جرائم بيئة الشبكات الاجتماعية
وآليات ضبطها في التشريع المقارن

رائد دكتور

مصطفى سامي علي مصطفى

دكتوراه القانون العام

كلية الحقوق جامعة بني سويف

المبحث التمهيدي

الإطار العام للدراسة

مقدمـــة

منذ ظهر الحاسب الآلي عام ١٩٤٦ على يد العالمين لأمريكيين(e.p.eckert_j.w.mauchly) في جامعة بنسلفانيا وشاع استخدامه في العالم بعد ذلك إلي أن وصل الي العالم العربي في مطلع الستينات على يد الشركات الأجنبية والمصارف، فإن العالم أصبح في مواجهة كائن ميكانيكي جديد بدأ يغزو الحياة بشكل تدريجي وتطور مضطرد في شكل ثورة علمية جديدة جعلت هذا الحاسب يؤدي من المهام والوظائف والتعامل مع المعلومات والوظائف مالا طاقة لآلاف الأشخاص بها، وأصبح هذا الجهاز مستودعاً لأسرار الناس وأبحاثهم وخططهم، وغداً الحاكم الآمر والموجه الأمين، لآلات المصانع والمعامل، والمتحكم في حركة الطائرات، والقاطرات ، والمنظم لعمل البنوك والشركات، والمنجز لمهام وأعمال وخدمات الحكومات.

من هنا يمكن القول بأن العالم أصبح أمام ثورة حقيقية هي ثورة المعلومات، أو العالم الرقمي، وصار الناس أحياناً مختارين وفي أحايين أخرى مضطرين للتعامل مع هذا العالم الجديد أو مجتمع المعلومات كما يحلو للبعض أن يسميه، وما لبث الناس قليلاً وهم يفيقون من صدمة ثورة المعلومات الجامحة حتى دهمتهم ثورة جديدة خلقها ذلك التزاوج أو الإتحاد الفريد بين هذا الجهاز وأنظمة الإتصالات الحديثة، لنصل في نهاية القرن الماضي وبدايات هذا القرن الي ما يسمى التواصل عبر شبكة الأنترنت العالمية، التي حطمت الحدود بين الدول وقصرت المسافات بين الأفراد والجماعات، واختصرت الزمن عبر شبكة لامرئية، أو محسوسة، سميت بشبكة الأنترنت العالمية،أو (الشبكة العنكبوتيه) أو (الفضاء السيبراني) والتي بدأ استعمالها للأمور العسكرية أولا في الولايات المتحدة الأمريكيه منذ عام ١٩٦٩، وبدأ العالم العربي يتعرف عليها في أواخر الثمانينات وبدأت تنتشر فيه تدريجيا، بل إن الأمر تطور إلى حد الاقتراع من خلال جهاز الكمبيوتر مباشرة.

وبعيدا عن الاستخدامات الحميدة أو السلمية للكمبيوتر، يمكن القول بأن التطور المذهل فى هذا المجال، قد ترتب عليه نشوء جرائم ناتجة عن استخداماته المتعددة، وهذه الجرائم إما أن تقع على الكمبيوتر ذاته، وإما أن تقع بواسطة الكمبيوتر حيث يصبح أداة في يد الجاني يستخدمه لتحقيق أغراضه الإجرامية.

ونظرا لازدياد الجرائم المتعلقة بتقانة المعلومات شرعت الدول المتمدينة بوضع تشريعات جنائية خاصة لمكافحة جرائم الكمبيوتر التي تعتبر ظاهرة مستحدثة علي علم الإجرام ومن هذه الدول، الولايات المتحدة الأمريكية وفرنسا وباقى دول الاتحاد الأوروبي الذي وضع اتفاقية حول جرائم الكمبيوتر سنة ٢٠٠١م، والتي أوصت فيها الدول الأعضاء باتخاذ كافة الإجراءات التشريعية أو غيرها حسب الضرورة لجعل الدخول إلى جميع نظم الكمبيوتر أو أي من أجزائه بدون وجه حق جريمة جنائية بحسب القانون المحلي، كما أوصت هذه الاتفاقية على مجموعة من المبادئ العامة المتعلقة بالتعاون

الدولي في مجال الشئون الجنائية، وحددت كذلك الإجراءات المتعلقة بطلبات المساعدة المتبادلة بين الدول الأعضاء في غياب الاتفاقيات الدولية. وهكذا وجد العالم نفسه في قرية صغيرة، وأصبحت قرية المعلومات هذه محط انظار جميع أصحاب المصالح المشروعة وغير المشروعة، وبدأت تقنية المعلومات تفرز أثارا شاملة على البنية الإدارية والاقتصادية والاجتماعية والسياسية،والثقافية ،والقانونية للدول ،ذلك أن كل إختراع علمي لابد ان يفتح افاقا جديدة ويرتب أثاراما كانت قائمة قبل وجوده وانتشاره، وهنا كان لابد للقانون أن يتدخل، كيف لا وهو المنظم بقواعده على اختلاف أنواعها، لجميع مناحى الحياة.

ويشير الباحثون في هذا الصدد إلي أن توقيت ولادة قانون الكمبيوتر، بدأ مع شيوع استعمال الكمبيوتر وانخفاض كلفة استخدامه وذلك في نهاية الستينات ومطلع السبعينات، حيث، كانت أولى التحديات القانونية التي أثارها استخدام الكمبيوتر هي اساءة استخدامه على نحو يضر بمصالح الأفراد والمؤسسات، وخاصة في حقل اساءة التعامل مع البيانات الشخصية المخزنة بالكمبيوترعلى نحو يمس أسرارهم وحياتهم الخاصة وحقهم في الخصوصية، والأمر الثاني هو المسئولية عن الأفعال التي تمثل اعتداء على الأموال والمصالح، وحق الأفراد في المعلومات ذات القيمة الإقتصادية.

وطبقا لما نشره معهد (ستانفورد) في الولايات المتحدة فإن أول محاولة لإساءة استخدام الكمبيوتر كانت عام ١٩٥٨، ليأتي بعدها موجة ظهور القوانين الوطنية في حقل جرائم الكمبيوتر مع نهاية السبعينات، حيث صدر قانون بالولايات المتحدة لأمريكية عام ١٩٧٨ سبقه إصدار السويد لقانون في العام ١٩٧٣ يتعلق بحماية الخصوصية، وهكذا نجد أول موجات التشريع التي حظيت بالاهتمام الدولي في مجال قانون الكمبيوتر كانت منصبة على حماية الخصوصية، وحماية تجميع ومعالجة وتخزين وتبادل البيانات الشخصية، وفي بداية فترة السبعينات أيضا، اتضح الإدراك الكبير لأهمية برامج الكمبيوتر وقيمتها بين عناصر صناعة الكمبيوتر وثار جدل حول موقع حمايتها، هل هو ضمن حماية برامج الكمبيوتر؟ ام هي تشريعات حماية حقوق المؤلف مع اتفاق الجميع على وجوب حمايتها؟ لنجد دولة مثل الفلبين تصدر في العام ١٩٧٣ تدابير تشريعية في حقل حماية البرمجيات ،توج ذلك التوجه الجهد الفعال لخبراء المنظمة العالمية للملكية الفكرية (الوايبو) الذين وضعو القواعد النموذجية لحماية برامج الكمبيوتر(حماية الملكية الفكرية لبرامج الكمبيوتر) ،والتي كانت من أكثر تشريعات قوانين الكمبيوتر نضجا ووضوحا حسبما يرى الكثير من الباحثين لتأتي بعد ذلك موجة تشريعية ثالثة لتشمل حماية البرمجيات في عقد الثمانينيات.

هذا ويوصف العصر الذي نعيشه بعصر التقنية العالية، عصر وسائل معالجة ونقل المعلومات التي غدت المحدد الاستراتيجي للبناء الثقافي والإنجاز الاقتصادي، وإذا كان خط ميلاد التقنية ونماءها، قد أظهر في البدايات اكتشاف وتطور وسائل التقنية العالية، الحاسب الآلي والاتصال، مستقلة عن بعضها البعض، فإن قطاعات التقنية قد تداخلت وتحقق الدمج المعقد بين الحاسبات الآلية ووسائل الاتصال، وبرز في قضاء التقنية من بين وسائلها الكثيرة، الحاسب الآلي، أداة التحكم بالمعلومات وتجميعها

ومعالجتها واختزانها واسترجاعها ونقلها في كافة قطاعات النشاط الإنساني، خاصة النشاط الثقافي والتجاري والصناعي.

وقد أثار إحصاء إجراءات تقنية المعلومات تحديات لها وزنها بالنسبة لقانون العقوبات في كل الأنظمة القانونية ويرجع السبب في ذلك إلى الحقيقة التي مؤداها أنه حتى هذه اللحظة، فإن الأشياء المادية والمرئية هي التي تكون محمية بالقوانين الجنائية، وحماية المعلومات والقيم المعنوي الأخرى وإن وجدت منذ فترة زمنية قصيرة إلا أنها حتى منتصف القرن العشرين كانت أقل أهمية، وقد طرأ تغيير جوهري على هذا الموقف أثناء العشر سنوات الأخيرة، حيث أدى تطور المجتمع من مجتمع صناعي إلى مجتمع ما بعد الصناعي، إلى تزايد قيمة المعلومات بالنسبة للاقتصاد والمجتمع والسياسة، فضلا عن الأهمية المتنامية لتقنية المعلومات خلال فترة زمنية قصيرة، وهو الأمر الذى رتب يعرف بقانون المعلومات.

وتنبع أهمية هذه الدراسة من كونها تتناول الثورة المعلوماتية من زاوية الجانب السلبى منها والمتعلق بجرائم المعلوماتية وتأثيره على مكونات المجتمع. وأمام هذا الشكل الجديد من الإجرام لا تبدو قوانين العقوبات الوطنية في حالتها الراهنة كافية أو فعالة على النحو المطلوب أو المرضي فنصوصها والنظريات والمبادئ القانونية التي تتضمنها أو تقف ورائها موروث بعضها من القرن ١٩ حيث لم يكن هناك فنيين حينذاك وإنما أصحاب مهن وحرفيين.

وتطبيق بعضها على أشكال جديدة للجرائم التي تستعير من تقنيات الحاسبات الآلية والمعلومات أساليبها، لا يصطدم فقط بصعوبات ناجمة عن الطبيعة الخاصة والخصائص الفنية الفريدة للوسائل المعلوماتية المستخدمة في ارتكابها. وإنما تعترضه كذلك صعوبات رئيسية أخرى مرجعها أن نصوص التجريم التقليدية قد وضعت في ظل تفكير يقتصر إدراكه على الثروة الملموسة والمستندات ذات الطبيعة المادية مما يتعذر معه تطبيقها لحماية القيم غير المادية المتولدة عن المعلوماتية.

والحقيقة التى يجب التأكيد عليها أن وسائل الاتصال لم تخترع الجريمة، بل كانت ضحية لها في معظم الأحوال حيث أن هذه الوسائل تعرضت لسوء الاستغلال من قبل كثيرين ، ومن الثابت أيضاً أن المجرمين وظفوا الاتصال تاريخياً – ضمن أدواتهم المختلفة – لخدمة النشاطات الإجرامية التي يقومون بها. أما الجريمة فهي ذاتها الجريمة في قديم التاريخ، وحديثه، لا يختلف على بشاعتها، وخطرها على المجتمع الإنساني أحد، ولذلك اتفق على مواجهتها، ومن أجلها أقيمت المحاكم، وسنت العقوبات، تستوي في النظرة إليها -كسلوك شاذ - كل الشرائع السماوية، والقوانين الوضعية. وعبر حقب التاريخ المختلفة كانت الظاهرة الإجرامية مرادفة للتجمع الإنساني، تعكس في أساليبها، وأنماطها، أحوال وتطورات المجتمع في مختلف النواحي السياسية، والاقتصادية، والاجتماعية، والثقافية، وغيرها. وفي عصر التقنية، وثورة الاتصالات الحديثة تعقدت الجريمة، وتنوعت أساليبها مستفيدة من التطور التقني في كافة مناحي الحياة، حيث وظف المجرمون هذه المستحدثات التقنية الحديثة في تطوير أساليبهم، بل حتى التقنية ذاتها لم تسلم من الجريمة فمنذ بداياتها ظهر معها ما يعرف بجرائم التقنية، أو الجرائم الإلكترونية التي أخذت أبعاداً جديدة مع بداية ثمانينات القرن الماضي

بعد انتشار الحاسبات الشخصية، وتطبيقاتها بشكل جماهيري في مختلف أرجاء العالم. ومع مطلع التسعينات من القرن الماضي ظهرت أنماط حديثة أخرى من الجريمة صاحبت انتشار (شبكة المعلومات العالمية الإنترنت) التي برزت كأسرع وسائل الاتصال الجماهيري نمواً في تاريخ وسائل الاتصال.

وإزاء ذلك كان لا بد من تكاتف الدول من أجل مكافحة هذا النوع المستحدث من الجرائم، التي لم تعد تتمركز في دولة معينة، ولا توجه لمجتمع بعينه بل أصبحت تعبر الحدود لتلحق الضرر بعدة دول ومجتمعات، مستغلة التطور الكبير للوسائل التقنية الحديثة في الاتصالات و المواصلات، وتعزيز التعاون بينها واتخاذ تدابير فعّالة للحد منها والقضاء عليها ومعاقبة مرتكبيها.

مشكلة الدراسة

لعله من نافلة القول أن جرائم تقانة المعلومات، هى ظاهرة إجرامية جديدة ومستجدة تقرع في جنباتها أجراس الخطر لتنبه مجتمعات العصر الراهن لحجم المخاطر وهول الخسائر الناجمة عن جريمة الحاسب الآلي التي تستهدف الاعتداء على المعطيات بدلالتها التقنية الواسعة (بيانات ومعلومات وبرامج بكافة أنواعها). فجريمة الحاسب الآلي جريمة تقنية تنشأ في الخفاء، يقترفها مجرمون أذكياء يمتلكون أدوات المعرفة التقنية، توجه للنيل من الحق في المعلومات، وتطال اعتداءاتها معطيات الحاسب المخزنة والمعلومات المنقولة عبر نظم وشبكات المعلومات.

هذه المعطيات هي موضوع هذه الجريمة وما تستهدفه اعتداءات الجناة، وهذا وحده – عبر دلالته العامة – يظهر مدى خطورة جرائم الحاسب الآلي، فهي تطال الحق في المعلومات، وتمس الحياة الخاصة للأفراد، وتهدد الأمن القومي والسيادة الوطنية، وتشيع فقدان الثقة بالتقنية وتهدد إبداع العقل البشري، لذا فإن إدراك ماهية جرائم الحاسب الآلي، منوط بتحليل وجهة نظر الدارسين لتعريفها والاصطلاحات الدالة عليها واختيار أكثرها اتفاقًا مع الطبيعة الموضوعية لهذه الجرائم، واستظهار موضوعها وخصائصها ومخاطرها وحجم الخسائر الناجمة عنها وسمات مرتكبيها ودوافعهم.

وترتيبا على ما سبق يمكن للباحث صياغة المشكلة البحثية للدراسة الحالية على هيئة تساؤل رئيس كما يلي:

ما هي الآليات المختلفة للجوانب الإجرائية والتشريعية للضبط القانوني العربي والدولي حيال جرائم تقانة المعلومات؟

تساؤلات الدراسة

تطرح الدراسة الحالية مجموعة من التساؤلات الفرعية التالية:

١) ما هو مفهوم الانترنت وشبكات التواصل الإجتماعي؟ وما هي المراحل التاريخية لتطور جرائم تقانة المعلومات؟

٢) ما هي التصنيفات المختلفة لتقانة المعلومات ؟ وما هي أسبابها وخصائصها؟

٣) ما هي الأبعاد المختلفة لجرائم الإنترنت والمعلوماتية في الدول العربية والغربية؟

٤) ما أبرز المعوقات التشريعية والقانونية المتعلقة بجرائم تقانة المعلومات ؟

٥) ما هي تدابير الضبط القانوني العربي والدولي في مجال مكافحة جرائم تقانة المعلومات ؟

أهمية الدراسة

يمكن تحديد أهمية هذه الدراسة في ضوء الاعتبارات التالية:

١- حداثة موضوع الدراسة على المستوى العربي ، إذ يجد الباحث ندرة في الكتابات الاكاديمية العربية التي سعت للخوض في هذا الموضوع.

٢- يستمد هذا الموضوع أهميته من طبيعة هذه الجرائم ودورها، فهذه الجرائم تعد حديثة على المجتمع العربي، وتحتاج للمزيد من الإهتمام والدراسة.

٣- الوقوف على بعض الجوانب والنقاط المهمة والمؤثرة في جرائم التواصل الاجتماعي، وعلاقتها بخلق عوالم جديدة من التحديات أمام القضاء العربي والعالمي.

٤- تمهيد الطريق أمام إجراء عدد من الدراسات التي تناولت الموضوعات المماثلة لموضوعنا هذا بصورة علمية وشاملة والتي تضيف المزيد من المتغيرات المؤثرة في هذه الدراسة، بما يسهم في تحقيق التراكم المعرفي والبحث.

مراجعة الأدبيات السابقة

يمكن تناول الدراسات السابقة ذات الصلة بموضوع الدراسة من خلال الاستناد الى محورين اساسيين على النحو التالي:

أولاً: الدراسات المتعلقة بمواقع التواصل الاجتماعي

ثانيا: الدراسات المتعلقة بتأثير الانترنت وشبكات التواصل الإجتماعي على الشباب

ومن ثم يمكن تناول المحاور السابقة على النحو التالي:

اولا: الدراسات المتعلقة بمواقع التواصل الإجتماعي

هناك عدة دراسات تطرقت لأثر استخدام مواقع التواصل الاجتماعي ، وفيما يلي عرض موجز لبعض الدراسات التي تناولت موضوع الدراسة:

١- دراسة أرين كاربنسكي(Aren karbsky 2017)[1]

هدف الدراسة: هدفت للتعرف إلى أثر استخدام موقع "فيس بوك" على التحصيل الدراسي لدي طلبه الجامعات، وقد طبقت الدراسة على (٢١٩) طالبا جامعيا.

نتائج الدراسة

[1] **Aren karbiniski (2017) face book and the technology revolution N , Y cestrum publications**

أظهرت النتائج أن الدرجات التي يحصل عليها طلاب الجامعات المدمنون على شبكة الانترنت وتصفح موقع "فيس بوك" أكبر الشبكات الاجتماعية، على الانترنت أدني بكثير من تلك التي يحصل عليها نظراؤهم الذين لا يستخدمون هذا الموقع، كما أظهرت النتائج أنه كلما أزداد الوقت الذي يمضيه الطالب الجامعي في تصفح هذا الموقع كلما تدنت درجاته في الامتحانات.

كما بينت النتائج أن الأشخاص الذي يقضون وقتا أطول على الانترنت يخصصون وقتا أقصر للدراسة مشيرا إلى أن لكل جيل اهتمامات تجذبه، وأن هذا الموقع يتيح للمستخدمة الدردشة وحل الفوازير وإبداء رأيه في كثير من الأمور والبحث عن أصدقاء جدد أو قدامي، وبينت النتائج أن (٧٩%) من الطلاب الجامعيين الذين شملتهم الدراسة اعترفوا بأن إدمانهم على موقع الفيس بوك أثر سلبيا على تحصيلهم الدراسي.

٢- دراسة ميشيل فانسون (Mwshel ,2016)[1]

هدف الدراسة: التعرف على أثر استخدام شبكات التواصل الاجتماعي على العلاقات الاجتماعية، وقد طبقت الدراسة على عينة بلغ قوامها (١٦٠٠) شاب من مستخدمي شبكات التوصل الاجتماعي في بريطانيا.

نتائج الدراسة

أظهرت النتائج أن أكثر من نصف الأشخاص البالغين الذين يستخدمون مواقع من بينها (الفيس بوك وبيبو ويوتيوب) قد اعترفوا بأنهم يقضون وقتا أطول على شبكة الانترنت من ذلك الوقت الذي يقضونه مع أصدقائهم الحقيقيين أو مع أفراد أسرهم.

وأظهرت الدراسة أيضا أنهم يتحدثون بصورة أقل عبر الهاتف، ولا يشاهدون التلفاز كثيرا، ويلعبون عددا أقل من ألعاب الكمبيوتر، ويرسلون كمية من الرسائل النصية وكذلك البريدية، وقد بينت الدراسة أنه نحو(٥٣%) من الذين شاركوا في الدراسة المسحية، بأن شبكات التواصل الاجتماعي على شبكة الانترنت تسببت بالفعل في تغيير أنماط حياتهم، وكشفت الدراسة عن أن نصف مستخدمي الانترنت في بريطانيا هم أعضاء في أحد مواقع التواصل الاجتماعي، مقارنة، بـ (٢٧%٩ فقط في فرنسا، (٣٣%) في اليابان، و (٤٠%) في الولايات المتحدة.

٣- دراسة شركة (Eversave 2015)[2]

هدف الدراسة

التعرف على تأثير موقع الفيس بوك على المجتمع

نتائج الدراسة

---

[1] Michele. Vinson(2016) face book and the invasion of technological communities, N . Y Newyurk .

[2] Daved smoloon (2015) the impact of the use of face book on the building society in the context of globalization, N Y sprctrum puplication .

أظهرت نتائجها أن (٨٥%) من النساء يتعرضن لمضايقات على الفيس بوك، كما أظهرت النتائج كذلك أن (٨٠%) من النساء تأثرن بعادات المستخدمات على الفيس بوك وتجاربهن، وأن (٨٥%) من النساء اللواتي مثلن عينة الدراسة أعربن عن شعورهن بالضيق من أصدقائهن وصديقاتهن على الفيس بوك، وتعددت أوجه الضيق وتفاوتت بالنسبة لكل منهن، فجاءت الشكوى على الدوام كأحد أكثر الأمور التي تزعج المستخدمات على الفيس بوك من صديقاتهم وأصدقائهم بنسبة٦٣%ثم تبادل الآراء السياسية بنسبة (٤٢%) ثم التفاخر والإدعاء بعيش حياة هادئة ومثالية بنسبة (٣٢%) كما كشفت الدراسة أن (٩١%) من النساء عبرن عن تقديرهن الكبير للدور الاجتماعي الكبير الذي يلعبه الفيس بوك في حياتهن وتحديدا إمكانية تبادل ومشاركة الفيديوهات والصور الخاص بأصدقائهن، فيما عبرت(٧٦%) من هؤلاء بالإعجاب بقدرة "الفيس بوك" على لم شمل الأصداء وبخاصة الذين لم يتقابلوا أو يجتمعوا منذ مدة طويلة.

٤- دراسة التعيبي (٢٠١٤)[١]

هدف الدراسة: للتعرف على تأثير الفيس بوك على طلبة الجامعات السعودية.

نتائج الدراسة

إن نسبة انتشار استخدام الفيس بوك بين طلاب الجامعات السعودية وطالباتها بلغت٧٧% وأن دور الأهل والأصدقاء وتأثيرها في التعرف عليه بدافع تمضية الوقت، كعامل رئيس لاستخدامه، حيث جاء هذا العامل في المرتبة الأولي في الإشاعات المتحققة من استخدامه وخلصت العينة إلى أن الفيس بوك حقق ما لم تحققه الوسائل الإعلامية الأخرى، وأن استخدام الفيس بوك كان له تأثيره على الشخصية أكثر من الوسائل الإعلامية الأخري.

ثانيا: الدراسات المتعلقة بتأثير الانترنت وشبكات التواصل الإجتماعي على الشباب

١- دراسة ناي واربنج Nie and Erbing (٢٠١٣) [٢]

هدف الدراسة:التعرف على اهمية الانترنت وفعالياته في الحياه المجتمعية

نتائج الدراسة

اكدت الدراسة ان الإنترنت يعتبر تقنية من التقنيات الحديثة ووسيلة من وسائل الاتصال مثله مثل كثير من الوسائل الأخرى. ولعل ما يميز الإنترنت عن غيره من وسائل الاتصال التكنولوجية الأخرى هو مستوى التفاعل الذي يجعل من المستخدمين الذين ينتشرون في أماكن متباعدة بالقيام بإرسال واستقبال ما يشاءون من المعلومات. فعندما نتحدث عن جهاز الحاسب الآلي والاستخدامات

---

[١] جارح التعيبي، (٢٠١٤) تأثير الفيس بوك على طلبة الجامعات السعودية رسالة ماجستير غير منشوره الرياض كلية الآداب جامعة الملك سعود

- [2] Nie, Norman and Erbing, Lutz (2013). Internet and Society: A Preliminary Report. Stanford Institute for the Quantitative Study of Society. Intersurvey Inc., and McKinsey and Co.

الخاصة بالإنترنت، فإننا نتحدث عن علاقات تفاعلية بين المستخدمين مع بعضهم البعض من جهة، وبين المستخدمين وجهاز الحاسوب من جهة أخرى. فلقد أثرت تكنولوجيا المعلومات هذه على كثير من النواحي الاجتماعية في حياة المجتمعات الحديثة. فدخلت هذه التكنولوجيا حاملة معها جملة من التفاعلات السلوكية الثقافية المرتبطة بها والتي أسهمت وتسهم بشكل مباشر في التأثير على الفرد والأسرة والمجتمع وذلك بحكم كونها مظهرا من مظاهر التغير المادي الذي أصاب كثير من المجتمعات المتحضرة.

٢- دراسة المزيدي وإسماعيل AL-Mazeedi and Ismail (١٩٩٨) [١]

هدف الدراسة

حاول الباحثان عرض بعض المتغيرات والخصائص الاجتماعية والتربوية على ٢٢٤ طالب وطالبة من جامعة الكويت غالبيتهم من كليتي الهندسة والعلوم ومن طلبة الفرقة الثالثة وأكثر، والتي تتراوح أعمارهم بين ٢٠ – ٢٣ عاماً.

نتائج الدراسة

ولعل من أبرز النتائج التي توصلت إليها الدراسة تتمثل في أن طلبة جامعة الكويت يستخدمون الإنترنت كوسيلة للاتصالات من خلال برنامجي المحادثة والبريد الإلكتروني (Email + I RC) ، وطلب بعض المعلومات التي ليست لها علاقة بموضوع دراستهم وتخصصاتهم أو بواجباتهم. وإن الطالبات يعتبرن أكثر استخداماً لشبكة الإنترنت من الطلبة الذكور. وأشارت الدراسة إلى أن غالبية الطلبة الذين يستخدمون الإنترنت في الجامعة يستخدمونه بمعدل ساعة واحدة يومياً بينما أغلب منازل المستجيبين غير مزودة بالإنترنت. إضافة إلى ذلك، فإن نصف العينة تقريباً يحادثون ويخاطبون الجنس الآخر، والتي تعتبر نسبة عالية مقارنه ببعض المجتمعات. ولقد أشارت الدراسة إلى أن ثلث العينة يقومون بإعطاء معلومات خاطئة عن أنفسهم عندما يتحدثون مع الآخرين عبر الشبكة، إضافة إلى أن نسبة كبيرة منهم يعتقدون بأن الإنترنت له تأثيره السيئ على الأخلاقيات والسلوك، وكثيرا منهم يرون بان درجاتهم ، وتحصيلهم الدراسي لا يتحسن من خلال استخدام شبكة الإنترنت. فالاستفادة محصورة على الاتصال دون طلب المعلومات وهذا الاتصال قد لا يولد فائدة مرجوة، وقد يتعارض مع السلوكيات والأخلاقيات العامة. فلقد أشارت هذه الدراسة إلى بعض من الجوانب والسلوكيات الاجتماعية السلبية لاستخدام الإنترنت لدى طلبة الجامعة.

٣- دراسة AL-Najran (١٩٩٨) [٢]

---

[1] Al-Mazeedi, Moosa, Ismail Ibrahim (1998). The Educational and Social Effect of the Internet on Kuwait University Students. In: Kuwait Conference on Information Highway. V:2 From : 16 – 18 March.

- [2 2] Al-Najran, Talal (1998). Internet adoption and use by Kuwait University students : new medium, same old gratifications. Unpublished Doctoral Dissertation. Ohio: The Ohio State University.

هدف الدراسة

إيجاد إجابات استكشافيه خاصة حول استخدام شبكه الإنترنت على عينه مقدارها ٥٩٨ طالباً وطالبة من جامعة الكويت، فلقد حاول الباحث تحديد الفئات المستفيدة وأغراض الاستخدام.

نتائج الدراسة

كان من ابرز النتائج التي توصل إليها الباحث في هذه الدراسة هو أن غالبية مستخدمي الشبكة هم أحد كليات الجامعة وهي من كلية الهندسة. وتتسم فئة المستخدمين لهذه التقنية بارتباطها مع بعض من الصفات والخصائص الشخصية مثل المهارة في استخدام برامج الحاسوب، والتميز بمعدلات عالية في الدراسة، والتميز بقدرة عالية على استخدام اللغة الإنجليزية . وخلص الباحث إلى ان فئة الأصدقاء تلعب دوراً بارزاً في انتشار استخدام الإنترنت كوسيلة تكنولوجية. فقد عكست الدراسة عن بعض السمات الإيجابية لمستخدمي الإنترنت. فاستخدامهم للإنترنت ارتبط ببعض المهارات والخصائص الإيجابية. فهي إشارة إلى حاجة استخدام مثل هذه التقنية بعض من المهارات الخاصة للمستخدم أو المستفيد.

٤- دراسة ليرى وحاجي (١٩٩٨)[١]

هدف الدراسة

تحديد بعض من المشكلات الاجتماعية والنفسية والصحية لمستخدمي الإنترنت

نتائج الدراسة

خلص الباحثان إلى أن اغلبيه المترددين على هذه المقاهي هم من الفئات السنية الصغيرة التي تتراوح أعمارهم بين ١٦ – ٣٠ سنة. وأن نسبة الذكور وغير المتزوجين هم الفئة الأكثر تردداً ومناسبا للتعارف مع الأصدقاء الجدد، وإن هناك أعراضاً صحية مضرة تتعلق بكثرة أعداد المدخنين واستخدام المنبهات بالنسبة لمستخدمي الجهاز. إضافة إلى أن هناك علاقة تفاعلية خاصة بين المستخدم وجهاز الحاسوب. حيث يتولد نوعاً عن الانشغال الذهني من قبل المستخدمين. ولقد أشارت الدراسة أيضا بأن كثير من أفراد العينة تميزوا بزيادة مشكلاتهم الأسرية ، واصبح كثير منهم أكثر توتراً في الأعصاب واتسامهم بعدم الصب. إضافة إلى ذلك، فهناك أيضا بعض التأثيرات على العين وإجهادها من كثرة استخدام الإنترنت.

٥- دراسة اللجنة العليا لاستكمال تطبيق أحكام الشريعة الإسلامية (١٩٩٧)[٢]

هدف الدراسة

---

[١] صالح ليري ومحمد حاجي (١٩٩٨) . أثر المشكلات الاجتماعية والنفسية المصاحبة لمستخدمة مقاهي الإنترنت : في مؤتمر الكويت حول الطرق السريعة للمعلومات : التقنية في خدمة المجتمع " . جـ ١ . ١٦ – ١٨ مارس . ص ص٢٠٥-٢١٨

[٢] الديوان الأميري . اللجنة الاستشارية العليا للعمل على استكمال تطبيق أحكام الشريعة الإسلامية (١٩٩٧) . شبكة الإنترنت : الفوائد وضوابط الاستخدام : الدراسة التحليلية . الكويت : مركز المعلومات والتوثيق .

التعرف على آراء ٢٧ شخصاً من المهتمين بعلوم الكمبيوتر، والمتعلقين به.

نتائج الدراسة

فلقد أشارت الدراسة على تأكيد المهتمين في مجال الكمبيوتر على أن استخدام الإنترنت له فوائد متعددة. فهو وسيلة عملية وأدبية تقدم المعرفة وتساعد الشخص المستفيد. فرأت ٧٣.١% من أفراد العينة بان متخذي القرار والمسئولين قد يستفيدوا من الإنترنت في مجال عملهم. ومن مجالاتها الإيجابية أيضا، إن الإنترنت يسهم في تنمية الأفراد والشعوب ، وانه يطرح قضايا مهمة وطنيه وعالمية. وكذلك يرى غالبيه المستجيبين بان استخدام هذه الشبكة يسهم في تنميه الوعي الديني الإسلامي، وممكن استغلالها في توعيه المجتمع الكويتي . وبالمقابل، فللإنترنت بعض المضار والجوانب السلبية المتعلقة به والخاصة بعملية عرض بعض من الجوانب غير الأخلاقية التي قد تؤثر في انحراف الشباب وتأثير الثقافة الغربية عليهم. إضافة إلى ذلك ، فلقد رأي كثيرين من أفراد العينة بان استخدام الإنترنت ممكن أن يضيع كثير من الحقوق الخاصة بحق الملكية الأدبية والعينية. ورأت غالبيه العينة على ضرورة وضع القيود والقوانين على المستفيدين من صغار السن.

المؤشرات التي أسفرت عنها الدراسات السابقة

استفاد الباحث من خلال البحث في الدراسات السابقة بلورة الأبعاد الموضوعية والمنهجية للمشكلة البحثية على النحو التالي:

١- بلورة المشكلة البحثية في إطار تحليل العلاقة بين جرائم الإنترنت وشبكات التواصل الإجتماعي وبين جوانب الضبط القانوني لتلك الجرائم.

٢- بيان أصالة البحث وأوجه النقص والخلل في الدراسات السابقة والتي سيغطيها هذا البحث، وبيان ما سيضيفه البحث للمعرفة وللعلم.

٣- الاستفادة من الدراسات السابقة في التعرف على الأخطاء التي وقع فيها الآخرون وتجنبها في البحث. الى جانب الاستفادة من الفرضيات والأهداف والنتائج، وأسئلة البحث الفرعية وتحديد المشكلة ونطاقها.

٤- الإطلاع والتعرف على أدوات التحليل وطريقة استخدامها. والاستفادة من المناهج التي استخدمت في الدراسات السابقة للتعرف على منهجية البحث وكيفية تحديد العينات.

٥- من خلال الدراسات السابقة حصل الباحث على فوائد تتعلق بما انتهى الآخرون وبما يراه من الأمور التي يبتدأ بها. كما فتحت الدراسات السابقة المجال للباحث للتعرف على أساليب القياس.

٦- الاستفادة من التعريفات والمصطلحات الحديثة التي قدمتها هذه الدراسات لعدد من المفاهيم العلمية الحديثة المتصلة بمشكلة البحث، والمتغيرات المختلفة التي تؤثر على كل مفهوم، خصوصاً مفهوم شبكات التواصل الاجتماعي وتقسيماتها المختلفة.

٧- الاستفادة من الدراسات السابقة في التعرف على طرق الربط بين العناصر والمشاهدات المختلفة

والعلاقات المتوقعة بين متغيرات الدراسة. الى جانب الاستفادة من الاقتراحات الموجودة في الدراسات السابقة حول الدراسات المستقبلية التي يمكن القيام بها.

الإطار المفاهيمي

يمكن تحديد ابرز المفاهيم التي ستتعرض لها الدراسة الحالية وذلك على النحو التالي:

١ـ شبكة الإنترنت

هي مجموعة من الشبكات المتصلة ببعضها البعض حول العالم لتبادل المعلومات فيما بينها. أي هي المنظومة العالمية التي تربط مجموعة من الحاسبات بشبكة واحدة وهي اختصار لكلمة internet work .

وقد بدأت شبكة الإنترنت في الولايات المتحدة الأمريكية شبكة عسكرية للأغراض الدفاعية . ولكن بانضمام الجامعات الأمريكية ثم المؤسسات الأهلية والتجارية – في أمريكا وخارجها – جعلها شبكة عالمية تستخدم في شتى مجالات الحياة.

٢ – شبكات التواصل الإجتماعي

الشبكات الاجتماعية هي مصطلح يطلق على مجموعة من المواقع على شبكة الإنترنت ظهرت مع الجيل الثاني للويب أو ما يعرف باسم ويب ٢.٠ تتيح التواصل بين الأفراد في بيئة مجتمع افتراضي يجمعهم حسب مجموعات اهتمام أو شبكات انتماء (بلد ، جامعة ، مدرسة ، شركة ... إلخ) كل هذا يتم عن طريق خدمات التواصل المباشر مثل إرسال الرسائل أو الاطلاع على الملفات الشخصية للآخرين ومعرفة أخبارهم ومعلوماتهم التي يتيحونها للعرض .

تصنّف مواقع الشبكات الاجتماعية ضمن مواقع الويب ٢.٠ لأنها بالدرجة الأولى تعتمد على مستخدميها في تشغيلها وتغذية محتوياتها. كما تتنوّع أشكال وأهداف تلك الشبكات الاجتماعية، فبعضها عام يهدف إلى التواصل العام وتكوين الصداقات حول العالم وبعضها الآخر يتمحور حول تكوين شبكات اجتماعية في نطاق محدد ومنحصر في مجال معين مثل شبكات المحترفين وشبكات المصورين ومصممي الجرافكس .

وخدمات الشبكات الاجتماعية هي خدمات تؤسسها و تبرمجها شركات كبرى لجمع المستخدمين والأصدقاء ومشاركة الأنشطة والاهتمامات أ،و للبحث عن تكوين صداقات و البحث عن اهتمامات و أنشطة لدى أشخاص آخرين .

معظم الشبكات الاجتماعية الموجودة حالياً هي عبارة عن مواقع ويب تقدم مجموعة من الخدمات للمستخدمين مثل المحادثة الفورية و الرسائل الخاصة و البريد الإلكتروني و الفيديو و التدوين و مشاركة الملفات و غيرها من الخدمات . و من الواضح أن تلك الشبكات الاجتماعية قد أحدثت تغيّر كبير في كيفية الاتصال و المشاركة بين الأشخاص و المجتمعات و تبادل المعلومات . و تلك الشبكات الاجتماعية تجمع الملايين من المستخدمين في الوقت الحالي و تنقسم تلك الشبكات الاجتماعية حسب

الأغراض فهناك شبكات تجمع أصدقاء الدراسة و أخرى تجمع أصدقاء العمل بالإضافة لشبكات التدوينات المصغرة ، و من أشهر الشبكات الاجتماعية الموجودة حالياً فيس بوك و ماي سبيس و تويتر و لايف بوون و هاي فايف و أوركت و الشبكة العربية عربيز .

تقسيم البحث

يأتي تقسيم البحث الحالي على النحو التالي:

المبحث الأول: جرائم تقانة المعلومات.. المفهوم والنشأة والتطور

المطلب الأول: الانترنت وشبكات التواصل الإجتماعي .. المفهوم والتطور

المطلب الثانى: نشأة وتطور جرائم تقانة المعلومات

المبحث الثانى: جرائم تقانة المعلومات... تعريفها.. أسبابها..خصائصها..تصنيفها

المطلب الأول: تعريف جرائم تقانة المعلومات وأسبابها وخصائصها

المطلب الثاني: تصنيف جـرائم تقانة المعلومات

المبحث الثالث: جرائم تقانة المعلومات في الدول العربية والغربية

المطلب الأول: جرائم الإنترنت والمعلوماتية في الدول العربية وأساليب مكافحتها

المطلب الثاني: جرائم تقانة المعلومات فى الدول الغربية

المبحث الرابع: الجوانب الإجرائية والتشريعية للضبط القانوني والدولي حيال جرائم الإنترنت

المطلب الأول: المعوقات التشريعية والقانونية المتعلقة بجرائم تقانة المعلومات

المطلب الثاني: تدابير الضبط القانوني العربي والدولي في مجال مكافحة جرائم تقانة المعلومات

المبحث الأول
جرائم تقانة المعلومات
المفهوم والنشأة والتطور

مقدمة

أحدثت التطورات التكنولوجية الحديثة في منتصف عقد التسعينات من القرن الماضي، نقلة نوعية وثورة حقيقية في عالم الاتصال، حيث انتشرت شبكة الإنترنت في كافة أرجاء المعمورة، وربطت أجزاء هذا العالم المترامية بفضائها الواسع، ومهدت الطريق لكافة المجتمعات للتقارب والتعارف وتبادل الآراء والأفكار والرغبات، واستفاد كل متصفح لهذه الشبكة من الوسائط المتعددة المتاحة فيها، وأصبحت أفضل وسيلة لتحقيق التواصل بين الأفراد والجماعات، ثم ظهرت المواقع الإلكترونية والمدونات الشخصية وشبكات المحادثة، التي غيرت مضمون وشكل الإعلام الحديث، وخلقت نوعاً من التواصل بين أصحابها ومستخدميها من جهة، وبين المستخدمين أنفسهم من جهة أخرى.

وهذه المواقع هي عبارة عن صفحات ويب على شبكة الإنترنت، يخصص بعضها للإعلان عن السلع والخدمات أو لبيع المنتجات، والبعض الآخر عبارة عن صحيفة إلكترونية تتوفر فيها للكتاب إمكانية للنشر، وللزوار كتابة الردود على المواضيع المنشورة فيها، وفرصة للنقاش بين المتصفحين، وكذلك مواقع للمحادثة (الدردشة)، وهناك المدونات الشخصية التي يجعلونها أصحابها كمحفظة خاصة يدونون فيها يومياتهم، ويضعون صورهم ويسجلون فيها خواطرهم واهتماماتهم.

ومن ثم فنتناول هذا الفصل من خلال مطلبين رئيسيين أما المطلب الأول فقد ركز على تعريف الإنترنت وشبكات التواصل الإجتماعي المختلفة، فيما اختص المطلب الثاني بتناول نشأة وتطور جرائم تقانة المعلومات.

المطلب الأول

الانترنت وشبكات التواصل الإجتماعي، المفهوم والتطور

لاشكّ أنّ ملامح الحياة البشريّة قد تغيّرت تغيّرات جوهريّة ملموسة مع تطوّر وسائل الاتصال الحديثة والمعاصرة. فعلى سبيل المثال، قد حلّت الرسائل الإلكترونيّة محلّ الرسائل الخطيّة، وشاركت "غرف الدردشة" الإلكترونيّة الجلسات والمجالس العائليّة والاجتماعيّة، ولم يعد السفر شرطاً لرؤية الأصدقاء أو سماع أصواتهم أو للبيع والشراء أو الدراسة.

ولا سبيل إلى اختزال كل ما وقع من تغيّرات تجاوزت البشريّة من خلالها حدود الزمان والمكان والجغرافيا، ولا إلى الإسهاب في تناول وسائل الاتصال الحديثة – تاريخها وتطوّرها وأنواعها وتأثيراتها. من آثار تلك التقنيات والوسائل نشأة ما أصبح يعرف بالفضاء الإلكتروني أو الرمزي cyberspace الذي يضمّ عدداً كبيراً من المجتمعات الافتراضية – بداية من غرف الدردشة والمجموعات البريدية وانتهاء بتويتر Twitter والفيسبوك، وغيرهما من مواقع التواصل الاجتماعي[1].

ومن ثم يسعى هذا المبحث للتعرض للمفاهيم الرئيسة لشبكة المعلومات الدولية " الانترنت" وكذلك مواقع التواصل الإجتماعي على النحو التالي:

أولا: تعريف الانترنت

الانترنت International Network/ Internet "هي تلك الوسيلة او الأداة التواصلية بين الشبكات دون اعتبار للحدود الدولية". وهذا التعريف يجعلنا نقف لا على طبيعة الانترنت وإنما على حقيقتها. إذ أن الانترنت من طبيعة تقنية- انسانية فهي نتاج اجتماع التقنية والمعلومات، ثم إنها في حقيقتها وسيلة تواصل بين الشبكات.

والاتصال الذي تحدثه الانترنت هو مجرد أحداث عملية تماس بين شبكة فأكثر او عملية انتقال، حيث يكون ملقم المستخدم، الى شبكة أخرى أينما كانت، وعليه فالإنترنت في الحقيقة كأداة تواصلية ينتهي دورها بمجرد الدخول الى شبكة الغير.

ويمكن تناول أهم خصائص شبكة المعلومات الدولية "الانترنت" من خلال ما يلي:

١- الانترنت وسيلة تواصلية

وهنا يأتي دور التقنية ، إذ أن عددا من أجهزة الحاسوب (أكثر من جهاز) متصلة ببعضها البعض ، تخلق نظاما System اتصاليا ، وعدة أنظمة متصلة ببعضها تخلق شبكة ، وعدة آلاف من الشبكات (منطلقة من المحلية LAN الى العالمية WAN) متصلة بشكل عنكبوتي (غير منظم او عشوائي)

[1] د. بهاء الدين محمد مزيد، المجتمعات الافتراضية بديلا للمجتمعات الواقعية. كتاب الوجوه نموذجا، الامارات، جامعة الامارات العربية المتحدة، قسم دراسات الترجمة،ص.٣

ببروتوكول اتصالي انفتاحي هو (T C P / I P) المنظم للاتصال بين اجهزة الحاسوب عبر الانترنت نكون قد وصلنا الى نقطة اللا مركزية وبالتالي يتم التواصل بين هذه الشبكات والأجهزة. وهذا كله تعبير عن التواصل بين الشبكات بحيث يبرز الدور الاتصالي الذي تقوم به التقنية تعبيرا عن تلك الوسيلة / الانترنت .

٢ـ الانترنت تستلزم المعلومات

إذ إنه بدون النظام المعلوماتي التبادلي بين الشبكات ، فإن الانترنت تصبح منهجا بدون موضوع ، حتى في افتراض التخصص والسرية والتشفير ـ وهو أمر موجود حاليا الا إنه مخترق ـ فإن الانترنت كانت قد خلقت نظاما تواصليا بين الشبكات هدفه تبادل المعلومات . فليست للتقنية قيمة في ذاتها وإنما هي وسيلة الى تنظيم العمل بموضوع ما والاستفادة منه . فهي كما الفلسفة منهج بدون موضوع ، فإذا أضفنا المعلومات كموضوع للتقنية فإننا نكون بصدد الانترنت. ولأجل ذلك فإن المعلومة Information ذات أهمية قصوى في اطار عمل الشبكة ، فهي سيدة الموقف عبر الانترنت . والمعلومة تحتاج الى الإنسان لكي يضعها ، والإنسان بحاجة الى دعم مادي ومعنوي في حمايته لهذه المعلومة يصل في بعض الاحيان هذا الدعم الى ضرورة التدخل ، ليس الحكومي فقط في اطار دولته وإنما الى الدعم ذي البعد الدولي على عمومه ايضا . ومن الضروري القيام في اطار التعاون الدولي من رصد اتفاقيات وتجديد تلك النافذة لحماية نظم المعلومات عبر الانترنت[١].

ومن أهم مظاهر الحماية الواردة على النظام المعلوماتي عبر الانترنت تلك الدعوة التي برزت في مقدمة عمل البيت الابيض الأمريكي حول التجارة الالكترونية White house paper on electronic commerce الصادرة في ٣٠ / ٦ / ١٩٩٧، وكذلك أعلان بون Bonn Declaration الصادر في ٢٤ / ١١ / ١٩٩٧ حول الادارة الذاتية او التنظيم الذاتي للعالم الافتراضي Cyber self - government عبر الانترنت بقصد التعرف الذاتي على الأحكام واستخلاص النظم، وهى دعوة يوجد لها أساس تاريخي، فقد نادى بها منذ اكثر من نصف قرن الأستاذ الإيطالي جورجيو ديل فيكيو/ أستاذ فلسفة القانون ومدير جامعة روما الذي وان كان يؤيد قاعدة أن الدولة هي صاحبة السمة الوضعية للقانون إلا أنه مع ذلك لم يمانع في التصريح بقبول الأنظمة القانونية التي تبتكرها المنظمات الخاصة في اطار الدولة ما دامت تعمل في اطار النظام الوضعي القائم. فكان البروفيسور ديل فيكيو من الاوائل الذين قاموا بطرح موضوع الحوكمة Governance وهي من الموضوعات التي تأثرت بها فلسفة هيكلة المجتمع المعلوماتي القائم.

٣ـ شبكة الانترنت عابرة للحدود الدولية

هذا العنصر يثير الكثير من المفاهيم وبالتالي الجدل حول الانترنت. ويكمن السبب الرئيسي في أن الانترنت ليست لها حدود دولية ولا تعترف كذلك بتلك الحدود القائمة بين الدول كما إنها ليس لها مالك

---

[١] راجع: د. محمد فهمى طلبه وآخرين، الحاسبات الالكترونية حاضرها ومستقبلها، موسوعة دلتا للكمبيوتر، مطابع الكتاب المصرى الحديث ١٩٩٢.

وليس هناك جهاز رقابي عليها ولا سلطة مركزية تتحكم فيها، ويعني هذا في حقيقة الأمر إنه كما يمكننا الدخول الى شبكات الغير فإن الغير ايضا يستطيع الدخول الى الشبكات الخاصة بنا وكذلك حواسيبنا ويستوي هنا أن يكون هذا الغير عدوا ام صديقا.

ولا يعني مثل هذا الأمر أن هناك تعارضا بين الانترنت وبين فكرة الدولة، إذ أن هذا الأمر ليس له وجود البتة، بل الحقيقة أن ظاهرة الانترنت العلمية هى ظاهرة دولية في الاساس من حيث انعدام مركزيتها بما يتساوى أمامها الدول الكبيرة والصغيرة، فما يحكم الانترنت هو القدرة المعلوماتية وسوف يأتي الوقت الذي يكون فيه التوثيق المعلوماتي والقدرة الإيجابية على التوثيق له قيمة مادية كبيرة بما يتساوى مع النفط وغيره من المركبات ذات القيمة الاقتصادية المادية بل أبعد من ذلك سوف يظهر أيضا ـ وهو ما بدأت تبرز في الأفق بوادره ـ مستويات اجتماعية واقتصادية مختلفة أكثرها تمييزا من يملك مصادر معلومات أكثر والتي تشكل قواعد بيانات لتحميلها Upload على الانترنت.

والتقسيم الراجح للانترنت والمعبر عن حركتها هو التقسيم الثلاثي على النحو التالي:

- شبكة المعلومات الدولية World Wide Web .
- البريد الإلكتروني Electronic Mail .
- الاتصال المباشر Direct Connection.

وهذه الأقسام الثلاثة لا تُعد في حقيقة الامر منتهى الحركة في الانترنت وإنما فقط ما هو موجود حاليا من أقسام لها، إذ يمكن أن تتزايد معدلات حركة الاستخدام لقسم جديد فتتزايد هذه الأقسام. ولعل الملاحظ على هذا التقسيم انه ليس هناك فاصل كلي بين هذه الأقسام، فهي متداخلة فيما بينها، لذلك يصعب ملاحظتها، فيستطيع مستخدم الانترنت أن يتصفح او يبحر وفي ذات الوقت يرسل رسالة إلكترونية وكذلك يتحادث مباشرة مع أشخاص في دول أخرى، وربما يأتي اليوم فتتجاوز الانترنت المجال الأرضي الى الكواكب الأخرى التي تدور حول الكرة الأرضية، وهو أمر ليس بعيد الاحتمال إذا استشعرنا مدى القدرة الإيجابية التي عليها الانترنت والمفارقة الحادثة في فكرة الأدب المعلوماتي/ الخيال العلمي بعد أن كان مجرد خيال أصبحت تصوراته ممكنة وأضحى العقل البشري منشغلا به، فيستطيع شخص في الرياض او نيويورك او بنغازي او القدس او طرابلس او بيروت او القاهرة الاتصال بأشخاص على القمر الآن والتحادث مباشرة معهم وبث رسالة إلكترونية الى آخرين في مكوك فضائي ... الخ.

<u>ثانيا: شبكات التواصل الإجتماعي</u>

لقد تزايد الاهتمام الأكاديمي بقضايا الشبكات الاجتماعية والمجتمع الافتراضي منذ أن شكل الإنترنت فضاءه المعلوماتي ونجاحه في تأسيس جماعاته الافتراضية، ويرجع المفهوم إلي هاوارد رينجولد Rhngold(١٩٩٣) الذي كتب الكتاب الأول والرائد في هذا السياق بعنوان المجتمع الافتراضي virtual community والذي عرف المجتمع الافتراضي علي أنه تجمعات اجتماعية تشكلت من أماكن متفرقة في أنحاء العالم يتقاربون ويتواصلون فيما بينهم عبر شاشات الكمبيوتر والبريد

الإلكتروني يتبادلون المعارف فيما بينهم ويكونون صداقات يجمع بين هؤلاء الأفراد اهتمام مشترك ويحدث بينهم ما يحدث في عالم الواقع من تفاعلات ولكن ليس عن قرب ،وتتم هذه التفاعلات عن طريق آلية اتصالية هي الإنترنت الذي بدوره ساهم في حركات التشكل الافتراضية[1] .

"ويشكل المجتمع الافتراضي مجالا لنمو الشبكات الاجتماعية ، ويشكل الفضاء المعلوماتي cyber space الحيز والإطار الذي تتم في سياقاته تجميع خيوط الشبكات الاجتماعية، فقد عرفه نبيل علي أنه " فضاء جديد تتفاعل فيه الجماعات وتمارس فيه الصفقات وتقام فيه المؤسسات والمتاحف والمعارف ومنافذ البيع تعقد فيه التحالفات وتحاك فيه المؤتمرات تنقل فيه المعلومات بسرعة فائقة ورغم محاكاته لفضاء الواقع إلا أنه يختلف في طبوغرافيته وطبيعته وقوانينه وأعرافه عن فضاء الواقع فليس هناك سلطة مركزية تحكمه أو جهة رقابية تراجعه بل مجرد لجان أو مجموعات غير حكومية"[2]. كما عرفه أحمد زايد بأنه العالم الفضائي غير المرئي وغير المرتبط بمكان وزمان والذي تتداول داخله المعلومات الإلكترونية"[3].

ومن الطرح السابق، يبدو أن هناك إعادة تشكل لقضايا المجتمع والسياسة علي نحو افتراضي ، فلقد نجح الإنترنت في تسهيل التفاعلات الاجتماعية ليس علي مستوي الإفادة فحسب ولكن علي مستوي الشبكات الاجتماعية . فلقد عرف السون وبويد Boyd ، Ellson الشبكات الاجتماعية علي أنها " مواقع تتشكل من خلال الإنترنت تسمح للأفراد بتقديم لمحة عن حياتهم العامة ، وإتاحة الفرصة للاتصال بقائمة المسجلين ، والتعبير عن وجهة نظر الأفراد أو المجموعات من خلال عملية الاتصال ، تختلف طبيعة التواصل من موقع لآخر"[4] . ولقد عرفت الشبكات الاجتماعية علي أنها " مجموعة من المواقع علي شبكة الإنترنت ظهرت مع الجيل الثاني للويب web 2 تتيح التواصل بين الأفراد في بنية مجتمع افتراضي يجمع بين أفرادها اهتمام مشترك أو شبة انتماء (بلد – مدرسة – جامعة – شركة ...الخ) يتم التواصل بينهم من خلال الرسائل أو الاطلاع علي الملفات الشخصية ،ومعرفة أخبارهم ومعلوماتهم التي يتيحونها للعرض . وهي وسيلة فعالة للتواصل الاجتماعي بين الأفراد سواء كانوا أصدقاء نعرفهم في الواقع أو أصدقاء عرفتهم من خلال السياقات الافتراضية "[5] .ولقد أوجز

---

[1] Haward Rhingold ,Virtual Community, http//:www .com .user/h(R)Vcboal accessed in 1/4/2021

[2] موسى جواد الموسوي و آخرون: الإعلام الجديد تطور الأداء و الوسيلة و الوظيفة، مكتبة الإعلام المجتمع، بغداد، ط ١، ٢٠١١،ص٤٧. كذلك وائل مبارك خضر فضل الله: اثر الفيسبوك على المجتمع، المكتبة الوطنية للنشر، الخرطوم، ط١، ٢٠١١، ص ٢٠.

[3] -أحمد زايد ، عولمة الحداثة وتفكيك الثقافات الوطنية،عالم الفكر،مجلد ٣٢، الكويت ، يوليو، سبتمبر، ٢٠٠٢ ، ص١٦.

[4] Danah M. Boyd, Nicole B.Ellison , Social Network Sites; Definition , History and Scholar Ship , Journal Of Computer Mediated Communication , vol(13),issue (1), 2014, P.P.8-10

http://icmc.indiana.edu/vol13issue1 /boyd.ellison.html

[5] مواقع الشبكات الاجتماعية وطريقة عملها ، وحدة المعرفة ، جوجل ، ٢٠٠٩ متاحة في http://knol.google .com مواقع الشبكات الاجتماعية وطريقة عملها

Swite(٢٠٠٩) مفهوم الشبكات الاجتماعية في أنها منظمة عصرانية غيرت في أسلوب الحياة من حيث الأسلوب والإدارة والممارسة "[١].

تتعدد الخدمات التي تبثها الشبكات الاجتماعية ، والدلائل علي مدي العموم والانتشار من حيث أعداد الشبكات أو المستخدمين يؤكد علي أنها تقدم خدمات تستدعي الاهتمام ومن أبرز الخدمات التي تقدمها الشبكات الاجتماعية:[٢]

١- الملفات الشخصية أو صفحات الويب: وهي ملفات تمكن من خلالها الفرد من كتابة بياناته الأساسية مثل الاسم والسن وتاريخ الميلاد والبلد والاهتمامات والصور الشخصية ، ويعد الملف الشخصي هو بوابة الوصول إلي عالم الشخص.

٢- الأصدقاء أو العلاقات : وهي خدمة تمكن الفرد من الاتصال بالأصدقاء الذي يعرفهم في الواقع ، أو الذين يشاركونه نفس الاهتمام في المجتمع الافتراضي . وتمتد علاقة الشخص ليس فقط بأصدقائه ولكن تفتح الشبكات الاجتماعية فرصة للتعارف مع أصدقاء الأصدقاء بعد موافقة الطرفين.

٣- إرسال الرسائل: تسمح هذه الخدمة بإرسال الرسائل سواء إلي الأصدقاء الذين في قائمة الشخص ، أو غير الموجودين في القائمة.

٤- البومات الصور: تتيح هذه الخدمة للمستخدمين إنشاء عدد لا نهائي من الألبومات ورفع مئات الصور ، وإتاحة المشاركات لهذه الصور للاطلاع عليها وتحويلها أيضا.

٥- المجوعات: تتيح الشبكات الاجتماعية فرص تكوين مجموعات الاهتمام ، حيث يمكن إنشاء مجموعة بهدف معين أو أهداف محددة ، ويوفر موقع الشبكات لمؤسس المجموعة أو المنتسبين والمهتمين بها مساحة من الحرية أشبه بمنتدى حوار مصغر ، كما تتيح فرصة التنسيق بين الأعضاء في الاجتماعات من خلال ما يعرف باسم Events ودعوة الأعضاء لتلك المجموعات ، ومعرفة عدد الحاضرين وأعداد غير الحاضرين[٣].

٦- الصفحات: ابتدع هذه الفكرة موقع face bock وتم استخدامها علي المستوي التجاري بشكل فعال ، حيث تسمح هذه الخدمة بإنشاء حملات إعلانية موجهة تتيح لأصحاب المنتجات التجارية فرصة عرض السلع أو المنتجات للفئات الذي يحددونها ، ويقوم موقع الفيس بوك باستقطاع مبلغ مع كل نقرة يتم التوصل إليها من قبل المستخدم[٤].

---

[1] O.C.Mcswete, The Challenge Of Social Networks, Administrative Theory and praxis, vol 13 , issue 1 , march , 2009 , p 95-96.

[٢] جمال معتوق وشريهان كريم: دور شبكات التواصل الاجتماعي في صقل سلوكيات و ممارسات الأفراد في المجتمع، ملتقى دولي حول شبكات التواصل الاجتماعي و التغير الاجتماعي، الجزائر، بسكرة ٩-١٠ ديسمبر ٢٠١٢،ص.ص. ٤-٥

[٣] مشري مرسي: شبكات التواصل الاجتماعي الرقمية نظرة في الوظائف، مجلة المستقبل العربي، لبنان، العدد ٣٩٥، يناير ٢٠١٢، ص ١٥٧.

[٤] سليمة رابحي، الحملات الانتخابية و شبكات التواصل الاجتماعي في الجزائر بين وسائط الاتصال الجديدة و أنماط التبليغ التقليدية، ملتقى دولي حول شبكات التواصل الاجتماعي، بسكرة، ٩/١٠ سبتمبر ٢٠١٢

وقد ارتبط تنوع الخدمات التي تقدمها الشبكات الاجتماعية في محيط الإنترنت بتنوع آخر يتمثل في تنميط الشبكات الاجتماعية . في هذا الصدد ليس من المنطقي أن نتحدث عن الشبكات العربية لان المجتمع الافتراضي هو مجتمع منفتح يضم في سياقاته الرحبة التفاعلات علي الصعيد العالمي ، ولكن يمكن الإشارة علي استحياء إلي أنماط الشبكات الاجتماعية علي النحو التالي[1]:

١- شبكات أساسية: وهي التي يمكن وصفها بالشبكات الاجتماعية العامة، والتي تضم ملفات شخصية للمستخدمين وخدمات عامة تتمثل في المراسلات الشخصية ومشاركة الصور والملفات الصوتية والمرئية والروابط والنصوص.

٢- شبكات عمل: وهي ليست شبكات ذات طابع عام وهي نمط من الشبكات ينصب اهتمامه علي المحترفين وترتبط بأصحاب الأعمال والشركات وتتضمن ملفات شخصية للمستخدمين تتضمن علي سيرتهم الذاتية وانجازاتهم[2].

٣- شبكات المميزات الإضافية: هناك بعض الشبكات تتيح الفرصة أمام أعضائها في توفير مزايا إضافية تتمثل علي سبيل المثال في التدوين المصغر Micro blogging مثل موقع تويتر وبلارك.

٤- الشبكات العربية هناك بعض الشبكات الاجتماعية التي ظهرت مؤخرا علي الإنترنت ،ولكنها لم ترتقي إلي مستوي الخدمات التي تقدمها الشبكات العالمية الكبرى . ومن أمثلة الشبكات الاجتماعية العربية مكتوب وفايح وعربيز Arabiz التي ظهرت في عام ٢٠٠٩ وكانت مخصصة للعرب المقيمين في ألمانيا ثم انتشرت في الدول العربية

وعند الحديث عن مراحل تطور الشبكات الاجتماعية في الفضاء المعلوماتي تجدر الإشارة إلي مرحلتين أساسيتين : [3]

المرحلة الأولي : يمكن وصف هذه المرحلة بالمرحلة التأسيسية للشبكات الاجتماعية، وهي المرحلة التي ظهرت مع الجيل الأول للويب web 1 وتشهد هذه المرحلة علي البداية التأسيسية للشبكات ومن أبرز الشبكات التي تكونت في هذه المرحلة هي شبكة موقع sixdegrees.com وهو الموقع الذي يمنح فرصة للأفراد المتفاعلين في إطاره فرصة طرح حياتهم ولمحاتهم العامة وإدراج أصدقائهم وبدأت فكرة قوائم الأصدقاء عام ١٩٩٨.، واخفق هذا الموقع عام ٢٠٠٠. ومن المواقع التأسيسية للشبكات الاجتماعية أيضا موقع classmates.com ذلك الموقع الذي ظهر في منتصف التسعينات وكان الغرض منه الربط بين زملاء الدراسة . شهدت هذه المرحلة مواقع متعددة من أشهرها أيضا موقع

---

[1] خدمات الشبكات الاجتماعية ، متاحة في
خدمات الشبكات الاجتماعية http:// ar.wikipedia.org/wiki/ accessed in 2/4/2021

[2] White, H. et al. . Surfing the net in Later Life: A review of the Literature and Pilot Study of Computer use and Quality of life. Journal of Applied Gevontolog . Sept. V. 18 (3) 2015.

[3] تقرير نقاش لليونسكو، عالمية الإنترنت: وسيلة لبناء مجتمعات المعرفة وإعداد خطة للتنمية المستدامة لفترة ما بعد عام ٢٠١٥، النسخة العربية، ٢٠١٥،ص. ٣

live journal وموقع cyworldالذي أنشئ في كوريا وموقع Ryze الذي تبلور الهدف منه في تكوين شبكات اجتماعية لرجال الإعمال لتسهيل التعاملات التجارية[1] . وتجدر الإشارة في الطرح التالي أن أبرز ما ركزت عليه مواقع الشبكات الاجتماعية في بدايتها هي خدمة الرسائل القصيرة والخاصة بالأصدقاء ، وعلي الرغم من أنها وفرت بعض خدمات الشبكات الاجتماعية الحالية إلا أنها لم تستطع أن تدر ربح علي مؤسسيها ولم يكتب لكثير منها البقاء[2].

المرحلة الثانية: يمكن وصف المرحلة الثانية بأنها مرحلة اكتمال الشبكات الاجتماعية ، ويمكن

التأريخ للمرحلة الثانية بالموجة الثانية للويب web 2 والمقصود هنا أنها ارتبطت بتطور خدمات الشبكة . ويمكن أن نؤرخ لهذه المرحلة بانطلاقة موقع my space وهو الموقع الأمريكي المشهور . ثم موقع الفيس بوك .وتشهد المرحلة الثانية من تطور الشبكات الاجتماعية علي الإقبال المتزايد من قبل المستخدمين لمواقع الشبكات العالمية[3] .

ومن خلال استعراض تطور أعداد المستخدمين لمواقع التواصل الإجتماعي، كان العام ٢٠١٢ الأكثر في عدد المسجلين فيها بنسبة ١٧.٣ بالمائة، و١٤.١ بالمائة عام ٢٠١٣، و١٢.٥ بالمائة في العام التالي، و٩.٣ بالمائة في ٢٠١٥، بينما يتوقع أن تصل النسبة إلى ٨.٧ بالمائة هذا العام و٧.٤ عام ٢٠١٧ و٦.٨ في العام ٢٠١٨[4].

كما أن عدد الحسابات النشطة على وسائل التواصل الاجتماعي تصل إلى ١.٧ مليار حساب، من أصل ٢.١ مليار حساب، في حين أن عدد المستخدمين للإنترنت يصل إلى ٣ مليارات مستخدم، أي ما يعادل ٤٥ بالمائة من إجمالي عدد سكان الأرض.

ويوضح الجدول التالي نسبة الإقبال على مواقع التواصل الإجتماعي من عام ٢٠١٢ الى عام ٢٠١٧ وفق رؤية دراسة مجلة محرك البحث الأمريكية

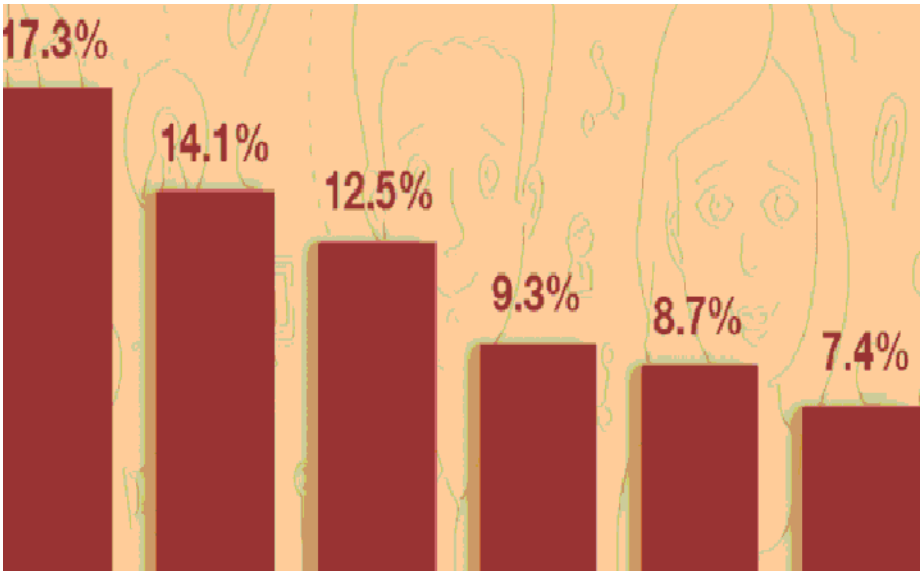
---

[1] Danah m. Boyd, Nicole B.Ellison , Social network sites; Definition , history and scholar ship ,op.cit. P. P. 6-7

[2] خالد غسان يوسف المقدادي، ثورة الشبكات الاجتماعية، دار النفائس للنشر، الأردن، ط ١،٢٠١٣،ص ٢٤.

[3] Wittkower, D:E. (October 1, 2010), Face book and Philosophy: What's on Y::our Mind?. USA: Open Court,p.p.12-14

[4] البيانات مشتقة من دراسة لمجلة محرك البحث وتم نشرها على موقع www.skynewsarabia.com تاريخ الدخول ٢٠١٦/٦/٢٠



ويتضح من خلال الطرح السابق أن الموجة الثانية للشبكات الاجتماعية ساهمت في جذب العديد من المتفاعلين علي مستوي العالم ، وتعد مواقع الشبكات الاجتماعية وسيلة للتواصل والتقاطع بين العالمية والمحلية . إذ أن الفكرة الأساسية التي تقوم عليها الشبكات الاجتماعية هي عالمية الاهتمامات ومحلية المردود . فالتفاعلات تتم علي خلفية السياق العالمي وتتبلور متغيراتها علي الصعيد المحلي[١]

[١] عبد الرزاق محمد الدليمي: الإعلام الجديد و الصحافة الالكترونية،دار وائل للنشر، ط١،الأردن،٢٠١١، ص ١٣ وما بعدها

المطلب الثانى

نشأة وتطور جرائم تقانة المعلومات

تاريخياً أرجع الفقه الجنائي جرائم الحاسوب إلى العام ١٩٦٠[١]. وأما جرائم الإنترنت فإنه يمكن القول إنها بدأت مع العام ١٩٨٨ وكانت أول الجرائم التي ترتبط عضوياً بالإنترنت هي جرائم العدوان الفيروسي فيما هو معروف في التاريخ القانوني بجريمة دودة موريس المؤخرة واقعتها في ٢ الحرث / نوفمبر ١٩٨٨.

ولا يزال الفقه والتشريع المقارن في حقيقة الأمر يستشعر الحرج في التمييز بين كل من جرائم الحاسوب وبين تلك الناجمة عن استخدام الإنترنت ، حتى إن تقرير الأمم المتحدة عن منع الجريمة عام ١٩٩٥ تبني الموقف المقارن المذكور هذا فصدر عنوان التقرير **Computer crimes & other crimes related to computer**

لذلك نجد أن تعريف جرائم الحاسوب في الفقه والتشريع يسوده اتجاه يجمع بين الجرائم التي تقع على الحاسوب ذاته وتلك التي يكون الحاسوب وسيلة ارتكابها، فهي لدي هذا الاتجاه تعرف بأنها "فعل غير مشروع يتورط نظام الحاسوب فيه، سواء كان الحاسوب كآلة هو موضوع الجريمة أو كان الوسيلة إلى ارتكابها أو مستودع الدليل المرتبطة بالجريمة". وهو تعريف مستمد من أكثر التعريفات شعبية لجرائم الحاسوب الذي قال به الأستاذ **Donn Parker** من حيث إن جرائم الحاسوب هي "جرائم تتطلب دراية ضرورية بالحاسوب لكي يتم ارتكاب الجريمة بنجاح"[٢]. ولم تأت الاتفاقية الأوروبية للجريمة عبر العالم الافتراضي المؤرخة ٢٠٠١/١١/٢٣ على تعريف محدد للجريمة عبر الإنترنت[٣]، وإنما اعترفت بنوعية من الجرائم يمكن ارتكابها عبر الإنترنت.

ولقد توسعت إدارة العدل الأمريكية في ربط الحاسوب بتقنيته فذهبت إلى تعريف جرائم الحاسوب بأنها "هي كل عدوان بالارتكاب على أي قانون يتضمن في محتواه تقنية الحاسوب ويكون عرضة للتحقيق والاتهام"[٤] كان ذلك بالطبع بتأثير من اتجاهات المشرع الأمريكي في تعديل ١٩٩٦ لقانون البنية

([1]) (SIEBER) Dr. Ulrich – Computer crimes & other crimes related to information technology rev. inter.de droit penal 1991 p. 1033.

([2]) Voir site : remp (the royal candian mounted police) " computer crimes is any illegal act which involves a computer systems whether the computer is an obect of crime, an instrument used to commit a crime or a respsitory of evidence related to a crime". Available online in feb. 2000 at: http://www.rcmp.com (mak d. rasch – criminal law and the internet – the internet and association. Copyright © 1996 by the computer law association, inc. p.6, donn parker of sri, is necessary for the successful commission of the offense.

([3]) Convention on CyberCrime – Explanatory Report, adopted on 8 Nov. 2001, op. cit.

([4]) (SCALION) Robert – crime on the internet, fall 1996, p. 1. "compuer crime is any violation of the law that involve a knowledge of computer technology for their

الوطنية للمعلومات The National Infrastructure Information Act (القسم ١٠٣٠)، الذي أستوحي التجريم من الربط بين الحاسوب وتقنيته ككل، فتمخض هذا الاتجاه عن وجود ثلاثة أنواع من الجرائم التي يمكن ارتكابها عر الحاسوب وذلك وفقاً للمنهج الأمريكي ، وهي [١] :

أولاً : الجرائم التي يكون الحاسوب هدفاً لها، وهي نوعية من الجرائم يكون هدف المجرم فيها التوصل إلى سرقة بيانات من الحاسوب أو إحداث إضرار به أو بنظام تشغيله أو بالشبكة التي يعمل خلالها.

ثانياً : الجرائم التي يكون الحاسوب وسيلة لارتكابها، وهذه النوعية من الجرائم تحدث عندما يستخدم المجرم الحاسوب لتسهيل ارتكاب بعض الجرائم التقليدية مثل الاحتيال على البنوك كما لو قام موظف بأحد البنوك باستخدام برمجية تحويل العملة لصالحه فيودع مبالغ محولة لحسابه عوضاً عن وضعها في مسارها الصحيح، وكذلك القيام بإعداد Produce أو نقل Transfer أو حيازة Possess آلة Device بما في ذلك الحاسوب بنية استخدامها في تزوير وثائق إثبات شخصية To Falsify Identification documentation (18 USCode Sec. 1028)

ولقد توسعت بعض التشريعات في مدلول مصطلح "أدوات التزوير Forgery Devices" لكي تشمل الحاسوب وملحقاته Equipment وبرمجياته Software إذا أعدت خصيصاً بغرض التزوير مثل قانون ولاية نيوجيرسي (N.J.Stat.ANN. Sec. 2 C : 21-1) ،

ثالثاً : الجرائم التي يكون فيها الحاسوب أداة لحفظ الأدلة دون أن يكون وسيطاً في الحصول عليها، كما هو الحال في قيام مروجي المخدرات والاتجار غير المشروع فيها، وكذلك معدي البرمجيات المعتدى على حقوق الملكية فيها وكذلك السرقة الإلكترونية التي تتم عدواناً على حقوق المؤلف بوضع سرقاتهم وملفاتهم وسجلاتهم في الحاسوب.

ومما تجدر الإشارة إليه إن مثل هذا التقسيم السالف ليس جامعاً مانعاً للتعبير عن جرائم الحاسوب، إذ هناك من الجرائم التي ترتكب بواسطة الحاسوب ومع ذلك لا يمكن إدراجها في أي من الأقسام أو الأشكال الثلاثة مثلما هو الحال في جريمة سرقة وقت الحاسوب مثلاً[٢] وهي جريمة يعرفها القسم Tit. 18 USCode Sec. 641 من التقنين الأمريكي كجريمة من جرائم المعلوماتية[٣].

---

perpetration, investigation, or prosecution" available online in feb. 2000 at : http://wings.buffallo.edu/complaw/complawpapers/scalion.html

- THOUMYRE - abuses in the cyberspace, op cit. P. 7

(١) ويلاحظ أن هذا التقسيم كان قد وضعه الأستاذ الدكتور جميل عبد الباقي في مؤلفه – الجرائم الناشئة عن الحاسب الآلي – تقرير مقدم إلى المؤتمر السادس للجمعية المصرية للقانون الجنائي – دار النهضة العربية القاهرة ١٩٩٢

(٢) د. جميل الصغير – الجرائم الناشئة عن استخدام الحاسب الآلي – المرجع السابق ، ص ٢٤

(3) United States v Sampsonm, 6 COMP, L. SERV. REP. 879 (N.D. Cal. 1978)

ففي هذه القضية فقد اعتبرت المحكمة أن الاستخدام غير المصرح به لحاسوب في مؤسسة حكومية Unauthorized use of computer time يشكل جريمة عدوان على أملاك الحكومة وفق ما هو مقرر في القسم Sec. 641 المشار إليه – انظر كذلك فيما يتعلق بالقسم ٦٤١ المذكور :

وربما يكون السبب في التوسع السالف عائداً إلى أن إمكانيات الحاسوب لم تبرز إلى الوجود بالشكل الذي يجب أن تكون عليه، فكل ما نعلمه عن قدرات الحاسوب يقل كثيراً عما نعلمه عن قدرات الإنترنت. فهذه الأخيرة، وإن كانت لم تأخذ حظها كما ينبغي، فقد تناولها الساسة وفقهاء القانون والاقتصاد على المستوي الإقليمي والدولي بكثير من الامل وهي بعد في بداياتها، في حين إن مسيرة الحاسوب تبدو هادئة أو طبيعية. ومثل هذا الأمر وجد له تأثير كبير في الاتفاقية الأوروبية للجريمة عبر العالم الافتراضي المؤرخة ٢٠٠١/١١/٢٣ حيث اعترفت الاتفاقية، في المادة الأولى منها، بمصطلح "نظام الحاسوب Computer System" ولم تأخذ في الاعتبار مجرد مصطلح "الحاسوب Computer" فقد حددت الاتفاقية هذا المصطلح بكونه يشمل "أية آلة أو مجموعة مرتبطة فيما بينها أو ذات علاقة من الآلات، يمكن بإضافة برمجية إلى واحد أو أكثر منها، أن تقوم بمعالجة آلية للبيانات"[١].

إننا إذن أمام مفارقة بين الحاسوب وبين أحد تقنياته. وهناك ما يميز الأثنين على الرغم من التعميم (الحاسوب) والتخصيص (الإنترنت). وهو تمييز يقوم على أكثر المظاهر بساطة إذ إنه لكي يتم لنا الولوج إلى الحاسوب فإن علينا فقط أن نضغط مفتاح تشغيله، أما الإنترنت فإننا نحتاج، فضلاً إلى جهاز حاسوب عامل، إلى الولوج إليها بالاتصال بوسيط هو مزود الإنترنت Provider يمكننا من التعامل مع الخادم Surver وهوة أمر يحتاج إليه خاصة من خلال الحاسوب.

وبدون إحداث اتصال بين الحاسوب وبين الإنترنت عن طريق وسيط – حتى الآن- لا يمكن القول بوجودنا على الإنترنت. وعليه فإن مجرد القول بارتكاب جريمة حاسوب لا يعني ضرورة وجودنا على الإنترنت وإنما يكفي أن يكون الحاسوب في حالة عمل، في حين أنه لا يمكن القول بارتكاب جريمة من جرائم الإنترنت دون أن نكون على الإنترنت Online[٢].

ومثل هذا القول نجده في القانون الأمريكي حيث يميز القسم 18USC Sec. 1030 ، بين مصطلحي حاسوب Computer وبين حاسوب مشمول بالحماية Protected computer، فهذا الأخير يعني ذلك الحاسوب المتصل بغيره عن طريق الشبكات / الإنترنت في حين إن إيراد مصطلح حاسوب

---

١8 U.S.C. & 641. See : United States v. Friedman. 445 F. 2d 1076, 1087 (9th Cir.) (Theft of grand jury transcripts and information contained therein was theft of government property). Cert. denied. 404 U.S. 958 (1971) : United States v. Morison, 604 F. Supp. 655, 663-65 (D. Md. 1985) ("theft" of classified information supports embezzlement conviction); United States v. DiGillo, 538 F. 2d 972 (3d Cir). Cert. denied. 429 U.S. 871 (1971) (theft by photocopying government secords sufficient to support & 641 convocation) : United States v. MeAusland, 979 F.2d 970 (4th Cir. 1992) (theft of competitior's confidential bid information violates & 641).

([1]) Art. 1 Definitions : "For purposes of this convention : Computer System means any device or a group of inter – connected or related devices, one or more of which, pursuant to a program, performs automatic processing of data"

([٢]) أن مصطلح Online يثير جدلاً حيث أنه بالإنجليزية يشير إلى وجودنا على الإنترنت حيث إن ما يؤخذ في الاعتبار أن النظرة إلى الإنترنت كونها خط مفتوح يلزم لكي نصل إليها أن نكون على هذا الخط في حين أنه إذا كان خارجها فإن المصطلح المستخدم هو Off Line .

Computer فقط فإنه يعني مجرد الحاسوب غير المتصل بأي شبكة ولو داخلية (حيث يُعد هنا أداة تخزين فقط).

هذه الخصوصية التي منحها الحاسوب للإنترنت جعلتها تتميز في الحقيقة عنه من حيث الجزئية التي تعمل خلالها، وإذا كان مثار اهتمام رجال القانون في زمننا المعاصر هو التعامل مع تفريع جديد في قانون المعلوماتية Droit Informatique ، هو قانون الإنترنت CyberLaw ، فهذا لا يعني في الحقيقة التعامل مع قانون الحاسوب Computer Law الذي يمثل أحد تفريعات قانون المعلوماتية أيضاً.

لذلك يتجه بعض القانونيين الى إحداث فصل في هذا الإطار من حيث تعريف جرائم الإنترنت تعريفاً منفصلاً عن جرائم الحاسوب، باعتبارها جرائم ناجمة عن استخدام الإنترنت، وهو التعريف المبني على فهم عميق لطبيعة المشكلة من حيث ضرورة الفصل بين نوعي هذه الجرائم. حيث إن الإنترنت أفاءت على القانون بأشكال إجرامية جديدة لم تكن معروفة، حتى في ظل التجريم عبر الحاسوب حيث إنه كنتيجة لظهور الإنترنت أضحت المشكلة ليست فقط إحداثيات التمييز في إطار التجريم عبر الحاسوب، في محاولة تتعدى منطق التبسيط إلى التعقيد (مثال جرائم الحاسوب – الجرائم المرتبطة بالحاسوب وتفصيلاتها أيضاً ...إلخ) [١]. ولعل ما أنتهي إليه التطور الذي نراه سلبياً في توصيات مؤتمر G8 (الثمانية الكبار) عام ١٩٩٨ ليدعو إلى مزيد من التأمل في هذا الشأن، إذ تم التوصل إلى مصطلح High- Tech Crime أو جرائم التقنية العالية أو المتقدمة كنوع من محاولة التوسع في جرائم الحاسوب لكي تشمل كافة الجرائم التي يكون الحاسوب طرفاً فيها. وهذا كله يجعلنا نقرر أن هناك مفارقة مصطنعة بين جرائم الحاسوب وجرائم الإنترنت، على الرغم من الالتصاق الذي يكاد يكون طبيعياً بينهما.

وهذا الاتجاه الذي نأخذ به يجد له أساساً فقهياً يسعي إلى إقامة بنيانة على النحو الذي يحقق مصلحة الإنسان قبل الآلة، إذ يذهب هذا الاتجاه إلى أن جرائم الإنترنت هي "كل فعل أو امتناع عمدي ينشأ عن الاستخدام غير المشرع لتقنية المعلومات ويهدف إلى الاعتداء على الأموال المادية والمعنوية[٢].

وعلى الرغم من التوجه الصحيح في تعريف جرائم الإنترنت على النحو السالف، سيما هو يوضح لزوم العمد، فكان هذا الرأي سباقاً عن اتجاهات الاتفاقية الأوروبية للجريمة عبر العالم الافتراضي المؤرخة

([1]) (KASPERSEN) Prof. Dr. Henrik W. K. – crimes related to the computer network. Threats and opportunities criminological perspective, p. 258. five issues in European criminal justice: corruption, women in the criminal justice system, criminal policy indicators, community crime prevention, and computer crime proccedings of the vi European colloquium on crime and criminal policy Helsinki 10-12 December 1998, European institute or crime prevention and control, affiliated with the united nations (heuni) p. O. Box 161, fin- 00131 Helsinki Finland publication series no. 34

- Thoumyre – abuses in the cyberspace, op. cit., p. 10

([٢]) د. محمد سامي الشوا، ثورة المعلومات وإنعكاساتها على قانون العقوبات، ص ٧ .

٢٠٠١/١١/٢٣، فإن هذا التعريف لا يخلو من نقد، حيث يستلزم الامتناع كنشاط مادي في مثل هذه الجرائم، وهو الأمر الذي لا يمكن تصوره في هذا الشأن.

وعندنا يمكن وضع تعريف جامع مانع لجرائم الإنترنت إذا أخذنا في الاعتبار ثلاث نقاط رئيسية، وعلى ضوئها يمكن وضع تعريف متكامل يفيد في تحديد الجرائم الناشئة عن الإنترنت.

النقطة الأولي : موضوع العالم الافتراضي Cyberspace (وبالفرنسية Cyberespace) الذي هو عبارة عن العالم المرئي The virtual world أو المجال الحيوي للبيانات وحركتها المعلوماتية، وهو العالم المختفي في الآلة التقنية[١]. والذي يطلق عليه الفقه العربي تسمية الفضاء الإلكتروني[٢]. وهو العالم الذي ابتكر فكرته كاتب الخيال العلمي الشهير William Gibson في روايته الشهيرة The NeuRomancer، التي أصدرها عام ١٩٨٤، حيث وصف في هذا الكتاب فانتازيا إلكترونية Fantasy Electronic[٣] تقابل فيها مجموعة هكرة من مهرة الحاسوب، وطالما نشاطهم الاختراق والعديد من المظاهر التي تكاد تصل في بعض الأحيان إلى منطق الجريمة عبر الإنترنت كما هي مقررة في التشريعات المعاصرة.

وإذا كانت الإنترنت لم يتم تعريفها بعد في النظم القانونية المقارنة بشكل مستقل، فإنه مع ذلك قد لجأت تلك النظم – بإيعاز من الفقه – إلى حيلة قانونية يمكن معها الحصول على تعريف قانوني لها، وذلك باستخدام مصطلح منبثق عن عالمها الافتراضي Cyberspace وهذا المصطلح هو CyberLaw أي النظام القانوني للعالم الافتراضي للإنترنت أو قانون الإنترنت وهو "مجموعة القواعد القانونية التي تنظم العالم الفعلي للإنترنت" ، وهي قواعد لم تزل بعد في طور النمو نتيجة لعدم إمكانية حدوث ملاءمة بين المنظومة التقليدية للقانون وبينها، حتى وإن وصفت بالغموض والإبهام.

وإذا كان قانون العالم الافتراضي / الإنترنت (Cyber Law)، لا يشكل عقبة في إطار بناء نظريته – إن أمكن تكاثف الجهود نظرياً على الأقل – فإن الحال غير ذلك فيما يتعلق بتطبيق هذه النظرية وتنفيذها سيما في النطاق القضائي. ذلك إن تركيبة قانون العالم الافتراضي/ الإنترنت ذات طبيعة مختلفة في الحقيقة عن تركيبة أي قانون آخر، فهو يتركب من طبيعة افتراضية ذات بعد دولي[٤] يتطابق شكلياً مع

([1]) RCMP, op-cit.

([٢]) د. جميل عبد الباقي الصغير، الأحكام الموضوعية للجرائم المتعلقة بالإنترنت، دار النهضة العربية، القاهرة ١٩٩٩، ص ٥ .

([3]) (NICHOLSON) Keith – International Computer Crime : A Global Village Under Siege – New England International & Comparative Law Annual 1996 – New England School of Law P. I. available online is Sep. 2001 at :

http://www.nest.edu/annual/vol2/computer.htm

([4])TRANSNAIONAL NATURE OF CYBERSPACE, (CYBERCRIME AND CYBERPUNISHMENT< ARCHAIC LAW THERATEN GLOBAL INFORMATION p. 2 report prepared by : McConnell INTERNATIONAL http://www.mcconnellinternational.com with support from WITSA

مفاهيم العولمة، وليس مع المفاهيم التي يعرفها القانون الدولي، في الوقت الذي يتسع مدلوله ليشمل فروع القانون الأخرى. ذلك إنه من خلال مصطلح CyberLawهرع الفقه المقارن ليضع تفريعات جدية لهذا المصطلح تعمل في إطاره ووفق فروع القانون المعمول بها، مثل Cyberbehavior للدلالة على سلوكيات القانون المدني، ومصطلح CyberCrime للدلالة على سلوكيات القانون الجنائي، ومصطلح Cybercommerce للدلالة على سلوكيات القانون التجاري، ومصطلح Cyberinvestigation للدلالة على الإجراءات الجنائية في إطار قانون الإنترنت، ومصطلح Cybertribunal على المحاكمات عبر الإنترنت ... إلخ.

هذا الاتجاه الفقهي يسعي إلى إقامة علاقة بين القانون وبين الإنترنت في معني إحداث ملاءمة بين الأثنين، بما يمكن معه تطويع القانون للإنترنت لمصلحة الإنسان في تعامله مع الآلة.

إن عملية إحداث ملاءمة بين النظام القانوني القائم وبين الإنترنت كانت قد برزت بداية حال موافقة الفقه النسبية على إمكانية التعامل القانوني مع الإنترنت بأسلوب التنظيم النفسي للإنترنت – Self regulation ، بحيث يجب ألا يكون هذا التنظيم هو الأداة الوحيدة وإنما يقبل إلى جوار التنظيم القانوني بالأداة التشريعية تواجد أدوات تنظيمية نابعة من طبيعة الإنترنت، أي التقنية المعلوماتية. وسببية رفض وحدة التنظيم الذاتي كنظام قانوني للإنترنت يكمن في أن التنظيم الذاتي ليس مقنعاً بالدرجة الكافية[١] بما يجعل العالم الافتراضي آمناً بالدرجة الكافية التي تسمح بالأمن والاستقرار [٢]. على إن الأمر ليس على ذلك القدر من السهولة إذا تأملنا الاتجاه المضاد الذي يأخذ بضرورة التدخل القانوني لتنظيم العالم الافتراضي حيث أنه توجد لديه صعوبات أيضاً، من حيث إن أهم صعوبة تتمثل في تحديد طبيعة النظام القانوني الذي يحكم الإنترنت، وهل تكفي النظم الأساسية في الدولة لحسم هذه الصعوبات وتذليل محتواها، أم إن العالم الافتراضي قام هكذا فجأة وبالتالي يمكن أن يوجد له أساس في النظم القانونية المعاصرة، إلا أن العقل القانوني لم يستظهر هذا الأساس بعد، وهنا فإن المسألة فقط تحتاج إلى مزيد من الوقت والتأمل والحكمة القانونية.

النقطة الثانية: ترتبط بالنتائج المترتبة في النظام القانوني حين فصل جرائم الحاسوب Computer Crimes عن جرائم الإنترنت CyberCrime ، ومدى إمكانية قيام هذا الفصل تقنياً. والحقيقة إنه من الصعوبة بمكان فصل جرائم الحاسوب عن جرائم الإنترنت، نتيجة لارتباط الإنترنت بالحاسوب ارتباطاً تقنياً. إلا أن هذه الصعوبة سوف تتقلص كثيراً إذا أدركنا أن تقنية الحاسوب أعم كثيراً من تقنية الإنترنت. فهو – أي الحاسوب- ثورة حقيقية ذات أبعاد اجتماعية وسياسية واقتصادية وقانونية ليس لها نهاية، إذ كما أنتجت تقنية الحاسوب الإنترنت فإن ذلك لا يعني نهاية المطاف في هذا الشأن،

---

http://www.witsa.com December 2000 availale online in dec. 2000, at : http://www.mcconnellinternational.com/services/cybercrime.html

([1])RCMP, op-cit.

([2]) CyberCrime And Cyberpunishment , archaic law threatens global information op-cit p. 2

فالمؤشرات السائدة تشير إلى أن تقنيات جديدة للحاسب تبرز في الأفق قريبا ، وتدليلا على ذلك فإن دولا مثل كندا تربط جرائم الانترنت بجرائم الاتصال عن بعد Telecommunication Crime التي يمكن أن تقع بواسطة الانترنت كما يمكن إن تقع بواسطة الهاتف وجهاز الموجات الصغيرة Microwave والأقمار الصناعية Satellite وغير ذلك [1]

وإذا كان حقيقي إن تقنية الحاسوب قد انطلقت لكي تبتكر الانترنت فإن منطقه الخلاف بين العمل السلبي الذي يكون محله الحاسوب وبين ذلك الناجم عن استخدام الانترنت يعد أحد الصعوبات الجديدة التي تواجه فقه القانون حقيقة فإذا تحدد هذا التعريف فإنه من السهولة التوصل إلى بحث التوجه السياسي والتشريعي في دولة ما . لأجل ذلك نجد إن البعض لا يمانع في إطلاق صفة جرائم الحاسوب Computer Crime على الاختراق Hacking إلا أنه يشترط بالضرورة أن يكون الحاسوب مرتبطا بشبكة Connected [2] أو Protected Computer ويمكن القول إجمالا إن هناك اتجاهين في إطار رصد تعريف جرائم الانترنت ، الاتجاه الأول بنحو منحى التعريف المضيق الذي يقوم برصيد جرائم الانترنت في ربط جرائم العالم الافتراضي ككل بالحاسوب حيث يذهب هذا الاتجاه إلى " إن مصطلح العالم الافتراضي مرجعه استخدام الحاسوب لتسهيل ارتكاب الجرائم [3] وهو تعريف مضيق لكونه يربط إجرام العالم الافتارضى بالحاسوب بالمفهوم الضيق ، حيث أن مصطلح الحاسوب يتسع لي أبعد من ذلك الذي نعرفه اليوم وبحيث يجب الأخذ في الاعتبار تلك النظرة المستقبلية للحاسوب التي تعنى حوسبة أو رقمية العالم البشرى على النحو الذي يحقق اعتماد الإنسان عليه في كل شيء لذلك فإن النقد الذي يمكن توجيهه إلى هذا التعريف إنه يربط تعريف جرائم الانترنت بالحاسوب فإن ذلك يعنى أن فصل الحاسوب عن الانترنت في أبسط مظاهر هذا الفصل (أي بفصله بعدم الدخول إلى الانترنت – أو بفضل الكهرباء عنه) يعنى أنتها الجريمة وعدم اتصالها بنا ، في حين أنذلك غير صحيح إذ تظل الجريمة قائمة وظاهرة في أماكن أخرى .

لذلك فإن الأرجح هو الاتجاه إلى التوسع في تعريف جرائم العالم الافتارضى / الانترنت ومكمن التعريف الموسع هو السعي إلى بحث استقلالية لجرائم الانترنت تتنافى مع ربطها بالحاسوب وجرائمه . ولما كنا فيما سبق قد عرفنا الانترنت هي في الحقيقة الجرائم الناشئة عن استعمال هذا التواصل بين الشبكات وهذا اتجاه المشرع الأوروبي في اتفاقية الجريمة عبر العالم الافتراضي المؤرخة ٢٠٠١/١١/٢٣

---

1 FGSSC – available online in feb 2000 at :

Http://www.usdoj.gov/criminal/cybercrime/search docs/toc.htm

2 Nicholson – International computer crime op – cit P.2

3 (KATYAL) Neal Kumar – criminal law in criminal law in Cyberspace , Georgetown University law center 2000< P.13 A revised version of This working paper is forthcoming in the university of Pennsylvania law review < Volume 149 April 2001 This paper can be downloaded without charge from the social science research Network Electronic paper collection at

Http://papers.ssrn.com/ aperitif abstract id=249030 working paper No 249030

وكذلك اتجاه المشرع الامريكى حين رصده لمصطلح Protected Computer ولما كان التقسيم الأمثل لهذه الشبكة إلى ثلاثة أقسام كما عرضنا لذلك فيما سلف (شبكة المعلومات الدولية – البريد الإلكترونى- الاتصال المباشر)، فإن العدوان باستخدام الانترنت من خلال أقسامها هو الوضع الصحيح الذي يجب أن يكون عليه التجريم هنا لذلك نجد إن جرائم الانترنت في حقيقتها هي تلك الجرائم التي ترتكب بدواسة التواصل بين الشبكات .

وإذا كان هذا التعريف يتميز بالعمومية إلا أنه مع ذلك يظل محصورا في إطار الانترنت وبالتالي كل جريمة من الجرائم كانت وسيلتها الانترنت أو أقسامها إنما هي من جرائم الانترنت

إن التعريف الذي نقول به يجعلنا في الحقيقة نعترف مسبقا بأن ظاهرة الانترنت لا زالت غامضة في دراسات القانون وفى هذا الإطار رصد المرشد الفيدرالي الأمريكي لتفتيش وضبط الحاسوب Federal guidelines for searching and computers أهمية الاعتراف بأن رجال القانون بدءوا في مواجهة مشاكل جديدة على اثر إنجاز ثورة معلومات الحاسوب والاتصالات في القرن الواحد والعشرين [١]

إن الفصل بين الحاسوب وبين برمجياته يعد تدليلا على قيمة الفصل بين الحاسوب وبين الانترنت . ولقد اشتد الصراع – بناء على ما سلف – بين فقه القانون وخبراء تكنولوجيا المعلومات خول الأبعاد الفلسفية لتحديد جرائم الانترنت أو جرائم العالم الافتراضي ، ما بين مؤيد لاعتبار هذه الجرائم مجرد جرائم عادية ترتكب بواسطة الحاسوب والياته – وهو الأمر الذي يترتب عليه تطبيق القانون السائد عليها وبما لا يخرج عما هو مقرر في هذا الشأن كما أنه يقود إلى القول بكفاية النصوص الجنائية للانطباق عنا لكونها لا تتعدى ما هو مقرر حين اختراق القانون الجنائي كما هو الشأن في الانتهاك Trespass والاختلاس larceny والقرصنة Conspiracy - وبين مؤيد لاعتبار جرائم الانترنت إنما هي جرام ذات أبعاد جديدة وتحتاج إلى إعادة نظر في هيكلة القانون الجنائي الحالية ويدلل هذا الاتجاه على ذلك بموضوعات القانون الجنائي وصعوبة الإثبات وكذلك حالة مرتكبي جرائم أو ما يطلق عليه مشكلة الهكرة Hacklers في هذا الإطار [٢] وإذا كان هذا الاتجاه له منطقة في ضرورة التعامل مع جرائم الانترنت بخصوصية ما إلا أن عملية الكشف عن هذه الخصوصية التي تتمتع بها هذه التوعية من الجرائم استلزم ضرورة التطرق إلى الخصوصية التي تمتع بها الانترنت ذاتها وأما النقطة الثالثة : التي يجب الانطلاق منها للتأكيد على تعريف جرائم الانترنت من منطلق أنها جرائم ترتكب بواسطة تلك الوسيلة أو الأداة التواصلية بين الشبكات دون اعتبار للحدود الدولية ، تتعلق بكينونة الانترنت كظاهرة لها ايجابياتها وسلبياتها فإنه يجب معاملتها على هذا الأساس مثلها في ذلك مثل الظواهر الجديدة . لذا فهي ليست مجرد وسيلة لارتكاب الجرائم وذلك لما توفره من مجموعة بدائل مختلفة عبرها ، حيث انه يمكن ارتكاب الجرائم بواسطة البريد الالكتروني مثلا (الذي يحتوى على

---

[1] Theoumyre – abuse in the cyberspace , op-citP.8

[2] Eric J . Sinrod and William P.reilly- Crimes : A practical approach to the application of federal computer crime laws P.3 Santa Clara computer and high technology law Journal may 2000 Volume 16, Number 2

مجموعة بدائل مختلفة) كما يمكن ارتكاب جرائم عبر البدائل التي توفرها شبكة المعلومات الدولية ... الخ

ومن هذا المنطلق فإن الروية المحددة للانترنت لا تنطلق من الفكر النظري وإنما من الواقع العملي ، وهذا يستدعى البحث في مدى إمكانية المجتمع للتقبل الفكري لها ، فهي مجال حيوي Atmosphere في المجتمع قابل لربط عقليته Mentality بها ففي بعض الدول التي مرت بتجارب واقعة عن الانترنت أمكن لها أن تحدث تفاعلا إيجابيا يتواصل مع قانون الانترنت مقلما حدث في الفيليبين على إثر قيام أحد طلبة الجامعة هناك بابتكار فيروس الحب I love You قامت الدولة بتكثيف جهودها لسن قانون في هذا الشأن سيما بعد التدخل الدولي نتيجة لكون الضرر عبر الحدود الدولية إلى نطاق عالمي فأصاب أجهزة حاسوب حول العالم .[١] فالعالم الفعلي هو جزء من عالمنا غير منفصل عنه ، لذلك فهو ليس بعيدا عن إمكانية إحداث تنظيم قانوني له [٢] ، بل إن الفقه ينادي بكينونة عقلية منفردة للانترنت فعلى مبدؤه عالمية التفكير وإقليمية الحركة [٣]

[1] Cyber crime And cyberpubishment , archaic law threatens global information op – Cit P.4

[2] Rcmp op-cit " a computers and telecommunications explode into the next century prosecutors and agents have begun to confront new Kind's explode into the next century prosecutors and agents have begun to confront new Kind's of problems "

[3] Thoumyre – abuse in the cyberspace op-cit P.9 : Think Globally and Act locally

المبحث الثانى

جرائم تقانة المعلومات...

تعريفها.. أسبابها..خصائصها..تصنيفها

لقد أفرزت ثورة الاتصالات والمعلومات: وسائل جديدة للبشرية تجعل الحياة أفضل من ذي قبل ؛ غير أنها فتحت الباب على مصراعيه لظهور صور من السلوك المنحرف اجتماعيا التي لم يكن من الممكن وقوعها في الماضي ؛ وتخرج عن دائرة التجريم والعقاب القائمة ؛ لأن المشرع لم يتصور حدوثها أصلاً .

فمن جهة أولى أتاحت نظم الكمبيوتر (الحاسوب) ظهور صور جديدة من الجرائم لم تكن موجودة في الماضي ؛ وذلك مثل سرقة المعلومات والأسرار المودعة في قواعد المعلومات ؛ ومن جهة ثانية أتاحت هذه النظم الفرصة لارتكاب الجرائم التقليدية بطرق غير تقليدية ؛ كما هو الشأن بالنسبة لجرائم الغش وإتلاف وإفساد المعلومات المخزنة في قواعد المعلومات.

ومن ثم ينقسم هذا المبحث إلى مطلبين، تناول المطلب الأول تعريف جرائم الانترنت وشبكات التواصل الإجتماعي ، وأسبابها وخصائصها والمجرم المعلوماتى، وجاء المطلب الثاني مركزا على تصنيف جرائم المعلوماتية والإنترنت.

المطلب الأول

تعريف جرائم تقانة المعلومات وأسبابها وخصائصها

تعددت التعريفات التي تناولت الجريمة المعلوماتية، ويرجع ذلك إلي الخلاف الذى أثير بشأن تعريف هذه الجريمة ومن قبلها تعريف المعلومة ذاتها، فالجرائم المعلوماتية هي صنف جديد من الجرائم، ذلك أنه مع ثورة المعلومات والاتصالات ظهر نوع جديد من المجرمين انتقلوا بالجريمة من صورتها التقليدية إلى أخرى إلكترونية قد يصعب التعامل معها، لأن الجريمة المعلوماتية هي من الظواهر الحديثة؛ وذلك لارتباطها بتكنولوجيا حديثة هي تكنولوجيا المعلومات والاتصالات. وقد أحاط بتعريف الجريمة المعلوماتية الكثير من الغموض حيث تعددت الجهود الرامية لوضع تعريف جامع مانع لها ولكن الفقة لم يجتمع علي وضع تعريف محدد لها بل أن البعض ذهب إلى ترجيح عدم وضع هذا التعريف بحجة أن هذا النوع من الإجرام ما هو إلى جريمة تقليدية ترتكب بأسلوب إلكتروني.

أولا: تعريف الجريمة المعلوماتية

على الرغم من تنامى جهود التصدي لظاهرة الإجرام المعلوماتى إلا أنه لا يوجد تعريف محدد ومتفق عليه بين الفقهاء حول مفهوم الجريمة المعلوماتية، فقد ذهب جانب من الفقه إلى تناولها بالتعريف على نحو ضيق وجانب أخر عرفها على نحو موسع.

١ـ التعريف الضيق للجريمة المعلوماتية

ذهب الفقيه (merwe) إلى أن الجريمة المعلوماتية هي الفعل غير المشروع الذي يتورط في ارتكابه الحاسب الآلى – أو هو الفعل الاجرامى الذي يستخدم في اقترافة الحاسب الآلى 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 الالى والى تحويل طريقه.

وعرفها كلاوس تايدومان بأنها كافة أشكال السلوك غير المشروع الذي يرتكب باسم الحاسب الآلى.

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

ويدخل فى 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 دورا رئيسيا.

٢ـ التعريفات الموسعة لمفهوم الجريمة المعلوماتية

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 الآلى بما تتضمنه من شيكات تحويل الحسابات المالية بطرق إلكترونية وتزييف المكونات المادية والمعنوية للحاسب، بل وسرقة الحاسب في حد ذاتة وأى من مكوناته. وذهب رأى أخر من الفقة إلى تعريف الجريمة المعلوماتية بأنها عمل أو امتناع يأتيه الإنسان، إضرارا بمكونات الحاسب وشبكات الاتصال الخاصة به التي يحميها قانون العقوبات ويفرض لها عقاب. ويرى جانب من الفقه من أنصار هذا الاتجاة الموسع بأنها كل سلوك اجرامى يتم بمساعدة الكمبيوتر أو كل جريمة تتم في محيط أجهزة الكمبيوتر[1].

٣- موقف بعض التشريعات والهيئات الدولية من تعريف الجريمة المعلوماتية

أشارت الأمم المتحدة في المدونة الصادرة عنها بشأن الجريمة المعلوماتية، إلي الخلاف الواقع بين الخبراء حول ماهية العناصر المكونة لجرائم الكمبيوتر أو حتى المتعلقة بالكمبيوتر ولعل ذلك ما يفسر عدم التوصل إلى تعريف متفق علية دوليا 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 دورا رئيسيا، فإن قانون الكيان الصهيوني(إسرائيل) رقم ٥٧٥٥لسنة ١٩٩٥ فى شأن جرائم الحاسب الآلى، قد عرفها بأنها تلك الجرائم التي تشمل العبث ببرامج الكمبيوتر على نحو يعوق استخدامها، أو تحل معلومات غير مصرح بها إلا للأشخاص محددين، وكذلك اختراق الكمبيوتر بغرض ارتكاب جريمة أخرى أو بث فيروس من شأنة التأثير على أداؤه.

- 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.

وسوف نعرض هنا لماهية المعلومة من حيث تعريفها ثم أنواعها والشروط اللازم توافرها فيها، وطبيعتها القانونية، والمسؤلية عنها.

- تعريف المعلومة

---

[1] يذهب البعض إلى أنه عند وضع تعريف محدد للجريمة المعلوماتية يجب مراعاة عدة اعتبارات 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 الاجرامى.
٤- أن يفرق هذا التعريف بين الجريمة العادية والجريمة المعلوماتية وذلك عن طريق إيضاح الخصائص المميزة للجريمة المعلوماتية.

لم تعد المعلومات الآن مجرد نوع من الرفاهية والترف تتباهى بة الشعوب أو المنظمات وإنما أصبحت ركيزة أساسية في تقدم وتطور المجتمع وتحقيق تقدمة ورفها يته المنشودة ،وفى سبيل ذلك وضع عدد غير قليل من التشريعات الوطنية المختلفة تعريفا للمعلومة وهوماسوف نعرض للعدد منها.

وقد عرف المشرع الامريكى، المعلومات في قانون المعاملات التجارية الإلكتروني لعام ١٩٩٩بالفقرة 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 تقريبا كل ما يتعلق بها بل أكثر من ذلك أنة تحسب ما قد يظهر من تتطور تكنولوجي جديد.

والمشرع الفرنسي ووفقا للقانون ٨٢-٦٥٢ الصادر في ٢٦ يوليو لسنة ١٩٨٢، تُعرف المعلومة على أنها صورة أو مستندات أو معطيات أو خطابات أيا كانت طبيعتها.

أما قانون البحرين رقم ٨٣ لسنة ٢٠٠٢بشأن 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)[١].

هذه مجموعة من التشريعات التي وضعت تعريفا واضح للمعلومة والمعلومات كان أغلبها كما رأينا يدور حول الأشكال المختلفة للمعلومات وصورها التي تظهر فبها 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 هذة البيانات.

<u>- أنواع المعلومات</u>

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

أما الطائفة الأولي وهى المعلومات الاسمية، فتنقسم إلي مجموعتين هما:

---

[١] انظر: د. محمد الأمين البشرى، التحقيق فى جرائم الحاسب الآلى، بحث مقدم إلى مؤتمر القانون والكمبيوتر والانترنت، جامعة الإمارات العربية المتحدة،سنة ٢٠٠٠.

١-المعلومات الموضوعية وهى تلك المعلومات المرتبطة بشخص المخاطب بها مثل اسمه وموطنه وحالتة الاجتماعية وهى معلومات لا يجوز الإطلاع عليها إلا بموافقة الشخص نفسه.

٢- المعلومات الشخصية ويقصد بها تلك المعلومات المنسوبة آخر مما يستدعى إدلاء الغير برأيه الشخصي فيها وهى مثل المقالات الصحفية والملفات الإدارية للعاملين لدى جه معينه.

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

وأما الطائفة الثالثة وهى المعلومات المباحة، فيقصد بها تلك المعلومات تكون مباحة للجميع الحصول عليها لأنها بدون مالك مثل تقارير البورصة والنشرات الجوية هذة المعلومات مباحة للكافة وغير محمية بأي من وسائل الحماية.

٤- الشروط التى يجب توافرها فى المعلومة محل الحماية

بصفة عامة هناك شروط يجب توافرها في المعلومة حتى تتمتع بالحماية القانونية وتتمثل هذة الشروط في الآتى:

أ- أن يتوافر فى 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 تحديدا دقيقا وخصوصا في مجال الاعتداء على الأموال فهذة الاعتداءات تتطلب أن يكون هناك شيء محددا ومبتكر أما الشيء الشائع فلا يتمتع بأي حماية قانونية.

ب- أن يتوافر فى 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 لان المعلومة العا مة الشائعة تكون بمنأى عن أي حيازة

وتكتسب المعلومة وصفها إما بالنظر إلى طبيعتها أو بالنظر إلا إرادة الشخص أو إلي الأمرين معا مثل الرقم السري(passwoard).

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.

ثانيا: أسباب جرائم تقانة المعلومات

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

[1]، فضلا عن ذلك، تتمتع جرائم الكمبيوتر والمعلوماتية بعدد من الخصائص التى تختلف تماما عن الخصائص التى تتمتع بها الجرائم التقليدية، كما أن الجانى الالكترونى(أو المجرم الالكترونى) يختلف أيضا عن المجرم العادى.

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.

١- غاية التعلم

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

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

ب- 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.

ويري 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.

([1]) وتتنوع الجرائم المعلوماتية على النحو التالي :

- إساءة استخدام الإنترنت.
- استخدام برامج حل وكشف كلمات المرور.
- نشر برامج حصان طروادة وغيرها من الفيروسات.
- هجمات المخربين.
- الهجمات الاختراقية.
- الانتهاكات الأمنية التي تتضمن حالات إساءة استخدام عن طريق الدخول غير المخول به على النظام : تنبع غالبية الانتهاكات الأمنية من مصادر داخلية، مثال : مستخدمين من داخل المؤسسة يحاولون الوصول إلى بيانات سرية غير مخول لهم بالإطلاع عليها.

راجع في ذلك :

Dr. Linda volonino.cyber terrorism. Op. cit.

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. ويقول "لانديس" أن هؤلاء القراصنة يرغبون في البقاء مجهولين حتى يتمكنوا من الاستمرار في التواجد داخل الأنظمة لأطول وق ممكن. ويكرس 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 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 أن قراصنة الأنظمة أنه ينتمي إلى مجموعة بحث مهمتها استخراج كميات كبيرة من المعلومات وتعلم أكبر قدر منها.

ويسعي أعضاء القراصنة إلى التخصص والتعاون في المشاريع البحثية وتقاسم البرامج والأخبار وكتابة المقالات وتعريف الآخرين بمجالات اختصاصهم ويدع قراصنة الأنظمة نظاماً خاصاً لمجال المعرفة الذي يجذبهم ويعلهم التفكير ويسمح لهم بتطبيق ما تعلموه في أنشطة هادفة وإن لم تكن قانونية دائمة[1].

٢- 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 قد بوشرت من أجل اختلاس الأموال.
- ٢٣% من أجل سرقة المعلومات.
- ١٩% أفعال اتلاف.
- ١٥% سرقة وقت الآلة vol detemps machine أي الاستعمال غير المشروع للحاسب الآلي لأجل تحقيق أغراض شخصية[2].

لذا نجد أن الدافع لارتكاب الجريمة المعلوماتية يمكن أن تكون سببه مجرد سداد الديون المستحقة أو مشاكل عائلية راجعة للنقود أو ادمان ألعاب القمار أو المخدرات لذا فإن بيع المعلومات

---

(1) قراصنة أنظمة الكمبيوتر إعداد : دورثي إي. دينغ ورقة مقدمة للمؤتمر القومي الثالث عشر لأمن الكمبيوتر، واشنطن، ترجمة : آمنة علي يوسف، ديسمبر ١٩٩٨، ص ٨.

(2) G. Delmare, securité informatique Ressource informatique no. 1. Juill 1984.

المختلسة هو نشاط متسع للغاية ويمكن أن نبين في هذا المجال واقعة استيلاء مبرمج يعمل لدي إحدى الشركات الألمانية على ٢٢ شريطاً ممغنطاً تحوي 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 أن الخسائر التي يمكن أن تنشأ عن إفشاء محتواها تفوق بكثير المطلب المطلوب فقد فضلت دفع المبلغ من أجل استرداد الشرائط المسروقة[١].

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 تلقائياً عن طريق ما يعرف بالقنابل المنطقية[٢].

٣- الإثارة والتحدي

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 عضواً 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 وأنسي جسدي تماماً بينما أتنقل من جهاز كمبيوتر إلى آخر محاولاً العثور على سبيل للوصول إلى هدفي. لقد كان الأمر يشبه سرعة العمل في متاهة إلى جانب الاكتشاف الكبير لإعداد 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 الي لم يكن من المفترض وجودي بها[٣].

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

٤- الدوافع الشخصية

([1]) Le Monde informatique 21 fev 1983, Etude la delinquance en col blanc se parte bien

([2]) Les escrocs a l'informatique in le Nouvel Economiste no. 202 du 1-10-1979.

([٣]) قراصنة أنظمة الكمبيوتر، إعداد : دروثي إي. دينغ، ورقة مقدمة للمؤتمر القومي الثالث عشر لأمن الكمبيوتر، واشنطن، ترجمة : آمنة علي يوسف، ديسمبر ١٩٩٨ ص ١١.

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[1].

ويتزايد شيوع هذا الدافع لدي فئات صغار السن من مرتكبي الكمبيور الذين يمضون وقتاً طويلاً أما 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 وهو الدافع لارتكاب فعل الجريمة المعلوماتية وفي هذا الشأن نجد المحلل أو المبرمج المعلوماتي وهو مفتاح سر كل نظام قد ينتابه إحساس بالإهمال أو بالنقص داخل المنشأة التي يعمل بها[2]. 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[3].

وبصفة عامة تتميز جرائم الحاسب بالصعوبات البالغة في اكتشافها وبالعجز في حالات كثيرة عن إمكان إثباتها في حالة إكتشافها. ومرد ذلك الأسباب التالية :

<u>أولاً</u> : لا تخلف جرائم الحاسب آثاراً ظاهرة خارجية 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 تمحي 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.

---

(1) يميل القراصنة إلى التحدي وإلى معرفة تفاصيل تكنولوجيا الكمبيوتر ويبدو أن ولعهم بالكمبيوتر يدفعهم إلى ارتكاب الجرائم وفي هذا الخصوص يحدثنا الدكتور Perey Black أستاذ علم النفس بجامعة نيويورك أن القراصنة يتملكهم جميعاً شعور بالبحث عن القوة ويؤدي ارتكابهم للجرائم بواسطة الكمبيوتر إلى تعويضهم عن الإحساس بالدونية.

راجع في ذلك :

CYBER CRIME op. cit. p. 25.

(2) تمت مقاضاة شركة مورجان ستانلي مر تبين من قبل الموظفين العاملين بها بسبب التمييز العنصري حيث كشفت مبادئ الطب الشرعي المستخدمة في مجال جرائم الكمبيوتر عن وجود "نكات عنصرية" يتم توزيعها عبر نظام البريد الإلكتروني الخاص بالشركة.

راجع في ذلك :

DR Linda Volonino op.cit.

(3) د. محمد سامي الشواء مرجع سابق، ص ص ٥٢-٥٣ .

ثانياً : 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.

ثالثاً : تبدو أكثر المشاكل جسامة لا في مجال 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[1] 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[2].

ثالثا: خصائص الجرائم المتصلة بتقانة المعلومات

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

([1]) 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

([2]) في إحدى الوقائع الشهيرة تعرض بنك merchant bank city في بريطانيا لنقل ٨ مليون جنيه من أحد أرصدته إلى رقم حساب في سويسرا، وقد تم القبض على الفاعل أثناء محاولته سحب المبلغ المذكور ولكن البنك يدل الادعاء على الفاعل قام بدفع مبلغ مليون جنيه له بشرط عدم إعلام الآخرين عن جريمته وشريطة إعلام البنك عن الآلية التي نجح من خلالها باختراق نظام الأمن الخاص بحاسوب البنك الرئيسي.

راجع في ذلك : يونس خالد عرب مصطفي، جرائم الحاسوب، دراسة مقارنة، رسالة ماجستير مقدمة إلى الجامعة الأردنية ١٩٩٤، ص ٧٢.

٥. عابرة للدول:إن ربط العالم بشبكة من الاتصالات من خلال الأقمار الصناعية والفضائيات والإنترنت جعل الانتشار الثقافي وعولمة الثقافة والجريمة أمرا ممكنا وشائعا، 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 واقعا 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 أثرا 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.

<u>رابعا: المجرم المعلوماتى</u>

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 الاجرامى النمطي. وهذا ماسو ف نعرض له موضحين أهم سمات المجرم المعلوماتى ثم خصائصة المميزة وأخيرا لأنماط هذا المجرم وذلك على النحو التالي.

<u>١ـ سمات المجرم المعلوماتي</u>

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 كونة مرتكبا لفعل إجرامى يتطلب توقيع العقاب علية.

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

<u>أـ المجرم المعلوماتى، مجرم متخصص</u>

تبين في عديد من القضايا أن عددا 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[١].

---

[١] يمكن الرجوع الى:

- Vonderau, Patrick. (December 30, 2009),The YouTube Reader, Sweden: National Library of Sweden.

ب- المجرم المعلوماتى، مجرم عائد إلى الإجرام

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

ج- المجرم المعلوماتى مجرم محترف

يتمتع المجرم المعلوماتى باحترافية كبيرة في تنفيذ جرائمة، حيث أنه يرتكب هذة 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.

د- المجرم المعلوماتى مجرم غير عنيف

المجرم المعلوماتى من المجرمين الذين لا يلجأون 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[١].

٢- الأنماط المختلفة للمجرم المعلوماتى

يقسم مجرمي المعلوماتية (cybr criminals) إلي مجموعة من الطوائف المختلفة، حيث أسفرت الدراسات المختلفة في هذا المجال إلي وجود عدد من الأنماط المختلفة لمجرمي المعلومات، نرصدها فيما يلى:

الطائفة الأولى(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):

- Wittkower, D:E. (October 1, 2010), Face book and Philosophy: What's on Y::our Mind?. USA: Open Court.

[١] انظر:

Jenkins, Henry. (September 1, 2008), Convergence Culture: Where Old and New Media Collide, USA: NYU Press; Revised edition.

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 هذة الأنظمة.

الطائفة الثالثة(malicious hackers):

وهم أشخاص هدفهم إلحاق خسائر بالمجني عليهم، دون أن يكون الحصول على مكاسب مالية ضمن هذة الأهداف، ويندرج تحت هذة 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 هذة 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 هذة الطائفة في سماتة إلى المجرم التقليدي.

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

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

٢ـ المعرفة والقدرة الفنية الهائلة .

٣ـ الحرص الشديد وخشية الضبط وافتضاح الأمر .

٤ـ ارتفاع مستوى الذكاء ومحاولة التخفي[١] .

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

---

[١] أكدت بعض الدراسات والأبحاث العلمية على أن فئات المجرمين(أو الجناة) تنحدر من:
١ـ مستخدمو الحاسب بالمنازل.
٢ـ الموظفون الساخطون على منظماتهم.
٣ـ المتسللون ومنهم الهواة أو العابثون بقصد التسلية.
٤ـ المحترفون الذين يتسللون إلى مواقع مختارة بعناية ويعبثون أو يتلفون النظام أو يسرقون محتوياته وتقع أغلب جرائم الانترنت حاليا تحت هذه الفئة بتقسيمها .
٥ـ العاملون في الجريمة المنظمة .
انظر:
Hawker, Mark. D, (August 25, 2010), Developer's Guide to Social Programming: Building Social Context Using Face book, Google Friend Connect, and the Twitter API, Canada: Addison-Wesley Professional; 1 edition.

- 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.

المطلب الثاني

تصنيف جـرائم تقانة المعلومات

تتعدد انماط الجريمة في مجال الإنترنت وشبكات التواصل الإجتماعي، والتي يمكن تصنيفها الى عدد من المحاور والتي تشكل جميعا انتهاكا يستحق العقاب وذلك على النحو التالي:

أولا: الجرائم المرتكبة أثناء أداء الحاسب لوظائفه العادية

لا يتطلب ارتكاب هذا النوع من الجرائم المساس بالوظائف العادية للحاسب الآلي ولا تعديل على البيانات المختزنة بذاكرته بل يقتصر الأمر على الدخول من جانب البعض إلى مركز نظم المعلومات وأداة إلكترونية تسمح بالتقاط المعلومات أو التنصت عليها من بعد.

ثانيا: الاختراق وانتحال الهوية

من الممكن الاختراق أو انتحال الهوية إما مادياً أو إلكترونياً. فالاختراق المادي يسمح بالدخول في مناطق خاضعة للسيطرة عن طريق بوابات إلكترونية أو آلية. وأسلوب الاختراق الأكثر شيوعاً هو أن يقف شخص غير مسموح له بالدخول أمام البوابة المغلقة حاملاً بين ذراعية متعلقات خاصة بالحاسب الآلي كالشرائط الممغنطة desbandes أو ينتظر حتى يتقدم شخص مسموح له بالدخول ويفتح له الباب فيدخل معه في نفس الوقت. لذا فإنه يمكن القول بأن التواجد في صالات الحاسبات الآلية هو أمر حتمي لارتكاب هذه الجرائم[1]. وينطوى الفعل غير المشروع هنا على اطلاع غير مسموح به على المعلومات المختزنة في نظم المعلومات وله صور عديدة.

١- سرقة القائمة وهي عملية مادية بحتة يكتفي فيها السارق بسحب القائمة من الطابعة.

٢- الإطلاع على المعلومات والمقصود بذلك مطالعة المعلومات التي تظهر على شاشة الحاسب الآلي.

٣- التصنت المجرد على المعلومات ويتم ذلك عن طريق استخدام مكبر للصوت[2] والذي يلتقط المعلومات والبيانات.

([1]) انظر :

D. Parker, op. cit., p. 44 et s.

([2]) قبل أن يقوم Hacker باقتحام شبكة الحاسب الآلي، يجب عليه استخدام تسهيلات اتصال لكي يرتبط بالشبكة وقد يكون تكاليف الاتصال القانوني مع نظام الكمبيوتر المستهدف معرفة الـ Hackers قد تكون مرتفعة للغاية وقد يكون من الممكن تعقبها. لذا يقوم الـ Hackers بتوظيف أساليب فنية لتجنب هاتين= =المشكلتين: يقوم الـ Hackers بتوظيف أساليب فينة يطلق عليها عادة الـ Phreaking ومن تطبيقاتها ما يلي :

١- الاتصال التليفوني بواسطة النغمة :

وهو أسلوب نقلي يمكن التلاعب من خلاله في شبكات الاتصالات عن طريق استعمال تردد النغمات، أن النغمات يمكن استعمالها لتنشيط وتفعيل رقم تليفون غير متصل بما يتيح القدرة لهذا الشخص لاستكمال هذه الخطوط غير المتصلة كما لو كانت خطوطه الخاصة، إنم الفوائد المترتبة على هذه التقنية تشمل تكلفة المكالمة التليفونية لتي تضاف إلى فاتورة التليفون غير المتصل، علاوة على منع حدود أو متابعة أو تقصي هذه المكالمة.

ويقصد بانتحال الهوية Iusurpation didentitie سرقة شخصية مستخدم آخر ويتطلب الوصل إلى الحاسب الآلي أو إلى الطرفيات معرفة دقيقة لمستعمل الجهاز.

كما أن فحص الهوية يرتكز على مجموعة معلومات متوافقة يستخدمها المستعمل ككلمة السر[1] أو أي جملة خاصة بالمستعمل أو أي خاصية فسيولوجية كالبصمة الرقمية أو ملامح للوجه أو هندسة الكف أو الصوت بالإضافة إلى أي شيء يمتلكه المستعمل كالبطاقة الممغنطة أو المفتاح المعدني. فلو تمكن أي إنسان من الحصول على هذه المجموعة من المعلومات المتوافقة يصبح قادراً على انتحال شخصية المستعمل وهناك مثال لشاب ذكي أدعي أنه صحفي في إحدى المجلات واتصل بشركة اتصالات هاتفية مدعياً أنه بصدد نشر مقالة عن النظام المعلوماتي المستخدم في الشركة، فدعته الشركة لزيارة مقرها

٢- تلاعب Pabx : وهو أسلوب تقني يمكن للشخص بموجبه أن يطلب رقم تليفون pabx (وهو صندوق تحويل معد يحتوي على عدد من خطوط التليفون المختلفة). ويتم من خلال توصيل مكالمتهم إلكترونياً لواحد من لخطوط في هذا الـ pabox ثم استعمال هذا الخط للأغراض الخاصة.

٣- الاتصال الخارجي بالكمبيوتر : وبموجب هذه الوسيلة يستطيع الشخص أن يتصل برقم تليفون معين يتيح لهم بدوره فرصة الوصول إلى نظام الكمبيوتر أو الوصول إلى مركز اتصالات يتيح لهم نفس المزايا الموضحة في الأسلوبين السابقين.

٤- Austpac : وهي شبكة اتصالات تشرف عليها هيئة المواصلات الرسمية التي تقدم وصلات معينة بين أنظمة الكمبيوتر، أن الفواتير الخاصة باستعمال هذا النظام تعتمد على استعمال شبكة التعرف على المستعملين Network User Identieication Cnut ويتكون هذا النظام عادة من سلسلة من ٩ أرقام وهي شبيهة من حيث المبدأ برقم الـ PIN.

٥- الغش في بطاقات الاعتماد : هذا الأسلوب التقنيي يتضمن اقتباس تفاصيل بطاقات الاعتماد الخاصة بأحد المشتركين الذي يقوم بدوره بطلب مكالمة تليفونية لصالح الطالب وقيد قيمة المكالمة على بطاقة الاعتماد.

٦- الاعتراض المادي : إن عملية الاعتراض المادي لخط تليفوني هي عملية بسيطة وتؤدي إلى نفس الفوائد مثل الاتصال بالنغمة.

٧- الوصلات غير القانونية : وهي عبارة عن تنشيط وتشغيل خدمة غير متصلة بدون علم شركة الاتصالات ثم استعمالها حسب رغبتك عن طريق تليفون عادي بدون أو تتلقي الفاتورة. وهذا النوع من الاعتراض يتميز بأنه دائم ومسمر.

انظر :

Franklinclrk, investigating computer crime, Ed. CRC page 50.

(1) بعض كلمات السر يتم وضعها من خلال مدير النظام المعلوماتي والبعض الآخر يتم استخدامه من وحي المستخدمين أنفسهم. وبصرف النظر عن ذلك فإن كلمة السر يجب أن تكون مميزة لكل حساب ويجب تغيير وحذف الحسابات التي ليس لها كلمة سر وينصح بتجنب استعمال كلمات السر التي يسهل الوصول إليها مثل استعمال الأسماء الأولى والأخيرة وتاريخ الميلاد وأرقام الضمان الاجتماعي أو رقم رخصة القيادة فهذه الكلمات يمكن التنبؤ بها.

كما يعرف القراصنة كلما السر الأكثر شهرة والتي يميل الناس إلى اختيارها لذا يحظر استخدامها مثل كلمة سر passwred وكلمة ادخل Enter وافتح Open وكمبيوتر Computer ويحذر هذا الاستخدام كلمات السر المرتبطة بالهواية كما يحذر تجنب كلمات السر ذات المقطع الكبير أو تلك المتعلقة بمجموعة حروف أو أرقام.

راجع في ذلك :

E. Quarantiello (cybercrime) p. 94.

وقدم له موظفيها عرضاً كاملاً ومفصلاً عن الأجهزة المعلوماتية وتطبيقاتها في الشركة وكانت النتيجة أنه سرق منهم معدات تزيد قيمتها على ١٠.٠٠٠.٠٠٠ دولار (مليون دولار) [١].

وفي حالة أخرى استطاع شخص أن يسرق بطاقات ائتمان ممغنطة لكل منها رقم سري يعرفه صاحبه حيث اتصل بأصحاب هذه البطاقات مدعياً أنه موظف بالمصرف وأخبرهم أنه قد نما إلى علمه أن بطاقاتهم قد سرقت وأنه بحاجة لمعرفة الرقم السري لحمايتهم وتزويدهم ببطاقات جديدة. وهكذا نجح المحتال في الحصول على الأرقام السرية لهذه البطاقات ثم استخدامها في سرقة مبالغ من المال من الموزعات الآلية للنقود[٢] des distributeurs وفي حالة ثالثة أرسل فيها بعض الطلبة مذكرة لكل مستخدمي الطرفيات في جامعتهم ذكروا فيها أن أرقام الاتصال قد تغيرت ومنحوهم أرقاماً جديدة تتصل مباشرة بأجهزة الكمبيوتر الخاص بهم والتي تمت برمجتها مسبقاً بشكل مطابق لأجهزة الجامعة. وهكذا كان يستخدم المستعمل الرقم السري الخاص به بدون تردد حيث يسجله الطلبة ويعاودون مراسلتهم مرة ثانية طالبين منهم أن يعودوا لاستخدام رقم الاتصال القديم. ولم تكن تلك سوي لعبة استخدام الطلبة من خلال كلمات السر most de pasdse .

<u>ثالثا: السطو المسلح الإلكتروني</u>

ترتب على ظهور تقنيات بث المعلومات على شبكة اتصالات بعدية telematique إلى نشوء مخاطر جديدة نتيجة للإمكانيات المستحدثة للدخول والاستفسار عن بعد من مراكز نظم المعلومات حيث تشكل عمليات بث المعلومات نقطة ضعف هامة في نظم المعلومات وذلك على النحو التالي :

١- التقاط المعلومات المتواجدة ما بين الحاسب الآلي والنهاية الطرفية :

يتيح هذا الالتقاط عن طريق توصيل خطوط تحويله un brnchement bretelles de derivaitions والتي ترسل إشارات إلكترونية "ذبذبات إلكترونية مكبرة" تمثل المعلومات المختلسة إلى النهاية الطرفية المتجسسة أو عن طريق مرسل صغير يسمح بنقل المعلومات من بعد. وعلى النقيض عندما تسلك المعلومات الطريق الجوي "كما في حالة البث عن طريق القمر الصناعي" توضع هوائيات مطاردة بالقرب من الهوائيات الاحتياطية والتي تسمح بالتقاط الاشعاعات faisceux واحتجاز مضمونها.

٢- التوصيل المباشر على خط تليفوني wiretape :

---

(١) انظر :

D. Parker, op. cit., p. 65.

(٢) راجع:

Burgess, Jean, (August 18, 2009), YouTube: Online Video and Participatory Culture, UK : Polity; 1 edition.

وقد سبق معرفة هذه التقنية في بعض المجالات وتباشر عن طريق وضع مركز تصنت unetable decoute يسهل تسجيل كل الاتصالات كما يمكن أن تؤدي هذه الوظيفة ميكروفونات صغيرة.

٣- التقاط الاشعاعات الصادرة عن الجهاز المعلوماتي Electromagnetic pickup

ويمكن عن طريق هذه التقنية إعادة تكوين خصائص المعلومات التي تتحرك وتنتقل من خلال نظام معلوماتي ويكفي لإتمام ذلك أن تسجل ثم تحل شفرة الاشعاعات الإلكترومغناطيسية المثبتة بواسطة أجهزة إلكترونية.

وفي الحقيقة تصدر بعض عناصر الأنظمة القوية وعلى وجه الخصوص الطابعات السريعة les imprimantesrapides أثناء تأدية وظيفتها إشعاعات الكترمغناطيسية، وقد ثبت أنه بإمكان شاحنة صغيرة مجهزة تجهيز خاص وقف بمحاذاة مبني مكتظ بالحاسبات الآلية، أن تلتقط وتسجل هذه الإشعاعات. ويمكن عن طريق جهاز لفك الرموز أن يطلب من طابعة متصلة بنظيرتها الموجودة في المركز المستهدف النسخ الحرفي لنفس هذه المعلومات.

٤- التدخل غير المشروع في نظام بواسطة طرفية phone Freak :

يمكن عن طريق تقنية telematique التدخل في نظام معلوماتي من بعد ثم يصبح بعد ذلك نسخ أو تدمير بعض المعلومات شيئاً سهلاً ويكفي لبلوغ ذلك الحصول على حساب آلي ميكروي ومودم Modem ولتزود بكلمة السر أو مفتاح الشفرة المناسب[١].

رابعا: جرائم الحاسب من خلال التعدي على وظائفه

وتعدد أنماط هذه الجرائم على النحو التالي :

١- تعديل المعطيات بدون إذن من صاحبه

أصبح تعديل المعطيات le tripatouillage des donnees تقنية سهلة وآمنة ومألوفة من تقنيات الإجرام المعلوماتى وهي تتمثل في تعديل المعطيات قبل أو أثناء إدخالها في نظم المعلومات أو في لحظة إخراجها من النظام المعلوماتي. ويمكن إجراء هذه التعديلات بواسطة أي شخص والذي ساهم أو له حق الولوج في عمليات نشاء وتشفير وتسجيل ونقل والتحقق من نقل البيانات المخصصة للإدخال في نظم المعلومات وهناك العديد من الأمثلة التي تنطوي على تزوير أو اختلاس الوثائق واستبدال الشرائط الممغنطة[٢] أو البطاقات المثقوبة أو أفعال تحطيم إدخال البيانات أو إحداث

---

(١) الدكتور محمد سامي الشوا، مرجع سابق، ص ٦٨ وما بعدها.

(٢) الشريط الممغنط : وهو شريط مغناطيسي يحوي المعلومات الخاصة بحامل البطاقة بعد تشفيرها بصورة إلكترونية ويمكن قراءة هذه البيانات باستعمال النهاية الطرفية الإلكترونية الموجودة بمقار البنوك ومنافذ البيع.

ثقوب إضافية في البطاقات المثقوبة أو على العكس سد هذه الثقوب وأخيراً أفعال التحييد أو إلغاء المراقبات اليدوية[١].

وأجريت في انجلترا ما بين عامي ١٩٨٣ و ١٩٨٦ دراسات مسحية قام بها Wong تتعلق بحالات الاحتيال في نظم المعلومات حيث تبين من خلالها أن ٦٣% من الحالات محل الدراسة قد ارتكبت عن طريق التلاعب في البيانات المدخلة أو في الوثائق الأصلية التي تستمد منها البيانات، وأن أبرز أشكال هذا التلاعب تم عن طريق تحويل المدفوعات من حساب إلى حساب آخر أو بوقف سداد المستحقات أو باصطناع موردين أو عملاء وهميين لهم مستحقات واجبة السداد أو بوضع أسماء زائفة لبعض الموظفين يستحقون أجوراً ومرتبات[٢].

ومن تحليل إجراء معهد ستانفورد الدولي للأبحاث (SRI) بالولايات المتحدة شمل مائة حالة من حالات إساءة استخدام الحاسبات، تبين أن ٣٧.٦% منها قد ارتكب بإحداث تغيير مباشر direct modification في البيانات المدخلة بينما وقع ٩.٥% منها فقط نتيجة تعديل وتلاعب في البرامج المستخدمة[٣].

٢- تقنية Superzapping :

يطلق مصطلح Superzapping على تقنية الاستخدام بأسلوب غير شرعي للبرامج الخدمية التي تؤثر على المعطيات المحفوظة في جهاز الكمبيوتر أو في ذاكرته وهذا التأثير قد يكون بالتعديل أو الإلغاء أو النسخ أو الإدخال أو الاستعمال أو المنع. ومصطلح Superzapping مشتق اسمه من Superzap وهو البرنامج الخدمي الذي يستخدم في العديد من مراكز نظم المعلومات كأداة نظام. وأي مركز نظم معلومات يسر وفقاً لخطة عمل ناجحة وفعالة لابد له من برنامج يلجأ إليه عند الحاجة بغرض التعديل أو الكشف عن أي غموض في جهاز الكمبيوتر.

وأحياناً تتوقف أجهزة الكمبيوتر أو لا تعمل بالكفاءة المرجوة ويصبح إصلاحها أو إعادة تشغيلها غير مفيدة وأحياناً أخرى يحتاج الكمبيوتر لعملية تعديل لا تسمح بها أساليب الولوج المألوفة. وفي مثل هذه الحالات فإن برامج الولوج الإجمالية تكون ضرورية، حيث يمكن تشبيهها في مثل هذه الأحوال بمفتاح يستخدم في حالات فقد كل المفاتيح الأخرى[٤].

---

(١) انظر في ذلك :

D. parker Op. Cit. p. 77

(٢) وهكذا استطاع أحد المسئولين عن نظم المعلومات بإحدى الشركات الفرنسية اختلاس أكثر من مليون فرنك فرنسي عن طريق إعادة ملفات الموظفين السابقين والذين لهم حقوق مالية وقامت بتحويلها إلى حسابه وحسابات أخرى تم افتتاحها خصيصاً لهذا الهدف وبعد ارتكاب الجريمة قام المجرم بمحو آثار كل فعل عن الغش المعلوماتي :

راجع في ذلك : Expertises no. 66 oct. 1984 مشار إليه في : د. محمد سامي الشوا، مرجع سابق، ص ٧٣.

(٣) راجع في ذلك الدكتور هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة، أسيوط، طبعة ١٩٩٤، ص ٥٩.

٤ راجع:

وهذه النوعية من البرامج الخدمية لها القدرة على فعل كل شيء وهي في نفس الوقت أدوات خطيرة إذا وصلت إلى أيدي أشخاص غير شرفاء لهذا يجب الحفاظ عليها بعناية ويجب أن توضع بمنأى عن المستخدمين غير الشرعيين. لكننا أحياناً نجدها في مكتبات البرامج، لذا فإن أي شخص سواء كان مبرمجاً أو مشرفاً فنياً والذي يعرف استخدامها ومكانها فإنه يمكنه الحصول عليها. وهناك مثال على سرعة هذا البرنامج تسبب في خسارة مقدارها ١٢٨.٠٠٠ دولار من أحد البنوك التي تقع في ولاية نيوجرسي حيث كان رئيس قسم الاستثمار لهذا البنك يستخدم برنامجاً من نوع Superzap لإجراء بعض التعديلات في الحسابات الراكدة le solde des comptes وتصحيح الأخطاء وفقاً للتوجيهات الممنوحة له من الإدارة حيث لاحظ أن التصحيح لا يتم على أحسن وجه. وفي أثناء محاولاته أيقن أنه من السهل إجراء التعديلات دون التعرض لأية رقابة ودون ترك أي دليل على قوائم المعطيات فبدأ يحول مبالغ إلى حسابات ثلاثة من أصدقائه وهو واثق أن الوسائل التكنولوجية ستعجز عن اكتشاف الاحتيال[١].

٣- تقنية الاسترجاع Recuperation

وهي عبارة عن تقنية يستخدمها شخص من أجل الحصول على معلومات موجودة في نظام معلوماتي أو قريبة من نظام معلوماتي بعد تنفيذ عمل ما. ويمكن أن يتمثل الاسترجاع البسيط والمادي في التفتيش في سلات المهملات لأجل الحصول على نسخ من القوائم الملقاة فيها أو العثور على ورقة كربون المستخدم في نسخ تلك القوائم وتستلزم الأساليب الأكثر تقنية وخداعاً للاسترجاع ضرورة البحث في المعطيات الموجودة داخل الحاسب الآلي بعد تنفيذ عمل ما، وعلى سبيل المثال لا يمكن لنظام التشغيل un systeme d'exploitation أن يمحو مناطق الذاكرة المغلقة les zones de memoiretampn والمستخدمة بواسطة الذاكرة المؤقتة لمعطيات الإدخال أو الخروج.

وهناك بعض أنظمة التشغيل التي لا تمحو مضمون ذاكرة الاسطوانة أو الشريط الممغنط والسبب في ذلك أن هذا العمل يستغرق وقتاً كبيراً. لذا فإن المعطيات الجديدة يتم كتابتها فوق المعطيات القديمة. ومن ثم يمكن بسهولة قراءة هذه المعطيات القديمة قبل أن يحل محلها المعطيات الجديدة. فإذا ما تم حفظ الذاكرة واستخدمت في عمل سابق ثم أسند إليها عمل جديد، فإن هذا الأخير يمكن من خلاله الولوج إلى نفس الذاكرة ولا يكتب إلا القليل من المعطيات لموجودة بهذه الذاكرة ولكن يمكن بعد ذلك أن يعيد قراءة كل محتوي الذاكرة المستولي عليها أو استعادتها، وكذلك البيانات المختزنة بواسطة العمل السابق.

٤- تقنية Chausse – trapes, techniques du cheval de troie et de salami

---

Nie, Norman and Erbing, Lutz (2000). Internet and Society: A Preliminary Report. Stanford Institute for the Quantitative Study of Society. Intersurvey Inc., and McKinsey and Co

(١) راجع :

D. Parker, op. cit., p. 85.

يقوم المبرمجون في مجال البرامج التطبيقية programmes d'application والتي تقوم بمعالجة البيانات الخاصة بالإدارة وأنظمة التشغيل والتي تنحصر مهمته في ضمان تشغيل أنظمة المعلومات بإدخال برامج اختبار وإضافة تعليمات تكميلية وأساليب للحصول على نتائج وسيطة ويمكن تشبيه هذه المساعدات بالسقالات المستخدمة في بناء المساكن. ومن بين أهداف نظام التشغيل مراقبة الولوج إلى النظام المعلوماتي من جهة، ومن جهة أخرى ضمان التحكم في استخدامه على نحو دقيق. وعلاوة على ذلك فهو لا يسمح لا بالتعديل ولا بإدخال تعليمات إلا باستثناء الحصول على تصريح لازم لمباشرة ذلك.

والذي يجب أن يكون على قدر من الدقة ويطبق حرفياً، ومن ثم فإن مبرمجي النظام يدخلون أحياناً أساليب منطقية ومؤقتة كي تسمح لهم بتخطي هذه القيود أثناء مراحل الاختبار وتزايد البرامج أو في مرحلة تأتي بعد ذلك عند صيانة النظام أو تعديله.

ويتغاضي المبرمجين أحياناً عن أخطاء موجودة في برامجهم وهذه لا يتم اكتشافها إلا في مرحلة الاختبار وتصبح بعد ذلك مهملة وعندئذ يضعون مختصرات والتي تخترق أساليب تصحيح البرامج وشروط استخدام النظام. وعلى سبيل المثال حينما يقوم برنامج يدعي "X" بالاتصال ببرنامج يدعي "Y" فإن المعطيات اللازمة لبرنامج "Y" فقط هي التي يجب أن تكون على قدر كبير من سهولة الوصول إليها.

وقد تكون الجهود الخاصة بالبرمجة اللازمة لجمع كل البيانات على قدر من الصعوبة في حين أن هناك تقنية على قدر كبير من البساطة ولكنها تبرهن على الإهمال وتتمثل في جعل المعلومات سهلة الوصول إلى البرنامج "Y" حيث يرشده إلى الأماكن الخاصة بالمعطيات والتي تسمح للبرنامج "Y" بالولوج إلى منطقة معطيات قريبة جداً وأكثر من اللازم، وهذا ينطوي على مخالفة مبدأ الامتياز الأقل moindre privilege.

والذي يقلل من معدل أمان النظام، وتبقي البرامج متزامنة في الذاكرة ويجب أن تصمم على نحو بحيث يحذر إحداها الأخرى كما لو كانت داخل بيئة عدوانية. والخسائر التي يمكن أن يسببها أي برنامج دخيل يجب أن تكون على نحو ضئيل. ويمكن أيضاً لمصممي البرامج الضخمة التدخل عن طريق السهو ومواطن الضعف وبسبب أوجه القصور على مستوي البرنامج أيضاً. ويكتشف المبرمجون المهرة – عند استخدام وصيانة البرامج والدوائر – بعض الفخاخ سواء لأجل تحقيق غايات مفيدة أو لتنفيذ أعمال غير مشروعة[1].

٥- القنابل المنطقية : Bombe Logique

إذا أراد محتال أن يسرق سيارة مصفحة مليئة بالنقود، فهو لن يفعل ذلك يوم الأثنين أو الثلاثاء ولكن سيختار بالأحرى يوم الجمعة لأن السيارة ستكون عندئذ مليئة بالمال ويتطابق الموقف في مجال

---

(1) انظر في ذلك :

D. Parker, op. cit. p. 93

الإجرام المعلوماتي وخصوصاً بالنسبة لأفعال الغش المبرمجة على الحاسبات الآلية ولكن يجب توافر بعض الشروط والتي يمكن اكتشافها بصفة آلية حتى يمكن أن ينجح الاحتيال وعلى نحو مؤكد. ومن هنا تصبح القنبلة المنطقية وسيلة سهلة وجذابة. والقنبلة المنطقية عبارة عن برنامج أو جزء من برنامج ينفذ في وقت محدد أو على فترات زمنية منتظمة ويتم وضعه داخل النظام المعلوماتي بهدف تحديد ظروف أو حالة محتويات النظام من أجل تسهيل تنفيذ عمل غير مشروع[١].

ويمكن على سبيل المثال إدخال تعليمات في برنامج نظام التشغيل (وهو البرنامج الذي يقوم بتحميل ذاكرة الحاسب بالبرامج المراد تنفيذها) وهو الذي ينفذ في كل مرة عمل جديد، وينصب البحث على عمل معين يمكن أن يكون محلاً للاعتداء، كأن تسعي القنبلة المنطقية إلى البحث عن حرق معين وليكن (حرف الباء) في أي سجل يتضمن أمر بالدفع وعندما تكتشفه تتحرك متتالية منطقية sequence loghique تعمل على إزالة هذا الحرف من السجل[٢].

والقنبلة الزمنية Bombe a retardement على عكس القنبلة المنطقية حيث تشير حدثاً في لحظة زمنية محددة بالساعة واليوم والسنة[٣]. ويتم إدخالها في برنامج وتنفذ في جزء من الملي ثانية أو في بضع ثواني أو دقائق وفقاً للتحديد المطلوب ويمكن على سبيل المثال ضبطها لكي تنفجر بعد عامين في يوم ١٢ يونيو الساعة أثنين وخمس وأربعون دقيقة (١٢.٤٥) عصراً لتحويل مبلغ من المال من حساب شخص معين تلاحظ في نفس اللحظة الذي يكون فيها مرتكب الجريمة متواجداً في البرازيل Riod Janeiro.

٦ - فيروس الحب:

تعاني شبكات الكمبيوتر من الإرهاب عبر الإنترنت بشكل متزايد وذلك على شكل محاولات متعددة لزرع فيروسات ببرامج الكمبيوتر عبر ملحقات البريد الإلكتروني. ومؤخراً فقد سبب فيروس الحب المدمر خسائر مدمرة لا تزال شركات عديدة تعاني منها، وأسلوب فيروس الحب في الهجوم يعتمد على إرسال رسالة مغزية شكلاً ومضموناً لحث المتلقين على فتحها. وفيروس الحب هو نوع من

---

(١) انظر في ذلك :

D. Parker, op. cit., p. 110.

(٢) انظر في ذلك:

Kraut, Robert et at (1998) . Internet Paradox : A Social Technology that Reduces Social Involvement and Psychological Well-Being . American Psychologist. V. 53, No. 9, 1017 – 1031

(٣) وعبارة أخري فالقنابل الزمنية : هي تلك الفيروست التي تطلق في تاريخ محدد. والقنابل المنطقية وهي تلك الفيروسات التي تطلق لشروط محددة.

راجع في ذلك :

Cr. Linda Volonino Cyber Terrorism. Op. cit.

الفيروس المعروف بـ "حصان طروادة" أو دودة البريد الإلكتروني وستظهر أنواع جديدة من هذا الفيروس قاردة على تهديد ملفات المعلومات الخاصة بالشركات التجارية الكبرى.

الطريقة التي يعمل بها فيروس الحب وما شابهه من فيروسات :

- يصل فيروس الحب على شكل رسالة إلكترونية عادية لها ملحق يسمي "رسالة حب لك نص" هذا في حال تعطيل خاصية الإظهار الكاملة لنهايات الملفات حيث أن الجزء الأخير من اسم الملف هو "في.بي.اس" وفي هذه الحالة يتنكر الفيروس في شكل رسالة بريدية نصية آمنة تماماً، بينما في الحقيقة تستطيع هذه الرسالة تنفيذ أوامر برمجة كمبيوترية مدمرة. وبعد فتح الملف المصاب بالفيروس، يقوم الفيروس بتنفيذ خمسة عمليات مدمرة :

١- يقوم بنسخ نفسه للعديد من الملفات الأخرى، بما يضاعف قدرته على الانتشار.

٢- يقوم بتعديل ملف التسجيل الخاص بالكمبيوتر المصاب حتى يمكنه إعادة تنفيذ البرنامج الخاص بالفيروس في كل مرة يتم فيها تشغيل الحاسوب، وكما يقوم ايضاً بتشغيل خاصية سرقة كلمة سر من موقع للإنترنت.

٣- يقوم بتحديد صفحة قياسية جديدة لبرنامج مايكروسوفت انترنت إكسبلورر.

٤- يقوم بإرسال رسالة بريد إلكتروني لكل مستخدمي الكمبيوتر المصاب وكذلك كافة قوائم التوزيع الموجودة بسجل العناوين الإلكترونية الخاص ببرنامج "أوت لوك".

٥- يقوم بإصابة كافة سائقات البحث بما في ذلك تلك الخاصة بالشبكة المستخدمة بالشركة والمرتبطة بالجهاز المصاب ويقوم الفيروس إما بحذف الملفات أو إخفائها ويستبدلها بنسخ منه.

<u>خامسا: أبرز جرائم تقانة المعلومات</u>

من الممكن التعرض بقدر من التفصيل لأبرز جرائم تقانة المعلومات بقدر من التفصيل وذلك على النحو التالي:

<u>١- جريمة العدوان على الائتمان الرقمي</u>

يعني الائتمان Credit إضافة مستقبلة للأموال المشمولة بالحماية بحيث تضمن هذه الإضافة كل التصرفات المالية للشخص. والمبدأ الأساسي في الائتمان هو الحماية، إذ برز الائتمان على إثر تصاعد حدة جرائم السرقة بالإكراه، والتي وصلت إلى أعلى معدلاتها في العدوان على الحياة في مقابل نهب المال من الضحايا. فالهدف يظل هو اختلاس الأموال إلا أن السارق فضلاً عن كونه يستخدم الإكراه فإنه كذلك يفضل ألا يترك أثراً وراءه يمكن أن يقود إليه. وعلى الرغم من كون قاعدة الحماية هي الأموال فإن الجريمة استطالت أيضًا الائتمان لكون إن الأموال عبر الائتمان تتحول إلى أرقام موضوعة على كروت يستلمها المؤتمن من المصرف الذي يتعامل معه.

ويتطور التقنية في ظل ثورة المعلومات نشط الائتمان، سيما عبر التجارة الإلكترونية/ الإنترنت على وجه التحديد. فالتعامل المالي عبر الإنترنت كما أنه استطاع استيعاب فكرة ظهور أشكال جديدة للنقود، فإنه كذلك يستطيع استيعاب فكرة الائتمان، خاصة إذا علمنا أن التعامل بالائتمان عبر الإنترنت له سوابق تاريخية. إذ يكفي أن تضع اسمك ورقم بطاقة الائتمان الخاصة بك لكي تصل إلى مبتغاك أو غرضك التجاري كالبيع والشراء والاشتراك في مؤسسات وأندية...الخ. ويمتد نشاط التعامل بهذه البطاقات إلى النواحي العالمية؛ إذ يجوز اختراق الحدود بمقتضى الائتمان[1] أو بالأحرى تقلص فكرة رقابة الدولة عليها[2].

وفي الفقرات التالية سوف نتعرض لموقف عدد من التشريعات المقارنة من هذه الجريمة ونتطرق بعد ذلك لمظاهر العدوان على الائتمان عبر الإنترنت.

أ- الجريمة في التشريع المقارن

كان التشريع الفرنسي من أوائل التشريعات التي قررت سلوك المسلك الجنائي حال العدوان الإجرامي على كروت الائتمان، وذلك منذ العام ١٩٨٨ بقانون Godfrain (نسبة إلى النائب الذي تقدم بمشروع القانون إلى الجمعية الوطنية) المؤرخ ١٩٨٨/١/٥، وهو القانون الذي أضيف إلى نص المادة (٥-٤٦٢ عقوبات فرنسي جديد) بشأن الاحتيال Faux على بطاقات الائتمان. ومما تجدر الإشارة إليه أن الاحتيال المذكور Faux قد تولى المشرع الفرنسي تفسيره على ضوء المادة (١-٤٤١- عقوبات فرنسي جديد). ويشار هنا إلى القانون المؤرخ ٣٠ سبتمبر ١٩٩١ المعدل للمرسوم المؤرخ ١٩٣٥/١٠/٣٠ بإصدار قانون الصك قد أضاف موادًا تتعلق ببطاقات الائتمان وذلك بالعقاب على تقليد Contrfacon وتزييف Falsification هذه البطاقات.

ب- مظاهر العدوان على الائتمان عبر الإنترنت

تتخذ أشكال العدوان على الائتمان عبر الإنترنت أحد شكلين:

(١) الاستيلاء على أرقام كروت الائتمان: إذ أن لكل كارت ائتمان عنوانًا فرديًا خاصًا ID number يتميز به عن غيره، تمنحه المؤسسة المالية للمشترك لديها في هذه الخدمة بحيث تحل محل التعامل بالأموال السائلة. ولقد امتد نشاط بطاقات الائتمان إلى الإنترنت فانفتح المجال لها لكي تضع عملية استخدامها في محك على درجة عالية من الخطورة إزاء مظاهر الاحتيال التي يتم بها الاستيلاء على أرقام هذه البطاقات بشكل غير مشروع، وعلى النحو الذي يحقق تكامل جريمة الاستيلاء على كروت ائتمان.

---

(١) د. حازم الببلاوي: النظام الاقتصادي الدولي المعاصر، عالم المعرفة، العدد ٢٥٧/الماء/ مايو ٢٠٠٠، الكويت، ص١٥٤.

(٢) المرجع السابق، ص١٦٥.

وعلى الرغم من أن اتجاهًا فنيًا يذهب إلى أن الحيازة غير المشروعة لأرقام كروت الائتمان التي تتم عبر الإنترنت إنما هي على درجة كبيرة من الصعوبة، كعملية تقنية تحتاج إلى برمجة معقدة، وبالتالي تعد حركة الحيازة المادية لها أسهل بكثير من حيازتها عبر الإنترنت فإن حالات اختلاس هذه الأرقام عبر الإنترنت من الخطورة بمكان وهو ما دفع المشروع الفيدرالي الأمريكي إلى عدها جريمة وفق 18 U.S.C. 1030(a)(1)(7) [1]. فقد حدث في عام ١٩٩٦ أن تم اختراق حاسوب محمول LAPTOP يحتوي على ٣١٤.٠٠٠ رقم لكروت ائتمان تخص أحد المكاتب التابعة لمؤسسة Visa Card INT في كاليفورنيا، وفي عام ١٩٩٧ قام Carlos Sadalgo Jr. (٣٧ عامًا) باستخدام حاسوب في جامعة سان فرانسيسكو واختلس أسماء مالكي وأرقام log-ons عدد ١٠٠.٠٠٠ كارت ائتمان وكذلك بيانات أخرى من خلال اختراقه لمجموعة مزودي خدمات إنترنت ISPs وقام بوضعها على اسطوانة مضغوطة CD ثم قام بتشفيرها وعرضها للبيع بمبلغ مائتين وخمسين ألف دولار، ولقد اكتشف عملاء المباحث الفيدرالية هذه الجريمة وحوكم سادالوجو وعوقب بالسجن ثلاثين شهرًا[٢].

(٢) العدوان على التوقيع الإلكتروني: التوقيع الإلكتروني كأحد مظاهر التوقيع عامة كان – ولا يزال – أحد اهتمامات المشرع المقارن، ومن ذلك المشرع الأوروبي الذي أصدر توجيهًا في عام ١٩٩٥ للشروع في تشكيل لجنة خبراء لكي تتولى وضع مشروع التوقيع الإلكتروني، وفي ١٦ الصيف/ يونيو ١٩٩٨ تقدمت اللجنة بمشروعها هذا مقترحة إصدار مجلس أوروبا توجيهًا بالخصوص، وفي ٢٢ الطير/ إبريل ١٩٩٩ وضع المشروع النهائي للتوجيه، ولقد قام البرلمان الأوروبي في ١٢ الكانون/ ديسمبر ١٩٩٩ بإعداد نصوص التوجيه المذكور ليخرج علينا في ثوبه الأخير. ولقد أصدر المشرع الألماني قانون الإنترنت لسنة ١٩٩٧ يتضمن مجموعة

---

[1] انظر:

- Hughes, Carole (1999). The Relationship of Use of the Internet and Loneliness among College Students. Dissertation Abstract . Vol. 60 (3 – A).

-

([2]) The CFAA makes it a crime for an unauthorized user to access a computer that is federally owned or is a « protected computer » for the purpose of 1) obtaining records from a bank, credit card issuer, or consumer reporting agency ; 2) committing fraud or extortion ; 3) transmitting destructive viruses or commands ; 4) trafficking in stolen passwords ; or 5) threatening to damage a computer system in order to extort money or other things of value. A « protected computer » is a computer 1) used exclusively by a financial institution or the United States Government ; 2) used on a nonexclusive basis but where the conduct affects use by the financial institution or the government ; or 3) used in interstate or foreign commerce or communication. This last element is intended to keep the federal government out of purely local computer crimes, but the multistate nature of Internet transmission suggests that almost any Internet activity will amount to « interstate commerce ». see : James Garrity & Eoghan Casey. Internet Missue in the Workplace : A Lawyer's Primer, op. cit., at 14.

نصوص حول الإنترنت المؤرخ في ٢٢ يوليو ١٩٩٧ ومن بينها نصوص تتعلق بالتوقيع الإلكتروني.

كذلك اعترف المشرع الفرنسي بالتوقيع الإلكتروني حيث تنص المادة (١٣١٦-٤) من القانون المدني الفرنسي بعد تعديلها بالقانون رقم ٢٣٠-٢٠٠٠ المؤرخ ١٣ مارس ٢٠٠٠ حيث تقرر بأن التوقيع الإلكتروني يعد وسيلة تعامل معترفًا بها، ومفترضًا صحته Pésumée إلى حين إثبات العكس. ولقد صدر المرسوم التنفيذي لهذا التعديل رقم ٢٧٢-٢٠٠١ المؤرخ ٢٠٠١/٣/٣٠ بشأن تطبيق المادة (١٣١٦-٤) من القانون المدني الفرنسي المتعلقة بالتوقيع الإلكتروني، حيث تضمن في المادة (١/١) تعريفًا أكثر تحديدًا للتوقيع الإلكتروني بأنه "معطيات ناتجة عن استعمال طريقة ردًا على شروط معرفة في صدر الجملة المقررة في الفقرة الثانية من المادة (١٣١٦-٦- مدني)".

وفي إطار النظام القانوني الإنجليزي استطاع القضاء الإنجليزي في قضية Goodman V. J. Eban. Ltd تحديد الأصالة Authentication بالإضافة إلى مناهج التوقيع الإلكتروني. على إن الأمر لم يقف عند هذا الحد وإنما قامت إدارة التجارة والصناعة الإنجليزية Department of Trade and Industry في مارس ١٩٩٩ بإصدار وثيقة استشارية Consultation Document بعنوان Building Confidence in Electronic Commerce تم هيكلتها على ضوء التوجيه الأوروبي المشار إليه أعلاه، وبناء على هذه الوثيقة أصدر البرلمان الإنجليزي قانون الاتصالات للمملكة المتحدة المؤرخ ٢٠٠٠/٥/٢٥ The UK Electronic Communications Act الذي ينص في القسم (٧) من على تعريف للتوقيع الإلكتروني[1]. وأما المشرع البلجيكي فقد أصدر القانون المؤرخ ٢٠ أكتوبر ٢٠٠٠ الذي أضاف إلى القانون المدني البلجيكي المادة (٢٢٨١) مقرراً الاعتراف بالتوقيع الإلكتروني إلى جوار اعترافه بالتوقيعات التي ترد عبر الفاكس والبريد الإلكتروني والبرقيات والتلكس وبأية وسيلة أخرى[2].

أما المشرع الأمريكي فقد اهتم اهتمامًا كبيرًا بموضوع التوقيع الإلكتروني لكونه أداة فعالة في حركة المعاملات المدنية والتجارية، وتحديدًا كان للمشرع الولائي الأمريكي الأسبقية في هذا

([1]) Section 7(1) provides: In any legal proceedings:
(a) an electronic signature incorporated into or logically associated with a particular electronic communication or particular electronic data, and
(b) the certification by any person of such a signature, shall each be admissible in evidence in relation to any question as to the authenticity of the communication or data or as to the integrity of the communication or data, See: Chris Reed- What is a signature?, op. cit., at 15.

([2]) 20 OCTOBRE 2000, Loi introduisant l'utitisation de moyens de télécommunication et de la signature électronique dans la procédure judiciaire et extrajudiciaire.
والمادة (٢٢٨١- مدني بلجيكي) هي المادة التي كان المشرع البلجيكي قد ألغاها بمقتضى القانون المؤرخ ١٩٤٩/١٢/١٥. ولقد أعادها إلى الحياة في ثوب جديد بمقتضى القانون المؤرخ ٢٠٠٠

الإطار، حيث أصدر مشرع ولاية Utah في عام ١٩٩٥ أول تشريع للتوقيع الإلكتروني The digital signature act of 1995 الذي تم إلغاؤه وإعادة إصدار تشريع آخر في عام ١٩٩٦، وكان من بين الأغراض التي سعى مشرع ولاية يوتا الأمريكية بإصداره هذا التشريع هو التخفيف من حدة الاحتيال بالتزوير والنصب على التوقيعات ككل[١]. ثم تلا ذلك ولاية كاليفورنيا بقانون ٥ سبتمبر ١٩٩٥ الذي، بعد أن اعتبر التوقيع الإلكتروني في مرتبة التوقيع المادي، قام بتعريف التوقيع الإلكتروني في القسم (٥-١٦) من كود الحكومة الولائية The Government Code بأنه "تحديد إلكتروني للهوية تم إعداده بواسطة الحاسوب ومعتمد من قبل مستخدمه لكي يكون له ذات القوة والأثر للتوقيع المادي أو اليدوي ولكن لا يشمل هذا التعريف إمكانيات التشفير"[٢]. ولتتولى بعد ذلك مظاهر الاهتمام بالتوقيع الإلكتروني من قبل المشرع الولائي الأمريكي مثل تشريع ولاية أويامنغ Wvoming لعام ١٩٩٥، ثم تشريع ولاية واشنطن Washington الصادر في ٢ مارس ١٩٩٦ الذي اعتمد على تشريع ولاية يوتا، ومما تجدر الإشارة إليه أن تشريع واشنطن تقرر نفاذه مع الأول من شهر يناير ١٩٩٨.

ولكي يتم العدوان على التوقيع الإلكتروني فإن ذلك يأخذ شكل العدوان على الأساليب الآمنة التي يتولاها طرف ثالث محايد Neutral Third Party، هو مقدم خدمات الإنترنت Online Service Provider OSPs، وذلك بالعدوان على وسائل التشفير الضرورية من مفتاح عام وآخر خاص. على إن الأمر قد يأخذ شكلاً آخر أكثر سهولة يتمثل في حالة تتبع التوقيع الإلكتروني لشخص ما، بما يستدعي الأمر هنا لزوم إحداث اختراق تام من خلال معرفة الخادم المشترك فيه هذا أو ذاك الشخص، ثم القيام بعد ذلك بالبحث فيه عن الهوية الإلكترونية IP الخاصة بذلك الشخص، حتى يتوصل إليها ثم بعد ذلك القيام باستنساخ التوقيع الإلكتروني خاص به.

ولقد ازداد الأمر تطورًا حال بروز فكرة البصمة الإلكترونية التي تتفق في التصنيف مع فكرة وحدانية التوقيع في العالم المادي. إذ أن البصمة الإلكترونية تعتبر عن وحدانية التوقيع من حيث نسبته إلى شخص واحد فقط. وتتخذ البصمة الإلكترونية هنا ذات الشكل التي هي عليه في العالم المادي فقد تكون على هيئة وضع بصمة الإصبع أو العين أو الأسنان أو الصوت...الخ، إلا أنها في كل الأحوال – سواء في العالم المادي أو الافتراضي – فإنها تحتاج إلى الآلة لإقرارها، فمثلاً من يريد الاتصال بحسابه المصرفي عبر الإنترنت، فإن الأمر لا يتطلب سوى وضع البصمة الإلكترونية على ماسح ضوئي خاص مرتبط بالحاسوب الذي يوصلها بحاسوب المصرف المذكور... وهكذا. ومثل هذا الاتجاه الجديد يمكن أن يكون أكثر ثقة في التعاملات

([1]) William E. Wyrough, JR & Ron Klein- The electronic signature act of 1996: Breaking down barriers to widespread electronic commerce in Florida, op. cit., at 429.

([2]) « An electronic identifier, created by computer, intended by the party using it to have the same force and effect as the use of a manual this definition does not include encryption. Further, signature », id at 431.

المالية لما تتمتع به بصمة الإنسان من ذاتية خاصة، حيث كل إنسان له بصمته الخاص. والعدوان على البصمة كما يمثل تزويرًا لتوقيع حيث تقوم البصمة مقام التوقيع إن لم تكن أقوى تأثيرًا منه، فإنه يمكن أن يكون الأمر كذلك عبر الإنترنت، حيث يقوم مقلد التوقيع بتزوير آليته.

٢- جرائم الأخلاق والترويج السمعي والبصري الفاضح

إن العدوان على الأخلاق عبر الإنترنت يُعد في الحقيقة من المشاكل التي جعلت الاصطدام قويًا بين المشرع والقضاء في القانون المقارن، ولقد احتلت مشكلة الأخلاق عبر الإنترنت حيزًا كبيرًا في بحوث الفقه المقارن، في عملية صراع كبيرة ما بين حرية التعبير واحترام أخلاقيات الشعوب. إذ أن المشرع المقارن لا يتوانى عن سن التشريعات التي تحمي القواعد الأخلاقية، إلا أن القضاء المقارن يقوم بإلغاء هذه التشريعات سعيًا وراء حماية حرية التعبير، كإحدى الحريات التي تتفوق على الأخلاق. ومع ذلك فإن المشرع، كردة فعل، يقوم مرة أخرى بإعادة سن التشريعات بغرض حماية الأخلاق، بحيث مثلت القاعدة الأخلاقية على هذا النحو تحديًا بين المشرع والقضاء في القانون المقارن. كما أن أشكال الجرائم الأخلاقية عبر الإنترنت تتميز بخصيصة ثابتة تتمتع بها كلها، وهذه الخصيصة تتمثل في أن كافة أنماط الجريمة الأخلاقية عبر الإنترنت تشترك في كونها لا تتجاوز الطابع المرئي/ المقروء، وغير المجسم، بحيث لا تسقط في مرحلة الحس الجسدي أو المادي، إلا إذا تحولت هذه النوعية من الجرائم إلى الاتصال المادي العادي بما يستدعي ذلك الخروج من العالم الافتراضي On line والعودة إلى العالم المادي Off Line، لذلك فمن غير المتصور أن تكون جرائم الأخلاق عبر الإنترنت جرائم مادية. وعليه فكل ما يمكن استحداثه من تقسيمات لنوعية جرائم الأخلاق عبر الإنترنت يجعلها كلها تشترك في طريقة تكوينها اللامادي أو المعنوي. ويظل السؤال هنا كامنًا في مدى إمكانية تعامل النصوص الجنائية الحالية مع جرائم الأخلاق عبر الإنترنت، وما إذا كانت هناك حاجة لتطوير النصوص المتعلقة بالجرائم الأخلاقية لكي تتوافق مع طبيعتها الرسمية وبحيث لا تكون الإنترنت وسيلة لارتكاب جرائم أخلاقية ويظل مرتكبها في مأمن من العقاب.

ويبرز هنا مصطلح الترويج لكونه قد يكون بمقابل أو بغير مقابل، فهو كمصطلح أعم من مجرد البث. والترويج وإن كان مجانيًا لا يعني إمكانية قيام الغير بملك منتجات ما، وإنما كل ما في الأمر أن انعدام المقابل إنما يعني انفتاح أو إمكانية وجود قدر من الحرية في استعمال الشيء أو المنتج.

ويمكن أن يتسع الترويج عبر الإنترنت كذلك ليشمل المحادثة الشفهية بأية وسيلة كانت كالتي تتم عبر الفيديو الرقمي أو البث الحي له بطريق الإنترنت أو بطريق الدوائر المغلقة كعرض الشهادة في المحاكم أو تناول موضوعات عامة عن بعد. ولعل أخطر مظاهر الترويج اسمعي المرئي هو أن يلحقه صفة الفضح فيما يصطلح عليه باللغة الإنجليزية بعبارة Cyber Audio

Visual Indecent –، فمثلاً القيام بالاتصال بالغير باستخدام الإمكانيات السمعية المرئية عبر الإنترنت، مع القيام بحركات أو إيماءات فاضحة، من الأمور التي يمكن أن تشكل جريمة ما هنا، ويزداد الأمر صعوبة حالة وجود نوع من التداول لمثل هذه الحركات السمعية المرئية الفاضحة، من خلال تسجيلها والقيام بتداولها عبر الإنترنت، والمشرع المقارن يهتم في صيغة تقليدية بمثل هذه الجرائم، من خلال التعامل بالفيديو في العالم المادي كما هو الشأن فيما هو مقرر في المادة (١/١٧٨- عقوبات مصري) [١] التي امتدت إلى المعاقبة على حيازة شرائط فيديو مخلة بالآداب، سواء كانت هذه الحيازة بقصد الاتجار أو العرض بمقابل أو بدون مقابل[٢]. وهو الأمر المعاقب عليه في القانون الأمريكي بمقتضى القسم (18 US Code Sec 2252) التي تعاقب على الاتجار والنقل Transporting والحيازة Possession لبرمجيات حاسوب تتضمن دعارة أطفال[٣].

على أنه نتيجة لتنوع أساليب الترويج السمعي المرئي الفاضح عبر الإنترنت، ما بين بث صور فاضحة ووثائق مكتوبة إلى عرض مرئي مختلف الأحجام، إلى ملفات صوتية تروي قصصًا جنسية. والغالب الأعم من هذه الأنماط والأنواع يتم بثه عبر شبكة المعلومات الدولية www. إلا أن البعض الآخر يتم ترويجه أيضًا عبر الشبكة القديمة كالمجموعات الإخبارية Use net Groups . فقد قام المشرع المقارن بتطوير آلية تشريعه لكي تتواءم مع هذا الأمر كما هو الشأن في التشريع الإنجليزي الذي وسع من فكرة النشر العلني Publication لمواد فاحشة Obscene matter المقررة في قانون الفحش العلني لسنة ١٩٥٩، بمقتضى قانون لعدالة الجنائية والنظام العام لسنة ١٩٩٤، لكي تشمل التداول بالحاسوب Computer Transmission لصور Images ونصوص Text[٤].

---

(١) تنص المادة (١/١٧٨- عقوبات مصري) على أنه "يعاقب بالحبس مدة لا تزيد على سنتين وبغرامة لا تقل عن خمسة آلاف جنيه ولا تزيد على عشرة آلاف جنيه أو بإحدى هاتين العقوبتين كل من صنع أو حاز بقصد الاتجار أو التوزيع أو الإيجار أو اللصق أو العرض مطبوعات أو مخطوطات أو رسومات أو إعلانات أو صورًا محفورة أو منقوشة أو رسومات يدوية أو فوتوغرافية أو إشارات رمزية أو غير ذلك من الأشياء أو الصور عامة إذا كانت منافية للآداب العامة.

(٢) طعن جنائي مصري رقم ٣١١٦ لسنة ٥٥ق جلسة ١٩٨٧/١٠/٢٨ المكتب الفني لمحكمة النقض المصرية السنة ٣٨ صفحة رقم ٨٧٨- ولقد أشارت المادة (٢/١) من قانون المطبوعات المصري رقم ٢٠ لسنة ١٩٣٦ (الوقائع المصرية العدد ٢٣ في ١٩٣٦/٣/٢- موسوعات التشريعات العربية) إلى أنه يقصد بالتداول بين المطبوعات أو عرضها لبيع أو توزيعها أو إلصاقها بالجدران أو عرضها في شبابيك المحلات أو أي عمل آخر يجعلها بوجه من الوجود في متناول عدد من الأشخاص. انظر: د. جميل الصغير، الأحكام الموضوعية، السابق، ص٨٩.

(3) USA v.Miller, App 11th Cir No.98-8228, Feb. 4-1999, Available online in March 1999 at: http://www.lp.findlaw.com/scripts/getcase.pl?navby=search&case.../988228man.htm

(4) Conseil Federal suisse: Message concernant la modification du code penal suisse et du code penal militaire (Infractions contre l'integrite sexuelle; prescription en cas d'infractions contre l'integrite sexuelle des enfants et interdiction de la possession de pornographie dure) du 10 Mai 2000, P.7/2775.

ومن الأشكال ذات الخطورة الخاصة في الترويج السمعي المرئي الفاضح عبر الإنترنت ما تتمتع به هذه الأخيرة من طبيعة اتصالية، إذ يمكن أن يقوم الأشخاص في هذا المجال بتبادل الأحاديث الجنسية، وهو ما يطلق عليه عبارة Cybersex، حيث يكون الحديث بين أشخاص لا يعرف بعضهم البعض، وبحيث يختلف الحال هنا عن الاتصال الذي يجريه الشخص بعاهرات بطريق الهاتف كنوع من الخدمات الإباحية التي تقدم في العالم الغربي في هذا المجال. حيث يمكن لأي أن يقوم بتنظيم نشاط إباحي عبر الإنترنت، كترتيب مواعيد جنسية وكذلك اختيار الهدف الجنسي من خلال العرض المرئي والسمعي مع دفع قيمة ذلك. كذلك يتم عبر الإنترنت الترويج للرقيق الأبيض وتجارة القاصرات ودعارة الأطفال بقصد الاستخدام الجنسي Cyber Teen في الوقت الذي يستمر مرتكب هذه الجريمة في حالة تخف قد لا يكون من السهولة التعرف عليه، خاصة إذا كان يباشر نشاطه عبر المواقع المجانية أو من خلال المجموعات الإخبارية أو القائمة البريدية[1].

ومن الوقائع الكبرى في مكافحة جريمة دعارة الأطفال تلك التي تعرف لدى الشرطة الإنجليزية، بعد تدخلها في يوليو ١٩٩٥ فيها بمصطلح Operation Starburst، حيث اتخذ التحقيق فيه هذه العملية بعدًا دوليًا، لاسيما وأن الإنترنت في هذه الواقعة قد استخدمت كمجال لدعارة الأطفال وتوزيع صور فاضحة للأطفال، ولقد أُدين في هذه الجريمة تسعة رجال إنجليز، كما تم الاستدلال على مجموعة أخرى عبر أوروبا وأمريكا الجنوبية وشرق آسيا وصل عدد المدانين في هذه الجريمة إلى سبعة وثلاثين شخصًا[2]. كما قامت المباحث الفيدرالية الأمريكية بالتحقيق في قضية أطلق عليها Innocent Images، وهو التحقيق الذي بدأ على إثر اختفاء طفل أمريكي، من ولاية مريلاند، في العاشرة من عمره. وهي القضية التي أُدين فيها ١٦١ شخصًا. وفي العام ١٩٩٧ كانت قضية Operation Rip Cord التي قامت بها المباحث الفيدرالية بالقبض على ١٥٠٠ شخص من المشتبه فيهم بالتعامل في دعارة الأطفال عبر الإنترنت وبث صور فاضحة Child pornographers للقصر. ولقد قادت عمليات البحث والتقصي حول دعارة الأطفال عبر الإنترنت، في ألمانيا والمملكة المتحدة والولايات المتحدة الأمريكية، إلى الكشف عن مائتي ألف صورة من صور دعارة الأطفال، كما تمت مصادرة مائة وسبعة وثلاثين ألف حاسوب شخصي/ منزلي Home PC. وفي العام ١٩٩٨ قام البوليس الإنجليزي بعملية كبرى أطلق عليها اسم Cathedral بالتعاون مع الشرطة في ٢١ دولة في أوروبا وأستراليا والولايات المتحدة والبوليس الدولي الإنتربول لضبط حوالي مائة شخص ممن يتعاملون في دعارة الأطفال عبر الإنترنت.

وفي شهر أكتوبر ٢٠٠٠ قام المدعي العام الإيطالي بإحالة ١٤٩١ من الإيطاليين إلى القضاء، لكونهم قاموا بإنزال download صور دعارة أطفال Child pornography عبر

---

(1) لمزيد من التفصيل في هذه القضية انظر الموقع التالي:
http://www.leeds.ae.uk/law/pgs/vaman/watchmen.htm

(2) Dr. Andrzej Adamski, op. cit at 223.

الإنترنت، بعد أن قامت الشرطة الإيطالية بتفتيش ستمائة منزل، وبينهم تسعة أشخاص كانوا يتاجرون في دعارة الأطفال عبر روسيا. وتعد هذه الدعوى الأكبر في إيطاليا في ذلك التاريخ، حيث قام المدعي العام الإيطالي Alfredo Ormanni بإحالة ٨٣١ متهمًا إلى القضاء الجنائي، وتم استدعاء ٦٦٠ من جنسيات أجنبية ويعتقد أن أغلبهم من روسيا وفرنسا وماليزيا[١].

وقد اهتمت التشريعات المقارنة بظاهرة الترويج السمعي - المرئي الفاضح، وبصفة خاصة موضوع دعارة الأطفال التي أخذت من المشرع المقارن اهتمامًا كاملاً في هذا الإطار. ففي الولايات المتحدة نشط الفقه والقضاء والتشريع في دراسة نظم القانون الأخلاقي وعملية نظمه في القانون الجنائي، على إثر الكارثة الحقيقية الممثلة في دعارة الأطفال عبر الإنترنت، وهي ظاهرة اعتبرت هناك خطرة على المثل القومية التي تقوم عليها دعائم المجتمع الأمريكي[٢]! لكون الإنترنت وسيلة تجعل ارتكاب مثل هذه الجرائم سهلاً، أو بمعنى أكثر دقة تجعل من الممكن ومن ثم توفر المناخ الملائم للحصول على ضحايا في مثل هذه النوعية من الجرائم. ومثل هذا الأمر جعل الفقه والقضاء والتشريع في الولايات المتحدة يتجه إلى الاستمرار في دراسة دعارة الأطفال عبر الإنترنت – وذلك بإيعاز من البيت الأبيض الأمريكي في بيانه المؤرخ ١٩٩٦/١/٢٦ الذي صدر ردًا على إلغاء القضاء الأمريكي لنصوص في قانون أخلاق الاتصالات لسنة ١٩٩٦ المعدل للقانون الصادر في ١٩٣٦[٣].

ونتيجة لمبادرة البيت الأبيض المذكورة فإنه في عام ١٩٩٨ أصدر الكونجرس الأمريكي القانون رقم Public Law 105-314 بشأن حماية الأطفال من التعدي الجنسي[٤]. ولقد تضمن هذا القانون حث النائب العام الأمريكي على التعاون مع الأكاديمية الوطنية للعلوم/ مجلس البحوث الوطنية فيها، على إعداد دراسة متكاملة لبحث مدى إمكانية تفعيل القانون الجنائي في القضايا الأخلاقية، والتي أنتجها التعامل السلبي مع تقنية المعلومات/ الإنترنت. على أن يتم وضع هذا التقرير في خلال سنتين من تاريخ صدور القانون المذكور. ولقد تم وضع التقرير في العام ٢٠٠٠ متضمنًا الخطوات الفعالة من الوجهة العلمية من قبل الأستاذين Herb Lin, PhD, Michele Kipke, PhD، بالتعاون مع جهات أخرى ذات علاقة. ولقد وجد التقرير إن مشكلة الدعارة المصورة Pornography ذات أساس من ناحيتين، الأولى كونها تعد داخلة في نطاق اهتمام قسم اجتماعي له دور في المجتمع، حتى وإن كان سلبيًا. أما

---

(1) Martin Stone, Italians charge 1491 in online pedophile sting, newsbytes, 30 Oct. 2000. http://www.newsbytes.com/news/00/157391.html.

(2) Herb Lin, PhD hlin@nas.edu, Michele Kipke, PhD mkipke@nas.edu – Tools and Strategies for protecting kids from pornography and their applicability to other inappropriate internet content, op. cit, P.1.

(3) Reno v. ACLU, US Supp. 521 U.S. 844 (1997).

(4) Protection of children from Sexual predators act of 1998 Title 9 section 901. US Code. Id at 422.

الناحية الثانية فيتعلق بالتحديد القضائي لمصطلح الدعارة الذي يتخذ مفهوم يتسع ليشمل الطابع المتغير فيها vary widely من نطاق اجتماعي إلى آخر Vary by community[1].

كذلك يجرم القانون الأمريكي تشغيل Employ القصر Minors أو دفعهم Induce إلى المشاركة في صور متحركة Visual depiction تتضمن حركة جنسية مباشرة، إذا كان التصوير قد تم باستخدام حاسوب عبر مؤسسات تجارية في الولايات أو في خارج الولايات المتحدة (18 US Code Sec. 2251). كذلك يحظر القانون الأمريكي استخدام الحاسوب لبيع Sell أو نقل Transfer حق الوصايا على قاصر مع العلم بأن هذا القاصر سوف يتم استخدامه لإعداد صور متحركة تتضمن سلوكًا جنسيًا مباشرًا (18 US Code Sec. 2251 ((A). كما يجرم القانون الأمريكي استخدام الحاسوب لنقل Transport دعارة الأطفال Child pornography عبر الولايات أو عبر مؤسسات تجارية أجنبية (18 US Code (Sec. 2252 & 2252 (A)[2].

أما في فرنسا فإن المادة (٢٤-٢٢٧) من قانون العقوبات الفرنسي الجديد تعد حجر الأساس في إطار دعارة الأطفال[3]. حيث يعاقب معد مواقع دعارة الأطفال وفقًا للمادة (٢٤-٢٢٧) في فقرتها الأولى من ذات القانون، أما الفقرة الثانية منها فتعاقب مستخدم الموقع. وأما قانون العقوبات البلجيكي فقد تضمن في المادة (383 bis) منه (المضافة بالقانون المؤرخ ١٩٩٥/٤/١٣) [4] العقاب على عرض Expose وبيع Vendu وتأجير Loue وتوزيع Distribute أو دعم موقع مرئي Remi des supports Visuals لأوضاع جنسية ذات طابع فاحش Pornographique، وذلك باستخدام قصر ممن لم يبلغوا السادسة عشر من عمرهم، ويعاقب كذلك معد مثل هذه المواقع وكذلك مستوردها[5].

([1]) Herb Lin, PhD hlin@nas.edu, Michele Kipke, PhD mkipke@nas.edu – Tools and Strategies for Protecting Kids from Pornography and Their Applicability to other Inappropriate Internet Content, P.4.

([2]) USA v. Hay, App. 9th Cir. No. 99-30101, 24 Oct. 2000, Available online in Oct. 2000 at: http://laws.findlaw.com/9th/9930101.html.

([3]) Guillam Desgens – Pasanau, Au Centre des debat actuels: La protection des mineurs sur l'internet -24/7/2001. disponible enligne en Juillet 2001 a: http://www.droit-technologie.org/1.2.asp?actuid=1604298204.

انظر القانون رقم ٩٨-٤٦٨ المؤرخ ١٩٩٨/٦/١٧ بأن منع والمعاقبة على الجرائم وحماية القصر تعاقب كل من يقوم ببث مواقع دعارة أطفال.

([4]) Sur le plan penal, deux infractions contenues dans le Nouveau Code Penal (NCP), ayant pour finalite la protection des mineurs, meritent, concernant le reseau Internet, une attention particuliere. Ainsi: - "le fait, en vue de sa diffusion, de fixer, d'enregistrer ou de transmettre l'image d'un mineur lorsque cette image presente un caractre pornographique".

([5]) Thibault Verbiest – Pornographique e Internet: comment reprimer? 19 Mai 2001, disponible enligne en juin 2001 a:

٣- جرائم السب والقذف والتشهير والمراسلة

تُعد هذه الجرائم من أقدم الجرائم المرتكبة عبر الإنترنت، وذلك لما يتمتع به عضو الإنترنت دائمًا – وبحسب المعتقد السائد – من حرية كاملة عبر الإنترنت، لذلك يجب ألا نستغرب إذا كنا قد ارتكبنا أيًا من الأفعال المشار إليها عبر الإنترنت في المساء، لنجد في صباح اليوم التالي دعوى تباشر ضدنا في أحد المحاكم وإعلانًا بالحضور لسماع الحكم علينا لأنه في يوم....الخ.

(أ) السب: وهو خدش شرف شخص أو اعتباره في حضوره، وذلك بتوجيه كلمات مقذعة في مواجهة شخص أو أشخاص معينين بدقة كافية[١]، على أن يكون حاضرًا كل من الجاني والمجني عليه الواقعة، ويشمل السب والقذف نسبة وقائع معينة لكي يصل إلى مجرد توجيه عبارات تعد خدشًا للشرف والاعتبار دون أن يكون فيه إسناد لواقعة معينة كما هو الشأن فيما هو مقرر في المادة (٣٠٦- عقوبات مصري) [٢]. وإن كانت بعض التشريعات تتطلب أن تكون الواقعة علنية. وذلك مثلما هو الحال فيما تقضي به المادة (R-624-4) من قانون العقوبات الفرنسي الجديد التي تنص على أنه "السب غير العلني الواقع في مواجهة شخص أو مجموعة أشخاص بسبب الأصل أو الانتماء أو عدم الانتماء، حقيقة أو مفترضا، على عرض أو أمة أو عنصر أو دين محدد، معاقب عليه بالغرامة المقررة على الجنحة من المستوى الرابع"[٣].

(ب) التشهير: والتشهير Libel من جرائم البث المباشر في القانون، وهو في كل الأحوال نوع من القذف، وإن كان يستلزم في القانون الأمريكي أن يكون كتابة. في حين أن التشهير بالكلام يُطلق عليه في المصطلح الأنجلوفوني Slander. فالأساس الذي يعتمد عليه التشريع الأمريكي في إطار التشهير ينطلق من تهديد سمعة شخص ما Man's Reputation التي تمثل المصلحة التي يحميها القانون هنا. حيث يؤدي التشهير إلى التقليل من قدر الشخص في نظر المجتمع والناس أيًا كانوا، مثل أقاربه وجيرانه والأشخاص الذين لهم علاقة بهم أيًا كانت نوعية هذه العلاقة، كما لو كانت هذه العلاقة عائلية أو شخصية أو تجارية أو مالية...الخ.

وهو ذات الأمر في القانون الفرنسي فالمادة (R. 624-3) من قانون العقوبات الفرنسي الجديد تنص على أنه "القذف غير العلني يقع في مواجهة شخص أو مجموعة أشخاص بسبب أصلهم أو انتمائهم أو عدم انتمائهم، الحقيقي أو المفترض، إلى عرق أو أمة أو جذر أو

---

http://www.droit-technologie.org/1.2.asp?actu.id=2099182987.

(١) طعن جنائي مصري رقم ٢٠٤٧١ لسنة ٦٠ق جلسة ١٩٩٩/١١/١٤. المحامي/ مصر ع. ١ لسنة ٢٠٠١، ص٢٠٦.

(٢) طعن جنائي مصري رقم ١٢٩٥٢ لسنة ٦٠ق جلسة ٢٠٠٠/٢/٢٢. المحامي/ مصر ع. ١ لسنة ٢٠٠١، ص٢٠٦.

(3) Art (R-624-4-CPN Fr.) « L'injure non puplique commise envers une personne ou un groupe de personnes a raison de leur origine ou de leur appartenance, vraie ou supposee, a une ethnic, une nation, une race ou une religion determince est punie de l'amende prevue pour les contraventions de la de classe ».

دين"[1]. كما تنص المادة (٤٣٩- عقوبات ليبي) على أن يعاقب بالحبس مدة لا تزيد على سنة أو بغرامة لا تجاوز خمسين دينارًا كل من اعتدى على سمعة أحد بالتشهير به في غير حضوره لدى عدة أشخاص، وذلك في الأحوال المنصوص عليها في المادة السابقة. وإذا وقع التشهير بإسناد واقعة معينة تكون العقوبة الحبس الذي لا تتجاوز مدته السنتين أو الغرامة التي لا تجاوز السبعين دينارًا. وإذا حصل التشهير عن طريق الصحف أو غيرها من طرق العلانية أو في وثيقة عمومية تكون العقوبة الحبس الذي لا يقل عن ستة أشهر أو الغرامة التي تتراوح بين عشرين دينارًا ومائة دينار. وإذا وجه التشهير إلى هيئة سياسية أو إدارية أو قضائية أو إلى من يمثلها أو إلى هيئة منعقدة انعقادًا صحيحًا لتزاد العقوبة بمقدار لا يجاوز الثلث".

(ج) السب عبر الإنترنت: إذا كان الفقه والقضاء قد وجد صعوبات حال البحث عن معيار يمكن بمقتضاه التمييز بين ما هو مقرر في التشريع من تمييز بين الطريقة التي يمكن بها ارتكاب السب والقذف[2]، فإن الأمر استقر فيما يبدو على المعيار الاحتياطي الدائم، وهو معيار واقعي مستمد من البحث في كل حالة على حده، وذلك لصعوبة التمييز بين السب والتشهير في الحالة الواقعية التي يكون فيها الفرد قائمًا وحاضرًا أمام الجاني. أما في الحالة الاعتبارية فإن المشرع كثيرًا ما يقوم بتحديد حالات يكون فيها المجني عليه غير حاضر واقعة السب حضورًا ماديًا كاملاً وإنما جزئيًا بحيث يستشعر أحد أعضاء المجني عليه واقعة السب كما هو الشأن في سماعة ورؤية واقعة السب عبر الاتصال الهاتفي والهاتف المرئي أو البرقي أو الكتابة في محرر أو إعداد رسوم ما، في حين إن التشهير يلزمه، فضلاً عن عدم وجود الشخص أو حضوره الواقعة، أن ترتكب أمام عدة أشخاص، كما يمكن أن ترتكب في الصحف أو غيرها من طرق العلانية أو في وثيقة عمومية، إذ كل ما يتطلبه المشرع في واقعة التشهير ألا يكون المجني عليه حاضرًا. أما إذا كان الشخص حاضرًا فإن الواقعة في هذه الحالة تكون سبًا وليست تشهيرًا.

لذلك فإن النطاق المادي لبحث مدى توافر واقعة السب وتمييزها عن التشهير يستلزم الحضور المادي كليًا أو جزئيًا لواقعة الجريمة، حتى يمكن القول بأن الواقعة تكون جريمة سب أو جريمة تشهير. ففي واقعة السب والقذف فإن الركن المادي يتم بناؤه على أساس تحديد شخص المجني عليه وتعيينه التعيين الكافي لا محل معه للشك في معرفة شخصيته[3]. على أن الأمر هنا ليس بهذه السهولة عبر الإنترنت، ذلك إنه لما كان من الصعوبة، إن لم يكن من

---

(1) La diffamation non puplique commise envers une personne ou un groupe de personnes a raison de leur origine ou de leur appartenance ou de leur non-appartenance, vrai ou supposee, a une ethnie, une nation, une race ou une religion determinee est punie de l'amende prevue pour les contravention de le 4e classe ».

(2) David Loundy – Computer information systems Law & system Operator Liabilty, the Seattle Uni. Law Review, Vol. 21, No.4, Summer 1998, P.16.

(٣) طعن جنائي مصري رقم ٢٠٤٧١ لسنة ٦٠ق جلسة ١٩٩٩/١١/١٤ (المحامي – صر العدد ١ لسنة ٢٠٠١، ص٢٠٩).

المستحيل، توافر الحضور الكلي للمتهم والمجني عليه حتى يمكن القول بوجود سب ما، فإن المسألة يمكن أن تكون محل جدل فيما يتعلق بارتكاب السب الجزئي. ذلك إنه يختلف الحال حول هذه المسألة فيما إذا كان المجني عليه حاضرًا على الإنترنت وفي حالة اتصال مباشر مع الجاني، كما لو كان الاثنان معًا في إحدى حلقات الناقش، وما إذا كان الاتصال مباشرًا بينهما أم إن الجاني يتحدث مع آخرين دون حضور للمجني عليه (تشهير) أم بحضور المجني عليه (سبًا) حسب الأحوال.

ومما يدخل في إطار التشهير قيام الجاني ولو باستخدام الاستعارة ببث رسالة باستخدام حلقات الناقش[١] وكذلك عبر قوائم المراسلة Mailing List التي تذخر بها المواقع عبر الإنترنت للتعبير عن الرأي أو الفكرة وكذلك البريد الإلكتروني[٢] إلى عدد غير محدود، وفي هذه الحالة يستفيد المجني عليه من الاحتمال إذا وصلته نسخة من هذه الرسالة. أما إذا لم تصله فإن الأمر يظل في إطار التشهير كقاعدة، وفي هذه الحالة فإن المثار هنا هو موضوع العلانية التي نرى توافرها عبر الإنترنت، إذ كل ما يتطلبه المشرع في التشهير أن تكون واقعته قد تمت لدى عدة أشخاص، دون استلزام لما إذا كان حضورهم المادي متطلبًا أم لا، وهو غير الأمر فيما يتعلق بالمحررات حيث يلزم أن يعترف المشرع بالوجود الرقمي لهذه المحررات. وتُعد حلقات النقاش والقوائم البريدية أو التراسلية مجالاً حيويًا لتطبيق قانون النشر الصحفي على وقائع التشهير عبر الإنترنت في فرنسا بمقتضى القانون المؤرخ ١٨٨١/٧/٢٩ بشأن الصحافة المعدل بالقانون المؤرخ ١٩٨٦. فالقانون الأخير يميز بين القذف وبين الإساءة بالسب وقفًا للمادة (٢٩) منه، حيث تُعرّف المادة الأخيرة القذف بأنه كل ادعاء أو اتهام بفعل يجلب عدوان على سمعة أو اعتبار لشخص ما أو لمجموعة ينسب إليها الفعل"[٣]. على أن السؤال الأكثر إثارة للجدل يتعلق بموضوع مضمون الرسالة التي يمكن أن تكون مجرمة بمقتضى التشريعات المختلفة في هذا الإطار.

(د) كون المراسلة الإلكترونية مجرمة

يُعد نظام التراسل فحوى الاتصال بالإنترنت، وإذا كانت التطورات المعاصرة في تكنولوجيا المعلومات قد وصلت إلى حدود الاتصال الفوري بالصوت والصورة، بحيث يجعل الإنسان في حركة اتصالية مباشرة مع الغير، دون اعتبار لما إذا كان هناك حاجز مادي من أي نوع، فإن مثل هذا الأمر بالطبع لن يترتب عليه تراجع من أي نوع أيضًا لنظام التراسل عبر الإنترنت. ولذلك عدة أسباب أبرزها على الإطلاق مسألة الاعتراف القانوني بموضوع الرسالة

---

(1) Guillame Desgens – Pasanau – Du Bon Usage d'un Forum de discussion, P.3- disponble en ligne en 13 Mars 2001 a : http://www.droit-technologiw.org.

(2) David Loundy, op. cit., at 17.

(3) L'article 29 de la Loi du 29 juillet 1881 definit la diffamation comme « toute allegation ou imputation d'un fait qui porte atteinte a l'honneur ou a la consideration de la personne ou du corps auguel le fait est impute ».

الإلكترونية تحديدًا حيث أخذت الرسالة الإلكترونية حظها القانوني ووصلت إلى مستوى الرسمية في هذا الإطار. بحيث يمكن تقديمها كدليل أمام المحاكم وذلك كنتيجة طبيعية للاعتراف القانوني المذكور بمخرجات الحاسوب.

والمراسلة الإلكترونية يتسع مدلولها لأبعد من الرسالة التي تبث عبر الإنترنت في صيغة رسالة عبر نظام البريد الإلكتروني. إذ يتسع مدلولها ليصل إلى قائمة التراسل أو ما يطلق عليها في المصطلح الإنجليزي **Mailing List**، وهو نظام تراسلي جماعي يمنح صلاحية بث رسالة إلى مجموعة من الأشخاص، قد تجمعهم أفكار مشتركة حول موضوع ما أو موضوعات متعددة، قاموا بتسجيل بريدهم الإلكتروني مسبقًا في هذه القائمة، بقصد تناول هذا أو ذاك الموضوع، فيقوم هذا النظام ببث هذه الأفكار التي أرسلها هذا أو ذاك العضو في هذه القائمة لكل من يشترك فيها من أشخاص دون حاجة لأن يكون على دراية بهم أو بشخصياتهم. وغني عن البيان أن مثل هذا النظام التراسلي كان قد نشأ في ظل أفكار العمل الجماعي، بحيث يتم تداول الأفكار في إطار المنظمة الواحدة حول موضوع ما، فهو في الحقيقة نظام مشجع للعمل الجماعي، حال تطلب وجود أكثر من رأي فيما يخص أحد الموضوعات.

ومما يندرج في إطار التراسل الإلكتروني أيضًا، كأثر لاتساع مدلوله عما هو عليه الحال في العالم المادي، ما يسمى بنظام حلقات النقاش **Newsgroups**، وهي تتناول في موضوعها جلسة لمناقشة موضوع أو موضوعات فورية، أو حديث الساعة. وقد تكون في إطار مجموعة على معرفة بأحدهم الآخر، بحيث يكون دور الدخيل مجرد دور استفهامي، وبحيث يترك سؤالاً فقط لأحد المناقشين دون أن يتدخل في موضوع المناقشة حيث يكون ذلك غير مسموح به، أو أن يسمح في مثل هذه المجموعات للغير بالدخول في حلقة النقاش فيطرح أفكاره علنًا على مجموعة النقاش هذه، كما لو كان الأمر مباحًا للجميع في المشاركة. والواقع أمام تعدد أنواع وبدائل النظام التراسلي عبر العالم الرقمي، فإن الأمر يبرز كما لو كان هناك نوع من الخلط، وبحيث يطغى هذا الخلط على تحديد التكييف المناسب للعدوان في هذا الإطار، وفيما إذا كان الأمر ينطبق عليه مفهوم الرسالة كما هي معرفة في العالم المادي أم أن لها مفهوما آخرًا موسعًا، وبحيث يكون مدلوله متوافقًا مع الصورة التي يمكن استخدامها بها في العالم الرقمي.

ومما يؤخذ في الاعتبار هنا إن القانون الجنائي المقارن يأخذ في الاعتبار الكيفية التي يتم بها التراسل ماديًا، دون أهمية لعامل الوقت، وبحيث يعد زمن الاتصال يبدو كما لو لم يكن له قيمة في هذا الشأن. إذ عديدة هي النصوص التي تشتبه على الكتابة، مثل الإبراق والفاكس والاتصالات الهاتفية، ومن ذلك ما هو مقرر في تشريع ولاية أركانساس الأمريكية **ARK CODE ANN. 5-41-108 (2000)** الذي يعترف بارتكاب جريمة التخويف أو الترهيب أو التهديد أو الإساءة ضد أي شخص باستخدام البريد الإلكتروني أو أية وسيلة اتصال أخرى، أو أني قوم الشخص بارتكاب جريمة بالمراسلة حال إرسال رسائل دعاية مثيرة وغير منظمة **Unsolicited bulk email** باستخدام شخصية وهمية **Forged identity**، مثلما هو

الحال في تشريع Illinois الذي يعاقب على تزييف أو تزوير Falsifies or forges التحويل المعلوماتي بطريق الرسالة الإلكترونية بأية مضمون، حال كون موضوع هذا التراسل بريد تافه عبر الإنترنت غير معروف مصدره.

وعليه يتسع مدلول الرسالة المجرمة عبر الإنترنت لكي تشمل في محتواها ليس فقط جرائم الأخلاق، وإنما أيضًا جرائم أخرى تتخذ الطابع التقليدي، كما هو الشأن في جرائم التهديد بالقتل أو بارتكاب جريمة ضد النفس والمال. كما يتسع أيضًا مدلولها في إطار الجريمة التقنية بحيث تتخذ أبعادًا تقنية محضة، كما هو الشأن في تخريب قواعد البيانات أو هدم نظام المعلومات باستخدام الرسائل الإعلانية مجهولة المصدر. ولعل أشهر قضية تهديد هي تلك التي قام بها Christopher James Reincke (١٨ عامًا) طالب في جامعة Illinois بالولايات المتحدة الأمريكية، حيث قام في ٢٠٠١/١٢/٤ بإرسال رسالة عبر البريد الإلكتروني إلى الرئيس كلينتون وقام بتهديده فيها بالقتل.

وفيما يتعلق بطبيعة العبارات التي استخدمت في السب والقذف، فإنه لا يختلف حالها عما هو عليه الحال في العالم المادي، إذ تستخدم ذات العبارات التي يتم استخدامها في العالم المادي في جرائم السب والقذف والتشهير عبر الإنترنت. ولا يقدح هنا في عملية التغاير والاختلاف الاجتماعي والثقافي بين الشعوب للقول بعدم إمكانية تحديد مفهوم العبارات المستخدمة. ذلك أن تحديد مرامي العبارات وتحري مطابقة الألفاظ للمعنى الذي انتهى إليه الحكم وتسميتها باسمها المعين في القانون وتحديد ما إذا كانت سبًا أم قذفًا أم عيبًا أم إهانة أم تشهيرًا هو من مسائل القانون التي يخضع فيه ما ينتهي إليه قاضي الموضوع لرقابة محكمة النقض[١]. ومثل هذا الأمر يتوافق مع وسيلة إثبات القصد الجنائي في هذه الجرائم، حيث يلزم لإثباته والتحقق من قيامه أن تكون الألفاظ المستخدمة في السب والقذف والتشهير شائنة بذاتها[٢]، وتبتعد عن مدلول مجرد النقد المباح الذي لا يتضمن المساس بشخص صاحب الأمر أو التشهير به أو الخط من كرامته[٣]. إذ يصلح أن يكون مبنى التجريم هنا أن يكون ذلك باستخدام نطاق اسم يحتوي على عبارات غير أخلاقية، مثل Fuckmickey.multimania.com حتى أن تضمن الموقع مجموعة صور لأفراد برزت فقط وجوههم[٤].

المبحث الثالث

جرائم تقانة المعلومات فى الدول العربية والغربية

---

(١) طعن جنائي مصري رقم ٣٠٨٧ لسنة ٦٢ق، جلسة ٢٠٠٠/٥/٨ (المحاماة/ مصر العدد ١ لسنة ٢٠٠١، ص٢٠٧).

(٢) طعن جنائي مصري رقم ٤٩٣٣ لسنة ٦٢ق، جلسة ٢٠٠٠/٥/١٥ (المحاماة/ مصر العدد ١ لسنة ٢٠٠١، ص٢٠٧).

(٣) طعن جنائي مصري رقم ٣٠٨٧ لسنة ٦٢ق، السابق.

(4) TGI Meaux, 3eme Ch, Correc. 19/11/2001 (Ste Eurodisney S. C. A. & autres c/ A. A.) http://www.juriscom.net.

ليست الدول العربية ببعيدة عن مرمى جرائم الإنترنت وشبكات التواصل الإجتماعي ، ذلك أن هذه الجرائم لم تترك بلدا من بلاد العالم إلا واخترقتها ونالت من أهداف محدده فيها، فالسعودية والإمارلات وسلطنة عمان والكويت فلسطين وغيرهم من الدول العربية بادروا إلى وضع – أو فى طريقهم لوضع- تشريعات إلكترونية لمواجهة الجرائم المعلوماتية.

وبالنظر إلي موقع العالم العربي في خريطة استخدام وسائل تقنية المعلومات الحديثة وموقع الدولة بين شقيقاتها الدول العربية فإن إحصائيات الاتحاد الدولي للاتصالات لعام ٢٠٠١ تشير إلى أن نسبة مواطني العالم العربي، الذين سبق أن استخدموا شبكة الإنترنت، لا يتعدى ١% رغم أن سكان العالم العربي ال ١٧٠ مليون نسمة يشكلون٥%من مجموع سكان العالم.

وإذا ما قارنا ذلك بنسبة الأوروبيين والأمريكيين التي تفوق ٥٨ في المائة فإن ذلك يدفع البعض إلى وصف تجربة العالم العربي في مجال تكنولوجيا الاتصالات والإنترنت بأنها في مرحلتها "الجنينية".

وإذا لم يكن الحاجز أخلاقيا أو سياسيا فقد يكون تقنيا أو ماليا. إذ ُتعدُ معظم شبكات الاتصال في العالم العربي غير متطورة وملكا للقطاع العام. كما تتباين نسبة توفير خدمات الاتصال من بلد عربي لآخر، ففي الوقت الذي نجد فيه أكثر من ١٠٠ خط هاتفي لكل ١٠٠ منزل في الإمارات والكويت، لا تتعدى النسبة في سوريا ومصر والمغرب حيث الكثافة السكانية كبيرة، خمسين خط هاتفي لكل مائة عائلة.

كما أن نفقات الاتصال لا تزال عالية في بلدان العالم العربي مما يحول دون التشجيع على استخدام الإنترنت بشكل مكثف. فقد تبلغتكلفة ثلاثين ساعة اتصال بالإنترنت شهريا في سوريا ٤٧ دولارا أمريكيا، وفي السعودية ٤١ دولارا، و ٢٤ دولارا في الإمارات العربية المتحدة، وعشر دولارات في مصر.

ووفقاً لدراسةٍ، أُعدت لصالح منتدى دافوس الاقتصادي الدولي حول تحديات تطور تكنولوجيا الاتصالات والإعلامفي العالم العربي، تم تصنيف الدول العربية إلى مجموعات ثلاث: مجموعة التطور السريع وتشمل الكويت والإمارات العربية المتحدة، و مجموعة الدول الصاعدة وتشمل كلا من مصروالأردن ولبنان والسعودية ، ومجموعة الدول السائرة في طريق النمو وتضم المغرب وعمان وسوريا.

ومن ثم يتناول هذا المبحث الجريمة الالكترونية عبر شبكة الإنترنت ومواقع التواصل الإجتماعي في الدول العربية والغربية عبر مطلبين أساسيين، يتناول المطلب الأول منها تنامى جرائم المعلوماتية والانترنت فى الدول العربية وآليات مواجهتها، في حين يتناول المطلب الثاني تطور وواقع جرائم الإنترنت ومواقع التواصل الإجتماعي في الدول الغربية.

المطلب الأول

جرائم الإنترنت والمعلوماتية في الدول العربية وأساليب مكافحتها

نتناول فى هذا المطلب انتشار جرائم تقانة المعلومات فى العالم العربي ثم الآليات التى قررتها تلك الدول لمواجهة الجرائم الالكترونية وذلك من خلال المحاور التالية

أولا: جرائم تقانة المعلومات فى مصر

دخلت خدمة الانترنت مصر عام ١٩٩٣ علي يد مركز المعلومات ودعم اتخاذ القرار بالتعاون مع شبكة الجامعات المصرية ومع بداية عام ١٩٩٧ بدأ المركز في خصخصة خدمات الانترنت في مصر وكانت البداية من خلال ١٦ شركة زادت الي ٦٨ شركة في عام ٢٠٠٠ وانتهت الي ٢١١ شركة هي اجمالي الشركات التي تقدم خدماتها في مجال الانترنت داخل مصر. وقد بلغ عدد مستخدمي الانترنت في مصر في العام الاول لاستخدامه حوالى ٧٥ ألف شخص ولكنه بعد تطبيق حملة حاسب لكل بيت وانخفاض أسعار خدمات الانترنت السريع وصل عدد مستخدمي الانترنت إلي ما يربو على خمسة ملايين و٣٠٠ ألف مستخدم يحصلون علي خدماتهم من خلال ٢١١ شركة تعمل في هذا المجال داخل حدود مصر.

وقد أكد تقرير صادر عن وزارة الاتصالات وتكنولوجيا المعلومات إلى ارتفاع عدد مستخدمى الإنترنت فى مصر إلى نحو ٧ ملايين مستخدم خلال عام، منهم نحو ٣ ملايين خلال شهر، حيث أشار التقرير إلى وصول عدد مشتركى الإنترنت إلى ٣٣.١٩ مليون مستخدم فى أبريل ٢٠١٧ مقارنة بـ٣٠.٤٥ مليون فى مارس ٢٠١٧، و ٢٦.٨ مليون فى أبريل ٢٠١٦.

وبلغت نسبة مستخدمى الإنترنت عن طريق المحمول من إجمالى مشتركى المحمول ٣٣.٢٢% أبريل ٢٠١٧، مقارنة بـ٣٠.٤٨% فى مارس ٢٠١٧ و ٢٧.٣٧% فى أبريل ٢٠١٦. فيما ارتفع عدد مشتركى الهاتف الثابت بنسبة ضئيلة، الى ٦.٥٥ مليون مشترك فى ابريل ٢٠١٧، مقارنة بـ٦.٢٢ مليون مشترك فى مارس ٢٠١٧ و ٦.٠٩ مليون مشترك فى مارس ٢٠١٦.

كما ذكر التقرير أن عدد نوادى التكنولوجيا فى المحافظات وصلت إلى ٧٧ ناديا، وذلك فى إطار تعزيز دور تكنولوجيا المعلومات بصورة فعالة ومستدامة فى التنمية المجتمعية، أغلبهم فى المنوفية والجيزة والدقهلية وسوهاج والوادى الجديد وأسوان والأقصر، وأسيوط والمنيا والفيوم وبنى سويف والبحر الأحمر والقليوبية والقاهرة والإسكندرية والسويس والإسماعيلية وبورسعيد. وكانت مؤشرات سابقة لوزارة الاتصالات وتكنولوجيا المعلومات قد ذكرت أن عدد الاشتراكات بالهاتف المحمول اقترب من نحو ١٠٠ مليون للشركات الثلاث العاملة فى السوق وهو ما يتجاوز عدد السكان فى مصر وذلك بنسبة انتشار بلغت نحو ١١١% على مستوى الجمهورية[١].

---

[١] أوضح تقرير مؤشرات وزارة الاتصالات الصادر فى اغسطس ٢٠١٧ أن مشتركى الإنترنت فائق السرعة ADSLارتفع إلى٤.٥٧مليون مشترك، فى أبريل ٢٠١٧، بمعدل تغيير شهرى ١.٧٧% ومعدل تغيير سنوى ١٢.٧٤%، وذلك مقارنة بـ٤.٤٩ مليون فى مارس ٢٠١٧ مشترك و٤.٠٥ مليون فى أبريل ٢٠١٦.

وأكدت مصادر بالإدارة العامة للمعلومات والتوثيق بوزارة الداخلية المصرية على إن البعض استغل ما أتاحه العلم والتقدم التكنولوجي الحديث، استغلالاً سيئًا وبدأ في ارتكاب أعمال أو أفعال ترقى لمستوى الجريمة، وأصبحت تشكل هاجسًا وتحديًا للأجهزة الأمنية، وبات واضحًا أن التهديد القادم شديد الخطورة في ظل ظروف دولية وإقليمية متشابكة، حيث جري الإعداد منذ أكثر من سنتين على تكوين وحدة مباحث جديدة تكون معنية بعملية رصد ومتابعة وضبط جميع الجرائم المستحدثة بجميع أشكالها وأساليبها والتي يكون الكمبيوتر عنصرًا في ارتكابها خاصة بعد أن بدأت هذه الجرائم تأخذ أشكالاً وأبعادًا دولية وعالمية جديدة وبشكل سريع[1].

ولعله من نافلة القول الإشارة إلى أهم الجرائم ذات الصبغة المعلوماتية التى انتشرت فى مصر ومنها، جرائم استخدام بطاقات الائتمان المملوكة للغير، حيث يتم سرقتها واستخدامها في شراء سلع وخدمات من الخارج، ثم ظهرت بعض الجرائم الأخرى ذات الصلة بالكمبيوتر مثل جرائم الشبكات واختراقها والدخول على أجهزة الحاسب الآلي للغير وسرقة المعلومات التي تمثل سرية خاصة لبعض الأشخاص أو المؤسسات أو الشركات، كما ظهرت جرائم الإنترنت وقيام البعض بنشر مواقع تسيء لأشخاص آخرين أو تسيء لشكل ومظهر الدولة، ثم ظهرت جرائم عالمية أخرى يقوم بها بعض الهاكرز ومنها إطلاق الفيروسات والاختراقات، ومنها اختراق المواقع الرسمية أو الشخصية أو اختراق الأجهزة الشخصية وأنظمة شفرات الكمبيوتر للمؤسسات والأفراد، وجرائم التجسس الصناعي، وجرائم الأموال مثل السطو والاحتيال والنصب وسرقة بطاقات الائتمان والتزوير والجريمة المنظمة، وجرائم المخدرات وغسل الأموال، وجرائم الآداب وتجارة السلاح وجرائم الابتزاز الإلكتروني، وجرائم الغش الإلكتروني، بالإضافة إلى جرائم القرصنة وجرائم محتوى الإنترنت من المواقع الإباحية أو المعادية سواء دينيًا أو سياسيًا.

ويجب التأكيد على أن إدارة المعلومات والتوثيق بوزارة الداخلية تحتضن مجموعات عمل تعكف على متابعة شبكة الإنترنت على مدار اليوم لمراقبتها وفحص التعاملات والمعاملات التي تتم عليها من وإلى الخارج، وإذا ما ظهر أية مخالفات أو أعمال تمثل خروجًا على القانون والشرعية أو تهديد أمن واستقرار الوطن يتم التدخل فورًا بالتنسيق مع الأجهزة النوعية الأخرى. ومما لا شك فيه أن التأثير المجتمعي الذي يحدثه التقدم التكنولوجي يحتاج إلي تنظيم قانوني، يضع إطارا للعلاقات التي تترتب علي استخدامه بما يكفل حماية الحقوق المترتبة علي هذا الاستعمال، ويحدد الواجبات تجاهها، فلابد للتقدم العلمي والتكنولوجي أن يواكبه تكيف في القواعد القانونية، إذ لا يجوز للقانون أن يقف صامتا مكتوف الأيدي حيال أساليب انتشار هذا التقدم، وحيال القيم التي يروجها.

وقد أرجع المتخصصون هذا الفراغ من أية عقوبات خاصة بجرائم الانترنت فى التشريع المصرى إلى حداثة هذا المجال الذي لم يتعد عمره سنوات قليلة وما يطبق حاليا علي جرائم الانترنت هو القانون التقليدى الذى يتم بموجبه على الجرائم العادية مثل جريمة سرقة، حيث يعاقب مرتكبها بالحبس مدة

---

[1] نجوى عبد السلام، التفاعلية في المواقع الإخبارية على شبكة الإنترنت - دراسة تحليلية، المجلة المصرية لبحوث الرأي العام، العدد الرابع، القاهرة، ت ٢/ ك١/ ٢٠٠١، ص٢٣

لاتقل عن ٢٤ ساعة ولاتزيد علي ثلاث سنوات وجريمة النصب التى يعاقب مرتكبها بعقوبة النصب المدرجة في قانون العقوبات[١].

أما السب والقذف الالكترونى، فتكون جنحة، وإذا كانت الجريمة تركيب صور فاضحة، توجه لمرتكبها، تهم خدش الحياء وهتك العرض والتحريض علي الفسق. أما اطلاق الشائعات والسطو علي أرقام الكروت الائتمانية واقتحام نظم البنوك فتوجه إلي مرتكبها تهم تكدير الأمن العام وتهديد الاقتصاد القومي والاضرار بالمصالح العليا للبلاد وهي اتهامات خطيرة تقود صاحبها الي محاكم الجنايات مباشرة. على أن هذا التكييف القانونى لجرائم المعلوماتية يظل عاجزا عن مواكبة هذه النوعية من الجرائم وما يصاحبها من تطور مستمر فضلا عن تنامى أنواعها وانتشارها بشكل مريب وهو الأمر الذى يحتم على المشرع المصرى سرعة اصدار قانون جديد يواجه الجرائم الالكترونية خاصة ان هناك بعض الجرائم المستحدثة التي لن تجد لها تكييفا قانونيا محددا في القانون التقليدى.

١ـ آليات مكافحة الجريمة الالكترونية فى مصر

فيما يتعلق بآليات مواجهة الجرائم المعلوماتية، فلا أحد ينكر الجهود الحكومية والأهلية فى مجال المكافحة، فقد أنشأت وزارة الداخلية المصرية عام ٢٠٠٢، آلية فى هذا الاطار تحت مسمى " إدارة مكافحة جرائم الحاسب الآلي وشبكة المعلومات التابعة للادارة العامة للمعلومات والتوثيق، بالقرار الوزارى رقم ١٣٥٠٧ لسنة ٢٠٠٢[٢].

وقد تحددت مهام الإدارة فى رصد ومتابعة جرائم التطور التكنولوجي وتتبع مرتكبيها من خلال أحدث النظم الفنية والتقنية الحديثة ويتم تقنين الاجراءات بعد عملية التتبع الفني وضبط القائم بارتكاب الجريمة التي يكون تكييفها القانوني من خلال قانون العقوبات والجريمة التى تتعامل معها الإدارة تتمثل فى الأنشطة غير القانونية التي يكون فيها الكمبيوتر وسيلة أو غاية أو كليهما وتتخذ أشكالا متعددة بما فيها الاحتيال باستخدام البطاقات الائتمانية وبيع المواد الالكترونية وانتهاك حقوق الملكية الفكرية في مصر وسرقة البريد الالكتروني والتزوير باستخدام الماسحات الضوئية والطابعات وجرائم الشبكات واختراقها والدخول على أجهزة الحاسب الآلي للغير وسرقة المعلومات التي تمثل سرية خاصة لبعض الأشخاص أو المؤسسات أو الشركات، وقيام البعض بنشر مواقع تسيء لأشخاص آخرين أو تسيء لشكل ومظهر الدولة، ثم ظهرت جرائم عالمية أخرى يقوم بها بعض الهاكرز ومنها إطلاق الفيروسات واختراق المواقع الرسمية أو الشخصية أو اختراق الأجهزة الشخصية وأنظمة شفرات الكمبيوتر للمؤسسات والأفراد، وجرائم التجسس الصناعي، وجرائم الأموال مثل السطو والاحتيال والنصب

---

[١] راجع:

شريف اللبان، ، تكنولوجيا الاتصال، المخاطر والتحديات والتأثيرات الإجتماعية، القاهرة، الهيئة المصرية العامة للكتاب، ٢٠٠٨ وكذلك د. هلالي عبد اللاه أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، القاهرة، دار النهضة العربية.٢٠٠٦

[٢] ـ قرار وزير الداخلية المصرى الرقيم ١٣٥٠٧ لسنة ٢٠٠٢ بشأن إدارة مكافحة جرائم الحاسب الآلي وشبكة المعلومات التابعة للادارة العامة للمعلومات والتوثيق، القاهرة ٢٠٠٢.

والجريمة المنظمة، وجرائم المخدرات وغسيل الأموال، وجرائم الآداب وتجارة السلاح وجرائم الابتزاز الإلكتروني، وجرائم الغش الإلكتروني، بالإضافة إلى جرائم القرصنة وجرائم محتوى الإنترنت من المواقع الإباحية أو المعادية سواء دينيًا أو سياسيًا.

٢-آلية عمل الإدارة ومراحل التحري والضبط

تمر القضايا التى ترد إلى إدارة مكافحة جرائم الحاسب الآلى وشبكة المعلومات، بالعديد من الإجراءات، منها: فحص البلاغ في القسم الفني، وتأكيد المعلومات الواردة به، ثم تثبيت الاتهامات عبر القسم الجنائي، ومهمته تحرير المحضر، ثم يعود الملف علي القسم الفني مرة أخري لمتابعة الإيميلات ونصب الكمائن الالكترونية، وتحديد شخصية المتهم، وعنوانه، واعداد تقرير فني برقم التليفون المستخدم في الدخول علي الإنترنت، أو مكان مقهي الانترنت المستخدم في ارتكاب الواقعة، ومن ثم يقوم القسم الجنائي بالتعاون مع قسم العمليات، حيث يتم استصدار إذن من النيابة العامة بضبط جهاز الحاسب الآلي المستخدم في ارتكاب الجريمة، وفحصه، وبعد ذلك يتم تسليم الجهاز إلي القسم الفني ليتولي مثل هذه العمليات، واستخراج الأدلة والصور التي تدين المتهم، ثم يتم إعداد تقرير فني استكمالي لإرفاقه مع المتهم الذي يتم إحالته للنيابة للتحقيق.

فضلا عما تقدم، يتم ضبط الجريمة من خلال بلاغ أو معلومة تصل إلي جهاز الأمن، وتقوم الإدارة بتتبعها وإثباتها بالأدلة وبالأسلوب التقني والفني ومدي الجرم والمخالفة التي تمت وتقديم مرتكبها إلي المحاكمة، ومما يساعد على السرعة فى الإنجاز والأداء أن الإدارة تضم نخبة متميزة من الضباط والفنيين المدربين علي مكافحة جرائم الانترنت، وكيفية التعامل مع أحدث اجهزة الفحص الفني الموجودة بالوزارة للتعامل مع مثل هذه الجرائم والتحفظ عليها بشكل آمن، وسحب كل البيانات، والصور، بطريقة سليمة لضمها إلي ملف القضية[١].

وتشير مصادر بوزارة الداخلية إلى أن جرائم انتهاك حقوق الملكية الفكرية خاصة قرصنة البرمجيات، أدت إلى خسائر كبيرة في منطقة الشرق الأوسط وأفريقيا وهاتين المنطقتين تعدان من المناطق التى شهدت ارتفاعا كبيرا في معدل قرصنة المعلومات بين عامي ٢٠٠٥، ٢٠٠٦، حيث وصلت نسبة انتشار البرمجيات المقلدة إلي ٦٠ % في منطقة الشرق الأوسط.

ومن مظاهر الجهود المبذولة من الإدارة الجديدة تشكيل مجموعات عمل لمتابعة شبكة الإنترنت يوميًا على مدى اليوم لمراقبتها وفحص التعاملات والمعاملات التي تتم عليها من وإلى الخارج، وإذا ما ظهر أية مخالفات أو أعمال تمثل خروجًا على القانون والشرعية أو تهديد أمن واستقرار الوطن يتم التدخل فورًا بالتنسيق مع الأجهزة النوعية الأخرى[٢].

---

[١] لمزيد من التفصيل يمكن الرجوع الى الموقع الرسمي لوزارة الداخلية المصرية على شبكة المعلومات الدولية "الانترنت" WWW.Moiegypt.gov.eg تاريخ الدخول ٢٠٢١/١/٢٣

[٢] - http://www.ahlalhdeeth.com/vb/showthread.php?t=169760

ويأتى فى إطار الآليات الخاصة بمواجهة الجرائم الالكترونية فى مصر، آلية الابلاغ عن الجرائم، حيث بإمكان المواطنين الإبلاغ عن الجرائم الإلكترونية عبر الوسائل الآتية:

١- الموقع الإلكتروني لوزارة الداخلية على شبكة الانترنت (WWW.Moiegypt.gov.eg).واخطار إدارة مكافحة جرائم الحاسبات وشبكات المعلومات بمقر وزارة الداخلية[١].

٢- يمكن تلقي البلاغات من خلال الخط الساخن (١٠٨) والذى تم إنشاؤه لهذا الغرض.

ولا يمكن إنكار الدور الذى تمارسه الجمعية المصرية لمكافحة جرائم الإنترنت فى مجال التصدى لهذا النوع من الجرائم باعتبارها إحدى الآليات الأهلية التى بذلت من جهود فنية وبحثية من أجل الحد من جرائم المعلوماتية والانترنت، ويمكن رصد بعضا من هذه الجهود فى النقاط التالية:

١- وقعت الجمعية بروتوكول تعاون مع كلية الحقوق جامعة عين شمس بهدف تثقيف وتدريب طلبة وخريجي كليات الحقوق و الآداب والإعلام والسياحة والآثار والتجارة والحاسبات والمتخصصين، والسادة القضاة واعضاء النيابة العامة والسادة المحاميين والعاملين في القطاعات القانونية في المؤسسات وتأهيل وإكساب المتدربين المهارات القانونية والعلمية والعملية والفنية الخاصة بارتباط المعلوماتية والاتصالات بتخصصاتهم ومدى تأثير استخدام تكنولوجيا المعلومات في انجاز مهام اعمالهم والتعريف بماهية التعامل مع الاشكاليات القانونية في حقل المعاملات الالكترونية حول موضوعات تشمل كيفية اثبات الشخصية، كيفية التوقيع الالكتروني، أنظمة الدفع النقدي الرقمي(المال الرقمي أو الالكتروني)، سرية وأمن المعلومات من مخاطر إجرام التقنية العالية، خصوصية العميل، المسئولية عن الأخطاء والمخاطر، حجية المراسلات الالكترونية، التعاقدات المصرفية الالكترونية، مسائل الملكية الفكرية لبرمجيات وقواعد معلومات البنك أو المستخدمة من موقع البنك أو المرتبطة بها، علاقات وتعاقدات البنك مع الجهات المزودة للتقنية أو الموردة لخدماتها أو مع المواقع الحليفة، مشاريع الاندماج والمشاركة والتعاون المعلوماتية[٢].

٢- مبادرة انطلقت من القاهرة كمبادرة دولية تبنتها الجمعية الدولية لمكافحة الإجرام السيبيرى بفرنسا، بالتعاون مع الجمعية المصرية لمكافحة جرائم الإنترنت، تحمل بارقة أمل لسن قوانين رادعة

---

[١] حددت وزارة الداخلية المصرية آلية للتعاون مع المواطنين في جرائم المعلوماتية سواء بالحضور الشخصي أو الاتصال من خلال أرقام هواتف محددة لتلك الجرائم ٢٧٩٢٨٤٨٤/ ٢٧٩٢٦٠٧١/ ٢٧٩٢٤٠٩٠/٢٧٩٢٤٠٩١.(٠٠٢٠)

[٢] تناولت العديد من الدراسات هذا الجانب منها: د. أسامة محمد محى الدين عوض، جرائم الكمبيوتر والجرائم الأخرى فى مجال تكنولوجيا المعلومات. بحث مقدم للمؤتمر السادس للجمعية المصرية للقانون الجنائى، القاهرة ١٩٩٣. وكذلك: د. محمد الأمين البشرى، التحقيق فى جرائم الحاسب الآلى، بحث مقدم إلى مؤتمر القانون والكمبيوتر والانترنت، جامعة الإمارات العربية المتحدة،سنة ٢٠٠٠.

تحمى رواد شبكة الإنترنت من التجاوزات غير اللائقة التي تحدث على الشبكة، بداية من الإرهاب الإلكتروني ومروراً بالسطو على الحقوق الفكرية، وانتهاء بتجريم تجارة الرقيق الأبيض على الشبكة العنكبوتية وماهية التنظيم القانوني للعالم الإفتراضي بأقسامه من المعاملات القانونية الرقمية وعقود التجارة الإلكترونية وحماية الملكية الفكرية عبر الإنترنت والتعريف بأنماط وأشكال الجرائم عبر الإنترنت وماهية الدليل الرقمي وحجيته في الإثبات وعرض احدث التقنيات الفنية العالمية للتعامل مع مثل هذه النظم. وغنى عن البيان أن الكثير من أهل الاختصاص فى مجال جرائم المعلوماتية والإنترنت، قد اقرحوا آلية متخصصة تماما فى هذا المجال هى "شرطة الانترنت" كجهة مسئولة عن مكافحة جرائم الإنترنت[1].

ثانيا: جرائم تقانة المعلومات في المملكة العربية السعودية

ارتفع معدل مستخدمي الإنترنت في السعودية حيث وصل عددهم إلى ٢٢.٤ مليون مستخدم عام ٢٠١٦، حسبما ذكرته هيئة الاتصالات وتقنية المعلومات السعودية، لكنه ارتفع أكثر في العام التالي ليصل الى ٣٠.٢٥ مليون شخص، وأن عدد حسابات التواصل الاجتماعي النشطة وصل إلى نحو ٢٥ مليون حساب في البلاد، وبلغ إجمالي الهواتف النقالة النشطة في مواقع التواصل الاجتماعي نحو ١٨ مليون جهاز، وارتفع عدد مستخدمي الإنترنت خلال عام ٢٠١٧ إلى نحو ثمانية ملايين شخص بارتفاع بنسبة ٣٤%، وارتفع عدد مستخدمي مواقع التواصل الاجتماعي المتفاعلين إلى نحو ستة ملايين خلال عام ٢٠١٧ بنسبة ٣٢%، إضافة إلى ارتفاع عدد الهواتف الذكية بنحو مليوني هاتف بما يعادل ١٢%. بحسب الصحف المحلية.

وبلغ إجمالي حاملي الهواتف الذكية في السعودية نحو ٩٦%، ونحو ١% يحملون قارئاً إلكترونياً، وما يقارب ٢٢% يحملون التابلت، إضافة إلى اقتناء ٥٦% جهاز "لابتوب" وكمبيوتر، ونحو ٨٣% أجهزة تلفزيون، فيما بلغ متوسط الوقت اليومي الذي يستغرقه السعوديون في الإنترنت نحو ٦:٤٥ ساعة، و٢:٣٤ ساعة في مواقع التواصل الاجتماعي، وبلغ إجمالي الساعات التي يستغرقها السعوديون لمشاهدة التلفاز ٣:٠٥ ساعات في اليوم[2].

وأظهر التقرير وصول متوسط سرعة الإنترنت في السعودية عبر الاتصالات الثابتة إلى ٢١.٢٦ ميجا بايت، في حين بلغ متوسط سرعة الإنترنت من الهواتف المحمولة ١٦.٢٢ ميجا بايت، وبيَّن التقرير أن نحو ٦٤% من السعوديين يشاهدون فيديو يومياً على الإنترنت، و٢٦% أسبوعياً، و٤% شهرياً، و٥% لم يسبق لهم مشاهدة الفيديو عن طريق الشبكة العنكبوتية.

---

[1] انظر: فتحي حسين عامر، وسائل الاتصال الحديثة من الجريدة إلى الفيس بوك، القاهرة، العربي للنشر والتوزيع، ٢٠١١

[2] كشف التقرير أن ٦٥% من السعوديين يؤمنون بأن التقنيات الجديدة ستوفر فرصاً كبيرة، و٦٣% يفضلون إكمال مهمة ما مع هذه التقنيات، و٧٨% من السعوديين يؤمنون بأن الخصوصية وحماية البيانات من أهم الأمور في التقنية، و٣٦% يستخدمون برامج حذف الإعلانات من الإنترنت.

أعلنت السلطات المختصة أنها تفرض عقوبات بالحبس لمدة عام واحد وغرامات لا تزيد عن ٥٠٠ ألف ريال فيما يعادل ١٣٣ ألف دولار لجرائم القرصنة المرتبطة بالانترنت واساءة استخدام كاميرات الهواتف المحمولة مثل التقاط صور دون تصريح، إلا أن المملكة وفى رغبة من أجل تقنين هذا الوضع، أصدرت تشريعا وطنيا فى هذا الخصوص مؤخرا تحت مسمى "نظام مكافحة جرائم المعلوماتية السعودى". وباصدار هذا التشريع تكون المملكة العربية السعودية[1]، قد سبقت نظيراتها من الدول العربية فى إصدار قانون جديد لمكافحة جرائم المعلوماتية التي تشمل التهديد والابتزاز والتشهير بالآخرين في مواقع الانترنت وإنشاء مواقع الإنترنت الإرهابية.

وذكرت مصادر بوزارة الداخلية السعودية أن نظام مكافحة جرائم المعلوماتية قد أصبح قيد التطبيق بعد صدور موافقة مجلس الوزراء عليه، باعتباره إطاراً قانونياً مهماً جداً في تعريف وتحديد الجرائم المعلوماتية والحد منها ومواجهتها بعد أن أصبحت تلك الجرائم من بين الجرائم التي تهدد أمن وسلامة المجتمعات الانسانية.

ويشمل النظام الجديد ١٦ مادة تتضمن عقوبات صارمة ضد مرتكبي هذه الجرائم تتراوح بين سنة و١٠ سنوات سجنا وغرامات مالية تصل الى خمسة ملايين ريال سعودي، مضيفاً أن النظام تضمن تعريفات المصطلحات والمسميات الواردة في النظام مثل "الشخص" و"النظام المعلوماتي" و"الشبكة المعلوماتية" و"البيانات والجريمة المعلوماتية الى جانب أهداف النظام بالحد من هذه الجرائم والعقوبات المقررة لكل منها. وحددت مواد النظام الأخرى الجرائم المعلوماتية وعقوباتها التي تنوعت بين السجن لمدد مختلفة والغرامات المالية بحسب نوع وطبيعة كل جريمة من الجرائم المعلوماتية واختصاصات كل من "هيئة الاتصالات وتقنية المعلومات" و"هيئة التحقيق والادعاء العام" في المساندة اللازمة للأجهزة الأمنية لتحقيق أهداف وغايات هذا النظام. ويهدف النظام الجديد الى حماية المجتمع من جرائم المعلوماتية والحد منها والمساعدة على تحقيق الأمن المعلوماتي وحفظ الحقوق المترتبة على الاستخدام المشروع للحاسبات الآلية والشبكات المعلوماتية وحماية المصلحة العامة والأخلاق والآداب العامة وحماية الاقتصاد الوطني.

ولقد عانت السعودية فى الفترة الأخيرة من محاولات اختراق مواقع الإنترنت، وكان آخرها، عندما تعرض أحد المواقع التعليمية الحكومية بالسعودية لاختراق استمر عدة ساعات كتب خلالها من قام بالاختراق ورمز لنفسه بالرمز (٠) عبارات ينصح من خلالها مشرفي الموقع على الاهتمام بالموقع وحمايته وعدم استخدام برامج تصميم مجانية. وتأخر كثيراً مشرفي موقع إدارة التربية والتعليم بمنطقة تبوك وهو الموقع الذي تم اختراقه، في صيانة الموقع وحل مشكلة الاختراق، حيث ظل فترة طويلة ورسالة الاختراق ظاهرة على واجهته.

---

[1] - راجع: "نظام مكافحة جرائم المعلوماتية السعودى" الصادر بالمرسوم رقم م/ ١٧ بتاريخ ٨/ ٣/ ١٤٢٨هـ وطبقا لقرار مجلس الوزراء رقم (٧٩)بتاريخ ٧/ ٣/ ١٤٢٨هـ.

الجدير بالذكر أن كثيراً من المواقع الحكومية قد تعرضت للاختراق إما بداعي التطفل أو لوجود كثير من الخلافات بين الجهة الحكومية ومن يقف خلف هذا الاختراق خاصة في المواقع التعليمة الحكومية مما اضطر مسؤولي وزارة التربية والتعليم السعودية و مؤخراً لنفي اختراق موقعه الخاص بشؤون المعلمين[1]

وبدأت السعودية فى التفكير فى تطبيق قانون الحبس في جرائم الإنترنت عندما أعلنت السلطات هناك أنها سفرض عقوبات بالحبس لمدة عام واحد وغرامات لا تزيد عن ٥٠٠ ألف ريال لجرائم القرصنة المرتبطة بالانترنت وإساءة استخدام كاميرات الهواتف المحمولة مثل التقاط صور دون تصريح. الجدير بالذكر أن هيئة الأمر بالمعروف والنهي عن المنكر في السعودية، قد عارضت الهواتف ذات الكاميرات، وحظرت السعودية بيع هذه الأجهزة لعدة أشهر عام ٢٠٠٤، غير أن تلك القيود فشلت في وقف انتشار أحدث الصيحات التكنولوجية في المملكة[2].

وتفرض السعودية رقابة شديدة على استخدام الانترنت من خلال تعقب المستخدمين وحظر المواقع الجنسية وبعض المواقع ذات المحتوى السياسين فبعد ازدياد الخطر من استخدام الانترنت بدأت العديد من المنظمات والهيئات إلى إطلاق الدعوات والتحذيرات من خطورة هذه الظاهرة التى تهدد كل مستخدمى الإنترنت خاصة بعد تقرير برلمانى وضعته لجنة العلوم والتكنولوجيا في مجلس اللوردات البريطانى أظهر أن شبكة الانترنت تحولت إلى حلبة يرتع فيها المجرمون، وتنفذ فيها العصابات عمليات سرقة الأموال من الحسابات المصرفية، محذراً الحكومات والمؤسسات والشركات المختصة التدخل لتنظيم عملها قبل فوات الأوان.

هذا ويتضمن النظام السعودي في قوانينه جريمة إنشاء موقع إرهابي على الإنترنت وفقا للمادة السابعة من نظام مكافحة جرائم المعلوماتية على أنه «يعاقب بالسجن مدة لا تزيد على ١٠ سنوات وبغرامة لا تزيد على ٥ ملايين ريال، أو بإحدى العقوبتين، كل شخص يرتكب أيا من الجرائم المعلوماتية التي تتضمن إنشاء موقع لمنظمات إرهابية على الشبكة المعلوماتية، والدخول غير المشروع إلى الموقع الإلكتروني أو النظام المعلوماتي»[3].

وفى سبيل تفعيل آليات العمل والتعاون الدولى فى مجال مكافحة الجرائم الإلكترونية، فإنه من الأهمية بمكان التنسيق وتبادل المعلومات والخبرات مع الأجهزة المعنية بمكافحة الإرهاب عبر الإنترنت في كافة دول العالم، ونقل التقنية التي تستخدم في الدول المتقدمة في مكافحة الإرهاب الإلكتروني،

---

[1] د. غانم محمد غانم، عدم ملائمة القواعد التقليدية فى قانون العقوبات لمكافحة جرائم الكمبيوتر، مؤتمر القانون والكمبيوتر والإنترنت- الإمارات، مايو ٢٠٠٠،ص. ١٠ وما بعدها

[2] راجع: نعوم تشو مسكي، السيطرة على الإعلام.. الإنجازات الهائلة للبروباجندا، تعريب: أميمة عبد اللطيف، القاهرة، مكتبة الشروق الدولية، الطبعة الثانية، ٢٠٠٥

[3] محمد صادق اسماعيل، الارهاب في المملكة العربية السعودية، القاهرة، دار العلوم للنشر والتوزيع، ٢٠١٠،ص. ١١٠-١١١

والتوسع في دراسة فكر التنظيمات الإرهابية التي تبث عبر شركة الإنترنت، وتعزيز التعاون مع المؤسسات الدولية المعنية خاصة "الإنتربول" لمواجهة كافة أشكال الجرائم، إضافة إلى الإسراع في الانضمام إلى المعاهدات الدولية الخاصة بمكافحة جرائم الإنترنت[1].

ثالثا: جرائم تقانة المعلومات في سلطنة عمان

في احصائية عن اعداد مستخدمي الانترنت في العالم حتى تاريخ ٢٠١٢ كانت نسبة اعداد مستخدمي الانترنت في عمان على العدد الكلي لسكان عمان ٦٨.٨% وهذه نسبة عاليه جدا بعدد ٢,١٠١,٣٠٢

مستخدم للانترنت في عمان عام ٢٠١٢ تشمل جميع شركات الاتصال لعدد سكان عمان وهو ٣,٠٩٠,١٥٠ ويعتبر هذا نمو هائل حيث كان عدد مستخمي الانترنت ٩٠,٠٠٠ عام ٢٠٠٠ .

وقد أصدرت السلطنة المرسوم السلطاني رقم ٢٠٠١/٧٢ الذي تضمن جرائم الحاسب الآلي وحدد فيه الجرائم التالية:

-الالتقاط غير المشروع للمعلومات أو البيانات وهو ما يمثل تعديا صارخا على حقوق المؤلف.

-الدخول غير المشروع على أنظمة الحاسب الآلي.

-التجسس والتصنت على البيانات والمعلومات.

-انتهاك خصوصيات الغير أو التعدي على حقهم في الاحتفاظ بأسرارهم وتزوير البيانات أو وثائق مبرمجة أيا كان شكلها.

-إتلاف ومحو البيانات والمعلومات.

-جمع المعلومات والبيانات وإعادة استخدامها.

-تسريب البيانات والمعلومات.

-نشر واستخدام برامج الحاسب الآلي بما يشكل انتهاكا لقوانين حقوق الملكية والأسرار التجارية[2]. .

رابعا: جرائم تقانة المعلومات في فلسطين

تشير بيانات وزارة الاتصالات وتكنولوجيا المعلومات الى أن عدد شركات الانترنت العاملة والمسجلة في الوزارة للعام ٢٠١٥ قد بلغ ٥٦ شركة موزعة على النحو الآتي؛ ٤٠ شركة للاتصال اللاسلكي بالانترنت (WI FI)، و٦ شركات للاتصال الهاتفي عبر بروتوكول الانترنت (VOIP)، و١٠ شركات

---

[1] - جريدة الشرق الاوسط ٤ يوليو ٢٠١٠.

[2] د. محمد صادق اسماعيل، جرائم شبكات التواصل الإجتماعي والإنترنت، المنامة، مركز معلومات المرأة والطفل، ٢٠١٣، ص. ١١٤

للاتصال السريع بالانترنت Broad Band. اما بخصوص عدد شركات استيراد أجهزة الاتصالات فقد بلغ ٤٠ شركة في العام ذاته[١].

بلغت نسبة الأسر التي تمتلك هاتف ذكي ٥١.٠% في العام ٢٠١٤، بواقع ٥٩.٤% في الضفة الغربية، و٣٤.٧% في قطاع غزة، في حين بلغت نسبة الأسر في فلسطين التي لديها حاسوب ٦٣.١% في العام ٢٠١٤، بواقع ٦٦.٩% في الضفة الغربية، و٥٥.٦% في قطاع غزة، مقارنة مع ما يقارب الثلث (٣٢.٨%) من الأسر في فلسطين كان لديها جهاز حاسوب في العام ٢٠٠٦.

وقد ارتفعت نسبة مستخدمي الانترنت من كلا الجنسين في العام ٢٠١٤ مقارنة بما كانت عليه في العام ٢٠٠٠ وانحسرت الفجوة بين الجنسين؛ فقد ارتفعت النسبة بين الذكور من ٧.٩% الى ٥٩.٦% وارتفعت النسبة بين الإناث من ٢.٨% الى ٤٧.٥%. كما أن ٤٨.٣% من الأسر في فلسطين لديها اتصال بالإنترنت، بواقع ٥١.٤% في الضفة الغربية، و٤٢.٢% في قطاع غزة للعام ٢٠١٤، مقارنة مع ٣٠.٤% من الأسر في فلسطين كان لديها اتصال بالإنترنت في العام ٢٠١١. أما بخصوص استخدام الانترنت من الأفراد (١٠ سنوات فأكثر) الذين يستخدمون الحاسوب في فلسطين فقد بلغت ٥٣.٧%، بواقع ٥٤.٥% في الضفة الغربية، مقابل ٥٢.٢% في قطاع غزة، ويوضح الشكل التالي التوزيع النسبي لأغراض استخدام الانترنت.

وقد بلغت نسبة الأفراد (١٠ سنوات فأكثر) الذين يستخدمون شبكات التواصل الاجتماعي ٧٥.١% من مجمل مستخدمي الانترنت. أما بخصوص الغرض من استخدام شبكات التواصل الاجتماعي، فإن ٧٥.٠% من الأفراد الذين يستخدمون شبكات التواصل الاجتماعي يستخدمونها بغرض التعارف، و٧٦.٥% يستخدمونها بغرض الألعاب والتسلية و٦٢.٠% بغرض الاتصال الهاتفي في العام ٢٠١٤[٢].

لا يوجد تشريع خاص يتعلق بجرائم سرقة المعلومات والتعدي على حقوق المؤلف في البيئة الرقمية، إلا أنه يمكن ملاحقة هذه الجرائم عن طريق تطويع نصوص قانون العقوبات الفلسطيني بحيث ينطوي تحت لوائها بعض الجرائم المتعلقة بالكمبيوتر كنصوص جرائم السرقة وخيانة الأمانة والإتلاف وغيرها. ولكن يهمنا أن نشير إلى أهمية التطور التشريعي لتحديد ماهية السياسة الجنائية الواجب

---

[١] بالنسبة لخطوط الهاتف الثابت والنقال فقد تجاوز عدد خطوط الهاتف الثابت في فلسطين ١٤٠٣. ألف خط في العام ٢٠١٤، وبلغ عدد مشتركي الهاتف النقال ٣.١ مليون مشترك فيما وصل عدد مشتركي الاتصال السريع بالانترنت الى أكثر من ٢٣٥ ألف مشترك في العام ٢٠١٤. وبلغ عدد الحواسيب لدى الأسر الفلسطينية ١.١ مليون حاسوب ما بين كمبيوتر مكتبي ولابتوب وتابلت في العام ذاته.

[٢] بلغ عدد العاملين في البحث والتطوير في العام ٢٠١٣ في فلسطين ٨,٧١٥ عاملا يشكلون ٥,١٦٢ عامل بمكافئ الوقت التام، فيما بلغ عدد الباحثين في فلسطين ٤,٥٣٣ باحثا وباحثة يشكلون ٢,٤٩٢ باحثا وباحثة بمكافئ الوقت التام، كما بلغ عدد الباحثين الذكور ٣,٥١٠ باحثين، وعدد الباحثات الإناث ١,٠٢٣ باحثة، وقد بلغ عدد الباحثين بمكافئ الوقت التام ٥٦٦ باحثا وباحثة لكل مليون نسمة من السكان.

إتباعها وفقا للقانون الأساسي المعدل ٢٠٠٣م، والذي أشتمل على الضمانات الدستورية الخاصة بمكافحة الجريمة ومن بينها إذ انه لا جريمة التعدى على حقوق المؤلف.

خامسا: جرائم تقانة المعلومات بالإمارات العربية المتحدة

تصدرت الإمارات دول منطقة الشرق الأوسط في استخدام موقع التواصل الاجتماعي، "فيسبوك" مسجلة نسبة انتشار بلغت ٤١% مقابل، ٣٩,٢% في الأردن التي حلت ثانيا، ونحو ٣٥,٢ % في لبنان التي جاءت في المرتبة الثالثة عربياً، بحسب تقرير الإعلام الاجتماعي الذي أصدرته كلية دبي الحكومية.حيث أن نسبة انتشار موقع التواصل الاجتماعي في تركيا، بلغت نحو ٣٣,٩% مقابل ٢٦,٨ % في الكويت، و٢٥,١ % في البحرين، و٢٥% في فلسطين، و١٨,٣% في المملكة العربية السعودية، و ١٧,٤% في سوريا، و١٦,٤% في المغرب و١٦,٢% في عمان، و١٦,٢% في مصر[١].

وفي المقابل، بلغ عدد مستخدمي موقع التواصل الاجتماعي "تويتر" في الإمارات نحو ٣٦٣ ألف مستخدم فعال بنهاية شهر مايو الماضي، لتصل نسبة انتشار الموقع في الدولة إلى نحو ٤,٤% من عدد السكان، ونحو ٦,٢% من اجمالي عدد مستخدمي شبكة الإنترنت، وسجلت الإمارات نحو٢,٥ مليون ألف تغريدة يوميا عبر موقع التواصل الاجتماعي "تويتر".

ويعتبر قانون مكافحة جرائم تقنية المعلومات الإماراتي رقم (٢) لسنة ٢٠٠٦[٢]، من أحدث التشريعات العربية في هذا المجال، والذي تم اقتراحه من قبل الدولة وإعتماده لدى الأمانة العامة لمجلس التعاون لدول الخليج العربية كمسودة لمشروع قانون خليجي موحد لمكافحة جرائم تقنية المعلومات، وتم إعتماد صيغة المشروع في الإجتماع العاشر لوكلاء وزارات العدل بدول مجلس التعاون المنعقد بمدينة أبوظبي في شهر سبتمبر ٢٠٠٦. على أنه من الضرورى أن نتعرف على القوانين الإماراتية فى مجال الاتصالات وتكنولوجيا المعلومات والتى كانت بمثابة آليات الدولة الوطنية فى ملاحقة المجرم الالكترونى، وفيما يلى بيان بهذه القوانين:

١- نصوص قانون العقوبات الإتحادي رقم ٣ لسنة ١٩٨٧

لقد وردت في قانون العقوبات بحكم أنه القانون الجنائي العام تقسيمات كثيره للجرائم[٣]، منها مايقع على أمن الدولة الداخلي والخارجي، والجرائم الواقعة على الأموال (مثل جريمة السرقه، والنصب، وخيانة الأمانه والأتلاف)، والجرائم الواقعة على الأشخاص كالجرائم المتعلقه بحرمة الحياة الخاصة، والجرائم المتعلقة بالسمعة، والجرائم الماسة بالآداب العامة، وجريمة التهديد) ،والجرائم الماسة بالعقيدة

[١] رصد التقرير تراجع أعداد مستخدمي موقع التواصل الاجتماعي فيسبوك في الدولة للمرة الأولى منذ ٥ سنوات، حيث تراجع عدد مستخدمي الموقع بنسبة ١,١% خلال الفترة من ٧ يناير إلى ١ مايو من العام الحالي، بعد توقف نحو ٣٩,٤٤٠ شخص عن استخدام الموقع.

[٢] - راجع القانون الاتحادى رقم ٢ لسنة ٢٠٠٦ بشأن مكافحة جرائم المعلومات، أبو ظبى ٢٠٠٦.

[٣] - راجع قانون العقوبات الاتحادى رقم ٣ لسنة ١٩٨٧، أابو ظبى ١٩٨٧.

والأديان، والجرائم الخاصه بوسائل المواصلات والإتصالات، وغيرها من الجرائم، وعلى ذلك فإن قانون القوبات الإتحادي وإن كان لاتوجد به نصوص خاصة، لجرائم الحاسب الألي، أو جرائم الشبكات إلا أن العديد من الجرائم الواردة فيه، يمكن أن يستخدم الحاسب الآلي في ارتكابها كوسيلة أو أداة متتمة للجريمة، وبالتالي إذا تم في مرحلة التحقيق إدانة المتهم، والوصول الي مرحلة اسناد التهمة اليه وفق نصوص قانون الأجراءات الجزائيه، وتحققت في حقه أركان الجريمه الموصوفه في قانون العقوبات الإتحادي فإنه سينال العقوبه الواردة في هذا القانون وخاصة أن هناك مبدأ قانوني مقرر بالمادة (٤٢) من قانون العفوبات نصها(لايعتبر الجهل بأحكام هذا القانون عذرا) هذه قاعده مسلم بها في جميع التشريعات الجنائيه، وبالتالي لايمكن لشخص ان يتعلل بأنه لا يعلم أن ارتكاب الجرائم عن طريق الحاسب الألي ليس مجرما أو ليس له نصوص خاصة، مادام فعله يشكل جريمه تنطبق عليها أوصاف وأركان الجريمه الوارده بقانون العقوبات الإتحادي، وذلك تحقيقا لمبدأ المشروعية، أو الشرعية الجنائية، ومقتضاه انه لاجريمه ولا عقوبه إلا بنص ، فحيثما وجد هذا النص سواء في قانون خاص او عام، وارتكب شخص ما الفعل المحظور بموجب ذلك النص فإن الجريمه تقع ،ويصبح من المشروع معاقبة مرتكبها، بغض النظر عن مسمى القانون، أو مكان ورود النص المحرم للفعل

ومن أمثلة الجرائم التي يمكن ان ترتكب عن طريق أجهزة الحاسب الألي والأجهزه المرتبطه بها ويمكن معاقبة مرتكبيها بالعقوبات الوارده بقانون العقوبات الأتحادي ،الجرائم الأتيه: [1]

<u>- جريمة تخريب أو تعطيل وسائل الاتصال الدولية</u>

حيث نصت المادة (٢١) على انه ((يسري هذا القانون على كل من وجد في الدولة بعد ان ارتكب في الخارج بوصفه فاعلا او شريكا في جريمة تخريب او تعطيل وسائل الاتصال الدوليه أو جرائم الاتجار بالمخدرات أو في النساء أو الصغار أو الرقيق أو جرائم القرصنة ،والإرهاب الدولي)).

<u>- جريمة التهديد</u>

من المتصور أن تتم جريمة التهديد المنصوص عليها في القانون عن طريق الحاسب الآلي، وذلك عن طريق، كتابة التهديد في برنامج معين أو نشره على صفحة الويب، أو إرسال رسالة تهديد برسالة إلكترونيه(إميل)، أو اثناء المحادثة التي تتم في غرف الدردشه(الشات) أو المنتديات ،أو غرف المحادثه (البالتوك)، كما نصت المادة (٣٥١) من قانون العقوبات على أنه (يعاقب بالسجن مدة لا تزيد على سبع سنوات من هدد آخر بأرتكاب جناية ضد نفسه أو ماله أو ضد أومال غيره أو بإسناد امور خادشه بالشرف أو إفشائها، وكان ذلك مصحوبا بطلب أو بتكليف بأمر أو الامتناع عن فعل أو مقصود به ذلك)).

<u>- الجرائم الماسة بالآداب العامة</u>

من جرائم الإخلال بالآداب والتحريض على الفجور والتي وردت في مواد القانون الإماراتى مايلي:

[1] د. محمد صادق اسماعيل، جرائم شبكات التواصل الإجتماعي والإنترنت، مرجع سابق، ص. ١٢٤

أ- الجهر بما يخالف الأداب، أو إغراء الغير علانية بالفجور

ورد النص على هذه الجرائم في المادة(٣٦١)، حيث نصت على(يعاقب بالحبس مدة لاتزيد على ستة شهور وبغرامة لا تزيد على خمسة آلاف درهم أو بأحدى هاتين العقوبتين كل من جهر بنداء أو أغان أو صدر عنه صياح لأي خطاب مخالف للآداب وكل من جهر علانية بالفجور بأية وسيلة كانت)

ب- تجريم نشر وتوزيع وعرض الصور والأفلام والرسومات المخلة بالآداب العامة

أما المادة رقم (٣٦٢) فقد جرمت وعاقبت بذات العقوبة الواردة بالمادة (٣٦١)المشار اليها سلفا، حيث حددت خمسة أفعال مختلفة، جرَّمتها المادة ولكن بشرط خاص ألا وهو اتجاه قصد الجاني إلي استغلالها أو توزيعها أو عرضها على الغير[١].

٢- قانون تنظيم قطاع الإتصالات رقم (٣) لسنة ٢٠٠٣

صدر قانون تنظيم قطاع الاتصالات ليكون القانون الذي ينظم عمل شركات الاتصالات بالدولة، وينشئ هيئة جديدة تسمى هيئة تنظيم قطاع الاتصالات بالدولة وحددت االمادة (١٢) من هذا القانون مهام وصلاحيات واختصاصات الهيئة بأنها هي السلطة المختصة بالرقابة على قطاع الاتصالات والمرخص لهم، وذلك وفقا لأحكام هذا المرسوم بقانون ولائحته التنفيذية والتعليمات الصادرة عن اللجنة العليا،....الخ).

وورد بالباب التاسع من هذا القانون مجموعة مواد تجرم بعض الأفعال وتفرض عقوبات على مخالفة الأحكام والالتزامات التي يفرضها القانون حيث نصت المادة (٧١) على عقوبة الحبس مدة لاتجاوز سنتين، وبغرامة لاتقل عن خمسين ألف درهم ولا تجاوز مائتي ألف درهم أو بإحدى هاتين العقوبتين كل من يباشر أي من الأنشطة التي نظمها القانون دون الحصول على ترخيص أو إعفاء وفقا لأحكام هذا القانون، أو يقوم متعمدا بتغيير أو اتلاف أو إخفاء أية وثيقة أو معلومة تطلبها اللجنة العليا أو الهيئة أو لم يقم بتعديل أوضاعة وفقا لأحكام هذا المرسوم بقانون خلال المدة المحددة. كذلك ورد النص صراحة على جرائم محددة وهي(تقديم أو المساهمة في تقديم خدمات اتصالات مخالفة للآداب العامة أو النظام العام) ويندرج تحت هذا المصطلح العديد من الجرائم وخاصة ترويج الصور والمواد الإباحية أو المشاهد الخادشة للحياء أو الدعوة للفجور والرذيلة أو الدعوة لتعكير صفو الأمن واشاعة الفوضى أو تعكير أمن الناس وسكينتهم وتعريض صحتهم للخطر، وهذه الجرائم إذا ارتكبت عن طريق شبكة الإنترنت التي هي خدمة من خدمات الاتصالات فمثل هذه الجرائم يمكن ملاحقة مرتكبيها وفقا لأحكام هذا القانون.

---

[١] حيث نصت على (كل من صنع أو استورد أو صدر أو حاز أو أحرز أو نقل بقصد الاستغلال أو التوزيع أو العرض على الغير كتابات أو رسومات أو صورا، أو أفلاما أو رموزا أو غير ذلك من الأشياء إذا كانت مخلة بالآداب العامة. ويعاقب بالعقوبة ذاتها كل من أعلن عن شيء من الأشياء المذكورة)،

كذلك جريمة تعطيل عمل شبكة الانترنت وهي من الجرائم الخطيرة والمؤثرة يمكن ملاحقة مرتكبيها بموجب نص المادة السابقة حيث ورد في البند رقم(٤) النص صراحة على تجريم تعطيل أي من خدمات الاتصالات والتي من ضمنها خدمة الإنترنت.

ومن ثم يعتبر قانون مكافحة جرائم تقنية المعلومات الإماراتي رقم (٢) لسنة ٢٠٠٦[١]، من أحدث التشريعات العربية في هذا المجال، والذي تم اقتراحه من قبل الدولة وإعتماده لدى الأمانة العامة لمجلس التعاون لدول الخليج العربية كمسودة لمشروع قانون خليجي موحد لمكافحة جرائم تقنية المعلومات، وتم إعتماد صيغة المشروع في الإجتماع العاشر لوكلاء وزارات العدل بدول مجلس التعاون المنعقد بمدينة أبوظبي في شهر سبتمبر ٢٠٠٦.

سادسا: جرائم تقانة المعلومات بالكويت

أظهر تقرير اقتصادي متخصص أن نسبة نمو مستخدمي الانترنت في دولة الكويت ارتفع بمعدل عال يزيد على ٦٠٠ في المئة على مدى عشر سنوات منذ عام ٢٠٠٠ حيث وصل اجمالي المستخدمين الى نحو مليون و١٥٠ ألف مستخدم مع نهاية ٢٠١٠. كما أن عدد مستخدمي الانترنت في الكويت سيمثل تقريبا نصف عدد سكانها والبالغ نحو ثلاثة ملايين نسمة في ٢٠١١، مشيرا الى أن عدد المستخدمين بلغ في عام ٢٠٠٠ نحو ١٥٠ ألف مستخدم.

وضمن جهود وزارة الداخلية لمحاربة الجرائم بجميع أنواعها وتطبيق القانون على الجميع، وفي خطوة تعد من الخطوات الهامة للقضاء على جرائم تقنية المعلومات وبعدما لوحظ في الآونة الأخيرة من تجاوزات وجرائم يقوم بها البعض من خلال استخدام أجهزة الحاسب الآلي..صدر قانون جرائم تقنية المعلومات رقم ٦٣ لسنة ٢٠١٥ والذي بدأ تطبيقه من يوم ٢٠١٦/١/١٢، وذلك بعد ما تم نشره في الجريدة الرسمية بتاريخ ٢٠١٥/٧/٧. وذلك سعيا من دولة الكويت في سياق دعم التوجهات الدولية الخاصة بمكافحة هذه الجرائم، والتزاما بأحكام الإتفاقية العربية لمكافحة جرائم تقنية المعلومات التي صادقت عليها دولة الكويت بموجب القانون رقم (٦٠) لسنة ٢٠١٣.

لذا فقد أعد القانون المرافق، الذي يتناول في الفصل الأول في المادة الأولى منه التعريفات التي تبين المقصود بالمصطلحات الفنية الواردة فيه .وشمل الفصل الثاني الجرائم والعقوبات، فنصت المادة (٢) على جريمة غير المشروع إلى جهاز حاسب آلي أو أنظمة معلوماتية باستخدام إحدى وسائل تقنية المعلومات وقضت فقراتها الثانية والثالثة بتشديد العقوبة في حالة إذا ما ترتب على هذا الدخول إلغاء أو إتلاف للبيانات أو في حالة المعلومات الشخصية، كما نصت الفقرة الرابعة على تشديد العقوبة إذا أرتكبت الجريمة أثناء أو بسبب تأدية الوظيفة[٢].

---

[١] - راجع القانون الاتحادى رقم ٢ لسنة ٢٠٠٦ بشأن مكافحة جرائم المعلومات، أبو ظبى ٢٠٠٦.

[٢] تم اصدار القانون بناء على المرسوم الأميري رقم (١٧) لسنة ١٩٥٩ بقانون إقامة الأجانب والقوانين المعدلة له وعلى المرسوم الأميري رقم (١٢) لسنة ١٩٦٠ بقانون تنظيم إدارة الفتوى والتشريع لحكومة الكويت، وعلى قانون الجزاء الصادر بالقانون رقم (١٦) لسنة ١٩٦٠ والقوانين المعدلة له، وعلى قانون الاجراءات والمحاكمات الجزائية الصادر بالقانون رقم (١٧) لسنة ١٩٦٠ والقوانين المعدلة له، وعلى القانون رقم (١) لسنة ١٩٩٣ بشأن

وكذلك تضمنت المادة (٣) تشديد العقوبة في حالة كون البيانات محل الجريمة حكومية أو متعلقة بحسابات العملاء في المنشآت المصرفية. وتناولت ذات المادة تجريم أفعال التزوير أو إتلاف المستندات الإلكترونية عرفية أو حكومية أو بنكية بما فيها تلك المتعلقة بالفحوصات الطبية، وكذلك استخدام أي وسيلة من وسائل تقنية المعلومات في تهديد الأشخاص أو ابتزازهم، مع تشديد العقوبة إذا كان التهديد بارتكاب جناية أو المساس بكرامة الأشخاص أو شرفهم.

ونصت المادة (٤) على عقاب من أعاق أو عطل عمدا الوصول الى مواقع إلكترونية، وكل من تنصت على ما هو مرسل عن طريق الشبكة المعلوماتية، وكل من أنشأ موقعا يتضمن مساسا بالآداب العامة أو تحريضا على أعمال الدعارة والفجور. وأوجبت المادة (٥) عقاب كل من توصل عن طريق إحدى وسائل تقنية المعلومات إلى بيانات بطاقة ائتمانية واستخدامها في الحصول على أموال الغير.

وقضت المادتان (٦) و (٧) بمعاقبة كل من ارتكب إحدى المحظورات المنصوص عليها في قانون المطبوعات والنشر باستخدام الوسائل الإلكترونية. وأوجبت المواد (٨) و (٩) و (١٠) عقاب كل من استخدم أي من هذه الوسائل في الترويج للإتجار بالبشر أو المواد المخدرة أو في تسهيل الاتصال بالمنظمات الإرهابية وترويج أفكارها أو غسل الأموال. وتضمنت المواد من (١١) إلى (١٩) الأحكام العامة ومنها حالات الإعفاء من العقوبة، والحكم بمصادرة أو إغلاق المحل أو الموقع، والمسئولية الجزائية للشخص الإعتباري، وإختصاص النيابة العامة وحدها بالتحقيق والتصرف والإدعاء في هذه الجرائم، وأحكام سقوط الدعويين الجزائية والمدنية.

حماية الأموال العامة والقوانين المعدلة له، وعلى القانون رقم (٦٤) لسنة ١٩٩٩ في شأن حقوق الملكية الفكرية، وعلى القانون رقم (٩) لسنة ٢٠٠١ بشأن إساءة استعمال أجهزة الاتصالات الهاتفية وأجهزة التنصت والقوانين المعدلة له، وعلى القانون رقم (٣) لسنة ٢٠٠٦ بشأن المطبوعات والنشر، وعلى القانون رقم (٦١) لسنة ٢٠٠٧ بشأن الإعلام المرئي والمسموع، وعلى القانون رقم (٧) لسنة ٢٠١٠ بشأن إنشاء هيئة أسواق المال وتنظيم نشاط الأوراق المالية المعدل بالقانون رقم (١٠٨) لسنة ٢٠١٤، وعلى القانون رقم (٨) لسنة ٢٠١٠ في شأن حقوق الأشخاص ذوي الإعاقة، وعلى القانون رقم (٥٣) لسنة ٢٠١١ بشأن الإدارة العامة للتحقيقات بوزارة الداخلية، وعلى المرسوم بالقانون رقم (٢٤) لسنة ٢٠١٢ بإنشاء الهيئة العامة لمكافحة الفساد والأحكام الخاصة بالكشف عن الذمة المالية، وعلى المرسوم بالقانون رقم (٢٥) لسنة ٢٠١٢ بإصدار قانون الشركات المعدل بالقانون رقم (٩٧) لسنة ٢٠١٣،وعلى القانون رقم (٩١) لسنة ٢٠١٣ في شأن مكافحة الاتجار بالأشخاص وتهريب المهاجرين، وعلى القانون رقم (١٠٦) لسنة ٢٠١٣ في شأن مكافحة غسل الأموال وتمويل الإرهاب، وعلى القانون رقم (١١١) لسنة ٢٠١٣ في شأن تراخيص المحال التجارية، وعلى القانون رقم (٢٠) لسنة ٢٠١٤ في شأن المعاملات الإلكترونية، وعلى القانون رقم (٣٧) لسنة ٢٠١٤ بإنشاء هيئة تنظيم الاتصالات وتقنية المعلومات،

المطلب الثاني

جرائم تقانة المعلومات فى الدول الغربية

يصعب تقدير حجم الخسائر المترتبة على جرائم نظم المعلومات[1] والسبب في ذلك الرقم الأسود الذي يسيطر على هذا النوع من الإجرام علاوة على الموقف السلبي للمجني عليهم في هذه الجرائم، ولصعوبة اكتشاف الجريمة المعلوماتية[2]. لذا فإنه من الصعوبة تقدير حجم الخسائر الناشئة عن هذه الجرائم[3] كما تشير بذلك الأبحاث التي أجريت في هذا الشأن سواء في فرنسا أو الولايات المتحدة الأمريكية أو إنجلترا.

أولا: خسائر جرائم تقانة المهلومات فى الدول الغربية

يمكن التعرض بقدر من التفصيل للخسائر التي تنجم عن جرائم الانترنت في الدول الغربية والامريكية على النحو التالي:

١- تقدير خسائر الجرائم المعلوماتية فى الولايات المتحدة الأمريكية

أجرى المكتب الأعلى للإحصاء general Accounting office تحقيقاً بخصوص ظاهرة الغش في الأنظمة المعلوماتية الخاصة بالحكومة الفيدرالية، وجاءت نتيجته على النحو التالي :

- ٤٠% حالات اختلاس أشياء مختزنة ترتب عليها خسارة قدرت بحوالي ٥٧.٠٠٠ دولار.
- ٣٩% حالات اختلاس أموال تسببت في خسارة قدرت بـ ٣٤.٠٠٠ دولار.
- ١٢% حالات تعديل غير مسموح به في البيانات.
- ٦% حالات استخدام غير مسموح به للأنظمة المعلوماتية.
- ٣% حالات اتلاف.

---

(1) المخربون : يقوم المخربون باستخدام بعض الوسائل الأوتوماتيكية لاكتشاف نقاط الضعف في نظم الكمبيوتر بغرض زرع البرنامج المدمر في تلك النظم، ويظل هذا البرنامج كامناً حتى يحين موعد الهجوم المحدد. فإذا ما قام المخربون بزرع البرنامج المذكور عبر جهاز كمبيوتر خاص بشخص آخر فإن ذلك يزيد من صعوبة تعقبهم. راجع في ذلك:

Dr: Linda Volonino. Cybet Terrorism. Op. cit.

(2) Bertin et Lambertie, la protection du logiciel, enjeux juridiques et economiques L.G.D.J. 1985, p. 30

(3) وتجدر الإشارة في هذا الصدد إلى أن إحجام ضحايا الجرائم المعلوماتية عن الإبلاغ عن الجرائم المرتكبة في حقهم – سواء لخوفهم من الفضيحة أو لاعتقادهم بعدم قدرة الشرطة على التعامل مع مثل هذه الجرائم، = = أو لعدم درايتهم من حيث المبدأ- لوقوع مثل هذه الجرائم – أن هذا الإحجام يؤدي إلى فرار المجرمين من العقاب كما أنه يترك وحدات جرائم الكمبيوتر الشرطية التي تتمتع بكفاءة عالية دون عمل يذكر ومن هنا يظل النطاق الحقيقي لجرائم الكمبيوتر : حجمها، طبيعتها ومداها وتهديداتها – تظل كلها أمور غامضة، انظر:

HACKER CRACK DOWN Law and Disorder on the Electronic Frontier b : Bruce sterling p. 168. 1994.

فغالبية أفعال الغش ارتكبت عن طريق إدخال بيانات مصطنعة ٦٢%. ثم يلي ذلك الاستعمال غير المشروع للوسائل المعلوماتية "٢٥%" ويأتي في المرتبة الثالثة تعديل المعالجات المعلوماتية "٢٣%" وأخيراً اختلاس الوثائق الصادرة عن الحساب الآلي "١٧%"[١].

وأجريت دراسة بواسطة المعهد الأمريكي للتصديق على الإحصاء العام بخصوص الغش المعلوماتي في البنوك وشركات التأمين والتي انتهت إلى أنه في غالبية الحالات "٦٠%" يتحقق الغش عن طريق التلاعب في الصفقات، إما بخلق معلومات مصطنعة أو اتلاف أو تعديل بيانات حقيقية، وفي ثلث الحالات عن طريق التعديل في مناطق تسجيل الملفات، وأن استمرار فعل الغش يرتبط بالوضع الوظيفي لمرتكبه. وهكذا فإن ٤١% من حالات الغش بوشرت عن طريق مستخدمين استمرت لمدة أقل من سنة واحدة، ١٥% من تلك الحالات نفذت بواسطة مسئولين استمرت لمدة أكثر من سنة، ويتوافر لهذه الفئة الأخيرة إمكانيات لإخفاء أفعالهم، ويتطابق الوضع الوظيفي والمبالغ المتحصلة من أفعال الغش حيث أن ٥٩ من حالات الغش والتي قدرت بأقل من ٢٥.٠٠٠ دولار قد تم ارتكابها بواسطة مستخدمين في البنوك و٨٥% في شركات التأمين، بينما نسبت أفعال الغش التي تجاوزت ١٠٠٠.٠٠٠ دولار إلى المستخدمين الذين يشغلون مراكز متقدمة.وباشر الاتحاد الأمريكي للمحامين تحقيقاً على ٢٨٣ منشأة ومؤسسة كبري، وتبين أن ثلثيهما وقعتا ضحية لظاهرة الغش المعلومات بدرجات متفاوتة. كما أظهر التحقيق، أنه عندما يكون الحاسب الآلي موضوعاً للجريمة، فإن ثماني منشآت من عشر يعتبرون أن محو أو إتلاف البيانات يمثل النمط الأكثر خطورة لهذه الظاهرة، ونفس الأمر بالنسبة لسرقة أو إتلاف البرامج، وعلى النقيض بالنسبة لسرقة أو إتلاف المعدات المادية فهي تبدو على وجه التحديد اقل خطورة.

ويستحيل نسبياً معرفة إجمالي الخسائر التي لحقت بالمنشآت الأمريكية ووفقاً لتقدير الاتحاد الأمريكي للمحامين، فإن ربع هذه المنشآت قد عانت من خسائر في العام السابق على إجراء التحقيق، تفاوتت من ١٤٥ إلى ٧٣٠ مليون دولار، وهذا يعكس تبايناً واضحاً في الخسارة من منشأة أخرى وعلى وجه العموم فقد قدرت بأقل ١٠٠.٠٠٠ دولار بالنسبة لـ ٢٠% من هذه المنشآت. وقدرت بأكثر من مليون دولار لـ ٤% منها، وأن ٢٨% من هذه المنشآت لم تعلم مقدار الخسارة التي لحقت بها من أثر الغش المعلوماتي[٢].

٢- تقدير حجم خسائر الجرائم المعلوماتية في إنجلترا

قدر اتحاد الصناعات الإنجليزية الخسائر الناشئة عن الغش المعلوماتي بمبلغ يتراوح ما بين ٢٥ إلى ٣٠ مليون جنيه إسترليني في السنة. وتوضح الدراسة التي قام بها K. Wong على ٩٥ حالة غش معلوماتي أن متوسط الخسارة فيها بلغ ٣٠.٠٠٠ جنيها إسترلينياً. كما أبانت عن أن سرقة

---

(١) انظر د. محمد سامي الشوا، – ثورة المعلومات وإنعكاساتها على قانون العقوبات، ص ٢٥.

(٢) راجع:

Daved smoloon (2009) the impact of the use of face book on the building society in the context of globalization, N Y sprctrum puplication .

المعدات المادية ولاسيما "الحاسبات الآلية الميكروية" والحرائق العمدية والإتلاف لا تمثل كل منها سوي ٣٠% من الحالات محل الدراسة. ومع ذلك فإن خسائرها كانت مرتفعة جداً.

وبالنسبة لسرقة المعلومات والبرامج "وتمثل ١٥% من الحالات"، فهي تباشر بصفة أساسية عندما يحل المستخدمون محل الإجراء، وأن إتلاف التجهيزات غالباً ما يتسبب عنه الطاقم المسئول عن تشغيل وتخزين الدعائم الممغنطة، ولكن بالنسبة لإتلاف وظيفة النظام bombes logiques " ٨%" فهو من صنع المبرمجين أو أصحاب البرامج. ويمثل انتهاك الأنظمة المعلوماتية بغرض الحصول على معلومات أو خدمات مجانية نسبة تقدر بحوالي العشر، ولكن هذا النمط من الإجرام سيتضاعف بسبب انتشار الحاسبات الميكروية المنزلية[١].

٣- تقدير خسائر الجرائم المعلوماتية في فرنسا

ارتفع معدل الخسائر الناتجة عن المعلوماتية في فرنسا حيث بلغت وفقاً لإحصاء الجمعية العمومية لشركات التأمين ضد الحرائق والمخاطر المختلفة APSAIRO حوالي ٧.٣ مليار فرنك فرنسي، ويرجع ٤٦% منها إلى الأفعال الإجرامية و ٣٠% إلى المخاطر العارضة و٢٤% إلى الأخطاء. ويتبين من تحليل الخسائر المرتبطة بجرائم المعلومات في فرنسا أن ٦٠% منها يتعلق بالبرامج، ويتركز الغش في معظم هذه الحالات في اتفاقات غير مشروعة (٣٥%) واستغلال الأعطال القائمة ١٠% وتضليل البرامج ٩% ومن ناحية التشغيل فإن ٢٥% من الخسائر ترجع إلى تعديل الإجراءات والملفات والسهو المتعمد ونقل البيانات.

وقد تضاعفت خسائر سرقة البرامج المنطقية ذو النمط الواحد وفقاً لتقدير وكالة حماية البرامج لتصل إلى ١.١٢ مليار فرنك ويرجع ٤٣% من هذه الخسائر إلى سرقة أدوات البرامج المنطقة ذو النمط الواحد "كبرامج الفائدة الخاصة بالتصنيف والمعاونة في تصميم برامج وإدارات البيانات والأمن وصيانة البرامج، و ٣٠% للبرامج المنطقية التطبيقية ذو النمط الواحد الخاصة بالسداد والمحاسبة وإدارة الوثائق، ١٧% للبرامج المنطقية الأساسية ذو النمط الواحد الخاصة بأنظمة التشغيل، وقدرت خسائر الألعاب بحوالي ١٠%. ويشهد معدل الخسائر في مجال صفقات الإنتاج وشركات الخدمات والمنشآت الناشرة للبرامج ارتفاعاً ملحوظاً حيث وصلت الخسائر إلى ١٩% في عام ١٩٨٥، ٥٠% منها للحاسب الآلي الميكروي، ١١% للأنظمة المتوسطة والكبيرة[٢].

---

[١] راجع في ذلك:

Christakis, Nicholas A. Fowler, James H. (January 12, 2011), Connected: The Surprising Power of Our Social Networks and How They Shape Our Lives -How Your Friends' Friends' Friends Affect Everything You Feel, Think, and Do, USA: Back Bay Books; Reprint edition

(٢) انظر في ذلك

Christakis, Nicholas A. Fowler, James H. (January 12, 2011), Connected: The Surprising Power of Our Social Networks and How They Shape Our Lives -How Your Friends' Friends' Friends Affect Everything You Feel, Think, and DoOp, Cit

ثانيا: جرائم تقانة المعلومات بين التشريع والقضاء في الدول الغربية

تعتبر السويد أول دولة تسن تشريعات خاصة بجرائم الحاسب الآلي والانترنت، حيث صدر قانون البيانات السويدي عام (١٩٧٣م) الذي عالج قضايا الاحتيال عن طريق الحاسب الآلي إضافة إلى شموله فقرات عامة تشمل جرائم الدخول غير المشروع على البيانات الحاسوبية أو تزويرها أو تحويلها أو الحصول غير المشرع عليها .

وتبعت الولايات المتحدة الأمريكية السويد حيث شرعت قانونا خاصة بحماية أنظمة الحاسب الآلي (١٩٧٦م – ١٩٨٥م)، وفي عام (١٩٨٥م) حدّد معهد العدالة القومي خمسة أنواع رئيسة للجرائم المعلوماتية وهي: جرائم الحاسب الآلي الداخلية، جرائم الاستخدام غير المشروع عن بعد، جرائم التلاعب بالحاسب الآلي، دعم التعاملات الإجرامية، وسرقة البرامج الجاهزة والمكونات المادية للحاسب. وفي عام (١٩٨٦م) صدر قانونا تشريعاً يحمل الرقم (١٢١٣) عرّف فيه جميع المصطلحات الضرورية لتطبيق القانون على الجرائم المعلوماتية كما وضعت المتطلبات الدستورية اللازمة لتطبيقه، وعلى اثر ذلك قامت الولايات الداخلية بإصدار تشريعاتها الخاصة بها للتعامل مع هذه الجرائم ومن ذلك قانون ولاية تكساس لجرائم الحاسب الآلي.

وتأتي بريطانيا كثالث دولة تسن قوانين خاصة بجرائم الحاسب الآلي حيث أقرت قانون مكافحة التزوير والتزييف عام (١٩٨١م) الذي شمل في تعاريفه الخاصة بتعريف أداة التزوير وسائط التخزين الحاسوبية المتنوعة أو أي أداة أخرى يتم التسجيل عليها سواء بالطرق التقليدية أو الإلكترونية أو بأي طريقة أخرى.

وتطبق كندا قوانين متخصصة ومفصلة للتعامل مع جرائم الحاسب الآلي والانترنت حيث عدلت في عام (١٩٨٥م) قانونها الجنائي بحيث شمل قوانين خاصة بجرائم الحاسب الآلي والانترنت، كما شمل القانون الجديد تحديد عقوبات المخالفات الحاسوبية، وجرائم التدمير، أو الدخول غير المشروع لأنظمة الحاسب الآلي.

وفي عام (١٩٨٥م) سنّت الدنمارك أول قوانينها الخاصة بجرائم الحاسب الآلي والانترنت والتي شملت في فقراتها العقوبات المحددة لجرائم الحاسب الآلي كالدخول غير المشروع إلى الحاسب الآلي أو التزوير أو أي كسب غير مشروع سواء للجاني أو لطرف ثالث أو التلاعب غير المشروع ببيانات الحاسب الآلي كإتلافها أو تغييرها أو الاستفادة منها .

وكانت فرنسا من الدول التي اهتمت بتطوير قوانينها الجنائية للتوافق مع المستجدات الإجرامية حيث أصدرت في عام (١٩٨٨م) القانون رقم (١٩-٨٨) الذي أضاف إلى قانون العقوبات الجنائي جرائم الحاسب الآلي والعقوبات المقررة لها.

أما في هولندا فلقاضي التحقيق الحق بإصدار أمره بالتصنت على شبكات الحاسب الآلي متى ما كانت هناك جريمة خطيرة، كما يجيز القانون الفنلندي لمأمور الضبط القضائي حق التنصت على المكالمات

الخاصة بشبكات الحاسب الآلي، كما تعطي القوانين الألمانية الحق للقاضي بإصدار أمره بمراقبة اتصالات الحاسب الآلي وتسجيلها والتعامل معها وذلك خلال مدة أقصاها ثلاثة أيام.

كما يوجد في المجر وبولندا قوانين خاصة بجرائم الحاسب الآلي والانترنت توضح كيفية التعامل مع تلك الجرائم ومع المتهمين فيها، وتعطي تلك القوانين المتهم الحق في عدم طبع سجلات الحاسب الآلي أو إفشاء كلمات السر أو الأكواد الخاصة بالبرامج[١].

وقد أدى ربط الحاسبات الآلية بعضها بالبعض الآخر عن طريق شبكة المعلومات إلى سرعة انتقال المعلومات من جهة وإلى سهولة التطفل عليها واختلاسها من جهة أخرى عن طريق استخدام(المودم) modem [٢]. حيث يسمح هذا الجهاز للمتطفلين من أي مسافة يتواجدون بها بالولوج فى الحاسبات الآلية المستهدفة ودون أي مساس مادى بحق ملكية الغير أو ترك أى أثر تدل على انتهاك المعلومات أو نسخها. ونظراً لجسامة هذا النوع من التعدى فقد حرص العديد من الدول على ارساء مبدأ لحماية وسلامة نظم المعلومات لديها وبغض النظر عن مبدأ حماية سرية البيانات المعالجة أو المتداولة. وسوف نستعرض الحلول التشريعية التى استحدثت فى هذا المجال في بعض الدول

١- جرائم تقانة المعلومات فى التشريع الفرنسى

استحدث القانون الفرنسى الصادر فى ٥ يناير ١٩٨٨ بموجب المادة ٢/٤٦٢ عقوبات، جريمة الولوج غير المشروع فى نظم المعلومات والتى تنص على" يعاقب .... كل من ولج أو تواجد بطريق الغش فى كل أو جزء من نظام مبرمج للبيانات". وتشدد العقوبة إذا ما ترتب على ذلك إلغاء أو تعديل للبيانات التى يحتويها النظام أو إتلاف لوظيفة هذا النظام".

ويستهدف هذا النص فى المقام الأول حماية الولوج فى نظم المعلومات لا حماية حق الملكية ذاته وهو بذلك سد فراغا تشريعيا هائلا فى القانون الفرنسى، ومن جهة أخرى استجاب لرغبة ملاك الأنظمة المعلوماتية [٣].

وتفترض هذه الجريمة توافر عنصرين أحدهما مادى والآخر معنوى.

أ-العنصر المادى: يتحقق العنصر المادى لهذه الجريمة بمجرد شروع أى شخص- ليس له الحق – فى الدخول، أو تدخل بالفعل فى نظام مبرمج للبيانات. ولكن هل يشترط لنشوء الجريمة أن يكون النظام محميا بواسطة جهاز أمن dispositif de securite! تمسك مجلس الشيوخ الفرنسى بهذا الشرط،

---

[١] انظر: د. هدى حامد قشقوش، جرائم الحاسب الالكتروني فى التشريع المقارن، القاهرة،دار النهضة العربية،د.ت

[٢] MODEM(): عبارة عن أداة لترجمة تعليمات مكتوبة بلغة الحاسب الآلى إلى رموز رقمية أو العكس حيث يسمح للحاسبات الآلية أن تستقبل وتنقل المعلومات عن طريق وسيط لخط تليفونى.

[٣] راجع فى ذلك:

J.P.Buffelan,art.Prec.P.99.

وحجته فى ذلك جذب انتباه أصحاب الأنظمة إلى هذه النقطة الأساسية كى يدعموا أنظمتهم بأجهزة الأمن [١].

بينما رأت الجمعية الوطنية الفرنسية، أنه من غير المناسب التمسك بهذا الشرط، لأنه سوف يترتب عليه قصر الحماية الجنائية على الأنظمة المحمية بواسطة أجهزة الأمن ومن ثم يستبعد من مجال تطبيق النص أفعال الولوج التى ترتكب ضد الأنظمة المفتوحة للعامة [٢] كالدليل الالكتروني أو الخدمات التى تقدم على رقم ٣٦-١٥. وكتب لهذا الرأي الأخير النجاح، وتم التصويت على النص بدون حاجة إلى اقتضاء هذا الشرط. ويتحقق التواجد غير المشروع، بمجرد علم الشخص بأنه تدخل بمحض الصدفة أو عن طريق الخطأ- وعلى نحو غير مشروع – فى نظام مبرمج للبيانات، ويستمر فى حال الاتصال به بدلا من الانفصال عنه فى الحال.

وهذه جريمة من جرائم الامتناع التى يصعب تقديم دليل أثبات فيها حيث يزعم المتهم دائما حال القبض عليه أنه كان على وشك الانفصال عن النظام المعتدى عليه [٣] ويستوى أن يكون الولوج فى النظام المعتدى عليه كليا أو جزئيا حيث يستطيع المعتدى فى حالة التدخل المقترن بالغش، أن يدعى بسهولة بأن تحوله كان محدودا بجزء ضيق جداً من النظام، ولا يمكن التحقق من مثل هذا الإدعاء من الناحية العلمية[٤].

ب-لعنصر المعنوى:

يجب أن يتوافر لدى الفاعل قصد خلاص علاوة على القصد العام " أى اتيان الفعل غير المشروع عن علم وإرادة". والذى يتمثل فى نية الغش **Fraudulcuscmcnt**. ويقصد بالغش أن يباشر الفاعل سلوكه عن طريق الخديعة وبسوء نية وبغرض خداع الغير[٥].

ويتمثل قصد الغش فى معرفة المتهم بأنه قد ولج أو تواجد فى نظام البيانات المبرمج ضد رغبة صاحب النظام وأيا كان الدافع إلى ذلك.

٢- موقف التشريعات الانجلوسكسونية من جريمة تقانة المعلومات

سوف نتعرض فى هذه النقطة لبعض النماذج التشريعية للدول الأنجلو سكسونية وذلك على النحو التالى:

---

(١) راجع فى ذلك:

J.Pradel,art prec,P.827, Lucas de leyssac, OP.CIT.P.21.

(٢) انظر:

Rapport de r.Andre, Assemble Nationale,no.1078 "1987, 1988"P.5.

(٣) راجع فى ذلك:

J.P.Buffelan,art. Prec,P.100.

(٤) راجع فى ذلك:

F.Chamoux ,art prec ,H..Croze ,ART,PREC V. ROULET ,art prec.

(٥) أنظر فى ذلك:

Lucas de Leyssac,OP.CIT.,P.20.

أ- التشريع الانجليزى فى مجال جرائم إساءة استخدام النظم المعلوماتية

استحدث المشرع الانجليزى عام ١٩٩٠ قانونا يعالج فيه إساءة استخدام نظم المعلومات وقد تم بموجب هذا التشريع تجريم عملية دخول أى فرد على البيانات المختزنة بالحاسب الآلى أو البرامج وكذلك عملية تعديلها بصورة غير مشروعة أو أى محاولة لفعل ذلك [١]. وقد نص القانون على ثلاثة جرائم محددة وهى [٢]:

١- الدخول المتعمد غير المشروع:

Access is deliberate and unauthorized

٢- الدخول غير المشروع والذى يتم بنية ارتكاب العديد من الجرائم.

٣- قيام الفرد بأى فعل متعمد ينشأ عنه إجراء تعديل غير مشروع لمحتويات أجهزة الكمبيوتر.

ويلاحظ من صياغة هذا القانون ما يأتى:

- أن المشرع الانجليزى يعاقب على التآمر والشروع والتحريض.

- لا تلزم جهة الادعاء أن تقدم دليل يستفاد منه أن الأفعال المقترفة قد استهدفت بيانات أو برامج معينة.

- لم يشترط القانون المشار إليه سلفا تواجد المتهم وقت ارتكاب الجريمة ولا بيانات الحاسب الآلى المستهدفة فى بريطانيا.

وتنص المادة ١٦ من نفس القانون على أنه " يعاقب كل من حصل بطريق غير مشروع وبأى وسيلة خداع سواء لنفسه أو للغير على منفعة مالية"[٣].

ب- التشريع الاسترالى

تبنت غالبية الولايات فى استراليا تفسيرا واسعا لمفهوم السرقة مستوحى من القانون الانجليزى. ويبدو ذلك واضحا فى قضية حيث أدانت إحدى المحاكم الاسترالية شخصا بجريمة السرقة

---

(١) راجع فى ذلك:

Rapport de Mr. Andre au nom de la commission delois constitu- tiannelles de LA legistation et de l" administration generale de la republique sur la Proposition de m.Godfrain relative a la fraude informatique no. 744.P. 13. DOC. Ass .nat(1986/87) lly aura acces Frauduleux des lorsqu on cherchera a sintrodiure indumenta dans un systeme prcetege par un disposetif de Securite.

(٢) وقد أدرج القانون بعضا لتعريفات الآتية:

- **البيانات: هى تلك المعلومات الكائنة فى صيغة قابلة للمعالجة.**
- **البيانات الشخصية: هى البيانات المتعلقة بأفراد أحياء يمكن تحديد هويتهم.**
- **الأشخاص المسند إليهم العمل فى مجال البيانات: هم الأفراد المعينون بها.**

(٣) انظر فى ذلك:

M. BRAIT,la fraude informatiqu.. une .Approche de droit compare REV. dr.pen.cirm.p.290.

لاحتياله على مدير إحدى البنوك فى سيدنى حيث أنه تلاعب فى برامج الحاسب الآلى كى تبدو الاعتمادات المالية فى صالحه[1]. ويختص قسم جرائم الكمبيوتر التابع للبوليس الفيدرالى الاسترالى والذى تكون عام ١٩٨٩ بمهمتين رئيسيتين – المهمة الأولى هى البحث والتقصى وجمع المعلومات الاستخباراتية عن جرائم محددة من جرائم الكمبيوتر بينما المهمة الثانية هى توفير الدعم الفنى لوحدات البحث والتحقيق السرى المنهمكة فى التحقيق فى الجرائم المتصلة بالكمبيوتر أو التى تعتمد عليه فى ارتكابها. والتشريع الذى يحدد مسئولية البوليس الفيدرالى الاسترالى بشأن جرائم الكمبيوتر المحددة يوجد فى قانون العقوبات لدول بالكومنولث والصادر عام ١٩١٤ (الجزء٦أ) والذى يشمل الأقسام من ٧٦ أ إلى ٧٦ف. هذه الأقسام المتعلقة بالأفعال الإجرامية تشمل قائمة بالظروف والملابسات التى تشكل فعلا إجراميا ودرجة العقوبة المحتملة المرتبطة بهذه الأفعال. وقد تم وضع هذا التشريع فى يوليو ١٩٨٩ وتم تعديله فى ١٩٩١. ولدى البوليس الفيدرالى الاسترالى الحق السيادى لتطبيق هذا التشريع فى أحد موقفين:

الموقف الأول: كان الكومنولث يتمتع بالسلطة والحق فى تطبيق هذا التشريع حينما كان الفعل الإجرامي موجها نحو الكمبيوتر التابع للكومنولث، أو أحد أجهزة الكمبيوتر التى تحتوى على بيانات أو معطيات لصالح الكومنولث. والإشارة إلى البيانات أو المعطيات التى تم تخزينها فى الكمبيوتر لصالح الكومنولث تشمل الوضع حينما يتم تخزين هذه البيانات والمعلومات بناء على توجيه أو طلب من الكومنولث.

الموقف الثانى: فيمكن تطبيق هذا التشريع حينما يكون الفعل الاجرامى موجها ضد أى كمبيوتر بواسطة أى تسهيل يتم تشغيله أو توفيره بمعرفة الكومنولث أو بمعرفة أى طرف وسيط، وتعريف الوسيط أمر واسع النطاق وهو يشمل كافة المنظمات، التى تقوم بتزويد هذه الخدمة بموجب ترخيص ممنوح طبقا لقانون الاتصالات عن بعد الصادر عام ١٩٩١.

ج- التشريع الكندى

استحدث قانون العقوبات الكندى [2] المادة ٣٠١ فقرة ٢ والتى تنص على:

أ- كل من حصل بطريق الغش وبدون وجه حق مباشرة أو بطريق غير مباشر على خدمات من حاسب آلى.

ب- كل من ولج بنية الغش، بواسطة جهاز الكتروني أو صوتى أو آلى مباشرة أو بطريق غير مباشر فى حاسب آلى.

---

(١) راجع فى ذلك:

m. Briat ,la fraude informatique ,art prec .p.291.

(٢) راجع فى ذلك:

Vivant et le stanc, lamy informatique no.2489.

جـ كل من استعمل حاسب آلى مباشرة أو بطريق غير مباشر بغرض ارتكاب جريمة منصوص عليها فى الفقرة أ،ب أو جريمة منصوص عليها فى المادة ٣٨٧ خاصة ببيانات أو حاسب آلى يعد مرتكبا لفعل إجرامى ويعاقب بالحبس لمدة عشر سنوات.

وتنص المادة ٣٨٧ يعد مرتكبا لعمل آثم كل من باشر عمداً:

أ- إتلاف أو تعديل البيانات.

ب- سرقة البيانات أو جعلها غير صالحة أو عديمة الفائدة.

جـ منع أو إعاقة الاستخدام المشروع للبيانات.

د- منع أو إعاقة شخص فى استخدام حقه المشروع للبيانات أو رفض ولوج شخص له الحق فى البيانات.

<u>د- التشريع الأمريكى</u>

يطبق فى الولايات المتحدة الأمريكية القوانين الخاصة بالغش فى مجال البنوك والبريد والتلغراف والاتفاق ألأجرامي لأغراض ارتكاب الغش على جرائم سرقة المعلومات. بل أن بعض الولايات الفيدرالية أصدرت قوانين بموجبها أعطت مفهوما واسعا للمال بحيث يشمل " كل شى ينطوى على قيمة" ويندرج تحت هذا التعريف الأموال المعنوية والبيانات المعالجة وتعاقب هذه القوانين على الاستخدام غير المسموح به بغرض ارتكاب أفعال الغش أو للاستيلاء على المال[1] وعلى المستوى

([1]) استحدثت الولايات الأمريكية " مثل أريزونا وكاليفورنيا وكولورادو وديلادار وفلوريدا وجورجيا والبنوى وميتشجان وميسورى ومونتانا وأوتارا ونيومكسكو...)العديد من =
= القوانين الجنائية التى تعاقب على الاستخدام غير المسموح به للحاسب الآلي بغرض الاحتيال أو الحصول على مال والمجال هنا ليس متسعا لفحص جميعها، ولذا نكتفي بإيراد ملاحظتين عليها:
أولاهما:أن آلبات التجريم فى هذه القوانين على درجة كبيرة من الاختلاف ويبدو ذلك من زاويتين:

(أ) أن جميع هذه القوانين إذا كانت تتمسك بضرورة توافر الغش أو سوء النية فى الأفعال المعاقب عليها إلا أن صيغتها فى هذا الشأن جاءت غير مطابقة وعلى سبيل المثال فقانون كاليفورنيا ينص على أن " يعاقب كل شخص ولج عن عمد أو سوء نية...." مادة ٥٠٢ من قانون عقوبات كاليفورنيا الصادر سنة ١٩٧٩ والمعدل سنة ١٩٨٢ " وقانون ديلادار" ينصان على" كل من .... وكان ذلك عن تبصر أو تروى مباشر أو بطريق غير مباشر" مادة ٥٥٨ والمعدلة فى سنة ١٩٨٢، وقانون فلوريدا ينص على " كل من باشر.... عن تروى وعلم وبدون إذن....." وقانون ١٩٧٨ سوقانون بنسلفانيا" ينص على" كل من ..... عمدا وبدون إذا " قانون سنة ١٩٨٣".

(ب) أن بعض هذه القوانين مال إلى تقنين وبشكل مختصر الأفعال المجرمة مقتديا فى ذلك بالنموذج الفيدرالى ومنها قانون كاليفورنيا والذى يعاقب " كل من ولج عمدا فى نظام أو شبكة معلوماتية بفرض محاولة أو تنفيذ أى مؤامرة أو حيلة بغرض الحصول على نقود أو خدمات " قانون العقوبات مادة ٥٠٢/ب" ويجرم هذا القانون أيضا " كل من ولج وبسوء نية فى نظام شبكة معلوماتية بغرض الحصول على معلومات غير مسموح بها تتعلق بسمعة الغير أو كل من أدخل معلومات مصطنعة بغرض تحسين أو اساءة سمعة الغير ويعاقب أخيرا كل شخص ولج بسوء نية أتلف أو محا أو أضر بأى نظام معلوماتي أو شبكة معلوماتية أو كيان منطقى أو بيانات وعلى النقيض تنبت بعض القوانين الأخرى المنهج التحليلى ومنها على سبيل المثال قانون فلوريدا والذى احتوى على ثلاث مجموعات أساسية إحداهما: مخصصة للجرائم التى تقع على البيانات الموجودة بالبرامج والثانية: خاصة بالجرائم التى تقع على المعدات والتجهيزات المعلوماتية والثالثة : خاصة بجرائم المستخدمين لنظم المعلومات، ولكل مجموعة منها قواعدها الداخلية الخاصة بها وثانيهما: تتعلق بالمنهج الانجلو سكسونى فى التعاريف القانونية حيث يلاحظ أن هذه

الفيدرالى صدر قانون الولوج المصطنع فى الحاسب الآلى فى أكتوبر سنة ١٩٨٤[1] counterfeit access device and computer

Fraud and abuse act والذى ولج عمدا فى حاسب آلى بدون إذن أو كان مسموحا بالولوج منه، واستغل الفرصة التى سنحت له عن طريق هذا الولوج لأغراض لم يشملها الإذن، وقام عمداً عن طريق هذه الوسيلة باستعمال أو تعديل أو إتلاف أو إفشاء معلومات مختزنة فى الحاسب متى كان هذا الأخير يعمل باسم ولصالح الحكومة الأمريكية، وطالما أثرت هذه الأفعال على أداء وظيفته. ويمكن لهذا النص وبطريق غير مباشر وبشروط معينة أن يشمل النصب الذى يرتكب عن طريق الحاسب الآلي،ولكن وزارة العدل الأمريكية قدمت فى أغسطس سنة ١٩٨٤[2] مشروعا بقانون يستهدف مباشرة حالة الغش المعلوماتى والذى يعاقب " كل من رتب أو صمم خطة ما أو حيلة بغرض ارتكاب غش أو الاستيلاء على مبلغ من النقود أو مال لا يخصه وولج أو حاول الولوج فى حاسب آلى بغرض تنفيذ أو محاولة تنفيذ هذه الخطة أو الحيلة أو لارتكاب أو محاولة ارتكاب مثل هذا النصب أو هذه السرقة أو الاختلاس....." ومصطلح المال property وفقا لهذا المشروع بقانون يشمل " كل الوسائل المالية والمعلومات التى تحتوى على بيانات معالجة والمكونات الالكترونية والكيانات المنطقية

التعاريف ليس لها أى قيمة خارج الولايات المتحدة بل وأيضا خارج الولاية التى تنص عليها، وفضلا عن ذلك فليس لها أى قيمة خارج النص=
= الذى يحتويها حيث أنها تعطى من أجل احتياجات النص.
راجع فى ذلك:

Vivant et le stanc, lamy droit de informatique ,no.2487.

(١) بدأت – أنفينا سيكوريتى كورب – فى بادئ الأمر وكأنها شركة انترنت نموذجية، بمكاتبها وحاسباتها وموظفيها ونظامها الأمنى الحاسوبي ولم يكن ينقصها سوى الزبائن. لكن تبين الآن أن تلك الشركة التى بدت مشروعا فاشلا للوهلة الأولى كانت شركة وهمية أنشاها مكتب التحقيقات الفيدرالية الأمريكى اف بى أى للايقاع بشابين روسيين متهمين باختراق كمبوترات شركات انترنت أمريكية واختلاس معلومات حساسة فى محاولة لابتزاز المال وتقول السلطات إن اليكسى ايفانوف ٢١ عاما وفاسيلى جورشكوف ٢٥ عاما وكليهما من مدنية شليابنسك الروسية قد ابتلعا الطعم ووقعا فى فخ الإف بى أى. وفى حين رفض مكتب التحقيقات الفيدرالية الإدلاء بأية تعليقات فإن وثائق قضائية كشف عنها النقاب مؤخراً تبدو وكأنها رواية جاسوسية يروى فيها عملاء الاف بى آي كيف تمكنوا من الإيقاع باللصين عن طريق انشاء شركة زائفة ودعوة ايفانوف وجوشكوف لمحاولة اختراق أنظمتها الحاسوبية المحصنة، وبعد أن نجح القرصانان الروسيان فى اختراق الأنظمة عن بعد وجه موظفوا شركة أنفيتا دعوة لهما للقدوم إلى سياتل فى الولايات المتحدة لمناقشة
ابرام عقد شراكة واستعراض كامل امكانياتهما فى مجا ل التسلل إلى أجهزة الكمبوتر عبر الانترنت، وبينا كان الشابان يستعرضان مهاراتهما فى الشراكة الوهمية استخدم الاف بى آي تقنية تصنت حاسوبية تبسط نشاطها عبر الانترنت وتخترق النظام الحاسوبي الخاص بالمتهمين فى روسيا.
ويقول خبراء أمن الانترنت أن القضية تعرض لمدى تطور مقدرات مكافحة جرائم الانترنت لدى مكتب التحقيقات الفيدرالية لكن الدفاع يشير الاستفهام حول مشروعية استخدام هذه الأساليب.
راجع فى ذلك: جريدة البيان – دبى – الإمارات العربية المتحدة، العدد ٧٦٣٣ تاريخ ١٢ مايو ٢٠٠١.
(٢) صدر فى الولايات المتحدة الأمريكية القانون الفيدرالى بشأن الغش والعبث المعلوماتي computer fraud & abuse act فى عام ١٩٨٤ وأدخل عليه تعديلات كان آخرها عام ١٩٩٦. ويواجه هذا القانون عدة أفعال تتصل بالدخول غير المشروع أو الحصول متجاوزا التصريح على معلومات تتعلق بالدفاع الوطنى أو العلاقات الخارجية لا يجوز الكشف عنها. ويعاقب أيضا على نقل مكونات لبرامج أو معلومات دون موافقة من صاحب الشأن فى حالة ما إذا ترتب على هذا النقل خسائر لشخص أو أكثر، ويواجه القانون أيضا مشكلة غش كلمات المرور بما يمكن مرتكبه من الدخول على نظام للكمبيوتر إذا كان من شأنه الإضرار بالتجارة بين الولايات بالتجارة الخارجية. راجع فى ذلك: د. طارق سرور، سابق الإشارة إليه ،ص٥٣.

وبرامج الحاسب الآلي سواء بلغة الآلة أو بلغة مقروءة للإنسان وكل قيمة أخرى ذات طابع مادى أو معنوى"[1].

وقد خول الكونجرس الأمريكى[2] قطاع الخدمة السرية سلطة التحقيق فى عمليات الاحتيال التى تتم عبر الشبكات والتى تعرف باسم " عمليات التحايل على وسائل الدخول للمعلومات. وذلك بموجب البند رقم ١٨ من قانون الولايات المتحدة الأمريكية القسم ١٠٢٩ ويضم القسم المذكور تعريفا عاما لمصطلح وسائل الدخول للمعلومات وهو:

" أية بطاقة أو لوحة أو رقم كودى أو رقم حساب أو أية وسيلة أخرى من وسائل الدخول على الحسابات بغرض التحصل على أموال أو بضائع أو خدمات أو أى شئ آخر ذو قيمة يمكن استخدامه كوسيلة من وسائل بدء نقل الأموال".

ومن هنا نرى أن المصطلح يمكن أن يتسع بحيث يشمل بطاقات الائتمان وأرقام حساباتها وكذا بطاقات الشحن الهاتفية وأكواد الدخول على التليفونات ويلاحظ على نص القسم ١٠٢٩ أنه وقد منح قطاع الخدمة السرية سلطة ومباشرة فى مواجهة ذلك" العالم الرقمى الخفى" دون أن يشير من قريب أو بعيد لكلمة كمبيوتر.

وتعد ماكينات الصرف الآلية – التى انتشرت فى سائر أرجاء الولايات المتحدة الأمريكية خلال حقبة الثمانينات- من بين " وسائل الدخول للمعلومات" وتعتبر أية محاولة للمسها بالضغط على لوحة مفاتيحها، أو التلاعب فى البطاقات البنكية البلاستيكية بمثابة فعل يندرج تحت طائلة العقوبات المدرجة بالتقسم ١٠٢٩. ويشتمل القسم ١٠٢٩ على بندين:

أولهما: ضرورة " تأثير الجرم على التجارة الداخلية أو الخارجية للدولة كى تقع تحت طائلة ونطاق الاختصاص الفيدرالى.

وثانيهما: فيتعلق بحجم المال، فهناك قاعدة تقضى بعدم قيام المسئولين الفيدراليين بتتبع المجرمين المتورطين فى جمع مبالغ بسيطة من المال. حيث أن الجرائم الفيدرالية يجب أن تتسم بالخطورة ويحدد القسم ١٠٢٩ الحد الأدنى للخسارة المالية التى تقع تحت طائلة القانون الفيدرالى بمبلغ ألف دولار أمريكى. وقد منح القسم ١٠٣٠ الخاص بـ" الاحتيال والأنشطة ذات الصلة المرتبطة بالكمبيوتر" منح قطاع الخدمة السرية السلطة القانونية المباشرة على كافة الأعمال المتصلة باختراق الكمبيوتر.

---

(١) راجع فى ذلك:

Mendes"m.w" la legislation penale en matiere d ordinateurs et les measures de securite aux ETATS- Unis , Droit de informatique mumero special 1985.p.41.

(٢) انظر فى ذلك:

The Hacher crackdown law and Disorder on the Electronic fron – tier by Bruce sterling p.0172,1994.

المبحث الرابع

الجوانب الإجرائية والتشريعية للضبط القانوني الدولي والوطني

حيال جرائم تقانة المعلومات

اقتناعا بالحاجة إلى تحقيق سياسة جنائية مشتركة رأت الدول الأعضاء في المجلس الأوروبي وبعد التوصيات التي تقدمت بها اللجنة الأوروبية حول مشكلات الجريمة في مجال جرائم الكمبيوتر تم توقيع الاتفاقية الأوروبية بشأن جرائم الكمبيوتر بتاريخ ٢٣/١١/ ٢٠٠١م بغرض حماية المجتمع الأوروبي من جرائم الكمبيوتر وذلك من خلال التقريب بين التشريعات القانونية الجزائية ولتمكين وسائل التحقيق الفعالة فيما يتعلق بهذه الجرائم، وفتح الباب أمام أكبر عدد ممكن من الدول لكي تصبح أطرافا في الاتفاقية لحاجة المجتمع إلى نظام سريع وفعال للتعاون الدولي ،والذي يأخذ بعين الاعتبار المتطلبات المحددة لمكافحة جرائم الكمبيوتر.

وبصفة عامة يلزم للمجتمع المعلوماتى فى مجال قانون الاجراءات الجنائية أن ينشئ قواعد قانونية حديثة بحيث تضع معلومات معينة تحت تصرف السلطة المهيمنة على التحقيق فى مجال جرائم الكمبيوتر. والسبب فى ذلك أن محترفى انتهاك شبكات الحاسبات الآلية ومرتكبى الجرائم الاقتصادية وتجار الأسلحة والمواد المخدرة يقومون بتخزين معلوماتهم فى أنظمة تقنية المعلومات وعلى نحو متطور. وتصطدم الأجهزة المكلفة بالتحقيق بهذا التكنيك لتخزين المعلومات وهى التى تسعى للحصول على أدلة الاثبات.

وتصادف الصعوبات عندما يتعلق الأمر على وجه الخصوص بتخزين بيانات بالخارج بواسطة شبكة الاتصالات البعدية[1].Telecommunication ويصعب حتى هذه اللحظة فى غالبية الأنظمة القانونية أن نحدد إلى أى مدى تكفى الأساليب التقليدية للإكراه فى قانون الإجراءات الجنائية من أجل مباشرة تحقيقات ناجحة فى مجال تقنية المعلومات . وقد اقترن بظهور تقنية المعلومات مشاكل خاصة ومستحدثة وعلى سبيل المثال التفتيش التحفظ على المعلومات

والزام الشاهد باسترجاع وكتابة المعلومات والحق فى مراقبة وتسجيل البيانات المنقولة بواسطة أنظمة الاتصالات البعدية وجمعها وتخزينها وضم المعلومات الإسمية إلى الدعوى الجنائية.

ونظرا لسهولة حركة المعلومات فى مجال أنظمة تقنية المعلومات حيث تجعل هذه السهولة لحركة المعلومات أنه بالإمكان ارتكاب جريمة عن طريق حاسب ألي موجود فى دولة معينة بينما يتحقق نتيجة هذا الفعل الاجرامى فى دولة أخرى .

---

(١) وعلاوة على ذلك فإن غالبية الاجراءات الجنائية لا تكون كافية ولا مناسبة لأغراض التحقيق والحكم في هذا النمط من أنماط الجرائم. ومؤدى ذلك فيبدو من الضروري أيجاد اجراءات لديها القدرة على الملائمة مع المتطلبات الحديثة التي تفرضها تكنولوجيا المعلومات راجع في ذلك : La criminamite informatique sur l'internet

لذا يقتضى الأمر ضرورة وجود تعاون دولى محكم فى مجال مكافحة هذا النوع من الجرائم ولأجل توفير حماية حقيقية لأنظمة الاتصالات البعدية.

على أية حال ينقسم هذا المبحث إلى مطلبين رئيسين، اختص المطلب الأول منها المعوقات التشريعية والقانونية المتعلقة بجرائم تقانة المعلومات أما المطلب الثاني فقد عكف على بيان تدابير الضبط القانوني العربي والدولي في مجال مكافحة جرائم تقانة المعلومات.

المطلب الأول

المعوقات التشريعية والقانونية

المتعلقة بجرائم تقانة المعلومات

إن أهم ما يميز جرائم نظم المعلومات صعوبة اكتشافها واثباتها وهى صعوبة يعترف بها جميع الباحثين فى هذا المجال[1]. علاوة على ما تتميز به اجراءات جمع الأدلة فى هذا المجال من ذاتية خاصة. ومن ثم يمكن التعرض لأبرز المعوقات في هذا الجانب، ثم يتم التعرض لأبرز أوجه القصور التشريعي العربي في هذا الموضوع.

أولا: المعوقات المتعلقة بجرائم الإنترنت وشبكات التواصل الإجتماعي

تنقسم المعوقات فى هذا الصدد إلى عدة أنواع نفصلها فيما يلى:

١ـ معوقات خاصة بطبيعة الجريمة وأدلتها

تتسم الجرائم التى تقع على الحاسبات وشبكات المعلومات بأنها غير مرئية فى العديد من حالاتها[2]. حيث لا يلاحظها المجنى عليه غالبا أو يدرك حتى بوقوعها .

واخفاء السلوك المكون لها وطمس أو تغطية نتائجها عن طريق التلاعب غير المرئى فى النبضات أو الذبذبات الالكترونية التى تسجل البيانات عن طريقها ليس مستحيلا فى الكثير من أحوالها بحكم توافر المعرفة والخبرة الفنية فى مجال الحاسبات لدى مرتكبها.[3]. اختلاس المال عن طريق التلاعب فى برامج الحاسب ومحتوياته، وغالبا ما يتم فى مخرجات الحاسب تغطيتة وستره. والتجسس

---

(1) انظر في ذلك :
د. محمد زكي – الاثبات في المواد الجنائية ، ص١٦ ، د.محمد محي الدين عوض ، مشكلات السياسة الجنائية المعاصرة في جرائم نظم المعلومات ، ص٣٩٨ – ٣٩٩ د. هدى حامد قشقوش ، جرائم الكمبيوتر والجرائم الأخرى في مجال تكنولوجيا المعلومات ، بحث مقدم للمؤتمر السادس للجمعية المصرية للقانون الجنائي ، القاهرة ٢٥-٢٨ أكتوبر ١٩٩٣ ، منشورات دار النهضة العربية ١٩٩٣ ، ص٤٥٠ و٤٧٦ و٥٧٦. د. زكي أمين حسونة ،جرائم الكمبيوتر والجرائم الأخرى في مجال التكتيك المعلوماتي – بحث مقدم للمؤتمر السادس للجمعية المصرية للقانون الجنائي القاهرة، ٢٥-٢٨ أكتوبر ١٩٩٣ ، العقيد علاء الدين محمد شحاته – رؤية أمنية للجرائم الناشئة عن استخدام الحاسب الآلي – بحث مقدم للمؤتمر السادس للجمعية المصرية للقانون الجنائي – القاهرة ٢٥-٢٨ أكتوبر ١٩٩٣.

(2) إذ تقع هذه النوعية من الجرائم في بيئة لا تعتمد التعاملات فيها أصلا على الوثائق والمستندات المكتوبة بل على نبضات اليكترونية غير مرئية لا يمكن قرائتها إلا بواسطة الحاسب الآلي والبيانات التي يمكن استخدامها كادلة ضد الفاعل يمكن في أقل من الثانية العبث به أو محوها بالكامل لذا فإن للمصادفة وسوء الحظ دورا في اكتشافها يفوق دور اساليب التدقيق والرقابة ومعظم مرتكبيها اللذين تم ضبطهم وفقا لما لاحظه أحد الخبراء، إما أنهم قد تصروفوا بغباء أو أنهم لم يستخدموا الأنظمة المعلوماتية بمهارة : انظر :
John Eaton and Jermy smithers, this is it. Amangagrs Guide to information technology , London, Philip Allan , 1982p.263
مشار إليه د. هشام محمد فريد رستم، بحث مقدم إلى مؤتمر القانون والكمبيوتر والانترنت في الفترة من ١-٣ مايو ٢٠٠٠ بجامعة الإمارات العربية المتحدة بعنوان الجرائم المعلوماتية).

(3) انظر في ذلك :
Jay , J. Becker the Trial of computer crime (1980), 2 computer Law , Journal 441
مشار إليه الدكتور هشام محمد فريد رستم ، سابق الإشارة إليه.

على ملف البيانات كان خطأ مصدره البرامج أو الأجهزة أو نظام التشغيل أو التصميم الكلى للنظام المعلوماتى.

ونتيجة لهذه الصعوبة أصبح لإمكانية أخفاء الجريمة المعلوماتية عن طريق التلاعب فى البيانات مصطلحا يستخدم فى أبحاث علم الاجرام الأمريكية وهو (الطبيعة غير الأولية لمخرجات الحاسب المطبوعة)[1] Second-hand Nature computer printouts.

٢ـ معوقات خاصة بأدلة الجريمة

تتمثل أهم المعوقات المرتبطة بأدلة جرائم الإنترنت وشبكات التواصل الإجتماعي كما يلي:

(أ) انعدام الدليل المرئى

يلاحظ أن ما ينتج عن نظم المعلومات من أدلة عن الجرائم التى تقع عليها أو بواسطتها ما هى إلا بيانات غير مرئية لا نفصح عن شخصية معينة وهذه البيانات مسجلة الكترونيا بكثافة بالغة وبصورة مرمزة[1]. غالبا على دعائم أو وسائط للتخزين ضوئية كانت أو ممغنطة لا يمكن للإنسان قراءتها وإن كانت قابلة للقراءة من قبل الآلة نفسها ولا يترك التعديل أو التلاعب فيها أى أثر مما يقطع أى صلة بين المجرم وجريمته ويعوق أو يحول دون كشف شخصيته[2].وكشف وتجميع أدلة بهذا الشكل لإثبات وقوع الجريمة والتعرف على مرتكبيها هو أحد أبرز المشاكل التى يمكن أن تواجه جهات التحرى والملاحقة. وتبدو هذه المشكلة بشكل عام فى سائر مجالات التخزين والمعالجة الآلية للبيانات حيث تنتفى غالبا قدرة ممثلى الجهات المختصة على أن يتولوا بطريقة مباشرة فحص واختبار البيانات المشتبه فيها وتزداد جسامة هذه المشكلة بوجه خاص فى حالة التلاعب فى برامج الحاسب نظرا لتطلب الفحص الكامل للبرنامج واكتشاف التعليمات غير المشروعة المخفية داخله قدرا كبيرا من الوقت والعمل،وغالبا ما لا يكون له من حيث التكلفة الاقتصادية مبررا[3].

([1]) Les dificultes techniques sont liees aux methoded de cryptologie employees sur le reseua .
La criminamite informatique sur linternet , p. 58

([2]) انظر في ذلك :

Ulrich , sieber, ibid, p. 140

([3]) وتدليلا على تأثير غياب الدليل المرئي في إعاقة اجراءات الضبط وملاحقة مرتكبي الجرائم التي تقع في مجال تكنولوجيا المعلومات يشير الأستاذ sieber إلى حالة واقعية شهدتها المانيا الاتحادية سابقا عام ١٩٧١ تلخص وقائعها في اكتشاف شركة طلبياتها بريدية mail order firm سرقة أشرطة ممغنطة تخصها تحتوي ٣٠٠٠٠٠ عنوانا لعملائها وتمكنها من استصدار أمر من المحكمة . معروف باسم وقف الأعمال injuction باستعادة كل العناوين من شركة منافسة كانت قد حصلت على هذه العناوين من مرتكبي السرقة ، وتنفيذا لهذاالأمر سمحت الشركة المنافسة لمساعدة مأمور التنفيذ بدخول مقرها ومركز الحاسب الخاص بها، حيث وجد نفسه أمام كم هائل من الأشرطة والاقراص الممغنطة التي لا يدري عنها شيئا أو يعرف محتوياتها أو لديه القدرة على فحصها ومعرفة مضمونها، مما اضطر إلى مغادرة مركز حاسب الشركة المنافسة خالي الوفاض ومع أن الشركة المناسبة قامت من تلقاء نفسها بعد ذلك بعدة أيام بتسليم بيانات العناوين إلى الشركة المجني عليه إلا أنه من الوارد بالتأكيد – أن تكون الاشرطة المعنية قد تم استنساخها قبل تسليمها ، وهو ما يكون قد افقد امر المحكمة جدواها. راجع

٣١- Lister, Martin. Dovey, Jon. Giddings, Seth. Grant, Iain. Kelly, Kieran. (January 29, 2009) New Media: A Critical Introduction, USA/UK Europe : Routledge; 2 edition.

(ب) سهولة محو الدليل أو تدميره فى فترة زمنية يسيرة

من الصعوبات التى يمكن أن تعترض عملية الاثبات فى مجال جرائم نظم المعلومات سهولة محو الجانى أو تدميره لأدلة الإدانة فى فترة زمنية وجيزة فضلا عن سهولة تنصله من هذا العمل بإرجاعه إلى خطأ فى نظام الحاسب أو الشبكة أو فى الأجهزة ومن الأمثلة الواقعية قيام أحد مهربى الأسلحة بإدخال تعديلات على الأوامر العادية لنظام تشغيل حاسب صغير يستخدمه فى تخزين عناوين عملائه والمتعاملين معه بحيث يترتب على إدخال أمر إلى الحاسب من خلال لوحة مفاتيحه بالنسخ أو الطبع أو تدمير البانات كلها.

ومع أن تعديل برمجة نظام تشغيل الحاسب كان قد أجرى خصيصا بواسطة الفاعل للحيلولة دون نجاح أجهزة الملاحقة فى اجراءات المتوقعة للبحث عن الأدلة وضبطها إلا أنه لم يفلح فى تحقيق هذا الهدف نتيجة لتوقع المتخصصين لمعالجة البيانات بالجهاز المركزى لمكافحة الغش المعلوماتى بالنمسا بأن شئ ما فى نظام تشغيل حاسب الفاعل قد جرى تغييره وقيامهم بناءا على ذلك باستنساخ الأقراص الممغنطة المضبوطة عن طريق أنظمة حاسباتهم[1].

وفى حالة أخرى شهدتها المانيا الاتحادية سابقا أدخل الجناة فى نظام الحاسب تعليمات أمنية لحماية البيانات المخزنة داخله من المحاولات الرامية إلى الوصول إليها ومن شأنها محو هذه البيانات بالكامل بواسطة مجال مهربائى وذلك إذا ما تم اختراقه من قبل شخص غير مرخص له[2].

(جـ) صعوبة الوصول إلى الدليل

تحاط البيانات المخزنة الكترونيا أو المنقولة عبر شبكات الاتصال بجدار من الحماية الفنية لإعاقة محاولة الوصول غير المشروعة إليها للاطلاع عليها أو استنساخها[3].. كذلك يمكن للمجرم المعلوماتى أن يزيد من صعوبة عملية التفتيش التى قد تباشر للحصول على الأدلة التى تدينه عن طريق مجموعة من التدابير الأمنية كاستخدام كلمة السر للوصول إليها أو دس تعليمات خفية بينها أو ترميزها لإعاقة أو منع الاطلاع عليها أو ضبطها . لذا فأن استخدام تقنيات التشفير لهذا الغرض يعد إحدى العقبات الكبرى التى تعوق رقابة البيانات المخزنة أو المنقولة عبر حدود الدولة والتى تقلل من قدرة جهات التحرى والتحقيق والملاحقة على الاطلاع عليها الأمر الذى يجعل حماية حرمة البيانات

---

(1) راجع في ذلك : د. هشام محمد فريد رستم ، مرجع سابق، ص٣٥-٣٦

(2) راجع في ذلك :

Ulrich sieber, ibid, p. 141

(3) تواجه عملية جمع الأدلة الاليكترونية واستعمالها بعض التحديات الرئيسية major challenges ومنها :

- **صعوبة الوصول إلى الملفات المحذوفة أو المخبأة أو المحمية بموجب كلمات مرور داخل النظم الضخمة المرتبطة من خلال الشبكات.**
- **صعوبة استعادة البيانات من بعض الوسائل أو الوسائط القديمة.**
- **صعوبة العثور على الملفات او السجلات المحورية من بين المجالات الشاسعة للبيانات (مثال : سجلات البريد الالكتروني)**
- **صعوبة تحليل صحة الملفات – ومعرفة ما إذا كان قد تم تعديلها او محوها :**

راجع في ذلك :

Linda volonino ph. D.ibid., p.14

الشخصية المخزنة فى مراكز الحاسبات والشبكات أو المتعلقة بالأسرار التجارية العادية والالكترونية أو بتدابير الأمن والدفاع أمر بالغ الصعوبة[١].

وتصطدم عقبة الوصول إلى الدليل المعلوماتى بمشكلة اجرائية تتعلق بمدى سريان القيود الخاصة بضبط الأوراق على ضبط محتوى نظام المعالجة الآلية للبيانات والمحمى فنيا فى مواجهة الاطلاع غير المسموح به حيث يحظر قانون الاجراءات الجنائية المصرية والإماراتى بمقتضى المادتين ٥٢، ٥٨ على التوالى [٢]. اطلاع مأمور الضبط القضائي على الأوراق المختومة أو المغلقة[٣]. الموجودة فى منزل المتهم أثناء تفتيشه[٤].وعلة ذلك الحفاظ على الآثار التى تتضمنها الأوراق وهنا يثور تساؤل عما إذا كان حكم هاتين المادتين واجب الإتباع بالنسبة لإطلاع مأمور الضبط القضائى على محتوى نظام المعالجة الآلية للبيانات من عدمه وذلك فى حالة ما إذا كان محاطا بجدار من الحماية الفنية تعوق الاطلاع عليه. ونبادر بالإيجاب على هذا التساؤل استنادا إلى سببين:

الأول: أن السبب الذى من أجله تم تقرير هذا الحكم بالنسبة للأوراق المختومة أو المغلقة يتوافر أيضا بالنسبة لمحتوى نظام المعالجة الآلية للبيانات المحمى فنيا ضد الإطلاع غير المسموح به. فحظر المشرع اطلاع مأمور الضبط القضائى على هذه الأوراق نما هو لمظنة أن الغلق أو التغليف يضفى عليها مزيدا من السرية ويفصح عن رغبة صاحبها فى عدم اطلاع الغير على مضمونها بغير إذنه وهو ما يتحقق فى البيانات المخزنة أو المنقولة عبر نظام أو شبكة حاسب إذا كانت محمية فنيا ضد الاطلاع غير المسموح به . فمحتوى النظام لا يكون بذلك مكشوفا بل محجوبا عن الغير حيث لا يتاح الوصول والاطلاع عليه بغير معرفة طريق ومفاتيح وكود التشغيل [٥].

الثانى:أن المادة ٥٢ اجراءات مصرى (٥٨ اجراءات اماراتى) تضع قاعدة عامة لضمان الأسرار التى تحتويها سائر وسائط وأوعية حفظ وتخزين ونقل المعلومات سواء ما كان منها تقليديا كالأوراق أو مستحدثا كالأقراص المرنة والأشرطة الممغنطة والذكرات الداخلية للحاسبات وشبكات المعلومات المحلية والإقليمية والعالمية.

---

(١) انظر في ذلك :
يشير الأستاذ sieber بأن مشاكل عديدة لا يستهان بها قد نجمت من استخدام الجناة في بعض الجرائم المعلوماتية التي وقعت بالمانيا الاتحادية سابقا لتقنيات التشفير أو الترميز لإعاقة اكتشاف أو الوصول إلى أدلة تدينهم وبوجه خاص في مجال وسائل التخزين التي يكون صعبها ضبطها.
راجع في ذلك : Ulrich Sieber Ibid, p. 141

(٢) تنص المادة الأولى منهما على أنه " إذا وجدت في منزل المتهم أوراق مختومة أو مغلقة بأية طريقة فلا تجوز لمأمور الضبط القضائي أن يفضها ، وبذات الصياغة تقريبا يسري نص المادة ٥٨ أ.ج. إماراتي .

(٣) فإذا كانت ظاهرا أن التغليف لا ينطوي وإنما يحوي جسما صلبا، فإنه يجوز لمأمور الضبط القضائي فض الغلاف لفحص محتوياته نقض مصري ٢٤ يونية ١٩٥٨ ، مجموعة أحكام النقض س٩ رقم ١٨٠ ص٧١٦.

(٤) قضى في مصر بعدم دستورية المادة ٤٧ من قانون الإجراءات الجنائية المصري في ٢ يونيه ١٩٨٤ ومن ثم لم يعد هناك مجال لتطبيق نص المادة ٥٢ من هذا القانون في حالة التلبس بالجريمة.

(٥) راجع في ذلك :
د. هشام محمد فريد رستم، سابق الإشارة إليه ص٣٤.

والجدير بالإشارة إليه أن كلا من التشريعين الإجرائيين المصرى والاماراتى لا ينفردا بهذه النتيجة بل يشاركهما فيها العديد من القوانين ومنها على سبيل المثال قانون الاجراءات الجنائية الالمانى ، فطبقا للمادة ١١٠ منه تقتصر سلطة الاطلاع على مخرجات الحاسب وغيرها من دعائم البيانات على المدعى العام وحده ، ولا يكون لضباط الشرطة حق الاطلاع على البيانات عن طريق تشغيل البرامج أو الاطلاع على ملفات البيانات المخزنة داخل الحاسب بغير إذن من له حق التصرف فيها ، ومالهم قانونا هو فحص دعائم البيانات عن طريق النظر فحسب دون استخدام مساعدات فنية[١].

(د) افتقاد الآثار المؤدية إلى الدليل

يحدث فى بعض الأحيان إدخال البيانات مباشرة فى نظام الحاسب دون تطلب وجود وثائق معاونة (وثائق خاصة بالإدخال) كما هو الحال فى بعض نظم العمليات المباشرة التى تقوم على استبدال الإذن الكتابى لإدخال البيانات بإجراءات أخرى تعتمد على ضوابط للإذن متضمنة فى برنامج الحاسب (مثل المصادقة على الحد الأقصى للإئتمان وفى مجال العمليات المالية قد يباشر الحاسب بعض العمليات المحاسبية بغير الحاجة إلى ادخال كما هو الحال لإحتساب الفائدة على الإيداعات البنكية وقيدها آليا بأرصدة حسابات العملاء على أساس الشروط المتفق عليها مسبقا والموجوة فى برنامج الحاسب.

ويكون من السهل فى كل من هذين النوعين من العمليات ارتكاب بعض أنواع من الجرائم كاختلاس المال والتزوير بإدخال بيانات غير معتمدة فى نظام الحاسب أو تعديل برامجه أو البيانات المخزنة داخله دون أن يترتب على ذلك أى أثر يشير ألى حدوث هذا الادخال أو التعديل . لذا يتعين على المحقق إزاء صعوبة الوصول إلى مرتكبى الجرائم فى كلا هذين النوعين من العمليات وعدم ترك التغيرات فى البرامج أو البيانات آثار كتلك التى يخلفها التزوير المادى فى المحررات التقليدية[٢]. أن يسعى لتحديد دائرة الأشخاص القائمين أو المتصلين فى عمليات ادخال ومعالجة البيانات وغيرها من عمليات التسجيل[٣]. مع الاستفادة من ضوابط الرقابة التى تباشر فى النظام المعلوماتى على الإدخال والمعالجة اضافة إلى تتبع الأموال المختلفة إن وجدت باعتبارها محصلة الجريمة التى يستولى عليها المجرم فى نهاية الأمر[٤].

٣- المعوقات الخاصة بالعامل البشرى

ويتعدد هذا النوع من المعوقات على النحو التالى:

---

(١) انظر في ذلك :
Manfred Mothren schlager, computer crimes and other crimes against information technology in Bermany , rev, inter, D.P. leret 2e trimesters 1993,p.351

(٢) راجع في ذلك :
Jack Bologena corporate faraud : the Basice of prevention and detection , Butterworth publishers 1984,p.75

(٣) راجع في ذلك :
J.Tappolet , La fracuc infromatieque, rev, int , crim poltech 1988,p.351

(٤) راجع في ذلك : د. هشام محمد فريد رستم ، سابق الإشارة إليه ص٣١.

أ- مكان ارتكاب الجريمة

يتم ارتكاب جريمة الحاسب الآلى عادة عن بعد حيث لا يتواجد الفاعل على مسرح الجريمة ومن ثم تتباعد المسافات بين الفعل (من خلال حاسب الفاعل) و النتيجة (المعطيات محل الاعتداء) وهذه المسافات لا تقف عند حدود الدولة بل قد تمتد إلى النطاق الإقليمى لدول أخرى مما يضاعف صعوبة كشفها أو ملاحقتها[1]. فقد أعلنت السلطات البريطانية أن أكثر من عشرة ألاف اسطوانة تعليمية عن الإيدز قد أدخلت إلى المستشفيات فى كل من بريطانيا والسويد والدنمارك والنرويج.

وقد اكتشفت أجهزة البيانات أنها مصابة بفبروس "نورجان " وهو فيروس يؤدى إلى تخريب أجهزة الكمبيوتر الشخصى واتلاف البرامج التى تعمل عليع وفى غضون ذلك. بدأت شرطة سكوتلانديارد تحقيقات واسعة النطاق فى هذه القضية باعتبارها جريمة تخريب وقد أثبتت التحقيقات مايلى:

(أ) أن هذه الاسطوانة وصلت إلى الأشخاص بالبريد من مصادر مختلفة بهدف تخريب البرامج المرسلة إليهم وأن أسماء الذين وجهت لهم الاسطوانات يبلغ عددهم نحو سبعة آلاف شخص قد تم بيعها إلى شركة تدعى " كيتيما " وهى مؤسسة تخص رجل أعمال كينى " يدعى كيتيما " وقد اتضح أن قائمة الأسماء التى أحضرت معه خلال زيارته لبريطانيا فى الفترة من ٣١ أكتوبر حتى ٣٠ نوفمبر ١٩٨٩ ولكنه لم يستدل له على عنوان.

(ب) أن عددا من هذه الاسطوانات ظهرت فى كاليفونيا وفى بلجيكا وزيمبابوى.

(ج) الرسائل أرسلت مع رسائل معنوية بـ "معلومات عن الإيدز " لكن تبين أنها تحتوى على فيروس نورجان الذى يهاجم أجهزة الحاسب الشخصى من نوع I . B . M والمتوافقة معه.

(د) تسأل الرسالة المرفقة مع الاسطوانة عن رسوم ملكية للبرنامج بمقدار ١٨٩ دولار أو ٣٧٨ دولارا حسب الطلب وإرسال الرد إلى عنوان فى بنما ولكن تبين أن معظم الرسائل أرسلت من لندن وبالتحرى تبين عدم وجود شركة بهذا الاسم ولا يوجد لها صندوق بريد فى بنما . بينما تبين أن مرسل الرسالة استخدام الاسم الأول من إحدى شركات البرامج الأمريكية العاملة فى بنما والتى أكدت عدم مسئوليتها عما حدث.

(و) تحذر الرسالة من أنه فى حالة عدم دفع الرسوم سيستخدم المرسل برنامجا لتخريب المعلومات ووقف جهاز الكمبيوتر بشكل تلقائى ولكن ما أثار الانتباه إلى هذه القضية حدث خلال تحميل الاسطوانة وفقا لما قاله "جرسيرست" خبير الفيروسات ومستشار التطبيقات البريطانى [2].

ب- نقص خبرة الشرطة وجهات لادعاء والقضاء

([1]) راجع في ذلك : د. أسامة محمد محي الدين عوض، جرائم الكمبيوتر والجرائم الأخرى في مجال تكنولوجيا المعلومات ، بحث مقدم للمؤتمر السادس للجمعية المصرية للقانون الجنائي، القاهرة ٢٥-٢٨ أكتوبر ١٩٩٣.

([2]) راجع في ذلك :

د. أسامة محمد محي الدين عوض ، سابق الإشارة غليه ، ص٤٣٠ -٤٣١

يتطلب كشف جرائم الكمبيوتر والوصول إلى مرتكبيها وملاحقتهم قضائيا استراتيجيات خاصة تتعلق بإكسابهم مهارات خاصة وعلى نحو يساعدهم على مواجهة تقنيات الحاسب الآلى المتطورة وتقنيات التلاعب به،حيث تنعقد وتتنوع التقنيات المرتبة بوسائل ارتكابها[١].

لذا يجب استخدام أساليب وتقنيات تحقيق جديدة ومبتكرة لتحديد نوعية الجريمة المرتكبة وشخصية مرتكبها وكيفية ارتكابها مع الاستعانة بوسائل جديدة أيضا لضبط الجانى والحصول على أدلة ادانته. إذ من المتصور أن يجد مأمورى الضبط القضائى أنفسهم غير قادرين على التعامل بالوسائل الاستدلالية والاجراءات التقليدية مع هذه النوعة من الجرائم [٢]. ومما يزيد من صعوبة هذا الأمر افتقار أنظمة الحاسبات وشبكات المعلومات فى البدايات الأولى لاستخدامها لأساليب الرقابة وضوابط التدقيق والمراجعة على العمليات والتطبيقات وعدم تزويدها بوسائل فنية لاكتشاف وتتبع مسار العمليات[٣] ، فضلا عن ما تصادفه هذه الجهات من صعوبات فى التحرى عن جرائم الحاسب عابرة الحدود لا سيما بعد انتشار استخدام شبكة المعلومات العالمية .

وكثيرا ما تفشل أجهزة الشرطة فى تقدير أهمية الجريمة المعلوماتية نظرا لنقص الخبرة والتدريب[٤]. وللسبب ذاته أيضا كثيرا ما تفشل جهات التحقيق فى جمع أدله جرائم الحاسب الآلى مثل مخرجات الحاسب وقوائم التشغيل ، بل أن المحقق كما هو الحال أحيانا فى بعض الجرائم الأخرى قد يدمر الدليل

---

(١)انظر في ذلك :

Donn, B., Parkar, vulnerabilities of EFT systm to intentionally causes losses in computers and Banking electronic funds transfer system and public poliecy edited by Kent w.colton and Keneth L. Kraemer, plenum press 1980,p. 97

(٢) جاء بتوصية المجلس الأوروبي رقم (٩٥) ١٣ في ١١ سبتمبر ١٩٩٥ في شأن مشاكل الاجراءات الجنائية المتعلقة بتكنولوجيا المعلومات ضرورة تشكيل وحدات خاصة لمكافحة جرائم الحاسب وإعداد برامج خاصة لتأهيل العاملين في مجال العدالة الجنائية لتطوير معلوماتهم في مجال تكنولوجيا المعلومات.

(٣) راجع في ذلك :

Bernard P. zajac Jr. police responses to computer crime in the united states the computer law and security report July – auyg 1985,pp.16-17

(٤) لقد علمت أن شابا طلب نسخة اسطوانة كمبيوتر وقام بتصوير البطاقة الملصقة عليها ثم قام بوضع الاسطوانة على السطح الزجاجي لآلة التصوير إلا أن الاستاتيكية التي نشأت عندما عملة الآلة أدت إلى مسح وإمالة كافة المعلومات المسجلة على الاسطوانة وهناك حالة أخرى حيث قام رجال الشرطة بوضع حقيبة كاملة تحتوي علىاسطوانات الكمبيوتر المصادرة وذلك في صندوق السيارة بالقرب من جهاز الإرسال والاستقبال اللاسلكي فكانت النتيجة أن الإشارات الكهربائية القوية تسبب في تدميرها جميعا.

انظر في ذلك :

Burici sterling ibid, p. 208

وصرح مكتب التحقيقات الفيدرالي بأن خبارته لم يتمكنوا من تحديد ما إذا كان الحدث قد وقع بسبب عطل فني أو هجوم ماكر وقد حجب الموقع الخاص بشركة السمسمرة الوطنية والذي يرتاده ٢٠٠ ألف عميل لمدة تفوق الساعة – حاول خلالها مهندسوا الشركة الدفاع عن النظام ضد ما رأوا أنه هجوم . فقد لاحظوا مسئولوا الشركة أن الموقع كان يعمل ببطء شديد عند افتتاح السوق وهو الأمر الذي أدى إلى انخفاض إمكانية الوصول إليه إلى ٥٠%.

راجع في ذلك

D. volоninalinu ibid, p. 6

بمحوه الاسطوانة الصلبة من خطأ منه أو أهمال أو بالتعامل مع الأقراص المرنة أو بالتعامل المتسرع أو الخاطئ مع الأدلة[١].

تكمن المشكلة فيما يقوم به رجال الشرطة حين يستخدم الكمبيوتر كأداة لارتكاب الجريمة فى المعوقات التى يمكن أن تواجه فى هذا المجال وهى:

- اما تجاهل هذا الدليل تماما.

- اما محاولة فحص هذا الدليل بدون أية مهارات فى مجال الكمبيوتر .

- اما حمل المشتبه فيه على استعادة معلومات من الكمبيوتر . ثم بعد ذلك عدم مصادرة نظام الكمبيوتر حيث أن الشهادة التى يدلى بها تصبح حرجة فى مواجهة المعلومات المستمدة من الكمبيوتر.

- واما مصادر جهازالكمبيوتر بدون معرفة ما يوجد فيه من معلومات وبالتالى زيادة الفرصة فى فقد هذه المعلومات.

ج- إحجام المجنى عليهم عن التبليغ

ويعد هذا الأمر على قدر من الصعوبة لا فى مجال اكتشاف واثبات جرائم الحاسب بل وفى دراسة هذه الظاهرة بمرمتها وهو ما يعبر عنه بالرقم الأسود[٢]. لجرائم الحاسب .

وفى هذا الشأن يحدثنا Beter swift يعتقد اتحاد الصناعة البريطانى confederation of britich «industry» أن العديد من الشركات تحرج من الاعتراف بأنها تعرضت للسلب حسب تعبيره من قبل مجرمى التقنية العالمية فبدلا من استدعاء الشرطة والاعتراف بأنهم ضحايا جرائم السرقة فإنهم يخلدون إلى الصمت[٣].

---

(١) انظر في ذلك :

Richard totta and antong hardcastle, computer related crime in information technology the law edited by chris Edwards and Nigel savage Macmillan publisher 1986,p.201

(٢) ويلاحظ في هذا الشأن أن المشرع الإمارتي جعل الإبلاغ عن الجرائم الزامي كقاعدة عامة وإلا تعرض المخالف للجزاء الجنائي، إذ أوجب لمقتضي المادة (٣٧) من قانون الإجراءات الجزائية رقم ٣٥ لسنة ١٩٩٢ ، وعلى كل من علم بوقوع جريمة مما يجوز للنيابة العامة رفع الدعوى عنها بغير شكوى أو طلب أن يبلغ النيابة العامة أو مأموري الضبط القضائي عنها ، ونص في المادة (٣٨) من القانون ذاته على أنه يجب على كل من علم من الموظفين العمومين أو المكلفين بخدمة عامة أثناء تأدية عمله أو بسبب تأديته بوقوع جريمة من الجرائم التي يجوز للنيابة العامة رفع الدعوى عنها بغير شكوى أو طلب. أن يبلغ عنها فورا النيابة العامة أو أقرب مأموري الضبط القضائي ورصد مخالفة هذاالواجب عقوبة جنائية ينصه في الفقرة الثانية من المادة (٢٧٢) من قانون العقوبات الاتحادي على " أن ... يعاقب بالغرامة كل موظف غير مكلف بالبحث عن الجرائم ا أو ضبطها أعمل أو أرجأ إبلاغ السلطة المختصة بجريمة علم بها في أثناء أو بسبب تأديته وظيفته ولا عقاب إذا كان رفع الدعوى .. معلقا على شكوى ... كما جاءت المادة (٢٧٤) من ذات القانون لتقضي بأن يعاقب بغرامة لا تجاوز ألف درهم كل من علم بوقوع جريمة وامتنع عن إبلاغ ذلك إلى السلطات المختصة، ويجوز الإعفاء من هذه العقوبة إذا كان من امتنع عن الإبلاغ زوجا لمرتكب الجريمة أو من أصوله أو فروعه أو أخوته أو اخوانه أو من هم منزلة هؤلاء نم الأقرباء بحكم المصاهرة،

(٣) انظر في ذلك :

Peter swift Hackmun – menace of the key board criminal brithish telecom world mag half of sep. 1989,p.13-14

ويلاحظ أن العديد من ضحايا جرائم الحاسب لا يقفون عن حد عدم الابلاغ عن الجريمة بل أنهم يرفضون أى تعاون مع الجهات الأمنية خشية معرفة العامة بوقوع الجريمة ويسعون بدلا من ذلك إلى محاولة تجاوز أثارها حتى لوكانت الوسيلة هى مكافأة المجرم ونذكر على سبيل المثال بنك Marchant bank city فى انجلترا لنقل ٨ مليون جنيه استرلينى من أحد أرصدته إلى رقم حساب فى سويسرا وقد تم القبض على الفاعل أثناء محاولته سحب المبلغ المذكور ولكن بدلا من أن يقوم البنك بتحريك الدعوى الجنائية ضده فقد قام بدفع مبلغ ١ مليون جنيه استرلينى له بشرط عدم اعلام الآخرين عن جريمته واخطار البنك بالألية التى نجح من خلالها باختراق نظام الأمن الخاص بحاسب البنك الرئيسى[١].

وفى دراسة أجريت عام ١٩٨٠ فى فرنسا أشارت النتائج إلى أن جرائم الحاسب التى تم الابلاغ عنها للسلطات الخاصة بلغت ١٥٪ من مجموع الجرائم وأن ادلة الادانة لم تتوافر إلا لنسبة تقدر بحوالى خمس النسبة المتقدمة أى ما يعادل حوالى ٣٪من مجموع جرائم الحاسب المرتكبة. كما تؤكد دراسة حديثة أجريت فى الولايات المتحدة الامريكية أن الرقم الأسود لجرائم الحاسب يميل إلى الارتفاع فإستنادا إلى تحليل الباحثين وفى ضوء تقارير جمعيات صانعى الحاسبات يظهر أن الرقم الأسود ما يقارب نسبة ٦٠٪ من جرائم الحاسب[٢].

<u>د- دور الخبراء فى فحص البيانات</u>

ويشكل الكم الهائل للبيانات التى يتم تداولها من خلال الأنظمة المعلوماتية أحد مصادر الصعوبات التى تعوق تحقيق الجرائم التى تقع عليها أو بواسطتها والدليل على ذلك أن طباعة كل ما يوجد على الدعامات الممغنطة لمركز حاسب متوسط الأهمية يتطلب مئات الآلاف من الصفحات والتى قد لا تثبت كلها تقريبا شيئا على الاطلاق. ويسلك المحقق غير المدرب لمواجهة هذه الصعوبة أحد سبيلين: إما حجز البيانات الالكترونية بقدر يفوق القدرة البشرية على مراجعتها أو الغاضى عن هذه البيانات كلها على أمل الحصول على اعتراف بالجريمة من المتهم[٣]. والواقع أنه بالامكان مواجهة هذة الصعوبة عن طريق أحد أمرين:

أ- الاستعانة بالخبرة الفنية لتحديد ما يجب دون سواه البحث عنه للإطلاع علية وضبطه واستعانة الجهات القائمة بالتحرى والتحقيق ، والحكم بالخبراء حين تتعامل مع الجرائم التى تقع فى مجال تكنولوجيا المعلومات تكاد تكون ضروره لاغنى عنها نظرا للطابع الفنى الخاص لأساليب ارتكابها والطبيعة المعنوية لمحل الاعتداء ونجاح هذه الجهات فى أداء رسالتها يتوقف إلى حد كبير علاوة على حسن إختيار الخبير على نجاحه فى المهمة التى عهد إليه بأدائها وموضوع هذه المهمة وان كان يمكن

---

(١) راجع في ذلك :

Peter swift Hackan , ibid , p. 3

(٢) راجع في ذلك :
يونس خليل عرب مصطفى جرائم الحاسب – دراسة مقارنة رسالة ماجستير – مقدمة إلى كلية الدراسات العليا الجامعة الأردنية ، ١٩٩٤ ، ص٧٣

(٣) راجع في ذلك : د. هشام محمد فريد رستم، مرجع سابق ، ص٣٧

للخبير نفسه أن يحدده إلا أن ذلك ليس مرغوبا فيه تجنبا لهيمنة دور الخبير على العملية الاثباتية وطغيانه على دور المحقق أو القاضى.

ب- الاستعانة بما تتيحه نظم المعالجة الآلية للبيانات من أساليب للتدقيق والفحص المنظم أو المنهجى ونظم ووسائل الإختبار والمراجعة.

٤- المعوقات الخاصة بالتنسيق الدولى فى مجال جمع الأدلة

من خصائص جرائم الإنترنت إنها جرائم عابرة للحدود الوطنية أو الإقليمية أو القارية وأن مواجهتها على نحو مؤثر يتطلب العمل من خلال محورين:

الأول : سن النصوص الجنائية الموضوعية على الصعيد الوطنى لتجريم صورها المختلفة والعقاب عليها إضافة إلى سن قواعد جنائية اجرائية تتلائم مع خصائصها وطبيعتها المميزة وثانيهما:خلق وتطوير وإنماء العمل الدولى المشترك لمواجهة هذه الظاهرة من خلال وضع حلول للمشاكل التى تحد من فاعلى مكافحتها سواء المشاكل الناجمة عن تطبيق القواعد الموضوعة أو القواعد الاجرائية عل هذا النمط المستحدث من الجرائم. وهناك عقبات عديدة تقف بمثابة حجر عثره من أجل التنسيق الدولى فى مكافحة جرائم سرقة المعلومات وأبرزها ما يلى:

١- عدم وجود مفهوم عام مشترك بين الدول حتى الآن حول نمازج النشاط المكون للجريمة المتعلقة للحاسب الآلى .

٢- عدم وجود تعريف قانونى موحد للنشاط الاجرامى المتعلق بهذا النوع من الاجرام.

٣- إختلاف مفهوم الجريمة لإختلاف التقاليد القانونية وفلسفة النظم القانونية المختلفة.

٤- انعدام التنسيق بين قوانين الاجراءات الجنائية للدول المختلفة فيما يتعلق بالتحرى والتحقيق فى الجريمة المعلماتية.

٥- تعقد المشاكل القانونية والفنية الخاصة بتفتيش نظم المعلومات خارج حدود الدولة أو ضبط معلومات مخزنة فيه أو الأمر بتسليمها.

٦- عدم وجود معاهدات للتسليم أو للتعاون الثنائى أو الجماعى بين الدول تسمح بالتعاون الدولى أو عدم كفايتها إن وجدت لمواجهة المتطلبات الخاصة للجرائم المعلوماتية وسرعة التحريات فيها[١].

---

(١) لمواجهة هذه المشكلات أو بعضها، ناشد مؤتمر الأمم المتحدة الثامن لمنع الجريمة ومعاملة المجرمين والذي عقد في هافانا عام ١٩٩٠ في قراره المتعلق بالجرائم ذات الصلة بالحاسب، الدول الأعضاء أن تكثف جهودها كي تكافح بمزيد من الفعاليات عمليات إساءة استعمال الحاسب التي تستدعي تطبيق جزاءات جنائية على الصعيد الوطني بما في ذلك النظر إذا دعت الضرورة في أ – تحديث القوانين والإجراءات الجنائية بما في ذلك اتخاذ تدابير من أجل
١- ضمان أن الجزاءات والقوانين الراهنة بشأن سلطات التحقيق وقبول الأدلة في الاجراءات لاقضائية تنطبق على نحو ملائم وإدخال تغييرات مناسبة عليها إذا دعت الضرورة لذلك .

ثانيا: أوجه القصور التشريعي بجرائم تقانة المعلومات في الدول العربية

إذا حاولنا الوقوف على أوجه القصور التشريعي في كثير من الدول العربية ؛ والتي تحول دون الملاحقة الجنائية لمرتكبي الجرائم المعلوماتية يمكننا أن نشير إلى مايلي:

(١) إن مبدأ الشرعية الجنائية يفرض عدم جواز التجريم والعقاب عند انتفاء النص. الأمر الذي يمنع مجازاة مرتكبي السلوك الضار أو الخطر على المجتمع بواسطة الحاسوب(الكمبيوتر) أو الإنترنت ؛ طالما أن المشرع الجنائي لم يقم بسن التشريعات اللازمة لإدخال هذا السلوك ضمن دائرة التجريم والعقاب. ولذا يتعين على المشرعين في سائر الدول العربية مواكبة التطورات التي حدثت في المجمعات العربية ؛ وسن التشريعات اللازمة للتصدي لظاهرة الإجرام المعلوماتي .

وهنا تجدر الإشارة إلى أن المشرع العماني كان له قصب السبق في هذا المضمار ؛ حيث نص على تجريم كثير من صور الجرائم المعلوماتية.

(٢) يعتبر مبدأ الإقليمية هو المبدأ المهيمن على تطبيق القانون الجنائي من حيث المكان، غير أن هذا المبدأ يفقد صلاحيته للتطبيق بالنسبة للجرائم المعلوماتية، التي تتجاوز حدود المكان، فجرائم الإنترنت عابرة للحدود .

(٢) انعدام وجود تصور واضح المعالم للقانون والقضاء تجاه جرائم الانترنت لكونها من الجرائم الحديثة وتلك مشكلة أكثر من كونها ظاهرة، ولانعدام وجود تقاليد بشأنها كما هو الشأن في الجرائم الأخرى، ويساعد على ذلك انعدام وجود مركزية وملكية عبر الانترنت .

(٣) رغم صدور عدد من التشريعات العربية بشأن حماية الملكية الفكرية والصناعية التي تضمنت النص على برامج الحاسب واعتبرتها من ضمن المصنفات المحمية في القانون ؛ إلا أن مكافحة الجرائم المعلوماتية في الدول العربية مازالت بلا غطاء تشريعي يحددها ويجرم كافة صورها بخلاف بعض

٢- النص على جرائم وجزاءات اجراءات تتعلق بالتحقيق والأدلة حيث تدعو الضرورة إلى ذلك للتصدي لهذا الشكل الجديد والمعقد من أشكال النشاط الإجرمي في حالة عدم وجود قوانين تنطبق على نحو ملائم. كما حث المؤتمر كذلك الدول الاعضاء على مضاعفة الأنشطة التي تبذلها على الصعيد الدولي من أجل مكافحة الجرائم المتصلة بالحاسبات بما في ذلك دخولها ، حسب الاقتضاء أطرافا في المعاهدات المتعلقة بتسليم المجرمين وتبادل المساعدات في المسائل الخاصة المرتبطة بالجرائم ذات الصلة بالحاسب وتصح القرار ذاته الدول الأعضاء بالعمل على أن تكون تشريعاتها المتعلقة بتسليم المجرمين وتبادل المساعدة في المسائل الجنائية منطبقة انطباقا كافيا على الأشكال الجدية للإجرام مثل الجرائم ذات الصلة بالحاسب وإن تتخذ خطوات محددة. حسب الاقتضاء من أجل تحقيق هذا الهدف وذلك بالإضافة إلى توصيات أخرى وقد يكون ملائمات كخطوة تعزز مسار التعاون الفعال وتكمل ما اتخذه مؤتمر الأمم المتحدة الثامن لمنع الجريمة ومعاملة المجرمين في هذا لاشأن من قرارات أن يسفر بحث مؤتمرات الأمم المتحدة لموضوع الجرائم ذات الصلة بالحاسب عن فتح آفاق جديدة للتعاوةن الدولي في هذا المضمار لا سيما فيما يتعلق بوضع أو تطوير أ – معايير دولية لأمن المعالجة الآلية للبيانات ب – تدابير ملائمة لحل مشكلات الاختصاص القضائي التي تثيرها الجرائم المعلوماتية العابرة للحدود أو ذات الطبيعة الدولية جـ - اتفاقيات دولية تنطوي على نصوص تنظم اجراءات التفتيش والضبط المباشر الواقع عبر الحدود على الأنظمة المعلوماتية المتصلة فيما بينها والأشكال الأخرى للمساعدة المتبادلة مع كفالة الحماية في الوقت نفسه لحقوق وحرياتهم وسيادة الدول.
راجع في ذلك :
د. هشام محمد فريد رستم سابق الإشارة، ص ٤٩

الاستثناءات[1].وإذا كان التشريعات العربية – فى الغالب الأعم - قاصرة في مجال ملاحقة صور السلوك الضار والخطر المتعلقة باستخدام الحاسوب (الكمبيوتر) والإنترنت ؛ فإن هذا القصور انعكس مردوده على الجانب الإجرائي المتعلق بمكافحة الإجرام المعلوماتي، فلم تصدر تشريعات جنائية إجرائية كافية لتعقب مقترفي هذا الإجرام .

(٤) تتعدد مظاهر القصور التشريعي التي يتعين أن تواجه كافة مظاهر السلوك السلبي المتعلقة بتقنية المعلومات . فالتشريعات مازالت ناقصة وقاصرة في المجالات التالية :

- **التشريعات الخاصة بالملكية الفكرية فيما يتعلق بأسماء مواقع الانترنت وعناصرها ومحتواها والنشر الإلكتروني وفي حقل التنظيم الصحفي للنشر الإلكتروني .**
- **تنظيم التجارة الإلكترونية والتشريعات الضريبية التي تغطي الميادين الخاصة بالضريبة في ميدان صناعة البرمجيات والأعمال على الانترنت والتجارة الإلكترونية .**
- **مقاييس إطلاق التقنية .**
- **القواعد التشريعية لنقل التكنولوجيا .**
- **التراخيص والاستثمار والضرائب المتعلقة بتكنولوجيا المعلومات .**
- **تنظيم حجية ومقبولية مستخرجات الحاسب .**
- **وسائل الإثبات التقنية والإثبات المدني .**
- **وتنظيم الصور الإجرامية في ميدان الحاسب والإنترنت .**
- **أنظمة الدفع النقدي الإلكتروني .**
- **تنظيم كيفي عمل مقاهي الإنترنت .**
- **البرمجيات الصناعية .**

(٥) عدم الاهتمام بالتفتيش على أجهزة الحاسوب (الكمبيوتر)، فالتشريعات العربية – في مجملها - لم تحدد قواعد خاصة للتفتيش على الحاسبات الآلية وكيفية وضبط المعلومات التي تحويها ومراقبة المعلومات أثناء انتقالها، كما أن الإجراءات الجنائية للجهات القائمة على التفتيش غير حاسمة بشأن مسألة ضبط برامج الحاسب والمعلومات الموجودة بالأجهزة وفقا للشروط الخاصة بإجراءات التفتيش العادية .

---

[1] **انظر: حسن عماد مكاوي، ليلى حسين، الاتصال ونظرياته المعاصرة، القاهرة، الدار المصرية اللبنانية، الطبعة الرابعة، أكتوبر ٢٠٠٣.**

(٦) إذا كان المحقق مهمته البحث عن الحقيقة، وإذا كان القاضي مهمته هي الفصل فيما يعرض عليه من أقضية ومنازعات، فإن عمل المحقق وعمل القاضي يحتاج إلى بيئة قانونية تساعدهما على أداء وظيفتهما .

الشيء المؤسف أن هذه البيئة القانونية إما غامضة ؛ وإما قاصرة .

ففيما يتعلق بمواطن القصور والغموض، فهى متعددة، ونستلهمها من التساؤلات الآتية:

- **هل اعتداءات الأشخاص على الأموال في البيئة الحقيقية يمكن تطبيق مفهومها على اعتداءات المجرم المعلوماتي ؟**
- **هل المعلومات بذاتها لها قيمة مالية ؟ أم هي تكون كذلك عندما تمثل أصولا أو حقوقا ؟ .**
- **كيف يمكن حماية السر التجاري أو الأسرار الشخصية وبيانات الحياة الخاصة من اعتداءات المجرم المعلوماتي أو المتطفل دون تصريح وإذن ؟ .**
- **وهل هناك معايير تحكم مقدمي خدمات الانترنت بأنواعها ؟ .**
- **ما مدى المسؤولية القانونية في حالة تحميل الملفات الموسيقية من الانترنت بغير موافقة صاحب الموقع ؟؟ .**
- **هل يعتبر النشر الإلكتروني على الانترنت من قبيل النشر الصحفي المنظم في تشريعات الصحافة والمطبوعات ؟ .**
- **وهل إبرام العقد عبر الانترنت تتوافر فيه سلامة وصحة التعبير عن الإرادة بنفس القدر الذي يوفره التعاقد الكتابي أو الشفهي في مجلس العقد العادي ؟**
- **وهل توقيع العقود والمراسلات إلكترونيا يتساوى مع توقيعها ورقيا ؟**
- **هل ما يعتد به من دفوع واحتجاجات بشأن التزامات أطراف التعاقد أو علاقات الدفع التقليدية متاح بذاته أو أقل منه أو أكثر في البيئة الرقمية ؟**
- **هل لرسائل البريد الإلكتروني حجية في الإثبات ؟ وهل لها ذات قيمة للمراسلات الورقية؟**
- **هل الانتخاب الإلكتروني هو تصويت صحيح ومقبول لمن اخترناه ممثلا لنا في عالم المكان والجغرافيا؟ .**
- **هل العلامة التجارية محمية من أن تكون اسم نطاق لطرف آخر ؟**
- **ماذا عن تصميم الموقع هل ثمة قدرة على منع الآخرين من سرقته واستخدامه؟**
- **ماذا إن تم ربط موقعك على الانترنت مع موقع لا ترغب في أن يكون بينهما رابط ؟**
- **ماذا عن فرض المحتوى على المستخدم هل يظل المستخدم عاجزا لا حول له ولا قوة أمام تدفق مواد لا يرغبها أو لا يطلبها على صندوق بريده أو خلال تصفحه المواقع التي يريدها ؟**

• هل إغلاق المواقع ذات المحتوى غير المشروع في بعض النظم والمشروع في غيرها تجاوز على ديمقراطية العالم التخيلي ؟

• متى نشأ النزاع أيا كان وصفه أو مصدره فمن هو القاضي الرقمي ؟

• ما هو القانون الذي سيحكم النزاع ؟

• ما المحكمة ومن هو المحكم ؟

• ما هي أخلاق المجتمع الرقمي وقواعد السلوك فيه هل هي ذاتها أخلاق العالم الحقيقي أم ثمة تباين في المفهوم والقيود ؟

• وهل ثمة قدرة للمستخدم أن يطالب بحقوق في مواجهة الطرف الوسيط في كل تعامل أو استخدام نتج عنه مساسا بحق من حقوقه .

• ومن هو حاكم الانترنت وما الدستور الذي يحكمه ومن هو الشرطي الذي يهرع له المستخدم إن تعرض لاعتداء سافر على حقوقه أو بياناته أو محتوى موقعه أو رسائله أو خصوصيته؟ .

• كيفية حماية برامج الحاسب .

• كيفية مقاضاة مزودي خدمة الانترنت على انقطاع الخدمة .

• مراقبة أداء الموظفين عبر البريد الإلكتروني ورسائلهم في بيئة العمل .

• مدى صحة إبرام العقد على الانترنت .

• كيفية حماية مواقع الانترنت .

• هل إرسال رسالة ممازحة عبر البريد الإلكتروني، يمكن ان تشكل جريمة جنائية ؟وهل يمكن أن ترتب مسئولية مدنية ؟

ويمكن أن نورد في هذا المقام جريمة وقعت في الإمارات بعد صدور قانون مكافحة جرائم تقنية المعلومات رقم ٢٠٠٦/٢

حيث وقعت هذه الجريمة في شهر يونيو من العام ٢٠٠٦ بدبي وقدمت النيابة العامة إثنين من المتهمين فيها للمحاكمة - وهي أول جريمة تقدم استنادا لقانون مكافحة جرائم المعلومات الإماراتى ويدان مرتكبها- واتهمت النيابة العامة بدبي المتهم الأول بأنه (توصل عن طريق الشبكة المعلوماتيه إلي الاستيلاء على مال منقول (عدد خمس تذاكر سفر)عائد لشركة سفريات وسياحة بدبي بطريقة إحتيالية وباتخاذ صفة غير صحيحة بأن تمكن من دخول موقع الشركة الإلكتروني عن طريق استخدام الرقم السري واسم المستخدم (الخاصين بالمتهم الثاني) وهو أحد موظفي الشركة وكان ذلك من شأنه خداع الشركة وحملها على تسليم تذاكر السفر .

واتهمت النيابة الثاني بأنه اشترك بالاتفاق والمساعدة مع المتهم الأول بارتكاب الجريمة المبينة في الوصف السابق فوقعت الجريمة بناء على ذلك الاتفاق والمساعدة، كما اتهمته بأنه بحكم عمله لدى

الشركة بمهنة بائع تذاكر افشى سر مهنته (الرقم السري واسم المستخدم) في غير الأحوال المصرح بها قانونا واستعمله لمصلحته الخاصة ومصلحة المتهم الأول دون إذن من صاحب الشأن.

وطلبت النيابة عقابهما بالمواد (١،١٠،٢٣،٢٥) من القانون الاتحادي رقم ٢ لسنة ٢٠٠٦ في شأن مكافحة جرائم تقنية المعلومات والمادة ٣٧٩ من قانون العقوبات الاتحادي.

وقد دافع المتهم الأول عن التهمة الموجهة له بأنه لم يكن يقصد الاحتيال وقد ردت المحكمة هذا الدفاع بأن المتهم قد اتفق مع المتهم الثاني (الموظف بالشركة الهارب) وحصل منه على الرقم السري واسم المستخدم الخاصين به، وقام في أزمنة مختلفة باستخدامها عن طريق الدخول على موقع الشركة وتمكن من الحصول على التذاكر بإعترافه، مع أنه ليس له صفة الدخول ولايحق له استخدام الرقم السري واسم المستخدم، مما يشكل فعله طريقة إحتياليه بإتخاذ صفة غير صحيحة ليتمكن من الدخول للموقع وكان من شأن ذلك خداع الشركة وحملها على تسليم تذاكر السفر المبينة بالأوراق. وقد أدانتهما المحكمة طبقا للمادة ٢١٢ من قانون الأجراءات الجزائية الإماراتى والمواد(١،١٠،٢٣،٢٥) من قانون جرائم تقنية المعلومات والمادة ٣٧٩ من قانون العقوبات وحكمت على المتهم الأول بالحبس لمدة شهرين وابعاده عن البلاد، وعلى المتهم الثاني بالحبس لمدة سنة واحدة وابعاده عن البلاد.

وقد أعملت المحكمة قواعد الارتباط المقررة في القانون بالنسبة للتهم الموجهه للمتهم الثاني وعاقبته بالعقوبة المقررة للجريمة الأشد، كما أنها طبقت أحكام المواد ٩٩ و١٠٠ من قانون العقوبات وعاملت المتهم الأول بقسط من الرأفة لظروف الدعوى وتنازل المجني عليها(الشركة).

<u>ثالثا: نحو ضرورة إنشاء محكمة إلكترونية (مصر نموذجا)</u>

بداية، يجب التأكيد على أن إدارة مكافحة جرائم الحاسبات وشبكات المعلومات بالإدارة العامة للمعلومات والتوثيق بوزارة الداخلية المصرية، إنما هى تعمل علي تطبيق القوانين المرتبطة بجرائم الإنترنت[١]، ومن الجدير بالذكر ان ساحات القضاء المصرى شهدت عشرات القضايا الناجمة عن جرائم الكترونية أغلبها قضايا متعلقة بالتشهير بالأفراد أو النصب والاحتيال، فمثلا شهد عام ٢٠٠٥، صدور أول حكم لجرائم التشهير عبر الإنترنت عندما قضت محكمة جنح مستأنف النزهة بمعاقبة الفلسطيني فيصل عدنان بالحبس لمدة ستة أشهر لإدانته بنشر صور إباحية ومعلومات خاصة عن فتاة خليجية علي شبكة الإنترنت. وقد بدأت القضية ببلاغ من الفتاة لمباحث المصنفات الفنية.

وتأتى ضمن القضايا التى لاقت اهتمام إعلاميا، قضية اقتحام الموقع الإلكتروني لمجلة روز اليوسف التي حدثت في نهاية عام ٢٠٠٥، فقد تقدمت المؤسسة ببلاغ لادارة مكافحة جرائم الحاسبات وشبكة المعلومات عن قيام مجهول باختراق موقع المجلة وتغيير المواد المنشورة، وتمكن ضباط المباحث من

---

[١] من هذه القوانين قانون العقوبات رقم ٥٨ لسنة ١٩٣٧ وقانون حماية حقوق الملكية الفكرية رقم ٨٢ لسنة ٢٠٠٢، وقانون تنظيم الاتصالات رقم ١٠ لسنة ٢٠٠٣، وقانون تنظيم التوقيع الإلكتروني رقم ١٥ لسنة ٢٠٠٤، والقانون رقم ١٢٦ لسنة ٢٠٠٨ بتعديل قانون الطفل رقم ١٢ لسنة ١٩٩٦، فضلا عن قوانين أخري – من المقرر الانتهاء منها- وتشمل قانون الجريمة الإلكترونية وإجراءاتها الجنائية، وقانون التجارة الإلكترونية، وقانون حماية البيانات الشخصية، وتأمين الفضاء الإلكتروني، ويتم اعداد وصياغة تلك القوانين من خلال تعاون وثيق بين أجهزة الدولة التشريعية والتنفيذية والفنية. ومن المؤكد أنه باكتمال صدور تلك التشريعات تكتمل منظومة مكافحة الجرائم الإلكترونية فى مصر

خلال التحليل والفحص الفني من تحديد الأرقام التعريفية التي استخدمت في عملية الاختراق وتم ضبط المتهم والجهاز المستخدم بمقر الشركة التي يعمل بها وبفحص الجهاز أمكن التوصل لادلة إثبات أنه هو الشخص الذي اخترق موقع مجلة روز اليوسف[1].

ويؤكد الكثير من رجال القانون على ضرورة إنشاء محكمة إلكترونية لسد الفجوة القانونية التي أحدثها التطور التكنولوجي الهائل في السنوات الأخيرة، فهناك جرائم ترتكب، وحرمات تنتهك، وحقوق تسلب على شبكة الإنترنت دون رقابة قانونية تذكر، والسبب في ذلك عدم وجود قانون دولي رادع يلاحق هواة الإجرام الإلكتروني، ويحاكمهم أمام محاكم دولية، إلا أن ذلك ليس من الأمور البعيدة التي يمكن أن تشق طريقها إلى التطبيق العملي في المستقبل القريب[2].

والمحكمة الالكترونية التى نتحدث عنها، تتطلب – بشكل عاجل- إصدار تشريعات متخصصة فى مجال مكافحة الجريمة الإلكترونية، فضلا عن توفير القضاة المتميزين للقيام على أعمال الفصل فى القضايا المطروحة على هذه المحاكم، على أن يتم تنظيم الدورات اللازمة لتأهيل القاضى الإلكترونى وتمكينه من ملاحقة التقدم الكبير فى مجال الجرائم الألكترونية.

إن الانتشار الكبير للإنترنت في الحياة العملية، أظهر الحاجة في وضع الحلول القانونية للمشاكل الناتجة عن استخدام الإنترنت في ضوء القواعد العامة للقانون إضافة إلى أهمية توجيه نظر المشرع للتدخل لوضع قواعد خاصة لتنظيم استخدام الإنترنت في بعض المجالات الحيوية، كما أن عليه وضع بعض النقاط صوب عينيه في تشريع قانون حماية المعلومات وهي الحماية المدنية لمواقع الإنترنت والإثبات والضوابط الشرعية لاستخدام الإنترنت والتقنية والجريمة المنظمة وتفعيل قانون العقوبات.

وإذا كانت هناك جرائم ذات طابع اقتصادي أو سياسي تلقى اهتمامًا واسعًا من المؤسسات المعنية بمكافحة جرائم الإنترنت، فإن الجرائم الأخلاقية على الإنترنت والتي يقوم بها أكبر مسوقي تجارة الجنس في العالم، كثيرًا ما تصطدم بعوائق تشريعية. ففي مصر مثلاً قامت شرطة الآداب بمراقبة ١٠ آلاف شاذ من المتغربين يعلنون عن عناوينهم على الإنترنت ويبدون استعدادهم لممارسة الفجور، لكن الشرطة لم تستطع إحالتهم إلى المحاكم لأنها لم تستطع إصدار إذن من النيابة لمعاقبتهم؛ لأنهم يمارسون فعلتهم الشنعاء من مواقع خاصة. أما تنظيم الشواذ الذي ألقي عليه القبض بالفعل فقد تجاوزوا الدعوة والتعارف على الإنترنت إلى الالتقاء الفعلي وهو ما مكّن الشرطة من إحالتهم إلى القضاء.

---

[1] - http://www.ng3awya.com/topic29076.html
[2] - http://www.moheet.com/show_news.aspx?nid=111727&pg=38

المطلب الثاني

تدابير الضبط القانوني العربي والدولي

في مجال مكافحة جرائم تقانة المعلومات

أصبح لكل شخص يعيش في المجتمع الحق بالاتصال بغيره وتبادل المنافع المعنوية والمادية معه ليس فقط داخل دولته بل كذلك خارجها مع أبناء الدول الأخرى . وإذا كانت الدول قد استطاعت الحد من ذلك الاتصال والتبادل في أوقات مضت تحت ستار حماية متطلبات أمنها القومي والاقتصادي إذ أنها لم تعد كذلك في ظل عصر السماوات المفتوحة بفعل تقدم وسائل الاتصال عبر الأقمار الصناعية [١] ووسائط نقل الأخبار المعلوماتية عبر الأثير والموجات الكهرومغناطيسية لدرجة يمكن القول معها أن سيادة الدولة الإقليمية قد انحسرت عن الإقليم الفضائي أو الهوائي واقتصرت على إقليمها الأرضي والمائي فقط [٢] .

وقد كرست الأعمال القانونية الدولية حق الاتصال والحصول على المعلومات وتداولها ،وأكدت على أهمية ضمان ممارسته [٣]. فقد نص القرار ٥٩ الصادر عن الأمم المتحدة في ١٤ ديسمبر ١٩٤٦ على أن "حرية الاستعلام هي حق أساسي للإنسان ،وهي حجر الزواية لكل الحريات التي كرست الأمم المتحدة نفسها للدفاع عنها،وحرية الاستعلام تشمل جمع ونقل ونشر المعلومات في كل دون عقبات ".

كما نصت المادة ١٩ من الاعلان العالمي لحقوق الإنسان الصادر عن الجمعية العامة للأمم المتحدة في ١٠ ديسمبر ١٩٤٨ على أن "لكل فرد الحق في حرية الرأي والتعبير ويشمل هذا الحق حرية اعتناق الآراء دون تدخل واستقاء وتلقي وإذاعة الأنباء والأفكار دون تقيد بالحدود الجغرافية وبأية وسيلة كانت "

وأخيرا نصت المادة ١٩ من العهد الدولي للحقوق المدنية والسياسية الصادر عن الأمم المتحدة في ١٦ ديسمبر ١٩٦٦ على أن "٢- لكل فرد الحق في حرية التعبير وهذا الحق يشمل حرية البحث عن المعلومات أو الأفكار من أي نوع واستلامها ونقلها بغض النظر عن الحدود ،وذلك إما شفاهة أو كتابة أو طباعة ،وسواء كان ذلك في قالب فني أو بأية وسيلة أخرى يختارها ". وتنشأ ضرورة وجود توافق دولي محكم في مجال الحق في المعلومات على وجه الخصوص من سهولة حركة المعلومات في أنظمة تقنية المعلومات حيث يرجع لهذه السهولة في حركة المعلومات بأنه بالامكان

---

(١) راجع في ذلك :

Ravillon (Hume) les telecommunications par sateliet aspects juridiques Paris , ed, lifec 1997,

Mateesco – Matte (N) droit aerospatical les telcomunnications par natellites Pars , 1982

(٢) راجع في ذلك

Park 9K-G) la protection de la souverainet aerienne Paris, 1977

(٣) راجع في ذلك :

Pinto ® la Liberte d'infromation ed d'opinion en droit international , paris , L.G.D.J. 1984

ارتكاب جريمة عن طريق حاسب آلي موجود في دولة معينة بينما يتحقق نجاح هذا النشاط الاجرامي في دولة أخرى.

وتستلزم مثل هذه الجرائم وجود تعاون دولي فعال [1] والذي يعتبر ضروريا من أجل حماية حقيقية لأنظمة الاتصالات البعدية التي تمر بالعديد من الدول وينشأ حتما عن وجود أوجه خلاف بين القوانين الوطنية والخاصة بتقينة نظم المعلومات ما يعرف بالمعلومات المختبئة والذي ستكون لها نتيجة عكسية في صورة قيود وطنية على حرية حركة المعلومات.

وفي مجال الاجراءات فإن التوافق بين مختلف سلطات التدخل الوطنية سيكون هاما من أجل التيسير دون عقبة لطلب المساعدة القانونية الوطنية ،أنه قد تلتمس إحدى الدول المساعدة القضائية من دولة أخرى بحيث يمكن لهذه الأخيرة أن تباشر التدابير التي تكون طبقا لقوانينها الخاصة .

<u>وفي سبيل ذلك يمكن التعرض لأبرز التدابير الواجب إتباعها سعيا لمكافحة جرائم الإنترنت وشبكات التواصل الإجتماعي وذلك على النحو التالي:</u>

<u>أولا: التدابير الواجب مباشرتها على المستوى الوطني</u>

يمكن تقسيم هذه التدابير إلى نوعين احداهما تدابير موضوعية والأخرى اجرائية . وذلك على النحو التالي :

<u>١- التدابير الموضوعية (٢)</u>

ينبغي على الدول أن تتبع سياسة جنائية مشتركة تهدف إلى حماية المجتمع من مخاطر الجريمة المعلوماتية وذلك من خلال تبنى التشريعات الملائمة لمواجهة الخطورة المتمثلة في إمكان إستخدام شبكات الكمبيوتر والمعلومات الالكترونية في إرتكاب أفعال إجرامية مع إمكانية تخزين ونقل الدليل المتعلق بمثل هذه الأفعال عبر تلك الشبكات . لذا من الأهمية بمكان مباشرة التدابير الآتية:

أ- يجب على كافة الدول أن تتبنى التشريعية وغيرها من التدابير اللازمة لإدراك عملية الدخول غير المشروع إلى سائر أو جزء من أجزاء نظام الكمبيوتر كجريمة جنائية وفقا لأحكام قوانينها الوطنية إذا

([1]) LA COmmision "invite fnstatment les autorites nationals compptentes a cooperer apin de parvenir a un accord international definissant les contenus illegaux et, par consequent, passibles de sanctions quelques soit le lieu de residence du fournisseur de contenu " et " propose Hume'etablissement de catalogues "nationaux " aisement accessibles recensant les contmis ou les operations illegales detectees sur intenrt ",
راجع في ذلك :

La criminamite infromatique sur L'internet

([2]) راجع في ذلك

European committee on crime problems 9cppc). Committee of experts on crime in cyber – space (pc-cy) draft convention on cybercirm 9draf N19) stansbourg, 25 April 2000

ما ارتكبت هذه الأفعال بصورة عمدية ويجوز لأي دولة أن تحدد من بين متطلبات ارتكاب الجريمة أن يكون ارتكابها من خلال اختراق تدابير الأمن أو بينة الحصول على بيانات الكمبيوتر .

ب- ينبغي على أن تتبنى التدابير التشريعية وغيرها من التدابير اللازمة لإدراك أعمال الاعتراض دون حق والتي تتم بأساليب فنية كعمليات نقل الكمبيوتر إلى أو من خلال حاسب آلي آخر وكذا الاشارات الالكترومغناطيسية الصادرة من أحد نظم المعلومات والتي تحمل مثل تلك البيانات واعتبارها جريمة جنائية لأحكام قوانينها الوطنية إذا ما ارتكبت بصورة عمدية .

ج- يجب على الدول أن تتبنى التدابير التشريعية اللازمة لإدراك أعمال الإضرار أو المحو أو الاتلاف أوالتعديل أو الإعاقة التي تستهدف بيانات الحاسب الآلي بدون وجه حق واعتبارها جريمة إذا ما ارتكبت بصورة عمدية .

د- يجب على الدول أن تتبنى التدابير التشريعية اللازمة لإدراج أعمال الإعاقة الخطرة دون وجه حق بوظائف نظام الكمبيوتر من خلال ادخال أو نقل أو الإضرار أو محو أو اتلاف أو تعديل أو اعاقة بيانات الكمبيوتر وادراكها باعتبارها جريمة جنائية إذا ارتكبت بصفة عمدية .

هـ -يجب على الدول أن تتبنى التدابير التشريعية اللازمة لامكانية مساءلة الأشخاص المعنوية جنائيا عن الجرائم الناشئة عن نظم المعلومات وذلك في الأحوال التي يؤدي فيها قصور الاشراف أو الرقابة من قبل الشخص الطبيعية إلى تسهيل ارتكابها.

<u>٢- التدابير الاجرائية (١)</u>

وتتمثل هذه التدابير على النحو التالي :

أ- يجب على الدول أن تتخذ التدابير التشريعية التي تخولها سلطة تفتيش ما يلي:

(١)أحد أنظمة الكمبيوتر أو جزء منه وبيانات الكمبيوتر المختزنة به .

(٢)أحد الوسائط التي قد تكون بيانات الكمبيوتر مختزنة به ،وذلك في أراضيها أو في أحد الأماكن الأخرى التي تمارس عليها سلطاتها لأغراض التحقيق .

ب- يجب على الدول أو تتخذ التدابير التشريعية اللازمة لتخويل سلطاتها المعنية في اصدار الأمر لأي شخص سواء كان متواجدا في إقليمها في أي مكان آخر عليه سلطاتها السيادية لكي يقدم أي بيانات محددة واقعة تحت سيطرته ومخزنة في أحد أنظمة الكمبيوتر أو أحد الوسائط المستخدمة في تخزين البيانات وذلك بالصورة التي تطلبها تلك السلطات لأغراض التحقيق.

---

(١) راجع في ذلك

Europan committee on crime problems (cppc) committee of experts on rime in cyber – space (pc – cy0 draft convention on cyber crimd (draft N 10) Strasbourg 25 april 2000

ج- يجب على الدول أن تتبنى التدابير التشريعية اللازمة لتمكين سلطاتها المعنية من الحصول على نسخة حفظ سريعة للبيانات المخزنة في أحد نظم الكمبيوتر وذلك لأغراض التحقيقات وذلك إذا تبين أنها معرضة بصفة خاصة للفقد والتعديل .

د- يجب على الدول أن تتبنى التدابير التشريعية اللازمة لإجبار الشخص الذي تتخذ حياله اجراءات الحفظ المشار إليها سلفا على الاحتفاظ بسرية الاجراءات لمدة محددة من الزمن وفقا للإطار الذي يسمح به القانون الوضعي .

هـ- يجب على الدول أن تتخذ التدابير التشريعية اللازمة التي تكفل حفظ بيانات النقل والخاصة بأحد الاتصالات المحددة كما تكفل الحفظ السريع لتلك البيانات الخاصة بعملية النقل وبغض النظر إذا كان مقدم الخدمة واحدة أو أكثر ممن شاركوا في عملية نقل هذا الاتصال .

و- يجب على الدول أن تتخذ التدابير التشريعية اللازمة لمد اختصاصها القضائي على أي من الجرائم المشار إليها إذا ما ارتكبت بصورة كليه أو جزئية على أراضيها أو على متن باخرة أو طائرة أو قمر صناعي يحمل علمها أو مسجل لديها. أو من قبل أحد مواطنيها إذا كانت الجريمة من الجرائم المعاقب عليها وفقا لأحكام القانون الجنائي الساري في محل ارتكابه أو إذا كانت الجريمة قد ارتكبت خارج الاختصاص الإقليمي لأي دولة .

<u>ثانيا: التدابير الواجب اتباعها على المستوى العربي</u>

نظرا لظهور مشكلة جرائم الكمبيوتر كمشكلة أمنية ، وقانونية واجتماعية ، فان خبراء الأمن المعلوماتي وصانعي السياسات الحكومية ومسوقي الكمبيوتر ، والأفراد المهتمين في هذا الموضوع بحاجة إلى تغيير نظرتهم تجاه جرائم الكمبيوتر ، ليس لأنها مشكلة وطنية فقط، وإنما كمشكلة عالمية ،وتتطلب الإجراءات الوطنية تعاونا في مجال القطاعين العام والخاص،فعلى القطاع الخاص الالتزام بإجراءات الوقاية، وعلى القطاع العام تنفيذ الإجراءات اللازمة لمكافحة الجريمة ،وبوجه عام هناك حاجة إلى تحقيق ما يلي على المستوى العربي:

١-وجود التشريعات اللازمة لحماية ملكية الكمبيوتر، وللبيانات،والمعلومات والمعدات اللازمة للتشغيل والتوصيل.

٢-زيادة الوعي الوطني في عالمنا العربي لجرائم الكمبيوتر وللعقوبات المترتبة عليها.

٣-إنشاء وحدات مختصة في التحقيق في جرائم الكمبيوتر في المحاكم والشرطة.

٤-إيجاد نوع من التعاون العربي في الحماية والوقاية من هذه الجرائم.

وقد عقدت الجمعية المصرية للقانون الجنائي مؤتمرها السادس في القاهرة في الفترة من ٢٥ إلى ٢٨ أكتوبر ١٩٩٣م وناقشت موضوع جرائم الكمبيوتر والجرائم الأخرى في مجال تكنولوجيا المعلومات من خلال الأبحاث والدراسات المقدمة من الباحثين والتي دارت حول تحديد أنواع الجرائم المختلفة المتعلقة بنظم المعلومات من اعتداء مادي على الأجهزة وأدوات الكمبيوتر بالسرقة أو التخريب أو

الإتلاف إلى اعتداء على البيانات والمعلومات المختزنة في قواعد المعلومات بالغش أو التزوير أو السرقة ، والحصول على تلك البيانات والمعلومات دون إذن أو الاتجار فيها، والتحايل على الأجهزة للحصول على الأموال ، وتحويل ونقل الأموال المتحصلة من الجرائم لغسلها. وأوضحت البحوث والمناقشات أن الاعتداء قد يحث أثناء إدخال البيانات والمعلومات أو إخراجها أو من خلال المعالجة الآلية لها،وذلك بالحذف أو المحو أو الإضافة أو التعديل دون حق،وأن هذه المعلومات قد تكون ثقافية أو سياسية أو عسكرية أو اقتصادية أو علمية أو اجتماعية. وقد بينت الأبحاث والدراسات والمناقشات التي اجريت خلال الفترة الماضية صعوبة اكتشاف جرائم نظم المعلومات وإثباتها، وأكدت على ضرورة تدريب رجال الشرطة القضائية ورجال التحقيق ورجال القضاء ، كما حذرت من تزايد احتمالات انتهاك حرمة الحياة الخاصة عن طريق التجسس والتنصت على الكابلات الرابطة بين القواعد الأساسية والوحدات الفرعية. وقد خلصت معظم الدراسات الاكاديمية العربية الى ضرورة اتخاذ التدابير والإجراءات اللازمة والتي تكون على النحو التالي:

١-حصول الشخص لنفسه أو لغيره على أموال عن طريق اختراق نظم المعلومات للاستيلاء عليها دون وجه حق.

٢-حصول الشخص لنفسه أو لغيره على بيانات أو معلومات أو مستندات عن طريق اختراق نظم المعلومات دون إذن.

٣-حصول الشخص لنفسه أو لغيره على أموال دون وجه حق عن طريق التحايل على الأجهزة.

٤-تحويل أموال دون حق عن طريق اختراق الأجهزة.

٥-تحويل أموال مستمدة بطريق غير مشروع عن طريق الأجهزة بقصد غسلها وتمويه مصدرها.

٦-إتلاف أو تشويه البيانات أو المعلومات أو المستندة المختزنة في قاعدة المعلومات.

٧-استخدام المعلومات المختزنة في قاعدة نظم المعلومات بقصد المساس بحرمة الحياة الخاصة للغير أو حقوقهم.

٨-تغيير الحقيقة في البيانات أو المعلومات أو المستندات التي تحويها قاعدة نظم المعلومات عن طريق الإضافة أو الحذف أو المحو الكلي أو الجزئي أو التعديل.

٩-حصول الشخص على نسخة من البرامج المختزنة في قاعدة نظم المعلومات دون إذن.

١٠-حصول الشخص على البيانات أو المعلومات أو المستندات التي تحويها قاعدة نظم المعلومات بقصد إفشائها أو قيامه بإفشائها فعلا أو الانتفاع بها بأي طريق.

١١-الاطلاع بأي طريق على المعلومات أو البيانات أو المستندات التي تحويها قاعدة نظم المعلومات دون إذن بقصد معرفتها.

١٢-التسبب خطأ في حصول الغير على أموال أو بيانات أو معدات أو معلومات أو مستندات أو في ارتكاب فعل من الأفعال المذكورة أعلاه.

ومن ثم فإن الإجراءات والتدابير الواجب إتباعها تكون على النحو التالي:

١-مساءلة الأشخاص الطبيعيين والأشخاص المعنويين والمؤسسات الفردية إذا اقترنت الجريمة لصالح الأشخاص والمؤسسات أو بأسمائها بالإضافة إلى مساءلة الأشخاص الطبيعيين من مقترفيها وشركائهم.

٢-إدماج نصوص جرائم نظم المعلومات في قانون العقوبات الوطني على أن يفرد لها فصل خاص.

٣-تدريب رجال الشرطة القضائية ورجال التحقيق والقضاء على كيفية استخدام أجهزة المعلومات وأدواتها وأشرطتها وآلات الطباعة الخاصة بها والإحاطة بكيفية إساءة استخدامها.

٤-تدريب رجال الشرطة القضائية والتحقيق والقضاء على كيفية الكشف عن هذه الجرائم وإثباتها.

٥-حث الدول على التعاون فيما بينها خاصة في مجال المساعدات والإنابة القضائية للكشف عن هذه الجرائم، وجمع الأدلة لإثباتها ، وتسليم المجرمين المقترفين لها، وتنفيذ الأحكام الأجنبية الصادرة بالإدانة والعقوبة على رعايا الدولة المقترفين لها بالخارج.

وقد قامت المنظمة العربية للتنمية الادارية ARADO بتبني فكرة المؤتمر الدولي لقانون الانترنت كمطلب حيوي وقيمي وعلمي للاكاديميين والباحثين في هذا الفرع الجديد من فروع القانون في العام ٢٠٠٦. ولقد تم وضع خطة عمل مبدئية مثارها ثلاثة نقاط:

- **أن هذا المؤتمر هو الاول من نوعه الذي يتخذ الطابع البحثي والعلمي سعيا الى تحقيق رؤية مشتركة دولية ومن ثم سوف يكون مقدمة الى الاستمرار فيه، وبشكل دوري، بحيث يكون أيضا أساسا وقاسما مشتركا يلتقي فيه المجتمع الدولي عند كلمة سواء ولتحقيق اهداف مشتركة.**

- **أن هذا المؤتمر ليس بالمؤتمر العربي، فهو مؤتمر دولي بكل معنى الكلمة، وسوف يكون شرف انطلاقه من قلب الوطن العربي. وسوف يكون هذا المؤتمر ملتقي دولي تجتمع فيه كافة الاطراف لمناقشة موضوعات السلام والحرية وعلى الاخص مسألة التنظيم القانوني للانترنت.**

- **أن قرار المنظمة العربية للتنمية الادارية ليس قرارا متفردا، فقد تم مشاورة خبراء في هذا الاطار، حيث تقرر أن ينعقد هذا المؤتمر بشكل دوري مفتوح ليس فيه تقييد او التزام بقضايا معينة، وانما تكون نقطة الارتكاز في هذا المؤتمر هو الالتزام ببحث القضايا المعاصرة التي يمكن أن تهم الانسانية في قطاعاتها المختلفة (قطاع حكومي- قطاع خاص- قطاع فردي- قطاع أهلي). لذلك فإن هذا المؤتمر هو نقطة انطلاق مفتوحة لكل الافكار التجديدية التي تتناول موضوع قانون الانترنت.**

ثالثا: التدابير الواجب مباشرتها على المستوى الدولي (١)

ويمكن تقسيم هذه التدابير إلى نوعين :الأولى :تتعلق بالتسليم والثاني :يتعلق بالمعونة المتبادلة .

---

(١) راجع في ذلك

Europan committee on crime problems (cppc) committee of experts on rime in cyber – space (pc – cy0 draft convention on cyber crimd (draft N ١٩) Strasbourg 25 april 2000

١ـ تسليم المجرم المعلوماتي

يجب على الدول أن تتعاو بعضها مع البعض ومن خلال تطبيق المواثيق الدولية ذات الصلة بشأن التعاون الدولي في المسائل الجنائية وعلى وجه الخصوص في مجال تسليم المجرم المعلوماتي حيث يجب يجب تسليم مرتكبيها وذلك وفقا لمعيار معين لتكييف الجريمة كجريمة يجوز تسليم مرتكبيها:

أ-أن يكون الدخول إلى النظام أو البيانات قد تم بدون وجه حق وبنية الاخلال بسرية البيانات أو اعاقة نظام الكمبيوتر .

ب- أن تبرم الدول فيما بينها اتفاقية تسليم مرتكبي الجرائم المعلوماتية .

ج- إذا ما رفض طلب التسليم الصادر في شأن مرتكبي إحدى الجرائم المعلوماتية بناءا على جنسية الشخص المراد تسلميه نظرا لأن طرف المدعى يعتبر أنه يختص قضائيا بالجرمية محل الادعاء ،يقوم الطرف المدعي عليه بتقديم القضية إلى سلطاته بغرض السير في الدعوى الجنائية وعلى أن يبلغ الطرف المدعي بالنتائج المترتبة عليه

٢ـ تفعيل إجراءات التعاون الدولي

وتتمثل المعونة المتبادلة في الاجراءات التالية :

أ- يجب على الدول أن تقدم لبعضها البعض المعونة المتبادل وذلك بأكبر قدر ممكن لاغراض التحقيق والاجراءات الخاصة بالجرائم الجنائية المتعلقة بنظم وبيانات الحاسب الآلي .

ب- يجب على الدول أنتقبل وتستجيب إلى طلبات المعونة المتبادلة من خلال وسائل الاتصال السريعة كالفاكس والبريد الالكتروني ،بالقدر الذي يوفر للطرف الطالب المستوى من الأمن والمصادقة.

ج- تخضع المعونة المتبادلة للاشتراطات المنصوص عليها في قوانين الدولة المدعية أو المنصوص عليها بموجب اتفاقيات المعونة المتبادلة .

د- في الأحوال التي يسمح فيها للطرف المدعي عليه بتعليق طلب المعونة المتبادلة على اشتراط وجود جريمة مزدوجة ،يعتبر هذا الشرط محل اعتبار وبغض النظر عما إذا كانت قوانين هذه الدولة تضع الجريمة في نطاق ذات تصنيف آخر .

هـ- تحدد كل دولة سلطة مركزية تنهض بالمسئولين ارسال طلبات المعونة المتبادلة والرد عليها وتنفيذها أو نقلها للسلطات المعنية للتنفيذ.

و- تنفذ طلبات المعونة المتبادلة وفقا للاجراءات التي تحددها الطرف المدعي قما عدا الأحوال التي لا تتصل فيها تلك الاجراءات مع أحكام القانون السائد بالدولة المعدي عليه .

ز- يجوز للدولة المدعي عليها أن ترفض طلب المعونة إذا ما توافرت لديها القناعة بأن الالتزام بما ورد بالطلب قد يخل بسيادتها أو أمنها أو نظامها العام أو بأي من مصالحها الأساسية الأخرى.

ح- يجوز للدولة المدعي عليها تأجيل التصرف في الطلب إذا كان هذا التصرف سيخل بالتحقيقات أو اجراءات الادعاء أو الاجراءات الجنائية التي تباشر بمعرفة السلطات المعنية .

ط- يجب على الدول المدعي عليها أن تخطر الدولة المدعية بصورة فورية بنتائج تنفيذ طلب المعونة فإذا ما رفض الطلب أو تم تأجيله يجب تقديم الأسباب إلى الرفض أو التأجيل .

ى- يجوز للدولة المدعية أن تطلب من الدولة المدعي عليها أن تحتفظ بسرية الوقائع والمحتويات التي يتضمنها الطلب ،فإذا لم يكن بمقدور الدولة المدعية عليها الوفاء بمتطلبات سرية الطلب فيجب عليها اخطار الدولة المدعية بذلك وعلى الاخيرة في هذه الحالة تحديد ما إذا كان سينفذ الطلب من عدمه .

ك- يجوز في حالة الاستعجال ارسال طلبات المعونة المتبادلة مباشرة إلي السلطات القضائية بما فيها النيابة العامة لدى الدولة الدعية عليها وفي مثل الحالة يجب ارسال نسخة بنفس الطلب إلى السلطة المركزية القائمة لدى الدولة المدعي عليها.

وترتيبا على ما سبق يمكن التأكيد أن العالم اصبح مترابط إلكترونيا، فيجب الاهتمام على المستوى الدولي بمشكلة جرائم الكمبيوتر وخاصة في مجال التشريعات والتعاون المتبادل، ويعتقد مركز الأمم المتحدة للتطوير الاجتماعي والشؤون الإنسانية أن الوقاية من جرائم الكمبيوتر تعتمد على الأمن في إجراءات معالجة المعلومات، والبيانات الإلكترونية، وتعاون ضحايا جرائم الكمبيوتر،ومنفذي القانون،والتدريب القانوني، وتطور أخلاقيات استخدام الكمبيوتر.والأمن الدولي لأنظمة المعلومات. ففي المجال الدولي هناك حاجة للتعاون المتبادل بين الدول، والبحث الجنائي والقانوني عن بنوك المعلومات، ففي أوروبا قدمت لجنة جرائم الكمبيوتر توصيات تتعلق بجرائم الكمبيوتر تمحورت في النقاط التالية:

- **المشكلات القانونية في استخدام بيانات الكمبيوتر والمعلومات المخزنة فيه في التحقيق الجنائي.**
- **الطبيعة العالمية لبعض جرائم الكمبيوتر.**
- **تحديد معايير لوسائل الأمن المعلوماتي وللوقاية من جرائم الكمبيوتر.**
- **مشكلة الخصوصية وخرقها في جرائم الكمبيوتر.**
- **موقف ضحايا جرائم الكمبيوتر.هذا وقد لخص التقرير الصادر عن اللجنة الأوروبية جرائم الكمبيوتر في التالي:**

١. الاحتيال.

٢. حذف وتدمير البيانات أو المعلومات أو البرمجيات في الكمبيوتر.

٣. الدخول غير القانوني.

٤. الاعتراض غير القانوني للاتصال بين الكمبيوتر وخاصة في مجال التحويل المالي.

٥. الإنتاج غير القانوني لبيانات، أو معلومات أو برمجيات الكمبيوتر.

وقد اقر الوزراء الأوروبيون التوصيات التالية:

١. إدراك أهمية الاستجابة الدقيقة والسريعة للتحدي الجديد للجرائم المتصلة بالكمبيوتر.

٢. أن يؤخذ بالحسبان أن الجرائم المتصلة بالكمبيوتر ذات خاصية تحويلية.

٣. الوعي بالحاجة الناجمة للتناغم بين القانون والتطبيق وتحسين التعاون الدولي القانوني.

<u>رابعا: أساليب الوقاية من فيروسات الإنترنت العالمية</u>

تتعدد أساليب الوقاية من الفيروسات المعلوماتية، ومن ثم يجب تحميل برنامج مضاد للفيروسات داخل كافة الأنظمة المعرضة لخطر الإصابة بها ويمكن الأخذ بالاحتياطات التالية للحد من انتشار الفيروسات وذلك على النحو التالي : [١]

١) أن يتم إدخال البرامج المحملة عن طريق الإنترنت من المواقع الموثوق فيها فقط.

٢) ألا يتم استخدام أي من الأقراص المرنة داخل الكمبيوتر ما لم يجر عليه فحص دقيق للتأكد من خلوه من الفيروسات. مع وقف عمل وحدة (الماكرو) كلما أمكن ذلك.

٣) يمكن تطعيم الأقراص المرنة ضد الفيروسات التي تصيب قطاع التحميل.

٤) الإبقاء على شريط الحماية الموجود بالبرامج الجديدة المسجلة على الأقراص المرنة.

٥) يجب على مهندسي الكمبيوتر الذين ينتقلون من شبكة إلى أخرى كفالة حماية الأقراص المرنة التي يستخدمونها.

وعلى أية حال ، لم يعد الشخص المتعامل مع الحاسب الآلى بحاجة لبرنامج مكافحة الفيروسات؛ وذلك نظراً لأن معظم شركات إنتاج هذه البرامج، بدأت تحرص على توفير العلاج ضد أى فيروس يكون قد ضرب ضربته الضارة بالفعل، وذلك إما باستخدام برنامج لفحص محتوي رسائل البريد الإلكتروني فيمكن منع وقوع الضرر قبل حدوثه، كما يُمكن لبرنامج الحماية الذي يفحص مضمون الرسائل الإلكترونية، اعتراض أي رسائل أو ملحقاتها تعتمد على لغة برمجة مثل نصوص لغة "فيجوال بيسك" أو أية ملفات أخري ذات أوامر تنفيذية وذلك على مستوي الجهاز الرئيسي (الخادم).

ومن المؤكد أن الطريقة الوحيدة للحصول على تأمين كامل ضد فيروسات البريد الإلكتروني وكافة النسخ المعدلة منه هو اعتراض وإيقاف كافة رسائل البريد الإلكتروني التي تحتوي نصوصاً خاصة بالبرمجة على مستوي الجهاز الرئيسي (الخادم). وذلك بعزل هذه الرسائل وهذه هي أكثر الطرق أماناً لمنع الإصابة بهذه الفيروسات.

---

(١) راجع في ذلك :

Dr : Linda Volonino Cyber Jerrorism op. cit.

وختاما فإن الواقع أن المخربين على الإنترنت يختلفون من جهة الخطورة؛ فمنهم المستخدم العادي الذي يستطيع الوصول لأغراض تخريبية، ومنهم الهاوي الذي يتعلم بعض المهارات على حساب الآخرين، ومنهم المحترف الذي يقصد التخريب، ومنهم العصابات المنظمة. ولهذا فمن أنجع الوسائل أن يتم التعامل مع الأشخاص على الإنترنت بحذر شديد، وألا يتم التعامل إلا مع أشخاص أو مواقع معروفة، بحيث لا يتم تحميل ملفات إلا من المواقع الموثوقة، ويمكن الاستفادة من تقنية التوقيع الرقمي والتي تعطى للمواقع عبر شركات كثيرة، حيث أن المواقع المعروفة لها توقيعات رقمية معترف بها. وهذه التقنية تدعمها برامج تشغيل الحاسبات المنتشرة في العالم مثل نظام التشغيل ويندوز من شركة مايكروسوفت، ولهذا يتم تحذيرك إذا كان الموقع غير معروف (ليس له توقيع رقمي معروف أو معترف به)، وأيضًا ينبغي التعامل بحذر مع رسائل البريد الإلكتروني بعدم فتح أي بريد يحوي مرفقات حتى لو كان من شخص نعرفه، إلا إذا كان المستخدم يتوقع وصول ذلك البريد، وذلك لاحتمال احتوائها على فيروسات أو ملفات تجسس.

خاتمة البحث

تناولنا فى هذا البحث جرائم تقانة المعلومات فى العالم العربى فى أسلوب مقارن مع الدول الأوروبية والولايات المتحدة الأمريكية، وقد ركزنا على تبيان الفرق بين الجرائم الواقعة على جهاز الحاسب ذاته والجرائم الإلكترونية الأخرى والتى منها جرائم المعلوماتية والإنترنت. وقد انتشرت جرائم المعلوماتية والانترنت بشكل كبير، وترتب على هذا الانتشار أضرارا بالغة فى حق الأفراد والمؤسسات بل والدول ذاتها، فمنظومة الأمن القومى لأى من الدول قد يخترقها أى من المجرمين الإلكترونيين كالهاكرز مثلا، فالأمر لا يحتاج أكثر من شخص اعتاد الإجرام الإلكترونى لكى يقوم باختراق مواقع الجهات السيادية والاطلاع على أسرارها وخصوصياتها. فضلا عن ذلك فالجرائم الإلكترونية، تأتى على أشكال وتصنيفات متنوعة، كما أن المجرم الإلكترونى له صفات خاصة تختلف عن تلك التى يتصف بها المجرم العادى.

ولاشك أن الجريمة الإلكترونية، ليست حكرا على بعض الدول دون الآخر، إذ أن الواقع الذى يفرضه التقدم التكنولوجى والمعلوماتى والذى أكده التطور المستمر فى وسائل معالجة ونقل المعلومات باعتبارها باتت المحدد الاستراتيجي للبناء الثقافي والإنجاز الاقتصادي، يؤكد أن هذه الجريمة الجديدة، آخذة فى الانتشار فى ربوع الأرض، فليس غريبا أن نجد مجرمى المعلوماتية والإنترنت فى العالم العربى، كما أن الدول الأوربية والولايات المتحدة الأمريكية ظلت لفترة طويلة – وما زالت- مرتعا خصبا للإجرام الإلكترونى بل إن هذه الدول بما حققته من تقدم علمى وتكنولوجى كانت أحد الأسباب الرئيسية لانتشار الجريمة الإلكترونية فى ربوع العالم.

وأمام هذا الانتشار الكبير لهذا النوع من الجرائم اتجهت الدول إلى تضمين أنظمتها القانونية قوانين لمكافحة الجريمة الإلكترونية من أجل إنزال حكم القانون على المجرم المعلوماتى أينما وجد وتوقيع العقاب عليه. فضلا عن اتجاه الكثير من الدول إلى تفعيل مبدأ التعاون الدولى فى مجال مكافحة الجريمة الإلكترونية.

ومما هو جدير بالذكر أن الجرائم الإلكترونية، هى ظاهرة إجرامية جديدة ومستجدة تقرع في جنباتها أجراس الخطر لتنبه مجتمعات العصر الراهن لحجم المخاطر وهول الخسائر الناجمة عن جريمة الحاسب الآلي التي تستهدف الاعتداء على المعطيات بدلالتها التقنية الواسعة، فجريمة الحاسب الآلي جريمة تقنية تنشأ في الخفاء، يقترفها مجرمون أذكياء يمتلكون أدوات المعرفة التقنية، توجه للنيل من الحق في المعلومات، وتطال اعتداءاتها معطيات الحاسب المخزنة والمعلومات المنقولة عبر نظم وشبكات المعلومات.

هذه المعطيات هي موضوع هذه الجريمة وما تستهدفه اعتداءات الجناة، وهذا وحده – عبر دلالته العامة – يظهر مدى خطورة الجرائم الإلكترونية، فهي تطال الحق في المعلومات، وتمس الحياة الخاصة للأفراد، وتهدد الأمن القومي والسيادة الوطنية، وتشيع فقدان الثقة بالتقنية وتهدد إبداع العقل البشري، لذا فإن إدراك ماهية الجرائم الإلكترونية ، منوط بتحليل وجهة نظر الدارسين لتعريفها

والاصطلاحات الدالة عليها واختيار أكثرها اتفاقًا مع الطبيعة الموضوعية لهذه الجرائم، واستظهار موضوعها وخصائصها ومخاطرها وحجم الخسائر الناجمة عنها وسمات مرتكبيها ودوافعهم.

وحرى بنا التأكيد على ما أثاره إحصاء إجراءات تقنية المعلومات من تحديات لها وزنها بالنسبة لقانون العقوبات في كل الأنظمة القانونية ويرجع السبب في ذلك إلى حقيقة مؤداها أنه حتى هذه اللحظة، فإن الأشياء المادية والمرئية هي التي تكون محمية بالقوانين الجنائية، وحماية المعلومات والقيم المعنوية الأخرى -وإن وجدت منذ فترة زمنية قصيرة- إلا أنها حتى منتصف القرن العشرين كانت أقل أهمية، وقد طرأ تغيير جوهري على هذا الموقف أثناء العشر سنوات الأخيرة، حيث أدى تطور المجتمع من مجتمع صناعي إلى مجتمع ما بعد الصناعي، إلى تزايد قيمة المعلومات بالنسبة للاقتصاد والمجتمع والسياسة، فضلا عن الأهمية المتنامية لتقنية المعلومات خلال فترة زمنية قصيرة، وهو الأمر الذى أوجد ما أصبح يعرف بقانون المعلومات.

وفى ضوء ما تقدم يمكننا القول بأن هذا البحث قد تناول موضوع الثورة المعلوماتية من زاوية الجانب السلبى منها والمتعلق بجرائم المعلوماتية وتأثيره على مكونات المجتمع. وأمام هذا الشكل الجديد من الإجرام لا تبدو قوانين العقوبات الوطنية في حالتها الراهنة كافية أو فعالة على النحو المطلوب أو المرضي فنصوصها والنظريات والمبادئ القانونية التي تتضمنها أو تقف ورائها موروث بعضها من القرن ١٩ حيث لم يكن هناك فنيين حينذاك وإنما أصحاب مهن وحرفيين.

وتطبيق بعض قواعد قوانين العقوبات الحالية على أشكال جديدة من الجرائم كتلك التى ترتب على استخدام تقنيات الحاسبات الآلية والمعلومات وأساليبها، ستواجه بصعوبات جمة منها صعوبات ناجمة عن الطبيعة الخاصة والخصائص الفنية الفريدة للوسائل المعلوماتية المستخدمة في ارتكابها، فضلا عن الصعوبات الرئيسية الأخرى والمتعلقة بنصوص التجريم التقليدية التى وضعت في ظل تفكير يقتصر إدراكه على الثروة الملموسة والمستندات ذات الطبيعة المادية مما يتعذر معه تطبيقها لحماية القيم غير المادية المتولدة عن المعلوماتية.

إن وسائل الاتصال لم تخترع الجريمة، بل كانت ضحية لها في معظم الأحوال حيث أن هذه الوسائل تعرضت لسوء الاستغلال من قبل كثيرين ، ومن الثابت أيضاً أن المجرمين وظفوا الاتصال تاريخياً لخدمة النشاطات الإجرامية التي يقومون بها. أما الجريمة فهي ذاتها الجريمة في قديم التاريخ، وحديثه، لا يختلف على بشاعتها، وخطرها على المجتمع الإنساني أحد، ولذلك اتفق على مواجهتها، ومن أجلها أقيمت المحاكم، وسنت العقوبات.

ومما لا شك فيه 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، فضلا عن ذلك، تتمتع جرائم الكمبيوتر والمعلوماتية بعدد من الخصائص التى تختلف تماما عن الخصائص التى تتمتع بها الجرائم التقليدية، كما أن الجانى الالكترونى(أو المجرم الالكترونى) يختلف أيضا عن المجرم العادى.

ويـأتي فـي مقدمـة أسـباب الجريمـة المعلوماتيـة، غايـة الـتعلم والتـي تتمثـل فـي اسـتخدام الكمبيـوتر 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.

وعلي الرغم من انتشار جرائم المعلوماتية في عالمنا العربي فى ظل جهود الحكومات العربية، من أجل جذب الاستثمارات في مجال التكنولوجيا إلا ان هناك فراغا تشريعيا في هذا المجال خاصة في قضايا النشر الالكتروني وقوانين جرائم الانترنت الخاصة باقتحام النظم وغيرها، فلا يوجد فى عالمنا العربي نظام قانوني متكامل خاص بجرائم المعلومات، إلا أن القانون يجتهد بتطبيق قواعد القانون الجنائي التقليدي على الجرائم المعلوماتية والتي تفرض نوعا من الحماية الجنائية ضد الأفعال الشبيهة بالأفعال المكونة لأركان الجريمة المعلوماتية.

وقد أرجع المتخصصون هذا الفراغ من أية عقوبات خاصة بجرائم الانترنت فى التشريع العربى إلى حداثة هذا المجال الذي لم يتعد عمره سنوات قليلة وما يطبق حاليا علي جرائم الانترنت هو القانون التقليدى الذى يتم بموجبه على الجرائم العادية مثل جريمة سرقة، حيث يعاقب مرتكبها بالحبس مدة لاتقل عن ٢٤ ساعة ولاتزيد علي ثلاث سنوات وجريمة النصب التى يعاقب مرتكبها بعقوبة النصب المدرجة في قانون العقوبات.

أما السب والقذف الالكترونى، فتكون جنحة، وإذا كانت الجريمة تركيب صور فاضحة، توجه لمرتكبها، تهم خدش الحياء وهتك العرض والتحريض علي الفسق. أما اطلاق الشائعات والسطو علي أرقام الكروت الائتمانية واقتحام نظم البنوك فتوجه إلي مرتكبها تهم تكدير الأمن العام وتهديد الاقتصاد القومي والاضرار بالمصالح العليا للبلاد وهي اتهامات خطيرة تقود صاحبها الي محاكم الجنايات مباشرة. على أن هذا التكييف القانونى لجرائم المعلوماتية يظل عاجزا عن مواكبة هذه النوعية من الجرائم وما يصاحبها من تطور مستمر فضلا عن تنامى أنواعها وانتشارها بشكل مريب وهو الأمر الذى يحتم على المشرع العربي سرعة اصدار قانون جديد يواجه الجرائم الالكترونية خاصة ان هناك بعض الجرائم المستحدثة التي لن تجد لها تكييفا قانونيا محددا في القانون التقليدى.

ويؤكد الكثير من رجال القانون على ضرورة إنشاء محكمة إلكترونية لسد الفجوة القانونية التي أحدثها التطور التكنولوجي الهائل في السنوات الأخيرة، فهناك جرائم ترتكب، وحرمات تنتهك، وحقوق تسلب على شبكة الإنترنت دون رقابة قانونية تذكر، والسبب في ذلك عدم وجود قانون دولي رادع يلاحق هواة الإجرام الإلكتروني، ويحاكمهم أمام محاكم دولية، إلا أن ذلك ليس من الأمور البعيدة التي يمكن أن تشق طريقها إلى التطبيق العملي في المستقبل القريب.

والمحكمة الالكترونية تتطلب إصدار تشريعات متخصصة فى مجال مكافحة الجريمة الإلكترونية، فضلا عن توفير القضاة المتميزين للقيام على أعمال الفصل فى القضايا المطروحة على هذه المحاكم.

وغنى عن البيان أن الدول العربية ليست ببعيدة عن مرمى الجرائم الإلكترونية، ذلك أن هذه الجرائم لم تترك بلدا من بلاد العالم إلا واخترقتها ونالت من أهداف محدده فيها، فالسعودية والإمارات وسلطنة عمان والكويت فلسطين وغيرهم من الدول العربية بادروا إلى وضع – أو فى طريقهم لوضع- تشريعات إلكترونية لمواجهة الجرائم المعلوماتية.

هذا ويلزم للمجتمع المعلوماتى فى مجال قانون الاجراءات الجنائية أن ينشئ قواعد قانونية حديثة بحيث تضع معلومات معينة تحت تصرف السلطة المهيمنة على التحقيق فى مجال جرائم الإنترنت وشبكات التواصل الإجتماعي. والسبب فى ذلك أن محترفى انتهاك شبكات الحاسبات الآلية ومرتكبى الجرائم الاقتصادية وتجار الأسلحة والمواد المخدرة يقومون بتخزين معلوماتهم فى أنظمة تقنية المعلومات وعلى نحو متطور. وتصطدم الأجهزة المكلفة بالتحقيق بهذا التكنيك لتخزين المعلومات وهى التى تسعى للحصول على أدلة الاثبات.

ونظرا لسهولة حركة المعلومات فى مجال أنظمة تقنية المعلومات حيث تجعل هذه السهولة لحركة المعلومات أنه بالإمكان ارتكاب جريمة عن طريق حاسب ألي موجود فى دولة معينة بينما يتحقق نتيجة هذا الفعل الاجرامى فى دولة أخرى، وهو الأمر الذى استلزم ضرورة وجود تعاون دولى محكم فى مجال مكافحة هذا النوع من الجرائم ولأجل توفير حماية حقيقية لأنظمة الاتصالات.

ونظرا للخطورة التى تمثلها الجرائم الإلكترونية فقد تناول البحث التشريعات المقارنة أنواعها بشىء من العناية والاهتمام، حيث ركز على جريمة العدوان على الإئتمان الرقمى وجرائم الأخلاق، ومنها جريمة الترويج السمعى-المرئى الفاضح، وجريمة البث العلنى وتشمل السب والقذف والتشهير والمراسلة باعتبار أن هذه جميعا تدخل فى عداد الجرائم الإلكترونية التى تستحق المواجهة التشريعية والتعاون الدولى لمواجهتها.

توصيات الدراسة

على أية حال فإنه فى سبيل الحد من جرائم تقانة المعلومات، فيجب ان نضع فى الاعتبار المقترحات والحلول اللآتية:-

١- ضرورة تقنين قواعد جديدة لمكافحة الجرائم المعلوماتية ؛ تأخذ بعين الاعتبار الطبيعة الخاصة لهذه الجرائم ولاسيما فيما يتعلق بالإثبات في الدعاوى الناشئة عن هذه الجرائم ؛ سواء في ذلك الدعاوى لجنائية والمدنية والتأديبية. كما ينبغي تعديل قواعد الإجراءات الجنائية لتتلاءم مع هذه الجرائم.

٢- ضرورة التنسيق والتعاون الدولي قضائيا وإجرائيا في مجال مكافحة الجرائم المعلوماتية .

٣- ضرورة تخصيص شرطة خاصة لمكافحة الجرائم المعلوماتية ؛ وذلك من رجال الشرطة المدربين على كيفية التعامل مع أجهزة الحاسوب والإنترنت.

٤- يتعين تدريب وتحديث رجال الادعاء العام – أو النيابة لعامة – والقضاء بشأن التعامل مع أجهزة الحاسوب والإنترنت .

٥- ينبغي أن تنص التشريعات العربية-مثلا- على اعتبار أن الانترنت يعتبر وسيلة من وسائل العلانية في قانون العقوبات والقوانين ذات الصلة بالجرائم المعلوماتية ؛ مع الأخذ بعين الاعتبار أن الإنترنت أوسع انتشارا من سائر وسائل النشر والعلانية الأخرى .

٦- يلزم تعديل قوانين ونظم الإجراءات الجزائية (الجنائية) ؛ بالقدر الذي يسمح ببيان الأحكام اللازم إتباعها حال التفتيش على الحاسبات وعند ضبط المعلومات التي تحتويها وضبط البريد الإلكتروني حتى يستمد الدليل مشروعيته .

٧- ينبغي أن يسمح للسلطات القائمة بالضبط والتحقيق بضبط البريد الإلكتروني وأية تقنية أخرى قد تفيد في إثبات الجريمة والحصول على دليل ؛ والكشف عن الحقيقة .

٨- يلزم أن تمتد إجراءات التفتيش إلى أية نظم حاسب ألي أخرى ؛ يمكن ان تكون ذات صلة بالنظام محل التفتيش وضبط ما بها من معلومات. ويشترط في هذه الحالة أن يكون هذا الإجراء ضروريا، والقاعدة العمة – في هذا الشأن – الضرورة تقدر بقدرها .

٩- يتعين أن تكون للسلطات القائمة بالضبط والتفتيش : سلطة توجبه أوامر لمن تكون لديه معلومات خاصة للدخول على ما يحويه الحاسب الآلي والانترنت من معلومات للإطلاع عليها .

١٠- ضرورة النص صراحة في القوانين المنظمة للإثبات – الجنائي والمدني – بما يسمح للقاضي بأن يستند إلى الأدلة المستخرجة من الحاسب الآلي والانترنت في الإثبات ؛ طالما أن ضبط هذه الأدلة جاء وليدة إجراءات مشروعة، على أن تتم مناقشة هذه الأدلة بالمحكمة وبحضور الخبير؛ وبما يحقق مبدأ المواجهة بين الخصوم .

١١- يتعين اعتبار نشر وطباعة الصور الجنسية عن طريق الانترنت مما يدخل ضمن زمرة جرائم الآداب .

١٢- ضرورة تجريم استخدام الأطفال في تصوير أفلام تمثلهم في أوضاع مخلة بالآداب العامة وعرضها على شبكة الانترنت وباستخدام البريد الإلكتروني.

١٣- يتعين النص صراحة على تجريم الدخول غير المصرح به على البريد الإلكتروني لإتلاف محتوياته أو إرسال صور إباحية أو تغيير محتواه أو إعاقة الرسائل أو تحويرها عبر الانترنت .

١٤- ضرورة سن التشريعات لمكافحة جرائم الإنترنت، وذلك بإدخال كافة صورالسلوك الضار والخطر على المجتمع التي يستخدم فيها انترنت .

١٥- يتعين اتاحة الفرصة للمواطنين في المشاركة في مكافحة الجرائم المعلوماتية ؛ وذلك من خلال إيجاد خط الساخن يختص بتلقي البلاغات المتعلقة بهذه الجرائم؛ ولاسيم الجرائم الأخلاقية كحالات الإعلان عن البغاء وممارسة الفجور أو الاستغلال الجنسي للأطفال عبر الانترنت .

١٦- ضرورة نشر الوعي بين صفوف المواطنين – ولاسيما الشباب – بمخاطر التعامل مع المواقع السيئة علي شبكة الإنترنت ؛مع ضرورة نشر الوعي المجتمعي بالمخاطر النفسية والاجتماعية وغيرها الناجمة عن الاستخدامات غير الآمنة للانترنت وتكثيف التوعية عن الآثار السلبية الصحية المترتبة عن الممارسات الجنسية الشاذة ؛ وذلك بأسلوب غير مباشر من خلال المواد الدرامية.

١٧- يتعين إدخال مادة "أخلاقيات استخدام الانترنت" ضمن المناهج الدراسية في التعليم ماقبل الجامعي .

١٨- إنشاء قسم جديد بكليات الحقوق بالجامعات العربية لدراسة الحماية القانونية للمعلوماتية أو تحت مسمى آخر "قانون المعلوماتية والانترنت" أو "قانون الحاسب الآلي والانترنت".

١٩- تفعيل دور المجتمع المدني ولاسيما الجمعيات الأهلية للقيام بدورها في وقاية الشباب من الوقوع في الممارسات الخاطئة للسلوكيات والممارسات الضارة أخلاقيا عبر شبكة الانترنت .

٢٠- من المناسب تعزيز التعاون والتنسيق مع المؤسسات الدولية المعنية بمكافحة الجرائم المعلوماتية ؛ وخصوصا الإنتربول.

وفي هذ المقام من الممكن أن تنضم الدول العربية إلى الاتفاقات الدولية الخاصة بمكافحة جرائم الانترنت وخاصة المعاهدة الدولية لمكافحة جرائم المعلوماتية والانترنت والعمل على دراسة ومتابعة المستجدات على الساحة العالمية.

٢١- أن تسعي الدول العربية إلى إنشاء منظمة عربية تهتم بالتنسيق في مجال مكافحة الجرائم المعلوماتية عبر الانترنت؛ مع تشجيع قيام إتحادات عربية تهتم بالتصدي لجرائم الانترنت وتفعيل دور المنظمات والإدارات والحكومات العربية في مواجهة هذه الجرائم عن طريق نظام الأمن الوقائي، ويكون من الأفضل إنشاء شرطة عربية تهتم بمكافحة الجرائم المعلوماتية.

المراجع

أولا: باللغة العربية:

١- الكتب

١) د. أبو اليزيد على المتيت، الحقوق على المصنفات الأدبية والفنية والعلمية، منشأة دار المعارف، الإسكندرية، الطبعة الأولى ١٩٩٧.

٢) د. أحمد فتحى سرور، الوسيط فى قانون العقوبات، القسم الخاص، القاهرة، دار النهضة العربية، ٢٠١٠.

٣) آمنة على يوسف، قراصنة أنظمة الكمبيوتر، المؤتمر القومى الثالث عشر لأمن الكمبيوتر، ، القاهرة، ١٩٩٩

٤) انتصار نورى الغريب، أمن الكمبيوتر والقانون٠ دار الراتب العالمية ، لبنان،١٩٩٤.

٥) د. جلال أحمد خليل، النظام القانونى لحماية الاختراعات ونقل التكنولوجيا إلى الدول النامية، جامعة الكويت،١٩٩٢.

٦) د. جميل عبد الباقى الصغير، القانون الجنائى والتكنولوجيا الحديثة، الكتاب الأول، الجرائم الناتجة عن استخدام الحاسب الآلى ، الطبعة الأولى، دار النهضة العربية، ١٩٩٢.

٧) حسن عماد مكاوي، ليلى حسين، الاتصال ونظرياته المعاصرة، القاهرة، الدار المصرية اللبنانية، الطبعة الرابعة، أكتوبر ٢٠١٣

٨) سليم خالد، ثقافة مواقع التواصل الاجتماعي والمجتمعات المحلية، دار المتنبي للنشر والتوزيع، قطر، ٢٠٠٥.

٩) شريف اللبان ، تكنولوجيا الاتصال. المخاطر والتحديات والتأثيرات الإجتماعية، القاهرة، الهيئة المصرية العامة للكتاب، ٢٠٠٨

١٠)د. طارق سرور، ذاتية جرائم الإعلام الإلكتروني (دراسة مقارنة)، القاهرة، دار النهضة النهضة العربية .٢٠٠١

١١)د. عبد الحميد الجمال، مبادئ القانون الكتاب الثانى، العلاقات القانونية، الفتح للطباعة والنشر، الإسكندرية، ١٩٩٠.

١٢)د. عبد الرزاق السنهورى، الوسيط فى شرح القانون المدنى، القاهرة ١٩٩٩.

١٣)د. عبد العظيم مرسى وزير، شرح قانون العقوبات- القسم الخاص- جرائم الاعتداء على الأموال، دار النهضة العربية ١٩٩٣.

١٤)د.عبد الفتاح الصيفى، قانون العقوبات اللبنانى – جرائم الاعتداء على أمن الدولة وعلى الأموال، دار النهضة العربية، بيروت ١٩٧٢.

١٥)د. عبد المهيمن بكر، القسم الخاص فى قانون العقوبات، الطبعة السابعة ١٩٧٧.

١٦)د٠ عمر السعيد رمضان، شرح قانون العقوبات، القسم الخاص، دار النهضة العربية ١٩٧٥.

١٧)د. عمر الفاروق الحسينى، المشكلات العامة فى جرائم الحاسب الآلى وأبعادها الدولية، دراسة تحليلية نقدية بنصوص التشريع المصري مقارنا بالتشريع الفرنسى ، الطبعة الثانية، ١٩٩٤.

١٨)د. عوض محمد، جرائم الأشخاص والأموال، دار المطبوعات الجامعية، الإسكندرية.

١٩)د. غانم محمد غانم، عدم ملائمة القواعد التقليدية فى قانون العقوبات لمكافحة جرائم الكمبيوتر، مؤتمر القانون والكمبيوتر والإنترنت- الإمارات، مايو ٢٠٠٠.

٢٠)فتحي حسين عامر، وسائل الاتصال الحديثة من الجريدة إلى الفيس بوك، القاهرة، العربي للنشر والتوزيع، ٢٠١١

٢١)د. فوزية عبد الستار، شرح قانون العقوبات، القسم الخاص، دار النهضة العربية،١٩٨٣.

٢٢)د. ماجد عمار، المسئولية القانونية الناشئة عن استخدام فيروس برامج الكمبيوتر ووسائل حمايتها، دار النهضة العربية، ٢٠٠٩

٢٣)د. محمد حسام لطفى، الحماية القانونية لبرامج الحاسب الآلي، دار الثقافة للطباعة والنشر. القاهرة ١٩٨٧.

٢٤)د.محمد سامى الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، القاهرة، دار النهضة العربية، الطبعة الثانية ٢٠١٥.

٢٥)د. محمد فهمى طلبه وآخرين، الحاسبات الالكترونية حاضرها ومستقبلها، موسوعة دلتا للكمبيوتر، مطابع الكتاب المصرى الحديث ١٩٩٢.

٢٦)د. محمد محيى الدين عوض، القانون الجنائى، جرائمه الخاصة ١٩٧٨/١٩٧٩.

٢٧)د. محمد مختار بربرى، قانون المعاملات التجارية، دار الفكر العربى، سنة ١٩٨٧.

٢٨)د.محمود محمود مصطفى، القسم الخاص، دار النهضة العربية، الطبعة الثامنة ١٩٨٤.

٢٩)د. محمود مصطفى القللى، شرح قانون العقوبات فى جرائم الأموال، الطبعة الأولى،١٩٣٩.

٣٠)د. محمود نجيب حسنى، جرائم الاعتداء على الأموال فى قانون العقوبات اللبنانى، دار النهضة العربية، بيروت

٣١)ـــــــ، شرح قانون العقوبات، القسم الخاص، دار النهضة العربية، ١٩٨٨.

٣٢)مصطفى الجمال، مبادئ القانون، الكتاب الثانى، العلاقات القانونية، الفتح للطباعة والنشر، الإسكندرية، ١٩٩٠.

٣٣)ميشال إنولا، تقنيات اتصال حديثة: الوسائط المتعددة وتطبيقاتها في الإعلام والثقافة والتربية، ترجمة: نصر الدين العياضي ورابح الصادق، باريس، دار الكتاب الجامعي، ٢٠٠٤.

٣٤)د. نبيل إبراهيم سعد، المدخل إلى القانون الكتاب الثانى، نظرية الحق، دار النهضة العربية، بيروت ١٩٩٥.

٣٥)نعوم تشومسكي، السيطرة على الإعلام.. الإنجازات الهائلة للبروباجندا، تعريب: أميمة عبد اللطيف، القاهرة، مكتبة الشروق الدولية، الطبعة الثانية، ٢٠٠٥

٣٦)د.هاني دويدار، نطاق احتكار المعرفة التكنولوجية بواسطة السرية، دار الجامعة الجديدة،١٩٩٦.

٣٧)د. هدى حامد قشقوش، جرائم الحاسب الالكتروني فى التشريع المقارن،القاهرة، دار النهضة العربية ١٩٩٢.

٣٨)د. هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة أسيوط ١٩٩٤.

٣٩)د. هلالي عبد اللاه أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، القاهرة، دار النهضة العربية.٢٠٠٦

٤٠)د. يسري أنور ود.آمال عثمان، شرح قانون العقوبات، القسم الخاص، الجزء الأول١٩٧٥.

٢- الرسائل العلمية

١)د. خالد حمدي عبد الرحمن، الحماية القانونية للكيانات المنطقية، رسالة دكتوراة، حقوق عين شمس ١٩٩٢.

٢)د. عزة محمود أحمد خليل، مشكلات المسئولية المدنية فى مواجهة فيروس الحاسب. رسالة دكتوراة، جامعة القاهرة، كلية الحقوق، ١٩٩٤.

٣) عماد إبراهيم، أثر استخدام الفيس بوك على سلوك طلبة الجامعات، رسالة ماجستير غير منشورة، كلية التربية، جامعة عين شمس القاهرة، ٢٠٠٩.

٤)د. محمد محمد عنب، معاينة مسرح الجريمة، رسالة دكتوراة، أكاديمية الشرطة، كلية الدراسات العليا القاهرة ١٩٨٨.

٥)د. يونس خالد عرب مصطفى، جرائم الحاسوب دراسة مقارنة، رسالة ماجستير، الجامعة الأردنية، ١٩٩٤.

٣- المقالات والدوريات

١) د. أسامة محمد محى الدين عوض، جرائم الكمبيوتر والجرائم الأخرى فى مجال تكنولوجيا المعلومات. بحث مقدم للمؤتمر السادس للجمعية المصرية للقانون الجنائى، القاهرة ١٩٩٣.

٢) د. برهام محمد عطا الله، المصنفات المحمية فى قانون حماية حق المؤلف، منشور فى كتاب حق المؤلف بين الواقع والقانون، مركز البحوث والدراسات القانونية، كلية الحقوق جامعة القاهرة، ١٩٩٠.

٣) توفيق التوجيري، الفيس بوك والاتجاهات السلوكية، مجلة الصحة النفسية جامعة القاهرة، عدد ٨ ، ٢٠٠٩.

٤) زاهر راضي، استخدام مواقع التواصل الاجتماعي في العالم العربي، مجلة التربية، عدد ١٥ جامعة عمان الأهلية، عمان، ٢٠٠٣.

٥) نجوى عبد السلام فهمي، التفاعلية في المواقع الإخبارية على شبكة الإنترنت. دراسة تحليلية، المجلة المصرية لبحوث الرأي العام، العدد الرابع، القاهرة، ٢٠٠١.

٤ـ الندوات والمؤتمرات

١) د. زكى أمين حسونة، جرائم الكمبيوتر والجرائم الأخرى فى مجال التكتيك المعلوماتى، بحث مقدم إلى المؤتمر السادس للجمعية المصرية للقانون الجنائى، القاهرة ١٩٩٣.

٢) علاء الدين محمد شحاته، رؤية أمنية للجرائم الناشئة عن استخدام الحاسب الآلى، بحث مقدم للمؤتمر السادس للجمعية المصرية للقانون الجنائي، القاهرة ١٩٩٣.

٣) د. محمد الأمين البشرى، التحقيق فى جرائم الحاسب الآلى، بحث مقدم إلى مؤتمر القانون والكمبيوتر والانترنت، جامعة الإمارات العربية المتحدة،سنة ٢٠٠٠.

٤) د. هدى حامد قشقوش، جرائم الكمبيوتر والجرائم الأخرى فى مجال تكنولوجيا المعلومات، ـ بحث مقدم للجمعية المصرية للقانون الجنائى ١٩٩٣

ثانيا: باللغة الانجليزية

1) Adams .L . Geverson , Media and society , Oxford publisher , London , 2006

2) Al-Mazeedi, Moosa, Ismail Ibrahim (1998). The Educational and Social Effect of the Internet on Kuwait University Students. In: Kuwait Conference on Information Highway. V:2 From : 16 – 18 March. P.p.

3) Al-Najran, Talal (1998). Internet adoption and use by Kuwait University students : new medium, same old gratifications. Unpublished Doctoral Dissertation. Ohio: The Ohio State University.

4) Bahgat Korany and others. The faces of national security in the Arab World, (England: Macmillan, 2009

5) Bajan, Peter, (1998). New Communities , New Social Norms. Studia-Psychologica. V. 40 (4.

6) Bartol, C. . Criminal behavior a psychosocial approach 5th, edition. New Jersey: Prentice Hall.2008

7) Bert Swart, "Modes of International Criminal Liability", in: Antonio Cassese, The Oxford Compaion to International Criminal Justice, Oxford University Press, 2009

8) Blackburn, R. . The psychology of criminal conduct: Theory, research and practice. Toronto:2006

9) Bolter, Jay David. Grusin Richard. (February 28, 2000), Remediation: Understanding New Media, USA: The MIT Press; 1st edition.

10) Brenner, V. (1997). Psychology of Computer Use: XL VII. Parameters of Internet Use, abuse and Addiction: The First 90 days of the Internet Usage Survey. Psychological Report, June, 80

11) Bright, J. "Community Safety, Crime Prevention and the Local Authority "in P. Willmott (ed) Poling and the Community, London PSL. 2008

12) Clinard, M. & Quinney, R. . Criminal behavior systems: A typology 6th, edition. Chicago: Pilgrimage.2007

13) Christakis, Nicholas A. Fowler, James H. (January 12, 2011), Connected: The Surprising Power of Our Social Networks and How They Shape Our Lives -How Your Friends' Friends' Friends Affect Everything You Feel, Think, and Do, USA: Back Bay Books; Reprint edition.

14) Cirel, P. Evans; McGillis, D. & Whit Comb, D. An Exemplary Project: Community Crime Prevention Programme, Seatte-Washington D.C.: Law Enforcement Assistance Administration, 2006

15) Daved smoloon (2009) the impact of the use of face book on the building society in the context of globalization, N Y sprctrum puplication .

16) Davis Lihmann, How can media improve our societies , George Publisher , New York , 2007

17) Diaz-Ortiz,Claire. (August 30, 2011), Twitter for Good: Change the World One Tweet at a Time, USA: Jossey-Bass; 1 edition.

18) Feldman, P. . The psychology of crime a social science textbook. Cambridge: Cambridge University Press.2006

19) Hawker, Mark. D, (August 25, 2010), Developer's Guide to Social Programming: Building Social Context Using Face book, Google Friend Connect, and the Twitter API, Canada: Addison-Wesley Professional; 1 edition.

20) Hollin, C. . Psychology and crime: An introduction to criminological psychology. New York: Routledge,2008

21) Hrdinová, J., Helbig, N., & Peters, C. S. (2010). Designing social media policy for government: Eight essential elements. Albany: Center for Technology in Government

22) Killy Nelson & Rinny Manwell , Media and crime , Media house , London , 2005

23) Kirkpatrick David,. (February 1, 2011), The Face book Effect: The Inside Story of the Company That Is Connecting the World. USA: Simon & Schuster.

24) Kraut, Robert et at (1998) . Internet Paradox : A Social Technology that Reduces Social Involvement and Psychological Well-Being . American Psychologist. V. 53, No. 9,.

25) Levinson, Paul. (September 5, 2009), New Media,USA: Allyn & Bacon;

26) Lister, Martin. Dovey, Jon. Giddings, Seth. Grant, Iain. Kelly, Kieran. (January 29, 2009) New Media: A Critical Introduction, USA/UK Europe : Routledge; 2 edition.

27) Nie, Norman and Erbing, Lutz (2017). Internet and Society: A Preliminary Report. Stanford Institute for the Quantitative Study of Society. Intersurvey Inc., and McKinsey and Co.

28) Prell, Christina. (November 9, 2011), Social Network Analysis: History, Theory and Methodology, USA/Austalia: Sage Publications Ltd.

29) Rowell, Rebecca. (January 2011), Youtube: The Company and Its Founders, UK Essential Library.

30) Sanders, CE; Field, TM.; Diego, M; and Kaplan (2000). The Relationship of Internet Use to Depression and Social Isolation among Adolescents. Adolescence. 35(138):

31) Schein, Levi, and Pollack, D, (1997). Social Work, Parenting and the Web. Journal of Family Social Work. 2(3): S/6.

32) Steward, Julian (1988). The Concept and Method of Cultural Ecology. In: High Points in Anthropology. Pual Bohannan and Mark Glazer (eds.). New York: McGraw-Hill, Inc.

33) Vonderau, Patrick. (December 30, 2009),The YouTube Reader, Sweden: National Library of Sweden.

34) White, H. et al. (1999) . Surfing the net in Later Life: A review of the Literature and Pilot Study of Computer use and Quality of life. Journal of Applied Gevontolog . Sept. V. 18 (3).

35) Wittkower, D:E. (October 1, 2010), Face book and Philosophy: What's on Y::our Mind?. USA: Open Court.