلة لا يعترف بها ذلك النظام، فيصبح القاضي كالآلة في إطاعته لنصوص القانون، ولذلك فإن هذا النظام بدأ ينحصر نطاقه حتى في الدول التي تعتبر الأكثر اعتناقاً له، فنجد بريطانيا مثلاً قد بدأت تخفف من غلوائه، حيث ظهر فيها ما يعرف بقاعدة الإدانة دون أدنى شك ، والتي مفادها أن القاضي يستطيع أن يكوِّن عقيدته من أي دليل وإن لم يكن من ضمن الأدلة المنصوص عليها متى كان هذا الدليل قاطعاً في دلالته .

٢. نظام الإثبات الحر:

يسود الإثبات الحر في ظل الأنظمة اللاتينية، ووفقا لهذا النظام يتمتع القاضي الجنائي بحرية مطلقة في شأن إثبات الوقائع المعروضة عليه، فلا يلزمه القانون بأدلة للاستناد إليها في تكوين قناعته، فله أن يبنى هذه القناعة على أي دليل وإن لم يكن منصوص عليه، بل إن المشرع في مثل هذا النظام لا يحفل بالنص على أدلة الإثبات، فكل الأدلة تتساوى قيمتها الإثباتية في نظر المشرع، والقاضي هو الذي يختار من بين ما يُطرح عليه ما يراه صالحاً للوصول إلى الحقيقة، وهو في ذلك يتمتع بمطلق الحرية لقبول الدليل أو رفضه إذا لم يطمئن إليه، فالمشرع لا يتدخل في تحديد القيمة الإقناعية للدليل، فعلى الرغم من توافر شروط الصحة في الدليل إلا أن القاضي يملك أن يرده تحت مبرر عدم الاقتناع، ولذلك فالقاضي في مثل هذا النظام يتمتع بدور إيجابي في مجال الإثبات في مقابل انحصار دور المشرع.

وعليه فإنه في مثل هذا النظام لا تثور مشكلة مشروعية الدليل الرقمي من حيث الوجود، على اعتبار أن المشرع لا يُعهد عنه سياسة النص على قائمة لأدلة الإثبات، ولذلك فمسألة قبول الدليل الرقمي لا ينال منها سوى مدى اقتناع

القاضي به إذا كان هذا النوع من الأدلة يمكن إخضاعه للتقدير القضائي، وهذه مسألة سنتناولها في الفرع الثاني من هذا المطلب .

إذن وفقا لهذا النظام فإن الأصل في الأدلة مشروعية وجودها، فالدليل الرقمي سيكون مشروعاً من حيث الوجود استصحاباً للأصل .

حجية الدليل الرقمي أمام القضاء الجنائي[14]

إن مجرد الحصول على الدليل الرقمي وتقديمه للقضاء لا يكفي لاعتماده كدليل للإدانة، فالطبيعة الفنية الخاصة للدليل الرقمي تُمكِّن من العبث بمضمونه على نحو يحرّف الحقيقة دون أن يكون في قدرة غير المتخصص إدراك ذلك العبث، فضلاً عن ذلك فإن نسبة الخطأ في إجراءات الحصول على دليل صادق في الإخبار عن الحقيقة تبدو عالية في مثل هذا النوع من الأدلة، ولذلك تثور فكرة الشك في مصداقيتها كأدلة للإثبات الجنائي، فهل من شأن ذلك استبعاد الدليل الرقمي من دائرة أدلة الإثبات الجنائي لتعارضه و قرينة البراءة.

في ظل النظم القانونية التي تعتمد النظام اللاتيني في الإثبات فإن القاضي يملك سلطة واسعة في تقييم الدليل من حيث قيمته التدليلية، فللقاضي قبول الدليل أو رفضه وهو يعتمد في ذلك على مدى اقتناعه الشخصي بذلك الدليل.

إن سلطة القاضي الجنائي في تقدير الدليل لا يمكن أن نتوسع في شأنها بحيث يقال إن هذه السلطة تمتد لتشمل الأدلة العلمية، فالقاضي بثقافته القانونية لا يمكنه إدراك الحقائق المتعلقة بأصالة الدليل الرقمي، فضلاً عن ذلك فإن هذا الدليل يتمتع من حيث قوته التدليلية بقيمة إثباتية قد تصل إلى حد اليقين، فهذا هو شأن الأدلة العلمية عموماً ، فالدليل الرقمي من حيث تدليله على الواقع تتوافر فيه شروط اليقين، مما لا يمكن معه القبول بممارسة القاضي لسلطته في التأكد من ثبوت تلك الوقائع التي يعبر عنها ذلك لدليل ، ولكن هذا لا يناقض ما سبق أن قدمناه من أن الدليل الرقمي هو موضع شك من حيث سلامته من العبث من ناحية وصحة الإجراءات المتبعة في الحصول عليه من ناحية أخرى، حيث يشكك في سلامة الدليل الرقمي من ناحيتين:

الأولى: الدليل الرقمي من الممكن خضوعه للعبث للخروج به على نحو يخالف الحقيقة، ومن ثم فقد يقدم هذا الدليل معبراً عن واقعة معينة صنع أساساً لأجل التعبير عنها خلافاً للحقيقة، وذلك دون أن يكون في استطاعة غير المتخصص إدراك ذلك العبث، على نحو يمكن معه القول إن ذلك قد أصبح هو الشأن في

[14] – د. ممدوح عبد الحميد عبد المطلب، زبيده محمد قاسم، عبد الله عبد العزيز، ص٢٢٥٣.

النظر لسائر الأدلة الرقمية التي قد تقدم للقضاء، فالتقنية الحديثة تمكِّن من العبث بالدليل الرقمي بسهولة ويسر بحيث يظهر وكأنه نسخة أصلية في تعبيرها عن الحقيقة.
الثانية: وإن كانت نسبة الخطأ الفني في الحصول على الدليل الرقمي نادرة للغاية، إلا أنها تظل ممكنة، ويرجع الخطأ في الحصول على الدليل الرقمي لسببين:

الأول: الخطأ في استخدام الأداة المناسبة في الحصول على الدليل الرقمي، ويرجع ذلك للخلل في الشفرة المستخدمة أو بسبب استخدام مواصفات خاطئة.

الثاني: الخطأ في استخلاص الدليل، ويرجع ذلك إلى اتخاذ قرارات لاستخدام الأداة تقل نسبة صوابها عن ٩٩،٠% ويحدث هذا غالباً بسبب وسائل اختزال البيانات أو بسبب معالجة البيانات بطريقة تختلف عن الطريقة الأصلية التي تم تقييمها.

ومن ذلك فإننا نخلص إلى أن الشك في الدليل الرقمي لا يتعلق بمضمونه كدليل، وإنما بعوامل مستقلة عنه، ولكنها تؤثر في مصداقيته، ولكن هل يمكن التثبت من سلامة الدليل الرقمي من حيث العيوب؟ وبكلمة أوضح هل من الممكن أن يُضفى على الدليل الرقمي اليقين من خلال إخضاعه للتقييم الفني الذي يمكِّن من تفادي تلك العيوب التي تشوبه وما موقف القاضي الجنائي من هذا الدليل إذا ما خضع لمثل ذلك التقييم؟

مثلما يخضع الدليل الرقمي لقواعد معينة تحكم طرق الحصول عليه، فإنه يخضع لقواعد أخرى للحكم على قيمته التدليلية، وذلك يرجع للطبيعية الفنية لهذا الدليل، عليه فهناك وسائل فنية من طبيعة هذا الدليل تمكن من فحصه للتأكد من سلامته وصحة الإجراءات المتبعة في الحصول عليه، وسوف نحاول فيما يلي تناول بعض هذه الوسائل.

وسائل تقييم الدليل الرقمي:[١٥]

سوف نتناول وسائل تقييم الدليل الرقمي من حيث سلامته من العبث، ثم وسائل تقييمه من حيث سلامة الإجراءات المتبعة للحصول عليه من الناحية الفنية وذلك على النحو التالي:

---

[15] -المرجع السابق .

- نصت قوانين بعض الدول التي تعتنق نظام الأدلة القانونية على الحجية القاطعة للأدلة الرقمية ، راجع : د .هلالي عبد الإله أحمد ، حجية المخرجات ، مرجع سبق ذكره ،ص. 95 .

تقييم الدليل الرقمي من حيث سلامته من العبث:
يمكن التأكد من سلامة الدليل الرقمي من العبث بعدة طرق نذكر منها:

١ . يلعب علم الكمبيوتر دوراً مهماً في تقديم المعلومات الفنية التي تساهم في فهم مضمون وهيئة الدليل الرقمي، وهذه العلوم يستعان بها في كشف مدى التلاعب بمضمون هذا الدليل، وتبدو فكرة التحليل التناظري الرقمي من الوسائل المهمة للكشف عن مصداقية الدليل الرقمي، ومن خلالها تتم مقارنة الدليل الرقمي المقدم للقضاء بالأصل المدرج بالآلة الرقمية، ومن خلال ذلك يتم التأكد من مدى حصول عبث في النسخة المستخرجة أم لا.

٢ . حتى في حالة عدم الحصول على النسخة الأصلية للدليل الرقمي أو في حالة أن العبث قد وقع على النسخة الأصلية، ففي الإمكان التأكد من سلامة الدليل الرقمي من التبديل أو العبث من خلال استخدام عمليات حسابية خاصة تسمى بالخوارزميات .

٣ . هناك نوع من الأدلة الرقمية يسمى بالدليل المحايد، وهو دليل لا علاقة له بموضوع الجريمة، ولكنه يساهم في التأكد من مدى سلامة الدليل الرقمي المقصود من حيث عدم حصول تعديل أو تغيير في النظام (الكمبيوتري).

فمن خلال هذه الطرق يمكن التأكد من سلامة الدليل الرقمي ومطابقته للواقع.
ثانياً: تقييم الدليل الرقمي من حيث السلامة الفنية للإجراءات المستخدمة في الحصول على الدليل الرقمي:

عادة تتبع جملة من الإجراءات الفنية للحصول على الدليل الرقمي، وقد قدمنا أن هذه الإجراءات من الممكن أن يعتريها خطأ قد يشكك في سلامة نتائجها ، ولذا فإنه يمكن في هذا الشأن اعتماد ما يعرف باختبارات(داو بورت) كوسيلة للتأكد من سلامة الإجراءات المتبعة في الحصول على الدليل الرقمي من حيث إنتاجها لدليل تتوافر فيه المصداقية لقبوله كدليل إثبات ، ولذا فإننا سنعرض باختصار للخطوات التي تتبع للتأكد من سلامة هذه الإجراءات من الناحية الفنية:

أ – إخضاع الأداة المستخدمة لعدة تجارب للتأكد من دقتها في إعطاء النتائج المبتغاة، وذلك بإتباع اختبارين رئيسين هما:
– اختبار السلبيات الزائفة: ومفاد هذا الاختبار أن تخضع الأداة المستخدمة في الحصول على الدليل لاختبار يبين مدى قدرتها على عرض كافة البيانات المتعلقة بالدليل الرقمي، وأنه لا يتم إغفال بيانات مهمة عنه.

– اختبار الايجابيات الزائفة : ومفاد ذلك أن تخضع الأداة المستخدمة في الحصول على الدليل الرقمي لاختبار فني يمكِّن من التأكد من أن هذه الأداة لا تعرض بيانات إضافية جديدة.
وبذلك يتم من خلال هذين الاختبارين التأكد من أن الأداة المستخدمة عرضت كل البيانات المتعلقة بالدليل الرقمي وفى ذات الوقت لم تضِف إليها أي بيان جديد، وهذا يعطي للنتائج المقدمة عن طريق تلك الآلة مصداقية في التدليل على الواقع.
ب– الاعتماد على الأدوات التي أثبتت البحوث العلمية كفاءتها في تقديم نتائج أفضل:
حيث تدل البحوث المنشورة في مجال تقنية المعلومات على الطرق السليمة التي يجب إتباعها في الحصول على الدليل الرقمي، وفى المقابل تثبت تلك الدراسات الأدوات المشكوك في كفاءتها، وهذا يساهم في تحديد مصداقية المخرجات المستمدة من تلك الأدوات.

من خلال ما تقدم يمكن الوقوف على سلامة الدليل الرقمي، فإذا توافرت في الدليل الرقمي الشروط العامة لما يمكن أن يمثل أساساً لانبعاث الثقة فيه، فإنه قد يبدو من غير المقبول أن يعيد القاضي تقييم هذا الدليل وطرحه من جديد على بساط البحث، فالدليل الرقمي بوصفه دليلاً علمياً فإن دلالته قاطعة بشأن الواقعة المستشهد به عنها، فإذا سلمنا سابقاً بإمكانية التشكيك في سلامة الدليل الرقمي بسبب قابليته للعبث ونسبة الخطأ في إجراءات الحصول عليه، فتلك مسألة فنية لا يمكن للقاضي أن يقطع في شأنهما برأي حاسم وإن لم يقطع به أهل الاختصاص، ولذلك فإذا توافرت في الدليل الرقمي الشروط المذكورة سابقاً بخصوص سلامته من العبث والخطأ، فإن هذا الدليل لا يمكن رده استناداً لسلطة القاضي التقديرية وفقاً للمادة (٢٧٥)، إذ سلطة القاضي في رد الدليل استناداً لفكرة الشك يلزم لإعمالها أن يكون هناك ما يرقى لمستوى التشكيك في الدليل، وهو ما لا يستطيع القاضي الجزم به متى توافرت في هذا الدليل شروط السلامة، بحيث يقتصر دور القاضي على بحث صلة الدليل بالجريمة.

ولا شك أن الخبرة تحتل في هذه الحالة دوراً مهما في التثبت من صلاحية هذا الدليل كأساس لتكوين عقيدة القاضي، فبحث مصداقية هذا الدليل هي من صميم فن الخبير لا القاضي.

ويجب التنويه إلى أنه لا يمكن اعتبار هذه القيمة التي ندعيها للدليل الرقمي بمثابة خروج مستحدث عن القواعد العامة للإثبات الجاني في القانون الليبي، حيث إن هناك من الأدلة ما لا يستطيع القاضي الجنائي تقديرها وفقاً لسلطته المقررة بالمادة (٢٧٥) كمحاضر المحالفات مثلا.

وهنا ننوه إلى عدم الخلط بين الشك الذي يشوب الدليل الرقمي بسبب إمكانية العبث به أو لوجود خطأ في الحصول عليه وبين القيمة الإقناعية لهذا الدليل، فالحالة الأولى لا يملك القاضي الفصل فيها لأنها مسألة فنية فالقول فيها هو قول أهل الخبرة، فإن سلم الدليل الرقمي من العبث والخطأ، فإنه لن يكون للقاضي سوى القبول بهذا الدليل ولا يمكنه التشكيك في قيمته التدليلية لكونه وبحكم طبيعته الفنية يمثل إخباراً صادقاً عن الواقع ، ما لم يثبت عدم صلة الدليل الجريمة المراد إثباتها.

الجريمة الالكترونية في مصر:

في الدستور المصري[16]:

مادة ٥٧: للحياة الخاصة حرمة، وهى مصونة لا تمس.
وللمراسالت البريدية، والبرقية، والإلكترونية، والمحادثات الهاتفية، وغيرها من وسائل الاتصال حرمة، وسريتها مكفولة، وال تجوز مصادرتها، أو الإطلاع عليها، أو رقابتها إلا بأمر قضائي مسبب، ولمدة محددة، وفى الأحوال التي يبينها القانون.

كما تلتزم الدولة بحماية حق المواطنين في استخدام وسائل الاتصال العامة بكافة أشكالها، وال يجوز تعطيلها أو وقفها أو حرمان المواطنين منها، بشكل تعسفي، وينظم القانون ذلك.

مادة ٧٠:
حرية الصحافة والطباعة والنشر الورقى والمرئي والمسموع والإلكتروني مكفولة، وللمصريين من أشخاص طبيعية أو اعتبارية، عامة أو خاصة، حق ملكية وإصدار الصحف وإنشاء وسائل الإعلام المرئية والمسموعة، ووسائط العالم الرقمي.

وتصدر الصحف بمجرد الإخطار على النحو الذي ينظمه القانون. وينظم القانون إجراءات إنشاء وتملك محطات البث الإذاعي والمرئي والصحف الإلكترونية.

[16] – دستور جمهورية مصر العربية ٢٠١٤.

في القانون:

– القانون رقم (٨٢) لسنة 2002 الخاص بحقوق الملكية الفكرية.
– القانون رقم (١٠) لسنة 2003 المعروف بقانون تنظيم الاتصالات.
– القانون رقم (١٥) لسنة 2004 الخاص بتنظيم التوقيع الالكتروني.

دراسة مقارنة

الولايات المتحدة الأمريكية[17]:

إن الولايات المتحدة الأمريكية، لا تتميز بأسبقية سن هذه التشريعات فحسب بل تتميز بسن تشريعات خاصة بكافة مسائل تقنية المعلومات وفي قطاعات الحوسبة والاتصالات والانترنت ترتبط أو تتعلق بجرائم الكمبيوتر والانترنت مباشرة أو على نحو غير مباشر ، كما أنها تشريعات تراعي خصائصها المميزة وتتطور تبعا لتطور قطاع التقنية ذاته ، وتتميز الولايات المتحدة الأمريكية أيضا بوضع عدة تشريعات على المستوى الفدرالي وحزمه معتبرة من التشريعات على مستوى الولايات. فعلى المستوى الفدرالي، تبلور نشاط لجنة الكونجرس الخاصة بحماية استخدام الحاسوب بتقديم مشروع (قانون حماية الحاسوب سنة ١٩٨٤) غير أن هذا المشروع لدى عرضه ودراسته من قبل الكونجرس ولجانه المختصة، جرى التعديل على أحكامه بشكل جوهري، وجرى إقراره بعد سلسلة من التعديلات والإضافات ولم يصدر باسمه المشار إليه، فصدر قانون (غش الحاسوب وإساءة استخدامه لعام ١٩٨٤) أو كما يترجم اسمه البعض (قانون الاحتيال وإساءة استخدام الحاسوب – Computer Fraud and abuse Act .) وأضيف إلى القانون مدونة القانون الأمريكي تحت قسم الجرائم.

وقد نص القانون المذكور، على تجريم مجرد الاتصال دون تصريح بنظام حاسوب، وعلى الاتصال المصرح به الذي يستخدم فيه الفاعل الحاسوب لأغراض غير مصرح بها كتعديل أو إتلاف أو تدمير أو إفشاء المعلومات المخزنة في الحاسب، كما نص على عقاب من يرتكب فعلا من شأنه منع الاستخدام المصرح به للحاسوب"، وخضع

[17] – د. يونس عرب – تطوير التشريعات في مجال مكافحة الجرائم الالكترونية–
_ See :- Susan W. Brenner, *State Cybercrime Legislation in the United States of America: A Survey*, 7 RICH. J.L. & TECH. 28 (Winter 2001), *at* http://www.richmond.edu/jolt/v7i3/article2.html. See

لاحقا لتعديلات واكبت التطورات التقنية . كما صدر أيضا في الولايات المتحدة على المستوى الفدرالي (قانون أمن الحاسوب لسنة ١٩٨٧) والذي يقضي باتخاذ الوكالات الفدرالية خطوات ملائمة لتأمين وحماية أنظمة حواسيبها، وينظم هذا القانون مستويات الحماية والرقابة عليها والمسؤولية عن اغفالها. وتوالت بعد ذلك في التسعينات التعديلات والتشريعات الفرعية والقطاعية ذات العلاقة بأمن المعلومات.

في الولايات المتحدة ينظم جرائم الكمبيوتر والانترنت مجموعة من التشريعات على المستوى الفدرالي وكذلك على المستوى المحلي في مختلف الولايات، فعلى المستوى الفدرالي يمثل القسم (١٨) من قانون الولايات المتحدة التشريع الرئيس لجرائم الكمبيوتر (المادة ١٠٣٠) حيث تتضمن اعتبار الأفعال التالية من قبيل الجريمة:-

١ – التوصل غير المصرح به (الدخول) إلى احد أنظمة الكمبيوتر الحكومية وكشف المعلومات السرية، وكشف المعلومات من جهة غير مصرح بها تلقيها.
٢ – الدخول غير المصرح به إلي إي كمبيوتر والتوصل إلى معلومات غير مسموح الإطلاع عليها.
٣ – الدخول غير المصرح به إلي إي كمبيوتر ومن ثم ارتكاب احتيال.
٤ – إلحاق أضرار جراء الدخول غير المصرح به سواء للنظام أو البرامج أو للمعلومات المخزنة فيه.
٥ – بث أو تهديد بارتكاب ضرر لأي كمبيوتر عبر الولايات أو للتجارة الأجنبية بغرض ابتزاز أموال أو منافع من إي شخص طبيعي أو معنوي.

أما القسم (١٤٦٢) من الفصل (١٨) من قانون الولايات المتحدة فانه يحظر استخدام الكمبيوتر لاستيراد مواد مخلة بالآداب إلي داخل الولايات المتحدة الأمريكية.

في حين أن القسم (١٤٦٣) من الفصل (١٨) يحظر نقل أية مواد فاحشة عبر الولايات أو الجهات خارجية.
ويجرم القسم (٢٢٥١) من ذات الفصل توظيف إي قاصر أو إغرائه في المشاركة في أنشطة جنسية بما فيها خلق وتصوير مواد وبثها لجهات خارجية.

ويحظر القسم (٢٢٥١) من ذات الفصل استخدام الكمبيوتر الإخلال برعاية قاصر بقبول استغلاله – مع العلم – في انتاج مواد تنطوي على استغلال جنسي.

ويعتبر القسمين (٢٢٥٢، ٢٢٥٢ /أ) من ذات الفصل نقل وتبادل المواد الفاحشة ذات الصلة بالأطفال جريمة.

أما القسم (١٠٢٨) من الفصل (١٨) من قانون الولايات المتحدة فانه يعتبر إنتاج أو نقل أو إدارة جهاز يتضمن نظام كمبيوتر بقصد استخدامه بتزوير الوثائق أو إنتاج وثائق تعريف مزورة جريمة ويعتبر القسم (٢٣١٩) من ذات الفصل الإخلال بحق المؤلف جريمة فدرالية.

وعلى مستوى الولايات، فان الإطار العام لتشريعات الولايات المتحدة في حقل جرائم الكمبيوتر والانترنت يتمثل بما يلي: –

١ . كل ولاية من الولايات الخمسين تملك حرية التشريع الخاص بها وليس هناك آلية على مستوى الولايات أو المستوى الفدرالي تتطلب تبني الولاية شكلا او محتوى محددا لقوانينها، وذلك بالرغم من وجود مشاريع توحيدية ومحاولات وتصريحات تهدف إلي توحيد التدابير الشتريعية.

٢ . إن الإطار العام لتوحيد قوانين جرائم الكمبيوتر يعتمد على مشروع قانون نموذجي تم وضعه من قبل هيئة أكاديمية عام (١٩٩٨)، حيث يقسم أحكام جرائم الكمبيوتر والانترنت إلي ثماني طوائف (ويجب أن يلاحظ إن هذا هو تقسيم القانون النموذجي لكنه يعتمد هنا كإطار للوقوف على مواقف التشريعات القائمة والنافذة في الولايات

فرنسا[١٨] :

سن المشرع الفرنسي القانون رقم ١٩ – ٨٨ بتاريخ ٥ كانون ثاني ١٩٨٨ الخاص ببعض جرائم المعلوماتية وضمنه قانون العقوبات الفرنسي في المادة (٤٦٢) وجرم فيه مجرد الولوج إلى نظام المعالجة الآلية أو البقاء فيه بطريق غير مشروع (٢/٤٦٢) وشدد العقوبة في الأحوال التي ينجم عن هذا الولوج محو أو تعديل في المعطيات المعالجة آليا. ونص القانون على تجريم إتلاف المعطيات وتزوير المستندات المعالجة آليا، واستعمال هذه المستندات. وعاقب على هذه الجرائم بعقوبة الحبس أو الغرامة. وقد خضع هذا القانون لتعديلات في العام ١٩٩٣ وسعت من نطاق السلوكيات محل التجريم إضافة إلي تعديل بعض العقوبات لتحقيق مزيد من الأبعاد الردعية.

[18] – د. يونس عرب – تطوير التشريعات في مجال مكافحة الجرائم الالكترونية–

بريطانيا :[19]

سن المشرع البريطاني قانون إساءة استخدام الحاسوب لسنة ١٩٩٠ – (Computer Misuse Act) وبدء سريانه بتاريخ ٢٩ آب / أغسطس ١٩٩٠، وقد خلق هذا القانون ثلاث جرائم جديدة لمواجهة جرائم الاختراق والتوصل غير المصرح به لتعديل معطيات الحاسوب وإتلافها بشكل عام وجرائم إدخال الفيروس بشكل خاص. هذه الجرائم هي:–

أ – الدخول غير المصرح به لنظام الحاسوب (النشاط الرئيسي للعبث أو التطفل)
ب – نفس الفعل السابق، ولكن بقصد ارتكاب أو تسهيل ارتكاب فعل آخر.
جـ – التعديل أو التحوير غير المصرح به لنظام الحاسوب بقصد إضعاف أو تعطيل النظام.

وبالرغم من أن الاستجابة البريطانية للتدابير التشريعية الجديدة في حقل تقنية المعلومات، وصفت بأنها متأخرة عن غيرها من الدول الأوروبية ومتأخرة بالتأكيد عن الاستجابة الأمريكية إلا أن السنوات الأخيرة وتحديدا الأعوام من ١٩٩٨ وحتى الآن تشهد تميزا في التجربة البريطانية سواء من حيث محتوى التنظيم أو الحلول التشريعية المقررة، ليس في نطاق امن المعلومات فحسب، بل في نطاق حماية البيانات الشخصية والخصوصية وتنظيم حرية البيانات والمعلومات وفي مختلف الفروع الأخرى لقانون تقنية المعلومات.

المانيا:[20]

صدر بتاريخ ١٥ أيار / مايو ١٩٨٦ (قبل اتحاد الألمانيتين) القانون الثاني لمكافحة الجريمة الاقتصادية، وسرى مفعولة في الأول من آب / أغسطس ١٩٨٦، وقد جرم هذا القانون إتلاف أو محو أو تغيير أو تزوير البيانات المعالجة آليا، وشدد العقوبة بالنسبة للبيانات ذات الأهمية الأساسية لقطاع الأعمال أو السلطة الإدارية لتصل إلى حد السجن لمدة خمس سنوات والغرامة، وكذلك جرم هذا القانون غش الحاسوب أو الاحتيال بواسطة الحاسوب وعاقب عليه بذات العقوبة المذكورة كما عاقب على الحصول دون تصريح من قبل الفاعل لنفسه أو غيره على بيانات غير معدة أو مخصصة له ومحمية بوجه خاص ضد الوصول غير المصرح به.

[19] – المرجع السابق .
[20] – المرجع السابق .

عمان:[21]

بموجب المرسوم السلطاني رقم ٢٠٠١/٧٢ المنشور في الجريدة الرسمية العمانية رقم ٦٩٨ تاريخ ٢٠٠١/٧/١ تم تعديل بعض أحكام قانون الجزاء العماني رقم ٧ لعام ١٩٧٤، ومن ضمن هذه التعديلات إضافة الفصل الثاني مكرر على الباب السابع تحت عنوان جرائم الحاسب الآلي (المواد ٢٧٦ مكررا و٢٧٦ مكرر ١ و٢٧٦ مكرر ٢ و ٢٧٦ مكرر ٣ و ٢٧٦ مكرر ٤.

وقد نصت المادة (٢٧٦ مكرراً) :على أن يعاقب بالسجن مدة لا تقل عن ثلاثة أشهر ولا تزيد على سنتين وبغرامة من مائة ريال إلى خمسمائة ريال أو بإحدى هاتين العقوبتين كل من تعمد استخدام الحاسب الآلي في ارتكاب احد الأفعال الآتية:-

١- الالتقاط غير المشروع للمعلومات أو البيانات
٢- الدخول غير المشروع على أنظمة الحاسب الآلي
٣- التجسس والتصنت على البيانات والمعلومات
٤- انتهاك خصوصيات الغير أو التعدي على حقهم في الاحتفاظ بأسرارهم
٥- تزوير بيانات أو وثائق مبرمجة أيا كان شكلها
٦- إتلاف وتغيير ومحو البيانات والمعلومات
٧- جمع المعلومات والبيانات وإعادة استخدامها
٨- تسريب المعلومات والبيانات
٩- التعدي على برامج الحاسب الآلي سوءا بالتعديل أو الاصطناع
١٠- نشر واستخدام برامج الحاسب الآلي بما يشكل انتهاكاً لقوانين حقوق الملكية والأسرار التجارية

كما نصت المادة (٢٧٦ مكرراً) (١): على انه "يعاقب بالسجن مدة لا تقل عن ستة أشهر ولا تزيد على سنتين وبغرامة لا تقل عن مائة ريال ولا تزيد على خمسمائة ريال أو بإحدى هاتين العقوبتين كل من أستولي أو حصل على نحو غير مشروع على بيانات تخص الغير تكون منقولة أو مختزنة أو معالجة بواسطة أنظمة المعالجة المبرمجة للبيانات.

ونصت المادة (٢٧٦) مكرراً (٢): على انه "تضاعف العقوبة إذا ارتكبت الأفعال المشار إليها في المادة (٢٧٦) مكرراً و(٢٧٦) مكرراً (١) من مستخدمي الكمبيوتر.
ونصت المادة (٢٧٦) مكرراً (٣): على أن "يعاقب بالسجن مدة لا تزيد على خمس سنوات وبغرامة لا تجاوز ألف ريال كل من:-

1 - قام بتقليد أو تزوير بطاقة من بطاقات الوفاء أو السحب
٢- استعمل أو حاول استعمال البطاقة المقلدة أو المزورة مع العلم بذلك
٣- قبل الدفع ببطاقة الوفاء المقلدة أو المزورة مع العلم بذلك

[21] -حسن حماد حميد – مدرس القانون الجنائي – الائتلاف المعلوماتي، كلية القانون جامعة البصرة.

ونص في المادة (٢٧٦) مكرراً (٤):- على انه " يعاقب بالسجن مدة لا تزيد على ٣ سنوات وبغرامة لا تجاوز خمسمائة ريال كل من -:

١- استخدم البطاقة كوسيلة للوفاء مع علمه بعدم وجود رصيد له

٢- استعمل البطاقة بعد انتهاء صلاحيتها أو إلغائها وهو عالم بذلك

٣- استعمل بطاقة الغير بدون علمه

نظرة تحليلية

وباستعراض ما تقدم من تعريف لماهية الجريمة الالكترونية وأنواعها وأشكالها ومرتكبيها، والدليل الرقمي وخصائصه ومميزاته وأنواعه ومشروعيته، نستخلص أن هناك قصور شديد ليس فقط في التشريعات المصرية ولكن العربية والدولية أيضا لمواجهة الجريمة الالكترونية التي تتزايد بشكل مخيف تواكبا مع التطور التكنولوجي في العالم ومهارات القرصنة التي من شأنها أن تهدد استقرار الدولة وسلامتها وحريات الأفراد.

ولكن بتسليط الضوء علي التشريعات المصرية يثور هنا التساؤل حول حجية الدليل الرقمي أمام القضاء المصري سواء كدليل إدانة أو دليل براءة، في حقيقة الأمر إن القانون المصري قد أعطي القاضي الجنائي سلطة تقديرية واسعة في الأحكام الجنائية، ولما كان هناك قصور في النصوص التشريعية في تنظيم الأدلة الرقمية كدليل إثبات فان السلطة التقديرية للقضاة في غالب الأحوال تكون هي معيار اعتبار الدليل الرقمي دليل إثبات من عدمه أو حتى علي سبيل الاستدلال.

وفي وجهة نظرنا حول مدي تكييف الدليل الرقمي وأدلة الإثبات المتعارف عليها قانونيًا مثل شهادة الشهود و البينة والقرائن والاعتراف والخبراء ودليل الثبوت الكتابي..الخ. فإننا نستطيع تصور أن "أ" إذا حرر خطابا علي صفحته علي احد مواقع التواصل الاجتماعي فإنه يمكن معه اتخاذ ذلك الخطاب كاعتراف منه علي نفسه أو علي الغير و يمكن اعتباره شهادة منه علي حدثا أو جريمة ما، كذلك يمكن اتخاذ قرينة كدلالة و يمكن اتخاذ دليل ثبوت كتابي مثل المحررات الرسمية والعرفية.

ولكننا نري أن الدليل الرقمي هو دليل إثبات قائم بذاته لا ينطوي تحت احد أدلة الإثبات المتعارف عليها و إن كان لا يوجد تشريعا في مصر حتى الآن ينص علي ذلك أو ينظمه، وهنا تثور المشكلة الحقيقة أننا في حاجة ملحة لوجود نص تشريعي لتعريف محدد للدليل الرقمي ومشروعيته وحجيته وإثره ينظمها القانون كدليل إثبات قائم بذاته حتى لا نتركها لأهواء القضاة وسلطتهم التقديرية.

وأخيرا،،

يوصي مركز هردو لدعم التعبير الرقمي بالاتي:

أولًا: أن تلتزم الحكومة المصرية بوضع تشريعات واضحة لمواجهة الجريمة الالكترونية وسرعة تطورها وتوفير خبرات فنية عالية قادرة على التعامل والتطور التكنولوجي للجريمة، كذلك تعديل القوانين المنظمة لتداول المعلومات عبر شبكة الانترنت بما لا يخل و حرية تداولها و أدراج تعريفات محددة للجرائم الالكترونية في قانون الإجراءات الجنائية و قانون العقوبات.

ثانيا: نشر الوعي المجتمعي بالمخاطر الاجتماعية والسياسية والاقتصادية والثقافية الناجمة عن الاستخدام غير الآمن للإنترنت، وتبني استراتيجية قومية لتنمية الرصد والتحقيق والتوعية والتثقيف بخطورة الجرائم الالكترونية.

ثالثا: العمل علي التواصل مع البلدان العربية والأفريقية والشرق الأوسط لتحقيق استراتيجية موحدة لمكافحة الجريمة الالكترونية، والاستفادة من خبرات تلك البلدان وغيرها في تحقيق ذلك.

رابعًا: وضع تعريف محدد وواضح للدليل الرقمي والاعتراف به كدليل إثبات في المواد الجنائية والمدنية والتعاملات القانونية أو إدراجه تحت أحد أدلة الإثبات المتعارف عليها حتى لا تخضع تلك الأدلة للسلطة التقديرية للمحاكم.

الجريمة الإلكترونية

وحجية الدليل الرقمي في الإثبات الجنائي

يتناول التقرير تعريف ماهية الجريمة الالكترونية وخصائصها وأسبابها ووسائل مكافحتها، وكيف تناولتها المواثيق والتعريفات الدولية، وكذا وضعها في الدستور والقانون المصري، والتشريعات الخاصة بمكافحة الجريمة الالكترونية ومعاقبة مرتكبيها.

يتناول التقرير بالتفصيل تعريف المعلومات والمفهوم القانوني لها، وأنواعها من حيث كانت تلك المعلومات متاحة للجميع مثل التقارير أو الدوريات، أم معلومات شخصية لصاحبها فقط، كما يتناول التقرير بالتفصيل الشروط الواجب توافرها في المعلومة محل الحماية.

يستعرض التقرير دراسة مقارنة حول كيفية التصدي للجريمة الالكترونية في بعض البلدان في أوروبا والولايات المتحدة والمنطقة العربية من حيث التشريعات التي وضعتها تلك البلدان وآلية تنفيذها بما يضمن ولا يخل بحق مواطنيها في تداول المعلومات وسرية مراسلتهم الالكترونية وحقهم في حرية التعبير عن رأيهم بشتى الوسائل.

يعرض التقارير بعض شهادات للمقرصنين، وبعض الكُتّاب المحللين في مجال القرصنة، وبعض تعليقاتهم حول انواع مرتكبي جرائم الإنترنت وبعض من الحقائق عن خلفياتهم النفسية والمجتمعية والعمرية، حيث يؤكد المحللون أن لكل فئة عمرية مختلفة سبب وحافز لإرتكاب الجريمة الالكترونية مختلف تمامًا عن أي فئة أخرى، حيث الفئات صغيرة السن يكون المحفز لهم هو إثبات أنفسهم ومحاولة البُعد عن سيطرة الكبار، أما الفئات الأكبر سنًا تختلف دوافعهم من شخص لآخر حسب الظروف المحيطة به، فمنهم من يرتكب الجريمة بقصد الانتقام من رئيس العمل مثلًا، ومنهم من يرتكبها بغرض المُتعة، أو الحصول على الأموال الطائلة..إلخ.

www.hrdoegypt.org