التكييف الفقهي والقانوني لجرائم الانترنت

اعداد

د. عمر طه خليل
قسم القانون
كلية التراث الجامعة

د.عفاف بديع جميل
قسم علوم الحاسبات
كلية التربية للبنات – جامعة بغداد

المستخلص:

يناقش هذا البحث واحدة من أهم القضايا التي تقلق فقهاء الشرع والقانون في الوقت الحاضر تلك هي الجريمة المعلوماتية. فأتساع استخدام الحاسوب وما تبعه من استخدام الشبكة الدولية (الانترنت) وما نجم عنه من أنماط جديدة للسلوك الإجرامي لم يكن يتوقعه المشرع في معظم بلدان العالم. الامرالذي دفع بالدول الى الوقوف وقفة جادة لمعالجة هذه المشكلة. وللوقوف على أهمية هذه المشكلة وأبعادها القانونية والاجتماعية والاقتصادية ولغرض معالجتها، فقد جاء البحث في ثلاثة مباحث تلتها الخاتمة وجملة من التوصيات.

يتناول المبحث الأول ماهية جرائم الحاسب الآلي والإنترنت من خلال التعرض الى تعريفها وخصائصها. ثم ناقش المبحث الثاني ركني هذه الجريمة المادي والمعنوي أوضحنا في الركن الأول السلوك المعلوماتي التقليدي وغير التقليدي(الحديث). أما الركن الثاني فأوضحنا بصدده ان الجريمة المعلوماتية كباقي الجرائم قد تكون عمديه(توافر القصد الجنائي)، كما يمكن أن تكون غير عمدية (عن طريق الخطأ). أما المبحث الثالث فقد تناول التكييف الفقهي والقانوني لجرائم الإنترنت.

Abstract:

This research discuss on of the Most important matter which worrys the Specialists of legal thought at present time, It is Information Crime. The expansion of using computers and Internet results new styles of criminal behavior, which is unexpected in most of world countries. The research divided into three sections followed by conclusion and recommendations. Section one explains what is informational crime, through the discussion of its definition and charastoristics. Section two discusses physical and moral aspects of this Crime. The first explain traditional and moderm informational behaviour. The second considered this crime as other crimes may be intentional and non intertional crime.

The third section showed the juristic and legal adaptation for internet crimes.

تمهيد وتقسيم:

اصبح جهاز الحاسب الآلي يقاسم الإنسان حياته في نهاره وليله ونومه ويقظته، اذ يستخدم جهاز الحاسب الآلي في الطائرة، في المعمل، في القوات المسلحة، وفي المواصلات والاتصالات على نحو يمكن معه القول اننا نعيش ثورة الحاسب الآلي. وقد تعززت منظومة الحاسب الالي بالكمال بظهور شبكة المعلومات الدولية(الانترنت) والتي جعلت من العالم قرية صغيرة من حيث العلوم والمعارف والاحداث التي يمكن متابعتها في اي زمان ومكان، في لحظة حصول الحدث.

لايخفى عن الجميع ان للانترنت خدمات عديدة من أهمها[1]:

1. البريد الإلكتروني: لإرسال واستقبال الرسائل ونقل الملفات مع أي شخص له عنوان بريدي اليكتروني بصورة سريعة جداً لا تتعدى ثواني.
2. القوائم البريدية: تشمل إنشاء وتحديث قوائم العناوين البريدية لمجموعات من الأشخاص لهم اهتمامات مشتركة.
3. خدمة المجموعات الإخبارية: تشبه خدمة القوائم البريدية باختلاف أن كل عضو يستطيع التحكم في نوع المقالات التي يريد استلامها.
4. خدمة الاستعلام الشخصي: يمكن الاستعلام عن العنوان البريدي لأي شخص أو جهة تستخدم الإنترنت والمسجلين لديها.
5. خدمة المحادثات الشخصية: يمكن التحدث مع طرف آخر صوتا وصورة وكتابة.
6. خدمة الدردشة الجماعية: تشبه الخدمة السابقة إلا انه، وفي الغالب، يمكن لأي شخص ان يدخل في المحادثة، أو يستمع اليها، دون اختيار الآخرين.
7. خدمة تحويل أو نقل الملفات(FTP): لنقل الملفات من حاسب إلى آخر وهي اختصار لـ(File Transfere Protocol).
8. خدمة الأرشيف الإلكتروني(Archieve): تُمكّن البحث عن ملفات معينة قد تكون مفقودة في البرامج المستخدمة في حاسب المستخدم.
9. خدمة شبكة الاستعلامات الشاملة(Gopher): تفيد في خدمات كثيرة كنقل الملفات والمشاركة في القوائم البريدية حيث يفهرس المعلومات الموجودة على الشبكة.
10. خدمة الاستعلامات واسعة النطاق(WAIS): تسمى باسم حاسباتها الخادمة وهي أكثر دقة وفاعلية من الأنظمة الاخرى، حيث تبحث داخل الوثائق أو المستندات ذاتها عن الكلمات الدالة التي يحددها المستخدم ثم تقدم النتائج في شكل قائمة بالمواقع التي تحتوي المعلومات المطلوبة.
11. خدمة الدخول عن بعد(TELNET): تسمح باستخدام برامج وتطبيقات في حاسب آلي آخر.

12. الصفحة الإعلامية العالمية(World Wide Web): أو الويب (WEB) تجمع معاً كافة الموارد المتعددة التي تحتوي عليها الإنترنت للبحث عن كل ما في الشبكات المختلفة وإحضارها بالنص والصوت والصورة، وتعد الويب نظاماً فرعياً من الإنترنت، لكنها النظام الأعظم من الأنظمة الأخرى فهي النظام الشامل باستخدام الوسائط المتعددة.

ولما كان التشريع وليد الحاجة، فمن الطبيعي ان يصاحب هذا التقدم العلمي ظهور انماط جديدة من الجرائم تطويها القوانين العقابية القائمة، وتبدو نصوص هذه القوانين قاصرة عن ملاحقتها، ولهذا فأن اغلب التشريعات العقابية العربية لم تتطرق لجرائم جهاز الحاسب الالي الا نادرا، ولعل السبب في ذلك ان ثورة الحاسب الالي في البلدان العربية لم تتعدى عقدا ونيف، وان كان دخوله اليها قد بدأ قبل ذلك، بفترة زمنية طويلة، ففي تونس مثلا صدر اول قانون للتجارة الالكترونية عام ٢٠٠٠ ، وفي امارة دبي عام ٢٠٠٢ اما في مصر فقد صدر قانون التوقيع الالكتروني المصري برقم ١٥ لسنة ٢٠٠٢ ، وصدر ايضا قانون التجارة الالكترونية الاتحادي في دولة الامارات العربية عام ٢٠٠٦ ، و كذلك قانون العقوبات المعلوماتي الاماراتي ٢٠٠٦م. وفي العراق صدر قانون التوقيع الالكتروني ولم يفعل. اما في البلدان الاوربية وغيرها من الدول المتقدمة فأن الامر يختلف حيث الاعتماد على الحاسب الالي من عقدين واكثر وبصفة تكاد تكون مطلقة، ولذلك نجد ان هذه الدول قد خطت خطوات واسعة وجريئة لمواجهة هذا النمط الجديد من الجرائم، وهي الجرائم المسماة بالجرائم المعلوماتية (الالكترونية)، فعلى سبيل المثال قامت فرنسا بتقنين ذلك عام ١٩٨٨ ثم ادخلت تعديلات جوهرية في قوانينها العقابية بهذا الخصوص عام ١٩٩٤ ، غير ان الولايات المتحدة الامريكية قد سبقت فرنسا بهذا المضمار حيث ظهر قانون الحاسب الالي في ولاية تكساس ثم في ولاية الينوي، ثم القانون الفيدرالي لامريكا كلها، وهناك ايضا بروتوكول الاتحاد الاوربي الذي تلتزم بموجبه الدول الاعضاء عند التشريع لجرائم المعلوماتية[2].

المبحث الأول: مفهوم الجريمة المرتكبة عبر الانترنت:

- أشْتُقتْ كلمة الجريمة في اللغة من الجُرم وهو التعدي أو الذنب، وجمع الكلمة إجرام وجروم وهو الجريمة. وقيل:جَرَمَ يَجْرِمُ واجْتَرَمَ وأجْرَمَ فهو مجرم وجريم[3]. اما الالكترونية فهي التي تدخل مادة الالكترون في ادق العمليات الحسابية وباسرع وقت ممكن, وهو فرع من فروع الفيزياء.
- وعرَّفت الشريعة الإسلامية الجريمة بأنها: "محظورات شرعية زجر الله عنها بحد أو تعزير"[4].
- تعريف الجريمة الالكترونية قانونا: ان حداثة هذه الجرائم واختلاف النظم القانونية والثقافية بين الدول، جعلها ليست محلاً للاتفاق بين الباحثين حول مفهومها فالبعض يطلق عليها جرائم الحاسبات؛ في حين أن فريق ثان يطلق عليها الغش المعلوماتي؛ ويذهب فريق ثالث إلى استخدام

مصطلح الجرائم المعلوماتية(الالكترونية)؛ بل بعضها يتعلق يدخل ضمن زمرة الجرائم ضد الأشخاص كالقتل والتحريض عليه [5] او انتهاك الحريات والمعتقد او الاعتداء على الاعراض.

ومن هذه التعريفات:

- عرفها الخبراء من بلجيكا أن (جريمة الكمبيوتر) هي "كل فعل أو امتناع عمدي ينشأ عن الاستخدام غير المشروع لتقنية المعلوماتية ويهدف إلى الاعتداء على الأموال المادية أو المعنوية" [6].
- في حين يذهب الفقيه الفرنسي الأستاذ (Massa) إلى أن المقصود بالجريمة المعلوماتية "الاعتداءات القانونية التي ترتكب بواسطة المعلوماتية بغرض تحقيق الربح"[7].
- بينما يذهب رأي ثالث إلى أنها كل "فعل أو امتناع عمدي ينشأ عن نشاط غير مشروع لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة في الحاسب، أو التي تحوّل عن طريقه"[5].
- في حين يذهب رأي رابع وهو منظمة التعاون الاقتصادي والتنمية OCDE وضعت التعريف التالي للجريمة المعلوماتية من أنها "كل فعل أو امتناع من شأنه الاعتداء على الأموال المادية أو المعنوية يكون ناتجاً بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية "[8].
- عرفت الجريمة بصفة عامة على انها "كل فعل غير مشروع صادر عن ارادة ائمة يقرر له القانون أو تدبير احترازيا, وتعتمد الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الانترنت على المعلومة بشكل رئيسي"[9].

وبعد استقراء التعريفات نجد ان تعريف الجريمة الالكترونية اعتمد على اربع اسس مختلفة لتحديد مفهومها: الاول: على اساس وسيلة ارتكاب الجريمة. الثاني: على اساس توافر المعرفة بتقنية المعلومات. الثالث: على اساس موضوع الجريمة. الرابع: على اساس اتجاه ياخذ بدمج عدة تعاريف[10]. ويمكن التوصل الى استخلاص تعريف للجريمة المعلوماتية الالكترونية منها:

"كل استخدام، في صورة فعل أو امتناع، غير مشروع للتقنية المعلوماتية ويهدف إلى الاعتداء على أي مصلحة مشروعة سواء أكانت مادية أم معنوية".

خصائص الجرائم الالكترونية:

ان للجريمة المعلوماتية خصوصية تميزها عن غيرها من الجرائم التقليدية ويمكن اجمالها بالاتي:-

1- أن معظم جرائم الانترنت تم اكتشافها بالمصادفة؛ بل وبعد وقت طويل من حدوثها.

2- من الناحية النظرية يسهل ارتكاب الجريمة ذات الطابع التقني؛ كما يسهل إخفاء معالمها وصعوبة تتبع مرتكبيها اذ ان هذه الجرائم لا تترك أثرا لها بعد ارتكابها؛ علاوة على صعوبة الاحتفاظ الفني بآثارها إن وجدت[5].

3- من جهة الفاعل انه لا يشترط في عموم الجرائم ان يكون مرتكبها على قدر من الثقافة والمعلومات ولا على مستوى من التحصيل العلمي كجريمة السرقة والرشوة والتهريب وغيرها ، الا ان مرتكب الجريمة المعلوماتية يتميز غالبا بأنه يحتل مكانة عالية في المجتمع ويتمتع بقدر عالٍ من العلم والمهارة والقدرة الفنية ، بل والتخصص في مجال انظمة الحاسب الالي وكيفية تشغيله، الا ان هذا لا يمنع ان يكون المحترف غير المتعلم فاعلا لهذه الجريمة[11]. بالمقابل يصعب على المحقق التقليدي التعامل مع هذه الجرائم. والكشف عنها وإقامة الدليل على اثباتها اذ يستوجب الاستعانة بخبرة فنية عالية المستوى.

4- صعوبة اثبات الدليل الجنائي لاثبات الجريمة المعلوماتية والذي يختلف تماما عن الدليل الجنائي في الجريمة التقليدية، وذلك من حيث البيانات والمعلومات المدونة في جهاز الحاسب وكيفية اثباتها، سواء من حيث وسيلة الاثبات او القائم به، وما اذا كانت تتوافر لديه الخبرة الكافية ام لا، سيما وان اجهزة العدالة الجنائية خصوصا العربية غير مؤهلة لهذا الدور وهي بحق ثغرة يعتمد عليها المجرم المعلوماتي الذي يتسم بأنه مجرم ذكي في ذاته يعكس اعلى درجات المهارة في فنون التعامل مع الحاسب الالي، ويكفى للتدليل على خطورة هذا الامر ان بعضهم يتعامل مع هذا النوع من الجرائم بوصفه يمارس هواية لا حرفة، فالصعوبات التي تعترض تحصيل الدليل الجنائي في هذه الجرائم كثيرة ومتنوعة منها ما يتعلق بالدليل الجنائي ذاته، ومنها ما يتعلق بموضوع الجريمة، والاخر يتعلق بجهات الضبط القضائي او التحقيق الجنائي في هذه الجرائم، على انه يمكن القول بأن استحصال الدليل الجنائي في هذه الجرائم محكوم بضابطين:

الاول: ضرورة وجود قاعدة قانونية تقرر الاجراء القانوني الواجب اتباعه في مثل هذه الجرائم مع مراعاة طبيعتها الخاصة.

الثاني: ضرورة المعرفة الفنية والتأهيل المهني والتقني لرجال الضبط والتحقيق الجنائي[12].

5- من حيث محل الحماية الجنائية يتكون الكومبيوتر – بوصفه الهدف المباشر للاعتداء او وسيلة الاعتداء من دائرة جرائم المعلوماتية لترتد الى موقعها الطبيعي وهو موقع الجرائم التقليدية، على اساس ان هذه من كيانات تقنية مادية (يتعدد وصفها ومهامها من الوجهة التقنية) والاعتداءات على

هذه الكيانات تخرج الماديات مجسدة لمال منقول تنهض به قواعد ومبادئ ونصوص القانون الجنائي، اما الشق الثاني من مكونات الكومبيوتر فهو الشق المعنوي (الكيان المعنوي) (المعلومات والبرامج) ونصوص قانون العقوبات تقف قاصرة عن حماية هذا الكيان، وهناك من يرى[13] بأن هذا الكيان المعنوي عبارة عن مال الا انه يختلف عن غيره من الاموال بأنه غير قابل للنفاذ بكثرة الاستعمال، ثم انه مال تتلاشى قيمته بظهور الجديد من المعارف والتقنيات، وان استعمال هذا المال يكون على متسع فمن الممكن ان يستعمله العديد في ان واحد، اخذين بعين الاعتبار ان نفقات نقل هذا المال تكاد تكون ضئيلة جدا.

6- عولمة هذه الجرائم يؤدي إلى تشتيت جهود التحري والتنسيق الدولي لتعقب مثل هذه الجرائم؛ فهذه الجرائم هي صورة صادقة من صور العولمة؛ فمن حيث المكان يمكن ارتكاب هذه الجرائم عن بعد وقد يتعدد هذا المكان بين أكثر من دولة؛ ومن الناحية الزمنية تختلف المواقيت بين الدول؛ الأمر الذي يثير التساؤل حول: تحديد القانون الواجب التطبيق على هذه الجريمة[5] باعتبار محل الجريمة.

7- من حيث الدافع لارتكاب هذه الجريمة على ضوء المادة(٣٨) من قانون العقوبات العراقي لا يعتد بالباعث على ارتكاب الجريمة ما لم ينص القانون على خلاف ذلك، وهذا هو المبدأ العام، ولكن يعتد بالباعث متى ما نص القانون على ذلك وهذا ما حصل حين جعله المشرع اما ظرفا مشددا للعقاب او عذرا قانونيا مخففا له[14] واذا كان الدافع لارتكاب الجرائم التقليدية غير محدد ومختلف من حالة لاخرى ومن مجرم لاخر[15]. فأنه في نطاق الجريمة المعلوماتية هو قهر النظام اكثر من شهوة الحصول على الربح السريع الذي ينشده مرتكبو الجرائم التقليدية، وبغض النظر عن صحة ذلك فأنه ما اقترن الدافعان ببعضهما فأن حصيلة الجريمة تكون اكبر[16].

8- من حيث العنف المستعمل اذ تتسم هذه الجريمة بأنها اقل عنفا وخشونة من الجرائم التقليدية الأخرى كالسرقة والقتل، إذ إن ركنها المادي قد لا يتجاوز مجرد لمسات بسيطة لمفاتيح التشغيل لجهاز الحاسب الآلي او ملحقاته[2].

المبحث الثاني: اركان الجريمة المعلوماتية

ان للجريمة العادية اركان هي ذاتها للجريمة الإلكترونية تتمثل في: الركن المادي والمعنوي.

الأول: الركن المادي. جاء وفق احكام المادة(٢٨) من قانون العقوبات العراقي (سلوك اجرامي بأرتكاب فعل جرمه القانون او الامتناع عن فعل يأمر به القانون)، ويتكون الركن المادي للجريمة الالكترونية من السلوك الاجرامي و النتيجة و العلاقة السببية مع العلم أنه يمكن تحقق الركن المادي دون تحقق النتيجة، كالتبليغ عن الجريمة قبل تحقق نتيجتها، مثل انشاء موقع للتشهير بشخص معين دون طرح هذا الموقع

على الشبكة فرغم عدم تحقق النتيجة الا أنه لا مناص من معاقبة الشخص ويتخذ الركن المادي عدة صور بحسب كل جريمة. فمثلا:

- جريمة الغش المعلوماتي: الركن المادي فيها هو تغيير الحقيقة في مستند رسمي أو محرر رسمي، ولكن المستند هنا ليس مستند عادي يدخل ضمن أدلة الاثبات، بل هي عبارة عن تسجيلات الكترونية أو محررات الكترونية.
- جريمة الارهاب الالكتروني والمواقع الاباحية ومواقع القمار: الركن المادي في هذه الجرائم هو اطلاق المواقع التي تحث اما على الانضمام الى الجماعات الارهابية، كما تورد كيفية صنع القنابل اليدوية.

- أما المواقع الاباحية فتزود مواقعها بالصور و أفكار الشذوذ الجنسي و هناك مواقع تنشر فكرة الانتحار أو تشويه صورة الاسلام[17].

- أما مواقع القمار فهي لغسيل الأموال فالركن المادي هنا سلوك المجرم المعلوماتي في تزويد المواقع بالمعلومات اللازمة للانحراف أو القتل و هذا المجرم أقل من المخترق أو المتسلل، هذا فيما يخص السلوك الاجرامي أما النتيجة فهي الاثر المادي المتمثل في انحراف المجتمع و تدمير الأخلاق و المعتقدات وظهور عادات غريبة على المجتمع زيادة الى تفشي العنف فتصميم الموقع من طرف المجرم مرتبطة بالتاثيرات الخطيرة التي يتحمل عبؤها المجتمع من انحراف و هذا ما يعرف بالعلاقة السببية[18].

الثاني: الركن المعنوي. اذ الجريمة ليست كيانا ماديًا خالصًا قوامه الفعل وما يترتب عليه، بل هي فوق ذلك كيان نفسي، ذلك ان ماديات الجريمة لا تنشئ لمفردها مسؤولية، وهذا المنطق يسري على الجرائم المعلوماتية شأنها شأن اية جريمة اخرى، فلا بد ان ترتكب من شخص قادر على تحمل تبعة افعاله (مسؤول جزائيا) وبذلك لا يسأل عنها من لا يعترف لهم قانون العقوبات بهذه الصفة وهم من كان فاقد الادراك او الارادة م /٦٠ و ٦١ من قانون العقوبات العراقي ومن يكون تحت تأثير الاكراه م /٦٢ والضرورة م /٦٣ وصغير السن م /٦٤.[2] ويعرف الركن المعنوي بأنه العلم بعناصر الجريمة و ارادة ارتكابها و بالتالي يتكون هذا الركن من عنصرين هما العلم و الارداة. فالعلم هو ادراك الأمور على نحو مطابق للواقع، يسبق الارادة. والارداة هي اتجاه لتحقيق السلوك الاجرامي.

صور القصد الجنائي، منها القصد العام والقصد الخاص.

1- القصد الجنائي العام: هو الهدف الفوري و المباشرللسلوك الإجرامي و ينحصر في حدود تحقيق الغرض من الجريمة أي لا يمتد لما بعدها.

2- القصد الجنائي الخاص: هو ما يتطلب توافره في بعض الجرائم فلا يكفي بمجرد تحقيق الغرض من الجريمة بل هو ابعد من ذلك أي انه يبحث في نوايا المجرم بطرحنا السؤال: ما هو الهدف الذي يريد الجاني تحقيقه من الجريمة ؟[19].

فأي قصد يجب توافره في الجريمة الالكترونية ؟

إن المجرم الالكتروني يتوجه من أجل ارتكاب فعل غير مشروع أو غير مسموح مع عليهم هذا المجرم بأركان الجريمة و بالرغم من أن بعض المخترقين يبررون أفعالهم بأنهم مجرد فضوليون و أنهم قد تسللوا صدفة، فلا انتفاء العلم كركن للقصد الجنائي، كان يجب عليهم أن يتراجعوا بمجرد دخولهم و لايستمروا في الاطلاع على اسرار الافراد و المؤسسات لأن جميع المجرمين و الأشخاص الذين يرتكبون هذه الأفعال يتمتعون بمهارات عقلية و معرفية كبيرة تصل في كثير من الأحيان الى حد العبقرية. فالقصد الجنائي متوافر في جميع الجرائم الالكترونية دون أي استثناء و لكن هذا لايمنع أن هناك بعض الجرائم الالكترونية تتطلب ان تتوافر فيها القصد الجنائي الخاص مثل جرائم تشويه السمعة عبر الأنترنيت. أما جرائم نشر الفيروسات عبر الشبكة فهي تتوفر على القصد الجنائي الخـــاص فالمجرم يهدف الى تعطيل عمل الشبكة و في جميع الحالات المشرع هو من يختص بتحديد الحالات التي يشترط فيها توافر القصد الجنائي الخاص [19].

ومعلوم ان هناك تقسيم للجرائم يعتمد الركن المعنوي اساسا له، وبموجبه تكون الجرائم اما عمدية واما غير عمدية، وهذا ما اخذ به المشرع العراقي اذ بموجب المادة 33/ 1 من قانون العقوبات تكون الجريمة عمدية اذا قام الفاعل بتوجيه ارادته الى ارتكاب الفعل المكون للجريمة هاد فا الى نتيجة الجريمة التي وقعت او اي نتيجة جرمية اخرى، وبموجب المادة ٣٥ تكون الجريمة غير عمدية اذا وقعت النتيجة الجرمية بسبب خطأ الفاعل، فالفاعل هنا لم يقصد سوى ارتكاب السلوك دون ارادة لتحقيق النتيجة، اما في الجريمة العمدية فأن ارادة الفاعل تتجه لارتكاب الفعل ولاحداث النتيجة معا.

الفرع الاول: الجريمة المعلوماتية كجريمة عمدية

كان هناك تصور بأن المجرم يمتاز بالغباء والسذاجة وبالانحطاط الثقافي والفكري، الامر الذي يجعل منه انسانًا معاديًا للمجتمع بصفته ذو خطورة اجرامية ، لكن هذا التصور سرعان ما انهارت ركائزه بظهور بعض انواع الجرائم كغسيل الاموال والارهاب والاتجار بالاعضاء البشرية والجريمة المنظمة واستخدام وسائل التكنولوجيا الحديثة في ارتكاب الجرائم، واصبح الكثير ينظر للمجرم بأنه يتمتع بفكر وذكاء كبير وحض من التعلم والاختصاص، فالجرائم التي قوامها سرقة الاعضاء البشرية تتطلب دراية ومهارة في علم الطب، وكذلك غسيل الاموال التي تستدعي معرفة

اقتصادية عالية بالبيع والشراء وفطنة في اخفاء الطابع الغير شرعي لهذه الاموال وإظهارها بمظهرالمشروعية، وكذلك الامر فيما يتعلق بالجريمة المعلوماتية حيث تتطلب نصيبا من المعرفة التخصصية بالكومبيوتر والانترنت الامر الذي لا يتوافر للجميع في مجتمعنا، بل يتوافر لمن كان له قسط كبير من التعلم ونصيب من المتابعة المستمرة لكل ما هو جديد في وسائل الاتصالات الحديثة، بل ان الامر قد حدى بالبعض[20] للقول بأن اصابع الاتهام والخوف قد اتجهت نحو المتعلمين بسبب ظهور اجرام على نحو عالي من التخصص والتقنية المتطلبة في مرتكب الجريمة حيث وصل الامر الى الاستعانة بعلماء من اجل إرتكاب الجريمة، على انه اذا سكت الشارع عن بيان صورة الركن المعنوي فأنه يكون قد تطلب العمد، فكون الجريمة عمدية هو ا لاصل الا ما استثنى المشرع بنص خاص فتكون الجريمة غير عمدية، والجريمة المعلوماتية حسب المتصور لا تقع الا بصورة عمدية يسبقها التفكير والتأمل في الحصول على المعلومات واختراق الكومبيوتر والانترنت من اجل تحقيق المنفعة او الهدف المرسوم للجاني، فالكومبيوتر قد يكون الاداة المستخدمة لاجراء التزوير وقد يكون وسيلة للاستحواذ بغير حق على مبالغ نقدية من الارصدة او وسيلة لتدمير معلومات مخزونة على كومبيوتر اخر، او وسيلة لتدمير ذاكرة كومبيوتر ثاني بعد نقل ما فيه من معلومات محاولة لازالة اثار الجريمة، او استخدام الفايروسات للتدمير والاتلاف، وكذلك جرائم القذف او السب او التحريض على الفسق والفجور فكل هذه الجرائم تتطلب ارادة السلوك وارادة تحقيق نتائجه فهي عمدية اذن ولا نرى موجبا لتطلب القصد الخاص في مثل هذه الجرائم اذ ان القصد العام يكفي لقيامها، ولكن هل يتصور ان تكون الجر يمة المعلوماتية غير عمدية ؟.

الفرع الثاني: الجريمة المعلوماتية كجريمة غير عمدية

بموجب نص المادة ٣٥ من قانون العقوبات العراقي تكون الجريمة غير عمدية اذا وقعت النتيجة الاجرامية بسبب خطأ الفاعل سواء كان هذا الخطأ اهمالا او رعونة او عدم انتباه او عدم احتياط او عدم مراعاة للقوانين والانظمة والاوامر، وبصفة عامة تكون الجريمة غير عمدية اذا اراد الفاعل السلوك ولم تتجه ارادته للنتيجة الجرمية، ومن الممكن تصور حصول الجريمة المعلوماتية وفق هذه الصورة، فمن يعتمد على مهارته في تلافي متاعب ومشاكل الفايروسات واد ى ذلك لتدمير اجهزة الدائرة التي يعمل فيها نتيجة افراطه في استخدام جهاز الكومبيوتر العائد للدائرة بعمليات لحسابه الخاص، تكون مسؤوليته هنا غير عمدية، وكذلك الامر لمن يستخدم اقراص مرنة خاصة به ولم يتاكد من خلوها من الفايروسات في اجهزة دائرته و تسبب بذلك في نقل فايروسات لهذه الاجهزة او تسبب في تدميرها، وغيرها من الحالات. الا ان ما يجري عليه العمل هو ان جرائم المعلوماتية قد تخرج من نطاق التجريم لتدخل نطاق مخافة لوائح وتعليمات المؤسسات او الهيئات التي يعمل فيها مرتكب الفعل، وتعتبر خرقا لقواعد القانون الاداري الذي يكون بمنأى من الخضوع لمبدأ الشرعية الجزائية ، ذلك ان وصف الجريمة الادارية يطوي كل مخالفة لقواعد وواجبات

الوظيفة العامة، ومع ذلك فأن هذه الافعال قد تشكل جرائم جنائية وادارية في ان واحد وهذا ما يثير المسؤولية المدنية اذا تحققت شروطها و الحق الفعل ضررا بالمؤسسة كالاستيلاء على اموال المستثمرين وحرمان المؤسسة من الاستفادة من هذه الاموال التي يقوم بتشغيلها مقابل نسبة من الارباح[21].
بعضهم اضاف ركنا ثالثا وهو الركن الشرعي للجريمة الالكترونية.

وهناك عدة تقسيمات لانواع وصور الجرائم الالكترونية او المعلوماتية اشهرها تقسيمان

- التقسيم الاول[22، 23، 24]: ويشمل

اولا: الافعال ضد السرية والنزاهة وتوافر بيانات الحاسب او النظم

- جريمة الدخول غير المشروع إلى منظومة معلوماتية.
- جريمة الاستيلاء على بيانات الحاسوب.
- جريمة الاستنتاج الغير مشروع لبيانات الحاسوب اونظامه.
- جريمة شغل اسم موقع إلكتروني.
- جريمة إعاقة الوصول إلى الخدمة.
- جريمة اعتراض المعلومات.
- جريمة إنتاج أو توزيع أو امتلاك لأدوات إساءة استعمال الحاسوب مثل تصميم البرمجيات الخبيثة واستخدامها.
- جريمة إرسال البريد المزعج.
- جريمة الاحتيال او التزوير عن طريق الشبكة. او تزوير المحررات.

ثانيا: افعال ذات الصلة بالحاسوب ومحتوياته لمصالح شخصية او مادية او اذى

الجرائم الجنسية والممارسات غير الأخلاقية وتشمل: المواقع والقوائم البريدية الإباحية، المواقع المتخصصة في القذف وتشويه سمعة الاشخاص، استخدام البروكسي للدخول إلى المواقع المحجوبة، إخفاء الشخصية، إنتحال الشخصية(الفرد والموقع)، جريمة الاغراء أو استمالة الأطفال المتعلق بالحاسوب و جريمة الإنتاج أو توزيع أو حيازة المواد الإباحية عن الأطفال .

ثالثا: الجرائم المالية: وتشمل

1- جريمة الاستعمال غير المشروع لبطاقات الدفع وهي جرائم الحاسوب ذات الصلة بالهوية.
2- القمار عبر الإنترنت

3- تزوير البيانات

4- الجرائم المنظمة

5- تجارة المخدرات عبر الإنترنت

6- غسيل الاموال

رابعا: المواقع المعادية

خامساً: جرائم القرصنة: وتشمل

1- جريمة اختراق أساليب حماية البيانات.

2- جريمة زرع الفايروسات في حواسيب الضحايا عن طريق شبكة الانترنت.

ويمكن تقسيم الفيروسات إلى خمسة انواع [22]:

الأول: فيروسات الجزء التشغيلي للاسطوانة كفيروس (Brain) و(Newzeland)

الثاني: الفيروسات المتطفلة كفيروس (Cascade) وفيروس (Vienna).

الثالث: الفيروسات المتعددة الانواع كفيروس (Spanish-Telecom) وفيروس (Flip)

الرابع: الفيروسات المصاحبة للبرامج التشغيلية (exe) سواء على نظام الدوس أو الوندوز

الخامس: يعرف بحصان طرواده

سادساً: جرائم اختراقات أخرى لم تتطرق اليها الدراسة:

1. التجسس الإلكتروني و انتهاك حرمة الحياة الخاصة.
2. جريمة الأفعال ذات الصلة بالحاسوب التي تنطوي على خطاب الكراهية.
3. . جرائم ذوي الياقات البيضاء: الجرائم ترتكب من قبل الطبقة الراقية في المجتمع ذوي المناصب الادارية الكبيرة، وتشمل انواعا مختلفة من الجرائم كالرشوة والتلاعب بالشيكات والاختلاس والسرقة وتزوير العلامات التجارية للشركات العالمية ووضعها على منتجات محلية أو عالمية غير مشهورة وشراء المعلبات قبل انتهاء صلاحيتها واستبدال تاريخ صلاحيتها.
4. الجرائم الاقتصادية

- التقسيم الثاني لصور الجرائم: لم يستقر الفقهاء على معيار واحد لتصنيف الجرائم المرتكبة عبر الانترنت وذلك راجع الى تشعب هذه الجرائم، وسرعة تطورها، فمنهم من يصنفها بالرجوع الى وسيلة ارتكاب الجريمة، او دافع المجرم، او على اساس محل الجريمة، وعلى هذا الاساس سوف نعتمد في التقسيم على فروع ثلاثة هي الجرائم الواقعة على الاموال، ثم الجرائم الواقعة على الاشخاص, واخيرا الى اساس الجرائم الواقعة على امن الدول.

الفرع الاول: الجرائم الواقعة على الاموال[10]:

صاحب ظهور شبكة الانترنت تطورات كبيرة في شتى المجالات، حيث اصبحت معظم المعاملات التجارية تتم من خلال هذه الشبكة، مثل البيع والشراء، مما انجز عنه تطور وسائل الدفع والوفاء واضحت جزء لا يتجزأ من هذه المعاملات، وفي خضم هذا التداول المالي عبر الانترنت انتهز بعض المجرمين من اجل السطو عليها، حيث ابتكرت عدة طرق من اجل ذلك، على غرار السطو والسرقة، والتحويل الالكتروني غير المشروع للاموال وقرصنة ارقام البطاقات الممغنطة.

اولا: جرائم السطو على ارقام بطاقات الائتمان والتحويل الالكتروني غير المشروع للاموال

واكب استخدام البطاقات الائتمانية من خلال شبكة الانترنت واكبه ظهور الكثير من المتسللين للسطو عليها، باعتبارها نقودا الكترونية، خاصة من جهة ان الاستيلاء على بطاقات الائتمان امرا ليس بالصعوبة بماكان، فلصوص بطاقات الائتمان مثلا يستطيعون الان سرقة مئات الالوف من ارقام البطاقات في يوم واحد من خلال شبكة الانترنت ومن ثم بيع هذه المعلومات للاخرين.

تتم عملية التحويل الالكتروني غير المشروع للاموال من خلال الحصول على كلمة السر المدرجة في ملفات انظمة الكومبيوتر الخاصة بالمجني عليه، مما يسمح للجاني بالتوغل في النظام المعلوماتي وعادة ما يكون هؤلاء العاملين على ادخال البيانات في ذاكرة الجهاز او من قبل المتواجدين على الشبكة اثناء عملية تبادل البيانات، وتتم عملية التحويل الالكتروني غير المشروع للاموال باحد الطرق الموالية:

1- الاحتيال: يتم ذلك بطرق احتيالية يوهم من اجلها المجني عليه بوجود مشروع كاذب او يحدث الامل لديه بحصول ربح، فيسلم المال للجاني بطريق معلوماتي او من خلال تصرف الجاني في المال وهو يعلم ان ليس له صفة التصرف فيه، وقد يتخذ اسم او صفة كاذبة، تمكنه من الاستيلاء على مال المجني عليه فيتم التحويل الالكتروني للاموال وذلك من خلال اتصال الجاني بالمجني عليه عن طريق الشبكة او يتعامل الجاني مباشرة مع بيانات الحاسب فيستعمل البيانات الكاذبة التي تساعده في ايهام الحاسب والاحتيال عليه فيسلمه النظام المال[10]. وقد اشار قانون العقوبات العراقي في مواده 456-459 [25]، مبينا طرق الاحتيال كالكذب وانتحال الصفه والادعاء باداء خدمة عامة وخاصة وكلها طرق تقليدية ولم يشر الى جرائم الاحتيال باستخدام بطاقات الدفع الالكتروني اذ يعتمد نظام بطاقات الدفع الالكتروني على عمليات التحويل الالكتروني من حساب بطاقة العميل بالبنك المصدر للبطاقة الى رصيد التاجر او الدائن الذي يوجد به حسابه وذلك من خلال شبكة التسوية الالكترونية للهيئات الدولية "هيئة الفيزا كارد"، وتعطي بطاقة الدفع الالكتروني الحق للعميل بالحصول على السلع والخدمات على الشبكة عن طريق تصريح كتابي او تلفوني، بخصم القيمة على حساب بطاقة الدفع الالكتروني الخاصة به، وتتم العملية بدخول العميل او الزبون الى موقع التاجر ويختار السلع المراد شرائها ويتم التعاقد بملأ النموذج

الالكتروني ببيانات بطاقة الائتمان الخاصة بالمشتري، وامام التطور التكنلوجي اصبحت امكانية ايجاد مفاتيح البطاقات والحسابات البنكية بالطريق غير المشروع ممكنة عبر قنوات شبكة الانترنت[10]. اما تكييف حكمها في الشريعة الاسلامية فقد احالته الى ولي الامر.

2- القمار وغسيل الاموال عبر الانترنت:

يعد الفضاء الالكتروني من اكثر الاسباب التي تشجع على ممارسة القمار عبر الانترنت مقارن بممارستها على الكازينوهات في الواقع المادي، اذ يمنح الراغب فب ممارسة القمار من خلال الكازينزوهات الافتراضية، الخصوصية وخفاء الشخصية التي يبحث عنها الكثيرون، حيث يستطيع الشخص ممارسة القمار دون حتى ان يغادر غرفة نومه.

وكثيرا ما تتداخل عملية غسيل الاموال مع ممارسة القمار عبر شبكة الانترنت، مما زاد من انتشار اندية القمار الافتراضية، الامر الذي جعل مواقع الكازينوهات الافتراضية على الانترنت محل اشتباه ومراقبة، ومن البديهي ان ياخذ المجرمون باحدث ما توصلت اليه التقنية لخدمة انشطتهم الاجرامية ويشمل ذلك بالطبع طرق غسيل الاموال التي استفادت من عصر التقنية فلجأ الى الانترنت لتوسعة وتسريع اعمالها في غسيل اموالها غير المشروعة.

ساعدت شبكة الانترنت القائمون بعمليات غسيل الاموال بتوفير عدة مميزات منها السرعة الشديدة وتخطي الحواجز الحدودية بين الدول وتفادي القوانين التي قد تضعها الدول من اجل اعاقة هذا النشاط، وكذا تشفير عملياتهم مما يعطيها قدر كبير من السرية، وخاصة في تسهيل على مرتكبي جرائم غسيل الاموال نقلها الى اي مكان في العالم، من اجل استثمارها في اقليم اي دولة من العالم، واعطاء هذه الاموال الصبغة المشروعة[10]. اما القمار من الناحية القانونية فيمنع تداوله في المرافئ العامة دون ترخيص. واما في الشرع فيعد جريمة بذاته في النصوص القرانية الواردة، قال تعالى (انما الخمر والميسر والانصاب والازلام رجس من عمل الشيطان)[المائدة: 90] وعقوبته 40 جلدة وتضاعف حسب اجتهاد ولي الامر. واما غسيل الاموال فقد شرع قانون خاص للاموال الغير المشروعة اصدره برايمر سنة 2004م الا انه لم يفعل. واما حكمه شرعا فمنوط لولي الامر.

3- جريمة السرقة والأستيلاء على اموال البنوك:

تعرف السرقة بانها اختلاس شئ منقول مملوك للغير بدون رضاه بنية امتلاكه، وتتم سرقة المال المعلوماتي عن طريق اختلاس البيانات والمعلومات، والافادة منها باستخدام السارق للمعلومات الشخصية مثل الاسم، العنوان، الارقام السرية الخاصة بالمجني عليهم، والاستخدام الغير الشرعي لشخصية المجني عليه ليبدأ بها عملية السرقة المتخفية عبر الانتلانت بحيث تؤدي بالغير الى تقديم الاموال (الالكترونية او المادية) الى الجاني عن طريق التحويل البنكي[10].

تتجسد جريمة السطو على اموال البنوك عن طريق استخدام الشخص الحاسب الالي للدخول الى شبكة الانترنت والوصول غير المشروع الى البنوك والمصارف والمؤسسات المالي، وتحويل الاموال من تلك الحسابات الخاصة بالعملاء الى حسابات اخرى، وذلك بادخال بيانات غير حقيقية او تعديل او مسح البيانات الموجودة بقصد اختلاس الاموال او نقلها او اتلافها، وتقوم هذه التقنية على الاستيلاء على الاموال بكميات صغيرة جدا من الحسابات الكبيرة بحيث لا يلاحظ نقصان هذه الاموال[10]. واما حكمها الشرعي قال تعالى:(والسارق والسارقة فاقطعوا ايديهما)[البقرة: 13]. لكن بشروط وضوابط احترازية. وقد اشار المشرع العراقي على جرائم السرقة في قانون العقوبات في المواد439-450, مفصلا انواعها واحكامها كجرائم تقليدية ولم يتطرق الى السرقة الالكترونية وهو بحاجة الى تضمينها في نصوص قانونية.

4- تجارة المخدرات عبر الانترنت:

ظهرت في عصر الانترنت مخاوف من مواقع السوء، وهي المواقع المنتشرة عبر الانترنت والتي لا تتعلق بالترويج للمخدرات وتشويق النشئ لاستخدامها بل وتتعداه الى تعليم كيفية زراعة وصناعة المخدرات بكافة اصنافها وانواعها وبابسط الوسائل المتاحة. ويمكن للمراهق الانزواء في غرفته والدخول الى هذه المواقع ومن ثم تطبيق ما يقراه ويؤكد هذه المخاوف احد الخبراء التربوييون في بتسبيرج بالولايات المتحدة الامريكية والذي اكد انه ثمة علاقة يمكن ملاحظتها بين ثالوث المراهقة والمخدرات والانترنت[10]. وحكمها الشرعي يقاس المخدرات على المسكرات بطريق القياس. ومن الناحية القانونية فقد شرع في العراق بقانون خاص وهو قانون الاتجار بالمخدرات رقم 65 لسنة 1968 المعدل.

الفرع الثاني: جرائم واقعة على الاشخاص:

يعد الهدف الاول والاسمى لوضع القوانين وسن التشريعات، حماية سلامة الاشخاص من مختلف الانتهاكات التي قد يتعرضون لها، سواء في ابدانهم او في حياتهم الخاصة، او في سمعتهم وشرفهم.

تطور الامر بعد ذلك مع ظهور شبكة الانترنت، فرغم الفوائد التي اتت بها، والتسهيلات التي قدمتها في الحياة اليومية للفرد والمجتمع على حد سواء، الا انها اصبحت سلاح فتاك في يد المجرمين، بالاضافة الى ذلك فان المعلومات المتعلقة بالافراد متداولة بكثرة عبرها، مما يجعلها عرضة للانتهاك والاستعمال من طرف هؤلاء المجرمين، وجعلت سمعة وشرف الافراد مستباحة.

1- جريمة التهديد والمضايقة والملاحقة:

يقصد بالتهديد الوعيد بالشر، وهو زرع الخوف في النفس بالضغط على ارادة الانسان، وتخويفه من اضرار ما سيلحقه او سيلحق اشياء او اشخاص له بها صلة، ويعد تهديد الغير من خلال البريد الالكتروني واحدا من اهم الاستخدامات غير المشروع للانترنت، حيث يقوم الفاعل بارسال رسالة الكترونية للمجني عليه تنطوي على عبارات تسبب خوفا او ترويعا لملتقيها[10].

تتم في هذا النطاق جرائم الملاحقة عبر شبكة الانترنت باستخدام البريد الالكتروني او وسائل الحوارات الانية المختلفة على الشبكة، وتشمل الملاحقة رسائل تخويف ومضايقة، وتتفق مع مثيلاتها خارج الشبكة في الاهداف المجسدة في رغبة التحكم في الضحية، وتتميز عنها بسهولة امكانية اخفاء هوية المجرم علاوة على تعدد وسهولة وسائل الاتصال عبر الشبكة، الامر الذي ساعد في تفشي هذه الجريمة[10]. وحكمها الشرعي مناط لولي الامر. ومن الناحية القانونية فقد اعتبر التهديد احد الجرائم المنصوص عليها في قانون العقوبات العراقي في المواد 430-432 عقوبات. وهذا بالطريقة التقليدية، اما التهديد عبر الانترنت فاعتبر كوسيلة اثبات.

تجدر الاشارة الى ان طبيعة جريمة الملاحقة عبر شبكة الانترنت لا تتطلب اتصال مادي بين المجرم والضحية، ولا يعني باي حال من الاحوال قلة خطورتها، فقدرة المجرم على اخفاء هويته تساعده على التمادي في جريمته والتي قد تفضي به الى تصرفات عنف مادية علاوة على الاثار السلبية النفسية على الضحية.

2- انتحال الشخصية والتغرير والاستدراج:

يقصد بانتحال الشخصية ما يعمد اليه المجرم من استخدام شخصية شخص اخر للاستفادة من سمعته مثلا او ماله او صلاحيته، ولذلك فهذا سبب وجيه يدعو للاهتمام بخصوصية وسرية المعلومات الشخصية للمستفيدين على شبكة الانترنت، وتتخذ جريمة انتحال الشخصية عبر الانترنت احد الوجهين التاليين: انتحال شخصية الفرد وانتحال شخصية المواقع. ولقد سماها بعض المختصين في امن المعلومات جريمة الالفية الجديدة، وذلك نظرا لسرعة انتشار ارتكابها خاصة في الاوساط التجارية[10].

اما فيما يخص التغرير والاستدراج فغالب ضحايا هذا النوع من الجرائم هم صغار السن من مستخدمي الشبكة، حيث يوهم المجرمون ضحاياهم برغبتهم في تكوين صداقة على الانترنت والتي قد تتطور الى التقاء مادي بين الطرفين، ان مجرمي التغرير والاستدراج على شبكة الانترنت يمكن لهم ان يتجاوزوا الحدود السياسية فقد يكون المجرم في بلد والضحية في بلد اخر، وكون معظم الضحايا هم من صغار السن، فان كثير من الحوادث لا يتم الابلاغ عنها، حيث لايدرك الكثير من الضحايا انهم قد غرر بهم[10]. ان انتحال شخصية المقترن بمحرر سيكون تكييفه القانوني على تزوير المحررات. وقد اشار اليه قانون العقوبات العراقي في مواده 298-299 جنايات. وكذلك المادة 456 نصب واحتيال.

3- صناعة ونشر الاباحة:

اذا كان لشبكة الانترنت وجه ايجابي فان لها وجه سلبي ايضا، ومن هذه الاوجه وجود مواقع على شبكة الانترنت تحرض على ممارسة الجنس للكبار والصغار على حد سواء، وتقوم هذه المواقع بنشر صور

جنسية فاضحة للبالغين والاطفال، واذا كانت الدعوى لممارسة الجنس الموجه للبالغين يمكن ان تلاقي الرفض لتوافر تمام العقل لديهم، فان الوضع بالنسبة للطفل يختلف لصغر وعدم اكتمال نضجه العقلي[10].

تعد صناعة ونشر الاباحة جريمة في كثير من دول اعالم خاصة تلك التي تستهدف او تستخدم الاطفال، حيث يضر استغلال الاطفال المستخدمين في انتاج هذه المواد ويمثل اعتداءا عليهم في كل مرة يتم فيها عرض هذه الصور، وبهذه الطريقة يظهر كل الاطفال كاهداف للاستغلال الجنسي، ويتخذ الاستغلال الجنسي للاطفال على الانترنت اشكالا متعددة انطلاقا من الصور ووصولا الى التسجيلات المرئية للجرائم الجنسية العنيفة، وتستمر معاناة الضحايا حتى بعد انتهاء الاعتداء الفعلي الذي تعرضوا له بسبب امكان تناقل الصور على الانترنت الى ما لا نهاية. وينتمي معظم منتجي هذه المواد الى فئتين واسعتين: هم المتربصون جنسيا بالاطفال وكذلك مجموعات الاجرام المنظم التي تجذبها الارباح الطائلة المتاتية من الترويج التجاري لمثل هذه الصور، ولقد عرفت سنوات التسعينات انفجارا في انشاء المواقع الالكترونية التي شهدت اتساعا في الجرائم المخلة بالحياء، وذلك بنشر وتوزيع الرسائل والصور والافلام الاباحية التي تستعمل في عروضها اطفالا ونساء، فاكثر من 470000 موقع اباحي موجود تم التعرف عليها ما بين 2004-2006، واكثر من 600000 صورة لاطفال في وضعيات غير مشروعة[10]. حكمها شرعا مناطة لولي الامر. اوردها المشرع العراقي في قانون العقوبات تحت جريمة الفعل الفاضح المخل بالحياء، في المواد 400-404 عقوبات.

4- جرائم القذف والسب وتشويه السمعة:

تعد جرائم السب والقذف الاكثر شيوعا في نطاق الشبكة، فتستعمل للمساس بشرف الغير او كرامتهم واعتبارهم، ويتم السب والقذف وجاهيا عبر خطوط الاتصال المباشر او يكون كتابيا، او عن طريق المطبوعات، وذلك عبر المبادلات الالكترونية(بريد الكتروني، صفحات الويب، غرف المحادثة)[10].

يستعمل الجاني حسب القواعد العامة لجرائم القذف والسب عبارات بذيئة تمس وتخدش شرف المجني عليه، ومهما كانت الوسيلة المعتمده، مع علمه ام ما يقوم به يعد مساسا بسمعة الغير، بل ان ارادته اتجهت لذلك بالذات، وبالتطور اصبحت الانترنت احدى هذه الوسائل ان لم نقل اكثرها رواجا، فعادة ترسل عبارات السب والقذف عبر البريد الصوتي او ترسم او تكتب على صفحات الويب ما يؤدي بكل من يدخل هذا الموقع لمشاهدتها او الاستماع اليها، على صفحات الويب ما يؤدي بكل من يدخل هذا الموقع لمشاهدتها او الاستماع اليها، ويتحقق بذلك ركن العلنية الذي تطلبه الكثير من التشريعات في السب العلني، واذا لم يطلع عليها احد فانه يمكن تطبيق مواد السب او القذف غير العلني[10]. والحكم الشرعي للقذف الجلد. والسباب مناط حكمه لولي الامر. وقد اورد المشرع العراقي جرائم القذف والسب في مواده 433-435 عقوبات.

الفرع الثالث: جرائم واقعة على امن الدول:

استغلت الكثير من الجماعات المتطرفة الطبيعة الاتصالية للانترنت من اجل بث معتقداتها وافكارها، بل تعداه الامر الى ممارسات تهدد امن الدولة المعتدى عليها، خاصة المتمثلة في الارهاب والجريمة المنظمة، اللذان اخذا منحى في استعمال الانترنت، التي سمحت لهم في ارتكاب جرائم غاية في الفتك في حق المجتمعات والدول، بل الاخطر من ذلك اتاحت الانترنت للكثير من الدول ممارسة التجسس على دول اخرى، وذلك بالاطلاع على مختلف الاسرار العسكرية والاقتصادية لهذه الاخيرة، خاصة فيما يتعلق بالدول التي يكون بينها نزاعات، ويبقى المساس بالامن الفكري من بين اخطر الجرائم المرتكبة عبر الانترنت، حيث تعطي الانترنت فرصا للتاثير على معتقدات وتقاليد مجتمعات باكملها مما يسهل انشاء الفوضى. وهي مقننه في العراق بقانون خاص هو قانون امن الدولة نظرا لخطورته. لكن بشكله التقليدي والجرائم الالكترونية الماسة بامن الدولة تعتبر اداة للجريمة.

اولا- الارهاب:

اصبح الارهاب في الوقت الحاضر ظاهرة عالمية، ترتبط بعوامل اجتماعية وثقافية وسياسية وتكنلوجية افرزتها التطورات السويعة والمتلاحقة في العصر الحديث، فقد شهدت العقود الاخيرة من القرن العشرين بروز العديد من التنظيمات المسلحة والعمليات الارهابية في مختلف انحاء العالم. يتم بث ثقافة الارهاب عبر الانترنت عن طريق تاسيس مواقع افتراضية تمثل المنظمات الارهابية، وهي مواقع اخذة في الازدياد مع ازدياي المنظمات الارهابية، حيث تعلن عبر هذه المواقع تحملها مسؤولية احدى الهجمات التي ارتكبت، او بيانات تنفي او تعلق على اخبار صادرة عن منظمات او جهات دولية اخرى[10].

تجند الجماعات الارهابية الاخرى من خلال الانترنت عناصر ارهابية جديدة تساعدهم على تنفيذ اعمالهم الاجرامية، وهم في ذلك يعتمدون على فئة الشباب، خصوصا ضعاف العقل والفكر، فتعلن الجماعات الارهابية عبر مواقعها على الانترنت عن حاجتها الى عناصر انتحارية كما لو كانت تعلن عن وظائف شاغرة للشباب، مستخدمة في ذلك الجانب الديني، فدائما ما تصف الاهداف التي تستهدفها عملياتهم بالكافرة، وتقوم بدعوى الشباب الى الجهاد وحثهم على الاستشهاد في سبيل الله والفوز بالجنة[10]. وخطف واحتجاز الرهائن وتصويرهم وغير ذلك. وقد صدر في العراق قانون خاص بالارهاب.

ثانيا- الجريمة المنظمة:

تعرف الجريمة المنظمة بانها تعبير عن مجتمع اجرامي يعمل خارج اطار الشعب والحكومة ويضم بين طياته الاف المجرمين الذين يعملون وفقا لنظام بالغ الدقة والتعقيد ويفوق النظم التي تتبعها اكثر المؤسسات تطورا وتقدما، كما يخضع افرادها لقواعد قانونية سنوها لانفسهم وترفض احكاما بالغة القسوة

على من يخرج عن نظام الجماعة ويلتزمون في اداء انشطتهم الاجرامية بخطط دقيقة مدروسة يلتزمون بها ويجنون من ورائها الاموال الطائلة.

الجريمة المنظمة ليست وليدة التقدم وان كانت استفادت منه، فالجريمة المنظمة وبسبب تقدم وسائل الاتصال والتكنلوجيا اصبحت غير محددة لا بقيود الزمان ولا بقيود المكان، بل اصبح انتشارها على نطاق واسع وكبير واصبحت لا تحدها الحدود الجغرافية، كما استغلت عصابات الجريمة المنظمة الامكانيات المتاحة في وسائل الانترنت في تخطيط وتمرير وتوجيه المخططات الاجرامية وتنفيذ وتوجيه العمليات الاجرامية بيسر وسهولة.

اكتشفت جماعات الجريمة المنظمة استخدام التكنلوجيات بصفتها فرص للاستغلال وتحقيق ارباح غير مشروعة، وفطن المجرمون ايضا ان شبكة الانترنت تستطيع ان تؤمن فرصا جديدة وفوائد جمة للاعمال الغير مشروعة[10]. وهذه الجريمة في العراق تحتاج الى تقنين قانوني.

ثالثا- جريمة التجسس:

ينتج عن الاستخدام المتزايد للحاسبات الالية في العديد من المجالات، تجميع المعلومات بدرجة كبيرة في موضع واحد، ويؤدي هذا التخزين في الحاسبات المركزية الى سهولة التجسس عليها، وعلى المعلومات المخزونة فيها بمختلف درجات سريتها. يقصد بالتجسس في هذا الموضع هو الاطلاع على المعلومات خاصة الغير مؤمنة في جهاز اخر، وليس مسموحا لغير المخولين بالاطلاع عليها. سهلت شبكة الانترنت الاعمال التجسسية بشكل كبير، حيث يقوم المجرمون بالتجسس على الاشخاص او الدول او المنظمات او الهيئات او المؤسسات الدولية او الوطنية، وتستهدف عملية التجسس في عصر المعلومات ثلاث اهداف رئيسية، وهي: التجسس العسكري، والتجسس السياسي، والتجسس الاقتصادي. كما تمارس العديد من الدول التجسس باستخدام التقنية المعلوماتية، وهذه الانشطة تمارس من قبل دولة او دول اخرى، او من قبل الدولة على مواطنيها، او من قبل شركة على شركات اخرى منافسة[10]. وقد قننها المشرع العراقي في قانون العقوبات.

رابعا- الجرائم الماسة بالامن الفكري:

ينطوي الخوف من عواقب ثورة المعلومات والاتصال على تيار عاطفي خفي وقوي، يتمسك بثقافة وقيم ومفاهيم اخذت قاعدتها الاجتماعية والمادية والتربوية تتزعزع، وغدا باديا للعيان انها الليوم تترنح تحت وطأة قوى التكنلوجيا والمعلوماتية والاتصالية التي تلح علينا بالانفتاح بالمعرفة والصوت والصورة، واذا كنا قد تغيرنا عن ابائنا دون ضجة كبيرة كالحاصلة اليوم، فهل يمكن ان نتوقع غير ذلك بصدد اولادنا؟[10].

تتجسد الاجابة في ان الاحتمال الاكبر هو ان التغيير سيحصل، كما تنبئ وقائع تكنلوجيا المعلومات اليوم، وكما دهشنا بالتلفزيون وتخوفنا من اثاره على حياتنا لاول مرة، وتغيرنا رغم النقد والتردد، فليس هنالك ما يدعونا لاعتقاد غير ذلك بصدد ثورة المعلومات اليوم وخاصة الانترنت. وبناء على خصائص الشبكة العالمية للانترنت، التي منحت المستخدم االكثير من الخيارات، من خلال عدم خضوعها لاي رقابة، وعبورها للحدود الجغرافية بين الدول، ونموها السريع المتواصل، وامكانية مشاركة الجميع من مختلف دول العالم، مع ما تمنحه من القدرة على التخفي وعدم المواجهة نتيجة للافتراضية التي تعد من اهم خصائص هذه الشبكة، اضافة الى الكم الهائل من المعلومات التي يمكن الحصول عليها من عدة مصادر لايمكن التحكم فيها ومتابعتها او الاشراف عليها، كل ذلك جعل هذه الشبكة من اهم مقومات المجتمع المعلوماتي التي تؤدي الى الانحراف الفكري، من خلال تعرض الشخص الى الكثير من المؤثرات الفكرية التي تستخدم الشبكة العالمية للانترنت، وتهدد الامن بابعاده كافة[10]. وهذه الجريمة تحتاج الى تقنين في القانون العراقي.

انواع الجناة في جرائم المعلوماتية:

يمكن حصر أنواع الجناة في جرائم الحاسب الآلي في أربعة فئات:

الفئة الأولى: العاملون على أجهزة الحاسب الآلي في منازلهم نظرا لسهولة اتصالهم بأجهزة الحاسب الآلي دون تقيد بوقت محدد أو نظام معين يحد من استعمالهم للجهاز[26].

الفئة الثانية: المثاليون (Idealists)(المراهقين): وعادة ما يكونون غير مدربين او مهرة، وهم الشباب الذين تتراوح اعمارهم بين 13-26 سنة والذين يسعون الى الاعتراف الاجتماعي. وتمتاز افعالهم باتها تسبب الخراب عالميا ولكنها لا تذكر على المستوى الفردي[24].

الفئة الثالثة: الموظفون الساخطون على منظماتهم التي يعملون بها فيعودون إلى مقار عملهم بعد انتهاء الدوام ويعمدون إلى تخريب الجهاز أو إتلافه أو حتى سرقته[26].

الفئة الرابعة: فئة المتسللين (Hackers) ومنهم الهواة أو العابثون بقصد التسلية، وهناك المحترفين اللذين يتسللون إلى أجهزة مختارة بعناية ويعبثون أو يتلفون أو يسرقون محتويات ذلك الجهاز، وتقع اغلب جرائم الإنترنت حاليا تحت هذه الفئة بقسميها[26].

الفئة الخامسة:الجشع-المدفوع(Greed-motivated): وهذه الفئة عادة ما تكون عديمة الضمير وهم على استعداد لارتكاب اي نوع من الجرائم، طالما انها تجلب لهم المال. مثل العاملون في الجريمة المنظمة وهؤلاء يرتكبون الجرائم الخطيرة، وخاصة في جرائم اباحية الاطفال والقمار الالكتروني[24].

الفئة السادسة: الافتراضي-الارهابيون(The Cyber terrorists): يمكن مقارنة تهديد الارهاب الالكتروني بتهديدات السلاح النووي، والبكتريولوجي او الكيميانية. وهم المجموعة الاحدث والاكثر

خطورة. والدافع الاساسي لهم ليس المال فقط ولكن ايضا لديهم قضية ما والتي يدافعون عنها. وعادة ما ينغمسون في ارسال رسائل التهديد وتدمير البيانات المخزونة في الغالب في نظم المعلومات الحكومية لمجرد ان يسجلوا وجهة نظرهم. وهم لا يعملون داخل حدود الدولة، بل من اي مكان في العالم لذا يصعب اقتناصهم[24].

صعوبة الكشف عن الجريمة المعلوماتية واثباتها:

بخلاف ما يتصوره كثير من الباحثين والمختصّين في مجال مكافحة الجريمة المعلوماتية، فإن ظاهرة انتشار التشريعات والقوانين للحد من هذه الآفة أخذت في الازدياد في كثير من دول العالم. وأغلب هذه القوانين لم تأخذ في الاعتبار عند إنشائها ان الجريمة المعلوماتية تنشأ في بلد ليحدث اثرها في بلد آخر[27].

1- سهولة محو الادلة في زمن قصير: لا تحتاج جرائم الاعتداء على برامج ومعلومات الحاسب الالكتروني الى أي عنف او جثث او سفك للدماء او اثار اقتحام لسرقة الاموال، وانما هي بيانات ومعلومات تغير او تعدل او تمحي كلياً او جزئياً من السجلات المخزونة في ذاكرة الحاسب الالكتروني[28] وبهذا لا تترك اثر لها بعد ارتكابها، لذا يكون من الصعب اكتشافها ومن ثم تطبيق الجزاء الجنائي على مرتكبها.

2- مهارة التخزين الإلكتروني للمعطيات الذي يجعلها غير مرئية وغير مدركة بالعين المجردة: اذ ان هذه الجرائم لا تترك أي اثر خارجي ومرئي لها، ومما يزيد من صعوبة اثباتها، ارتكابها في الخفاء وعدم وجود أي اثر كتابي ملموس لما يجري خلال تنفيذها من عمليات وافعال اجرامية حيث يتم استخدام النبضات الالكترونية في نقل المعلومات[27، 28] .

3- تشفير البيانات المخزنة إلكترونياً أو المنقولة عبر شبكات الاتصال.

4- المجرمين الذين يخططون لمثل هذا النوع من الجرائم هم دائما اصحاب ذكاء ودهاء وخبرة ودراية واحتراف في مجال تقنية المعلومات وبالتالي فهم يخططون لهذه الجرائم بطرق محكمة تكفل نجاحهم في ارتكاب الجريمة وفرارهم من اعين السلطات كما يستخدم المجرمون المخططون لهذه الجريمة وسائل تقنية متطورة يصعب على الغير معرفتها والتعامل معها بالاضافة الى عدم ملائمة الادلة التقليدية في القانون الجنائي لاثبات هذه الجرائم[27، 28] . (فهي جرائم تحتاج إلى خبرة فنية ويصعب على المحقق التقليدي التعامل معها)، بالشكل الذي يوجب البحث عن ادلة جديدة وحديثة ناتجة من ذات الحاسب الالي، وهنا تبدأ صعوبات البحث والتحري عن الدليل، وجمع هذا الدليل، وتبدأ اشكالية قبوله ان وجد ومدى مصداقيته على اثبات جريمة تنصب على عناصر غير مادية معلومات وبرامج.

5- البعد الدولي: يجري النفاذ إلى أنظمه الحاسوب في أحد البلدان ويتم التلاعب بالبيانات في بلد آخر وتسجّل النتائج في بلد ثالث، ناهيك عن أنه يمكن تخزين أدلة الجريمة الإلكترونية في جهاز حاسوب موجود في بلد غير الذي ارتكب فيه المجرم فعله، بالتالي يستطيع المجرم الإلكتروني إخفاء هويته،

ونقل المواد من خلال قنوات موجودة في بُلدان مختلفة، في قارات مختلفة قبل الوصول إلى المرسَل إليهم، نتيجة القدرة على التنقل إلكترونياً من شبكة إلى أخرى والنفاذ إلى قواعد البيانات في قارات مختلفة، بحيث تقع الجريمة في عدة دول وتحكمها عدة قوانين وقواعد معنية بذلك، مما يشكل تحدياً أمام الجهات القضائية في تطبيق القانون ويزيد من صعوبة التحقيق فيها[27].

المبحث الثالث: التكييف القانوني والشرعي لجرائم الإنترنت

المطلب الأول: التكييف القانوني لجرائم الانترنت.

"يمكن النظر للانترنت كمهدد للأمن الاجتماعي وخاصة في المجتمعات الشرقية المحافظة، حيث أن تعرض مثل هذه المجتمعات لقيم وسلوكيات المجتمعات الأخرى قد تسبب تلوثا ثقافيا يؤدي إلى تفسخ اجتماعي وانهيار في النظام الاجتماعي العام لهذه المجتمعات. إن الاستخدام غير الأخلاقي واللاقانوني للشبكة قد يصل إلى مئات المراهقين والهواة مما يؤثر سلبا على نمو شخصياتهم النمو السليم ويوقعهم في أزمات نمو، وأزمات قيمية لا تتماشى مع النظام الاجتماعي السائد، وبخاصة عند التعامل مع المواضيع الجنسية وتقديم الصور والمواد الإباحية" [29].

والمخاطر الأمنية متجددة وليست قاصرة على وقت أو نوع معين، ومع دخول الكمبيوتر(الحاسب الآلي) الذكي إلى المنازل فان ذلك سيفتح الباب لأنواع متطورة من الجرائم كالجرائم الجنسية والمالية وغيرها والتي تستغل إمكانية برمجة الأجهزة المنزلية ووصلها بالحاسب الآلي وبشكبة الانترنت، كسرقة ارصدة البطاقات الائتمانية، والمعلومات والصور والافلام الشخصية وابتزاز اصحابها مثلا.

واستلزم التطور التقني تطورا في طرق إثبات الجريمة والتعامل معها، فالجرائم العادية يسهل غالبا تحديد مكان ارتكابها، بل أن ذلك يعتبر خطوة أولى وأساسية لكشف ملابسات الجريمة، في حين انه من الصعوبة بمكان تحديد مكان وقوع الحادثة عند التعامل مع جرائم الانترنت، لكون الرسائل والملفات الحاسوبية تنتقل من نظام إلى آخر في ثواني قليلة، كما انه لا يقف أمام تنقل الملفات والرسائل الحاسوبية أي حدود دولية أو جغرافية. ونتيجة لذلك فإن تحديد أين تكون المحاكمة وما هي القوانين التي تخضع لها أمر في غاية الحساسية والتعقيد خاصة وان كل دولة تختلف قوانينها عن الدولة الأخرى، فما يعتبر جريمة في الصين مثلا قد لا يعتبر جريمة في أمريكا والعكس صحيح، بل أن الأمر يصل إلى حد اختلاف قوانين الولايات المختلفة داخل الدولة الواحدة كما في الولايات المتحدة الأمريكية[30].

وأدى التطور التقني إلى ظهور جرائم جديدة لم يتناولها القانون الجنائي التقليدي، مما اجمع معه مشرعي القانون الوضعي في الدول المتقدمة على جسامة الجريمة المعلوماتية والتهديدات التي يمكن أن تنشأ عن استخدام الحاسب الآلي وشبكة الإنترنت، ودفعهم هذا إلى دراسة هذه الظاهرة الإجرامية الجديدة وما اثارته من مشكلات قانونية حول تطبيق القانون الجنائي من حيث الاختصاص القضائي ومكان وزمان ارتكاب

الجريمة حيث يسهل على المجرم في مثل هذه الجرائم ارتكاب جريمة ما في مكان غير المكان الذي يتواجد فيه أو الذي حدثت فيه نتائج فعله[31].

وتطوير القوانيين الجنائية وتحديثها امر يستغرق بعض الوقت فـ" هناك تعديلات كثيرة مطلوب ادخالها على التشريعات التي تتعامل مع الجريمة كي تأخذ في الاعتبار المعطيات الجديدة التي نشأت عن إستخدام الحاسب الآلي في مجال المعلومات وعن ظهور شبكات المعلومات العالمية"[32].

ولاقت جرائم الحاسب الآلي اهتماما عالميا فعقدت المؤتمرات والندوات المختلفة ومن ذلك المؤتمر السادس للجمعية المصرية للقانون الجنائي عام (1993م) الذي تناول موضوع جرائم الحاسب الآلي والجرائم الأخرى في مجال تكنلوجيا المعلومات وتوصل الي توصيات احاطت بجوانب مشكلة جرائم الحاسب الآلي الا انها لم تتعرض لجزئية هامة وهي التعاون الدولي الذي يعتبر ركيزة اساسية عند التعامل مع هذه النوعية من الجرائم[33].

وعقدة مؤتمرات لهذا الغرض منها المؤتمر الدولي الخامس عشر للجمعية الدولية لقانون العقوبات الذي عقد في البرازيل عام (1994م) والذي وضع توصيات حول جرائم الحاسب الآلي والانترنت والتحقيق فيها ومراقبتها وضبطها وركز على ضرورة ادخال بعض التعديلات في القوانين الجنائية لتواكب مستجدات هذه الجريمة وافرازاتها[34].

والتعاون الدولي مهم عند التعامل مع جرائم الإنترنت، كونه سيطور اساليب متشابهة لتحقيق قانوني واجراني لحماية شبكات المعلومات الدولية ،خاصة ان هذه الجرائم هي عابرة للقارات ولا حدود لها، وفي المقابل فان عدم التعاون الدولي سيؤدي إلى زيادة القيود على تبادل المعلومات عبر حدود الدول مما سيعطي الفرصة للمجرمين من الإفلات من العقوبة ومضاعفة أنشطتهم الإجرامية[35].

وتعتبر السويد أول دولة تسن تشريعات خاصة بجرائم الحاسب الآلي والانترنت، حيث صدر قانون البيانات السويدي عام (1973م) الذي عالج قضايا الاحتيال عن طريق الحاسب الآلي إضافة إلى شموله فقرات عامة تشمل جرائم الدخول غير المشروع على البيانات الحاسوبية أو تزويرها أو تحويلها أو الحصول غير المشرع عليها[33، 35].

وتبعت الولايات المتحدة الأمريكية السويد حيث شرعت قانونا خاصة بحماية أنظمة الحاسب الآلي (1976م – 1985م)، وفي عام (1985م) حدّد معهد العدالة القومي خمسة أنواع رئيسة للجرائم المعلوماتية وهي: (جرائم الحاسب الآلي الداخلية، جرائم الاستخدام غير المشروع عن بعد، جرائم التلاعب بالحوسب الآلي، دعم التعاملات الإجرامية، وسرقة البرامج الجاهزة والمكونات المادية للحاسب). وفي عام (1986م) صدر قانونا تشريعاً يحمل الرقم (1213) 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، وقد خولت وزارة العدل الأمريكية في عام (2000م) خمسة جهات منها مكتب التحقيقات الفيدرالي (FBI) للتعامل مع جرائم الحاسب الآلي والانترنت[33، 35، 36].

وتأتي بريطانيا كثالث دولة تسن قوانين خاصة بجرائم الحاسب الآلي حيث أقرت قانون مكافحة التزوير والتزييف عام (1981م) الذي شمل في تعاريفه الخاصة بتعريف أداة التزوير وسائط التخزين الحاسوبية المتنوعة أو أي أداة أخرى يتم التسجيل عليها سواء بالطرق التقليدية أو الإلكترونية أو بأي طريقة أخرى[33، 35].

وتطبق كندا قوانين متخصصة ومفصلة للتعامل مع جرائم الحاسب الآلي والانترنت حيث عدلت في عام (1985م) قانونها الجنائي بحيث شمل قوانين خاصة بجرائم الحاسب الآلي والانترنت، كما شمل القانون الجديد تحديد عقوبات المخالفات الحاسوبية، وجرائم التدمير، أو الدخول غير المشروع لأنظمة الحاسب الآلي، كما وضّح فيه صلاحيات جهات التحقيق كما جاء في قانون المنافسة (The Competition Act) مثلا الذي يخول لمأمور الضبط القضائي متى ما حصل على أمر قضائي حق تفتيش أنظمة الحاسب الآلي والتعامل معها وضبطها[33، 34، 35].

وفي عام (1985م) سنّت الدنمارك أول قوانينها الخاصة بجرائم الحاسب الآلي والانترنت والتي شملت في فقراتها العقوبات المحددة لجرائم الحاسب الآلي كالدخول غير المشروع إلى الحاسب الآلي أو التزوير أو أي كسب غير مشروع سواء للجاني أو لطرف ثالث أو التلاعب غير المشروع ببيانات الحاسب الآلي كإتلافها أو تغييرها أو الاستفادة منها [33، 35].

وكانت فرنسا من الدول التي اهتمت بتطوير قوانينها الجنائية للتوافق مع المستجدات الإجرامية حيث أصدرت في عام (1988م) القانون رقم (19-88) الذي أضاف إلى قانون العقوبات الجنائي جرائم الحاسب الآلي والعقوبات المقررة لها، كما تم عام (1994م) تعديل قانون العقوبات لديها ليشمل مجموعة جديدة من القواعد القانونية الخاصة بالجرائم المعلوماتية وأوكل إلى النيابة العامة سلطة التحقيق فيها بما في ذلك طلب التحريات وسماع الأقوال[31، 37].

أما في هولندا فلقاضي التحقيق الحق بإصدار أمره بالتصنت على شبكات الحاسب الآلي متى ما كانت هناك جريمة خطيرة، كما يجيز القانون الفنلندي لمأمور الضبط القضائي حق التنصت على المكالمات الخاصة بشبكات الحاسب الآلي، كما تعطي القوانين الألمانية الحق للقاضي بإصدار أمره بمراقبة اتصالات الحاسب الآلي وتسجيلها والتعامل معها وذلك خلال مدة أقصاها ثلاثة أيام [34].

وفي اليابان قوانين خاصة بجرائم الحاسب الآلي والانترنت ونصت تلك القوانين على انه لا يلزم مالك الحاسب الآلي المستخدم في جريمة ما التعاون مع جهات التحقيق أو إفشاء كلمات السر التي يستخدمها إذا ما كان ذلك سيؤدي إلى إدانته،كما أقرت عام (1991م) شرعية التنصت على شبكات الحاسب الآلي للبحث عن دليل [34].

كما يوجد في المجر وبولندا قوانين خاصة بجرائم الحاسب الآلي والانترنت توضح كيفية التعامل مع تلك الجرائم ومع المتهمين فيها، وتعطي تلك القوانين المتهم الحق في عدم طبع سجلات الحاسب الآلي أو إفشاء كلمات السر أو الأكواد الخاصة بالبرامج، كما تعطي الشاهد أيضا الحق في الامتناع عن طبع المعلومات المسترجعة من الحاسب الآلي متى ما كان ذلك إلى إدانته أو إدانة احد أقاربه. بل تذهب القوانين الجنائية المعمول بها في بولندا إلى ابعد من هذا حيث أنها تنص على أن لا يقابل ذلك أي إجراء قسري أو تفسيره بما يضر المتهم [34].

اما على مستوى الدول العربية فان الامارات العربية تعتبر اول دولة عربية تسن قوانين خاصة بجرائم الحاسب الآلي والانترنت، واما في الدول العربية كالعراق ومصروغيرها لا يوجد نظام قانوني خاص بجرائم المعلومات، إلا أن القانون يجتهد بتطبيق قواعد القانون الجنائي التقليدي على الجرائم المعلوماتية والتي تفرض نوعا من الحماية الجنائية ضد الأفعال الشبيهة بالأفعال المكونة لأركان الجريمة المعلوماتية.

ولا تزال في الامصار العربية يستندون قضاء في تحديد الجرائم الالكترونية وتكييف احكمها اعني العقوبة المناسبة لكل جريمة الى قانون العقوبات المقر للبلاد ويعتبر وسائل الاتصال الالكتروني كاداة الجريمة. واوصي ان الدول العربية بحاجة الى انشاء قوانين تواكب الجرئم الالكترونية والمعلوماتية المعاصرة ولايقتصر على القوانين التقليدية.

المطلب الثاني: التكييف الشرعي لجرائم الانترنت.

ان انواع الجرائم في الشريعة الاسلامية ثلاثة كما هو معلوم, جرائم الحدود والقصاص والتعازير. اما الاولى والثانية فمنصوص عليها وقد ذكر الشارع أصول الجرائم فيها, واما الثالثة أعني التعازير وهي عقوبة لـ جريمة ليس لها حد مقررفي الشرع ولم يترتب الشارع عليها قصاص ولا ديه. وترد في حقوق الله كما ترد في حقوق العباد ايضا, ويكون هذا الحق لولي الامر في تحديد ما يقرره من جرائم وما يرتب عليه من عقوبات, وذلك مقصود من الشارع لتحقق مرونة في التشريع . ويمكن تقسيم جرائم العازير ثلاثة أصناف, الاول جرائم ذكرت في النصوص الشرعية وحددت عقوبات لها الا انها لم تستوفي احد شروطها او اركانها فتحولت الى احكام تعزيرية كالسرقة او الزنا مثلا. والثانية جرائم ذكرها الشارع دون ان يحدد لها عقوبة كالتجسس والغش والرشوة والاحتكار وخيانة الامانة وغير ذلك. والثالثة جرائم لم يرد لها ذكر في النصوص الشرعية مثل المخدرات وتزييف العملة وتزوير المحررات وغير ذلك. وهذا النوع هو الاوسع بين الجرائم وذلك لتكون أحكام الشريعة الغراء ذات مرنة عالية وصالحة لكل زمان ولكل مكان. اذ اوكل الشارع الى ولي الامر انه هو من يقرر ان هذا النوع جريمة وهو من يحدد نوع العقوبة الرادعة لها شريطة ان يكون منظبطا بضوابط الشرع.

وقد تركت الشريعة الغراء الباب مفتوحا لتجريم الجرائم المستحدثة التي لم يرد حكما لها في مصادرالتشريع الاصلية كالكتاب والسنة والاجماع , فيلجأ الى المصادرالتبعية كالقياس, والمصلحة مراعات لمقاصد

التشريع, والاستحسان, والاستصحاب, وسد الذرائع وغيرها, مستعينين بالقواعد الفقهية المعتبرة بين المذاهب الفقهية كقاعدة " لا ضرر ولا ضرار" و "درء المفاسد مقدم على جلب المصالح" وغيرها. كل ذلك لتحقيق مرونة عالية في التشريع للوقائع والمستجدات لذا اناطت الامر الى ولي الامر في بناء الاحكام وتكييف العقوبة المناسبة مرعيا حاجيات عصره ومصالح بلاده.

ولعلنا لا نغفل العادات والتقاليد المستوحاة من شريعتنا الإسلامية وتقاليدنا العربية الأصيلة والتي تزرع بداخل المواطن الوازع الديني الرادع عن ارتكاب المخالفات والنواهي، ومع كل هذه الضوابط فالنفس أمارة بالسوء والشيطان يجري من ابن ادم مجرى الدم، فيجب أن يكون هناك ضوابط عقابية تحد من يضعف رادعه الإيماني ليجد الرادع السلطاني له بالمرصاد فان الله ليردع بالسلطان ما لا يردع بالقرآن.

الخاتمة:

وبعد، فهذا جهد المقل في محاولة لتحديد جرائم الانترنت المرتكبة أثناء استخدام الشبكة العنكبوتية،مع تكيفها قانونا وشرعيا، والتى أمل ان تساهم هذه الدراسة في مواجهة هذه الجرائم الحديثة والتعامل معها ومكافحتها، وفي طرح افتراضات تصورية تلفت انتباه الباحثين في العلوم الشرطية والعلوم الاجتماعية والعلوم الإنسانية، بشكل عام، إلى كثير من الظواهر السلوكية المتعلقة باستخدام الإنترنت، والتي تتطلب البحث والدراسة.

كما اتمنى لفت انتباه المعنيين والمسئولين عن الأجهزة والتنظيمات التربوية، والإعلامية، وخطباء المساجد، والمؤسسات العلمية، للمساهمة في مكافحة هذه الانماط الحديثة من الجرائم والحد منها، ولتحذير أولياء الأمور وكافة شرائح المجتمع من التعامل معها، ولبيان عظيم خطورتها بشكل عام.

واخيراً ارجوا ان اكون قد وفقت في ابراز الصورة الحقيقية لجرائم الانترنت، فإن كان ذلك فمن الله وحده وله الفضل والمنة، وان لم اوفق فمن نفسي والشيطان ولكن عذري انني اجتهدت ولكل مجتهد نصيب.

المراجع:

1-عرب، يونس. "موسوعة القانون وتقنية المعلومات ، دليل أمن المعلومات والخصوصية، جرائم الكمبيوتر والانترنت"، الجزء الأول، منشورات إتحاد المصارف العربية، الطبعة الأولى، 1421هـ.

2-غايب، محروس نصار. "الجريمة المعلوماتية". المعهد التقني، الانبار، 2011م.

3-ابن منظور، أبي الفضل جمال الدين محمد بن مكرم.(بدون). "لسان العرب" . بيروت: دار صادر. ص : 605. – 604

4-الماوردي، محمد حبيب.(1407هـ). "الاحكام السلطانية". القاهرة : دار التراث العربي. ص: 19.

5- العادلي,محمود صالح. "الجرائم المعلوماتية: ماهيتها وصورها ورشة العمل الإقليمية حول تطوير التشريعات في مجال مكافحة الجرائم الالكترونية". مسقط 2-4 ابريل 2006م.

6-عفيفي، كامل عفيفي. "جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون – دراسة مقارنة". - منشورات الحلبي الحقوقية - بيروت- 2003 - ص 32) .

7- www.arablaw/Download cyber crimes_General,doc

8-رستم, هشام محمد فريد. "قانون العقوبات ومخاطر تقنية المعلومات". مكتبة الآلات الكاتبة، أسيوط – مصر، 1995، ص 34 .

9- الكعبي, محمد عبيد. "الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الانترنت", دار النهضة العربية, القاهرة, ص 32

10- صغير, يوسف. "الجريمة المرتكبة عبر الانترنت". رسالة ماجستير، جامعة مولود معمري- تيزي وزو، 2013م.

11-الصغير, جميل عبد الباقي. "القانون الجنائي والتكنلوجيا الحديثة". الكتاب الاول، الجرائم الناشئة عن استخدام الحاسب الالي، ط1، دار النهضة العربية، القاهرة، ص8، 1992م.

12- حجازي,عبد الفتاح بيومي. "الدليل الجنائي والتزوير في جرائم الكومبيوتر والانترنت". دار الكتب القانونية، المحلة الكبرى، 2001م.

13-عيسى, حسام محمد. "نقل التكنلوجيا: دراسة من الاليات القانونية للتبعة الدولية". دار المستقبل العربي.

14-لاحظ نصوص المواد 128و المادة 135 من قانون العقوبات العراقي.

15-الحديثي، د. فخري عبد الرزاق. "شرح قانون العقوبات، القسم العام". مطبعة اوفسيت الزمان، بغداد ص11، 1992م.

16-السعيد، د. كامل. "دراسات جنائية معمقة في الفقه والقانون والقضاء المقارن". ط1، عمان، ص13، 2002م.

17- الرومي، محمد أمين. "جرائم الكمبيوتر و الانترنيت". دار المطبوعات الجامعية 2003 ،ص 182

18- والجي، عزيز. "أركان الجريمة الإلكترونية في القانون الجزائري". 2013م.

19- سليمان، عبد الله. "شرح قانون العقوبات - قسم عام الجزء الأول للجريمة". دار الهدى .

20-الداود, عبد المحسن. "التحديات الثقافية العلمية للامن العربي". ورقة عمل مقدمة الى المؤتمر العربي العلمي عن التعليم والامن، اكاديمية نايف العربية للعلوم الامنية ، ص8، 4-1999/10/6.

21-الحلو، ماجد راغب. "القانون الادارى وقانون الخدمة المدنية". دون سنة الطبع ودون مطبعة، ص254.

22-منشاوي، محمد عبد الله. "جرائم الانترنت من منظور شرعي وقانوني". 1423هـ.
http://www.khayma.com/education-technology/Study33.htm

23- الخن, محمد طارق. "جرائم المعلوماتية والاحكام الموضوعية والاحكام الاجرائية".

24- البداينة, ذياب موسى. "الجرائم الالكترونية المفهوم والاسباب". ورقة علمية مقدمة في الملتقى العلمي بعنوان الجرائم المستحدثة في ظل المتغيرات والتحولات الاقليمية والدولية، كلية العلوم الاستراتيجية، 2014م.

25-حياوي، نبيل عبد الرحمن. "قانون العقوبات رقم 111 لسنة 1969 وتعديلاته"، النسخة المنقحة، ط3. عام 1985م مع تعديلاته التشريعية وما اصابها من قرارات سلطة الائتلاف المؤقت سنة (2003م-2005م). المكتبة القانونية. بغداد.

26-محمد، عادل ريان. "جرائم الحاسب الآلي وأمن البيانات". العربي، 1995م. (440)، 74- 75.

27-العبادي، احمد بن عبد الرحمن. "دعاوى الجرائم الالكترونية وادلة اثباتها في التشريعات العربية بين الواقع والمامول". المؤتمر الثالث لرؤساء المحاكم العليا بالدول العربية، الخرطوم، 2012م.

28-الشكري، عادل يوسف عبد النبي. "الجريمة المعلوماتية وأزمة الشرعية الجزائية". جامعة الكوفة / كلية القانون، 2008
http://www.iasj.net/iasj?func=fulltext&aId=29515

29- البداينة، ذياب. "التطبيقات الاجتماعية للإنترنت". ورقة قدمت في الدورة التدريبية حول شبكة الإنترنت من منظور أمنى، أكاديمية نايف العربية للعلوم الأمنية، بيروت، لبنان, 1999م.ص 101.

30- Thompson, R. "Chasing after petty computer crime". IEEE Potentials, 18 (1), 20-22. 1999.

31-تمّام، احمد حسام طه. "الجرائم الناشئة عن استخدام الحاسب الآلي". القاهرة : دار النهضة العربية, 2000م. ص1-3.

32-داود، حسن طاهر. "الحاسب وامن المعلومات". الرياض : معهد الادارة العامة, 1421هـ .ص.68

33-عيد، محمد فتحي. "الإجرام المعاصر". الرياض : أكاديمية نايف العربية للعلوم الأمنية.1419هـ.

34-احمد، هلالي عبدالاله. "تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي". عابدين : النسر الذهبي للطباعة, 2000م. ص5 – 10.

35- الشنيفي، عبدالرحمن عبدالعزيز. أمن المعلومات وجرائم الحاسب الآلي. (ط1) الرياض : 1414هـ.

36-عبدالمطلب، ممدوح عبدالحميد, "جرائم استخدام الكمبيوتر وشبكة المعلومات العالمية: الجريمة عبر الإنترنت". الشارقة: مكتبة دار الحقوق.2001م.

37-شتا، محمد محمد. "فكرة الحماية الجنائية لبرامج الحاسب الآلي". الإسكندرية: دار الجامعة الجديدة للنشر. 2001م.