فعالية القوانين الوطنية والدولية في مكافحة الجرائم الإلكترونية

Effectiveness of National and International laws regarding Cyber Crimes

الدكتورة ليلى حسين

قسم القانون في الاكاديمية العربية في الدنمارك

مفردات البحث: الجرائم الإلكترونية، الاتفاقيات الدولية، التشريعات الوطنية.

إهـــــداء: إلى قدوة المدافعين عن حقوق الإنسان في كل زمان وفي كل مكان.

ملخص البحث:

يواجه العالم أخطر المشاكل، تتمثل في مشكلة الجرائم الإلكترونية، وحيث أصبحت هذه المشكلة أكثر إلحاحاً على حياة ونشاط الإنسان، لذا تنبهت دول العالم اليها وأسفر عن تظافر جهود الدول والمنظمات الدولية إلى عقد العديد من المؤتمرات وأبرام الاتفاقيات على المستوى الدولي والإقليمي والوطني من أجل مكافحة هذه الجرائم والحد منها.

تم اختيار موضوع البحث في هذا النطاق لأهميته، ولبيان وتحليل أهم الاتفاقيات والمؤتمرات والبروتوكولات الدولية والإقليمية. وحاولت الباحثة ايضاً إلقاء الضوء على مدى فعالية التشريعات الوطنية في التعامل مع هذا النوع من الجرائم.

Abstract:

The world faces the most dangerous problems which are represented by Cyber crimes. This problem has become more urgent for life and human activity. Most of the states realized this problem so they held many conferences and made many agreements at the global, regional and national levels to face the problem and reduce its effect.

This topic was chosen because of its importance and to gives details and analysis about the most important international conventions, conferences and international protocols on global and regional level. The researcher tried also throwing spotlight on national legislations dealing with such type of crimes.

مقدمة:

في ظل اتساع ثورة تقنية المعلومات والاتصالات وتأثيرها في كافة شؤون الحياة المختلفة لما لها من فائدة وأهمية مادية ومعنوية في توفير الوقت والجهد وسرعة وسهولة نقل المعلومات وتبادلها وتخزينها، وكان لها الوقع الكبير في تحريك عجلة التنمية الاقتصادية والاجتماعية والثقافية، والتي جعلت من العالم قرية صغيرة، وأخذت طابع الانتشار الواسع والتطور في مختلف أنحاء العالم، واثبت واقع الحال ان أهمية هذه الثورة ومنها شبكة المعلومات الدولية (World Wide Web)، والاستخدام المتزايد لمواقع التواصل الاجتماعي مثل موقع الفيس بوك (Face book) وموقع (Twitter) من الامور الحياتية المهمة وأداة مساعدة وفاعلة في تطوير وتنمية استراتيجيات المؤسسات الخاصة والعامة والأفراد وتمكنهم من التقدم، لذا كانت الدول المتقدمة سباقة في الاستفادة منها ومواكبتها، وأصبح من الصعوبة الاستغناء عنها. ورغم هذه الإيجابيات التي وفرتها هذه النظم التقنية والبرامج والشبكات الإلكترونية، لكن من المؤسف له أفرزت أنواعاً جديدة من الجرائم ألا وهي الجرائم الإلكترونية (cybercrimes) كجرائم القرصنة hacking والاختراق cracking تلك التي جلبت معها تجاوزات يقوم بها البعض لديهم من التسلح المعرفي في إستخدام هذه النظم والبرامج مستخدمين غالباً أساليب التخفي في الإيقاع بالضحايا، وكون هذه النظم مخزن أسرار فقد شكلت مخاطر لتهديدات أمنية إلكترونية وتعطيل عمل المراكز الحيوية العامة والخاصة والتسبب في الخسائر الاقتصادية الضخمة ليس على المستوى الوطني بل على المستوى الدولي، ولما كانت النصوص الجزائية القائمة لا تكفي لدرء هذه المخاطر، لذا فطن المشرع إلى ضرورة سن القوانين التنظيمية والإجرائية الخاصة لمكافحة الجرائم السيبرانية ضمنتها العديد من العقوبات الجنائية ألاصلية تصل إلى الإعدام كما في المادة (٢٥) من قانون مكافحة جرائم تقنية المعلومات لسلطنة عمان لعام ٢٠١١م، ألتي من شأنها توفير الحماية القانونية لمواجهة الجرائم الخطيرة كالجرائم المتعلقة بالإتجار أو الترويج للمخدرات أو المؤثرات العقلية. وحفلت العقود الأخيرة تقديم جهود دولية استثنائية لمحاربتها لأجل تقديم الحماية للأفراد وللمؤسسات في

القطاع الحكومي والخاص من مخاطر هذه الجرائم. وقد ارتأينا تقسيم البحث إلى ثلاثة مباحث تضمن المبحث الأول وصف الجريمة الالكترونية (cybercrime) والتعريف بها وأسبابها وخصائصها، وفي المبحث الثاني جاء موضوع مكافحة الجرائم الإلكترونية في ضوء القوانين الوطنية، أما المبحث الثالث تناول موضوع الجرائم الإلكترونية في إطار التشريعات والاتفاقيات الدولية، وتم ترتيب البحث وفق السياق الآتي:

- **مشكلة الدراسة**

تتمثل الإشكالية الرئيسية للدراسة من خلال طرح التساؤلات التالية:

- بيان المراحل التي مرت بها التشريعات الدولية والإقليمية والوطنية في تقنين الجرائم الإلكترونية؟ ومدى وفاء وفعالية هذه التشريعات في مكافحة هذه الجرائم الخطيرة، كالجرائم المتعلقة بالاستغلال الجنسي للأطفال، والجرائم الماسة بأمن الدولة، والجرام المتعلقة بالتهديدات الإرهابية؟

- **أهمية البحث**

تنبع أهمية هذه الدراسة من كونها تتناول التأثير السلبي للثورة المعلوماتية وما نتج عنها من جرائم إلكترونية، وفي إلقاء الضوء على جهود المشرع الدولي والوطني في تقنين هذه الجرائم، لذا نرى أن تطويق ومكافحة هذه الظاهرة الخطيرة وإيضاح مخاطرها هي ضرورة قانونية وواجب أخلاقي، ويستلزم منا البحث في القوانين والتشريعات والتوجهات الفقهية التي تصدت لها.

- **أهداف البحث**

تكمن الاهداف: ان الاهتمام بمكافحة الجرائم الالكترونية، تتطلب منا وضع إستراتيجية وإيجاد الحلول، منها التركيز على جانب ثقافة ووعي المجتمع وتبصيره بمخاطر هذه الجرائم، وذلك بمواصلة الأعمال البحثية بشأن الأبعاد القانونية والأخلاقية لاستخدام تكنولوجيا المعلومات والاتصالات، وهذا أهم حافز للبحث، ومنه تعزيز الجهود الوطنية والإقليمية والدولية في مكافحة هذه الجرائم.

- **منهجية البحث**

١. المنهج التحليلي، من خلال عرض وتحليل نماذج من القوانين الوطنية، والمؤتمرات والمعاهدات والإعلانات والبروتوكولات الدولية ألتي اهتمت بموضوع الجرائم الالكترونية .

٢. المنهج التاريخي وذلك بسرد بعض الوقائع والأحداث المتعلقة بموضوع البحث، والوقوف على المواثيق ذات العلاقة.

المبحث الأول
مقدِّمات تعريفيَّة

وصف الجريمة الالكترونية (cybercrime) والتعريف بها

المطلب الاول: تعريفات definitions

أولاً: تعريف الجريمة الالكترونية (cyber crime) على صعيد التشريعات الوطنية:

حاولت العديد من الأعمال الأكاديمية تعريف "الجريمة الإلكترونية"، ومع ذلك فلا تبدو التشريعات الوطنية، مهتمة بتعرف دقيق للمصطلح. فمن أصل حوالي ٢٠٠ مكون منبثقة من التشريعات الوطنية التي استشهدت بها البلدان في الرد على الاستبيان الدولي في تحديد معنى الجريمة الإلكترونية، أستخدم أقل من خمسة في المئة كلمة "جرائم الإلكترونية" في العنوان أو في السياق التشريعي وبدلا من ذلك فالاستخدام الأكثر شيوعا في التشريعات هو لمصطلح "جرائم الكمبيوتر"، و"الاتصالات الإلكترونية"، و"تكنولوجيا المعلومات"، أو الجريمة ذات التقنية العالية. وفي الممارسة العملية، فإن العديد من هذه المفردات من التشريعات والتي هي المدرجة في مفهوم الجريمة الإلكترونية، مثل الدخول غير المصرح به لنظام الكمبيوتر، أو التدخل في نظام الكمبيوتر أو البيانات، حيث لم تستخدم التشريعات الوطنية على وجه التحديد مصطلح "الجريمة الإلكترونية" في عنوان فعل أو قانون (مثل " قانون الجرائم الإلكترونية ")، ومن النادر أن يتضمن جزء التعريفات تعريف الجريمة، وعندما يضمن مصطلح" الجريمة الإلكترونية" كتعريف قانون كان التعريف العام له ببساطة باسم " الجرائم المشار إليها في هذا القانون.[١] وجاء تعريف الجريمة الالكترونية في قانون مكافحة الجرائم المعلوماتية السعودي، بتاريخ: ١٤٢٨/٣/٨هـ بأنها: (أي فعل يُرتكب متضمّنًا استخدام الحاسب الآلي أو الشبكة المعلوماتية بالمخالفة لأحكام هذا النظام). وفي قانون دولة الكويت رقم ٦٣ لسنة ٢٠١٥ في شأن مكافحة جرائم تقنية المعلومات جاء تعريف الجريمة المعلوماتية: (كل فعل يرتكب من خلال استخدام الحاسب الالي أو الشبكة المعلوماتية أو غير ذلك من وسائل تقنية المعلومات بالمخالفة لأحكام هذا القانون).

---

[١]. أ. د. ذياب موسى البداينة . مصدر سابق . ص ٥.

ثانيـاً: تعريـف الجريمـة الالكترونيـة (cybercrime) علـى صـعيد التشـريعات الدوليـة والإقليمية:

عـدد قليـل جـدا مـن الصـكوك القانونيـة الدوليـة أو الإقليميـة تعـرف الجريمـة الإلكترونيـة، فـلا اتفاقيـة مجلـس أوروبـا للجـرائم الإلكترونيـة (Council of Europe Cybercrime Convention)، واتفاقيـة جامعـة الـدول العربيـة (League of Arab States Convention، ولا مشروع اتفاقية الاتحاد الافريقي Union Convention Draft African)، علـى سـبيل المثـال، تضـمنت تعريفـا للجريمة الالكترونية لأغراض الصك، لقد عـرفت اتفاقيـة كومنولـث الـدول المسـتقلة مـن دون اسـتخدام مصـطلح " جـرائم الإلكترونيـة" فعرفـت ' الجريمـة المتصـلة بمعلومـات الحاسوب ' بأنها ' العمل الإجرامي الذي يستهدف معلومات الحاسوب (UNODC, 2013،).[٢] وقد تحدَّث الفقه القانوني المعاصر طويلًا حول التعريف العلمي القانوني للجريمة الإلكترونية، وتعدَّدت المدارس والاتجاهـات فـي ذلـك، ومـن أحسـن وأجمـع وأشـمل هـذه التعـاريف، تعريـف منظمـة التعـاون الاقتصـادي والتنميـة (OCDE)؛ إذْ عَرَّفـت الجريمـة المعلوماتيـة فـي اجتمـاع بـاريس عـام (١٩٨٣م) بأنها: (كل سلوك غير مشروع أو غير أخلاقي أو غير مصرَّح بـه، يتعلَّق بالمعالجة الآليّة للبيانات أو نقلها).[٣]

ثالثاً: تعريف الجريمة الالكترونية لدى الفقهاء

١. عرفهـا الفقيـه الالمـاني تاديمـان بأنهـا: (هـي كـل اشـكال السـلوك غيـر المشـروع او الضار بالمجتمع والذي يرتكب باستخدام الحاسب الالي).
٢. ويعرفها الفقيه الفرنسي Masse بأنها: (الاعتداءات القانونية التي ترتكب بواسطة المعلوماتية بغرض تحقيق ربح).[٤]
٣. ويعرفهـا الفقيهـان الفرنسيان Le stanc, Vivant بأنهـا : "مجموعـة مـن الأفعـال المرتبطة بالمعلوماتية والتي يمكن أن تكون جديرة بالعقاب". [٥]

---

[2] . أ. د. ذياب موسى البداينة . مصدر سابق .ص ٦.

[٣] . «دعـاوى الجـرائم الإلكترونيـة وأدلـة إثباتهـا فـي التشـريعات العربيـة بـين الواقـع والمـأمول»، ضـمن فعاليـات المؤتمر الثالث لرؤساء المحاكم العليا (النقض، التمييز، التعقيب) في الدول العربية المنعقد في جمهورية السودان الشقيقة خلال الفترة ٢٣-٢٥/٩م الموافق ٧-٩/١١/١٤٣٣هـ.ص ٣.

[٤] . أ . عادل يوسف عبد النبي الشكري، الجريمة المعلوماتية وأزمة الشرعية الجزائية،مجلة ـ العراق ـ جامعة الكوفة ـ العدد السابع ٢٠٠٨.نقل بتصرف ص ١١٣.

وتعرف الباحثة الجريمة الالكترونية من الجانب القانوني: " كل سلوك ضار سواء على مستوى القطاع العام أم الخاص أم الأفراد، يعاقب عليه القانون يرتكب عبر الشبكات المعلوماتية".

المطلب الثاني: خصائص الجرائم الالكترونية

فيما يلي مجموعة من خصائص الجرائم الإلكترونية والتي تؤدي إلى ارتكابها، منها:

١. الازالة (Removable). الجريمة الإلكترونية لا تتطلب الإزالة فيمكن نسخها فقط.
٢. التوافر (Available). المعلومات في كل مكان، جاهزة لتستهدف من الجريمة.
٣. القيمة (Valuable). معلومات بطاقات الائتمان والحسابات المصرفية والتصاميم... قيمة.
٤. المتعة (Enjoyable). كثير من الجرائم الإلكترونية ممتعة من مثل سرقة الموسيقى والمال.
٥. الديمومة (Durable). المعدات والبرامج المسروقة يمكن أن تستخدم لفترة طويلة.
٦. سرعة التنفيذ: لا يتطلب تنفيذ الجريمة الإلكترونية الوقت الكثير وبضغطة واحدة على لوحة المفاتيح يمكن أن تنتقل ملايين الدولارات من مكان إلى آخر. وهذا لا يعنى أنها لا تتطلب الإعداد قبل التنفيذ أو استخدام معدات وبرامج معينة.
٧. التنفيذ عن بعد: لا تتطلب الجريمة الإلكترونية في أغلبها (إلا جرائم سرقة معدات الحاسب) وجود الفاعل في مكان الجريمة بل يمكن للفاعل تنفيذ جريمته وهو في دولة بعيدة عن مكان الجريمة سواء كان من خلال الدخول للشبكة المعنية أو اعتراض عملية تحويل مالية أو سرقة معلومات هامة أو تخريب، الخ.
٨. إخفاء الجريمة: إن الجرائم التي تقع على الحاسبات الآلية أو بواسطتها (كجرائم الإنترنت) جرائم مخيفة، إلا أنه تلاحظ آثارها والتخمين بوقوعها.
٩. الجاذبية: نظرا لما تمثله سوق المعلومات والحاسب والانترنيت من ثروة كبيرة للمجرمين أو للإجرام المنظم فقد غدت أكثر جذباً لاستثمار الاموال وغسيلها وتوظيف

---

٥. د. يونس حرب - جرائم الكمبيوتر والانترنت- ايجاز في المفهوم والنطاق والخصائص والصور والقواعد الاجرائية للملاحقة والاثبات- ورقة عمل مقدمة الى مؤتمر الامن العربي ٢٠٠٢ – تنظيم المركز العربي للدراسات والبحوث الجنائية - ابو ظبي ١٠-١٢ /٢٠٠٢/٢. بحث منشور - ص ٤.

الكثير منها في تطوير تقنيات واساليب تمكن الدخول الى الشبكات وسرقة المعلومات وبيعها أو سرقة البنوك أو اعتراض العمليات المالية وتحويل مسارها أو استخدام أرقام البطاقات ... ألخ .

١٠. عابرة للحدود الدولية (Transnational): إن ربط العالم بشبكة من الاتصالات من خلال الأقمار الصناعية والفضائيات والإنترنت جعل الانتشار الثقافي وعولمة الثقافة والجريمة أمرا ممكنا وشائعا لا يعترف بالحدود الإقليمية للدول، ولا بالمكان، ولا بالزمان، أصبحت ساحتها العالم أجمع.

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

١٢. صعوبة إثباتها: تتميز عن الجرائم التقليدية بأنها صعبة الإثبات، وهذا راجع إلى افتقاد وجود الآثار التقليدية للجريمة، وغياب الدليل الفيزيقي (بصمات، تخريب، شواهد مادية) وسهولة محو الدليل أو تدميره في زمن متناه القصر، يضاف إلى ذلك نقص خبرة الشرطة والنظام العدلي وعدم كفاية القوانين القائمة (البحر، ١٩٩٩).[٦]

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

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

١٥. عولمة هذه الجرائم يؤدي إلى تشتيت جهود التحري والتنسيق الدولي لتعقب مثل هذه الجرائم ؛ فهذه الجرائم هي صورة صادقة من صور العولمة؛ فمن حيث المكان يمكن

---

٦. أ. د. ذياب موسى البداينة . مصدر سابق . ص ١٩ ـ ٢٠ .

ارتكاب هذه الجرائم عن بعد وقد يتعدد هذا المكان بين أكثر من دولة؛ ومن الناحية الزمنية تختلف المواقيت بين الدول ؛ الأمر الذي يثير التساؤل حول: تحديد القانون الواجب التطبيق على هذه الجريمة.

١٦. صعوبة المطالبة بالتعويض المدني بخصوص جرائم الانترنت.[٧]

المطلب الثالث: صور ومجالات ارتكاب الجرائم المعلوماتية

أ - **صور ارتكاب الجرائم الالكترونية:** تتعدد صور ارتكاب الجرائم الالكترونية، فمنها ما يمس استقلال البلاد ويتعلق بالمحافظة على الأمن والاستقرار، ومنها ما يتعلق باستخدام الانترنت في ارتكاب جرائم الإتجار بالبشر والمخدرات والممارسات الجنسية والاحتيال والتزوير والقرصنة الالكترونية او يتعلق بالحقوق المالية للدولة او الشركات او الافراد. ونتناول في هذا الفرع من البحث صور الجرائم المعلوماتية:

اولا: جرائم الإرهاب الالكتروني: في كتاب الارهاب على الشبكة العالمية لجابريال ويمان Gabriel Weimann, Terror on the Internet, Potomac Books, Inc, April 2006، الذي صدر عن معهد السلام الامريكي في واشنطن تعرض بالتحليل لزيادة عدد المواقع الالكترونية التي تديرها المنظمات الارهابية على الانترنيت، فقد قفز عدد المواقع من ١٢ موقعاً عام ١٩٩٨ الى ٤٨٠٠ موقع في تاريخ صدور الكتاب (٢٠٠٦م) ما يعتبر مؤشرا لكثافة استخدام الارهاب للشبكة العالمية. والإرهاب تعددت وسائل ارتكابه للجريمة واضطر الارهابيون إلى استخدام اجهزة الحاسوب وشبكة المعلومات بقصد ارتكاب الجرائم التي تمس استقلال البلاد ووحدتها وسلامتها ومصالحها الاقتصادية أو السياسية أو العسكرية أو الامنية العليا من خلال اتلاف أو تعيب أو إعاقة اجهزة أو انظمة أو برامج أو شبكة المعلومات العائدة للجهات الامنية أو العسكرية أو الاستخباراتية بقصد المساس بأمن الدولة الداخلي أو الخارجي أو ارسال محتويات اجهزة الحاسوب إلى الجهات المعادية و استخدام مواقع بقصد تنفيذ برامج مخالفة للنظام العام أو الترويج لها أو تسهيل تنفيذها أو تنفيذ عمليات ارهابية تحت مسميات وهمية أو تسهيل الاتصال بقيادات واعضاء الجماعات الارهابية و الترويج للأعمال الارهابية وافكارها أو نشر عمليات تصنيع واعداد وتنفيذ الاجهزة المتفجرة أو الحارقة أو اية ادوات أو مواد تستخدم في التخطيط أو

[٧]. د. عبد العال الديربي - الجريمة المعلوماتية تعريفها أسبابها خصائصها. مصدر .

التنفيذ للأعمال الارهابية وان الجرائم الارهابية معاقب عليها وفق قانون مكافحة الإرهاب رقم ١٣ لسنة ٢٠٠٥. [٨]

ثانيا: جرائم الاتجار بالبشر عن طريق الانترنت: وتتمثل هذه الجريمة بأنشاء أو نشر موقع على شبكة الانترنت بقصد الاتجار بالبشر أو تسهيل التعامل به باي شكل من الاشكال أو روج له أو ساعد على ذلك أو تعاقد أو تعامل أو تفاوض بقصد ابرام الصفقات المتعلقة بالإتجار بالبشر.

ثالثا: تجارة المخدرات باستخدام الانترنت: ان المخاوف من استخدام الانترنت لا تقتصر على ارتكاب الانترنت في ارتكاب الجريمة بل تساهم بعض المواقع في انحراف الشباب وخصوصا من المراهقين وذلك من خلال انشاء مواقع الالكترونية بقصد الاتجار بالمخدرات أو المؤثرات العقلية أو الترويج لها أو تعاطيها أو سهل التعامل فيها أو تعاقد أو تعامل أو تفاوض بقصد ابرام الصفقات المتعلقة بالإتجار بها باي شكل من الاشكال.

رابعا: استخدام الانترنت في ارتكاب الجريمة المنظمة: وهي استخدام شبكة الانترنت بقصد اشاعة الفوضى بقصد اضعاف النظام أو الثقة بالنظام الإلكتروني للدولة أو اتلاف وتعطيل أو اعاقة أو الاضرار بأنظمة الحاسوب أو شبكة المعلومات العائدة للدولة بقصد المساس بنظامها أو البنى التحتية ونشر أو اذاعة وقائع كاذبة أو مظللة بقصد اضعاف الثقة بالنظام المالي الإلكتروني أو الاوراق التجارية والمالية الالكترونية وما في حكمها بقصد الاضرار بالاقتصاد الوطني والثقة المالية للدولة واستخدام الانترنت في ارتكاب جرائم غسيل الاموال حيث يأخذ المجرمون بأحدث التقنيات لغرض خدمة نشاطاتهم سيما وان جرائم غسيل الاموال عابرة للحدود.

خامسا: تزوير البيانات : وهي من الجرائم المعلوماتية الاكثر انتشارا فلا تكاد تخلو جريمة من جرائم نظم المعلومات من شكل من اشكال التزوير للبيانات من خلال تزوير أو تقليد أو اصطناع توقيع أو سند أو كتابة الكترونية أو ذكية أو اية وسيلة اخرى أو استعمال البطاقة الالكترونية المقلدة أو المزورة مع علمة بذلك أو اصطنع عمدا وثائق أو

[٨]. القاضي كاظم عبد كاظم الزيدي بحث بعنوان مكافحة الجرائم المعلوماتية في التشريع العراقي موقع السلطة القضائية الإتحادية ٢٠١٢/١٠/١٥.متاح على الرابط http://www.iraqja.iq/view.1645

سجلات أو قيود الكترونية أو احدث تغييرا أو تلاعبا في سند الكتروني صحيح و الاستيلاء عمدا على توقيع أو كتابة أو سند واستخدامها لمصلحته الشخصية.

سادسا: القرصنة الالكترونية: ويقصد بها النسخ الغير مشروع لنظم التشغيل للحاسب والدخول غير المشروع بقصد تدمير المواقع الالكترونية وكل من فك او نزع او اتلف تشفيرا لتوقيع الكتروني او اجهزة الحاسوب او شبكة المعلومات. [٩] وفي عام ١٩٨٤م كان عالم الكمبيوتر Fred cohen أول من استخدم مصطلح الفايروس للإشارة إلى كودة الاستنساخ الذاتي. [١٠] ومن الامثلة حادثة الفيروس أحبـــــك (I love you) الذي انتشر في كل أرجاء العالم عن طريق البريد الإلكتروني في خسائر قدرت بنحو ٧ مليارات دولار. [١١]

سابعا: انتحال الصفة عن طريق الانترنت: توجد الكثير من برامج الحاسوب تمكن المستخدم من اخفاء شخصيته وتتمثل هذه الجريمة بانتحال شخصية الفرد كذبا وانتحال شخصية المواقع بقصد ارتكاب الجريمة وجريمة تدمير المواقع الالكترونية واختراق المواقع الرسمية أو الشخصية واختراق الاجهزة الشخصية واختراق البريد الإلكتروني للأخرين والاستيلاء عليه والاستيلاء على الاشتراكات والارقام السرية للأخرين وارسال الفيروسات، ويعتبر الهجوم على المواقع المختلفة من الجرائم الشائعة في العالم (اختراق المواقع) وتخريب الحواسيب وقيام الفيروسات بمسح محتويات الجهاز أو العبث بالملفات الموجودة فيه.

ثامنا: جريمة الاحتيال عن طريق الانترنت: من الجرائم الي شاع استخدامها مؤخرا استخدام الانترنت في ارتكاب جريمة الاحتيال واستخدام اجهزة الحاسوب بقصد التضليل أو الغش وافشاء اسرار وبيانات المشتركين للغير واستخدام شبكة الانترنت بقصد الغش علامة تجارية تعود للغير، وهذه الجرائم يعاقب عليها قانون العقوبات العراقي رقم ١١١ لسنة ١٩٦٩ المعدل.

---

[٩]. القاضي كاظم عبد كاظم الزيدي، نقل بتصرف – مصدر سابق.

[10] - Susan W.Brenner .Cybercrime and the law. HIOA- bibliotekene- norge- p 29.

[١١]. أ . جـــان فرنســـوا هنـــروت - أهميـــة التعـــاون الـــدولي والتجريـــة البلجيكيـــة فـــي تبـــادل المعلومـــات بـــين عناصـــر الشـــرطة والتعـــاون القضـــائي- أعمـــال النـــدوة الاقليميـــة حـــول : «الجـــرائم المتصـــلة بـــالكمبيوتر- برنـــامج تعزيـــز حكـــم القـــانون فـــي بعـــض الـــدول العربيـــة - مشروع تحديث النيابات العامة – ص ٩٥.

تاسعا: استخدام الانترنت في ارتكاب الجرائم الجنسية: من الجرائم المرتكبة عن طريق الانترنت انشاء المواقع الالكترونية أو المساعدة في انشاء مواقع على شبكة المعلومات للترويج أو إنتاج أو توزيع مواد الدعارة والمواقع التي تساعد في التحريض على الفسوق والفجور . [١٢]

عاشراً: جرائم الانتحار باستخدام الأنترنت : ترى الباحثة أن من أخطر صور ارتكاب الجرائم الإلكترونية، جرائم الانتحار، وتجد إنها لم تحظى باهتمام من المختصين في الجرائم الالكترونية باعتبارها أحد أخطر صور ارتكاب الجرائم الالكترونية. فقد أدت لعبة جديدة منتشرة بين المراهقين في روسيا إلى وفاة ١٣٠ منهم، ووفقا لصحيفة "ميرور" البريطانية، فإن اللعبة التي ابتكرتها صفحات على مواقع التواصل الاجتماعي، تشجع المراهقين على حفر شكل معين على أجسادهم باستخدام أداة حادة، كما تحثهم على مشاهدة أفلام الرعب وتنتهي اللعبة عندما ينتحر الشخص في اليوم الخمسين من بدأ هذه العادات الغريبة [١٣]. وحادثة سبعة أشخاص قتلوا أنفسهم في غضون ساعات في اليابان بحالات انتحار ارتكبت بعد اتفاقات تمت على الإنترنت. [١٤]

ب - الاتجاه الأساسي لجرائم نظم المعلومات: يتركز الاتجاه الأساسي لجرائم نظم المعلومات وفقاً لتحقيق أجرته مجلة Ressources informatiqes تبين أن:

١. ١٩% من أفعال الغش المعلوماتي تستهدف البنوك .
٢. ١٦% للإدارة .
٣. ١٠% للإنتاج الصناعي .
٤. ١٠% للمعلومات .

---

[١٢] - القاضي كاظم عبد كاظم الزيدي - نقل بتصرف - مصدر سابق.
[١٣] - وكالة سكاي برس، لعبة تؤدي بحياة عشرات المراهقين الروس، نقل بتصرف،١,٣,٢٠١٧. متاح على الرابط%D9%84%http://www.skypressiq.net/2017/3/1/.
[14] - the guardian, Seven die in online suicide pact in Japan, 3.3.2017. https://www.theguardian.com/technology/2005/mar/02/japan.

ثـم يلـي ذلـك شـركات التـأمين والشـركات الخاصـة، وفـي واقـع الأمـر أن جـرائم نظـم المعلومات تستهدف في المقام الأول المؤسسات المالية والتي تتحكم في القيم الرأسمالية.[١٥]

المطلب الرابع: أسباب الجريمة الالكترونية، والصعوبات التي تواجه مكافحتها على المستوى الوطني والدولي

أولاً: أسباب الجريمة الإلكترونية : لاشك أن فئات مرتكبي الجريمة المعلوماتية تختلف عن مرتكبي الأفعال الإجرامية التقليدية، لذا من الطبيعي أن نجد نفس الاختلاف في الأسباب والعوامل التي تدفع في ارتكاب الفعل غير المشروع. فضلا عن ذلك، تتمتع جرائم الكمبيوتر والمعلوماتية بعدد من الخصائص التي تختلف تماما عن الخصائص التى تتمتع بها الجرائم التقليدية، كما أن الجاني الالكتروني (أو المجرم الإلكتروني) يختلف أيضا عن المجرم العادي. ويأتي أهمها:

١. غاية التعلم: يشير الأستاذ ليفي مؤلف كتاب قراصنة الأنظمة HACKERS إلى أخلاقيات هؤلاء القراصنة والتي ترتكز على مبدأين أساسيين: أ. أن الدخول إلى أنظمة الكمبيوتر يمكن أن يعلمك كيف يسير العالم. ب. أن جمع المعلومات يجب أن تكون غير خاضعة للقيود. وبناء على هذين المبدأين فإن أجهزة الكمبيوتر المعنية ما هي إلا آلات للبحث، والمعلومات بدورها ما هي إلا برامج وأنظمة معلومات. ومن وجهة نظر هؤلاء القراصنة فإن جميع المعلومات المفيدة بوجه عام يجب أن تكون غير خاضعة للقيود، وبعبارة أخرى أن تتاح حرية نسخها وجعلها تتناسب مع استخدامات الأشخاص. ويرى هؤلاء القراصنة إغلاق بعض نظم المعلومات وعدم السماح بالوصول إلى بعض المعلومات وخاصة بعض المعلومات السرية التي تخص الأفراد. ويعلق قراصنة الأنظمة أنهم يرغبون في الوصول إلى مصادر المعلومات والحاسبات الإلكترونية والشبكات بغرض التعلم. وقد لاحظ كل من "ليفي" و "لاندريس" أن قراصنة الأنظمة لديهم الاهتمام الشديد بأجهزة الكمبيوتر وبالتعلم ويدخل العديد منهم في أجهزة الكمبيوتر على أنهم محترفون، ويختار بعض القراصنة الأنظمة لتعلم المزيد عن كيفية عمل الأنظمة.

[١٥]. د. عبد العال الديبري، الاستاذ محمد صادق إسماعيل، كتاب الجرائم الالكترونية،المركز القومي للإصدارات القانونية. الطبعة الاولى ٢٠١٢. ص ١٩٦ــ ١٧٠. ٢٠١٧,١,٢٠. متاح على الرابط https://books.google.no/books?id=4d4sDAAAQBAJ&pg=PT377&lpg=PT377&

٢. السعي إلى الربح: أشارت إحدى المجلات المتخصصة في الأمن المعلوماتي securite informatique إلى الرغبة في تحقيق الثراء من بين العوامل الأساسية لارتكاب الجريمة المعلوماتية، حيث أشارت: أن ٤٣% من حالات الغش المعلن عنها قد بوشرت من أجل اختلاس الأموال. و٢٣% من أجل سرقة المعلومات. و١٩% أفعال اتلاف. و١٥% سرقة وقت الآلة؛ أي الاستعمال غير المشروع للحاسب الآلي لأجل تحقيق أغراض شخصية.

٣. الإثارة والمتعة والتحدي: يدرك القراصنة شيئاً عن أساسيات الكمبيوتر وأن هذا الأمر يمكن أن يكون ممتعاً، حيث جاء على لسان أحد القراصنة ما يأتي: كانت القرصنة هي النداء الأخير الذي يبعثه دماغي فقد كنت أعود إلى البيت بعد يوم ممل آخر في المدرسة، وأدير تشغيل جهاز الكمبيوتر، وأصبح عضواً في نخبة قراصنة الأنظمة، كان الأمر مختلفاً برمته حيث لا وجود لعطف الكبار وحيث الحكم هو موهبتك فقط. في البدء كنت أسجل أسمي في لوحة النشرات Bulletin Borard الخاصة حيث يقوم الأشخاص الآخرون الذين يفعلون مثلي بالتردد على هذا الموقع، ثم أتصفح أخبار المجتمع وأتبادل المعلومات مع الآخرين في جميع أنحاء البلاد. وبعد ذلك أبدأ عملية القرصنة الفعلية، وخلال ساعة واحدة يبدأ عقلي بقطع مليون ميل في الساعة وأنسى جسدي تماماً بينما أتنقل من جهاز كمبيوتر إلى آخر محاولاً العثور على سبيل للوصول إلى هدفي.

٤. الدوافع الشخصية: إن الدافع لارتكاب جرائم الكمبيوتر يغلب عليه الرغبة في قهر النظام أكثر من شهوة الحصول على الربح، ويميل مرتكبو جرائم نظم المعلومات إلى إظهار تفوقهم ومستوى ارتقاء براعتهم لدرجة أنه إزاء ظهور أي تقنية مستحدثة فإن مرتكبي هذه الجرائم لديهم شغف الآلة، يحاولون إيجاد – وغالباً ما يجدون – الوسيلة إلى تحطيمها بل والتفوق عليه[١]، ويتزايد شيوع هذا الدافع لدى فئات صغار السن من مرتكبي الكمبيوتر الذين يمضون وقتاً طويلاً أمام حواسبهم الشخصية في محاولة لكسر حواجز الأمن لأنظمة الكمبيوتر وشبكات المعلومات وإظهار تفوقهم على وسائل التكنولوجيا الأمر الذي دفع بالعديد من الفقهاء إلى المناداة بعدم مساءلة مرتكبي جرائم الحاسب الآلي الذي يتمثل باعثهم في إظهار تفوقهم واعتبار أعمالهم غير منطوية على نوايا آثمة. [١٦]

[١٦]. د. عبد العال الديربي .الجريمة المعلوماتية تعريفها أسبابها خصائصها . نقل بتصرف. مصدر سابق.

٥. الدوافع السياسية يتم غالبا في المواقع السياسية المعادية للحكومة، ويتمثل في تلفيق الاخبار والمعلومات ولو زورا او حتى الاستناد الى جزء بسيط جدا من الحقيقة ومن ثم نسخ الاخبار الملفقة حولها، وتعد الدوافع السياسية من ابرز المحاولات الدولية لاختراق شبكات حكومية في مختلف دول العالم.[١٧]

٦. البطالة: يشير العديد من مفكري الجريمة للعلاقة بين البطالة والفراغ وبين السلوك الإجرامي، الأمر الذي يهيء ويمهد الفرص لارتكاب الجرائم الالكترونية.

ثانياً: صعوبة مكافحة الجريمة الإلكترونية

أ: الصعوبات على المستوى الوطني: تتعدد الصعوبات التي تواجه الدور الذي تقوم به الأجهزة الأمنية في مكافحة الجرائم الإلكترونية على المستوى الوطني، وأهم هذه الصعوبات تتمثل في:

١- عدم كفاية القوانين الحالية: هذا التطور المتلاحق في مجال تقنية المعلومات والاتصالات يقابله استغلال الجناة لهذه التقنية المتطورة بابتكار أساليب جديدة لارتكاب الجرائم الإلكترونية، ولذلك يتطلب الامر مواكبة القوانين لهذه التطورات واستيعابها.

٢- احجام الكثير من الجهات عن التبليغ عن تلك الجرائم : يهدف هذا الإحجام من قبل هذه الجهات إلى عدم الإساءة لطبيعة عمل المنشأة، وعدم بيان عجزها عن تحقيق الأمان الكافي للمعلومات، وبالتالي لأصول الأموال التي تتعامل معها، وقد يكون لذلك مردود سيء لدى العملاء الذين ربما يلجأ كثير منهم لسحب أموالهم ووقف تعاملاتهم مع المنشأة.

٣- سهولة إخفاء معالم الجريمة: ويتمثل ذلك في عدم معرفة مصدر مرتكب الفعل، بحيث إذا تم ارتكاب الفعل وظهرت نتيجته بعد فترة زمنية، مثل قيام شخص ما بزرع برنامج فيروسي يكتشف بعد تحقق آثاره التدميرية والسالبة.

٤- عدم وجود دليل مادي واضح: الدليل المادي الذي يتوافر قد يكون في الغالب أوراق متحصلة من الطابعة من خلال الجهاز والدليل هنا يكون الأوراق المتحصلة وليس ما يحويه الجهاز في حد ذاته.

---

[١٧]- ويكيبيديا – الجريمة الالكترونية- ٢٣,١,٢٠١٧.
https://ar.wikipedia.org/wiki/%D8%AC%D8%B1%D9%8A%D

٥- صعوبة الوصول إلى الدليل في بعض الأحيان: الدليل في الجريمة الإلكترونية عبارة عن معلومات قد تحاط بوسائل فنية لحمايتها، وتلك الوسائل قد تكون عائقا أمام عملية البحث والتحري والإطلاع .

٦- وجود كم كبير من المعلومات يتعين فحصها: يتطلب البحث عن معلومات تفيد في كشف أدلة جرمية معينة البحث في كم كبير من الملفات والبرامج المخزنة والتي قد يكون لها ارتباط بمعلومات خاصة بارتكاب الجريمة.

ب: الصعوبات على المستوى الدولي: يمكن تفصيل الصعوبات على المستوى الدولي كالتالي:

١- اختلاف مفاهيم الجريمة لإختلاف التقاليد القانونية وفلسفة النظم القانونية.

٢- عدم التناسق في القوانين الإجرائية فيما يتعلق بالتحري والتحقيق في الجرائم الإلكترونية.

٣- عدم وجود الخبرة الكافية لدى الأجهزة الأمنية والعدلية لتمحيص عناصر الجريمة.

٤- عدم كفاية الإتفاقيات الدولية والثنائية في مجال تسليم المجرمين . [١٨]

المبحث الثاني

مكافحة الجريمة الالكترونية في ضوء القوانين الوطنية

أصبحت جرائم الإنترنت مشكلة عالمية تؤثر على كل الدول تقريبا.[١٩] ولا تخضع الجرائم السيبرانية في الوقت الحالي للسيطرة القوية كما يتضح من تفحص المرء للإحصائيات السنوية التي ينتجها معهد أمن الحاسوب (CSI) أو الفريق المعني بطوارئ الحاسوب والاستجابة لها (CERT) [٢٠]، ووفقاً لمكتب الأمم المتحدة لمكافحة الجرائم والمخدرات (UNODC) أن تهديدات سلامة الانترنيت قد ارتفعت بشكل كبير في السنوات الأخيرة، وأن عدد ضحايا الجريمة الالكترونية على الصعيد العالمي بلغ ٤٣١ مليون.[٢١] وامام هذا الرقم من ضحايا التجاوزات الغير مشروعة، ومع عدم وجود مواكبة قانونية للمستجدات لهذه الجرائم،

---

[١٨]- الجريمة الالكرتونية في المجتمع الخليجي وكيفية مواجهتها، ص ٤٢-٤٣ . مصدر سابق.

[١٩] - Petter Gottschalk,datakriminalitet i Norge,2011,fylkesbiblioteket i Akershus,p 241.

[٢٠]- دليل الامن السيبراني للدول النامية،الإتحاد الدولي للإتصالات،ص ١٧-٢٧,٢,٦٢. متاح على الرابط https://www.itu.int/ITU-D/cyb/publications/2007/cgdc-2007-a.pdf

[21] - *UN conference weighs efforts to combat cybercrime, create safer digital world- UN news centre- 2017.1.18-available at http://www.un.org/apps/news/story.asp?NewsID=50610#.WH7PThvhC03.*

أيقنت الدول الى ضرورة تبني قوانين صارمة للتصدي للجريمة الالكترونية، وتبني برامج وخطط لمكافحتها ومنها إشاعة ثقافة الأمن السيبراني، لذا اصدرت العديد من الدول التشريعات والقوانين الوطنية لمكافحة هذه الجريمة، من أجل ضمان توفير الحماية القانونية الفاعلة للأفراد وللمؤسسات الحكومية والخاصة من هذه الجرائم. وفي بحثنا هذا حرصنا على تناول واقع التشريعات العربية في مكافحة الجريمة المعلوماتية مع استعراض لنموذج من هذه النظم المتمثل في القانون الاتحادي رقم ٥ لسنة ٢٠١٢ لمكافحة الجرائم الإلكترونية لدولة الإمارات العربية المتحدة، وتم تناول البحث فق السياق الآتي:

المطلب الأول : التشريعات والقوانين العربية

أولاً: واقع التشريعات والممارسات لمكافحة الجرائم الإلكترونية: مع إتساع إستخدام الفضاء الالكتروني كشبكة التواصل الاجتماعي أصبحت الجريمة الالكترونية أكثر تنوعاً. وتلعب أجهزة الكمبيوتر والإنترنت دورا أساسيا في تسهيل ارتكاب الجرائم التقليدية بطرق عدة.[٢٢] فمواقع الفيسبوك وتويتر وغيرها من مواقع الشبكات الاجتماعية يمكن أيضا أن تستخدم من قبل المجرمين .[٢٣] وأكدت دراسة شركة الخليج للحاسبات الالية G.BM في يونيو ٢٠١٣ أن خبراء تكنولوجيا المعلومات في دول مجلس التعاون يؤكدون أن منطقة الخليج تشكل هدفاً رئيسياً للجرائم الالكترونية، كما ذكرت الدراسة أن زيادة شبكات التواصل الإجتماعي يصاحبه إزدياد في مخاطر الأمن الالكتروني. وورد في تقرير نورتن سيمانتيك Norton Symantec للعام ٢٠١٣ أن كلا من المملكة العربية السعودية، ودولة الامارات العربية المتحدة من دول مجلس التعاون الخليجي، ضمن الـ ٢٤ دولة الاولى في العالم التي تزيد فيها التهديدات المقلقة بتسرب البيانات.[٢٤] حتى وقتٍ قريب، كان للحكومات مقاربات مختلفة بشأن التشريعات الخاصة بالإنترنت. فمعظم دول العالم تنظّم الإنترنت ضمن حدود قيمها السياسية والقانونية والأخلاقية والثقافية. لكن بما أن تطوّر تكنولوجيا الإتصالات والمعلومات يجري على مستوى دولي خارجًا عن نطاق سيطرة هذه الدول، فإن اعتماد تشريعات فعالة وتنفيذها لمكافحة جرائم الإنترنت يشكّل تحديًا كبيرًا للحكومات. وبالتالي إن جرائم الإنترنت تمثّل تحديًا كبيرًا للأجهزة القانونية في

---

[22] - Oerlemans, Jan-Jaap, Investigating cybercrime,2017, Leiden University,HIOA bibliotik, norway ,chapter 2 ,p 24.

[23] -Shipley , Todd G. Bowker, Art, Investigating internet Crimes, HIOA bibliotik, Norway,p 388.

[٢٤]- الجريمة الالكترونية في المجتمع الخليجي وكيفية مواجهتها، ص ٣٩. مصدر سابق.

كلّ من البلدان المتقدمة والنامية.[٢٥] وبينت دراسات الإسكوا الفجوة القانونية، في مجال التشريعات السيبرانية، بين البلدان العربية والبلدان المتقدمة من جهة، وبين البلدان العربية نفسها من جهة أخرى. ونظراً للطبيعة الشمولية للفضاء السيبراني وتجاوزه حدود البلدان والأقاليم، فالتنسيق الدولي والإقليمي مهم جداً بالنسبة للتشريعات السيبرانية، ويأخذ البعد الإقليمي أهمية كبرى بالنسبة للمنطقة العربية، إذ يساهم تنسيق التشريعات السيبرانية في المنطقة العربية ببناء مجتمع معرفة عربي متكامل، من خلال التعاون والتنسيق لمواجهة المخاطر المعلوماتية، وتحفيز المعاملات والخدمات الإلكترونية بين البلدان العربية، والمساهمة في حماية الملكية الفكرية للفضاء السيبراني على المستوى الإقليمي العربي [٢٦].

وضمن جهود مجلس وزراء العدل العرب في مكافحة الجرائم السيبرانية قرر إعتماد "قانون الإمارات العربي الإسترشادي لمكافحة جرائم تقنية أنظمة المعلومات وما في حكمها (٢٠٠٤)"، يتكون القانون من (٢٧) مادة التي عالجت موضوع الجرائم الالكترونية [٢٧] ، وعن مبادرة تحديث وتطوير عمل النيابات العامة في الدول العربية التي يقوم بتنفيذها برنامج الأمم المتحدة الإنمائي – برنامج إدارة الحكم في الدول العربية UNDP -POGAR منذ العام 2002، تم تنظيم مجموعة من الانشطة تتضمن ندوات تثقيفية ودورات تدريبية بغية توطيد المعرفة لدى أعضاء النيابات العامة حول الجرائم الحديثة من أجل تفعيل دورهم في تعزيز حكم القانون وبناء قدراتهم لجهة استخدام أساليب ومنهجيات التحقيق المتطورة. وقد ركز المشروع ضمن إطار نشاطاته على موضوع مكافحة الجرائم الالكترونية، وتحقيقا لهذه الغاية قام بتنظيم ندوة إقليمية تحت عنوان "الجرائم المتصلة بالكمبيوتر"، في المملكة المغربية بتاريخ ١٩/٢٠ يونيو ٢٠٠٧، وذلك بناء على طلب من النيابات العامة في عدد من الدول العربية. ولقد هدفت هذه الندوة إلى تعزيز وبناء معرفة النيابات العامة بالجرائم المتعلقة بالكمبيوتر والاساليب والتقنيات الحديثة المستخدمة لمواجهة هذا النوع من الجرائم .[٢٨] وقامت الدول العربية بوضع

---

[٢٥]. د. جورج لبكي- المعاهدات الدولية للأنترنيت – مجلة الدفاع الوطني- لبنان – العدد ٨٣ كانون الثاني ٢٠١٣ – متاح على الرابط
https://www.lebarmy.gov.lb/ar/content/%D8%A7%D9%84%D9

[٢٦]- د. نبال إدلبي و السيدة هانيا ديماسي، مذكرة سياساتية تطوير وتنسيق التشريعات السيبرانية في المنطقة العربية،(اللجنة الاقتصادية والاجتماعية لغربي آسيا، الإسكوا) . ٣١،١،٢٠١٧. ص ١. متاح على
https://www.unescwa.org/sites/www.unescwa.org/files/publications/files/e_escwa_ictd_13_tp-2_a_0.pdf

[٢٧]- ينظر قانون الإمارات العربي الإسترشادي لمكافحة جرائم تقنية أنظمة المعلومات وما في حكمها (٢٠٠٤).

[٢٨]. أ. وسيم حرب – كتاب برنامج تعزيز حكم القانون في بعض الدول العربية – مشروع تحديث النيابات العامة- كتاب أعمال الندوة حول الجرائم المتصلة بالكمبيوتر.المملكة المغربية ٢٠٠٧.ص ٨. متاح على الرابط
ftp://pogar.org/localuser/pogarp/ruleoflaw/cybercrime-09a.pdf

العديد من القوانين السيبرانية في السنوات الخمس الأخيرة، وتعتبر قوانين التعاملات الإلكترونية بما فيها التوقيع الإلكتروني من أكثر القوانين انتشاراً في المنطقة العربية، وقامت العديد من الدول بوضع قوانين للجرائم السيبرانية. وتعاني معظم الدول من نقص في مجال التشريعات الخاصة بمحاور: معالجة وحماية البيانات ذات الطابع الشخصي، وحماية المستهلك في التعاقدات الإلكترونية، والمسائل المتعلقة بالملكية الفكرية على الإنترنت.

ثانياً: تحديات التشريعات السيبرانية في المنطقة العربية:

١. غياب المرجعية الموحدة المعنية بالمسائل التنظيمية والقانونية للفضاء السيبراني.
٢. عقبات صياغة وإقرار القوانين السيبرانية على الصعيد الوطني.
٣. نقص كبير في اللوائح التنفيذية والقرارات الإجرائية والأدوات التنظيمية لتطبيق القوانين. [٢٩]

وتجدر الإشارة ان بعض الانظمة لا يوجد لديها قانون متخصص بمعالجة الجرائم الإلكترونية، كما هو الحال في العراق حيث تعالج هذه الجرائم بقانون العقوبات العراقي رقم ١١١ لسنة ١٩٦٩ المعدل، وقانون مكافحة الارهاب وغيرها، وان هناك تشريعا لقانون جرائم المعلوماتية مقدما من مجلس النواب وفي إنتظار تشريعه، لذا توصي الباحثة على أهمية إصدار وتنفيذ القانون في أقرب وقت لحاجة المجتمع للقانون وتطبيقاً للمعايير الدولية على الصعيد العالمي والاقليمي في مكافحة هذه الجرائم الخطيرة.

ثالثاً: نماذج لبعض القوانين العربية القائمة الخاصة بمكافحة الجرائم السيبرانية التي ساهمت في مكافحة هذه الجرائم:

١. الإمارات العربية المتحدة: القانون الاتحادي رقم ٥ لسنة ٢٠١٢ م في شأن مكافحة جرائم تقنية المعلومات.
٢. المملكة العربية السعودية: نظام مكافحة جرائم المعلوماتية الصادر بالمرسوم الملكي رقم م/ ١٧ وتاريخ: ١٤٢٨/٣/٨هـ.
٣. سلطنة عُمان: قانون مكافحة جرائم تقنية المعلومات بالرقم ٢٠١١/١٢م في ٦/٢/٢٠١١ .

[٢٩]- د. نضال أدلبي، بحث الكتروني بعنوان تطوير وتنسيق التشريعات السيبرانية في المنطقة العربية ومواجهة الجرائم السيبرانية، الأمم المتحدة، الإسكوا،نقل بتصرف، ص ١٤- ١٨.

٤. دولة الكويت: قانون رقم ٦٣ لسنة ٢٠١٥ في شأن مكافحة جرائم تقنية المعلومات، يتكون القانون من ٢١ مادة، صدر بتاريخ ٧. ٧. ٢٠١٥م.
٥. دولة قطر: قانون مكافحة الجرائم الالكترونية رقم (١٤) لسنة ٢٠١٤.
٦. مملكة البحرين: قانون رقم (٦٠) لسنة (٢٠١٤) بشأن جرائم تقنية المعلومات.
٧. الجمهورية العربية السورية: قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية رقم (١٧) لسنة (٢٠١٢م).
٨. مملكة الاردن: قانون الجرائم الإلكترونية رقم ٢٧ لسنة ٢٠١٥م.

وبالبحث في التشريع المصري لم نعثر على ما يشير إلى صدور قانون خاص لمكافحة الجرائم الإلكترونية.

المطلب الثاني: الأمن السيبراني

"الأمن السيبراني هو مجموع الأدوات والسياسات ومفاهيم الأمن وضوابط الأمن والمبادئ التوجيهية ونهج إدارة المخاطر والإجراءات والتدريب وأفضل الممارسات وآليات الضمان والتكنولوجيات التي يمكن استخدامها في حماية البيئة السيبرانية وأصول المؤسسات والمستعملين". وسنتناول في هذا المطلب المراكز الوطنية الخليجية لحماية الامن السيبراني فرق الاستجابة لطوارئ الحاسب الآلي، والمركز الإقليمي للأمن الإلكتروني للمنطقة العربية، وفق السياق الآتي:

أولاً: المراكز الوطنية الخليجية لحماية الأمن السيبراني فرق الإستجابة لطوارئ الحاسب الآلي Computer Emergency Response Teams (CERTs)

مواكبة للجهود الدولية والإقليمية في حماية الأمن السيبراني الوطني، تم تأسيس مراكز وطنية لهذا الغرض في عدد كبير من دول العالم وفي غالبية دول مجلس التعاون لدول الخليج العربية. وسنتناول فيما يلي موجزاً بهذه المراكز:

١. مركز الإستجابة لطوارئ الحاسب الآلي Computer Emergency Response Centre Team (ae CERT) أنشأت هيئة تنظيم الإتصالات بدولة الإمارات العربية المتحدة مركز الإستجابة لطوارئ الحاسب الآلي عام ٢٠٠٧م، لتحسين معايير وممارسات أمن المعلومات وحماية البيئة التحتية لتقنية المعلومات من مخاطر إختراقات الأنترنيت.

٢. القطاع الخاص يؤسس فريق الإستجابة لطوارئ الحاسب الآلي بالبحرين: بالبحث في شبكة الأنترنيت، وبالإطلاع على موقع إدارة مركز البيانات ORG وجدنا أن شركة "تحديث للإستشارات" Reload Consulting Services وهي شركة خاصة مقرها البحرين، قامت بتأسيس مركز الإستجابة لطوارئ الحاسب الآلي CERT في ٤ نوفمر ٢٠١٢م لأول مرة في مملكة البحرين.

٣. المركز الوطني الإرشادي لأمن المعلومات: فريق الإستجابة لطوارئ الحاسب الآلي (Saudi Arabia Computer Emergency Response Team CERT-SA) تم إنشاء هذا المركز بواسطة هيئة الإتصالات وتقنية المعلومات السعودية Communication and Information Technology Commission ويهدف للكشف عن التهديدات والمخاطر، ومنع الاختراقات والانتهاك للأمن السيبراني والتنسيق والاستجابة للمعلومات عن حوادث الأمن السيبراني على مستوى المملكة.

٤. في ١٩ مايو ٢٠١٢ م تم افتتاح النسخة الرابعة من مؤتمر ومعرض الكويت لأمن المعلومات "Kuwait Info Security Conference Exhibition". وفي كلمة الافتتاح أعلن وزير المواصلات الكويتي عن إنشاء المركز الوطني للاستجابة لطوارئ الحاسب في دولة الكويت (KW-CERT) والذي سيرتبط بالمراكز المماثلة المنتشرة حول العام.

٥. المركز الوطني للسلامة المعلوماتية (National Information Safety (Oman Center تم في هذا المركز إنشاء فريق الاستجابة لطوارئ الحاسب الآلي Computer Emergency Response Team (CERT) ويتبع لهيئة تقنية المعلومات بسلطنة عُمان وافتتح في إبريل ٢٠١٠ م.

٦. فريق الاستجابة لطوارئ الحاسب الآلي القطري: (Qatar Cybercrime Emergency Response Team " (Q-CERT "، تم إنشاء "المركز الوطني لأمن المعلومات »National Information Security Center بواسطة المجلس الأعلى لهيئة تقنية المعلومات والإتصالات القطرية (ict QATAR في ديسمر ٢٠٠٥ م.[٣٠]

[٣٠]- الجريمة الالكرتونية في المجتمع الخليجي وكيفية مواجهتها،مجمع البحوث والدراسات أكاديمية السلطان قابوس لعلوم الشرطة نزوى- سلطنة عمان-٢٠١٦، ص ٧٩ -87-، نقل بتصرف .

ثانياً: المركز الإقليمي للأمن الإلكتروني للمنطقة العربية

(Arab Area Cyber Security Regional Center) تم التوقيع على اتفاقية المركز بتاريخ ١٥ ديسمر ٢٠١٢م بين الإتحاد الدولي للإتصالات (ITU) وهيئة تقنية المعلومات بإستضافة سلطنة عُمان للمركز الإقليمي للأمن الإلكتروني للمنطقة العربية، وقد تم بموجب مبادرة الإتحاد الدولي للإتصالات ومنظمة امباكت تفويض المركز الوطني للسلامة المعلوماتية بالسلطنة القيام بإدارة وتشغيل المركز الإقليمي للأمن الالكتروني للمنطقة العربية، إلى حين إنشائه على غرار مراكز إقليمية مماثلة في دول الإتحاد الأوربي وآسيا وغيرها من الأقاليم الأخرى.

- **أهداف المركز الإقليمي للأمن الإلكتروني للمنطقة العربية:**

١. تقديم الخدمات والمبادرات التي تنفذها منظمة (إمباكت) والاتحاد الدولي للإتصالات للمنطقة العربية، لتحسين قدرات الأمن الإلكتروني في المنطقة عن طريق التنسيق الإقليمي في هذا المجال .
٢. يقوم المركز بدور المنسق الإقليمي لجميع الفعاليات والانشطة والمشاريع المتعددة والتي يتبناها وينفذها الاتحاد الدولي للإتصالات ومنظمة "إمباكت" في مجال الأمن الإلكتروني في المنطقة العربية . [٣١]

المطلب الثالث: مشروع الإسكوا لتنسيق التشريعات السيبرانية في المنطقة العربية

باشرت الإسكوا منذ عام ٢٠٠٩م بإعداد دراسات وتنظيم أنشطة للبحث في ملامح التشريعات السيبرانية وتحفيز تطويرها في المنطقة. وقد كانت أولى هذه الأنشطة دراسة بعنوان "نماذج تشريعات الفضاء السيبراني في الدول الأعضاء بالاسكوا"، التي تستعرض وضع التشريعات السيبرانية على المستويين الإقليمي والدولي، ثم تقارن وضع المنطقة العربية بمناطق أخرى في العالم. وقد بينت الدراسة حجم الفجوة القانونية السيبرانية بين هذه المناطق، لا سيما بين المنطقة العربية ودول الإتحاد الأوروبي التي أقرت واعتمدت عدداً من الإرشادات والتوجيهات الخاصة بتنظيم العمل في الفضاء السيبراني. ثم أصدرت الإسكوا عام ٢٠٠٩م (Template)[٣٢] نموذجا يحدد المواضيع الهامة لكل قانون من قوانين الفضاء السيبراني،

---

[٣١]- الجريمة الالكرتونية في المجتمع الخليجي وكيفية مواجهتها، ٢٠١٦، ص ٨٩ . مصدر سابق.

[32].Template.http://isper.escwa.un.org/FocusAreas/CyberLegislation/Template/tabid/201/language/en-US/Default.aspx.

لمساعدة البلدان في وضع تشريعاتها السيبرانية وفي تقييم قوانينها القائمة وتحديد مواضع النقص فيها. وقد طبقت الإسكوا هذا النموذج على عدد من بلدان المنطقة، وأصدرت جداول للبلدان الأعضاء تبين القوانين الصادرة في كل منها استناداً إلى هذا النموذج. وتجدر الإشارة إلى أن الإسكوا ناقشت الدراسة السابقة والنموذج في عدد من الإجتماعات وورش العمل، مع خبراء في التشريعات السيبرانية في المنطقة. وفي ضوء تكرار توصيات المشاركين في اجتماعات الإسكوا على ضرورة القيام بعمل إقليمي يسعى إلى تنسيق القوانين على مستوى بلدان العالم العربي ويستجيب للحاجة والنقص فيها، قامت الإسكوا بإطلاق مشروع "تنسيق التشريعات السيبرانية لتحفيز مجتمع المعرفة في المنطقة العربية" الذي بدأ تنفيذه عام ٢٠٠٩م وانتهى بنهاية عام ٢٠١٢م [٣٣]، وقد هدف هذا المشروع إلى تعزيز وتنسيق التشريعات السيبرانية في المنطقة العربية بغية بناء قطاع متين ومستدام لتكنولوجيا المعلومات والاتصالات عبر وضع الأطر التشريعية والقانونية الملائمة. وقد تخلل هذا المشروع تنفيذ عدد من الأنشطة المتنوعة التي صدر عنها مخرجات مختلفة أبرزها "إرشادات الإسكوا للتشريعات السيبرانية" والتي صُممت لتساعد البلدان العربية في تطوير قوانين سيبرانية وطنية، وتكوين اللُبنة الأساسية للتكامل الإقليمي بين البلدان العربية عبر تنسيق التشريعات السيبرانية فيما بينها بهدف بناء مجتمع معرفة عربي. وتغطي هذه الإرشادات ستة محاور أساسية لتنظيم الفضاء السيبراني، والتي يمكن استخدامها إما كقوانين منفصلة بحسب المحور، أو كقانون واحد وشامل. والمحاور الستة هي: الاتصالات الالكترونية وحرية التعبير، والمعاملات الالكترونية والتواقيع الالكترونية، والتجارة الالكترونية وحماية المستهلك، ومعالجة البيانات ذات الطابع الشخصي، والجرائم السيبرانية، والملكية الفكرية في المجال المعلوماتي والسيبراني. ويتضمن كل محور ورقة بحثية خلفية تتناول موضوع الإرشاد، يتبعها مقدمة ومن ثم عرض لأبواب ومواد القانون المختلفة. فهدف هذه الإرشادات لا ينحصر بعرض النصوص القانونية فقط، بل يتعداه إلى تقديم المادة البحثية للمهتمين من الباحثين ومراكز الدراسات في المجال القانوني، إضافة إلى شروحات للنصوص القانونية. وقد تعاونت الإسكوا مع مجموعة مميزة من الخبراء القانونيين ذوي الخبرة في مجال تكنولوجيا المعلومات والاتصالات من أجل إعداد وصياغة هذه

[33] http://isper.escwa.un.org/FocusAreas/CyberLegislation/Projects/tabid/161/language/en-US/Default.aspx.

الإرشادات، كما نظمت اجتماعاً ضم مجموعة من الخبراء في المنطقة، تم خلاله عرض ومناقشة الإرشادات قبل صياغة النسخة النهائية منها. [٣٤]

المطلب الرابع: القانون الاتحادي رقم ٥ لسنة ٢٠١٢ م بشأن مكافحة جرائم تقنية المعلومات لدولة الإمارات العربية المتحدة

أمام ثورة تقنية المعلومات والإتصالات وما خلفته من مشكلات وتحديات ذات أبعاد إجرامية متزايدة، وتواصلاً مع توجهات العمل الدولي بشأن سياسة مكافحة هذه الجرائم، عملت بهذا الاتجاه الدول العربية فشهدت ولادة قوانين خاصة أو تعديل القوانين القائمة بما يتيح توفير الحماية لاستخدام برامج الكمبيوتر والأنترنيت، وقد جاء إتجاه تشريع القواعد القانونية في التعامل مع جرائم الحاسوب مواءمة مع اتجاهات القواعد والمواثيق الدولية. وفي بحثنا هذا إرتأينا تناول نموذج لهذه النظم المتمثل في القانون الاتحادي رقم ٥ لسنة ٢٠١٢ م بشأن مكافحة جرائم تقنية المعلومات لدولة الإمارات العربية المتحدة، هذه الدولة التي تميزت بإنجازاتها الحضارية، وبالسياسات والتشريعات الحكيمة التي جعلت من دولة الإمارات العربية المتحدة مثالاً عالمياً يحتذى به في كافة المجالات ومنها مجال تكنلوجيا المعلومات والإتصال، ومن الإنجازات المهمة في هذا المجال تأسيس (مدينة دبي للأنترنيت). ومن الإنجازات أيضاً لغرض الحماية من مخاطر واختراقات الإنترنت وبناء ثقافة آمنة في هذا المجال تأسيس مركز الاستجابة لطوارئ الحاسب الآلي،(The Computer Emergency Response Team (aeCERT. وقد توج المشرع الإماراتي جهوده في هذا المجال بسنّ القانون الاتحادي رقم ٥ لسنة ٢٠١٢م بشأن مكافحة جرائم تقنية المعلومات، وسنتناول نصوص مواد القانون مستخدمين منهجية تحليل النص القانوني وفق السياق التالي:

- **القانون الإماراتي الاتحادي رقم ٥ لسنة ٢٠١٢ م بشأن مكافحة جرائم تقنية المعلومات:**

يعد القانون الاتحادي رقم ٢ لسنة ٢٠٠٦م من القوانين النموذجية التي تطرقت إلى أغلب الجرائم المعلوماتية. وهو أول قانون في الدول العربية يصدر بشكل مستقل لمواجهة الجرائم المعلوماتية. [٣٥] وبتاريخ ١٣ أغسطس ٢٠١٢م صدر القانون الإماراتي الاتحادي رقم ٥ لسنة ٢٠١٢م في شأن مكافحة جرائم تقنية المعلومات، بموجب المادة (٥٠) منه ألغي القانون

[٣٤]- د. نبال إدلبي و السيدة هانيا ديماسي، ص ٤-٥، مصدر سلبق.

[٣٥]- د. ناصر بن محمد البقمي، مكافحة الجرائم المعلوماتية وتطبيقاتها في دول مجلس التعاون لدول الخليج العربي، ١١٦ سلسة محاضرات الامارات، مركز الإمارات للدراسات والبحوث الإستراتيجية، الطبعة الاولى ٢٠٠٨م .

الاتحادي رقم ٢ لسنة ٢٠٠٦ م في شأن مكافحة جرائم تقنية المعلومات بعد أن أثبت الواقع العملي قصوره. يتكون القانون من (٥١) مادة، وتضمنت عقوبات أصلية وتكميلية، وغطى القانون غالبية المسائل المتعلقة بالجرائم الالكترونية، وإهتم بالمسائل التي يترتب عليها جرائم كبرى وغلظ العقوبات الجنائية بحق مرتكبيها، لكي يوفر الحماية القانونية للمجتمع والحفاظ على أمنه واستقراره، ولأجل أن يضمن حق كل من يتعرض لخطورة هذه الجرائم. تضمنت المادة (١) منه بيان معاني بعض المصطلحات مثل نظام المعلومات الالكتروني، والموقع الالكتروني، والشبكة المعلوماتية ...ألخ. والملاحظ في هذه المادة أن المشرع لم يرد نصاً لتعريف الجريمة الالكترونية، وإنما تركها للاجتهادات الفقهية، لكنه حدد الأفعال التي إعتبرها جرائم ألكترونية كما سيأتي بيانها لاحقاً. ونظمت المادة (٢/ ١) جريمة الدخول الغير مشروع حيث نصت على: (يعاقب بالحبس والغرامة التي لا تقل عن مائة ألف درهم ولا تزيد على ثلاثمائة ألف درهم أو بإحدى هاتين العقوبتين كل من دخل موقع الكتروني أو نظام معلومات الكتروني أو شبكة معلومات، أو وسيلة تقنية معلومات، بدون تصريح أو بتجاوز حدود التصريح، أو بالبقاء فيه بصورة غير مشروعة) . يتضح من خلال النص أن الجريمة عمدية تقوم بمجرد دخول المجرم مع علمه بعدم جواز دخوله للموقع ألإلكتروني ويقصد به مكان إتاحة المعلومات الالكترونية على الشبكة المعلوماتية ومنها مواقع التواصل الاجتماعي والصفحات الشخصية والمدونات أو أنظمة المعلومات الالكترونية وهي مجموعة برامج معلوماتية ووسائل تقنية المعلومات المعدة لمعالجة وإدارة وتخزين المعلومات الالكترونية أو ما شابه ذلك، أو شبكة معلومات وهي ارتباط بين مجموعتين أو أكثر من البرامج المعلوماتية ووسائل تقنية المعلومات التي تتيح للمستخدمين الدخول وتبادل المعلومات، أو وسيلة تقنية معلومات ويقصد بها وفق هذا القانون اي اداة مغناطيسية، كهروكيميائية، أو اي اداة اخرى تستخدم لمعالجة البيانات الالكترونية وأداة العمليات المنطقية والحسابية، أو الوظائف التخزينية ويشمل اي وسيلة موصلة أو مرتبطة بشكل مباشر تتيح لهذه الوسيلة تخزين المعلومات الالكترونية أو إيصالها للأخرين، ويتم ذلك بدون تصريح، أو أن يتجاوز حدود التصريح، أو السلوك الإجرامي المتمثل البقاء في الموقع الالكتروني أو شبكة المعلومات بصورة غير مشروعة، أي تتم هذه الأفعال دون رضاء صاحب الحق بمعنى دون إحترام وإلتزام المتهم للقيود المفروضة. ونرى ان المادة جرمت صراحة هذه الأفعال حتى وأن لم يترتب على هذا الدخول أي أثر، فالقانون لم يشترط تحقيق نتيجة، وان العقوبة التي قررها القانون الحبس وهي عقوبة سالبة للحرية، ومالية وهي الغرامة، أو بإحدى هاتين العقوبتين، والملاحظ ايضاً في هذه

الفقرة أن المشرع لم يشترط تبعية الموقع الالكتروني أو شبكات المعلومات سواء كان عاما أم خاصا وإنما جاء النص شاملا. [٣٦]

اما في الفقرة (٢/٢) جاءت العقوبة أشد من سابقتها، حيث قضت بتشديد العقوبة إذا ما ترتب على دخول المجرم الالكتروني تحقيق أي من النتائج التي نصت عليها هذه الفقرة، حيث نصت على: (تكون العقوبة الحبس مدة لا تقل عن ستة أشهر والغرامة التي تقل عن مائة وخمسين ألف درهم ولا تجاوز سبعمائة وخمسون ألف درهم أو بإحدى هاتين العقوبتين إذا ترتب على أي فعل من الافعال المنصوص عليها بالفقرة (١) من هذه المادة إلغاء أو حذف أو تدمير أو إفشاء أو إتلاف أو تغيير أو نسخ أو نشر أو إعادة نشر أي بيانات أو معلومات). وهنا بينت المادة الصور المستخدمة في تخريب البيانات أو المعلومات، والتي تعتبر من الجرائم الأخطر أثراً.

وقاعدة أخرى أقرها القانون وشدد العقوبة فيها لضمان سرية البيانات الشخصية ذلك في الفقرة (٢/٣) حيث نصت على: (تكون العقوبة الحبس مدة لا تقل عن سنة واحدة والغرامة التي لا تقل عن مائتين وخمسين ألف درهم ولا تجاوز مليون درهم أو بإحدى هاتين العقوبتين إذا كانت البيانات أو المعلومات محل الافعال الواردة في الفقرة (٢) من هذه المادة شخصية)، وهنا نرى أن المشرع في تشديد العقوبة حدد أي نوع من البيانات أو المعلومات، فالحكمة من التجريم حماية البيانات والمعلومات الشخصية التي تحميها القوانين الداخلية للدول والمواثيق والأعراف والقوانين الدولية.

وعاقب القانون كل من إرتكب أي من الجرائم المنصوص عليها في البندين (١) و (٢) من المادة (٢) من هذا المرسوم بقانون بمناسبة أو بسبب تأدية عمله، بالحبس مدة لا تقل عن سنة واحدة والغرامة التي لا تقل عن مائتين وخمسين ألف درهم ولا تجاوز مليون درهم أو بإحدى هاتين العقوبتين (المادة ٣). وشددت هذه المادة العقوبة كون الموظف مؤتمن على أسرار ومصالح مكان عمله وأنه من السهولة حصوله على المعلومات بحكم عمله مستغلاً نفوذه في ارتكابه لهذه الجرائم وأضراره لأصحاب ومكان العمل.

وفق هذا القانون تعتبر الجرائم الواردة في نص المادة (٤) من الجرائم الماسة بأمن الدولة، وأن القانون أقر عقوبة جنائية سالبة للحرية وهي السجن المؤقت وبعقوبة مالية وهي الغرامة على كل من دخل بدون تصريح إلى موقع الكتروني، أو نظام معلومات

[٣٦]- ينظر المواد (١) و (١/ ٢) من القانون .

الكتروني، أو شبكة معلوماتية، أو وسيلة تقنية معلومات، سواء كان الدخول، بقصد الحصول على بيانات حكومية الخاصة أو العائدة الى الحكومة الإتحادية أو الحكومات المحلية لإمارات الدولة أو الهيئات العامة أو المؤسسات العامة الإتحادية أو المحلية، أو كان بقصد الحصول على معلومات سرية خاصة بمنشأة مالية أو تجارية أو اقتصادية ويقصد بها المشرّع وفق هذا القانون أي منشأة تكتسب وصفها المالي أو التجاري أو الاقتصادي بموجب الترخيص الصادر لها من جهة الاختصاص بالدولة. ومن هنا نرى أن المشرّع إستلزم أن يكون دخول المتهم بدون تصريح وأن تتجه نيته الحصول على بيانات حكومية، أو معلومات سرية. وأنه شدد العقوبة في ذات المادة لتصل الى السجن مدة لا تقل عن خمس (٥) سنوات والغرامة التي لا تقل عن خمسمائة ألف درهم ولا تجاوز (٢) مليون درهم، إذا تعرضت هذه البيانات أو المعلومات للإلغاء أو الحذف أو الإتلاف أو التدمير أو الإفشاء أو التغيير أو النسخ أو النشر أو إعادة النشر.

وعن جريمة الدخول بغير تصريح موقعاً الكترونيا بقصد تغيير تصاميمه أو إلغائه أو إتلافه أو تعديله أو شغل عنوانه، قرر المشرّع عقوبة الحبس والغرامة التي لا تقل عن مائة ألف درهم ولا تجاوز ثلاثمائة ألف درهم أو بإحدى هاتين العقوبتن (المادة ٥).

وعاقبت المادة (٦) بالسجن المؤقت والغرامة جريمة تزوير المستندات الالكترونية والتي يقصد بها وفق هذا القانون سجل أو بيان معلوماتي يتم إنشاؤه أو تخزينه أو استخراجه أو نسخه أو إرساله أو إبلاغه أو استلامه بوسيلة ألكترونية على وسيط . وعاقبت نفس المادة بالحبس والغرامة إذا وقع التزوير في مستندات جهة غير تلك المنصوص عليها في الفقرة الاولى من هذه المادة. كما وعاقبت بذات العقوبة المقررة لجريمة التزوير، بحسب الاحوال، من استعمل المستند الالكتروني المزور مع علمه بتزويره.

اما المادة (٧) التي عاقبت بالسجن المؤقت، نجد أن الجريمة تقوم على كل من حصل أو استحوذ أو عدل أو أتلف أو أفشى بغير تصريح بيانات أي مستند الكتروني أو معلومات الكترونية عن طريق الشبكة المعلوماتية أو موقع الكتروني أو نظام المعلومات الالكتروني أو وسيلة تقنية معلومات وكانت هذه البيانات أو المعلومات تتعلق بفحوصات طبية أو تشخيص طبي، أو علاج أو رعاية طبية أو سجلات طبية.

وجاء الجزاء القانوني على كل من أعاق أو عطل الوصول إلى شبكة معلوماتية أو موقع الكتروني أو نظام معلومات الكتروني بعقوبة سالبة للحرية بالحبس وعقوبة مالية وهي

الغرامة التي لا تقل عن مائة ألف درهم ولا تجاوز ثلاثمائة ألف درهم أو بإحدى هاتين العقوبتين وذلك وفق المادة (٨).

وقررت المادة (٩) بعقوبة سالبة للحرية هي الحبس، ومالية وهي الغرامة التي لا تقل عن مائة وخمسين ألف درهم ولا تجاوز خمسمائة ألف درهم أو بإحدى هاتين العقوبتين على كل من تحايل على العنوان البروتوكولي للأنترنت باستخدام عنوان وهمي أو عنوان عائد للغير أو بأي وسيلة أخرى، وذلك بقصد ارتكاب جريمة أو الحيلولة دون اكتشافها. ويقصد بمعنى العنوان البروتوكولي وفق هذا القانون معرف رقمي يتم تعيينه لكل وسيلة تقنية معلومات مشاركة في شبكة معلومات، ويتم استخدامه لأغراض الاتصال.

أما المادة (١٠) فمن الملاحظات التي أفرزتها أن الجريمة عمدية وان القانون شدد العقوبة لتصل إلى السجن والغرامة، وأن النظام إستلزم توافر القصد الجنائي بإدخال المجرم الالكتروني عمداً وبدون تصريح برنامج معلوماتي الى الشبكة المعلوماتية ويقصد بالبرنامج المعلوماتي مجموعة من البيانات والتعليمات والأوامر، القابلة للتنفيذ بوسائل تقنية المعلومات والمعدة لإنجاز مهمة معينة. أو نظام معلومات الكتروني أو إحدى وسائل تقنية المعلومات وسبب هذا السلوك إلى إيقافها عن العمل أو تعطيلها أو تدمير أو مسح أو حذف أو إتلاف أو تغيير البرنامج أو النظام أو الموقع الالكتروني أو البيانات أو المعلومات. وعاقب القانون في نفس المادة سلوك المتهم بعقوبة السجن والغرامة التي لا تجاوز خمسمائة ألف درهم أو إحدى هاتين العقوبتين حتى في حالة عدم تمكنه من تحقيق النتيجة المرجوة لفعله. وعاقبت بالحبس والغرامة أو بإحدى هاتين العقوبتين عن أي فعل عمدي يقصد به إغراق البريد الالكتروني بالرسائل وإيقافه عن العمل أو تعطيله أو إتلاف محتوياته.

ولقيام الجريمة وفقاً للمادة (١١) يأتي بالاستيلاء بغير حق على مال منقول أو منفعة أو على سنداً أو توقيع هذا السند بالاستعانة بأي طريقة احتيالية أو باتخاذ اسم كاذب أو انتحال صفة غير صحيحة عن طريق الشبكة المعلوماتية أو نظام معلومات الكتروني أو إحدى وسائل تقنية المعلومات. وحددت المادة لهذه الجريمة عقوبات سالبة للحرية بالحبس مدة لا تقل عن سنة واحدة ومالية بالغرامة التي لا تقل عن مائتين وخمسين ألف درهم ولا تجاوز مليون درهم أو بإحدى هاتين العقوبتين. نلاحظ أن هذه المادة عالجت جريمة الاحتيال وكذلك المادة (٩) عالجت أيضاً جريمة الاحتيال.

وحرصاً من المشرّع على حماية الحقوق المالية، ومن منطلق مكافحة الجرائم المتعلقة بأرقام أو بيانات بطاقة ائتمانية أو الكترونية أو أرقام أو بيانات حسابات مصرفية، أو أي وسيلة من وسائل الدفع الالكتروني، فقد جاء تنظيمها وفق المادة (١٢) من القانون.

وعن جرائم تزوير أو تقليد أو نسخ بطاقة ائتمانية أو بطاقة مدينة، أو أي وسيلة أخرى من وسائل الدفع الالكتروني، وذلك باستخدام إحدى وسائل تقنية المعلومات، أو برنامج معلوماتي. فقد نظمتها المادة (١٣) من القانون.

وعاقبت المادة (١٤) من القانون بالحبس والغرامة التي لا تقل عن مائتي ألف درهم ولا تزيد على خمسمائة ألف درهم أو بإحدى هاتين العقوبتين كل من حصل بدون تصريح مسبق ممن يملك هذا التصريح، على رقم سري أو شفرة أو كلمة مرور أو أي وسيلة أخرى للدخول إلى وسيلة تقنية معلومات، أو موقع الكتروني، أو نظام معلومات الكتروني، أو شبكة معلوماتية، أو معلومات الكترونية. وعاقب المادة بذات العقوبة كل من أعد أو صمم أو أنتج أو باع أو اشترى أو استورد أو عرض للبيع أو أتاح أي برنامج معلوماتي أو أي وسيلة تقنية معلومات، أو روج بأي طريقة روابط لمواقع الكترونية أو برنامج معلوماتي، أو أي وسيلة تقنية معلومات مصممة لأغراض ارتكاب أو تسهيل أو التحريض على ارتكاب الجرائم المنصوص عليها في هذا المرسوم بقانون.

وتعاقب المادة (١٥) من القانون بالحبس والغرامة التي لا تقل عن مائة وخمسين ألف درهم ولا تجاوز خمسمائة ألف درهم أو بإحدى هاتين العقوبتين كل من التقط وقصد بها المشرع مشاهدة البيانات أو المعلومات أو الحصول عليها، أو اعترض عمداً وبدون تصريح أي اتصال عن طريق أي شبكة معلوماتية. فإذا أفشى أي شخص المعلومات التي حصل عليها عن طريق استلام أو اعتراض الاتصالات بغير وجه حق فإنه يعاقب بالحبس مدة لا تقل عن سنة واحدة. ومن هنا توصف الجريمة بأنها جريمة عمدية تتحقق بتوافر القصد الجنائي للمجرم في قيامه بالتقاط أو الاعتراض عمداً وبدون تصريح ممن يملك هذا التصريح أي اتصال عن طريق أي شبكة معلوماتية. وشدد القانون العقوبة في حالة إفشاء المجرم هذه المعلومات بغير وجه حق.

وتضمنت المادة (١٦) من القانون عقوبة الحبس مدة لا تزيد على سنتين والغرامة التي لا تقل عن مائتين وخمسين ألف درهم ولا تجاوز خمسمائة ألف درهم أو بإحدى هاتين العقوبتين كل من ابتز أو هدد شخص آخر لحمله على القيام بفعل أو الامتناع عنه وذلك

باستخدام شبكة معلوماتية أو وسيلة تقنية معلومات. نرى ان المادة أوجبت ان يكون السلوك الإجرامي للمجرم هو الابتزاز أو التخويف للشخص لإرغامه على القيام بفعل أو الامتناع عنه. وفي منظورنا أن القاعدة القانونية لم توضح القصد إذا كان الفعل أو الامتناع عنه معاقبا عليه أم غير معاقب عليه، او لا فرق اذا كان الفعل أو الامتناع عنه معاقبا عليه أم غير معاقب عليه . وفي ذات المادة شدد القانون العقوبة لتصل إلى السجن اذا استهدفت الجريمة شخصية الانسان المعنوية بمدة لا تزيد على عشر سنوات إذا كان التهديد بارتكاب جناية أو بإسناد أمور خادشه للشرف أو الاعتبار.

ونظم المنظم معنى "مواد إباحية الاحداث " وفق هذا القانون على أنها أي صور أو تسجيلات أو رسومات أو غيرها مثيرة جنسياً لأعضاء جنسية أو أفعال جنسية حقيقية أو افتراضية أو بالمحاكاة لحدث لا يتجاوز الثامنة عشر من عمره، أو أنشطة للقمار، وكل ما من شأنه المساس بالآداب العامة. وحيث تعتبر المواد الإباحية وممارسة ألعاب القمار منافية لمبادئ الشريعة الإسلامية ولآداب وتقاليد المجتمع وتعتبر واحدة من أخطر الأمور التي ساعد الأنترنيت على انتشارها، عاقب القانون بالحبس والغرامة التي لا تقل عن مائتين وخمسين ألف درهم ولا تجاوز خمسمائة ألف درهم أو بإحدى هاتين العقوبتين كل من أنشأ أو أدار موقعاً الكترونيا أو أشرف عليه أو بث أو أرسل أو كل من نشر أو أعاد نشر عن طريق الشبكة المعلوماتية مواد إباحية. وشدد العقوبة في حالة توافر ظرف مشدد إذا كان موضوع المحتوى الإباحي حدثا لم يتجاوز الثامنة عشر من عمره، أو كان مثل هذا المحتوى مصمما لإغراء الأحداث (المادة ١٧).

وإيضاً في موضوع المواد الإباحية شدد القانون العقوبة في المادة (١٨) على كل من حاز عمداً مواد إباحية الأحداث باستخدام نظام معلومات الكتروني، أو شبكة معلوماتية، أو موقع الكتروني، أو إحدى وسائل تقنية المعلومات.

ومن منطلق محاربة جرائم الدعارة الالكترونية وحرص المشرع الإماراتي الحفاظ على المجتمع من مخاطرها، ومنع استغلال وسائل تقنية المعلومات لإرتكابها أو الترويج لها، عاقب القانون جرائم ارتكاب الدعارة أو الفجور باستخدام شبكة معلوماتية أو إحدى وسائل تقنية المعلومات بالسجن والغرامة التي لا تقل عن مائتين وخمسين ألف درهم ولا تجاوز مليون درهم أو بإحدى هاتين العقوبتين (المادة ١٩)، وفي نفس المادة شدد المشرع العقوبة لتصل الى

السـجن مدة لا تقل عن خمس سنوات والغرامة التـي لا تجـاوز مليون درهـم، فـي حالـة تـوفر ظرف مشدد إذا كان المجني عليه حدثا لـم يتم الثامنة عشر من عمره.

وحيث أن جرائم السب والقذف معاقب عليها ومن الجرائم الواقعة على السمعة كما وردت في مواد تجريمها في قانون العقوبات[٣٧]، ومن مبدأ الالتزام بالمعايير الأخلاقية، عاقب المنظم على هذه الجرائم بالحبس والغرامة أو بإحدى هاتين العقوبتين، وإذا وقع السب أو القذف في حق موظف عام أو مكلف بخدمة عامة بمناسبة أو بسبب تأدية عمله عد ذلك ظرفا مشدداً للجريمة (المادة ٢٠).

وعن ضمان توفير الحماية لحرمة الحياة الشخصية ولا يجوز للغير إنتهاكها بطرق حددها القانون والتي تعتبر من الجرائم المعاقب عليها [٣٨]، وذلك باستخدم شبكة معلوماتية، أو نظام معلومات الكتروني، أو إحدى وسائل تقنية المعلومات، وفي غير الاحوال المصرح بها، وهي استراق السمع، أو اعتراض، أو تسجيل أو نقل أو بث أو إفشاء محادثات أو اتصالات أو مواد صوتية أو مرئية، أو التقاط صور الغير أو إعداد صور الكترونية أو نقلها أو كشفها أو نسخها أو الاحتفاظ بها، أو نشر أخبار أو صور الكترونية أو صور فوتوغرافية أو مشاهد أو تعليقات أو بيانات أو معلومات ولو كانت صحيحة وحقيقية. ولمرتكبها عقوبة الحبس والغرامة أو بإحدى هاتين العقوبتين (المادة ٢١). وشدد القانون العقوبة بذات المادة في حالة إجراء أي تعديل أو معالجة على تسجيل أو صورة أو مشهد، بقصد التشهير أو الاساءة إلى شخص آخر، أو الاعتداء على خصوصيته أو إنتهاكها. وذلك بإستخدم نظام معلومات الكتروني، أو إحدى وسائل تقنية المعلومات.

وقررت المادة (٢٢) الحبس والغرامة أو بإحدى هاتين العقوبتين على كل من استخدم، بدون تصريح، أي شبكة معلوماتية، أو موقعاً الكترونيا، أو وسيلة تقنية معلومات لكشف معلومات سرية حصل عليها عن طريق عمله أو بسببه . ويقصد معنى سرية في هذا القانون أي معلومات أو بيانات غير مصرح للغير بالإطلاع عليها أو بإفشائها إلا بإذن مسبق ممن يملك هذا الإذن.

---

[٣٧]- ينظر المواد من (٣٧١- ٣٧٦)، من الفصل السادس المنظم لجرائم القذف والسب وإفشاء الاسرار من قانون العقوبات لدولة الإمارات العربية المتحدة رقم (٥٢) لسنة ٢٠٠٦.

[٣٨]- ينظر المواد من (٣٧٨- ٣٨٠)، من الفصل السادس المنظم لجرائم القذف والسب وإفشاء الاسرار من قانون العقوبات لدولة الإمارات العربية المتحدة رقم (٥٢) لسنة ٢٠٠٦.

وعن المواجهة الجنائية لجرائم الإتجار بالبشر نظراً لخطورتها عاقبت المادة (٢٣) بالسجن المؤقت والغرامة التي لا تقل عن خمسمائة ألف درهم ولا تجاوز مليون درهم أو بإحدى هاتين العقوبتين كل من أنشأ أو أدار موقعاً الكترونيا أو أشرف عليه أو نشر معلومات على شبكة معلوماتية أو بإحدى وسائل تقنية المعلومات، بقصد الاتجار في البشر أو الاعضاء البشرية، أو التعامل فيها بصورة غير مشروعة.

وتعتبر الجرائم الواردة في نص المادة (٢٤) من الجرائم الماسة بأمن الدولة وفق هذا القانون، وجاءت العقوبة بالسجن المؤقت والغرامة التي لا تقل عن خمسمائة ألف درهم ولا تجاوز مليون درهم، إذا كان قصد المجرم الالكتروني من أنشاء أو أدارة موقعاً الكترونيا أو أشرف عليه أو نشر معلومات على شبكة معلوماتية أو إحدى وسائل تقنية المعلومات لغرض الترويج أو التحبيذ الى برامج أو أفكار من شأنها إثارة الفتنة أو الكراهية أو العنصرية أو الطائفية أو الإضرار بالوحدة الوطنية أو السلم الاجتماعي أو الإخلال بالنظام العام أو الآداب العامة. وقد حرص المشرّع الاماراتي على إصدار ثقافة تشريعية قانونية في تعزيز قيم التسامح والتآخي، وعلى حماية السلم الاجتماعي وأمن الدولة، حيث جرم قانون مكافحة التمييز والكراهية رقم (٢) لسنة ٢٠١٥م [٣٩] الافعال المرتبطة بالتمييز والكراهية والفتن، وجاء اصداره قانوناً نموذجاً في هذا المجال.

وفي المادة (٢٥) جاء النص واضحاً في منهجية المشرّع في مكافحة جرائم الإتجار بالأسلحة، حيث عاقب القانون كل من أنشأ أو أدار موقعاً الكترونيا أو أشرف عليه أو نشر معلومات على شبكة معلوماتية أو إحدى وسائل تقنية المعلومات اذا ارتكبت بقصد الإتجار أو الترويج للأسلحة النارية أو الذخائر أو المتفجرات في غير الاحوال المصرح بها قانوناً، بالحبس مدة لا تقل عن سنة واحدة والغرامة التي لا تقل عن خمسمائة ألف درهم ولا تجاوز مليون درهم، أو بإحدى هاتين العقوبتين.

وفي إطار جهود المشرع الإماراتي لمكافحة الإرهاب وتقويضه ومحاربة مخططات الإرهابيين ومنها الجرائم الالكترونية، يظهر تنظيم مكافحة جرائم الإرهاب الالكتروني وإستخدام مواقع الكترونية أو اي وسيلة تقنيات في الأغراض الإرهابية في المادة (٢٦) من

[٣٩]- ينظر القانون الاتحادي رقم ٢ لسنة ٢٠١٥ في شأن مكافحة التمييز والكراهية لدولة الامارات العربية المتحدة.

القانون [٤٠].وجاء النص واضحاً وصريحاً لمواجهة هذه الجرائم الكبرى، والتي تعتبر من الجرائم الماسة بأمن الدولة. وقد حرص المشرّع الاماراتي على محاربة الجرائم الإرهابية ووضع لها أحكام قانون خاص لمكافحتها وهو القانون الاتحادي رقم (٧) لسنة ٢٠١٤م بشأن مكافحة الجرائم الالكترونية. [٤١] وعن الدعوة أو الترويج لجمع التبرعات بدون ترخيص معتمد من السلطة المختصة، جاء تنظيمها وفق المادة (٢٧) من القانون.

وحيث أن الامن الشامل لا يتحقق إلا بالحفاظ على أمن الدولة، حرص المشرّع وفق المادة (٢٨) على وجوب الحفاظ على أمن الدولة، حيث جرم فعل التحريض الذي من شأنه تعريض أمن الدولة ومصالحها العليا للخطر أو المساس بالنظام العام. وجاء النص صريحاً حيث نص على: (يعاقب بالسجن المؤقت والغرامة التي لا تجاوز مليون درهم كل من أنشأ أو أدار موقعاً الكترونيا أو أشرف عليه أو استخدم معلومات على الشبكة المعلوماتية أو وسيلة تقنية معلومات بقصد التحريض على أفعال، أو نشر أو بث معلومات أو أخبار أو رسوم كرتونية أو أي صور أخرى، من شأنها تعريض أمن الدولة ومصالحها العليا للخطر أو المساس بالنظام العام). يلاحظ في هذا النص حرص المشرّع على الحفاظ على أمن الدولة والنظام العام، وان الجرائم الواردة في هذه المادة من الجرائم الماسة بأمن الدولة، وإن الجريمة الجنائية تقع بتوافر القصد الجنائي، وإتجاه نية المتهم التحريض على أفعال لتعريض أمن الدولة ومصالحها للخطر أو المساس بالنظام العام.

وعن الجرائم التي تمس بشكل مباشر أمن الدولة عاقبت المادة (٢٩) كل من نشر معلومات أو أخبار أو بيانات أو إشاعات على موقع الكتروني أو أي شبكة معلوماتية أو وسيلة تقنية معلومات بقصد السخرية أو الاضرار بسمعة أو هيبة أو مكانة الدولة أو أي من مؤسساتها أو رئيسها أو نائبه أو حكام الامارات أو أولياء عهودهم أو نواب حكام الامارات أو علم الدولة أو السلام الوطني أو شعارها أو نشيدها الوطني أو رموزها، بالسجن المؤقت والغرامة التي لا تجاوز مليون درهم.

وفي نص المادة (٣٠) اتجه المشرع نحو تشديد العقوبة على الجرائم الخطيرة التي تمس بأمن الدولة، وجاء نص التجريم صريحاً وواضحاً، حيث نصت على (يعاقب بالسجن المؤبد كل من أنشأ أو أدار موقعاً الكترونيا أو أشرف عليه أو نشر معلومات على الشبكة

---

[٤٠]- ينظر نص المادة (٢٦) من القانون.

[٤١]- ينظر القانون الاتحادي رقم (٧) لسنة ٢٠١٤م بشأن مكافحة الجرائم الالكترونية لدولة الامارات العربية المتحدة.

المعلوماتية أو وسيلة تقنية معلومات، تهدف أو تدعو إلى قلب أو تغيير نظام الحكم في الدولة أو الاستيلاء عليه أو إلى تعطيل أحكام الدستور أو القوانين السارية في البلاد أو المناهضة للمبادئ الاساسية التي يقوم عليها نظام الحكم في الدولة. ويعاقب بالعقوبة ذاتها كل من روج إلى أو حرض على أي من الافعال المذكورة أو سهلها للغير). وتعتبر الجرائم الواردة في هذه المادة من الجرائم الماسة بالأمن الداخلي للدولة وعاقب عليها قانون العقوبات الإماراتي.

ونظمت المادة (٣١) عقوبة الحث والتحريض الى عدم الانقياد الى القوانين والأنظمة المعمول بها في الدولة عن طريق نشر معلومات، باستخدام الشبكة المعلوماتية او وسيلة تقنية، وجاءت العقوبة سالبة للحرية هي الحبس، ومالية وهي الغرامة، أو بإحدى هاتين العقوبتين.

وفي مكافحة جرائم الإتجار بالآثار أو التحف الفنية في غير الأحوال المصرح بها قانوناً، فقد عاقبت المادة (٣٣) بالحبس والغرامة التي لا تقل عن خمسمائة الف درهم ولا تجاوز مليون درهم او بإحدى هاتين العقوبتين كل من أنشأ او أدار موقعا إلكترونيا او أشرف عليه او استخدم الشبكة المعلوماتية او وسيلة تقنية معلومات للإتجار بالآثار أو التحف الفنية في غير الأحوال المصرح بها قانوناً.

وعن الانتفاع وتسهل للغير بغير وجه حق بخدمات الاتصالات أو قنوات البث المسموعة أو المرئية فقد نظمتها المادة (٣٤) من القانون.

وأفرد القانون نصاً خاصاً لجرائم الإساءة إلى أحد المقدسات أو الشعائر الإسلامية أو أحد الاديان السماوية المعترف بها، وذلك وفق المادة (٣٥) منه.

وعن مشكلة تعاطي المخدرات والمؤثرات العقلية لما لها من آثار مدمرة على المجتمعات على الصعيد الإجتماعي والإقتصادي والصحي، دفعت الدولة إلى بذل جهود متميزة على الصعيد التشريعي والتنفيذي للقضاء عليها ومحاربة انتشارها، حيث عاقب القانون في المادة (٣٦) منه بالسجن المؤقت والغرامة التي لا تقل عن خمسمائة ألف درهم ولا تجاوز مليون درهم أو بإحدى هاتين العقوبتين كل من أنشأ أو أدار موقعاً الكترونيا أو أشرف عليه أو نشر معلومات على الشبكة المعلوماتية، أو وسيلة تقنية معلومات وذلك لغرض الإتجار أو الترويج للمخدرات أو المؤثرات العقلية وما في حكمها أو كيفية تعاطيها أو لتسهيل التعامل فيها في غير الاحوال المصرح بها قانونا.

وحيث أن لجرائم الاموال الغير مشروعة أضرار وتبعات خطيرة، كاستنزاف الاقتصاد الوطني، وعدم استثمار الاموال في مشاريع تنموية الذي يساعد في ظهور مشاكل اقتصادية واجتماعية وسياسية منها تفشي ظاهرة البطالة. كما ان جرائم الاموال الغير مشروعة ترتبط بأخطر الجرائم كجرائم الاتجار بالمخدرات. ومن أجل ذلك لم يغفل المشرع عن خطورة إستخدام تقنية المعلومات وتسخيرها في جرائم الأموال الغير المشروعة، حيث عاقبت المادة (٣٧) بالحبس مدة لا تزيد على سبع سنوات وبالغرامة التي لا تقل عن خمسمائة الف درهم ولا تجاوز مليوني درهم كل من أتى عمداً، باستخدام شبكة معلوماتية، أو نظام معلومات إلكتروني، أو إحدى وسائل تقنية المعلومات، اي من الأفعال الآتية:تحويل الأموال غير المشروعة او نقلها او إيداعها بقصد إخفاء او تمويه المصدر غير المشروع لها. إخفاء او تمويه حقيقة الأموال غير المشروعة او مصدرها او حركتها او الحقوق المتعلقة بها او ملكيتها. اكتساب او حيازة او استخدام الأموال غير المشروعة مع العلم بعدم مشروعية مصدرها.

ويعاقب بذات العقوبة كل من أنشأ او أدار موقعا إلكترونيا او أشرف عليه او نشر معلومات على الشبكة المعلوماتية او وسيلة تقنية معلومات لتسهيل ارتكاب أي من الأفعال المنصوص عليها في الفقرة الأولى من هذه المـــادة او للتحريض عليها.

وجاءت العقوبة بالسجن المؤقت وفق المادة (٣٨) على كل مـن قـدم إلـى أي منظمات أو مؤسسات أو هيئات أو أي كيانات أخرى معلومات غير صحيحة أو غير دقيقة أو مضللة، وكان من شأنها الاضرار بمصالح الدولة، أو الاساءة إلى سمعتها أو هيبتها أو مكانتها. بإستخدام الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات. ووفق نص المادة (٤٤) من هذا القانون تعتبر الجرائم الواردة في نص هذه المادة من الجرائم الماسة بأمن الدولة.

وعن التخزين والإتاحة المتعمدة من قبل مالك أو مشغل لموقع إلكتروني أو شبكة معلوماتية، أي محتوى غير قانوني مع علمه بذلك، أو لم يبادر بإزالة أو منع الدخول إلى هذا المحتوى غير القانوني خلال المهلة المحددة في الإشعار الخطي الموجه له من الجهات المختصة والذي يفيد بعدم قانونية المحتوى وأنه متاح على الموقع الالكتروني أو شبكة المعلوماتية. فقد جاءت العقوبة الحبس والغرامة أو بإحدى هاتين العقوبتين (٣٩). وعاقب القانون على الشروع في الجنح المنصوص عليها في هذا المرسوم بقانون بنصف العقوبة المقررة للجريمة التامة (المادة ٤٠).

ولدى قراءة نص المادة (٤١) [٤٢] يتضح أن القانون يشترط عدم الإخلال بحق حسني النية فإذا كان مالك جهاز الكمبيوتر أو البرنامج سواء بعلمه أو بدون علمه اخذت منه لا يعلم إنها أخذت لغرض ارتكاب جريمة، كما اشترط القانون للحكم بعقوبة المصادرة أن تكون الاشياء التي يحكم بمصادرتها قد استعملت في ارتكاب الجرائم أو الأموال المتحصلة منها. ويتبين من نص المادة أيضا أن القانون قرر فضلاً عن العقوبات الاصلية أوجد عقوبة تكميلية وهي مصادرة الاجهزة أو البرامج أو الوسائل المستخدمة في ارتكاب الجريمة، او بإغلاق محل إرتكاب الجريمة أما إغلاق كلي أو مدة تركها المشرع للمحكمة لتقديرها. وعن إبعاد الاجنبي الذي يحكم عليه بالإدانة لارتكاب أي جريمة من الجرائم المنصوص عليها في هذا المرسوم . فقد نظمته المادة (٤٢) من القانون.

ومع عدم الاخلال بالعقوبات المنصوص عليها في هذا المرسوم بقانون. أجاز القانون للمحكمة وفق المادة (٤٣) أن تأمر بوضع المحكوم عليه تحت الاشراف أو المراقبة أو حرمانه من استخدام أي شبكة معلوماتية، أو نظام المعلومات الالكتروني، أو أي وسيلة تقنية معلومات أخرى، أو وضعه في مأوى علاجي أو مركز تأهيل للمدة التي تراها المحكمة مناسبة.

وفي المادة (٤٤) اعتبر القانون الجرائم الواردة في المواد (٢٨،٢٦،٢٤،٤،٣٨،٣٠،٢٩) من الجرائم الماسة بأمن الدولة. كما أعتبر من الجرائم الماسة بأمن الدولة أي جريمة منصوص عليها في هذا المرسوم بقانون إذا ارتكبت لحساب أو لمصلحة دولة أجنبية أو أي جماعة إرهابية أو مجموعة أو جمعية أو منظمة أو هيئة غير مشروعة.

وعن تخفيف العقوبة أو الإعفاء منها لمن أدلى من الجناة إلى السلطات القضائية أو الادارية بمعلومات تتعلق بأي جريمة من الجرائم المتعلقة بأمن الدولة وفقا لاحكام هذا المرسوم بقانون...، فقد نظمتها المادة (٤٥) وفق شروط متى أدى ذلك إلى الكشف عن الجريمة ومرتكبيها أو إثباتها عليهم أو القبض على أحدهم.

ويعد ظرفا مشدداً استخدام شبكة المعلومات أو الانترنت أو أي نظام معلوماتي الكتروني أو موقع الكتروني أو وسيلة تقنية معلومات عند ارتكاب أي جريمة لم ينص عليها هذا المرسوم بقانون. كما يعد ظرفا مشدداً ارتكاب أي جريمة منصوص عليها في

[٤٢]- ينظر نص المادة (٤١) من القانون.

هـذا المرسـوم بقانون لحسـاب أو لمصلحة دولة أجنبيـة أو أي جماعة إرهابية أو مجموعة أو جمعية أو منظمة أو هيئة غير مشروعة (المادة ٤٦).

ومـع عدم الإخلال بأحـكام الفصل الثاني من البـاب الثاني من الكتـاب الاول مـن قانـون العقوبـات، تسـري أحـكام هذا المرسوم بقانـون على كل من ارتكب إحـدى الجرائم الواردة به خارج الدولة، إذا كان محلهـا نظـام معلوماتـي الكترونـي أو شـبكة معلوماتية أو موقع الكتروني أو وسيلة تقنية معلومات خاصة بالحكومة الاتحادية أو إحـدى الحكومـات المحلية لإمـارات الدولـة أو إحـدى الهيئـات أو المؤسسات العامة المملوكة لأي منهما (المادة٤٧).

وقضت المادة (٤٨) بأنه لا يخل تطبيق العقوبات المنصوص عليها في هذا المرسوم بقانون بأي عقوبة أشد ينص عليها قانون العقوبات او اي قانون آخر. ويكـون للموظفين الذين يصدر بتحديدهم قرار من وزير العدل صفـة مأمـوري الضبط القضائـي في إثبات الأفعال التـي تقع بالمخالفة لأحكام هذا المرسوم بقانون، وعلى السلطات المحلية بالإمارات تقديم التسهيلات اللازمة لهؤلاء الموظفين لتمكينهم من القيام بعملهم.

ونظمت (المادة ٤٩) للموظفين الذين يصدر بتحديدهم قرار من وزير العدل صفـة مأمـوري الضبط القضائـي في إثبات الافعال التـي تقع بالمخالفة لأحكام هذا القانون، وعلى السلطات المحلية تقديم التسهيلات اللازمة لهؤلاء الموظفين لتمكينهم من القيام بعملهم. وتضمنت الأحكام الختامية للقانون المواد (٥٠ و ٥١) منه. [٤٣]

مما سبق يتضح أن القانون جاء موائماً لمعايير التشريعات والتنظيمات الدولية، وبشكل يتناسب ومتطلبات المجتمع، وغطى أغلب الجرائم المعلوماتية، كتنظيم جرائم الدخول للبرامج بغير تصريح، والجرائم المتعلقة بالتعدي على البيانات والمعلومات الشخصية، وجرائم إستغلال الاحداث، وجرائم البطاقات الائتمانية أو الالكترونية أو حسابات مصرفية، وجرائم الارهاب الالكتروني، والجرائم الماسة بأمن الدولة والنظام العام، وجرائم الإساءة للذات الالهية أو لذات الرسل والانبياء، وجرائم الإساءة إلى احد المقدسات أو الشعائر الإسلامية أو الإسـاءة إلى أحد المقدسـات أو الشـعائر المقـررة فـي الاديـان الاخـرى المصونـة وفقـا لاحكـام الشـريعة

[٤٣]- ينظر القانون رقم (٥) لسنة (٢٠١٢) في مكافحة جرائم تقنية المعلومات الإماراتي،٢٣,٢,٢٠١٧. متاح على الرابط
http://www.adjd.gov.ae/portal/binary/com.epicentric.contentmanagement.servlet.ContentDeliveryServlet/

الاسلامية، وجرائم الاتجار أو الترويج للمخدرات. وجاءت صياغة القواعد القانونية ملبية لمعايير الوضوح والدقة، وأوجد عقوبات تبعية كمصادرة الاجهزة أو البرامج أو الوسائل المستخدمة في ارتكاب الجريمة إضافة إلى العقوبات الأصلية. من حيث أن طبيعة الجريمة الالكترونية ذات طابع دولي عابرة للحدود، ورغم أن دولة الإمارات العربية المتحدة حققت مكانة دولية متقدمة في مجال التعاون الدولي لمكافحة الجريمة، يلاحظ في القانون أنه خلا من أحكام تتعلق بالتعاون الدولي في هذا الجانب. كما أن القانون خلا من أحكام تنظم جرائم حقوق الملكية، حيث أصدر المشرع الإماراتي عدداً من القوانين الخاصة في حماية الملكية الفكرية وهي تطبق الان.[٤٤]

وتبقى المتابعة المستمرة في مكافحة هذه الجرائم وتحديث القواعد القانونية لها ضرورة ملزمة للنظم القانونية في ضوء التطور السريع في تقنية المعلومات، أحد أهم الحلول المثلى لمكافحة هذه الجرائم والحد منها.

المبحث الثالث

مكافحة الجرائم الالكترونية في إطار التشريعات والاتفاقيات الدولية

تم قبول مصطلح "جرائم الإنترنت" على نطاق واسع واعتمد من قبل مجلس أوروبا في اتفاقية الجرائم الحاسوبية (٢٠٠١م) [٤٥]، ومن الصعب قياس تكاليف الجريمة الالكترونية، ولكنها تنمو وتكثر بشكل متزايد.[٤٦] وقد حذر الخبير الروسي يوجين كاسبرسكي Eugene Kaspersky المدير العام لشركة كاسبرسكي لاب Kaspersky Lab المتخصصة في مجال أمن الحواسيب، خلال كلمته أمام مؤتمر الفضاء السيبراني السنوي عام ٢٠١٢،الذي نظمته ورشة عمل "يوفال نيئمان" بمركز بحوث الامن القومي الاسرائيلي، من أن استمرار تطوير الاسلحة السيبرانية وانتشارها Cyber Weapons من شأنه أن يغير

[٤٤]- ينظر نص قانون اتحادي لدولة الإمارات العربية المتحدة رقم (٧) لسنة ٢٠٠٢م في شأن حقوق المؤلف والحقوق المجاورة.

[45] - Oerlemans, Jan-Jaap, Investigating cybercrime,2017, Leiden University,HIOA bibliotik, norway ,p 20.

[46] - Sofaer and Goodman (Cyber Crime and Security The Transnational Dimension), page 4, available at http://media.hoover.org/sites/default/files/documents/0817999825_1.pdf. 11.1.2017

وجه العامل الذي نعرفه، وأن البنية التحتية للعالم ليسـت مستعدة بعد لحامية نفسها من مثل هذه الاسـلحة.[٤٧]

وضمن الجهود الدولية لمكافحة الجرائم الالكترونية، تم إطلاق برنامج اليوم العالمي للأنترنيت الأمن (Safer internet Day) [٤٨] الذي يحتفل العالم به خلال شهر شباط/فبراير من كل عام -لأول مرة عام ٢٠٠٤ كمبادرة من الاتحاد الأوروبي والمنظمة الأوروبية للتوعية بشبكة الإنترنت "إنسيف" المهتمة بالقضايا ذات الصلة بالإنترنت .ويهدف اليوم العالمي إلى رفع الوعي بالمخاطر الكامنة في الإنترنت وأهمية الحفاظ على الخصوصية لدى الآخرين من خلال رفع الوعي بحالات الخطر والاستخدام السيء وعواقبه القانونية إضافة إلى تطوير معايير وأنظمة أخلاقية وسلوكية لائقة عند استخدام الإنترنت، إلى جانب توفير أدوات وبرامج تقنية وعملية مفيدة وسهلة الاستخدام وصولًا إلى تعزيز العمل المشترك نحو إيجاد آليات مناسبة للعمل نحو استخدام آمن للإنترنت. [٤٩] ومن هذا المنطلق وفي محاولة للإحاطة بأهم جانب من البحث، ولتوضيح نطاق تطور الحماية الدولية على الصعيد العالمي من هذه الجرائم، سنعرض أهم وابرز هذه الجهود، وتم تناول البحث وفق السياق الآتي:

المطلب الأول: مجموعة الدول الثماني: G8

اعتمد وزراء العدل والداخلية التابعين لبلدان الـ G8 في اجتماعاتهم المختلفة سياسات لمكافحة العديد من جرائم الإنترنت تستند إلى المبادئ التالية: عدم إتاحة ملاذات آمنة للمعتدين على تكنولوجيا المعلومات، التنسيق بين جميع الدول المعنية في ملاحقة مرتكبي جرائم الإنترنت ومحاكمتهم بغض النظر عن مكان حدوث الضرر، تدريب الموظّفين المكلفين تنفيذ القوانين، وتجهيزهم بالمعدات الضرورية للتعامل مع الجرائم ذات التقنية العالية. بالإضافة الى ذلك، دعت دول الـ G8 إلى مواصلة العمل حتى التوصّل إلى حلول دولية ناجحة، من خلال عقد اتفاقات دولية، لمعالجة الجريمة ذات التقنية العالية والاستفادة من عمل المنظمات الدولية المختلفة ومن تثمير الدراسات العديدة التي وضعتها دول الـ G8 ومن بينها: مبادئ وخطة العمل بشأن الجريمة ذات التكنولوجيا العالية وجرائم الكمبيوتر (١٩٩٧) ومبادئ بشأن الحصول على المعلومات المخزّنة على الكمبيوتر خارج حدود الدول (١٩٩٩) وتوصيات لتعقّب الاتصالات

---

[٤٧]- أ. ربيع محمد يحيى، ص ٧٧،مصدر سابق.

[48] . UK Safer internet Day.4.2.2014. https://www.saferinternet.org.uk/safer-internet-day/safer-internet-day-2016.

[٤٩]. Ait news. Safer internet Day.4.2.2017. https://aitnews.com/2016/02/09/%D8%AF%D9%88

على الشبكة خارج الحدود الوطنية في التحقيقات الإرهابية والإجرامية (٢٠٠٢) ومبادئ توافر البيانات الأساسية لحماية السلامة العامة (٢٠٠٢) وإعلان بيان دول G8 على نظم حماية المعلومات (٢٠٠٢).

وترى دول الـ G8 أن الحماية الفعالة ضد الجرائم ذات التقنية العالية تتطلّب الاتصال والتنسيق والتعاون داخليًا ودوليًا بين جميع أصحاب المصلحة في القطاع الخاص والأوساط الأكاديمية، والمؤسسات الحكومية. بناءً على ذلك، فإن دول الـ G8 التزمت تدريب جميع العاملين في مجال تطبيق القانون وتجهيزهم بالمعدات الضرورية لمكافحة جرائم الإنترنت. كما تعهّدت بمساعدة جميع البلدان الأعضاء على إقامة مراكز اتصال تعمل على مدار ٢٤ ساعة سبعة أيام في الأسبوع. إن وجود جرائم تعتمد التكنولوجيا المتقدّمة تطرح تحديات كبيرة على الأجهزة القضائية. فغالبًا ما يكون من الصعب على المحققين ذات المهارة العالية العمل بسرعة فائقة لحماية البيانات الالكترونية وتحديد المتهمين بخرق القانون. من هنا أهمية الشبكة التي طرحت دول الـ G8 إنشاءها لأنها ستمكّن من الاستجابة بسرعة كبيرة لطلبات السلطات الرسمية أو مستخدمي شبكات الانترنت. [٥٠]

المطلب الثاني: الاتفاقيات والمؤتمرات والبروتوكولات الدولية

لما كانت شبكة الانترنيت لا تخضع لأية حدود ولا لسيادة دولة وبالتالي للسيادة القانونية لدولة معينة ظهرت الجرائم الالكترونية على الصعيد الدولي فمرتكب الجريمة يكون في دولة مختلفة عن الدولة التي تقع فيها جريمته وأصبحت الجرائم منظمة organised crime الأمر الذي حدا بالمشرع الدولي للبحث عن إطار قانوني دولي يكون فيه التعاون بين الدول أمرا يكاد يكون ليس اختياريا لإيجاد حل لهذه الجرائم الحديثة. [٥١] وعلى طوال عقود من السنين، عقدت العديد من الإتفاقيات والمعاهدات والإعلانات والبروتوكولات الدولية المعنية بمكافحة الجرائم الالكترونية. وسنتناول في هذا المطلب هذه الجهود وفق السياق الآتي:

---

[٥٠]- د. جورج لبكي، مصدر سابق.

[٥١]. د. وليد طه – التنظيم التشريعي للجرائم الالكترونية في إتفاقية بودابست – بحث ألكتروني - ص ١٥ – ١١,١,٢٠١٧ - متاح على الرابط
http://www.lasportal.org/ar/legalnetwork/Documents/%D8%A7%D9%84%D8%AA

أولاً: الاتفاقيات الدولية

تعتبر الاتفاقية الدولية الأكثر أهمية في هذا المجال هي اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية، التي اعتمدت في عام ٢٠٠١. [٥٢] وفي بحثنا هذا حرصنا على استعراض هذه الإتفاقية كونها نموذج للجهود الدولية لمعالجة هذه الجرائم والتصدي لها، ومن ثم نستعرض أهم الاتفاقيات الدولية في هذا الجانب، وتم تناول البحث وفق السياق الآتي:

أ : الإتفاقية الاوربية لمكافحة الإجرام المعلوماتي والمســـماة (بودابست) لعام ٢٠٠١م:

هو صك دولي ملزم بشأن هذه المسألة، وهو بمثابة المبدأ التوجيهي لأي بلد لوضع تشريع وطني شامل لمكافحة جرائم الإنترنت وكإطار للتعاون الدولي بين الدول الأطراف في هذه المعاهدة. [٥٣]

ونظرا لازدياد الجرائم المتعلقة بالكمبيوتر شرعت الدول المتمدينة بوضع تشريعات خاصة لمكافحة جرائم الكمبيوتر التي تعتبر ظاهرة مستحدثة على علم الإجرام ومن هذه الدول الولايات المتحدة وفرنسا وباقي دول الإتحاد الاوربي الذي وضع إتفاقية حول جرائم الكمبيوتر سنة ٢٠٠١م، والتي أوصت فيها الدول الأعضاء بإتخاذ كافة الإجراءات التشريعية وغيرها حسب الضرورة لجعل الدخول إلى جميع نظم الكمبيوتر أو أي من أجزائه بدون وجه حق جريمة جنائية بحسب القانون المحلي، كما أوصت هذه الاتفاقية على مجموعة من المبادئ العامة المتعلقة بالتعاون الدولي في مجال الشئون الجنائية، وحددت كذلك الإجراءات المتعلقة بطلبات المساعدة المتبادلة بين الدول في غياب الاتفاقيات الدولية. [٥٤] وقد اعتمد الاتحاد الأوروبي التشريع على غرار اتفاقية بودابست. [٥٥] ويهدف واضعوا هذه الإتفاقية حث الدول الأعضاء على المواءمة بين القوانين الوطنية ونصوص الإتفاقية علاوةً على ضرورة استكمال

---

[٥٢] . How can we combat cyber crime?. A group of researchers are aiming to shed new light on how legislation can be used to stop these criminals. Article from university of oslo. 2017.1.17. available at http://sciencenordic.com/how-can-we-combat-cyber-crime.

[53] . Cypercrime-Budapest Convention and related standards-council of europe. 2017.1.17. availble at http://www.coe.int/en/web/cybercrime/the-budapest-convention.

[٥٤]. د. عبد العال الديبري الاستاذ محمد صادق إسماعيل ـ كتاب الجرائم الالكترونية . ص ٨. مصدر سابق.

55 . Cybercrime. EU Regulatory Framework on Cybercrime.norway.university of oslo. 2017.1.17. available at http://www.jus.uio.no/ifp/english/research/projects/nrccl/signal/research-prongs/cybercrime/.

الادوات القانونية لهذه الدول في المسائل الإجرائية وذلك بُغية تحسين الإتفاقية قدرات النيابات العامة على إجراء التحقيقات وجمع الادلة.[٥٦]

وقّعت على هذه الاتفاقية ٣٠ دولة، ولأهمية هذه الاتفاقية انضمَّ إليها العديد من الدول من خارج المجلس الأوروبي، وأبرز هذه الدول الولايات المتحدة الأمريكية، التي صادقت عليها في ٢٢ سبتمبر (٢٠٠٦ م). ودخلت حيز النفاذ في الأول من يناير (٢٠٠٧م).[٥٧] اما جمهورية المانيا الفدرالية فقد صادقت على الاتفاقية عام ٢٠٠٩، وصادقت فرنسا على الاتفاقية في ١٠ كانون الثاني ٢٠٠٦. أما مملكة النرويج فقد صادقت على هذه الاتفاقية سنة ٢٠٠٦.[٥٨] واشتملت على عدة جوانب من جرائم الإنترنت، بينها الإرهاب وعمليات تزوير بطاقات الائتمان ودعارة الأطفال.[٥٩] وتهدف الاتفاقية إلى:

١. توحيد عناصر القانون الجزائي المحلي مع الأحكام المتعلقة بالجرائم الإلكترونية.
٢. توفير الاجراءات القانونية اللازمة للتحري وملاحقة الجرائم المرتكبة الكترونيًا بواسطة الكمبيوتر.
٣. تعيين نظام سريع وفعال للتعاون الدولي.
٤. الحفاظ بشكل سريع على البيانات المخزّنة على أجهزة الكمبيوتر وحفظها والإفصاح الجزئي عن حركة هذه البيانات المخزنة على الكمبيوتر.
٥. جمع معلومات عن حركة البيانات وعن إمكان وجود تدخّل في محتواها .[٦٠]

واستنادا إلى المواد المشار إليها (٢- ١٣) فإن الاتفاقية تلزم الدول الاعضاء فيها (دول الاتحاد الاوربي وأية دولة توقع عليها أو تريد أن تنضم إليها) باتخاذ الاجراءات والتدابير التشريعية الملائمة لتجريم تسع جرائم في ميدان الجرائم المعلوماتية وهي:

١. الدخول غير القانوني المتعمد illegal access .
٢. الاعتراض غير القانوني illegal interception .

---

[٥٦]. أ. وسيم حرب - كتاب برنامج تعزيزحكم القانون في بعض الدول العربية- ص٧.
[٥٧]. «دعاوى الجرائم الإلكترونية وأدلة إثباتها في التشريعات العربية بين الواقع والمأمول»، ضمن فعاليات المؤتمر الثالث لرؤساء المحاكم العليا (النقض، التمييز، التعقيب) في الدول العربية المنعقد في جمهورية السودان الشقيقة خلال الفترة ٢٣-٢٥/٩م الموافق ٧-٩/١١/١٤٣٣هـ.ص ١٠.
[58] . Avner Levin and Daria Ilkina – p 20- 27.
[٥٩]. «دعاوى الجرائم الإلكترونية وأدلة إثباتها في التشريعات العربية بين الواقع والمأمول»، مصدر سابق .ص ١٠.
[٦٠]. د. جورج لبكي- المعاهدات الدولية للأنترنيت – مصدر سابق.

٣. التـدخل المتعمـد أو الارادي فـي المعطيـات data interference بالتـدمير damagin أو الحذف deletion أو التشويه والافساد deterioration أو تبديلها أو تغيرهـــا أو تعـــديلها alteration أو تعطيلهـــا أو كبتهـــا أو إخمادهـــا supperession.

٤. التدخل المتعمد في الانظمة system interference .

٥. التزوير المتعمد باستخدام جهاز الكمبيوتر computer-related forgery .

٦. إساءة استخدام الاجهزة Misuse of devices .

٧. الاحتيال المتعمد باستخدام الكمبيوتر computer-related fraud .

٨. الجـرائم المرتبطـة بـدعارة الأطفـال offences related to child pornography.

٩. الجرائم المرتبطة بحق المؤلف copyright and related offences .

وتناولت المادة (١١) من الاتفاقية القواعد العامة المتعلقة بالمساهمة الجنائية والعقوبة بشأن الجرائم المشار في المواد من (٢- ١٠)، وقد أوجبت الاتفاقية على الدول الاعضاء اتخاذ تدابير تشريعية للنص على المسؤولية عن الشروع والتدخل والتحريض في ارتكاب هذه الجرائم أو ما تختاره الدولة منها وذلك بغرض وجود رادع عام لما لهذه الجرائم من تأثير شديد على إقتصاديات الدول، وكذلك النص على مسؤولية الاشخاص المعنوية عن الافعال التي ترتكب لمصلحة الشخص المعنوي من قبل أي شخص يتصرف لمصلحته سواء كان إستنادا الى تمثيل قانوني أو باعتباره مناطاً به إتخاذ قرار عن الشخص القانوني أو لأنه خاضع لسلطته بما في ذلك افعال التحريض والتدخل والمساعدة الجنائية، وكذلك مسؤولية الرؤساء عن غياب أو تخلف الرقابة والإشراف والتحكم بتصرفات الاشخاص المعنيين بالعمل . يلاحظ هنا وفقاً للإتفاقية إمتداد نطاق المساءلة الجنائية للشخصين الطبيعي والمعنوي. أما بالنسبة للعقوبات والتدابير فقد أوجبت الاتفاقية على الدول الاعضاء في الإتفاقية إقرار العقوبات الملائمة والفعالة لهذه الجرائم بما فيها العقوبات المانعة للحرية بالنسبة للأشخاص الطبيعيين مثلما هو الحال في القانون الامريكي والغرامات المالية بالنسبة للأشخاص المعنوية. [٦١]

[٦١]. وليد طه – ص ١٥ - نقل بتصرف – مصدر سابق.

ومن أهداف الاتفاقية حماية الأطفال من الاستغلال الجنسي، فقد صاغت الإتفاقية في إطار دولي قواعد قانونية لمكافحة هذا الاستغلال الغير قانوني وهذا ما نظمته المادة (٩) من الإتفاقية.[٦٢]

وفي احترام حقوق الانسان، تؤكد ديباجتها وكذلك المادة رقم (١٥) أنه يجب الاخذ بعين الاعتبار الحاجة إلى ضمان وجود توازن مناسب بين المصالح المتحصلة من إجراء عملية قمعية واحترام حقوق الانسان الاساسية، ونص على ذلك أيضا العهد الدولي الخاص بالحقوق المدنية والسياسية التابع للأمم المتحدة. [٦٣]

ونظمت الاتفاقية تسليم المتهمين، حيث تنص المادة ٢٤ على وجوب تسليم المتهمين بين الاطراف فيما يتعلق بالجرائم الملحوظة في المواد من (٢ – ١١) من الإتفاقية، شرط أن تكون تلك الجرائم معاقبا عليها بموجب القوانين المرعية الإجراء في بلد كل من الطرفين المعنيين بحرمان من الحرية لفترة أقصاها سنة على الاقل، أو بعقوبة أشد في غياب اتفاق آخر جاري على أساس التشريعات المتبادلة الموحدة أو معاهدة نافذة حول موضوع تسليم المتهمين . [٦٤] وحول التنسيق التقني، تفرض المادة (٢٥/ ٣) من الاتفاقية، في حالة الاتصالات المتعلقة بطلبات التعاون المشترك » أن تتم هذه الاتصالات عبر قنوات توفر القدر الكافي من الامان والتوثيق بما في ذلك التشفير إذا تطلب الامر ذلك.

وعن التعاون الدولي، تنص المادة (٣٥) من الاتفاقية "كل دولة نقطة اتصال يمكن الاتصال بها على مدار 24 ساعة وكذا على مدار الاسبوع لضمان تقديم المساعدة الفورية أثناء التحقيق في الإنتهاكات القانونية المتعلقة بنظم وبيانات إلكترونية، أو بهدف جمع أدلة ذات طابع إلكتروني عن إنتهاكات قانونية.[٦٥] وقد طبقت كثير من البلدان الإتفاقية في إطار قوانينها الوطنية. ويتضح ذلك على سبيل المثال في تشريع رومانيا الذي يلتزم بنص الإتفاقية بشكل كبير. ويعتبر التشريع الروماني كاملاً وسهل الفهم وفعالاً في الوقت نفسه.[٦٦]

---

[٦٢]. أنظر المادة (٩) من الإتفاقية .

[٦٣]. جان فرنسوا هنرت – أهمية التعاون الدولي والتجربة البلجيكية في تبادل المعلومات بين عناصر الشرطة والتعاون القضائي- نقل بتصرف- مصدر سابق – ص ١٠٦- ١٠٩ .

[٦٤]. كرستينا سكولمان - كتاب برنامج تعزيزحكم القانون في بعض الدول العربية- مصدر سابق ص ١٢٠.

[٦٥]. جان فرنسوا هنرت – أهمية التعاون الدولي والتجربة البلجيكية في تبادل المعلومات بين عناصر الشرطة والتعاون القضائي- نقل بتصرف- مصدر سابق – ص ١٠٦- ١٠٩ .

[٦٦]. كرستينا سكولمان- مصدر سابق. ص ٦٤.

وبالتالي يمكن القول ان الاتفاقية ضمت مجموعة كبيرة من الجرائم الجنائية، وأنها تميزت بأهمية قانونية من حيث ركزت على اتخاذ التدابير التشريعية الموضوعية لمكافحة هذه الجريمة، وألزمت الدول إضافةً للقواعد الموضوعية الاهتمام بالقواعد الإجرائية، وعن أهمية المسؤولية الجنائية جاهد المشرع لتقنين قواعدها، وألزم الدول الاعضاء اتخاذ تدابير تشريعية ووضع القواعد القانونية لتنظيمها، وأوجب تعزيز أطر التعاون الدولي والإقليمي لاسيما توقيع معاهدات لتسليم المجرمين بين الدول حتى يفوت الفرصة على المجرمين الهروب من هذه الجرائم.

ب: أهم الاتفاقيات والمعاهدات الدولية المتعلقة بالجرائم الإلكترونية:

بعد أن أيقنت الدول هناك حاجة ملحة لعقد اتفاقيات من أجل مكافحة الجرائم السيبرانية لذا تم عقد العديد من الاتفاقيات والمعاهدات الدولية التي ساهمت في مكافحة الجرائم الالكترونية، منها:

١. إتفاقية حماية الأفراد في مجال المعالجة الالية للبيانات الشخصية (١٩٨١م).[٦٧]
٢. الاتفاقية الامريكية المتعلقة بجرائم الحاسب الالي والانترنيت لسنة ١٩٩٩: عقد في جامعة ستانفورد في ولاية كال فيورنيا في الولايات المتحدة مؤتمر للفترة من ٦ــ٧ ديسمبر ١٩٩٩ بمشاركة العديد من الهيئات والمنظمات الدولية والممثلين القانونيين وتم اقتراح هذه الاتفاقية لتعزيز الحماية من الارهاب وجرائم الحاسب الالي[٦٨].
٣. إتفاقية الامم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية، تم التوقيع عليها في مدينة باليرمو عام ٢٠٠٠ م.
٤. الإتفاقية الاوربية لمكافحة الإجرام المعلوماتي (بودابست)عام ٢٠٠١م.
٥. أتفاقية الامم المتحدة بشأن استخدام الخطابات الالكترونية في العقود الدولية (نيويورك، ٢٠٠٥).

---

67 . Council of Europe. Convention for the Protection of Individuals with regard to Automatic
Processing of Personal Data.
4.2.2017.https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId.

٦٨. د. محروس نصار غايب- الجريمة المعلوماتية- بحث منشور- ص ٢١.

ثانياً: المؤتمرات الدولية

لأبراز الجهود التي قطعتها الدول لمكافحة الجرائم السيبرانية في إطار المؤتمرات الدولية، سنحاول استعراض أهم وابرز هذه المؤتمرات التي ساهمت في مكافحة الجرائم الالكترونية، منها:

١. المؤتمر الدولي الاول لحقوق الإنسان الخاص بأثر التقدم التكنولوجي على حقوق الإنسان "مؤتمر طهران 1968" التي تبنت الجمعية العامة للأمم المتحدة توصياته، حيث تم الاعتراف بحق الخصوصية وبأن من حق الانسان أن يعيش لوحده بعيدا عن كشف أسراره، فسنت بعض دول العالم في أوربا وآسيا وأمريكا واليابان تشريعاتها في مجال حماية الخصوصية من الاعتداء عليها ألزمت من خلالها مواقع الانترنت المعنية بجمع المعلومات بتسجيل أغراضها وإخضاع عملياتها لرقابة مفوض الخصوصية في الدولة باعتباره جهة قضائية معنية بحماية الافراد من أي اعتداء عليها. [٦٩]
٢. مؤتمر الامم المتحدة الثامن لمنع الجريمة ومعاملة المجرمين والذي عقد في هافانا عام ١٩٩٠.
٣. مؤتمر الامم المتحدة العاشر الذي عقد في فيينا عام ٢٠٠٠م .
٤. القمة العالمية لمجتمع المعلومات التي عقدت في جنيف،١٠-١٢ ديسمبر ٢٠٠٣.
٥. أجندة تونس ٢٠٠٥ [٧٠]. الفقرة (١٥) من مبادىء المرحلة الثانية من القمة العالمية لمجتمع المعلومات تحت رعاية الامم المتحدة. [٧١]
٦. توصيات مؤتمر ورشة العمل على «التدابير الرامية إلى مكافحة الجريمة المتصلة بأجهزة الكمبيوتر»، الذي عقد في بانكوك في ٢٢ نيسان/أبريل ٢٠٠٥ كجزء من مؤتمر الأمم المتحدة الحادي عشر لمنع الجريمة والعدالة الجنائية. [٧٢]
٧. ورشتا عمل حول مكافحة استخدام الإرهابيين للإنترنت (١٨-٢٠٠٩/١٠/١٩) ومنع الإرهابيين من حيازة واستخدام أسلحة الدمار الشامل أو مكوناتها (٢٠-٢٠٠٩/١٠/٢١)، وقد عقدتا بمشاركة الأمانة العامة لمجلس وزراء الداخلية

---

[٦٩] .السيدة سيناء عبد هلال محسن - المواجهة التشريعية للجرائم المتصلة بالكمبيوتر في ضوء التشريعات الدولية والوطنية- أعمال الندوة الاقليمية حول« :الجرائم المتصلة بالكمبيوتر» - مصدر سابق – ص ٥٤.
[٧٠]. أجندة تونس، التي تم تبنيها في ١٥ نوفمبر ٢٠٠٥،متاح على الموقع pdf.fr_agenda_tunis/pdf.fr_agenda_11327544873tunis/20687/files/fr/ci/org
[٧١]. الاتحاد الدولي للاتصالات،القمة العالمية لمجتمع المعلومات،الوثائق الصادرة عن القمة، جنيف ٢٠٠٣ وتونس ٢٠٠٥م،مصدر سابق،ص ٥٩- ٧٧.
[٧٢]- د. جورج لبكي- المعاهدات الدولية للأنترنيت، نقل بتصرف – مصدر سابق.

العرب وخبراء من الدول العربية والأمم المتحدة والمنظمة العربية لتكنولوجيات الاتصال والمعلومات والمنظمات الإقليمية والدولية المعنية وصدر عن كل منهما مجموعة من التوصيات. [٧٣]

٨. المؤتمر العالمي لتنمية الاتصالات في حيدر آباد، الهند، (WTDC-10)، في يونيو ٢٠١٠م . و كان من بين المقررات أن الاتحاد ينبغي أن يساعد الدول الأعضاء، وخصوصاً البلدان النامية، في وضع التدابير القانونية المناسبة والعملية المتصلة بالحماية من التهديدات السيبرانية. [٧٤]

٩. مؤتمر الامم المتحدة الثاني عشر- البرازيل – سلفادور عقد عام ٢٠١٠م، غطى ثمان مسائل منها مشاكل جرائم الانترنت او الشبكة العنكبوتية. [٧٥]

١٠. مؤتمر الأمم المتحدة الثالث عشر لمنع الجريمة والعدالة الجنائية (٢-١٢ نيسان/ابريل لسنة ٢٠١٥) المنعقد في الدوحة.[٧٦]

١١. مؤتمر قمة الأمن السيبراني - مملكة البحرين ٢٢- ٢٠ أكتوبر ٢٠١٤: ناقشت هذه القمة الموضوعات التالية: بحث سبل إعادة الأمن واستراتيجية تكنولوجيا المعلومات، وإعادة تعريف المخاطر، وتنفيذ أفضل الممارسات لتحقيق مدونه التهديدات، وتخفيف مخاطر أدوات التواصل الاجتماعي الجديدة، واستراتيجية مواجهة التهديدات المتنقلة، والاستغلال الجنسي للأطفال.

١٢. مؤتمر قمة الأمن السيبراني مينابولس، مينيسوتا، الولايات المتحدة الامريكية ٢٢-٢١اكتوبر ٢٠١٤. شارك فيه ممثلون من القطاعين العام والخاص لمناقشة التدابر المضادة للتهديدات الالكترونية وتعزيز أمن القطاع العام والخاص في مواجهة الجرمية الالكترونية وقياس مدى تأمين برامج الحاسب الالي ضد الهجمات

---

[٧٣]. أ. عبد الله حامد الكيلاني، بحث ألكتروني منشوربعنوان جهود مكافحة الإرهاب النووي على الصعيد العربي،قطاع الشؤون القانونية جامعة الدول العربية،الرياض،٢٠١٣،ص ١٠.

[٧٤]. الاتحاد الدولي للإتصالات (ITU)، الأمن السيبراني ص٢١، متاح على الرابط https://www.itu.int/net/itunews/issues/2010/09/pdf/201009ar.pdf.١١,١,٢٠١٧

[٧٥]- wikipedia. - مؤتمرات الجريمة ومؤتمر ٢٠١٥. ٢٣,١,٢٠١٧.نقل بتصرف، متاح على https://ar.wikipedia.org/wiki/%D9%85%D8%A4%D8%AA%D

[٧٦]- UN. تقرير مؤتمر الأمم المتحدة الثالث عشر لمنع الجريمة والعدالة الجنائية الدوحة ٢٠١٥م، الفقرة ج من حلقة العمل بشأن تعزيز تدابير منع الجريمة والعدالة الجنائية للتصدِّي للأشكالالمتطوِّرة للجريمة، مثل الجرائم الإلكترونية (السيبرانية) والاتِّجار بالممتلكات الثقافية، بما في ذلك الدروس المستفادة والتعاون الدولي،ص٨٨. ٨,٢,٢٠١٧ . متاح على الرابط https://www.unodc.org/documents/congress//Documentation/Report/ACO

وتطوير تحقيقات الشرطة ومهارات التحقيق التقنية والادلة العلمية والاستراتيجيات الشاملة لمواجهة الجريمة الالكترونية.

١٣. مؤتمر الاتنربول واليورو بول الثاني للجريمة الإلكترونية سنغافورة ٣-١ أكتوبر ٢٠١٤م. INTERPOL/EUROPOL Cybercrime Conference 2014 ،1-3 October 2014

دعمت عقد هذا المؤتمر أحد الجهات الاعتبارية الدولية الفاعلة في مكافحة الجريمة الالكترونية وتعرف بـ "الجهود الدولية في الجريمة الالكترونية " وتسمى اختصارا "١٢٠" (GLACy) وقد أسهمت بدعمها بتمكين خبراء في الجريمة الإلكترونية من أكثر عشرين دولة من المشاركة في المؤتمر الذي يهدف الى تسهيل مهمة الوحدات المتخصصة في مكافحة الجريمة الإلكترونية في الاتصال بين بعضها البعض من خلال الشبكة الدولية International Networking.

١٤. مؤتمر الامن السيبراني/ جامعة نيويورك للتكنولوجيا ١٨سبتمرب ٢٠١٤: شارك في هذا المؤتمر خبراء الانترنيت والشركات والحكومات وناقش المؤتمر الموضوعات التالية: الخصوصية - الابتكارات في المؤسسة الاجنبية - أنظمة الأمن والأنترنت حماية البنية التحتية الحساسة والمنظمات والأفراد من الهجمات الإلكترونية.

١٥. مؤتمر (GLACY) لبناء القدرات في بور لويس عاصمة جزر موريشيوس ١٤ - ١١أغسطس٢٠١٤:

- GLACY :Capacity Building in Mauritius – Conference and workshops عقد هذا المؤتمر تحت رعاية "الجهود الدولية في الجريمة الالكرتونية GLACY" وقام مجلس أوربا للجرمية الالكرتونية بدعم سلسله من نشاطات بناء القدرات في الفترة من ١٤-١١ أغسطس ٢٠١٤ وناقشت ورش العمل والمؤتمر الموضوعات التالية: اتفاقية مجلس أوربا للجريمة الالكترونية. ومدى إمكانية حصول سلطات انفاذ القانون على المعلومات،
- (Law enforcement access to data)، واستراتيجيات تدريب منسوبي سلطات انفاذ القانون ومنسوبي السلطات القضائية. وحماية الطفل. وإعادة النظر في القانون الجنائي لمواكبة مقتضيات مكافحة الجريمة الإلكترونية. والتعاون الدولي.[٧٧]

[٧٧]- الجريمة الالكرتونية في المجتمع الخليجي وكيفية مواجهتها، ص ٧١- ٧٢ – مصدر سابق.

١٦. المؤتمر الدولي الأول لمكافحة الجرائم المعلوماتية الذي نظمته جامعة الأمام محمد بن سعود الإسلامية ممثلة في كلية علوم الحاسب والمعلومات وذلك في الفترة من ١٠ إلى ١٢ نوفمبر ٢٠١٥ م .[٧٨]

١٧. المؤتمر العالمي الرابع للفضاء الإلكتروني" الذي إنعقد في مدينة لاهاي بهولندا خلال الفترة ١٦-١٧ أبريل لعام ٢٠١٥م.

ثالثاً: البروتوكولات والإعلانات الدولية

من الجهود التي قطعتها الدول لمكافحة الجرائم السيبرانية في إطار البروتوكولات والإعلانات الدولية والتي ساهمت في مكافحة هذه الجرائم والتصدي لها:

١. إعلان فينا لعام ٢٠٠٠ م، حيث قررت الفقرة 18 من الإعـــــــلان (نقرر صوغ توصيات سياساتية ذات توجه عملي بشأن منع ومكافحة الجريمة المتعلقة بالحواسيب، وندعو لجنة منع الجريمة والعدالة الجنائية إلي الاضطلاع بعمل في هذا الشأن، آخذة في الاعتبار الأعمال الجارية في محافل أخرى. ونعلن التزامنا أيضا بالعمل على تعزيز قدرتنا على منع الجريمة المرتبطة بالتكنولوجيا الراقية والحواسيب والتحري عن تلك الجرائم وملاحقتها).[٧٩]

٢. إعلان بانكوك (18 to 25 April 2005) الفقرة ١٥، ١٦، حيث أكد على اهمية تعاون الدول في المسائل الجنائية لا سيما ضد جرائم الإنترنت. وملاحقة التكنولوجيا العالية والجرائم ذات الصلة بالحاسوب. [٨٠]

٣. بروتوكول ستراسبورغ تم وضعه سنة ٢٠٠٣، وهو إمتداد لإتفاقية بودابست لمكافحة الجرائم الالكترونية. [٨١]

٤. إعلان دوفيل لمجموعة دول G8 لعام ٢٠١١م، إتفقت الدول الأعضاء على إلتزامها على حماية حقوق الملكية الفكرية من الإنتهاكات التي تحصل على شبكة الأنترنيت. [٨٢]

---

78 - www.arabnews.com/saudi-arabia/news/778886. 25.2.2017.

79 . UN. Vienna Declaration on Crime and Justice. Article 18. 1.2.2017. available at https://www.unodc.org/documents/commissions/CCPCJ/Crime

80 .UN. BANGKOK DECLARATION. . Article 15-16. 1.2.2017. . available at http://www.un.org/events/11thcongress/declaration.

81 . Council of Europe- Details of Treaty No.189- 2017.1.18-available at https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189

82 -For more information visit . university of Toronto. 2011 Deauville G8 Summit

رابعاً: القوانين والقرارات الدولية:

أهم القرارات والقوانين الدولية التي ساهمت في مكافحة الجرائم السيبرانية:

١. قانون الانسيترال بشأن التوقيعات الالكترونية عام ٢٠٠١م.[٨٣]
٢. قانون الانسيترال النموذجي بشأن التجارة الإلكترونية لعام ١٩٩٦: تاريخ الاعتماد 12 :حزيران/ يونيه ١٩٩٦ (المادة الإضافية ٥ مكررا بصيغتها المعتمدة في عام ١٩٩٨(يهدف القانون النموذجي بشأن التجارة الإلكترونية (القانون النموذجي) إلى التمكين من مزاولة التجارة باستخدام وسائل إلكترونية وتيسير تلك الأنشطة التجارية من خلال تزويد المشرعين الوطنيين بمجموعة قواعد مقبولة دوليا ترمي إلى تذليل العقبات القانونية وتعزيز القدرة على التنبّؤ بالتطورات القانونية في مجال التجارة الإلكترونية.[٨٤]
٣. القرار ١٢١/٤٥ العام ١٩٩٠، وكذلك نشر دليل منع الجرائم المتصلة بأجهزة الكمبيوتر ومكافحتها في العام ١٩٩٤.
٤. القرارات ٧٠/٥٣ في ٤ كانون الأول/ديسمبر ١٩٩٨، و٤٩/٥٤ في ١ كانون الاول/ديسمبر ١٩٩٩، ٢٨/٥٥ في ٢٠ تشرين الثاني/نوفمبر ٢٠٠٠ و١٩/٥٦ في ٢٩ تشرين الثاني/نوفمبر ٢٠٠١ و٥٣/٥٧ في ٢٢ تشرين الثاني/نوفمبر ٢٠٠٢ و٣٢/٥٨ في ١٨ كانون الأول/ديسمبر ٢٠٠٣ حول موضوع «التطورات في ميدان المعلومات والاتصالات في سياق الأمن الدولي».
٥. القرارات ٦٣/٥٥ في ٤ كانون الأول/ديسمبر ٢٠٠٠، و١٢١/٥٦ في ١٩ كانون الأول/ديسمبر ٢٠٠١ بشأن «مكافحة إستخدام نظم المعلومات الإدارية الجنائية لتقنية المعلومات».
٦. القرار ٢٣٩/٥٧ في ٢٠ كانون الاول/ ديسمبر ٢٠٠٢ بشأن «إنشاء ثقافة عالمية للأمن السيبراني».

Final Compliance Report.25.2.2017.p.238. http://www.g8live.org/wp-content/uploads/2014/09/2011g8finalcompliance.pdf.

[83].available.www.uncitral.org/uncitral/ar/uncitral_texts/electronic_commerce/2001Model_23. 1.2017.

[84] . UNCITRAL Model Law on Electronic Commerce (1996). 9.1.2017.

http://www.uncitral.org/uncitral/en/uncitral_texts/electroni

٧. قرارات الجمعية العامة ٢٣٩/٥٧ في ٣١ كانون الثاني/يناير ٢٠٠٣ و١٩٩/٥٨ في ٣٠ كانون الثاني/يناير ٢٠٠٤ بشأن «إنشاء ثقافة عالمية للأمن السيبراني».

٨. القرار CCPCJ 16/2/2007 من نيسان/أبريل ٢٠٠٧ «المنع الفعال للجريمة والعدالة الجنائية لمكافحة الاستغلال الجنسي للأطفال» (الفقرات ٧، ١٦).

٩. قرار المجلس الاقتصادي والاجتماعي E/2007/20 بتاريخ ٢٦ تموز/يوليو ٢٠٠٧ بعنوان «التعاون الدولي من أجل منع وتحري ومقاضاة ومعاقبة جرائم الاحتيال الاقتصادي والجرائم المتصلة بالهوية» (E/2007/30 وE/2007/SR.45).

١٠. قرار المجلس الاقتصادي والاجتماعي ٢٦/٢٠٠٤ بتاريخ ٢١ تموز/يوليو ٢٠٠٤ بعنوان «التعاون الدولي لمنع التحقيق والمقاضاة والمعاقبة على الاحتيال، وإساءة استعمال الهوية وتزييفها والجرائم ذات الصلة».

١١. قرار لجنة مكافحة المخدرات ٥/٤٨ حول «تعزيز التعاون الدولي من أجل منع استخدام شبكة الإنترنت لارتكاب الجرائم المتصلة بالمخدرات».

١٢. الفقرة ١٧ من قرار الجمعية العامة ١٧٨/٦٠ المؤرخ ١٦ كانون الاول/ديسمبر ٢٠٠٥ بخصوص «التعاون الدولي لمكافحة مشكلة المخدرات العالمية».

١٣. قرار لجنة مكافحة المخدرات ٨/٤٣ في ١٥ آذار/مارس ٢٠٠٠ عبر الإنترنت.

١٤. قرار المجلس الاقتصادي والاجتماعي ٤٢/٢٠٠٤ بشأن «بيع المخدرات المشروعة الخاضعة للمراقبة الدولية إلى الأفراد عن طريق الإنترنت».

١٥. مختلف توصيات الهيئات الفرعية التابعة للجنة مكافحة المخدرات واللجنة الفرعية المعنية بالإتجار غير المشروع بالمخدرات والمسائل المتعلقة بالشرقين الأدنى والأوسط.

١٦. التوصيات والمبادئ التوجيهية للهيئة الدولية لمراقبة المخدرات(INCB)التي نشرت العام ٢٠٠٥ وتوصيات للحد من انتشار المبيعات غير المشروعة من المواد الخاضعة للرقابة ولا سيما المستحضرات الصيدلانية، عبر الإنترنت. [٨٥]

١٧. ووفقاً للقرار56/183 للجمعية العامة للأمم المتحدة تم تنظيم القمة العالمية من مرحلتين- جنيف، 10-12 ديسمبر 2003 وتونس 16-18 نوفمبر 2005.[٨٦]

---

[٨٥]. د. جورج لبكي- المعاهدات الدولية للأنترنيت، نقل بتصرف – مصدر سابق.

[٨٦]. القمة العالمية لمجتمع المعلومات، جنيف ٢٠٠٣ وتونس ٢٠٠٥م،٢٩,١,٢٠١٧. متاح على الرابط http://www.itu.int/net/wsis/index-ar.html

المطلب الثالث: التشريعات الدولية الإقليمية التي اهتمت بمعالجة هذه المشكلة والتصدي لها:

لإبراز الجهود الإقليمية للدول في مكافحة الجرائم السيبرانية، سنحاول استعراض أهم وابرز هذه الجهود على صعيد التشريعات العربية والاجنبية منها:

١. الاتفاقية العربية لمكافحة جرائم تقنية المعلومات في عام ٢٠١٠. (League of Arab States Convention) .
٢. الإتحاد الاوربي.[٨٧] قرار اتخذه المجلس يحث فيه الدول الاعضاء على تكثيف وتعزيز التعاون الدولي بين أجهزة الشرطة لمكافحة استغلال الاطفال في إنتاج المواد الاباحية على الانترنت.[٨٨]
٣. قرار مجلس الاتحاد الاوروبي رقم ٦٨ لعام ٢٠٠٤ بشأن مكافحة تعرض الاطفال للفساد الجنسي وإباحية الاطفال. [٨٩]
٤. قانون الإمارات العربي الإسترشادي لمكافحة جرائم تقنية المعلومات وما في حكمها، اعتمده مجلس وزراء العدل العرب في دورته التاسعة عشرة بالقرار رقم ٤٩٥ - د ١٩ – ٨,١٠,٢٠٠٣ ومجلس وزراء الداخلية العرب في دورته الحادية والعشرين بالقرار رقم ٤١٧ - د ٢١. ٢٠٠٤.
٥. عام ٢٠٠٦ تم في بوخارست، تنظيم المؤتمر الاقليمي لدول شرق أوروبا وأسيا الوسطى بشأن مكافحة التزييف والقرصنة في ١١ و١٢ يوليو ٢٠٠٦. [٩٠]
٦. المؤتمر الاقليمي للدول العربية حول جرائم الانترنت والذي عقد في القاهرة بتاريخ ٢٦ و٢٧ نوفمبر 2007 م.
٧. القانون العربي الإسترشادي للإثبات بالتقنيات الحديثة (٢٠٠٨م): إعتمده مجلس وزراء العدل العرب بقرار رقم (٧٧١/ د٢٤ – ٢٠٠٨/١١/٢٧).
٨. إتفاقية الإتحاد الافريقي الخاصة بمجال الامن السيبراني لعام ٢٠١٤م.
٩. إتفاقية كومنولث الدول المستقلة The Commonwealth of Independent States.

---

[٨٧]. قرار المجلس بتاريخ ٢٩ مايو ٢٠٠٠،متعلق بمكافحة استغلال الاطفال في إنتاج المواد الاباحية على الانترنت (JAI/٣٧٥/٢٠٠٠) الجريدة الرسمية للاتحاد الاوروبي، ٩ يونيو ٢٠٠٠،سطر ١/١٣٨.
[٨٨]. جان فرنسوا هنرت – مصدر سابق - ص ١٠٧.
[٨٩]. أ. خالد محي الدين احمد – الجرائم المتعلقة بالرغبة الأشباعية باستخدام الكمبيوتر- اعمال الندوة الاقليمية حول الجرائم المتصلة بالكمبيوتر- الدار البيضاء- ٢٠٠٧- ص ٣٧.
[٩٠]- السيدة كريستينا سكولمان- مصدر سابق- ص ٤٧.

١٠. المؤتمر الإقليمي العربي التحضيري للقمة العالمية لمجتمع المعلومات لعام ٢٠٠٣م، والذي استضافته جمهورية مصر العربية، بالتعاون مع جامعة الدول العربية وبحضور وزراء الاتصالات العرب.

١١. المؤتمر الإقليمي للأمن السيبراني الثالث، خلال الفترة من ٢٠ إلى ٢١ مارس ٢٠١٤ الذي نظمه المركز الاقليمي العربي للأمن السيبراني للاتحاد الدولي للاتصالات في سلطنة عمان ،الذي تستضيفه السلطنة ممثلة في هيئة تقنية المعلومات.

١٢. المؤتمر الإقليمي للأمن السيبراني ،خلال الفترة من ٢٩ إلى ٣٠ مارس ٢٠١٥ الذي نظمه المركز الاقليمي العربي للأمن السيبراني للاتحاد الدولي للاتصالات في سلطنة عمان ، وبالتعاون مع المكتب الإقليمي العربي للاتحاد الدولي للاتصالات.[٩١]

النتائج: خرجت الدراسة بجملة من النتائج منها:

١. عدم الإجماع الدولي في تعريف الجريمة الالكترونية لغاية إعداد هذا البحث.

٢. تستهدف جرائم نظم المعلومات في المقام الأول المؤسسات المالية.

٣. عدم توافر إحصاءات دولية دقيقة حول حجم هذه الجرائم، إلا أن التقارير والوقائع، تشير إلى ظاهرة إتساعها.

٤. عدم كفاية الإتفاقيات الدولية في مجال تسليم المجرمين، وهناك حاجة إلى تشريعات أكثر فاعلية كعقد الإتفاقيات الثنائية أو متعددة الاطراف لتفعيل التعاون الدولي لمكافحة هذه الجرائم، وتضمين بنودها بموضوع التعاون الدولي القانوني والقضائي والأمني نظراً لطابع الجريمة الدولي.

٥. رغم تنامي التشريعات التي نظمت مكافحة الجرائم الإلكترونية على الصعيد الوطني والإقليمي والدولي. هناك حاجة في التنفيذ والتطبيق الأمثل وبمهنيـــة لهذه التشريعات والقوانين.

٦. ترى الباحثة من أخطر صور إرتكاب الجرائم الالكترونية جرائم الإنتحار، ولم يحظى بإهتمام المختصين في الجرائم الالكترونية باعتباره أحد أخطر صور إرتكاب الجرائم الالكترونية.

٧. بعض الدول ليس لديها قانون خاص مستقل يعاقب كل تلك الجرائم ويتصدى لها واكتفت بالإعتماد على قانون العقوبات وغيره من القوانين.

---

[٩١]- شبكة الهيئات العربية لتنظيم الاتصالات. http://www.aregnet.org/ar/%D9%85%D9%. ٢٦,٢,٢٠٢٧

التوصيات: خرجت الدراسة بجملة من التوصيات منها:

١. إصدار القوانين الخاصة المستقلة في مكافحة الجرائم السيبرانية، لتلبية الحاجة للنصوص القانونية العقابية والإجرائية.
٢. تضمين النصوص القانونية الوطنية والدولية بقواعد تنظم جرائم الانتحار عن طريق الأنترنيت بإعتبارها من أخطر صور إرتكاب الجرائم الالكترونية.
٣. مواكبة تطورات هذه الجريمة وأساليبها وهذا يستوجب تحديث القواعد القانونية لهذه الجرائم، هي أحد أهم الحلول المثلى لمكافحة هذه الجرائم .
٤. التنفيذ والتطبيق الأمثل وبمهنيـــة للتشريعات والقوانين الخاصة بمكافحة هذه الجرائم.
٥. تفعيل نصوص القوانين الوطنية والدولية الخاصة بالتعاون الدولي في مجال الامان السيبراني والعمل القضائي كالملاحقات القضائية وسرعة محاكمة مرتكبي هذه الجرائم، ذلك ان جهود مكافحة هذه الجرائم لا يمكن أن تكون فعالة إلا بتعاون جميع الدول والمنظمات الدولية والإقليمية، على سبيل المثال . وتشجيع الدول الإنضمام إلى الصكوك الدولية لمحاربة هذه الجرائم العابرة للحدود.
٦. رفع ثقافة القائمين على إنفاذ القانون وتدريبهم سواء من السلطة القضائية أم من السلطة التنفيذية وإيلاء إهتمام بالخبراء وتأهيلهم على مستوى عال من المعرفة بتقنية المعلومات.
٧. أحد اهم الحلول نشر الثقافة المجتمعية في كيفية إستخدام تقنية المعلومات بالصورة التي تجنب مخاطر القرصنة hacking والاختراق cracking وغيرها من صور الجرائم الإلكترونية، وذلك بتضمين المناهج الدراسية عموماً والجامعية خصوصاً بهذه الثقافة. وعقد الندوات للتوعية والتركيز على فئة الشباب والأطفال من كلا الجنسين وبمشاركة واسعة من المجتمع المدني.

المراجع باللغة العربية:

أولاً: الكتب

١. أ .د. علي علي فهمي، دور الشبكات الاجتماعية في تمويل وتجنيد الارهابيين، كتاب إستعمال الانترنيت في تمويل الارهاب وتجنيد الارهابيين، مكتبة جامعة نايف، الطبعة الاولى، الرياض، ٢٠١٢.

٢. . د. عبد العال الديبري، الاستاذ محمد صادق إسماعيل، كتاب الجرائم الالكترونية، المركز القومي للإصدارات القانونية. الطبعة الاولى ٢٠١٢.
٣. أ. وسيم حرب – كتاب برنامج تعزيز حكم القانون في بعض الدول العربية – مشروع تحديث النيابات العامة- كتاب أعمال الندوة حول الجرائم المتصلة بالكمبيوتر. المملكة المغربية ٢٠٠٧.

ثانياً: المجلات العلمية

١. أ . عادل يوسف عبد النبي الشكري، الجريمة المعلوماتية وأزمة الشرعية الجزائية، مجلة ـ العراق ـ جامعة الكوفة ـ العدد السابع ٢٠٠٨.
٢. د. جورج لبكي- المعاهدات الدولية للأنترنيت – مجلة الدفاع الوطني.

ثالثاً: المراجع من المواقع الكترونية

١. ذياب موسى البداينةـ ورقة علمية بعنوان الجرائم الالكترونية المفهوم والأسباب - الملتقى العلمي الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية- ٢٠١٤- عمان . المملكة الاردنية الهاشمية.
٢. ويكيبيديا – الجريمة الالكترونية.
٣. «دعاوى الجرائم الإلكترونية وأدلة إثباتها في التشريعات العربية بين الواقع والمأمول»، ضمن فعاليات المؤتمر الثالث لرؤساء المحاكم العليا (النقض، التمييز، التعقيب) في الدول العربية المنعقد في جمهورية السودان الشقيقة خلال الفترة ٢٣-٩/٢٥/م الموافق ٧-١٤٣٣/١١/٩هـ.
٤. د. يونس حرب - جرائم الكمبيوتر والانترنت- ايجاز في المفهوم والنطاق والخصائص والصور والقواعد الاجرائية للملاحقة والاثبات- ورقة عمل مقدمة الى مؤتمر الامن العربي ٢٠٠٢ – تنظيم المركز العربي للدراسات والبحوث الجنائية - ابو ظبي ١٠- ١٢ /٢٠٠٢/٢.
٥. . القاضي كاظم عبد كاظم الزيديـ بحث بعنوان مكافحة الجرائم المعلوماتية في التشريع العراقي موقع السلطة القضائية الإتحاديةـ ٢٠١٢/١٠/١٥.
٦. أ . جان فرنسوا هنروت - أهمية التعاون الدولي والتجربة البلجيكية في تبادل المعلومات بين عناصر الشرطة والتعاون القضائي- أعمال الندوة الاقليمية حول : «الجرائم المتصلة بالكمبيوتر- برنامج تعزيز حكم القانون في بعض الدول العربية.

٧. وكالة سكاي برس، لعبة تؤدي بحياة عشرات المراهقين الروس.
٨. الجريمة الالكرتونية في المجتمع الخليجي وكيفية مواجهتها.اعداد مجمع البحوث والدراسات أكاديمية السلطان قابوس لعلوم الشرطة،٢٠١٦.
٩. دليل الامن السيبراني للدول النامية،الإتحاد الدولي للإتصالات.
١٠. د. نبال إدلبي و السيدة هانيا ديماسي، مذكرة سياساتية تطوير وتنسيق التشريعات السيبرانية في المنطقة العربية،(اللجنة الاقتصادية والاجتماعية لغربي آسيا، الإسكوا).
١١. د. وليد طه – التنظيم التشريعي للجرائم الالكترونية في إتفاقية بودابست.
١٢. د. ناصر بن محمد البقمي، مكافحة الجرائم المعلوماتية وتطبيقاتها في دول مجلس التعاون لدول الخليج العربي، ١١٦ سلسة محاضرات الامارات، مركز الإمارات للدراسات والبحوث الإستراتيجية، الطبعة الاولى ٢٠٠٨م .
١٣. كرستينا سكولمان، اعمال الندوة الاقليمية، برنامج تعزيزحكم القانون في بعض الدول العربية.
١٤. د. محروس نصار غايب- الجريمة المعلوماتية.
١٥. السيدة سيناء عبد هلال محسن،أعمال الندوة الاقليمية حول«الجرائم المتصلة بالكمبيوتر» .
١٦. أجندة تونس، التي تم تبنيها في ١٥ نوفمبر ٢٠٠٥ .
١٧. . الاتحاد الدولي للاتصالات،القمة العالمية لمجتمع المعلومات،الوثائق الصادرة عن القمة، جنيف ٢٠٠٣ وتونس ٢٠٠٥م.
١٨. أ. عبد الله حامد الكيلاني، بحث ألكتروني منشوربعنوان جهود مكافحة الإرهاب النووي على الصعيد العربي،قطاع الشؤون القانونية جامعة الدول العربية،الرياض .
١٩. الاتحاد الدولي للإتصالات (ITU)، الأمن السيبراني .
٢٠. - wikipedia. - مؤتمرات الجريمة.
٢١. تقرير مؤتمر الأمم المتحدة الثالث عشر لمنع الجريمة والعدالة الجنائية الدوحة ٢٠١٥م.
٢٢. أ. خالد محي الدين احمد،الجرائم المتعلقة بالرغبة الأشباعية باستخدام الكمبيوتر، اعمال الندوة الاقليمية حول الجرائم المتصلة بالكمبيوتر- الدار البيضاء- ٢٠٠٧.

in English and Norwegian:

1. Petter Gottschalk,datakriminalitet i Norge, 2011, fylkesbiblioteket i Akershus.
2. UN conference weighs efforts to combat cybercrime, create safer digital world- UN news centre.
3. Oerlemans, Jan-Jaap, Investigating cybercrime,2017, Leiden University,HIOA bibliotik, norway.
4. Shipley , Todd G. Bowker, Art, Investigating internet Crimes, HIOA bibliotik, Norway.
5. Template.http://isper.escwa.un.org/FocusAreas/CyberLegislation/Template/tabid/201/language/en-US/Default.aspx.
6. http://isper.escwa.un.org/FocusAreas/CyberLegislation/Projects/tabid/161/language/en-US/Default.aspx. .
7. The Computer Emergency Response Team. About (aeCERT) .. https://www.tra.gov.ae/aecert/en/about-us/our-story-and-goals.aspx
8. Oerlemans, Jan-Jaap, Investigating cybercrime,2017, Leiden University,HIOA bibliotik, norway.
9. Sofaer and Goodman (Cyber Crime and Security The Transnational Dimension), page 4, available at http://media.hoover.org/sites/default/files/documents/0817999825_1.pdf.
10. UK Safer internet Day.4.2.2014. https://www.saferinternet.org.uk/safer-internet-day/safer-internet-day-2016.
11. Ait news. Safer internet Day.4.2.2017. https://aitnews.com/2016/02/09/%D8%AF%D9%88

12. How can we combat cyber crime?. A group of researchers are aiming to shed new light on how legislation can be used to stop these criminals. Article from university of oslo. 2017.1.17. available at http://sciencenordic.com/how-can-we-combat-cyber-crime.
13. Cypercrime-Budapest Convention and related standards-council of europe. 2017.1.17. availble at http://www.coe.int/en/web/cybercrime/the-budapest-convention.
14. Cybercrime. EU Regulatory Framework on Cybercrime.norway.university of oslo. 2017.1.17. available at http://www.jus.uio.no/ifp/english/research/projects/nrccl/signal/research-prongs/cybercrime/.
15. Avner Levin and Daria Ilkina.
16. Council of Europe. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.
17. https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId.
18. UN. Vienna Declaration on Crime and Justice. Article 18. 1.2.2017. available at https://www.unodc.org/documents/commissions/CCPCJ/Crime
19. UN. BANGKOK DECLARATION. . Article 15-16. 1.2.2017. available at http://www.un.org/events/11thcongress/declaration.
20. Council of Europe- Details of Treaty No.189- 2017.1.18- available at https://www.coe.int/en/web/conventions/full-lis

21. For more information visit . university of Toronto. 2011 Deauville G8 SummitFinal Compliance Report.25.2.2017. http://www.g8live.org/wp-content/uploads/2014/09/2011g8finalcompliance.pdf.
22. .available.www.uncitral.org/uncitral/ar/uncitral_texts/electronic_commerce/2001Model_23. 1.2017.
23. UNCITRAL Model Law on Electronic Commerce (1996). 9.1.2017.http://www.uncitral.org/uncitral/en/uncitral_texts/electroni