جرائم تقنية المعلومات في التشريع الأمريكي مقارنة بالتشريعات العربية

Information Technology Crimes in US Legislation As Compared to Arab Legislations

إعداد

د / نايف شافي المظافره الهاجري

أستاذ مساعد - أكاديمية سعد العبدالله للعلوم الأمنية

دولة الكويت

Dr/ Naif Shafi Al-Mozafarah Al-Hagri

Assistant Professor at Saad Al-Abdullah Academy for Security Sciences State of Kuwait

جرائم تقنية المعلومات في التشريع الأمريكي مقارنة بالتشريعات العربية

المستخلص

نظرا لازدياد الجرائم المتعلقة بتقانة المعلومات شرعت الدول المتمدينة بوضع تشريعات جنائية خاصة لمكافحة جرائم الحاسب الآلي التي تعتبر ظاهرة مستحدثة علي علم الإجرام ومن هذه الدول، الولايات المتحدة الأمريكية وفرنسا وباقي دول الاتحاد الأوروبي الذي وضع اتفاقية حول جرائم الحاسب الآلي سنة ٢٠٠١م، والتي أوصت فيها الدول الأعضاء باتخاذ كافة الإجراءات التشريعية أو غيرها حسب الضرورة لجعل الدخول إلى جميع نظم الحاسب الآلي 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 بمثابة 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.

هذه المسببات 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 اتفاقا 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 رئيسي كما يلي:

ما هي الأطر التشريعية المختلفة لجريمة سرقة المحتوى التقني ومكوناتها في البيئة الرقمية في التشريع الجنائي الأمريكي؟

الكلمات الدالة

١. سرقة المحتوى التقني
٢. البيئة الرقمية
٣. التشريع الجنائي الأمريكي

Abstract

Due to the increase in crimes related to information technology, civilized countries have begun to put in place special criminal legislation to combat computer crimes, which is an emerging phenomenon in criminology. All legislative or other measures as necessary to make unlawful access to all computer systems or any of its parts a criminal offense according to domestic law. between member states in the absence of international agreements.

Thus, the world found itself in a small village, and this village of information became the focus of the attention of all legitimate and illegitimate stakeholders, and information technology began to produce comprehensive effects on the administrative, economic, social, political, cultural, and legal structure of countries, because every scientific invention must open new horizons and arrange Effects that existed before its existence and spread, and here it was necessary for the law to intervene, how not, while it is regulated by its rules of all kinds, for all walks of life.

These data are the subject of this crime and what the perpetrators' attacks target, and this alone - through its general significance - shows the seriousness of computer crimes, as it affects the right to information, affects the private lives of individuals,

threatens national security and national sovereignty, spreads a loss of confidence in technology and threatens the creativity of the human mind Therefore, realizing the nature of computer crimes is dependent on analyzing the scholars' viewpoint to define them and the conventions indicating them, choosing the most consistent with the objective nature of these crimes, and memorizing their subject, characteristics, risks, size of losses resulting from them, and the characteristics and motives of the perpetrators.

In order of the above, the researcher can formulate the research problem of the current study in the form of a main question as follows:

What are the different legislative frameworks for the crime of stealing technical content and its components in the digital environment in the US criminal legislation?

Key words

1. Technical content theft

2. Digital environment

3. US criminal legislation

مقدمـــة

لاشـك أن بدايـة ظهـور الحاسـب الآلـي عـام ١٩٤٦ علـى يـد العـالمين الأمريكيين(e.p.eckert_j.w.mauchly) في جامعة بنسلفانيا وانتشر استخدامه في الكرة الأرضية بعد ذلك إلى أن وصل إلى عالمنا العربي في مطلع الستينات من القرن الماضي على يد الشركات الأجنبية، فإن العالم أصبح في مواجهة تقنيات جديدة وغير مألوفة تغزو الحياة بشكل تدريجي وتطور مضطرد في شكل ثورة علمية جديده، جعلت هذا الحاسب يؤدي من المهام والوظائف والتعامل مع المعلومات والوظائف، والتي لا يستطيع الكثير من الأفراد القيام بها.

من هنا يمكن القول بأن العالم أصبح أمام ثورة حقيقية هي عالم المعلومات والإتصالات، أو العالم الرقمي، وصار الناس أحيانا مختارين وفي أحايين أخرى مجبرين للتعامل مع هذا العالم الجديد أو مجتمع المعلومات كما يحلو للبعض أن يسميه، وما لبث الناس قليلا وهم يفيقون من صدمة ثورة المعلومات المتنامية حتى دهمتهم ثورة جديدة خلقها ذلك التزاوج أو الإتحاد الفريد بين هذا الجهاز وأنظمة الإتصالات الحديثة، لنصل في نهاية القرن الماضي وبدايات هذا القرن إلى ما يسمى التواصل عبر شبكة الشبكة الدولية للمعلومات " الإنترنت" العالمية، والتي اختصرت الزمن عبر شبكة لامرئية، أو محسوسة، سميت بشبكة الشبكة الدولية للمعلومات " الإنترنت" 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 الحاسب الآلي مباشرة([1]).

([1]) Please refer to:

Adomi, Overnight internet browsing among cybercafé users in Abraka, Nigeria. J. Community Inf. 3(2), (2007)

=

ونظرا لازدياد الجرائم المتعلقة بتقانة المعلومات او ما يطلق عليه الثورة السيبرانية شرعت الدول المتقدمة بوضع تشريعات جنائية خاصة لمكافحة جرائم السيبرانية التي تعتبر ظاهرة مستحدثة على علم الإجرام ومن هذه الدول، الولايات المتحدة الأمريكية وفرنسا وباقي دول الاتحاد الأوروبي الذي وضع اتفاقية حول جرائم الحاسب الآلي سنة ٢٠٠١م، والتي أوصت فيها الدول الأعضاء باتخاذ كافة الإجراءات التشريعية أو غيرها حسب الضرورة لجعل الدخول إلى جميع نظم الحاسب الآلي 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، 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([1]).

=

E. Adomi, Combating cybercrime in Nigeria. Electron. Libr. 26(5), (2008)

P. Bocij, The Dark Side of the Internet: Protecting Yourself and Your Family from Online Criminals (Praeger Publishers, Westport, 2006)

([1]) Acemoglu, D. and P. Restrepo (2017): "Robots and Jobs: Evidence from US Labor Markets," NBER Working Paper, 23285.

Amir, E., S. Levi, and T. Livne (2018): "Do firms underreport information on cyberattacks? Evidence from capital markets," Review of Accounting Studies, 23.

وهنا يتضح أن توقيت ظهور قانون الحاسب الآلي، بدأت مع شيوع وتوسع استخدامه وذلك في نهاية الستينات ومطلع السبعينات من القرن الماضي، حيث كانت أولى التحديات القانونية التي أثارها استخدام الحاسب الآلي هي اساءة استخدامه على نحو يضر بمصالح الأفراد والمؤسسات، وخاصة في حقل اساءة التعامل مع البيانات الشخصية المخزنة بالحاسب الآلي على نحو يمس أسرارهم وحياتهم الخاصة وحقهم في الخصوصية، والأمر الثاني هو المسئولية عن الأفعال التي تمثل اعتداء على الأموال والأفراد، وحق الأفراد في المعلومات ذات القيمة الإقتصادية([1]).

هذا ويوصف العصر الذي نعيشه بعصر الرقمنة أو العصر السيبراني، 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([2]).

([1]) Eisenbach, T., A. Kovner, and M. J. Lee (2020): "Cyber Risk and the U.S. Financial System: A Pre-Mortem Analysis," Federal Reserve Bank of New York Staff report, 909.

([2]) Hassan, T., S. Hollander, L. v. Lent, and A. Tahoun (2019): "Firm-Level Political Risk: Measurement and Effects," Quarterly Journal of Economics, 134(4)

وتنبع أهمية هذه الدراسة من كونها تتناول الثورة المعلوماتية من زاوية الجانب السلبي 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 بعض الأبعاد التاريخية في القرن التاسع عشر حيث لم يكن هناك فنيين حينذاك وإنما أصحاب مهن وحرفيين.

وتطبيق بعضها على أشكال جديدة للجرائم التي تستعير من تقنيات التحولات الرقمية 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 التي يجب التأكيد عليها أن وسائل الاتصال والمعلوماتية الجديدة لم تدشن الجريمة، بل كانت ضحية لها في معظم الأحوال حيث أن هذه الوسائل تعرضت لسوء الاستغلال من قبل البعض ، ومن الثابت أيضاً أن بعض الخارجين عن القانون وظفوا الاتصال تاريخياً – ضمن أدواتهم المختلفة – لخدمة النشاطات الغير شرعية التي يقومون بها. 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 المعلوماتية 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 السيبرانية 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 أن تسعى كافة دول العالم من أجل مكافحة هذا النوع المستحدث من الجرائم ذات البعد الإلكتروني، التي لم تعد تقف على حد دولة معينة، ولا توجه لمجتمع بعينه بل أصبحت تعبر الحدود لتلحق الضرر بعدة دول ومجتمعات، مستغلة التطور الكبير للوسائل التقنية الرقمية الحديثة في مجالات الاتصالات و المواصلات، وتعزيز التعاون بينها واتخاذ تدابير فعّالة للحد منها والقضاء عليها خاصة أن تلك الجرائم قد توسعت لدرجة مثلت تهديدا للأمن الدولي خاصة مع انتشار الإرهاب الرقمي والحروب السيبرانية الجديدة..

مشكلة الدراسة

تتمحور مشكلة دراستنا الحالية حول التأكيد أن جرائم تقانة المعلومات أو الجرائم ذات البعد الرقمي، هي ظاهرة إجرامية مستجدة تمثل خطرا كبيرا على كافة المجتمعات والشعوب وذلك لحجم المخاطر والخسائر الفادحة الناجمة عن جريمة المعلوماتية التي تستهدف الاعتداء على المعطيات بدلالتها التقنية الواسعة (بيانات ومعلومات وبرامج بكافة أنواعها). فجريمة تقنية المعلومات تعد جريمة رقمية تنشأ دون أن تترك ضجيجا أو اثارا تدل على الجاني، يقترفها مجرمون أذكياء يمتلكون أدوات المعرفة التقنية، توجه للنيل من الحق في المعلومات، وتطال اعتداءاتها معطيات الحاسب المخزنة والمعلومات المنقولة عبر نظم وشبكات المعلومات.

ومن هنا تأتي مشكلة دراستنا حيث يظهر مدى خطورة جرائم التقنية الحديثة، 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 رئيسي كما يلي:

ما هي الأطر التشريعية المختلفة لجريمة سرقة المحتوى التقني ومكوناتها في البيئة الرقمية في التشريع الجنائي الأمريكي؟

تساؤلات الدراسة

تطرح الدراسة الحالية مجموعة من التساؤلات الفرعية التالية:

١) ما هي المراحل التاريخية لتطور جرائم تقانة المعلومات؟

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

٣) ما هي الأبعاد المختلفة لجرائم الشبكة الدولية للمعلومات " الإنترنت" والمعلوماتية في الولايات المتحدة الأمريكية؟

٤) ما هي تدابير الضبط القانوني في مجال مكافحة جرائم تقانة المعلومات في الولايات المتحدة الأمريكية ؟

أهمية الدراسة

يمكن تحديد أهمية هذه الدراسة في ضوء الاعتبارات التالية:

١- حداثة موضوع الدراسة داخل محيطنا 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 العالمي.

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.

المبحث الأول

جرائم تقانة المعلومات وسرقة المحتوى الرقمي..

المفهوم والنشأة والتطور

أحدثت التطورات التكنولوجية الحديثة في منتصف عقد التسعينات من القرن الماضي، نقلة نوعية وثورة حقيقية في عالم التقنيات الحديثة، حيث انتشرت شبكة الشبكة الدولية للمعلومات " الإنترنت" في كافة أرجاء العالم، وربطت أجزاء هذا العالم الكبير بفضائها الواسع، ومهدت الطريق لكافة المجتمعات للتقارب والتعارف وتبادل الآراء والأفكار، واستفاد كل مرتاد لهذه الشبكة من الوسائط المتعددة المتاحة فيها، وأصبحت أفضل وسيلة لتحقيق التواصل بين المجتمعات المختلفة عبر العالم، ثم ظهرت المواقع الإلكترونية والمدونات الشخصية وبرامج المحادثة والشبكات الاجتماعية، التي غيرت مضمون وشكل الإعلام الحديث Social Media، وخلقت نوعاً من التواصل بين أصحابها ومستخدميها من جهة، وبين المستخدمين أنفسهم من جهة أخرى وهو ما أدى الى اطلاق مصطلح العالم البديل على الشبكات الاجتماعية([1]).

وهذه المواقع هي عبارة عن صفحات على شبكة المعلومات الدولية، يخصص بعضها للإعلان عن السلع والخدمات أو لبيع المنتجات، والبعض الآخر عبارة عن صحف ومجلات إلكترونية تتوفر فيها للكتاب إمكانية للنشر، وللزوار كتابة الردود على

([1]) Kamiya, S., J. Kang, J. Kim, A. Milidonis, and R. Stulz (2020): "Risk Management, Firm Reputation, and the Impact of Successful Cyberattacks on Target Firms," Journal of Financial Economics, Forthcoming

المواضيع المنشورة فيها، وفرصة للنقاش بين المتصفحين من خلال مساحات تتسم بالحرية، وكذلك مواقع للمحادثة (الدردشة)، وهناك المدونات الشخصية التي يجعلونها أصحابها كمحفظة خاصة يدونون فيها يومياتهم، ويضعون صورهم ويسجلون فيها خواطرهم واهتماماتهم.

أولا: نشأة وتطور جرائم تقانة المعلومات

لقد أرجع الفقه الجنائي جرائم تقنية المعلومات إلى العام ١٩٦٠[1]. وأما جرائم الشبكة الدولية للمعلومات " الإنترنت" فإنه يمكن القول إنها بدأت مع العام ١٩٨٨ وكانت أول الجرائم التي ترتبط عضوياً بالشبكة الدولية للمعلومات " الإنترنت" هي جرائم العدوان الفيروسي فيما هو معروف في التاريخ القانوني بجريمة دودة موريس المؤرخة واقعتها في ٢ الحرث / نوفمبر ١٩٨٨.

ولا يزال الفقه والتشريع المقارن في حقيقة الأمر يستشعر الحرج في التمييز بين كل من جرائم جهاز الحاسب الآلي وبين تلك الناجمة عن استخدام الشبكة الدولية للمعلومات " 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 جهاز الحاسب الآلي في الفقه والتشريع يسوده اتجاه يجمع بين الجرائم التي تقع على جهاز الحاسب الآلي ذاته وتلك التي يكون جهاز الحاسب الآلي وسيلة ارتكابها، فهي لدى هذا الاتجاه تعرف بأنها "فعل غير مشروع يتورط نظام جهاز الحاسب الآلي فيه، سواء كان جهاز الحاسب الآلي كآلة هو موضوع

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

الجريمة أو كان الوسيلة إلى ارتكابها أو مستودع الدليل المرتبطة بالجريمة". وهو تعريف مستمد من أكثر التعريفات شعبية لجرائم جهاز الحاسب الآلي الذي قال به الأستاذ Donn Parker من حيث إن جرائم جهاز الحاسب الآلي هي "جرائم تتطلب دراية ضرورية بجهاز الحاسب الآلي لكي يتم ارتكاب الجريمة بنجاح"[١]. ولم تأت الاتفاقية الأوروبية للجريمة عبر العالم الافتراضي المؤرخة في ٢٠٠١/١١/٢٣ على تعريف محدد للجريمة عبر الإنترنت[٢]، وإنما اعترفت بنوعية من الجرائم يمكن ارتكابها عبر الإنترنت.

واذا نظرنا الى التشريع الأمريكي نجد أن إدارة العدل الأمريكية قد توسعت في ربط جهاز الحاسب الآلي بتقنيته فذهبت إلى تعريف جرائم جهاز الحاسب الآلي بأنها "هي كل عدوان بالارتكاب على أي قانون يتضمن في محتواه تقنية جهاز الحاسب الآلي ويكون عرضة للتحقيق والاتهام"[٣] كان ذلك بالطبع بتأثير من اتجاهات المشرع

---

(1) 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.

(2)Lallie, H. S., L. A. Shepherd, J. R. Nurse, A. Erola, G. Epiphaniou, C. Maple, and X. Bellekens (2021): "Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic," Computers Security, 105.

(3) (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 perpetration, investigation, or prosecution"

=

الأمريكي في تعديل ١٩٩٦ لقانون البنية الوطنية للمعلومات The National Infrastructure Information Act (القسم ١٠٣٠)، الذي أستوحى التجريم من الربط بين جهاز الحاسب الآلي وتقنيته ككل، فتمخض هذا الاتجاه عن وجود ثلاثة أنواع من الجرائم التي يمكن ارتكابها عن طريق تقنية المعلومات وذلك وفقاً للمنهج الأمريكي، وهي [1] :

أولاً : الجرائم التي يكون جهاز الحاسب الآلي هدفاً لها، وهي نوعية من الجرائم يكون هدف المجرم فيها التوصل إلى سرقة بيانات من جهاز الحاسب الآلي أو إحداث إضرار به أو بنظام تشغيله أو بالشبكة التي يعمل خلالها. اذن يكون جهاز الحاسب الآلي هو الهدف الرئيس لها

ثانياً : الجرائم التي يكون جهاز الحاسب الآلي وسيلة لارتكابها، وهذه النوعية من الجرائم تحدث عندما يستخدم المجرم جهاز الحاسب الآلي 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

=

available online in feb. 2000 at : http://wings.buffallo.edu/complaw/complawpapers/scalion.html

- Kashyap, A. and A. Wetherilt (2019): "Some Principles for Regulating Cyber Risk," AEA Papers and Proceedings, 109, 482–487.

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

Moll, B., L. Rachel, and P. Restrepo (2021): "Uneven Growth: Automation's Impact on Income and Wealth Inequality," 28440.

Possess آلة Device بما في ذلك جهاز الحاسب الآلي بنية استخدامها في تزوير وثائق إثبات شخصية Falsify Identification documentation To 18) USCode Sec. 1028) ومن أمثلة تلك الجرائم سرقة بطاقات الإئتمان أو الترويج عبر الشبكة الدولية للمعلومات " الإنترنت" وهو أمر سيتم التعرض له بالتفصيل عبر صفحات دراستنا الحالية

ولقد توسعت بعض التشريعات في مدلول مصطلح "أدوات التزوير Forgery Devices" لكي تشمل جهاز الحاسب الآلي 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 جهاز الحاسب الآلي 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 جهاز الحاسب الآلي. ولاشك أن العديد من الدول قد سعت لتدشين تشريعات حول حماية وحفظ الحقوق الرقمية للمؤلف وهو ما سيتم التعرض له في التشريع الأمريكي عبر الدراسة الحالية

ومما تجدر الإشارة إليه إن مثل هذا التقسيم السالف ليس صحيحا بالكلية للتعبير عن جرائم جهاز الحاسب الآلي، إذ هناك من الجرائم التي ترتكب بواسطة جهاز الحاسب الآلي ومع ذلك لا يمكن إدراجها في أي من الأقسام أو الأشكال الثلاثة مثلما هو

الحال في جريمة سرقة وقت جهاز الحاسب الآلي مثلاً[١] وهي جريمة يعرفها القسم Tit. 18 USCode Sec. 641 من التقنين الأمريكي كجريمة من جرائم المعلوماتية[٢].

وربما يكون السبب في التوسع السالف عائداً إلى أن إمكانيات جهاز الحاسب الآلي لم تبرز إلى الوجود بالشكل الذي يجب أن تكون عليه، فكل ما نعلمه عن قدرات جهاز الحاسب الآلي يقل كثيراً عما نعلمه عن قدرات الشبكة المعلوماتية. 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 جهاز الحاسب الآلي تبدو هادئة أو طبيعية. ومثل هذا الأمر وجد له تأثير كبير في

---

(١) في تفصيل ذلك يمكن مراجعة:

Wachter, J. and J. Tsai (2015): "Disaster Risk and Its Implications for Asset Pricing," Annual Review of Financial Economics, 7.

(2) 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 :

(3) 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).

الاتفاقية الأوروبية للجريمة عبر العالم الافتراضي المؤرخة في ٢٠٠١/١١/٢٣ حيث اعترفت الاتفاقية، في المادة الأولى منها، بمصطلح "نظام جهاز الحاسب الآلي Computer System" ولم تأخذ في الاعتبار مجرد مصطلح "جهاز الحاسب الآلي 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"[1].

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

وبدون إحداث اتصال بين جهاز الحاسب الآلي وبين الشبكة الدولية للمعلومات " الإنترنت" عن طريق وسيط – حتى الآن- لا يمكن القول بوجودنا على الشبكة المعلوماتية. وعليه فإن مجرد القول بارتكاب جريمة حاسوب لا يعني ضرورة وجودنا على الشبكة الدولية للمعلومات " الإنترنت" وإنما يكفي أن يكون جهاز الحاسب الآلي

([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"

في حالة عمل، في حين أنه لا يمكن القول بارتكاب جريمة من جرائم الشبكة الدولية للمعلومات " الإنترنت" دون أن نكون على الشبكة الدولية للمعلومات " الإنترنت" Online[1].

وبالرجوع الى مجال تطبيق دراستنا وهو القانون الأمريكي يميز القسم 18USC Sec. 1030 ، بين مصطلحي حاسوب Computer وبين حاسوب مشمول بالحماية Protected computer، فهذا الأخير يعني ذلك جهاز الحاسب الآلي المتصل بغيره عن طريق الشبكات / الشبكة الدولية للمعلومات " الإنترنت" في حين إن إيراد مصطلح حاسوب Computer فقط فإنه يعني مجرد جهاز الحاسب الآلي غير المتصل بأي شبكة ولو داخلية (حيث يُعد هنا أداة تخزين فقط).

هذه الخصوصية التي منحها جهاز الحاسب الآلي 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 الشبكة الدولية للمعلومات " الإنترنت" CyberLaw ، فهذا لا يعني في الحقيقة التعامل مع قانون جهاز الحاسب الآلي Computer Law الذي يمثل أحد تفريعات قانون المعلوماتية أيضاً[2].

---

(1) 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 .

(2) Woods, D., T. Moore, and A. Simpson (2019): "The County Fair Cyber Loss Distribution: Drawing Inferences from Insurance Prices," Working Paper.

لذلك يتجه بعض الإتجاهات التشريعية الى إحداث فصل في هذا الإطار من حيث تعريف جرائم الشبكة الدولية للمعلومات " الإنترنت" تعريفاً منفصلاً عن جرائم جهاز الحاسب الآلي، باعتبارها جرائم ناجمة عن استخدام الإنترنت، وهو التعريف المبني على فهم عميق لطبيعة المشكلة من حيث ضرورة الفصل بين نوعي هذه الجرائم. حيث إن الشبكة الدولية للمعلومات " الإنترنت" أفاءت على القانون بأشكال إجرامية جديدة لم تكن معروفة، حتى في ظل التجريم عبر جهاز الحاسب الآلي حيث إنه كنتيجة لظهور الشبكة الدولية للمعلومات " الإنترنت" أضحت المشكلة ليست فقط إحداثيات التمييز في إطار التجريم عبر جهاز الحاسب الآلي، في محاولة تتعدى منطق التبسيط إلى التعقيد (مثال جرائم جهاز الحاسب الآلي – الجرائم المرتبطة بجهاز الحاسب الآلي وتفصيلاتها أيضاً ...إلخ) [1]. ولعل ما أنتهى إليه التطور الذي يبدو أنه غير ايجابي وفقا لتوصيات مؤتمر G8 (الثمانية الكبار والذي أصبح سبعة فقط او ما يطلق عليه G7حاليا) عام

([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

- Barry M. Leiner, V. G. (s.j.). Brief History of the Internet. Onttrek Dec. 20, 2015 uit

http://www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet

available under Creative Commons Attribution-NonCommercial-ShareAlike 3.0 Unported License.

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 جهاز الحاسب الآلي لكي تشمل كافة الجرائم التي يكون جهاز الحاسب الآلي طرفاً فيها. وهذا كله يجعلنا نقرر أن هناك مفارقة مصطنعة بين جرائم جهاز الحاسب الآلي وجرائم الإنترنت، على الرغم من الالتصاق الذي يكاد يكون طبيعياً بينهما.

وهذا الاتجاه الذي يجده الباحث سليما يجد له أساساً فقهياً يسعي إلى إقامة بنيانة على النحو الذي يحقق مصلحة الإنسان قبل الآلة، إذ يذهب هذا الاتجاه إلى أن جرائم الشبكة الدولية للمعلومات " الإنترنت" هي "كل فعل أو امتناع عمدي ينشأ عن الاستخدام غير المشروع لتقنية المعلومات ويهدف إلى الاعتداء على الأموال المادية والمعنوية[١].

وعلى الرغم من التوجه الصحيح في تعريف جرائم الشبكة الدولية للمعلومات " الإنترنت" على النحو السالف، خاصة أن هذا الرأي كان سباقاً عن اتجاهات الاتفاقية الأوروبية للجريمة عبر العالم الافتراضي المؤرخة في 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.

ومن خلال ما سبق يمكننا طرح تعريف شامل لجرائم الشبكة الدولية للمعلومات " الإنترنت" إذا أخذنا في الاعتبار ثلاث نقاط رئيسية، وعلى ضوئها يمكن وضع تعريف متكامل يفيد في تحديد الجرائم الناشئة عن الإنترنت.

---

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

النقطــة الأولــي : موضــوع العــالم الــسيبراني Cyberspace (وبالفرنــسية Cyberespace) الـذي هـو عبـارة عـن العـالم المرئـي The virtual world أو المجال الحيوي للبيانات وحركتها المعلوماتية، وهو العالم المختفي في الآلـة التقنيـة[١]. والذي يطلق عليه الفقـه العربـي تـسمية الفضاء الإلكترونـي[٢]. وهـو العـالم الـذي ابتكـر فكرتـه كاتـب الخيـال العلمـي الـشهير William Gibson فـي روايتـه الـشهيرة The NeuRomancer، التـي أصـدرها عـام ١٩٨٤، حيـث وصـف فـي هـذا الكتـاب فانتازيـا إلكترونيـة Fantasy Electronic[٣] تقابـل فيهـا مجموعـة هكـر مـن مهـرة جهـاز الحاسب الآلي، وطالما نشاطهم الاختراق والعديد من المظاهر التي تكاد تصل في بعض الأحيان إلى منطق الجريمة عبر الشبكة الدولية للمعلومات " الإنترنت" كما هي مقررة في التشريعات المعاصرة.

وإذا كانت الشبكة المعلوماتية لـم يـتم تعريفهـا بعد فـي النـظم القانونيـة المقارنـة بشكل مستقل، فإنه مع ذلك قد لجأت تلك النظم – بإيعاز من الفقـه – إلـى حيلـة قانونيـة يمكـن معهـا الحـصول علـى تعريـف قـانوني لهـا، وذلـك باسـتخدام مـصطلح منبثـق عـن

---

(1)Cone, M. (2011, Dec. 17). How to Configure Your Mac's Firewall. Onttrek Oct. 24, 2015 uit MACINSTRUCT: http://www.macinstruct.com/node/165 available under Creative Commons Attribution-NonCommercial-ShareAlike 3.0 Unported License.

(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

عالمها الافتراضي Cyberspace وهذا المصطلح هو CyberLaw أي النظام القانوني للعالم الافتراضي للإنترنت أو قانون الشبكة الدولية للمعلومات " الإنترنت" وهو "مجموعة القواعد القانونية التي تنظم العالم الفعلي للإنترنت" ، وهي قواعد لم تزل بعد في طور النمو نتيجة لعدم إمكانية حدوث ملائمة بين المنظومة التقليدية للقانون وبينها، حتى وإن وصفت بعدم الوضوح .

وإذا كان قانون العالم الافتراضي / الشبكة الدولية للمعلومات " 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/ الشبكة الدولية للمعلومات " الإنترنت" ذات طبيعة مختلفة في الحقيقة عن تركيبة أي قانون آخر، فهو يتركب من طبيعة افتراضية ذات بعد دولي[1] يتطابق شكلياً مع 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

([1])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 http://www.witsa.com December 2000 availale online in dec. 2000, at : http://www.mcconnellinternational.com/services/cybercrime.html

Cybercommerce للدلالة على سلوكيات القانون التجاري، ومصطلح Cyberinvestigation للدلالة على الإجراءات الجنائية في إطار قانون الإنترنت، ومصطلح Cybertribunal على المحاكمات عبر الشبكة الدولية للمعلومات " الإنترنت" ... إلخ.

ومن هنا يمكننا التأكيد أن هذا الاتجاه الفقهي يسعى إلى إقامة علاقة بين القانون وبين الشبكة الدولية للمعلومات " الإنترنت" في معنى إحداث ملائمة بين الأثنين، بما يمكن معه تطويع القانون للإنترنت لمصلحة الإنسان في تعامله مع الآلة.

إن عملية إحداث ملائمة بين النظام القانوني القائم وبين الشبكة الدولية للمعلومات " الإنترنت" كانت قد برزت بداية حال موافقة الفقه النسبية على إمكانية التعامل القانوني مع الشبكة الدولية للمعلومات " 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

([1])Email tips. (s.j.). Onttrek Oct. 29, 2015 uit Digital Survival:https://survival.tacticaltech.org/internet/email/tips available under a Creative Commons Attribution-Share Alike 3.0 Unported License.

([2])Gallagher, S. (2013, Oct. 02). We are not who we are. Onttrek Sep. 26, 2015 uit Security Blog: https://securityblog.redhat.com/tag/two-factor-authentication/ available under a Creative Commons Attribution-ShareAlike 3.0 Unported License.

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 جهاز الحاسب الآلي Computer Crimes عن جرائم الشبكة الدولية للمعلومات " الإنترنت" CyberCrime لانه كما اشرنا سابقا هناك جرائم للحاسب وهناك جرائم يكون فيها الحاسب أداة فقط للتنفيذ من خلالها، ومدى إمكانية قيام هذا الفصل تقنياً. والحقيقة إنه من الصعوبة بمكان فصل جرائم جهاز الحاسب الآلي عن جرائم الإنترنت، نتيجة لارتباط الشبكة الدولية للمعلومات " الإنترنت" بجهاز الحاسب الآلي ارتباطاً تقنياً. إلا أن هذه الصعوبة سوف تتقلص كثيراً إذا أدركنا أن تقنية جهاز الحاسب الآلي أعم كثيراً من تقنية الإنترنت. فهو – أي جهاز الحاسب الآلي- ثورة حقيقية ذات أبعاد اجتماعية وسياسية واقتصادية وقانونية ليس لها نهاية، إذ كما أنتجت تقنية جهاز الحاسب الآلي الشبكة الدولية للمعلومات " الإنترنت" فإن ذلك لا يعني نهاية المطاف في هذا الشأن، فالمؤشرات السائدة تشير إلى أن تقنيات جديدة للحاسب تبرز في الأفق قريبا ، وتدليلا على ذلك فإن دولاً مثل كندا تربط جرائم الشبكة الدولية للمعلومات " الإنترنت" بجرائم الاتصال عن بعد Telecommunication Crime التي يمكن أن

تقع بواسطة الشبكة الدولية للمعلومات " الإنترنت" كما يمكن إن تقع بواسطة الهاتف وجهاز الموجات الصغيرة Microwave والأقمار الصناعية Satellite وغير ذلك [١]

وإذا كان حقيقي إن تقنية جهاز الحاسب الآلي قد انطلقت لكي تبتكر الشبكة الدولية للمعلومات " الإنترنت" فإن منطقه الخلاف بين العمل السلبي الذي يكون محله جهاز الحاسب الآلي وبين ذلك الناجم عن استخدام الشبكة الدولية للمعلومات " الإنترنت" يعد أحد الصعوبات الجديدة التي تواجه فقه القانون حقيقة فإذا تحدد هذا التعريف فإنه من السهولة التوصل إلى بحث الرؤية السياسية والتشريعية في دولة ما . لأجل ذلك نجد إن البعض لا يمانع في إطلاق صفة جرائم جهاز الحاسب الآلي Computer Crime على الاختراق Hacking إلا أنه يشترط بالضرورة أن يكون جهاز الحاسب الآلي مرتبطا بشبكة Connected [٢] أو Protected Computer ويمكن القول إجمالا إن هناك اتجاهين في إطار رصد تعريف جرائم الشبكة الدولية للمعلومات " الإنترنت" ، الاتجاه الأول ينحو منحى التعريف الضيق الذي يقوم برصيد جرائم الشبكة الدولية للمعلومات " الإنترنت" في ربط جرائم العالم الافتراضي ككل بجهاز الحاسب الآلي حيث يذهب هذا الاتجاه إلى " إن مصطلح العالم الافتراضي

([1]) Gupta, A. (2011, March 01). Digital Forensic Analysis Using BackTrack, Part 1. Onttrek Sep. 26, 2015 uit opensourceforu: http://opensourceforu.efytimes.com/2011/03/digital-forensicanalysis-using-backtrack-part-1/ available under Creative Commons AttributionNonCommercial 3.0 Unported License.

([2]) Havercan, P. (2015, July 17). A plain person's guide to Secure Sockets Layer. Onttrek Sep. 26, 2015 uit http://peter.havercan.net/computing/plain-persons-guide-to-secure-socketslayer.html available under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License.

مرجعه استخدام جهاز الحاسب الآلي لتسهيل ارتكاب الجرائم [1] وهو تعريف مضيق لكونه يربط إجرام العالم البديل أو الإفتراضي بجهاز الحاسب الآلي بالمفهوم الضيق ، حيث أن مصطلح جهاز الحاسب الآلي يتسع لأبعد من ذلك الذي نعرفه اليوم وبحيث يجب الأخذ في الاعتبار تلك النظرة المستقبلية للحاسوب التي تعني حوسبة أو رقمية العالم البشري على النحو الذي يحقق اعتماد الإنسان عليه في كل شيء لذلك فإن النقد الذي يمكن توجيهه إلى هذا التعريف إنه يربط تعريف جرائم الشبكة الدولية للمعلومات " الإنترنت" بجهاز الحاسب الآلي فإن ذلك يعنى أن فصل جهاز الحاسب الآلي عن الشبكة الدولية للمعلومات " الإنترنت" في أبسط مظاهر هذا الفصل (أي بفصله بعدم الدخول إلى الشبكة الدولية للمعلومات " الإنترنت" وهذا ما تقوم به حتى بعض الدول في مجال حجب شبكة الشبكة الدولية للمعلومات " الإنترنت" عن الجماهير في حالات التظاهرات والثورات وما الى ذلك مثلما حدث في بعض البلدان العربية ابان احداث العام ٢٠١١ – أو بفصل الكهرباء عنه) يعنى نهاية الجريمة وعدم اتصالها بنا ، في حين أنذلك غير صحيح إذ تظل الجريمة قائمة وظاهرة في أماكن أخرى . وكذلك الأمر حينما اعلنت روسيا غزوها لأوكرانيا في فبراير ٢٠٢٢ حيث قامت بقطع كافة وسائل الإتصالات عن الدولة قبل الهجوم السيبراني.

([1]) (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

لذلك فإن الأرجح هو الاتجاه إلى التوسع في تعريف جرائم العالم الإفتراضي أو البديل / الشبكة الدولية للمعلومات " الإنترنت" ومكمن التعريف الموسع هو السعي إلى بحث استقلالية لجرائم الشبكة الدولية للمعلومات " الإنترنت" تتنافى مع ربطها بجهاز الحاسب الآلي وجرائمه . ولما كنا فيما سبق قد عرفنا الشبكة الدولية للمعلومات " الإنترنت" هي في الحقيقة الجرائم الناشئة عن استعمال هذا التواصل بين الشبكات وهذا اتجاه المشرع الأوروبي في اتفاقية الجريمة عبر العالم الافتراضي المؤرخة في ٢٠٠١/١١/٢٣ 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 E-Mail- الاتصال المباشر)، فإن العدوان باستخدام الشبكة الدولية للمعلومات " الإنترنت" من خلال أقسامها هو الوضع الصحيح الذي يجب أن يكون عليه التجريم هنا لذلك نجد إن جرائم الشبكة الدولية للمعلومات " الإنترنت" 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 الشبكة الدولية للمعلومات " الإنترنت" وبالتالي كل جريمة من الجرائم كانت وسيلتها الشبكة الدولية للمعلومات " الإنترنت" أو أقسامها إنما هي من جرائم الشبكة الدولية للمعلومات " الإنترنت"

ومن خلال ما سبق ذكره يمكننا التأكيد وفق مجال تطبيق دراستنا وهو التشريع الأمريكي بأن ظاهرة الشبكة الدولية للمعلومات " الإنترنت" لا زالت غامضة في دراسات القانون وفي هذا الإطار رصد المرشد الفيدرالي الأمريكي لتفتيش وضبط جهاز الحاسب الآلي Federal guidelines for searching and computers أهمية

الاعتراف بأن رجال القانون بدءوا في مواجهة مشاكل جديدة على اثر إنجاز ثورة معلومات جهاز الحاسب الآلي والاتصالات في القرن الواحد والعشرين ([1])

إن الفصل بين جهاز الحاسب الآلي وبين برمجياته يعد تدليلا على قيمة الفصل بين جهاز الحاسب الآلي وبين الشبكة الدولية للمعلومات " الإنترنت" . ولقد اشتد الصراع – بناء على ما سلف – بين فقه القانون وخبراء تكنولوجيا المعلومات خول الأبعاد الفلسفية لتحديد جرائم الشبكة الدولية للمعلومات " الإنترنت" أو جرائم العالم الافتراضي ، ما بين مؤيد لاعتبار هذه الجرائم مجرد جرائم عادية ترتكب بواسطة جهاز الحاسب الآلي 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 الشبكة الدولية للمعلومات " الإنترنت" إنما هي جرائم 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 الهكر Hacklers في هذا الإطار [2] وإذا كان هذا الاتجاه له منطقة

([1]) How do I know if a website is secure? (2015, Oct.). Onttrek Oct. 29, 2015 uit ccm.net: http://ccm.net/faq/2-how-do-i-know-if-a-website-is-secure available under the Creative Commons Attribution - NonCommercial - ShareAlike 3.0 France license.

([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

في ضرورة التعامل مع جرائم الشبكة الدولية للمعلومات " الإنترنت" بخصوصية ما إلا أن عملية الكشف عن هذه الخصوصية التي تتمتع بها هذه التوعية من الجرائم استلزم ضرورة التطرق إلى الخصوصية التي تمتع بها الشبكة الدولية للمعلومات " الإنترنت" ذاتها وأما النقطة الثالثة : التي يجب الانطلاق منها للتأكيد على تعريف جرائم الشبكة الدولية للمعلومات " الإنترنت" من منطلق أنها جرائم ترتكب بواسطة تلك الوسيلة أو الأداة التواصلية بين الشبكات دون اعتبار للحدود الدولية ، تتعلق بكينونة الشبكة الدولية للمعلومات " الإنترنت" 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 يحتوي على 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 يستدعي 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 الشبكة الدولية للمعلومات " الإنترنت" أمكن لها أن تحدث تفاعلا إيجابيا يتواصل مع قانون الشبكة الدولية للمعلومات " الإنترنت" مثلما 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 .([1]) فالعالم الفعلي هو جزء من عالمنا غير منفصل عنه ، لذلك فهو ليس بعيدا عن إمكانية إحداث تنظيم قانوني له ([2]) ، بل إن الفقه ينادي برؤية عقلية للانترنت عبر عالمية التفكير وإقليمية الحركة ([3])

ثانيا: ماهية جرائم تقانة المعلومات وأسبابها وخصائصها

تعددت التعريفات التي تناولت الجريمة السيبرانية ، 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 السيبرانية هي من الظواهر الحديثة؛ وذلك لارتباطها بتكنولوجيا حديثة هي تكنولوجيا المعلومات والاتصالات. وقد أحاط بتعريف الجريمة السيبرانية 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.

([1]) Introduction to Digital Forensics. (2011, Nov. 16). Onttrek Sep. 28, 2015 uit Wikibooks: https://en.wikibooks.org/wiki/Introduction_to_Digital_Forensics available under the Creative Commons Attribution-ShareAlike License

([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

تعريف الجريمة السيبرانية

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

١- التعريف الضيق للجريمة المعلوماتية السيبرانية

ذهب الفقيه (merwe) إلى أن الجريمة السيبرانية هي الفعل غير المشروع الذي يتورط في ارتكابه الحاسب الآلي – أو هو الفعل الاجرامي الذي يستخدم في اقترافة الحاسب الآلي كأداة رئيسية. فيما عرفها الفقية (ros blat) بأنها كل نشاط غير مشروع موجة لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب الالي والى تحويل طريقه.

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

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 في نطاق تعريفات مفهوم الجريمة السيبرانية الضيقة، تعريف مكتب تقييم التقنية بالولايات المتحدة الأمريكية، حيث يعرف الجريمة السيبرانية من خلال تحديد مفهوم جريمة الحاسب بأنها الجرائم التي تلعب فيها بيانات الحاسب الآلي والبرامج المعلوماتية دورا رئيسيا.

٢- التعريفات الموسعة لمفهوم الجريمة السيبرانية

ذهب الفقيهان (michel&credo) إلى أن جريمة الحاسب تشمل استخدام الحاسب كأداة لارتكاب الجريمة هذا بالإضافة إلى الحالات المتعلقة بالولوج غير المصرح به لحاسب المجني عليه أو بياناته، كما تمتد جريمة الحاسب لتشمل الاعتداءات المادية سواء على بطاقات الائتمان، وانتهاك ماكينات الحساب الآلي بما تتضمنه من شيكات تحويل الحسابات المالية بطرق إلكترونية وتزييف المكونات المادية والمعنوية للحاسب، بل وسرقة الحاسب في حد ذاتة وأي من مكوناته. وذهب رأي أخر من الفقة إلى تعريف الجريمة السيبرانية 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 اجرامي يتم بمساعدة الحاسب الآلي أو كل جريمة تتم في محيط أجهزة الحاسب الآلي[١].

وقد أشارت الأمم المتحدة في المدونة الصادرة عنها بشأن الجريمة السيبرانية ، إلي الخلاف الواقع بين الخبراء حول ماهية العناصر المكونة لجرائم الحاسب الآلي أو حتى المتعلقة بالحاسب الآلي ولعل ذلك ما يفسر عدم التوصل إلى تعريف متفق علية

(١) 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 الاجرامي.

٤- أن يفرق هذا التعريف بين الجريمة العادية والجريمة المعلوماتية وذلك عن طريق إيضاح الخصائص المميزة للجريمة المعلوماتية.

دوليا لهذه المصطلحات وإن كان هؤلاء قد اتفقوا ضمنا على وجود ظاهرة تتزايد بمعدلات عالمية لتلك الجرائم.

- المفهوم القانونى للمعلومات Information

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

- تعريف المعلومة

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

ووفقا لمجال دراستنا الحالية فقد عرف المشرع الامريكي، المعلومات في قانون المعاملات التجارية الإلكتروني لعام ١٩٩٩ بالفقرة العاشرة من المادة الثانية بأنها تشمل (البيانات والكلمات والصور والأصوات والوسائل وبرامج الحاسب الآلي 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 أنه تحسب ما قد يظهر من تتطور تكنولوجي جديد.

المبحث الثاني

تصنيف جرائم تقانة المعلومات وسرقة المحتوى الرقمي في التشريع الأمريكي

تتعدد انماط الجريمة في مجال الشبكة الدولية للمعلومات " الإنترنت" وشبكات التواصل الإجتماعي، والتي يمكن تصنيفها الى عدد من المحاور والتي تشكل جميعا انتهاكا يستحق العقاب خاصة ما يتعلق منها بسرقة المحتوى الرقمي وهو مجال دراستنا الحالية 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 الخاصة بالأفراد

تعد هذه الجريمة من الجرائم الشائعة في مجال الحاسب الآلي وهي تهدد الأمن الشخصي وكذلك أمن دولنا العربية والعالم ككل، ذلك أنه 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(١). وينطوي 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(٢) والذي يلتقط المعلومات والبيانات.

---

(١) انظر :

Bada, M. and Sasse, A; (2014) Cyber Security Awareness Campaigns: Why do they fail to change behaviour? Global Cyber Security Capacity Centre, University of Oxford: Oxford, UK. BH Co

(٢) 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 التي 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

=

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

=

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 أدعى أنه صحفي في إحدى المجلات واتصل بشركة اتصالات هاتفية مدعياً أنه بصدد نشر مقالة عن النظام المعلوماتي المستخدم في الشركة، فدعته الشركة لزيارة مقرها 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

=

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 كلمات 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 :

Bossong R. & Wagner B. (2018) A Typology of Cybersecurity and Public–Private Partnerships in the Context of the European Union. In: Bures O., Carrapico H. (eds) Security Privatization. Springer, Cham

(١) انظر :

Central Statistics Office (CSO) (2018). Information Society Statistics – Households:

https://www.cso.ie/en/releasesandpublications/er/isshh/informationsocietystatisticshouseholds2018/ CETs No. 185 (200

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[1] 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 الحاسب الآلي 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 سوى لعبة استخدام الطلبة من خلال كلمات السر most de pasdse .

ثالثا: السطو المسلح الإلكتروني " السرقة السيبرانية"

لاشك أن جرائم جديدة قد ظهرت الى عالمنا عقب ظهور شبكة الشبكة الدولية للمعلومات " الإنترنت" واتجاه البعض الى استخدامها سلبيا وهو ما نتج عنه العديد من الجرائم ومنها ما هو محل دراستنا الحالية، وقد 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 :

---

(1) راجع:

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

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

٢- التوصيل المباشر على خط تليفوني wiretape :

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.

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 وأدواره الرقمية

تتعدد أنماط هذه الجرائم على النحو التالي :

([1]) الدكتور محمد سامي الشوا، مرجع سابق، ص ٦٨ وما بعدها.

١ـ تعديل المعطيات الرقمية بدون إذن من صاحبه

أصبح تعديل المعطيات الرقمية تقنية سهلة وآمنة ومألوفة من تقنيات الإجرام المعلوماتي 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[١] أو البطاقات المثقوبة أو أفعال تحطيم إدخال البيانات أو إحداث ثقوب إضافية في البطاقات المثقوبة أو على العكس سد هذه الثقوب وأخيراً أفعال التحييد أو إلغاء المراقبات اليدوية[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

(١) 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.

Document that is being prepared with a view to submission to the Europen Union in Brussels.

(٢) انظر في ذلك :

Chatterjee S, Kar AK, Dwivedi YK et al (2019) Prevention of cybercrimes in smart cities of India: from a citizen's perspective. Information Technology & People. 32(5): 1153-1183.

بإحداث تغيير مباشر direct modification في البيانات المدخلة بينما وقع ٩,٥% منها فقط نتيجة تعديل وتلاعب في البرامج المستخدمة(١).

خامسا: أبرز جرائم تقانة المعلومات والرقمنة الجديدة

من الممكن التعرض بقدر من التفصيل لأبرز جرائم تقانة المعلومات والتي تمثل بعدا هاما في دراستنا الحالية بقدر من التفصيل وذلك على النحو التالي:

١- جريمة العدوان على الائتمان الرقمي

يمكننا التأكيد أن مفهوم 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 الرقمنة الحديثة في ظل ثورة المعلومات نشط الائتمان، سيما عبر التجارة الإلكترونية/ الشبكة الدولية للمعلومات " الإنترنت" على وجه

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

التحديد. فالتعامل المالي عبر الشبكة الدولية للمعلومات " الإنترنت" كما أنه استطاع استيعاب فكرة ظهور أشكال جديدة للنقود، فإنه كذلك يستطيع استيعاب فكرة الائتمان، خاصة إذا علمنا أن التعامل بالائتمان عبر الشبكة الدولية للمعلومات " الإنترنت" له سوابق تاريخية. إذ يكفي أن تضع اسمك ورقم بطاقة الائتمان الخاصة بك لكي تصل إلى غرضك التجاري كالبيع والشراء والاشتراك في مؤسسات وأندية...الخ. وهو الأمر الذي صار عاديا ومتاحا في ظل تنامي الثورة المعلوماتية كذلك ازداد الأمر اتساعا عقب جائحة كوفيد ١٩ Covid 19 والتي جعلت من الشبكة الدولية للمعلومات " الإنترنت" بديلا للحياة الطبيعية في ظل فترات الحظر الطويلة التي كانت سائدة، ويمتد نشاط التعامل بهذه البطاقات إلى النواحي العالمية؛ إذ يجوز اختراق الحدود بمقتضى الائتمان[١] أو بالأحرى تقلص فكرة رقابة الدولة عليها[٢].

ويمكننا في هذا المقام التعرض لأشكال العدوان على الائتمان عبر الشبكة الدولية للمعلومات " الإنترنت" وهي كما يلي:

(١) الاستيلاء على أرقام كروت الائتمان الخاصة بالأفراد والمؤسسات: 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 الشبكة الدولية للمعلومات " الإنترنت" فانفتح المجال لها لكي تضع عملية

---

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

(٢) المرجع السابق، ص١٦٥.

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.

وعلى الرغم من أن أحد الإتجاهات تذهب إلى أن الحيازة غير المشروعة لأرقام كروت الائتمان التي تتم عبر الشبكة الدولية للمعلومات " 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 الشبكة الدولية للمعلومات " الإنترنت" فإن حالات اختلاس هذه الأرقام عبر الشبكة الدولية للمعلومات " 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

---

(١) انظر:

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

للبيع بمبلغ مائتين وخمسين ألف دولار، ولقد اكتشف عملاء المباحث الفيدرالية هذه الجريمة وحوكم سادالوجو وعوقب بالسجن ثلاثين شهرًا[١].

(٢) العدوان على التوقيع الإلكتروني الرقمي: التوقيع الإلكتروني كأحد مظاهر التوقيع عامة كان – ولا يزال – أحد اهتمامات المشرع المقارن، وهو ما برز مع التوسع في استخدامات الشبكة الدولية للمعلومات " الإنترنت" من خلال تقريب المسافات وتوقيع صفقات تجارية كبيرة واستخدام هذا التوقيع الالكتروني لانهاء تلك الصفقات، 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

---

(1) 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.

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 الشبكة الدولية للمعلومات " الإنترنت" لسنة ١٩٩٧ يتضمن مجموعة نصوص حول الشبكة الدولية للمعلومات " الإنترنت" المؤرخ في ٢٢ يوليو ١٩٩٧ ومن بينها نصوص تتعلق بالتوقيع الإلكتروني.

أما محور تطبيق دراستنا الحالية وهو 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 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[1]. 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 جهاز الحاسب الآلي ومعتمد من قبل مستخدمه لكي يكون له ذات القوة والأثر للتوقيع المادي أو اليدوي ولكن لا يشمل هذا التعريف إمكانيات

(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.

التشفير"[1]. 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 الرقمي فإن ذلك يأخذ شكل العدوان على الأساليب الآمنة التي يتولاها طرف ثالث محايد Neutral Third Party، هو مقدم خدمات الشبكة الدولية للمعلومات " 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

([1]) « 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.

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 بجهاز الحاسب الآلي الذي يوصلها بحاسوب المصرف المذكور... وهكذا. ومثل هذا الاتجاه الجديد يمكن أن يكون أكثر ثقة في التعاملات 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 الشبكة الدولية للمعلومات " الإنترنت" ذات البعد الأخلاقي

في البداية يمكننا التأكيد أن تلك الجرائم هي أكثر الأمور سلبية تجاه الشبكة العنكبوتية حيث يتسع الضرر ليشمل الأفراد حول العالم ويتسبب في مشكلات اجتماعية ونفسية كبيرة، ويمكن أن يتسع الترويج عبر الشبكة الدولية للمعلومات " الإنترنت" كذلك ليشمل المحادثة الشفهية بأية وسيلة كانت كالتي تتم عبر الفيديو الرقمي أو البث الحي له بطريق الشبكة الدولية للمعلومات " الإنترنت" أو بطريق الدوائر المغلقة كعرض الشهادة في المحاكم أو تناول موضوعات عامة عن بعد. ولعل أخطر مظاهر الترويج السمعي 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].

(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

وقد اهتمت التشريعات الدولية المقارنة بظاهرة الترويج السمعي - المرئي الفاضح، وبصفة خاصة موضوع دعارة الأطفال التي أخذت من المشرع المقارن اهتمامًا كاملاً في هذا الإطار. ففي محور دراستنا الحالية في التشريع الأمريكي، نجد أن الفقه والقضاء والتشريع قد اجتهد 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[١]! لكون الشبكة الدولية للمعلومات " 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 الشبكة الدولية للمعلومات " الإنترنت" – وذلك بإيعاز من البيت الأبيض الأمريكي في بيانه المؤرخ في ١٩٩٦/١/٢٦ الذي صدر ردًا على إلغاء القضاء الأمريكي لنصوص في قانون أخلاق الاتصالات لسنة ١٩٩٦ المعدل للقانون الصادر في ١٩٣٦[٢].

وهنا يمكننا طرح رد الفعل الأمريكي باعتباره مجال دراستنا، نتيجة لمبادرة البيت الأبيض المذكورة فإنه في عام ١٩٩٨ أصدر الكونجرس الأمريكي القانون رقم Public Law 105-314 بشأن حماية الأطفال من التعدي

---

(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, op. cit, P.1.

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

الجنسي[١]. 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 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[٢].

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.

---

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

(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, P.4.

(2251. كذلك يحظر القانون الأمريكي استخدام جهاز الحاسب الآلي 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 جهاز الحاسب الآلي لنقل Transport دعارة الأطفال Child pornography عبر الولايات أو عبر مؤسسات تجارية أجنبية (18 US Code Sec. 2252 & 2252 (A)).[1]

٣- جرائم التعدي على الآخرين عبر الشبكة المعلوماتية الرقمية

تُعد هذه الجرائم من أقدم الجرائم المرتكبة عبر الشبكة العنكبوتية، وذلك لما يتمتع به عضو الشبكة الدولية للمعلومات " الإنترنت" دائمًا – وبحسب المعتقد السائد – من حرية كاملة عبر الإنترنت، ومن تلك الجرائم يمكننا التركيز على ما يلي:

(أ) التشهير وتشويه السمعة الخاصة بالأشخاص والمؤسسات: 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

(1) 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.

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.

(ب) تجريم المراسلةعبر الشبكة السيبرانية العالمية

يأخذ القانون الجنائي المقارن 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، وبالعودة الى مجال دراستنا الحالية وهو التشريع الأمريكي، نجد أنه من 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 الشبكة الدولية للمعلومات " الإنترنت" غير معروف مصدره.

وعليه يتسع مدلول الرسالة المجرمة عبر الشبكة المعلوماتية 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 عبر الشبكة السيبرانية، 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]،

(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).

وتبتعد عن مدلول مجرد النقد المباح الذي لا يتضمن المساس بشخص صاحب الأمر أو التشهير به أو الخط من كرامته[١]. 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[٢].

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

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

المبحث الثالث

جرائم تقانة المعلومات فى الولايات المتحدة الأمريكية

يـصعب تقـدير حجـم الخـسائر المترتبـة علـى جـرائم نظـم المعلومـات[١] والسبب في ذلك الرقم الأسود الذي يسيطر على هذا النوع من الإجرام علاوة على الموقف السلبي للمجني عليهم في هذه الجرائم، ولصعوبة اكتشاف الجريمة السيبرانية [٢]. لذا فإنه من الصعوبة تقدير حجم الخسائر الناشئة عن هذه الجرائم[٣] كما تشير بذلك الأبحاث التي أجريت في هذا الشأن سواء في فرنسا أو الولايات المتحدة الأمريكية أو إنجلترا.

---

(١) 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

(٣) 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.

أولا: تقدير خسائر الجرائم السيبرانية في الولايات المتحدة الأمريكية

في البداية يمكننا القول أن جرائم تقانة المعلومات السيبرانية قد سببت خسائر فادحة على المستوى الدولي ومنها بالطبع الولايات المتحدة الأمريكية محل دراستنا الحالية، حيث 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.**

فغالبية أفعال الغش والنصب الإلكتروني 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

---

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

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[١].

ثانيا: الجرائم السيبرانية بين التشريع والقضاء فى الدول الغربية

عقب التعرض للوضع الأمريكي محل دراستنا الحالية، يمكن التعرض لوضعية الدول الغربية والأوروبية، حيث 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 جهاز الحاسب الآلية 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.

---

(١) 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 .

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 جهاز الحاسب الآلية 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 والشبكة الدولية للمعلومات " الإنترنت" حيث عدلت في عام (١٩٨٥م) قانونها الجنائي بحيث شمل قوانين خاصة بجرائم الحاسب الآلي والانترنت، كما شمل القانون الجديد تحديد عقوبات المخالفات جهاز الحاسب الآلية، وجرائم التدمير، أو الدخول غير المشروع لأنظمة الحاسب الآلي[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 التي استحدثت فى هذا المجال في بعض الدول

---

(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 الآلي إلى رموز رقمية أو العكس حيث يسمح للحاسبات الآلية أن تستقبل وتنقل المعلومات عن طريق وسيط لخط تليفوني.

وقد استحدث قانون العقوبات الكندى [1] 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 آلي

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

جـ- كل من استعمل حاسب آلي مباشرة أو بطريق غير مباشر بغرض ارتكاب جريمة منصوص عليها في الفقرة أ،ب أو جريمة منصوص عليها فى المادة ٣٨٧ خاصة ببيانات أو حاسب آلي يعد مرتكبا لفعل إجرامي 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 في استخدام حقه المشروع للبيانات أو رفض ولوج شخص له الحق في البيانات.

([1]) راجع في ذلك:

Vivant et le stanc, lamy informatique no.2489.

التشريع الأمريكي

بالعودة الى مجال دراستنا في التشريع الأمريكي، يطبق فى الولايات المتحدة الأمريكية القوانين الخاصة بالغش في 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 شي ينطوي 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 الفيدرالى صدر قانون الولوج المصطنع في

(١) استحدثت الولايات الأمريكية " مثل أريزونا وكاليفورنيا وكولورادو وديلادار وفلوريدا وجورجيا والبنوى وميتشجان وميسورى ومونتانا وأوتارا ونيومكسكو...)العديد من القوانين الجنائية التي 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 آليات التجريم في 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 في الأفعال المعاقب عليها إلا أن صيغتها في 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 تروي مباشر أو بطريق غير مباشر" مادة ٥٥٨ والمعدلة في سنة ١٩٨٢، وقانون فلوريدا ينص على " كل من باشر.... عن تروي 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 في ذلك بالنموذج الفيدرالي ومنها قانون كاليفورنيا والذي 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 في 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 بأي نظام معلوماتي أو شبكة معلوماتية أو كيان منطقي أو بيانات وعلى =

الحاسب الآلي في أكتوبر سنة ١٩٨٤[1] counterfeit access device and computer

=

النقيض تنبت بعض القوانين الأخرى المنهج التحليلي ومنها على سبيل المثال قانون فلوريدا والذي احتوى على ثلاث مجموعات أساسية إحداهما: مخصصة للجرائم التي 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 سكسوني في التعاريف القانونية حيث يلاحظ أن هذه التعاريف ليس لها أي قيمة خارج الولايات المتحدة بل وأيضا خارج الولاية التي تنص عليها، وفضلا عن ذلك فليس لها أي قيمة خارج النص الذي يحتويها حيث أنها تعطي من أجل احتياجات النص.

راجع فى ذلك:

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

(١) بدأت – أنفينا سيكوريتى كورب – في بادئ الأمر وكأنها شركة انترنت نموذجية، بمكاتبها وحاسباتها وموظفيها ونظامها الأمني الحاسوبي ولم يكن ينقصها سوى الزبائن. لكن تبين الآن أن تلك الشركة التي بدت مشروعا فاشلا للوهلة الأولى كانت شركة وهمية أنشاها مكتب التحقيقات الفيدرالية الأمريكي اف بي أي للايقاع بشابين روسيين متهمين باختراق كمبوترات شركات انترنت أمريكية واختلاس معلومات حساسة فى محاولة لابتزاز المال وتقول السلطات إن اليكسي ايفانوف ٢١ عاما وفاسيلي جورشكوف ٢٥ عاما وكليهما من مدنية شليابنسك الروسية قد ابتلعا الطعم ووقعا في فخ الإف بي أي. وفي حين رفض مكتب التحقيقات الفيدرالية الإدلاء بأية تعليقات فإن وثائق قضائية كشف عنها النقاب مؤخراً تبدو وكأنها رواية جاسوسية يروي فيها عملاء الاف بي آي كيف تمكنوا من الإيقاع باللصين عن طريق انشاء شركة زائفة ودعوة ايفانوف وجوشكوف لمحاولة اختراق أنظمتها الحاسوبية المحصنة، وبعد أن نجح القرصانان الروسيان في اختراق الأنظمة عن بعد وجه موظفوا شركة أنفيتا دعوة لهما للقدوم إلى سياتل فى الولايات المتحدة لمناقشة

ابرام عقد شراكة واستعراض كامل امكانياتهما في مجا ل التسلل إلى أجهزة الكمبوتر عبر الانترنت، وبينا كان الشابان يستعرضان مهاراتهما في الشراكة الوهمية استخدم الاف بي 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.

=

Fraud and abuse act والذي ولج عمدا فى حاسب آلي 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 في 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 الذي يرتكب عن طريق الحاسب الآلي،ولكن وزارة العدل الأمريكية قدمت في أغسطس سنة ١٩٨٤[1] مشروعا بقانون يستهدف مباشرة حالة الغش المعلوماتي والذي 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 في حاسب آلي 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 التي تحتوي على بيانات معالجة والمكونات الالكترونية والكيانات المنطقية وبرامج

=

راجع في ذلك: جريدة البيان – دبي – الإمارات العربية المتحدة، العدد ٧٦٣٣ تاريخ ١٢ مايو ٢٠٠١.

(١) صدر في الولايات المتحدة الأمريكية القانون الفيدرالي بشأن الغش والعبث المعلوماتي abuse act &raud computer f في 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 الوطني 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 في ذلك: د. طارق سرور، سابق الإشارة إليه ،ص٥٣.

الحاسب الآلي سواء بلغة الآلة أو بلغة مقروءة للإنسان وكل قيمة أخرى ذات طابع مادي أو معنوي"[١].

وقد خول الكونجرس الأمريكي[٢] قطاع الخدمة السرية سلطة التحقيق فى عمليات الاحتيال التي 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 كودي أو رقم حساب أو أية وسيلة أخرى من وسائل الدخول على الحسابات بغرض التحصل على أموال أو بضائع أو خدمات أو أي 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 الرقمي الخفي" دون أن يشير من قريب أو بعيد لكلمة كمبيوتر.

---

(١) راجع في 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 في ذلك:

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

وتعد ماكينات الصرف الآلية A.T.M – التى انتشرت في 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 كي تقع تحت طائلة ونطاق الاختصاص الفيدرالي.

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

المبحث الرابع

الجوانب الإجرائية والتشريعية للضبط القانوني الأمريكي حيال جرائم تقانة المعلومات

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

أولا: المعوقات المتعلقة بجرائم السيبرانية الجديدة

تنقسم المعوقات في هذا الصدد إلى عدة أنواع نفصلها فيما يلي:

---

(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.

١ـ معوقات خاصة بطبيعة الجريمة السيبرانية وأدلتها

تتسم الجرائم التي تقع على الحاسبات وشبكات المعلومات بأنها غير مرئية فى العديد من حالاتها[١]. حيث لا يلاحظها المجني عليه غالبا أو يدرك حتى بوقوعها .

واخفاء السلوك المكون لها وطمس أو تغطية نتائجها عن طريق التلاعب غير المرئي في النبضات أو الذبذبات الالكترونية التي تسجل البيانات عن طريقها ليس مستحيلا في الكثير من أحوالها بحكم توافر المعرفة والخبرة الفنية في مجال الحاسبات لدى مرتكبها.[٢]. اختلاس المال عن طريق التلاعب في برامج الحاسب ومحتوياته، وغالبا ما يتم في مخرجات الحاسب تغطيتة وستره. والتجسس على ملف البيانات كان خطأ مصدره البرامج أو الأجهزة أو نظام التشغيل أو التصميم الكلي للنظام المعلوماتي.

---

(١) 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).

(٢) 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.

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

٢- معوقات خاصة بأدلة الجريمة السيبرانية

تتمثل أهم المعوقات المرتبطة بأدلة جرائم الشبكة الدولية للمعلومات " الإنترنت" وشبكات التواصل الإجتماعي كما يلي:

(أ) انعدام الدليل المرئى أو دليل الإدانة الموجب للعقاب

يلاحظ أن ما ينتج عن نظم المعلومات من أدلة عن الجرائم التى تقع عليها أو بواسطتها ما هي 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 أي أثر مما يقطع أي 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 التي يمكن أن تواجه جهات التحري والملاحقة. وتبدو هذه المشكلة بشكل عام في سائر مجالات

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

(٢) انظر في ذلك :

Ulrich , sieber, ibid, p. 140

التخزين والمعالجة الآلية للبيانات حيث تنتفي غالبا قدرة ممثلي الجهات المختصة على أن يتولوا بطريقة مباشرة فحص واختبار البيانات المشتبه فيها وتزداد جسامة هذه المشكلة بوجه خاص في حالة التلاعب في 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[1].

(ب) سهولة محو الدليل الرقمي أو تدميره في فترة زمنية يسيرة

من الصعوبات التى يمكن أن تعترض عملية الاثبات الجنائي فى مجال جرائم نظم المعلومات سهولة محو الجاني أو تدميره لأدلة الإدانة في فترة زمنية وجيزة فضلا عن سهولة تنصله من هذا العمل بإرجاعه إلى خطأ في نظام الحاسب أو الشبكة أو في الأجهزة ومن الأمثلة الواقعية قيام أحد مهربي الأسلحة بإدخال تعديلات على الأوامر العادية لنظام تشغيل حاسب صغير يستخدمه في تخزين عناوين عملائه والمتعاملين

(١) 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 لعملاتها 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

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

معه بحيث يترتب على إدخال أمر إلي 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 المعلوماتي بالنمسا بأن شيء ما في نظام تشغيل حاسب الفاعل قد جرى تغييره وقيامهم بناءا على ذلك باستنساخ الأقراص الممغنطة المضبوطة عن طريق أنظمة حاسباتهم(١).

وفي حالة أخرى شهدتها المانيا الاتحادية سابقا أدخل الجناة في نظام الحاسب تعليمات أمنية لحماية البيانات المخزنة داخله من المحاولات الرامية إلى الوصول إليها ومن شأنها محو هذه البيانات بالكامل بواسطة مجال كهربائي وذلك إذا ما تم اختراقه من قبل شخص غير مرخص له(٢).

(جـ) صعوبة الوصول إلى الدليل المثبت للجريمة السيبرانية

تحاط البيانات المخزنة الكترونيا أو المنقولة عبر شبكات الاتصال بجدار من الحماية الفنية لإعاقة محاولة الوصول غير المشروعة إليها للاطلاع عليها أو استنساخها(٣).. كذلك يمكن للمجرم المعلوماتي أن يزيد من صعوبة عملية التفتيش التى

---

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

(٢) راجع في ذلك :

Ulrich sieber, ibid, p. 141

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

=

قد تباشر للحصول على الأدلة التي 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 التي تعوق رقابة البيانات المخزنة أو المنقولة عبر حدود الدولة والتي تقلل من قدرة جهات التحري والتحقيق والملاحقة على الاطلاع عليها الأمر الذي يجعل حماية حرمة البيانات الشخصية المخزنة في مراكز الحاسبات والشبكات أو المتعلقة بالأسرار التجارية العادية والالكترونية أو بتدابير الأمن والدفاع أمر بالغ الصعوبة[1].

وتصطدم عقبة الوصول إلى الدليل المعلوماتي بمشكلة اجرائية تتعلق بمدى سريان القيود الخاصة بضبط الأوراق على ضبط محتوى نظام المعالجة الآلية للبيانات والمحمي فنيا في مواجهة الاطلاع غير المسموح به حيث يحظر قانون الاجراءات

=

- 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

(1) 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

الجنائيـة المـصرية والإمـاراتي بمقتـضى المـادتين ٥٢، ٥٨ علـى التـوالى [١]. اطـلاع مـأمور الـضبط القـضائي علـى الأوراق المختومـة أو المغلقـة[٢]. الموجـودة فـى منـزل المتهم أثناء تفتيشه[٣].وعلة ذلك الحفاظ على الآثار التى تتضمنها الأوراق وهنا يثور تساؤل عما إذا كان حكم هاتين المادتين واجب الإتباع بالنسبة لإطلاع مأمور الضبط القضائي 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 الذي من أجله تم تقرير هذا الحكم بالنسبة للأوراق المغلقة يتوافر أيضا بالنسبة لمحتوى نظام المعالجة الآلية للبيانات المحمي فنيا ضد الإطلاع غير المسموح به. فحظر المشرع اطلاع مأمور الضبط القضائي على هذه الأوراق نما هو لمظنة أن الغلق أو التغليف يضفي 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

(١) 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 .

(٢) 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.

(٣) 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.

المسموح به . فمحتوى النظام لا يكون بذلك مكشوفا بل محجوبا عن الغير حيث لا يتاح الوصول والاطلاع عليه بغير معرفة طريق ومفاتيح وكود التشغيل [١].

الثاني:أن المادة ٥٢ اجراءات مصري (٥٨ اجراءات اماراتي) 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.

والجدير بالإشارة إليه أن كلا من التشريعين الإجرائيين المصري والاماراتي لا ينفردا بهذه النتيجة بل يشاركهما فيها العديد من القوانين ومنها على سبيل المثال قانون الاجراءات الجنائية الالماني ، فطبقا للمادة ١١٠ منه تقتصر سلطة الاطلاع على مخرجات الحاسب وغيرها من دعائم البيانات على المدعي 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[٢].

---

(١) راجع في ذلك :

د. هشام محمد فريد رستم، سابق الإشارة إليه ص٣٤.

(٢) 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

(د) افتقاد الآثار الالكترونية المؤدية إلى دليل الإدانة

يحدث في بعض الأحيان إدخال البيانات مباشرة في نظام الحاسب دون تطلب وجود وثائق معاونة (وثائق خاصة بالإدخال) كما هو الحال في بعض نظم العمليات المباشرة التي تقوم على استبدال الإذن الكتابي لإدخال البيانات بإجراءات أخرى تعتمد على ضوابط للإذن متضمنة في برنامج الحاسب (مثل المصادقة على الحد الأقصى للإئتمان وفي 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 في برنامج الحاسب.

ويكون من السهل فى كل من هذين النوعين من العمليات ارتكاب بعض أنواع من الجرائم كاختلاس المال والتزوير بإدخال بيانات غير معتمدة في نظام الحاسب أو تعديل برامجه أو البيانات المخزنة داخله دون أن يترتب على ذلك أي أثر يشير ألى حدوث هذا الادخال أو التعديل . لذا يتعين على المحقق إزاء صعوبة الوصول إلى مرتكبي الجرائم فى كلا هذين النوعين من العمليات وعدم ترك التغيرات في البرامج أو البيانات آثار كتلك التى يخلفها التزوير المادي في المحررات التقليدية[١]. أن يسعى لتحديد دائرة الأشخاص القائمين أو المتصلين في عمليات ادخال ومعالجة البيانات وغيرها من عمليات التسجيل[٢]. مع الاستفادة من ضوابط الرقابة التي تباشر في النظام

---

(١) راجع في ذلك :

Jack Bologena corporate faraud : the Basice of prevention and detection , Butterworth publishers 1984,p.75

(٢) راجع في ذلك :

=

المعلومـاتي علـى الإدخـال والمعالجـة اضـافة إلـى تتبـع الأمـوال المختلفـة إن وجـدت باعتبارها محصلة الجريمة التى يستولي عليها المجرم في نهاية الأمر[١].

ثانيا: المعوقات الخاصة بالعامل البشرى

يمكننا القول أن هنـاك العديد من المعوقـات البشرية الخاصـة بتقنيـة المعلومـات وذلك على النحو التالي:

١ـ مكان ارتكاب الجريمة السيبرانية

يـتم ارتكـاب جريمـة الحاسب الآلـي السيبرانية عـادة عن بعد حيث لا يتواجد الفاعل علـى مسرح الجريمـة ومـن ثم تتباعد المسافات بين الفعل (مـن خـلال حاسب الفاعل) و النتيجـة (المعطيـات محـل الاعتـداء) وهـذه المسافات لا تقـف عنـد حـدود الدولـة بـل قـد تمتـد إلـى النطـاق الإقليمـي لـدول أخـرى ممـا يضاعف صعوبة كشفها أو ملاحقتها[٢]. فقد أعلنت السلطات البريطانية أن أكثر من عشرة ألاف اسطوانة تعليميـة عـن الإيـدز قـد أدخلـت إلـى المستـشفيات فـي كـل مـن بريطانيـا والـسويد والـدنمارك والنرويج.

وقد اكتشفت أجهزة البيانات أنهـا مصابة بفبروس "نورجـان " وهو فيروس يؤدي إلى تخريب أجهزة الحاسب الآلي الشخصى واتلاف البرامج التى تعمل عليه وفـي

=

J.Tappolet , La fracuc infromatieque, rev, int , crim poltech 1988,p.351

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

(٢) 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.

غضون ذلك. بدأت شرطة سكوتلانديارد تحقيقات واسعة النطاق فى هذه القضية باعتبارها جريمة تخريب وقد أثبتت التحقيقات مايلي:

(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 " وهي مؤسسة تخص رجل أعمال كينى " يدعى كيتيما " وقد اتضح أن قائمة الأسماء التي أحضرت معه خلال زيارته لبريطانيا في الفترة من ٣١ أكتوبر حتى ٣٠ نوفمبر ١٩٨٩ ولكنه لم يستدل له على عنوان.

(ب) أن عددا من هذه الاسطوانات ظهرت في كاليفونيا وفي بلجيكا وزيمبابوى.

(ج) الرسائل أرسلت مع رسائل معنوية بـ "معلومات عن الإيدز " لكن تبين أنها تحتوي على فيروس نورجان الذى يهاجم أجهزة الحاسب الشخصي 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 في بنما ولكن تبين أن معظم الرسائل أرسلت من لندن وبالتحري تبين عدم وجود شركة بهذا الاسم ولا يوجد لها صندوق بريد في بنما . بينما تبين أن مرسل الرسالة استخدام الاسم الأول من إحدى شركات البرامج الأمريكية العاملة في بنما والتي أكدت عدم مسئوليتها عما حدث.

(و) تحذر الرسالة من أنه في حالة عدم دفع الرسوم سيستخدم المرسل برنامجا لتخريب المعلومات ووقف جهاز الحاسب الآلي بشكل تلقائى ولكن ما أثار

الانتباه إلى هذه القضية حدث خلال تحميل الاسطوانة وفقا لما قاله "جرسيرست" خبير الفيروسات ومستشار التطبيقات البريطاني [١].

٢ـ نقص خبرة الشرطة وجهات لادعاء والقضاء تجاه الجرائم السيبرانية

يمكننا التأكيد أن هذا الجانب مهم للغاية ويتطلب المزيد من التركيز والتدريب ، حيث يتطلب كشف جرائم تقنية المعلومات والوصول إلى مرتكبيها وملاحقتهم قضائيا استراتيجيات خاصة تتعلق بإكسابهم مهارات خاصة وعلى نحو يساعدهم على مواجهة تقنيات الحاسب الآلي المتطورة وتقنيات التلاعب به،حيث تنعقد وتتنوع التقنيات المرتبة بوسائل ارتكابها[٢].

لذا يجب استخدام أساليب وتقنيات تحقيق جديدة ومبتكرة لتحديد نوعية الجريمة المرتكبة وشخصية مرتكبها وكيفية ارتكابها مع الاستعانة بوسائل جديدة أيضا لضبط الجاني والحصول على أدلة ادانته. إذ من المتصور أن يجد مأموري الضبط القضائي أنفسهم غير قادرين على التعامل بالوسائل الاستدلالية والاجراءات التقليدية مع هذه النوعة من الجرائم [٣]. ومما يزيد من صعوبة هذا الأمر افتقار أنظمة الحاسبات

---

(١) راجع في ذلك :

د. أسامة محمد محي الدين عوض ، سابق الإشارة غليه ، ص٤٣٠ ـ٤٣١

(٢)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

(٣) 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.

وشبكات المعلومات في البدايات الأولى لاستخدامها لأساليب الرقابة وضوابط التدقيق والمراجعة على العمليات والتطبيقات وعدم تزويدها بوسائل فنية لاكتشاف وتتبع مسار العمليات[١] ، فضلا عن ما تصادفه هذه الجهات من صعوبات في التحري عن جرائم الحاسب عابرة الحدود لا سيما بعد انتشار استخدام شبكة المعلومات العالمية .

وكثيرا ما تفشل أجهزة الشرطة في تقدير أهمية الجريمة السيبرانية نظرا لنقص الخبرة والتدريب[٢]. وللسبب ذاته أيضا كثيرا ما تفشل جهات التحقيق فى جمع أدله جرائم الحاسب الآلي مثل مخرجات الحاسب وقوائم التشغيل ، بل أن المحقق كما هو الحال أحيانا في بعض الجرائم الأخرى قد يدمر الدليل بمحوه الاسطوانة الصلبة من

---

(١) 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

(٢) 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. voloninalinu ibid, p. 6

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 الحاسب الآلي كأداة لارتكاب الجريمة في المعوقات التى يمكن أن تواجه في هذا المجال وهي:

- اما تجاهل هذا الدليل تماما.
- اما محاولة فحص هذا الدليل بدون أية مهارات فى مجال الحاسب الآلي .
- اما حمل المشتبه فيه على استعادة معلومات من الحاسب الآلي . ثم بعد ذلك عدم مصادرة نظام الحاسب الآلي حيث أن الشهادة التى يدلى بها تصبح حرجة في مواجهة المعلومات المستمدة من الحاسب الآلي.
- واما مصادر جهازالحاسب الآلي بدون معرفة ما يوجد فيه من معلومات وبالتالي زيادة الفرصة في فقد هذه المعلومات.

٣- إحجام المجنى عليهم عن التبليغ حيال الجرائم السيبرانية

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

---

(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 =

ويلاحظ أن العديد من ضحايا جرائم الحاسب لا يقفون عن حد عدم الابلاغ عن الجريمة بل أنهم يرفضون أي تعاون مع الجهات الأمنية خشية معرفة العامة بوقوع الجريمة ويسعون بدلا من ذلك إلى محاولة تجاوز أثارها حتى لوكانت الوسيلة هي مكافأة المجرم ونذكر على سبيل المثال بنك Marchant bank city في انجلترا لنقل ٨ مليون جنيه استرليني من أحد أرصدته إلى رقم حساب في 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 استرليني له بشرط عدم اعلام الآخرين عن جريمته واخطار البنك بالألية التى نجح من خلالها باختراق نظام الأمن الخاص بحاسب البنك الرئيسي[١].

=

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 العموميين 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،

(١) راجع في ذلك :

Peter swift Hackan , ibid , p. 3

وفي دراسة أجريت عام ١٩٨٠ في فرنسا أشارت النتائج إلى أن جرائم الحاسب التي تم الابلاغ عنها للسلطات الخاصة بلغت ١٥٪ من مجموع الجرائم وأن ادلة الادانة لم تتوافر إلا لنسبة تقدر بحوالي خمس النسبة المتقدمة أي ما يعادل حوالي ٣٪من مجموع جرائم الحاسب المرتكبة. كما تؤكد دراسة حديثة أجريت في الولايات المتحدة الامريكية أن الرقم الأسود لجرائم الحاسب يميل إلى الارتفاع فإستنادا إلى تحليل الباحثين وفي ضوء تقارير جمعيات صانعي الحاسبات يظهر أن الرقم الأسود ما يقارب نسبة ٦٠٪ من جرائم الحاسب[١].

٤- دور الخبراء فى فحص البيانات الإلكترونية

ويشكل الكم الهائل للبيانات التى يتم تداولها من خلال الأنظمة المعلوماتية أحد مصادر الصعوبات التي تعوق تحقيق الجرائم التي تقع عليها أو بواسطتها والدليل على ذلك أن طباعة كل ما يوجد على الدعامات الممغنطة لمركز حاسب متوسط الأهمية يتطلب مئات الآلاف من الصفحات والتي 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 التغاضي عن هذه البيانات كلها على أمل الحصول على اعتراف بالجريمة من المتهم[٢]. والواقع أنه بالامكان مواجهة هذة الصعوبة عن طريق أحد أمرين:

---

(١) راجع في ذلك :

يونس خليل عرب مصطفى جرائم الحاسب – دراسة مقارنة رسالة ماجستير – مقدمة إلى كلية الدراسات العليا الجامعة الأردنية ، ١٩٩٤ ، ص٧٣

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

أ- الاستعانة بالخبرة الفنية لتحديد ما يجب دون سواه البحث عنه للإطلاع علية وضبطه واستعانة الجهات القائمة بالتحري والتحقيق ، والحكم بالخبراء حين تتعامل مع الجرائم التي تقع فى مجال تكنولوجيا المعلومات تكاد تكون ضروره لاغنى عنها نظرا للطابع الفني الخاص لأساليب ارتكابها والطبيعة المعنوية لمحل الاعتداء ونجاح هذه الجهات في أداء رسالتها يتوقف إلى حد كبير علاوة على حسن إختيار الخبير على نجاحه في المهمة التى عهد إليه بأدائها وموضوع هذه المهمة وان كان يمكن للخبير نفسه أن يحدده إلا أن ذلك ليس مرغوبا فيه تجنبا لهيمنة دور الخبير على العملية الاثباتية وطغيانه على دور المحقق أو القاضي.

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

المبحث الخامس

تدابير الضبط القانوني الأمريكي

في مجال مكافحة جرائم السيبرانية الجديدة

يأتي هذا المبحث ليتناول التدابير الخاصة بالضبط القانوني تجاه تلك الجرائم والتي تعرضنا لها خلال الصفحات السابقة من دراستنا، حيث 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] .

---

(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

وقد كرست الأعمال القانونية الدولية حق الاتصال والحصول على المعلومات وتداولها ،وأكدت على أهمية ضمان ممارسته [١]. 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 ارتكاب جريمة عن طريق حاسب آلي موجود في دولة معينة بينما يتحقق نجاح هذا النشاط الاجرامي في دولة أخرى.

([١]) راجع في ذلك :

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

وتستلزم مثل هذه الجرائم وجود تعاون دولي فعال [١] 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 .

وفي سبيل ذلك يمكن التعرض لأبرز التدابير الواجب إتباعها سعيا لمكافحة جرائم تقنية المعلومات وذلك على النحو التالي:

التدابير التفاعلية الواجب مباشرتها على المستوى الدولي [٢]

ويمكن تقسيم هذه التدابير إلى نوعين :الأولى :تتعلق بالتسليم والثاني :يتعلق بالمعونة المتبادلة .

([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

([٢]) 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 19) Strasbourg 25 april 2000

١- تسليم المجرم المعلوماتى أو مجرم الشبكة السيبرانية

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 الحاسب الآلي .

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

٢- تفعيل إجراءات التعاون الدولى فى مجال السيبرانية الجديدة

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 المدعى 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 فيما عدا الأحوال التي لا تتصل فيها تلك الاجراءات مع أحكام القانون السائد بالدولة المعتدى عليها .

ز- يجوز للدولة المدعى 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 المدعى 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 المدعى 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 .

وترتيبا على ما سبق يمكن التأكيد أن العالم اصبح مترابط إلكترونيا، فيجب الاهتمام على المستوى الدولي بمشكلة جرائم الحاسب الآلي وخاصة في مجال التشريعات والتعاون المتبادل، ويعتقد مركز الأمم المتحدة للتطوير الاجتماعي والشؤون الإنسانية أن الوقاية من جرائم الحاسب الآلي تعتمد على الأمن في إجراءات معالجة المعلومات، والبيانات الإلكترونية، وتعاون ضحايا جرائم الحاسب الآلي،ومنفذي القانون،والتدريب القانوني، وتطور أخلاقيات استخدام الحاسب الآلي.والأمن الدولي لأنظمة المعلومات. ففي المجال الدولي هناك حاجة للتعاون المتبادل بين الدول، والبحث الجنائي والقانوني عن بنوك المعلومات، ففي أوروبا قدمت لجنة جرائم الحاسب الآلي توصيات تتعلق بجرائم الحاسب الآلي تمحورت في النقاط التالية:

- المشكلات القانونية في استخدام بيانات الحاسب الآلي والمعلومات المخزنة فيه في التحقيق الجنائي.
- الطبيعة العالمية لبعض جرائم الحاسب الآلي السيبرانية.
- تحديد معايير لوسائل الأمن المعلوماتي وللوقاية من جرائم الحاسب الآلي.
- مشكلة الخصوصية وخرقها في جرائم الحاسب الآلي.
- موقف ضحايا جرائم الحاسب الآلي.هذا وقد لخص التقرير الصادر عن اللجنة الأوروبية جرائم الحاسب الآلي في التالي:

١. الاحتيال الى جانب حذف وتدمير البيانات أو المعلومات أو البرمجيات في الحاسب الآلي.

٢. الدخول غير القانوني. والاعتراض غير القانوني للاتصال بين الحاسب الآلي وخاصة في مجال التحويل المالي.

٣. الإنتاج غير القانوني لبيانات، أو معلومات أو برمجيات الحاسب الآلي.

وقد اقر الوزراء الأوروبيون التوصيات التالية:

١. إدراك أهمية الاستجابة الدقيقة والسريعة للتحدي الجديد للجرائم المتصلة بالحاسب الآلي.

٢. أن يؤخذ بالحسبان أن الجرائم المتصلة بالحاسب الآلي ذات خاصية تحويلية.

٣. الوعي بالحاجة الناجمة للتناغم بين القانون والتطبيق وتحسين التعاون الدولي القانوني.

وبالتالي يمكن للباحث التأكيد في ختام الدراسة أن هذا الموضوع يتطلب دراسات عديدة حتى يتم عرضه والوصول الى توصيات بشأنه بصورة أكثر علمية خاصة مع تنامي الجوانب السلبية العديدة لتقنية المعلومات أو ما يعرف بالجرائم السيبرانية المعلوماتية الحديثة.

خاتمة البحث

لاشك أن الجريمة السيبرانية، ليست حكرا على بعض الدول دون الآخر، إذ أن الواقع الذى يفرضه التقدم التكنولوجي والمعلوماتي والذي أكده التطور المستمر في وسائل معالجة ونقل المعلومات باعتبارها باتت المحدد الاستراتيجي للبناء الثقافي والإنجاز الاقتصادي، يؤكد أن هذه الجريمة الجديدة، آخذة في الانتشار في ربوع الأرض، فليس غريبا أن نجد مجرمي المعلوماتية والشبكة الدولية للمعلومات " الإنترنت" في العالم العربي، كما أن الدول الأوربية والولايات المتحدة الأمريكية ظلت لفترة طويلة – وما زالت- مرتعا خصبا للإجرام الإلكتروني بل إن هذه الدول بما حققته من تقدم علمي وتكنولوجي كانت أحد الأسباب الرئيسية لانتشار الجريمة الإلكترونية في ربوع العالم.

وأمام هذا الانتشار الكبير لهذا النوع من الجرائم السيبرانية اتجهت الدول إلى تضمين أنظمتها القانونية قوانين لمكافحة الجريمة الإلكترونية من أجل إنزال حكم القانون على المجرم المعلوماتي أينما وجد وتوقيع العقاب عليه. فضلا عن اتجاه الكثير من الدول إلى تفعيل مبدأ التعاون الدولي في مجال مكافحة الجريمة الإلكترونية.

ومما هو جدير بالذكر أن الجرائم الرقمية الجديدة، هي 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 اتفاقا مع الطبيعة الموضوعية لهذه الجرائم، واستظهار موضوعها وخصائصها ومخاطرها وحجم الخسائر الناجمة عنها وسمات مرتكبيها ودوافعهم.

وفي هذا المقام يمكن للباحث 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 الذي أوجد ما أصبح يعرف بقانون المعلومات.

وفي ضوء ما تقدم يمكننا القول بأن هذا البحث قد تناول موضوع الثورة الرقمية الأمريكية من زاوية الجانب السلبي 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 التي 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 التي 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 الرقمي 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 السيبرانية 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 الحاسب الآلي والمعلوماتية بعدد من الخصائص التي تختلف تماما عن الخصائص التي تتمتع بها الجرائم التقليدية، كما أن الجاني الالكتروني(أو المجرم الالكتروني) يختلف أيضا عن المجرم العادي.

ويأتي في مقدمة أسباب الجريمة السيبرانية ، غاية التعلم والتي تتمثل في استخدام الحاسب الآلي 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 السيبرانية .

وقد أرجع المتخصصون هذا الفراغ من أية عقوبات خاصة بجرائم الشبكة الدولية للمعلومات " الإنترنت" في التشريع العربي إلى حداثة هذا المجال الذي لم يتعد عمره سنوات قليلة وما يطبق حاليا على جرائم الشبكة الدولية للمعلومات " الإنترنت" هو القانون التقليدي الذى يتم بموجبه على الجرائم العادية مثل جريمة سرقة، حيث يعاقب مرتكبها بالحبس مدة لاتقل عن ٢٤ ساعة ولاتزيد على ثلاث سنوات وجريمة النصب التي يعاقب مرتكبها بعقوبة النصب المدرجة في قانون العقوبات.

أما السب والقذف الالكتروني، فتكون جنحة، وإذا كانت الجريمة تركيب صور فاضحة، توجه لمرتكبها، تهم خدش الحياء وهتك العرض والتحريض على الفسق. أما اطلاق الشائعات والسطو على أرقام الكروت الائتمانية واقتحام نظم البنوك فتوجه إلى مرتكبها تهم تكدير الأمن العام وتهديد الاقتصاد القومي والاضرار بالمصالح العليا للبلاد وهي اتهامات خطيرة تقود صاحبها الى محاكم الجنايات مباشرة. على أن هذا التكييف القانوني لجرائم المعلوماتية يظل عاجزا عن مواكبة هذه النوعية من الجرائم وما يصاحبها من تطور مستمر فضلا عن تنامي أنواعها وانتشارها بشكل مريب وهو الأمر

الذى يحتم على المشرع سرعة اصدار قانون جديد يواجه الجرائم الالكترونية خاصة ان هناك بعض الجرائم المستحدثة التي لن تجد لها تكييفا قانونيا محددا في القانون التقليدي.

ويؤكد الكثير من رجال القانون على ضرورة إنشاء محكمة رقمية لسد الفجوة القانونية التي أحدثها التطور التكنولوجي الهائل في السنوات الأخيرة، فهناك جرائم ترتكب، وحرمات تنتهك، وحقوق تسلب على شبكة الشبكة الدولية للمعلومات " 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 الرقمية تتطلب إصدار تشريعات متخصصة في مجال مكافحة الجريمة الإلكترونية، فضلا عن توفير القضاة المتميزين للقيام على أعمال الفصل فى القضايا المطروحة على هذه المحاكم.

هذا ويلزم للمجتمع المعلوماتي في مجال قانون الاجراءات الجنائية أن ينشئ قواعد قانونية حديثة بحيث تضع معلومات معينة تحت تصرف السلطة المهيمنة على التحقيق فى مجال جرائم الشبكة الدولية للمعلومات " الإنترنت" وشبكات التواصل الإجتماعي. والسبب فى ذلك أن محترفي انتهاك شبكات الحاسبات الآلية ومرتكبي الجرائم الاقتصادية وتجار الأسلحة والمواد المخدرة يقومون بتخزين معلوماتهم في أنظمة تقنية المعلومات وعلى نحو متطور. وتصطدم الأجهزة المكلفة بالتحقيق بهذا التكنيك لتخزين المعلومات وهي التي 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 في دولة معينة بينما يتحقق نتيجة هذا الفعل الاجرامي في دولة أخرى، وهو الأمر الذي استلزم ضرورة وجود تعاون دولي محكم في مجال مكافحة هذا النوع من الجرائم ولأجل توفير حماية حقيقية لأنظمة الاتصالات.

ونظرا للخطورة التي تمثلها الجرائم الرقمية فقد تناول البحث التشريع الأمريكي، حيث ركز على جريمة العدوان على الإئتمان الرقمي وجرائم الأخلاق، ومنها جريمة الترويج السمعي-المرئي الفاضح، وجريمة البث العلني وتشمل السب والقذف والتشهير والمراسلة باعتبار أن هذه جميعا تدخل في عداد الجرائم الإلكترونية التي تستحق المواجهة التشريعية والتعاون الدولي لمواجهتها.

توصيات الدراسة

على أية حال فإنه في سبيل الحد من جرائم تقانة المعلومات، فيجب على المشرع الكويتي ان يضع في الاعتبار المقترحات والحلول اللآتية:-

١- ضرورة تقنين قواعد جديدة لمكافحة الجرائم المعلوماتية بدولة الكويت؛ تأخذ بعين الاعتبار الطبيعة الخاصة لهذه الجرائم ولاسيما فيما يتعلق بالإثبات في الدعاوى الناشئة عن هذه الجرائم ؛ سواء في ذلك الدعاوى الجنائية والمدنية والتأديبية. كما ينبغي تعديل قواعد الإجراءات الجنائية لتتلاءم مع هذه الجرائم.

٢- ضرورة التنسيق والتعاون الدولي بين دولة الكويت والدول الأخرى قضائيا وإجرائيا في مجال مكافحة الجرائم المعلوماتية .

٣- ضرورة تخصيص وتعيين ذوي المؤهلات الفنية في مجال جهاز الحاسب الألي والأنترنت خاصة في إدارة مكافحة الجرائم الألكترونية ؛ وذلك من رجال الشرطة المدربين على كيفية التعامل مع أجهزة جهاز الحاسب الآلي والإنترنت.

٤- يتعين تدريب وتحديث رجال الادعاء العام بدولة الكويت – أو النيابة لعامة – والقضاء بشأن التعامل مع أجهزة جهاز الحاسب الآلي والشبكة الدولية للمعلومات " الإنترنت" .

٥- ينبغي أن تنص التشريعات الكويتية على اعتبار أن الشبكة الدولية للمعلومات " الإنترنت" يعتبر وسيلة من وسائل العلانية في قانون الجزاء والقوانين ذات الصلة بالجرائم المعلوماتية ؛ مع الأخذ بعين الاعتبار أن الشبكة الدولية للمعلومات " الإنترنت" أوسع انتشارا من سائر وسائل النشر والعلانية الأخرى.

٦- يلزم تعديل قوانين ونظم الإجراءات الجزائية (الجنائية) بدولة الكويت ؛ 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 بدولة الكويت بضبط البريد الإلكتروني وأية تقنية أخرى قد تفيد في إثبات الجريمة والحصول على دليل ؛ والكشف عن الحقيقة .

٨- يلزم أن تمتد إجراءات التفتيش بدولة الكويت 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 العامة – في هذا الشأن – الضرورة تقدر بقدرها .

٩- يتعين أن تكون للسلطات القائمة بالضبط والتفتيش بدولة الكويت : سلطة توجيه أوامر لمن تكون لديه معلومات خاصة للدخول على ما يحويه الحاسب الآلي والشبكة الدولية للمعلومات " الإنترنت" من معلومات للإطلاع عليها .

١٠- ضرورة النص صراحة في القوانين المنظمة للإثبات – الجنائي والمدني بدولة الكويت – بما يسمح للقاضي بأن يستند إلى الأدلة المستخرجة من الحاسب الآلي والشبكة الدولية للمعلومات " الإنترنت" 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 النص صراحة في القانون الكويتي على تجريم الدخول غير المصرح به على البريد الإلكتروني لإتلاف محتوياته أو إرسال صور إباحية أو تغيير محتواه أو إعاقة الرسائل أو تحويرها عبر الشبكة الدولية للمعلومات " الإنترنت" .

١٢- ضرورة سن التشريعات الكويتية لمكافحة جرائم الإنترنت، وذلك بإدخال كافة صورالسلوك الضار والخطر على المجتمع التي يستخدم فيها انترنت .

١٣- يتعين اتاحة الفرصة للمواطنين في المشاركة في مكافحة الجرائم المعلوماتية ؛ وذلك من خلال إيجاد خط الساخن يختص بتلقي البلاغات المتعلقة بهذه الجرائم؛ ولاسيما الجرائم الأخلاقية .

١٤- ضرورة نشر الوعي بين صفوف المواطنين – ولاسيما الشباب الكويتي– بمخاطر التعامل مع المواقع السيئة علي شبكة الشبكة الدولية للمعلومات " الإنترنت" ؛مع ضرورة نشر الوعي المجتمعي بالمخاطر النفسية والاجتماعية وغيرها الناجمة عن الاستخدامات غير الآمنة للانترنت وتكثيف التوعية عن الآثار السلبية الصحية.

١٥- يتعين إدخال مادة "أخلاقيات استخدام الانترنت" ضمن المناهج الدراسية في التعليم الكويتي ماقبل الجامعي .

١٦- إنشاء قسم جديد بكليات الحقوق بالجامعات الكويتية لدراسة الحماية القانونية للمعلوماتية أو تحت مسمى آخر "قانون المعلوماتية والانترنت" أو "قانون الحاسب الآلي والانترنت".

١٧- تفعيل دور المجتمع المدني الكويتي ولاسيما جمعيات النفع العام للقيام بدورها في وقاية الشباب من الوقوع في الممارسات الخاطئة للسلوكيات والممارسات الضارة أخلاقيا عبر شبكة الشبكة الدولية للمعلومات " الإنترنت" .

أهم المراجع

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.