آليات مواجهة جرائم الانترنت
بين
التصورات النظرية والتطبيقات العملية

إعداد :
د. رانيا حاكم كامل
مدرس بقسم الاجتماع بكليه البنات
جامعة عين شمس

" آليات مواجهة جرائم الانترنت
بين
التصورات النظرية والتطبيقات العملية "

الملخص باللغة العربية :

هدفت الدراسة إلى : مناقشة وتحليل آليات " مكافحة جرائم الانترنت" على ثلاث مستويات (عالمياً وعربياً ومحلياً)، وذلك من خلال القاء الضوء على تعريف جرائم الانترنت، وتاريخ ظهورها، وخطورتها على ضحاياها. **وتوصلت نتائج الدراسة إلى :** أ-عدم وجود اتفاق سواء بين الدول الأوروبية أو الدول العربية على وضع مسمى محدد للجريمة التى تحدث فى بيئة تكنولوجيا المعلومات والاتصالات،ومن ثم وضع تعريف محدد لها وما تتسم به من حيث كونها جرائم عالمية الطابع وعابرة للحدود الوطنية، ب- ثمة قصور تشريعى واضح فى الكثير من دول العالم، والتى تحول دون مكافحة جرائم الإنترنت، مما يتطلب ضرورة الاهتمام بسن تشريعات ونصوص قانونية تُجرم جميع أشكال الأفعال الاجراميه الالكترونية وما يستحدث فيها، مع تشديد العقوبات بشكل يتناسب مع نوعية كل جريمة والضرر الناتج عنها . ج- وأخيراً أشارت الدراسة أن النتائج المأساوية لانتشار جرائم الإنترنت لا تقتصر على دولة دون الأخرى فهى بمثابة وباء حقيقى يحتاج إلى تحرك عالمى.

الكلمات الافتتاحية: مكافحة جرائم الانترنت، نظرية مجتمع المعلومات ، الدول العالمية، الدول العربية، المجتمع المصرى.

" آليات مواجهة جرائم الانترنت بين التصورات النظرية والتطبيقات العملية"

أولاً : موضوع الدراسة وإشكاليته

واكبت الثورة العلمية والتكنولوجية الثالثة (ثورة الاتصالات والمعلومات) ظهور العديد من التطورات التكنولوجية والعلمية والثقافية، ولعل من أبرزها شبكة الانترنت العالمية التى أصبحت من أهم إنجازات القرن الحادى والعشرين، وفى ظل هذا التطور التكنولوجى وإعتماد قطاعات عديدة فى المجتمع على استخدام شبكة الانترنت ودخولها فى شتى مناحى الحياة، فإنتشرت جرائم الانترنت وإزدادت معدلاتها وتوغلت فى الحياة اليومية من خلال إرتكاب العديد من السلوكيات غير المشروعة وغير الإخلاقية عبر الشبكة . (رانيا حاكم، ٢٠١٦ :٢٢١)

وقد ظهر مصطلح **" الجرائم المستحدثة"** *نتيجة للتغيرات فى البنية الاجتماعية والاقتصادية للمجتمعات الحالية، فمن الناحية الاجتماعية جاء تغير منظومة الأنساق والقيم الاجتماعية وتحولها من المحلية إلى العالمية (التعولم) ليولد سلوكيات جديدة -منحرفة ومجرمة- متعارضة مع الخصوصية الحضارية والثقافية والدينية لمجتمعنا، ومن الناحية الاقتصادية فإن عولمة المال والاقتصاد والاعتماد المتزايد على التقنية والاتصالات وما نجم عن ذلك من مؤسسات وشركات متعددة الجنسيات وعابرة للحدود فقد أسهمت فى بروز جرائم اقتصادية مستحدثة .(محمد الألفى ،٢٠٠٥: ١٨)

وبهذا أحدث التحول الحضارى والتقدم الذى إجتاح العالم فى العصر الحديث تغيراً ملموساً فى نوعية الجرائم والمجرمين، فبعد ان كانت الغلبة للجرائم القائمة على العنف أو القسوة أصبحت الغلبة للجرائم القائمة على المقدرة الذهنية والذكاء. (حسين الغافرى، ٢٠٠٧: ٣٨)

كما إرتبط الانترنت **بظهور انواع مستحدثة من الجرائم المنظمة**، كجرائم التسلل المعلوماتى، وجرائم الترويج للسياحة الجنسية، وجرائم الكراهية Hate Crimes والتى تتمثل فى التمييز والنقد المباشر والمتكرر لجنس معين أو ديانة معينة أو ثقافة أو لمجتمع بعينه، وأيضاً الجرائم التى توجه إلى الاطفال وإستغلالهم من خلالها بشكل مباشر. (محمود الرشيدى،٢٠٠٥: ٢٨-٢٩)

وكذلك تسمح شبكة الانترنت بتسهيل الاتصال بين عصابات الجريمة المنظمة لضمان تدفق أموال المخدرات وغيرها من الأنشطة الإجرامية المنظمة وإنتقالها من بلد إلى آخر، كما تسهل الشبكة تهريب الأسلحة وتسويق عمليات الدعارة وتنشيط عمليات التجسس والتخاب المنى والإرهابى بل والصناعى والتجارى .(عبد الله سيف ،٢٠٠٣ :٥٠)

لذا أصبحت شبكة الانترنت تمثل هاجساً أمنياً خطيراً، فبقدر ما تقدمه للإنسان من خدمات جليلة بقدر ما تساعد المجرمين على التخطيط للجريمة والإعداد لها وتنفيذها والتخلص من آثارها (على مجاهد، ٢٠٠٩ : ٩) .

وعلى الرغم من أن هناك إجراءات أمنية لمواجهة الجريمة مثل محطات التشفير عبر الانترنت وكذلك الحوائط النارية إلا أن ذلك لا يشكل عائقاً يذكر أمام القدرات الإجرامية التى تتعامل مع الانترنت، والغريب فى هذا الشأن أن مثل هذه الجرائم لم تؤد إلى تناقص استخدام الانترنت بل ازدادت معدلات استخدامها، بما يمكن القول أنها شكلت دعاية مثيرة للإنترنت، ولعل حادثة اختراق بريد شركة مايكروسوفت Microsoft hotmail من قبل إحدى البرمجيات التى أعدها أحد الهواة فى أوروبا عام (١٩٩٨) لم تؤثر على ثقة مستخدمية، بل إزدادت الشركات التى توفر هذه الخاصية عبر الانترنت بشكل مضاعف (عمر أبو بكر، ٢٠٠٤ : ١١٢) .

* وعادة ما يشير مصطلح الجرائم المستحدثة فى التراث النظرى إما إلى إستحداث وسيلة جديدة فى إرتكاب الجرائم التقليدية، أو إلى إستحداث أفعال إجرامية لم تُجرم من قبل فى قانون العقوبات .

والجدير بالذكر أن مصطلح **جرائم الإنترنت Internet crime**، أو الجرائم السيبرانية Cyber crimes كما يطلق عليه فى التراث العالمى يشير عادة إلى الجرائم التى تتم فى بيئة الشبكات أو عبر الفضاء الإلكترونى.

وتتمثل **خطورة هذة الجرائم** فى إنها لا تقف عند حد الإضرار بالإفراد بل أنها تؤثر أيضاً على إقتصاد الدول، والشركات والمؤسسات المالية العملاقة، بل قد تصل إلى اعمال التجسس والوصول إلى معلومات سرية عن الحكومات.

(Center For Strategic And International Studies(CFSAIS) , 2013:10)

ووفقاً للتقرير الصادر عن **مركز شكاوى جرائم الانترنت IC3** *فى (٧مايو٢٠١٨)، والذى يدعمه مكتب التحقيقات الفيدرالى الأمريكى ،أنه قد تلقى حوالى (اربعة مليون) شكوى منذ إنشائة فى عام (٢٠٠٠)، وقد قُدرت الخسائر بنحو ١,٤ مليار دولار لعام (٢٠١٨/٢٠١٧).

FBI National Press)

(Office(NPO),2018:1

وأوضح التقرير الصادر عن مؤسسة HERJAVEC GROUP بعنوان (**جرائم الانترنت لعام ٢٠١٧**) أن الجريمة السيبرانية تُعد أحد أكبر التحديات التى ستواجهها البشرية فى العقدين القادمين، حيث تتوقع مشاريع الأمن السيبرانى أن الجريمة السيبرانية ستُكلف العالم أكثر من (٦تريليون دولار) سنوياً بحلول عام ٢٠٢١. (Steve Morgan , 2017:3)

وعلى ضوء ما تم عرضه تبرز مشكلة البحث فى طرح تساؤل رئيسى مؤداه : ماهية الأساليب التى تتخذها الدول سواء أكانت عالمية أم عربية أم محلية لمواجهة جرائم الإنترنت فى ظل التحديات الاجتماعية والتكنولوجية والقانونية التى تواجهها ؟

ثانياً : أهمية الدراسة وأهدافها

تستمد الدراسة أهميتها من عدة إعتبارات، يمكن إيجازها على النحو التالى :

- بإستقراء التراث البحثى فى المكتبة العربية تبين وجود اهتمام كبير بتناول هذا الموضوع وبصفة خاصة فى الدراسات القانونية نظراً لارتباطها بالتخصص الدقيق لهذا العلم، اما الدراسات الاجتماعية فقد جاء تناول هذا الموضوع فى ثنايا بعض الموضوعات وفى أجزاء متفرقة منه، مما كان دافع للباحثة لتناول هذا الموضوع الجاد من منظور سوسيولوجى فى شكل دراسة متكاملة الجوانب والأركان.
- وعلاوة على ذلك فتتبدى أهمية الدراسة أيضاً فى حجم الخسائر الباهظة الناجمة عن جريمة إلكترونية واحدة، حيث أن أضرارها تتعدى المساس بحرمة الحياة الخاصة للإفراد، إلى الاضرار بالمؤسسات والشركات المالية العملاقة، وإحداث إضرار فادحة بالبنية التحتية للدولة، وأيضاً الاعتداء على مواقع عسكرية والحصول على بيانات حساسة منها ،مما يُعد مؤشر هام على الضرر الذى قد يلحق بالمجتمع كله .
- وأخيراً تظهر أهمية الدراسة بوضوح من خلال انتشار الممارسات اللاأخلاقية على شبكة الانترنت وخاصة فى الفترة الأخيرة، كإستخدام مواقع التواصل الاجتماعى لنشر أخبار كاذبة، وإنتشار الفتن والشائعات، وإستخدام اسماء مستعارة للتضليل والخداع، ومشاركة الاخبار والفيديوهات دون التأكد من مصدرها، وهكذا تحولت تلك الاستخدامات من الشكل اللاأخلاقى إلى أفعال يعاقب عليها القانون، الأمر الذى يتوقع معه إزدياد معدل هذه الجرائم فى المستقبل القريب.

وتأسيساً على ما تقدم تهدف الدراسة إلى : مناقشة وتحليل آليات " مكافحة جرائم الانترنت" على ثلاث مستويات (عالمية وعربية ومحلية) فى ضوء نظرية مجتمع المعلومات ل " دانيال بيل "، وذلك من خلال القاء الضوء على تعريف جرائم الانترنت، وتاريخ ظهورها، وخطورتها على

* مركز شكاوى جرائم الانترنت Internet Crime Complaint Center (Ic3) : هو مكتب يعمل بجهود مشتركة بين مكتب التحقيقات الفيدرالى (FBI) ، والمركز الوطنى لذوى الياقات البيضاء ، وتتمثل مهمته الاساسية فى تزويد الجمهور بآلية الإبلاغ عن أى نشاط إجرامى يتم عبر شبكة الانترنت ، ويستقبل المركز الشكاوى عبر الموقع الاليكترونىwww.ic3.gov // :http من خلال استمارة يتم ملئها الكترونيا من كافة انحاء العالم .

ضحاياها، و التعرف على الأساليب والتدابير الأمنية التى تتخذها الدول لمواجهة هذه النوعية من الجرائم المستحدثة.

وتأسيساً على ما تقدم تم تقسيم البحث النظرى الحالى الى ست محاور أساسية، جاءت على الوجه الآتى:

المحور الأول: نظرية مجتمع المعلومات

يُعد " دانيال بيل Daniel Bell" هو أول من طرح مفهوم مجتمع ما بعد الصناعة عام (١٩٧٣) ، ثم اعاد تسميته بمجتمع المعلومات عام (١٩٧٩) ، ويفرق "بيل" بين مصطلحى المعرفة والمعلومات ، حيث يرى الأول يشير الى مجموعة من الأفكار أو الحقائق الذى يتم إرسالها إلى الأخرين من خلال بعض وسائل الاتصال ، أما المصطلح الثانى " المعلومات " فيتعلق بمعالجة البيانات بأوسع معانيها ، أى أن يصبح تخزين البيانات وأسترجاعها ومعالجتها مورداً أساسياً لجميع التبادلات الاقتصادية والاجتماعية . (Daniel Bolotsky,2018:1)

ويرى "بيل" ان مجتمع المعلومات يحتوى دائماً على ثلاثة فروع أو عناصر مميزة هى : العنصر الأول يتعلق بالقوى العاملة فى مجال المعلومات ، والعنصر الثانى يتناول تدفقات المعلومات خاصة المعرفة العلمية ، اما العنصر الثالث فيتعلق بالحواسيب وثورة المعلومات ، ويؤكد "بيل" ان أفضل فهم لرسالة مجتمع المعلومات هو توليف لهذة العناصر الثلاثة معاً . (A.S.Duff,1998: 1)

ويشرح " بيل" اقتصاد الخدمات بإنه تحول من اقتصاد يعتمد فى المقام الأول على إنتاج السلع إلى اقتصاد قائم على الخدمات ،وبالتالى تزداد قيمة المعلومات المتعلقة سواء بشكل مباشر أو غير مباشر بالأنشطة الاقتصادية وذلك لأنها ترتبط بالمنتج الوطنى والدخل القومى والقوى العاملة ، لتصبح المعلومات مورد استراتيجى فى حد ذاتها، كما ناقش "بيل" التوسع فى اقتصاد الخدمات من خلال تركيزه على العمل المكتبى والتعليم والحكومة ، وقد أدى هذا إلى ظهور مجتمع ذوى الياقات البيضاء ، مما يعنى أن " تفوق الكفاءة المهنية والتقنية" هى الأساس فى مجتمع المعلومات . (Samba,2005:3)

لذا فان المعلومات تحتل مركز الصدارة باعتبارها المورد الاستراتيجى الرئيسى الذى تعتمد عليه منظمه الاقتصاد العالمى ، حيث سهلت تكنولوجيا الحاسوب والاتصالات من معالجة المعلومات على نطاق لم يسبق له مثيل ، كما وفرت قواعد البيانات على الانترنت المعلومات عن مجموعة من الموضوعات تتراوح من معاملات سوق الأوراق المالية ، وأسعار السلع ، وقوائم براءات الاختراع ، وأسعار العملات ، إلى ملخصات المجلات العلمية والتكنولوجية ،وقد أدت هذة التطورات إلى اعادة تنظيم النظام المالى العالمى جذرياً ، مما أدى إلى انهيار الحدود التقليدية التى كانت فى الماضى تفصل بين الخدمات المصرفية والوساطة المالية والخدمات المالية ووكالات الائتمان . (Frank Webster,2018 : 6-8)

ومما سبق يتضح أن البعدين (المعرفى والتقنى) هما أساس تحديد التصنيف الفئوى لطبيعة المهن الرئيسية فى مجتمع المعلومات ، حيث يعتقد "بيل" أن استخدامات المعلوماتية تشمل فئات عديدة منهم الصفوة فى الطبقة الوسطى ثم الطبقة الغالبة وهم من المشتغلين فى تقنية المعلومات والدارسيين ، وعلى الرغم من ذلك فهناك اختلافات فارقة فى مجتمع المعلومات حيث تتاح الفرصة لبعض الافراد للقيام بأدوار وظيفية ومهنية قائمة على الاستفادة من تطبيقات تقنيات المعلومات ، فى حين لا تتاح مثل هذه الفرص لأفراد آخرين بسبب تدنى مستوى المعيشة لاعتبارات اقتصادية وثقافية . (صباح محمد ، ٢٠٠٧ : ٢٩٠)

وبالتالى يمكن القول : أن هناك علاقة طردية بين الأبعاد المعرفية والتكنولوجية فى مجتمع المعلومات، ويتضح ذلك من اتجاه المجتمعات الآن إلى التخطيط المستقبلى الدائم والقائم على البحث العلمى والوعى الفردى لمتطلبات الغد وتنمية روح التجديد والابتكار. ، لذا فأبعاد استشراف المستقبل التقنى لابد أن تضع فى الحسبان الاهتمام بالعنصر البشرى لأنه العامل الأساسى والمحرك لتطور المجتمع وتحوله إلى مجتمع المعلومات.(وائل اسماعيل عبد البارى ، ٢٠٠٢، ١-٣)

وفى ضوء ما سبق، يؤكد بيل Bell على ضرورة وجود وسائل ضبط اجتماعى للتحقق من مدى وعى الأفراد بالعمل على تطوير آليات استشراف المستقبل، وفى هذا السياق يبرز دور المؤسسات الحكومية

كأحد هذه الوسائل الاجتماعية المعنية بالتطور والتحول المجتمعى، ويذكر بيل عدة مهام تتعلق بالأبعاد المعرفية والتكنولوجية فى مجتمع المعلومات منها: تحديد الاتجاهات البناءة فى المجتمع والتى تؤثر فى عامل الاستفادة التقنية والمعرفية، تحليل بعض المشكلات التى قد تنجم عن التحول المجتمعى، وجوب استشراف المستقبل خاصة لطبقة وفئات عمال المعلومات Information Workers . (وائل اسماعيل عبد البارى ، ٢٠٠٢ ، ٣)

واستناداً لما سبق يمكن القول :

لا أحد لا يستطيع أن ينكر أن شبكة المعلومات هى سمة المجتمعات فى العصر الحديث ، وأنها استطاعت الغاء الحدود الجغرافية والفواصل الزمنية بين المجتمعات بعضها وبعض ، والتقارب بين الثقافات وسهولة الاتصالات والتدفق المعلوماتى الهائل فى جميع جوانب الحياة ، وقد ادى ذلك الى زيادة استخدامها وخاصة فى الحياة اليومية ، إلا ان تلك الاستخدامات قد تحولت لدى البعض من الشكل اللاأخلاقى إلى أفعال يعاقب عليها القانون،كجريمة السب والقذف عبر الشبكة ، والنصب والاحتيال الالكترونى ، والاستيلاء على بريد الكترونى ، والتزوير الالكترونى ، وجريمة الاختراق وانتحال صفة وغيرها .

واذا حاولنا تطبيق سمات مجتمع المعلومات كما يرى " بيل " لتفسير موضوع الدراسة يتضح أن :

أ- تفوق حاجة الأفراد إلى المعرفة عن حاجتهم إلى علاقاتهم بالمجتمع ، حيث يزداد التعامل مع كل آليات التكنولوجيا الحديثة التى سهلتها الانترنت ، فاصبحت تلك التكنولوجيا جزء لا يتجزأ من الحياة اليومية للفرد ، بحيث زاد الاعتماد على هذه الوسائل بشكل كبير الأمر الذى ترتب عليه سوء استخدامها من قبل بعض الافراد ، وإنفصالهم عن الواقع الحقيقى إلى واقع افتراضى وهمى.

ب- ونتيجه لما سبق فلم تعد استخدام شبكة الانترنت تقتصر على فئه معينة ، أو طبقة ما ، بل تتعددت استخداماتها وتعددت كذلك فئات مستخدميها ، ولعل هذا أنعكس بأثره على تغير سمات مرتكبى جرائم الانترنت عن المجرمين التقليدين ، ومما يدعم هذه النتيجه ما توصلت إليه (دراسة رانيا حاكم ٢٠١٦) من عدة نتائج ، من أهمها : تنوع مهن المتهمين فى جرائم الحاسب وشبكات المعلومات وذلك منذ عام (٢٠٠٣ – ٢٠١١) ، حيث جاء الموظفون والعمال فى شركات حكومية وخاصة فى المرتبة الأولى ، يليها أصحاب ومديروا الشركات التى يعمل أغلبها فى مجال الحاسبات فى المرتبة الثانية ، فمجرمى الانترنت ذو مهارات تقنية ومهارية عالية، يتمتعون بالذكاء والقدرة العالية فى استخدام الشبكة ، كما انهم لا يميلون إلى العنف بقدر استخدامهم لقدرتهم الذهنية والعقلية والمهارية فى ارتكاب جرائمهم . (رانيا حاكم ، ٢٠١٦: ٩٠- ٩٧)

ج – ومن الإشكاليات المطروحة فى مجتمع المعلومات تتعلق باضطراب المعايير والقيم الاجتماعية والأخلاقية عبر الشبكة وانتشار لبعض القيم السلبية والهدامة فى المجتمع، ولعل هذا يشير إلى ان التطور التكنولوجى عادة ما يحمل فى طياته عواقب اجتماعية بالغة الاهمية .

المحور الثانى : تعريف جرائم الانترنت

يرى فريق من الباحثيين صعوبة وضع تعريف محدد لجرائم الانترنت، حيث أن هناك العديد من المصطلحات التى تستخدم للإشارة إلى نفس المعنى تقريباً، ومنها : جرائم الحاسب، الجرائم ذات الصلة بالحواسيب، الجرائم ذات التكنولوجيا الفائقة. (Fausto Pocar,2004:32) والجدير بالذكر أن المراجع الأجنبية ترادف بين مصطلحى جرائم الإنترنت Internet crime، والجرائم السيبرانية Cyber crimes أى الجرائم التى تتم فى بيئة الشبكات أو عبر الفضاء الإلكترونى.

وبالرجوع للمراجع التى تناولت جرائم الإنترنت اتضح أن هناك شبه اتفاق على تعريفها، فتُعرف بأنها "أى نشاط إجرامى يتم أو يجرى عبر شبكة الإنترنت، ويتضمن سرقة الملكية الفكرية، ومصادرة الحسابات المصرفية عبر الإنترنت، وإنشاء وتوزيع الفيروسات على أجهزة الكمبيوتر الأخرى، ونشر المعلومات التجارية السرية على الشبكة، وتعطيل الهياكل أو البنية التحتية للبلد، وفقدان أو إساءة استخدام المعلومات" (Ponemon Institute(PI), 2012: 1).

أو هى "كافة الأنشطة الإجرامية التى ترتكب عبر الشبكات الإلكترونية ونظم المعلومات، بما فيها الجرائم التقليدية مثل الغش والتزوير، والجرائم الجديدة التى ظهرت بسبب الفرص الفريدة التى قدمها

الإنترنت للمجرمين مثل القرصنة الإلكترونية" (Rohini Tendulkar, 2013: 6). وهناك من عرَّفها بأنها "أى أفعال إجرامية تنطوى على استخدام شبكة الإنترنت، وتشمل الاحتيال المالى، والقرصنة، وتحميل الصور الإباحية من الإنترنت، وهجمات الفيروسات، والبريد الإلكترونى المزعج، وإنشاء مواقع المطاردة التى تعزز الكراهية العنصرية، والتجسس الإلكترونى" (John Herhalt, 2011: 31). **أو** هى "استغلال شبكة الإنترنت فى ارتكاب أفعال إجرامية، سواء كانت جرائم جديدة مثل الحرمان من الخدمة، أو فى ارتكاب جرائم تقليدية ولكنها تنفذ بأساليب حديثة، كما هو الحال فى الاحتيال المصرفى" (Peter Grabosky, 2007: 202).

وتعرف أيضاً بأنها الجرائم التى يستخدم فيها الحاسب وشبكة الإنترنت للقيام بأعمال من شأنها الإضرار بمستخدمى الشبكة أو مصالحهم أو القيام بأعمال احتيال أو مظاهر إجرامية أخرى تنافى الأغراض التى أنشئت من أجلها الشبكة وتؤدى إلى إضرار بالمجتمع أو الأفراد (أيمن الدسوقى، ٢٠٠٨: ٣١). ونظراً لأن جرائم الإنترنت كغيرها من جرائم التكنولوجيا المستحدثة التى لا تزال تتطور ويظهر بها أشكال جديدة من الجرائم باستمرار، فهناك من قام بتوسيع التعريف ليشمل أى عمل غير قانونى ينطوى على شبكة الإنترنت، أو يعرفها بأنها جميع الأنشطة غير القانونية التى تتم فى الفضاء الإلكترونى (Sylvia Kierkegaard, 2007: 19). أوكافة الأنشطة التى تستخدم أجهزة الكمبيوتر والهواتف الخلوية والمعدات وغيرها من الإجهزة التكنولوجية لإغراض غير مشروعة مثل الاحتيال والسرقة والتخريب الالكترونى منتهكة بذلك حقوق الملكية الفكرية وكسر والدخول إلى نظم الكمبيوتر والشبكات. (David L. speer,2000: p. 260)

كما تعرف كذلك بإنها: "كل نشاط إجرامى يكون لشبكة الإنترنت دوراً فى إتمامه على أن يكون هذا الدور على قدر من الأهمية، ولا يختلف الأمر سواء تم النشاط عبر الشبكة أم كانت الشبكة وسيلة لارتكابه، ففى كلتا الحالتين ينبغى أن يكون لشبكة الإنترنت دور مؤثر فى إتمام النشاط الإجرامى" (شمسان ناجى، ٢٠٠٩: ٣٦).

وأخيراً نجد من عرفها بأنها: كافة الأفعال الإجرامية التى ترتكب عبر شبكة الإنترنت، والتى تتم من خلال ضلعى الجريمة الجانى والمجنى عليه، سواء كانت جرائم مستحدثة أو تقليدية ولكنها تنفذ بأساليب حديثة، ولهذه الجرائم عدة أشكال (منها : سب وقذف وتشهير، والاعتداء على حرمة الحياة الخاصة، والتهديد والابتزاز، والنصب والاحتيال، الاتلاف، وسرقة البريد الإلكترونى، والاعتداء على حقوق الملكية الفكرية، وانتحال صفة، والاختراق، وإفشاء معلومات، وتمرير مكالمات دولية، وجريمة التزوير واستخدام محررات إلكترونية مزورة) مما يترتب عليه خطورة تهدد الحياة الخاصة للأفراد والأمن القومى للمجتمع.(رانيا حاكم ،٢٠١٦ :٢١-٢٢)

والجدير بالذكر أن هناك بعض الباحثين حاولوا ربط مصطلح جرائم الانترنت بمصطلح أخر وهو(حرب المعلومات Information Warfare)، حيث يتضمن هذا المصطلح الأنشطة المتعلقة بالحرب سواء قام بها أفراد أم منظمات أم حكومات، وعادة ما تنفذ هذة الأنشطة ضد البنية التحتية ونظم الحاسوب للمنظمات أو الحكومات الأخرى، ويتشابة هذان المصطلحان (حرب المعلومات وجرائم الانترنت) فى إنهما يشكلان خطورة سواء على مستوى الأمن الوطنى أو الدولى.

(David L. speer,2000: p. 260)

ومن العرض السابق لتعريف الباحثين لمصطلح جرائم الانترنت، يمكن أن نخرج بمجموعة من السمات لهذة الجرائم جاءت على النحو التالى:

- **تفرد جرائم الانترنت عن غيرها من الجرائم :** فعلى الرغم من أن **جرائم الحاسب الآلى** Computer crimes تتشابه مع جرائم الإنترنت إلا أنها لا يشترط فى ارتكابها أن تتم عبر شبكة الإنترنت، كما أن **الجرائم المعلوماتية** Information crime تقتصر على نوعية محددة من الجرائم، وهى تلك الجرائم التى تعتمد على المعلومة بشكل أساسى سواء تمت عن طريق الحاسب أو من خلال شبكة الإنترنت. أما بالنسبة لمصطلح **الجرائم الإلكترونية**Techno crime فهو مصطلح فضفاض، يمكن أن يدخل ضمن نطاقه جميع التقنيات والتكنولوجيا الحديثة كجرائم التليفون

المحمول والأقمار الصناعية... وغيرها. مما يجعل من جرائم الإنترنت Internet crimes جرائم فريدة فى نوعها ومختلفة عن غيرها من الجرائم.

- **تتسم جرائم الانترنت ببعض الخصائص المنفردة بها** : والتى لا تتوافر فى الجرائم التقليدية، سواء من حيث أنها تتم عبر الفضاء الإلكترونى أو من حيث أساليب ارتكابها، وخصائص مرتكبيها، أو من حيث ارتكاب بعض الجرائم التقليدية ولكن بأسلوب حديث ومختلف عن الماضى، مما أفرز ظهور نوعية جديدة من الجرائم لم تشهدها المجتمعات من قبل.
- **التطور التكنولوجى:** حيث يستغل مرتكبى هذا النوع من الجرائم استغلال هذه التكنولوجيا التى تتطور بسرعة هائلة وتوظيفها سواء فى إرتكاب الجريمة أو تضليل الشرطة فى البحث والتعقب، او فى التوصل لإكبر عدد من الضحايا، أو فى التواصل بين الخارجين عن القانون عبر المواقع الالكترونية المختلفة .
- **صعوبة مواجهة جرائم الانترنت** : فأصبح من الصعب مواجهة جرائم الانترنت بالطرق والاساليب التقليدية خاصة اذا أخذنا فى الاعتبار ان التكنولوجيا تتطور بشكل أسرع من تطور القوانين، وظهور جرائم جديدة و مستحدثة لم تكن موجودة فى قانون العقوبات من قبل، هذا فضلاً عن إعادة إرتكاب الجرائم التقليدية ولكن بأسلوب حديث ومختلف عن الماضى، مما ترتب عليه عدم إستطاعة التشريعات والقوانين لمواكبة هذة التغيرات التكنولوجية السريعة والمتلاحقة .

المحور الثالث : تاريخ جرائم الإنترنت

يؤرخ لجرائم الإنترنت عام (١٩٨٨)، فقد كانت أول الجرائم التى ترتبط عضوياً بالإنترنت هى جرائم العدوان الفيروسى فيما هو معروف فى التاريخ القانونى بجريمة دودة موريس المؤرخة فى نوفمبر ١٩٨٨. (عمر أبو بكر، ٢٠٠٤: ٦١،٦٢) فتُعد **دودة موريس** أحد أول الهجمات الكبيرة والخطيرة فى بيئة الشبكات، حيث تمكن طالب يبلغ من العمر ٢٣ عاماً ويدعى Rober Morris من إطلاق فيروس عبر الإنترنت أدى إلى إصابة (٦آلاف) جهاز يرتبط معها حوالى (٦٠٠٠٠) نظام عبر الإنترنت من ضمنها أجهزة العديد من المؤسسات والدوائر الحكومية، وقد قُدرت الخسائر لإعادة تصليح الأنظمة وتشغيل المواقع المصابة بحوالى (مائة مليون دولار) إضافة غلى مبالغ أكثر من ذلك تمثل الخسائر غير المباشرة الناجمة عن تعطل هذة الأنظمة، وقد حُكم على موريس بالسجن لمدة ثلاث أعوام وعشرة آلاف غرامة . (يوسف المصرى، ٢٠١١ : ٢٠)

ومن بين **الأحداث الشهيرة** التى حدثت فى هذا الحقل، نذكر منها :

- **قضية الجحيم العالمى:** تَعامل مكتب التحقيقات الفدرالية مع قضية أطلق عليها أسم مجموعة الجحيم العالمى Global Hell ، فقد تمكنت هذة المجموعة من أختراق مواقع البيت البيض والشركة الفيدرالية الأمريكية والجيش الأمريكى ووزارة الداخلية الإمريكية، وقد أُدين إثنين من هذه المجموعة جراء تحقيقات الجهات الداخلية فى الولايات المتحدة، وقد ظهر من التحقيقات أن هذة المجموعة تهدف إلى مجرد الإختراق أكثر من التدمير أو إلتقاط المعلومات الحساسة، وقد أمضى المحققون مئات الساعات فى ملاحقة ومتابعة هذه المجموعة عبر الشبكة وتتبع آثار أنشطتها، وقد كُلف التحقيق مبالغ طائلة كما تطلب وسائل معقدة فى المتابعة . (جعفر جاسم، ٢٠١٢: ١٢٤، ١٢٥)
- **فيروس ميلسا :** وفى حادثة هامة أخرى، أنخرطت جهات تطبيق القانون وتنفيذه فى العديد من الدول فى تحقيق واسع حول إطلاق فيروس عبر الإنترنت عرف باسم ميلسا Mellissa، حيث تم التمكن من إعتقال مبرمج حاسوب من ولاية نيوجرسى فى شهر إبريل عام ١٩٩٩، وإتهم بإختراق اتصالات عامة والتآمر لسرقة خدمات الحاسوب، ووصلت العقوبات فى الإتهامات الموجهه له إلى السجن لمدة ١٤ عاماً وغرامة قُدرت بحوالى ٥٠٠ الف دولار. (خالد الفار وآخرون ،٢٠١٠: ١٥٨)
- **حادثة المواقع الإستراتيجية :** وفى ١٩ نوفمبر عام ١٩٩٩ تم إدانة Eric burns من قبل محكمة فيرجينيا الغربية بالحبس لمدة (١٥) شهراً، والبقاء تحت المراقبة السلوكية لمدة ثلاث سنوات بعد أن أقر بذنبه، وأنه قام وبشكل متعمد بإختراق كمبيوترات محمية الحق فيها وتسبب بإضراراً بالغة،

وقد تضمن هجومة الإعتداء على مواقع لحلف الإطلسى إضافة على الأعتداء على موقع نائب رئيس الولايات المتحدة، والعديد من المواقع الحكومية، كما قام بالهجوم على مواقع لثمانين مؤسسة اعمال فى منطقة فيرجينيا والعديد من مؤسسات الأعمال فى واشنطن، إضافة إلى جامعة واشنطن والمجلس الأعلى لتعليم فى فيرجينيا، وأيضاً مزود خدمات إنترنت فى لندن، وكان عادة يستبدل صفحات المواقع بصفحات خاصة به تحت أسم Zyklon أو باسم المرأة التى يحبها Cryatal . (خالد الفار وآخرون، المرجع السابق :١٥٨،١٥٩)

ونذكر بعض الأمثلة فى هذا الصدد، ففى دراسة أجريت عام ١٩٩٦ قدرت بأن موقع المكتب العام لوزارة الدفاع بالولايات المتحدة قد أقتحم عام ١٩٩٥ إلى ما يصل إلى (٢٥٠ الف مرة)، هذا فضلاً عن أن موقع الويب التابع لوزارة العدل قد أجُتيح من قبل قراصنة إحتجاجاً على قانون " الاتصالات الحر"، وقام المتسللين بإرسال صورة جورج واشنطن مع كتابة جملة " نقل القبر إلى بلد حر" . (Susan J. Drucker,2000:138- 139)

المحور الرابع : خطورة جرائم الإنترنت

لا يزال يشكل التصدى للجرائم السيبرانية*– التى تتم عبر الشبكة – تحدياً رئيسياً للمجتمعات فى جميع أنحاء العالم، فأصبح التهديد بالجريمة السيبرانية مصدر قلق ليس فقط فى المجتمعات التى تعتمد بشكل مكثف على توافر تكنولوجيا المعلومات، وإنما أصبح مصدر قلق أيضاً للمجتمعات فى البلدان الامية، فتشير الإحصاءات إلى أنه ابتداء منذ عام (٢٠٠٥) تجاوز عدد مستخدمى الإنترنت فى البلدان النامية عدد المستخدمين فى البلدان الصناعية. (Marco Gercke, 2009 : 409-410)

وبالنسبة لإعداد جرائم الإنترنت على المستوى العالمى، فقد أظهرت دراسة شاملة أجرتها **مؤسسه "جافلين للبحوث الاستراتيجية" عام ٢٠١٨**، والتى تضمنت (٦٩ الف مستخدم) أن (٥,٦%) من الأفراد جاءوا ضحايا للاحتيال الالكترونى، وقد بلغت حجم الخسائر نحو ١٦ بليون دولار، وأن الاحتيال الالكترونى يستهدف الشركات الصغرى بنسبة بلغت (٤٣%)، ومن المتوقع أن يزيد هذا العدد فى المستقبل . (Brad Smith, 2018 : 1-2)

كما كشف التقرير الذى صدر من **معهد بونمون Ponemon Institute عام (٢٠١٢)** بعنوان" تكلفة الجريمة السيبرانية " لخمس عينات من البلاد وهم (الولايات المتحدة، ألمانيا، وأستراليا، واليابان، والمملكة المتحدة)، أرتفاع تكلفة الجريمة السيبرانية لتصل إلى اعلى معدل لها فى الولايات المتحدة بخسائر قُدرت ب (٨,٤ مليون دولار فى السنة)، بينما جاءت المملكة المتحدة فى أدنى مرتبة بخسائر قُدرت ب (٣,٣ مليون دولار فى السنة).(Ponemon Institute, 2012: 1-3)

وقد أصبح الجميع **هدفاً للهجمات السيبرانية** Target Of Cyber Attacks، حتى موظفى جوجل"Google"، فقد طُلب من بعضهم إرسال رقم البطاقة المصرفية الخاصة بهم إلى الصفحة الرئيسية لهذا النظام الشهير وذلك لإسترجاع المعلومات الخاصة بهم لأنهم قد فازوا بجائزة ما . (A.Akopyan & D.Yelyakov, 2009 :338)

كما أصبحت **مؤتمرات القمة العالمية** أهدافاً رئيسية للمتسللين، ففى كانون الأول / ديسمبر ٢٠١٠ قام قراصنة الكمبيوتر بالهجوم على ما يقرب من (١٥٠) من أجهزة الكمبيوتر لوزارة المالية الفرنسية، وأستطاعوا الوصول إلى العديد من الوثائق التى كانت تمثل معلومات حساسة تتعلق بمؤتمر قمة مجموعة العشرين الذى عقد فى فرنسا . (John Herhalt, 2011:36).

وعرضت **شركة مايكروسوفت Microsoft الشهيرة** فى عام (٢٠٠٩) مكافأة بلغت قدرها (٢٥٠ الف دولار) مقابل المعلومات التى تؤدى إلى إعتقال وإدانة المسئولين عن إطلاق (دودة الكمبيوتر كونفكيرConficker)، تلك الدودة التى أصابت ما يزيد على (١٠ مليون) من انظمة التشغيل Microsoft Windows لأجهزة الكمبيوتر على مستوى العالم . (A.Akopyan & D.Yelyakov, 2009 :410)

* عادة ما يستخدم مصطلح الجرائم السيبرانية cyber crime فى التراث النظرى العالمى للدلالة على الجرائم التى تتم فى بيئة الشبكات أو عبر الفضاء الإلكترونى.

ووفقاً للبحث الذى اجرته شركة (Panda Security) فإن ما يقُدر بحوالى (٥٧%) من جميع الحواسيب فى الصين مصابة بالبرامج الضارة، يليها تايلوان بنسبة بلغت (٤٢%)، لذا تُعد الصين اكبر دوله لديها برامج ضاره على حواسيبها على مستوى العالم . (Brad Smith, 2018: p 4)

وأعلنت شركة "مزاد الأنترنت" - وهى واحدة من أكبر مواقع التسوق عبر الشبكة فى كوريا - فى ٤ فبراير ٢٠٠٨، أنها تعرضت لهجمات على قاعدة بيانات العملاء بها، وتم سرقة معلومات سرية للعملاء منها هوية المستخدم (أى الأسم الحقيقى)، ورقم الحساب البنكى، وتاريخ المعاملات ... وغيرها من البيانات، وقد تأثر بهذا الحادث (١٠,٨) مليون عميل أى ما يقارب من ربع الشعب الكورى بإسرة . (Min Jae Lee& Jinkyu lee, 2010: p55)

ونظراً لخطورة جرائم الأنترنت فقد زاد معدل إنفاق الحكومات على الأمن المعلوماتى إلى حد كبير، ففى شباط /فبراير ٢٠١١ خصصت حكومة المملكة المتحدة ٦٣ مليون إسترلينى لدعم وحدة الجريمة الإلكترونية المركزية داخل المملكة، كما زاد "البنتاجون الإمريكى" ميزانية لعام ٢٠١٢ لحماية الشبكات العسكرية إلى (٣,٢ بيلون دولار) .(John Herhalt , 2011:46)

حيث أعلن مسئول أمريكى فى وحدة مكافحة الإرهاب والأمن السيبرانى أن الهجمات السيبرانية أصبحت تتجة إلى البنية التحتية للبلد مثل أنظمة البريد الإلكترونية العسكرية، نظم مراقبة الحركة الجوية، الأسواق المالية، والمرافق العامة . (John Herhalt , 2011:12)

ونتيجة لمخاطر جرائم الأنترنت فقد حرصت العديد من الدول على إتاحة مراكز متخصصة لمساعدة ضحايا جرائم الأنترنت عبر الشبكة، ومن أمثلتها (الهند) حيث قامت بإنشاء مركز يسمى "Centre For Cyber Victim Counselling "Helping Cyber Crime Vicitims، وهو يختص بتقديم المساعدة - المشورة والتوجية- من قبل خبراء فى التعامل مع ضحايا الجريمة السيبرانية على المستوى الوطنى، وكذلك على الصعيد الدولى، وتعرض هذه المنظمة جميع خدماتها بشكل مجانى . (Center For Cyber Victim Counselling, 2013: 1)

لذلك فقد اشار مكتب التحقيقات الفيدرالى FBI بالتعاون مع مؤسسهIC3 فى عام ٢٠١٨ إلى ضرورة زيادة الوعى العام للجمهور، وأيضاً ضرورة الابلاغ عن جرائم الانترنت، ونشر ذلك من خلال إعلان يذاع عبر الاذاعة والتليفزيون لتشجيع الجمهور على الابلاغ عن أى نشاط إجرامى يتم عبر الانترنت، حيث يؤكد التقرير أن الإبلاغ يُساعد فى المكافحة الشاملة للجريمة السيبرانية. (FBI National Press Office, Op.Cit:1)

المحور الخامس: الجهود الدولية والعربية والمحلية لمكافحة جرائم الإنترنت

أولاً: الجهود الدولية لمكافحة جرائم الإنترنت

تشهد المجتمعات الغربية جهوداً كبيرة للتصدى لجرائم الإنترنت، وما يترتب عليها من مشكلات لضحايا الإنترنت والمجتمع على السواء، وذلك من خلال إنشاء إدارات متخصصة لتعقب مجرمى الإنترنت والوصول إليهم وتقديمهم للعدالة. (Burns Ronald,2004: 477)

فعلى سبيل المثال تبذل **الولايات المتحدة الأمريكية** العديد من الجهود للحد من هذه الجرائم، من خلال إنشاء إدارة لمكافحة جرائم الإنترنت بالتعاون مع المباحث الفيدرالية (FBI) وبعض الإدارات الأخرى التابعة لوزارتى العدل والأمن الأمريكية، ومن أهم مهام هذه الإدارة : أ- تأمين أجهزة الحاسبات وشبكة المعلومات ضد هجمات القرصنة الإلكترونية، ب- نشر الوعى بخطورة هذه الهجمات وكيفية التصدى لها وخاصة لدى شباب الجامعات. (Wilson David,1995: 25)

كما قامت **وزارة العدل الأمريكية** بإنشاء فرقة للبحث فى جرائم الإنترنت التى يتعرض لها الضحايا من الأطفال؛ التابعة لشعبة حماية الطفل، وذلك فى محاولة لحماية الأطفال ومنعهم من الانحراف، والتحقيق فى جرائم الاستغلال الجنسى للأطفال الذى يتم عبر الشبكة. (Cullen Thomas, 2001, 1)

حيث تبين أن للإنترنت دوراً قوياً فى رواج وانتشار عمليات الاستغلال الجنسى للأطفال أو ما يطلق عليه مفهوم دعارة الأطفال child prostitution، حيث ساهمت هذه التقنية فى تطور هذه الجريمة وشيوعها. بل والطلب عليها من خلال شبكة الإنترنت. (Cooper Sharon, 2005: 528)

ويتأكد ذلك من خلال تبنى البروتوكول الاختيارى لاتفاقية الأمم المتحدة لحقوق الطفل المرتبط ببيع الأطفال، ودعارة الأطفال، والمواد الإباحية الأثمة للأطفال.(سهير العطار،٢٠٠٤: ٢١)

كما قامت **بريطانيا** بإنشاء وحدة تسمى "الوحدة الوطنية البريطانية لجريمة التكنولوجيا الفائقة The British National Hi-tech crime unit" التى تُعنى بالجرائم التى تحدث فى البيئة التكنولوجية الجديدة، وتهدف إلى تحديد أشكال الاجرام ذات التكنولوجيا الفائقة، وتعزيز التعاون الدولى بغية وضع معايير دولية مشتركة لمكافحة هذا النوع من الاجرام. (Fausto Pocar,2004:33-35)

وأشارت تقارير **"الوحدة الوطنية البريطانية** لجرائم التكنولوجيا الفائقة" أن الجرائم السيبرانية تكلف الشركات البريطانية حوالى (٢.٤ بيليون جنيه استرلينى) أى ما يعادل (٤.٥ بيليون دولار) وذلك فى عام (٢٠٠٤)، نتيجة الخسائر التى تكبدتها هذه الشركات من جراء جرائم الإنترنت. (Sylvia Kierkegaard, 2007: 17-18)

وفى **"الهند"**، فإن المكتب المركزى للتحقيقات (CBI) قدم قانون "تكنولوجيا المعلومات" للمساعدة فى التحقق من الجرائم الحاسوبية وتقنين المعاملات الإلكترونية فى فبراير ١٩٩٩، حيث أدرك المسئولون الهنود أنه لابد من تعديل القوانين الهندية لتكون قادرة على تقنين استخدام الكمبيوتر، ومكافحة الجرائم الإلكترونية فى المستقبل. (David L. speer,2000: p. 267)

أما **الحكومة الصينية** فقد فرضت رقابة مشددة على صناعة الاتصالات السلكية واللاسلكية، وقد حاولت الحفاظ على استخدام العامة لشبكة الانترنت لمحاربة تزايد جرائم الانترنت (liang Bin,2010:103-120).

وفى يناير ٢٠١١ أطلقت **إيران** رسمياً وحدة الشرطة السيبرانية لتكثيف حربها ضد الجريمة السيبرانية، وبخاصة تلك المواقع التى تشارك فى التجسس والتحريض على الشغب، أما **الحكومة الهندية** فقد أعلنت أيضاً فى نفس العام أنها تخطط لإنشاء معهد مخصص لتدريب المهنيين للتصدى للجريمة السيبرانية، وسيكون المعهد مبادرة شراكة بين القطاعين العام والخاص بتكلفة قُدرت ما يعادل (٢١ مليون دولار). (John Herhalt , 2011:39)

وعلى العكس من ذلك فنجد أن **"روسيا"** لديها بيئة صديقة للقرصنة، حيث تباهى جنرال بالشرطة الروسية إلى أن القراصنة الروس هم الأفضل فى العالم، وقال "كتابنا حول البرمجيات هو الأفضل على مستوى العالم، وأما عن السبب فلأننا لدينا قراصنة هم الأفضل فى العالم". Sylvia (Kierkegaard, 2007: 20)

هذا فضلاً عن وجود عدد من المحاولات – فى السنوات الأخيرة – **لإنشاء هيئات للشرطة** تكون قادرة على التصدى لمختلف الجرائم المرتكبة فى الفضاء الإلكترونى cyber space، فالشرطة تواجه صعوبات عديدة على الشبكة من حيث السرية التى يوفرها العالم الافتراضى، ونطاقه الغير محدود، هذا فضلاً عن الصعوبات فى مجال التعاون عبر الحدود الجغرافية، وجهات تنفيذ القانون، والنظم القانونية، وغيرها من الصعوبات الخاصة بعدم كفاية الموارد، كل هذه العوامل تشكل عقبات أمام الشركة للتصدى لجرائم الإنترنت. (Yar Majid, 2010: 546)

وتشير دراسة Nhan Johnny **"الشرطة فى الفضاء الإلكترونى عام ٢٠٠٩"** إلى وجود قصور شديد فى آليات الرقابة على المحتوى الموجود عبر الشبكة، بالإضافة لوجود العديد من الممارسات والتصرفات غير الأخلاقية التى تتم عبر الإنترنت، والتى تُشكل فى ذات الوقت جرائم يُعاقب عليها القانون. (Nhan Johnny, 2009: 2887)

ونظراً للصعوبات التى تتعرض لها الشرطة الخاصة بجرائم الإنترنت، فقد ظهرت طائفة كبيرة من منظمات القطاع الخاص والمجتمعات المحلية والأفراد والشركات لتتولى جزءاً كبيراً من المسئولية فى حفظ الأمن عبر الإنترنت. (Yar Majid, 2010: 550) لذا قامت بعض الشركات والمنظمات بإتخاذ تدابير أمنية لحماية أمنها الداخلى وقامت بتنفيذ هذه التدابير بالفعل، فعلى سبيل المثال شركة Sun Micro systems، قد عملت على عدم وجود أجهزة مودم وذلك لمنع المتسللين والمتطفلين من اقتحام شبكة الشركة، كما قامت بعض الشركات بإتخاذ إجراءات أكثر صرامة ضد المتطفلين بما فى ذلك

الشركات الكبرى والمؤسسات العملاقة والبنتاجون وذلك بتثبيت برامج كمبيوتر مضادة، وهذه البرامج سوف تهاجم قراصنة الكمبيوتر أو أى متسلل يحاول إحداث اختراق أمنى بنظامها.

(David L. Speer, 2000: 261)

وقد أخذت الحكومية الفيدرالية فى الولايات المتحدة هذه المسألة التنظيمية على محمل الجد، وقامت بتعيين رئيس للجنة (حماية البنية التحتية الحيوية)، كما أنشأ مكتب التحقيقات الفيدرالية فرقة عمل للنظر فى سبل حماية الشبكات، وقد تم اكتشاف التشفير Encryption كوسيلة لمكافحة القرصنة الإلكترونية. (Susan J. Drucker,2000: 139)

والجدير بالذكر تعمل عدد من **المنظمات الدولية** باستمرار لمواكبة التطورات فى شأن أمن الفضاء الإلكترونى، وقد أسست مجموعات عمل لوضع استراتيجيات لمكافحة جرائم الإنترنت، ويستخدم مصطلح "الأمن السيبرانى" لتلخيص أنشطة مختلفة كجمع المعلومات ووضع السياسات العامة والتدابير الأمنية، والمبادئ التوجيهية، وطرق إدارة المخاطر، والحماية، والتدريب، ودليل لأفضل الممارسات المهنية، ومختلف التقنيات التى يمكن استخدامها لحماية شبكة الإنترنت، ويهدف الأمن السيبرانى جاهداً لضمان تحقيق سلامة المؤسسات والأفراد فى مواجهة المخاطر الأمنية وكل ما يتعلق بشبكة الإنترنت. (جورج لبكى ،٢٠١٣ : ٤)

ومن أبرز المنظمات الدولية التى عملت فى موضوع جرائم شبكة الإنترنت هى : (مجلس أوروبا، الاتحاد الأوروبى ،الأمم المتحدة ومنظماتها ،مجموعة الدول الثمانى ،المنظمة الدولية للشرطة الجنائية "الانتربول")، وفيما يلى تناول تلك المنظمات على الوجه التالى :

(١)مجلس أوروبا * :

اعتمد المجلس الأوروبى الطابع الدولى لجرائم الكمبيوتر منذ عام ١٩٧٦، وفى عام ١٩٩٦ قررت اللجنة الأوروبية المعنية بمشاكل الجريمة (CDPC) إلى تشكيل لجنة من الخبراء للتعامل مع جرائم الإنترنت، وقد عملت اللجنة بين عامى ١٩٩٧، ٢٠٠٠ لصياغة اتفاقية تسعى لمكافحة جرائم الإنترنت، وعقدت اللجنة عشرة اجتماعات فى جلسات عامة وخمس عشرة اجتماعاً مفتوحاً لها، وفى عام (٢٠٠١) اعتمدت الجمعية مشروع اتفاقية جرائم الإنترنت خلال الجزء الثانى من الجلسة العامة لها. (Marco Gercke, 2009: 412)

وفى هذا الصدد لابد أن نشير إلى أن **اتفاقية جرائم الإنترنت** هى المعاهدة الدولية الأولى التى تسعى لمعالجة الجرائم المتعلقة بالكمبيوتر والإنترنت عبر التنسيق بين القوانين الوطنية وقوانين الدول الأخرى. (Sylvia Kierkegaard, 2007: 22)

وقد افتتح باب التوقيع على الاتفاقية خلال حفل التوقيع فى بودابست فى ٢٣ تشرين الثانى/ نوفمبر عام ٢٠٠١، حيث وقعت (٣٠) دولة على الاتفاقية، وبحلول عام ٢٠٠٩ كانت (٤٦) دولة قد وقعت على الاتفاقية، كما صدقت (٢٥) دولة أخرى على اتفاقية جرائم الإنترنت ومن بين هذه الدول (الأرجنتين، وباكستان، الفلبين، مصر، نيجيريا)، وعلى الرغم من أن تلك البلدان لم توقع بعد – حتى عام ٢٠٠٩ – على هذه الاتفاقية إلا أنها دعمت عملية التنسيق بين الدول، بوصف هذه الاتفاقية أداة دولية هامة فى مكافحة جرائم الإنترنت، ومعتمدة من قبل المنظمات الدولية المختلفة. Marco (Gercke, 2009: 413)

وتهدف هذه الاتفاقية إلى : "وضع سياسة جنائية مشتركة تهدف إلى حماية المجتمع من الجريمة السيبرانية من خلال اعتماد التشريعات المناسبة وتعزيز التعاون الدولى".ومن أهم البنود التى تناولتها اتفاقية جرائم الإنترنت هى : الجرائم المتصلة بانتهاكات حقوق التأليف والنشر، وجرائم الاحتيال والتزوير الإلكترونى، واستغلال الأطفال فى المواد الإباحية، والجرائم المتصلة بأمن الشبكات. Sylvia (Kierkegaard, 2007: 23-24)

* مجلس أوروبا هو منظمة متعددة الجنسيات، تأسست فى عام ١٩٤٩، ويتألف من ٤٦ بلداً، بما فى ذلك ٢١ بلداً من أوروبا الوسطى والشرقية، وأنشأ هذا المجلس أساساً كمنتدى دعم وتعزيز حقوق الإنسان وتعزيز الديمقراطية وسيادة القانون فى أوروبا، ويختلف مجلس أوروبا عن الأتحاد الأوروبى المكون من ٢٥ دولة، ومع ذلك تنتمى جميع الدول الأعضاء فى الأتحاد الأوروبى إلى مجلس أوروبا.

وتوفر اتفاقية جرائم الإنترنت (مجلس أوروبا ٢٠٠١) الإطار الأساسى للقوانين الموضوعية والإجرائية المحلية الرامية إلى مكافحة جميع أنواع الجرائم ذات الصلة بالحاسوب، والوسائل التى يمكن للدول أن تتعاون مع بعضها البعض أثناء سير التحقيقات العابرة للحدود الوطنية، أما بروتوكولها الإضافى (مجلس أوروبا ٢٠٠٣) فهو مخصص لمكافحة الأفعال ذات الطبيعة العنصرية مثل خطابات الكراهية، ونشر الدعاية العنصرية، وكره الأجانب من خلال شبكات الإنترنت، الذى يعد وفقاً لهذه الاتفاقية عملاً إجرامياً. (Fausto Pocar, 2004: 30)

(٢) الاتحاد الأوروبى :

عقد كل من الاتحاد الأوروبى ومجموعة الدول الثمانى *G8 عدداً من المؤتمرات حول جرائم الإنترنت بإعتبارها من الجرائم الدولية العابرة للحدود التى لابد من التركيز عليها، ومن أمثلة هذه المؤتمرات :

المؤتمر الذى عقده الاتحاد الأوروبى عام ١٩٩٥ بعنوان : "إعداد معايير للتعامل مع تهديدات الجرائم السيبرانية"، والذى كان له تأثير واضح على قمم عامى ١٩٩٧ (مؤتمر القمة عام ١٩٩٧ الذى عقد فى دنفر، كولورادو)، و١٩٩٨ (والذى أطلق عليه قمة مجموعة الثمانى، برمنغهام، ١٩٩٨) وفى كل من هذه القمم كانت الولايات المتحدة البلد الأكثر احتجاجاً لنظام حظر "الجريمة السيبرانية"، وقد ولدت هذه القمم قائمة تحتوى على عشر خطوات يتعين تنفيذها من قبل المشاركين، بما فى ذلك تعديل الأنظمة المحلية القائمة، والعمل من أجل تحقيق معايير للتعاون الدولى. (David L. speer, 2000: 263)

ونتيجة لهذه المؤتمرات، وضعت الولايات المتحدة تصنيفاً – مختلفاً – لجرائم الحاسب وشبكة الإنترنت، وهذا التصنيف يقوم على أربعة فئات هما :

الفئة الأولى (الكمبيوتر كهدف Computer as target) : ويقصد بها أن تكون أجهزة الحاسب هدفاً للجريمة مثل التخريب، والتعدى على ممتلكات الغير، وسرقة المعلومات.

الفئة الثانية (الكمبيوتر كأداة للجريمة Computer as the instrumentality of the crime) : وفيها يقوم الجانى بتعديل بعض عمليات النظام الموجودة بالفعل على الحاسب الآلى، أى يقوم باستخدام جهاز مشروع – الحاسب الآلى – ويغير أولويته لاستخدام شئ غير مشروع، وهذا النوع من الجرائم يتكون معظمه من الاحتيال، وسرقة المعلومات وخاصة أرقام بطاقات الائتمان.

الفئة الثالثة (استخدام الكمبيوتر – بشكل عارض – لارتكاب عدد من الجرائم Computer is incidental to other crime) : وفى هذه الحالة فإن جهاز الكمبيوتر ليس ضرورياً لارتكاب الجريمة، ولكنه يسهل عملية الارتكاب، كما هو الحال فى جريمة غسل الأموال، وانتشار المواد الإباحية عن الأطفال عبر شبكة الإنترنت.

الفئة الرابعة (الجرائم المرتبطة مع انتشار الحواسيب Crimes Associated with the prevalence of computers) : وهى الجرائم التى تتصل بجهاز الكمبيوتر والمعدات الطرفية له، وتشمل هذه الفئة قرصنة البرامج، وانتهاكات حقوق التأليف والنشر، وتزوير البرمجيات. David L. (speer, Ibid:263- 264)

وأصدرت **المفوضية الأوروبية** فى عام ١٩٩٦ الورقة الخضراء التى أكدت على ضرورة تبنى سياسة التنظيم الذاتى للمحتوى الضار المتاح على شبكة الإنترنت، وذلك من خلال التعاون بين دول الاتحاد الأوروبى والتعاون على المستوى الدولى فى مجالى استخدام برامج الترشيح وتقدير الأنظمة، وقد قررت المفوضية الأوروبية أن مزود الخدمة ليس ناشراً وليس مسئولاً عنها لأنه ليست لديه السيطرة على المحتوى الضار وأيدت ذلك قرارات اللجنة الاقتصادية والاجتماعية للبرلمان الأوروبى ١٩٩٦ ومجلس الاتحاد الأوروبى فى ٢٨ مايو ١٩٩٨. (محمد سعد، ٢٠٠٨: ٢٤٦)

كما نشر **الاتحاد الأوروبى** فى ديسمبر ١٩٩٨ مشروع قرار أعده المجلس الوزارى للعرض على البرلمان الأوروبى خاص بالجوانب القانونية المرتبطة بالتجارة الإلكترونية، وسبق للأتحاد فى عام

* سوف تخصص الباحثة لمجموعة الدول الثمانى عنصراً مستقلاً بها، أنظر صـ١٥

١٩٩٧ أن تبنى قرار يتناول حقوق الطبع والقوانين المرتبطة فى عصر المعلومات. (شمسان ناجى،٢٠٠٩: ٦١)

والجدير بالذكر أن **الاتفاقيات الدولية*** أو المعاهدات تُعد من أفضل الوسائل لمكافحة جرائم الإنترنت – دولياً -، حيث أنها تسمح بمستويات عالية من التعاون بين البلدان وأجهزتها المعنية بإنفاذ القانون، كما أنها تساعد فى القضاء على العديد من الصعوبات، ولعل من أهمها مسألة الاختصاص بين البلدان. (David L. Speer, 2004: 269) وقد بدأ "الاتفاق متعدد الأطراف" فى التبلور فى الاتحاد الأوروبى مع توجيه خصوصية البيانات، ويهدف هذا التوجيه إلى إقامة "إطار تنظيمى مشترك لنقل البيانات لضمان مستوى عالى من الخصوصية وحرية حركة البيانات"، وبحلول تشرين الأول/ أكتوبر عام ١٩٩٨ كانت جميع الدول الأعضاء الخمسة عشر تنفذ هذا التوجيه، إلا أن بعض الدول لم تلتزم بتنفيذ هذا التوجيه، ونتيجة لذلك اتخذت "المفوضية الأوروبية" هذه الدول إلى "محكمة العدل الأوروبية" لحل هذه المسألة، وهكذا فإن عدم التنفيذ من قبل بعض الدول الأكثر نفوذاً فى الاتحاد الأوروبى يمثل بعض الصعوبات فى تأسيس الاتفاقيات متعددة الأطراف التى تتعامل مع الجرائم السيبرانية. (David L. Speer, Ibid: 269-270)

(٣) الأمم المتحدة *:

تلعب الأمم المتحدة دوراً هاماً فى مكافحة الجرائم السيبرانية منذ فترة طويلة، وتعمل هذه المنظمة من خلال هيئة لصنع سياستها، مع عدد من الوكالات التابعة لها مثل لجنة منع الجريمة والعدالة الجنائية (فى إطار قرار المجلس الاقتصادى والاجتماعى)، ومكتب مراقبة المخدرات ومنع الجريمة. (Fausto Pocar, 2004:29) ويولى مكتب الأمم المتحدة للمخدرات والجريمة موضوع التقنيات الحديثة ويشجع الدول على سن القوانين والتعاون فى مجال مكافحة تجارة المخدرات عبر وسائل الاتصال الحديثة، حيث أثبتت التقارير الدولية استخدام تجار المخدرات لشبكة الإنترنت فى الاتصال، والتنسيق، وعرض ما لديهم عبر البريد الإلكترونى، وغرف الحوارات، والهواتف المتنقلة. (فايز الشهرى،٢٠٠٥: ١٦٣)

وظهر اهتمام الأمم المتحدة بضرورة مكافحة الجرائم السيبرانية منذ دعوتها للتصدى لجرائم الفضاء الحاسوبى، ففى عام (١٩٩٠) أصدر مؤتمر الأمم المتحدة الثامن لمنع الجريمة ومعاملة المجرمين قراراً يدعو دول الأعضاء إلى تكثيف الجهود الرامية لمكافحة الجريمة السيبرانية ولا سيما من خلال تحدث قوانينها الوطنية، وفى عام (١٩٩٤) نشرت الأمم المتحدة دليلاً لمنع ومكافحة الجريمة المتعلقة بالكمبيوتر. (Peter Grabosky, 2007: 217)

كما عقدت العديد من **المؤتمرات والندوات** على المستوى الدولى، من بينها :

مؤتمر الأمم المتحدة الثانى عشر لمنع الجريمة والعدالة الجنائية، والذى تستضيفه حكومة البرازيل فى سلفادور فى الفترة من ١٢ إلى ١٩ أبريل ٢٠١٠، تحت عنوان : "استراتيجيات شاملة لتحديات عالمية – نظم منع الجريمة وتطورها فى عالم متغير". ويتضمن المؤتمر العمل فى ثلاث محاور رئيسية هما : (إنشاء نظام للعدالة الجنائية كركيزة أساسية فى هيكلة سيادة القانون، وتسليط الضوء على الدور المحورى لنظام العدالة الجنائية فى مجال التنمية، وأخيراً تحديد الأنماط الجديدة من الجريمة والتى تشكل خطراً على المجتمعات فى جميع أنحاء العالم، واكتشاف السبل للوقاية منها والسيطرة عليها). وبالنسبة لجدول الأعمال فقد تناول ثمانية بنود هما : (الأطفال والشباب والجريمة –

---

* الاتفاقيات الدولية : هى الوسيلة التى تمكن الدول من خلق القانون الدولى، وهى اتفاقيات ملزمة قانوناً، يحكمها القانون الدولى، تكون مبرمة بين الدول بالأهلية القانونية للدخول فى الاتفاقية أو المعاهدة، وبالتالى فهى تُنشئ مجموعة من الحقوق والواجبات التى هى قابلة للتنفيذ بموجب القانون الدولى. وطبقاً لإتفاقية فيينا لقانون المعاهدات فإن الاتفاقيات أو المعاهدات تعرف بأنها "اتفاق دولى معقد بين الدول بصورة خطية وخاضع للقانون الدولى، سواء تضمنته وثيقة واحدة أو فى اثنين أو أكثر من الصحكوك ذات الصلة وأياً كانت تسميته، فتفرض الاتفاقيات التزامات قانونية محددة على الدول الأطراف، وأن عدم الالتزام ببنود الاتفاقية تفرض المسئولية على هذه الدول، فيقال أن الدولة قد انتهكت القانون الدولى عندما تتصرف خلافاً للمعاهدة. ولمزيد من التفاصيل حول هذا الموضوع راجع : Sylvia kierkegaard, Op. Cit., p. 20, p. 21.

* تعقد الأمم المتحدة مؤتمرات لمنع الجريمة كل خمس سنوات فى أنحاء مختلفة من العالم منذ سنة ١٩٥٥، وتبحث مجموعة واسعة من القضايا، وقد كان لهذه المؤتمرات أثر كبير على السياسات الوطنية والممارسات المهنية فى مجال منع الجريمة الدولية والعدالة الجنائية.

الإرهاب – الوقاية من الجريمة – تهريب المهاجرين والاتجار بالأشخاص – غسل الأموال – جرائم الإنترنت أو الشبكة العنكبوتية – التعاون الدولى فى مكافحة الجريمة – والعنف ضد المهاجرين وأسرهم. (مؤتمر الأمم المتحدة الثانى عشر لمنع الجريمة والعدالة الجنائية، ٢٠١٣ : ١- ٢)

مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاملة المجرمين، والذى عقد بالعاصمة النمساوية (فيينا) خلال الفترة من ١٠-١٧ أبريل سنة ٢٠٠٠، وأفرد هذا المؤتمر على جدول أعماله دراسة الجرائم المتصلة بالحواسيب وبشبكة الإنترنت، وأشير خلال المناقشات إلى جرائم الحاسب الآلى والإنترنت باعتبارها جرائم عبر وطنية تمثل أحد تحديات القرن الحادى والعشرين، وتضيف عبئاً وهماً جديدين للبشرية لسهولة ارتكاب الجريمة عبر هذه الشبكة وسهولة إخفائها وسهولة تحريف الأدلة الخاصة بها. (أحمد وهدان ،٢٠٠٤: ١١٢)

وأما عن أبرز قرارات الجمعية العامة للأمم المتحدة فى مجال تأمين سلامة استخدام التكنولوجيا وشبكات المعلومات (الإنترنت) يتمثل فى :

قرار الجمعية العامة للأمم المتحدة بخصوص **"خلق ثقافة عالمية للأمن السيبرانى"** والذى ينص على : أنه يجب أن تطبق الإجراءات الأمنية بطريقة لا تتناقض مع القيم المعترف بها من قبل المجتمعات الديمقراطية، ومن ضمن هذه القيم حق تبادل الأفكار والمعلومات والتدفق للحر للمعلومات، وضمان خصوصية وسرية المعلومات والإتصالات والحماية المناسبة للمعلومات الشخصية، والانفتاح والشفافية، وتم ذلك القرار فى ٢٠ ديسمبر عام ٢٠٠٢. (Yar, Majid, 2010: 548)

(٤) مجموعة الدول الثمانى G8*:

عقدت مجموعة الدول الثمانى فى واشنطن فى الفترة من ١٠-١٢ ديسمبر ١٩٩٧ مؤتمر بعنوان "مجموعة الدول الثمانى لمكافحة الجريمة المعلوماتية"، وقد شارك فيه وزراء العدل والداخلية فى البلدان التى مثلتها مجموعة الدول الثمانى. (محمد عبد الخالق ،١٩٩٨: ٦٢)

وتبنت الدول الثمانى خطة عمل من عشر نقاط تتعلق بمواجهة الجريمة على شبكة الإنترنت (الجرائم المعلوماتية) والوسائل التكنولوجية المتطورة الأخرى، وتعهدت الدول الثمانى بسن قوانين تتيح اعتبار الاستخدام الإجرامى لشبكات الكمبيوتر مخالفة وحفظ أدلة تلك الجرائم وجمعها، كما قررت هذه الدول الاستعانة بعدد كاف من الأشخاص المدربين والمجهزين لكشف هذه الجرائم وملاحقتها، كما شددت هذه الدول على ضرورة الإسراع فى وضع القوانين المناسبة لمواجهة أشكال الاتصال الجديد وعلى ضرورة التعاون أمنياً وقضائياً فى هذا المجال لقناعة تلك الدول لاستحالة أن تعمل كل دولة بمفردها لمواجهة المشكلة الجديدة المتمثلة بالجريمة المرتبطة بالتكنولوجيا المتطورة. (محمد عبد الخالق ،المرجع السابق: ٦٣)

(٥) المنظمة الدولية للشرطة الجنائية (الإنتربول):

أدرك الانتربول خطورة الجرائم السيبرانية منذ منتصف العقد الأخير من القرن الماضى، واستضاف فى عام (١٩٩٥) المؤتمر الدولى الأول بشأن الجرائم الحاسوبية، وأنشأ المؤتمر وحدة مركزية داخل الانتربول وأربعة أفرقة عاملة معنية بالجرائم المتصلة بالتكنولوجيا، وهذه الأفرقة مثلتها أفريقيا، الامريكتين، آسيا، وأوروبا، واختصت هذه الأفرقة بإتاحة التدريب والتعاون على المستوى الإقليمى لدول كل قارة. (محمد عيد، ٢٠٠٣: ١٩٩) ومن أجل ذلك أصدر كتيباً إرشادياً للمحققين الجدد فى الجرائم السيبرانية ودليلاً أكثر تفصيلاً يعرض للصعوبات التى يمكن أن تواجه أجهزة إنفاذ القانون ويبين أفضل الممارسات والتقنيات التى يجب على المحققين القيام بها لتخطى هذه الصعوبات. (محمد عيد، المرجع السابق: ٢٠٠)

ثانياً: الجهود العربية لمكافحة جرائم الإنترنت

أما فيما يخص بالعالم العربي فقد حرصت جامعة الدول العربية على عقد الاتفاقية العربية لمكافحة جرائم تقنية المعلومات الموقعة بالقاهرة فى ٢١ديسمبر ٢٠١٠، وذلك إقتناعاً منها بضرورة الحاجة إلى تبنى سياسة جنائية مشتركة تهدف الى حماية المجتمع العربى ضد جرائم تقنية المعلومات، وكان الهدف

* تضم هذه المجموعة كبريات الدول المتقدمة صناعياً ممثلة فى الولايات المتحدة الأمريكية وكندا وألمانيا واليابان وإيطاليا وفرنسا وبريطانيا بالإضافة إلى روسيا.

الرئيسى من تلك الاتفاقية هو : تعزيز التعاون وتدعيمه بين الدول العربية فى مجال مكافحة جرائم تقنية المعلومات، لدرء أخطار هذه الجرائم حفاظاً على أمن الدول العربية ومصالحها وسلامة مجتمعاتها وأفرادها .(جامعة الدول العربية، ٢٠١٨ :١)

وقد تضمنت هذة الاتفاقية تجريم أربعة عشر نوعاً من جرائم تقنية المعلومات وهم : (جريمة الدخول غير المشروع، جريمة الاعتراض غير المشروع، الاعتداء على سلامة البيانات، جريمة إساءة استخدام وسائل تقنية المعلومات، جريمة التزوير، جريمة الاحتيال، جريمة الاباحية، الجرائم الأخرى المرتبطة بالإباحية، جريمة الاعتداء على حرمة الحياة الخاصة، الجرائم المتعلقة بالإرهاب والمرتكبة بواسطة تقنية المعلومات، الجرائم المتعلقة بالجرائم المنظمة والمرتكبة بواسطة تقنية المعلومات، الجرائم المتعلقة بانتهاك حق المؤلف والحقوق المجاورة، الاستخدام غير المشروع لأدوات الدفع الالكترونية، وأخيراً الشروع والاشتراك فى ارتكاب الجرائم). (جامعة الدول العربية، المرجع السابق :٢-٤)

كما تبنت إدارة البحث الجنائى **بالمملكة الأردنية الهاشمية** مواجهة ما يسمى بالجرائم المستحدثة cyber crimes من خلال إنشاء قسم الإسناد والتحقيق الفنى فى بداية عام (٢٠٠٨) فى شعبة المتابعة والتحقيق الخاصة، ويُعنى هذا القسم بالتحقيق فى الجرائم الواقعة من خلال شبكة الإنترنت(كجرائم الاحتيال الإلكترونى، وجرائم الاحتيال المالى والمقامرة الإلكترونية، وجرائم الدفع الإلكترونى وتشمل العملة الرقمية وخدمات الدفع الإلكترونى ومحتويات البطاقات الرقمية، ومراقبة تكنولوجيا المعلومات للمنظمات الإجرامية وتطورها، وغيرها). (الصفحة الرسمية لمديرية الأمن العام بالإردن، ٢٠١٣: ١-٢)

وأهتمت **دولة الجزائر** بإصدار بعض التشريعات القانونية للحماية من جرائم الإنترنت، كتشريع القانون الجزائرى لسنة ٢٠٠٩ المتعلق بجرائم الإنترنت، والذى ينص على رصد الاتصالات الإلكترونية لضبط أية تهديدات ضد السلامة العامة، أو الدفاع الوطنى، أو مؤسسات الدولية، أو الاقتصاد الوطنى، كما يشمل هذا القانون بمواده التسعة عشر أحكاماً متعلقة بمحاربة التزوير الرقمى، وإنشاء هيئة لمكافحة جرائم الإنترنت، وحماية التحقيقات القضائية، وتبادل المعلومات على الصعيد الدولى. (بسمة الشريفى ،٢٠٠٣: ١-٣)

اما **المملكة العربية السعودية** فقد صدرت العديد من الأنظمة واللوائح المنظمة للتعامل مع إساءة استخدام الحاسبات والشبكة العالمية وتطبيقاتها المختلفة ، منها لائحة " قواعد ترخيص مقدمى خدمة الإنترنت" عام ١٩٩٩ ، ثم تلتها لائحة تختص بجرائم " الاختراقات وجزاءاتها التفصيلية "عام٢٠٠٠، كذلك صدرت فى العام نفسه اللائحة التنظيمية لاستخدام الإنترنت فى الأماكن العامة. (فايز عبد الله الشهرى، مرجع سابق : ١٧٠)

وقد أظهرت دراسة حديثة أجريت فى المجتمع السعودى عام ٢٠١٨، أن أكثر صور الجرائم الإلكترونية شيوعاً لدى أفراد الدراسة هى الصور المادية ، كما جاءت الدوافع الجنسية بالمرتبة الأولى يليها الدوافع المادية، وأخيراً بينت نتائج الدراسة أن هناك فروقاً دالة إحصائياً فى درجة تقدير الآثار النفسية لجرائم الابتزاز الإلكترونى تعزى لاختلاف فئة المستجيب (المعلمين والمعلمات، والمستشاريين النفسيين). (سليمان بن عبد الرزاق وآخرون، ٢٠١٨: ١٥٩-١٦٠)

وفى ضوء اهتمام الدول العربية بإصدار تشريع لمكافحة الجرائم الإلكترونية، فقد أعلنت وزارة الداخلية **الكويتية** بيان عبر برنامج بتليفزيون الكويت – القناة الأولى – يوم الجمعة الموافق ٢٠٠٩/٢/١ بأنها قد انشأت شرطة مختصة لمكافحة جرائم الإنترنت ودعت كل من أصابه ضرر ناتج عن عمليات السطو الإلكترونى والاختراقات الأمنية والسرقات وإفشاء المعلومات السرية ونشر الصور وانتهاك حقوق الملكية الفكرية .. إلى سرعة الإبلاغ أو أن يتصل فوراً بأحد أرقامها، كما طلبت من مستخدمى الإنترنت أن يحافظوا على معلوماتهم الشخصية والسرية وأن يبتعدوا عن المواقع والمنتديات المشبوهة وأن يحذروا من تحديث أى بيانات بنكية عبر الإنترنت حتى لا يقعوا فى فخ النسخ المزور لها. (وكالة الأنباء الكويتية كونا، ٢٠١٣: ٢)

وفى ظل الاهتمام العالمى بظاهرة استغلال الأطفال جنسياً عبر شبكة الإنترنت، فشارك الانتربول الكويتى فى الحملات التى يشنها الانتربول الدولى على المواقع الإباحية فى العديد من دول العالم فى

أوروبا وأمريكا الشمالية، ومن بينها حملة "تورنادو" التى انطلقت من مدينة فيسبادن الألمانية ضد استغلال الأطفال وممارسة الجنس معهم ومع القصر، وهى الظاهرة المعروفة عالمياً بإسم Child abuse.(الصفحة الرسمية لوزارة الداخلية بدولة الكويت، ٢٠١٣: ١)

كما قامت دولة **الإمارات العربية المتحدة** بعدة خطوات لمكافحة جرائم الإنترنت، منها ما أصدره الشيخ خليفة بن زياد آل نهيان رئيس دولة الإمارات مرسوماً بقانون إتحادى رقم ٥ لسنة ٢٠١٢ فى شأن مكافحة جرائم تقنية المعلومات، وجاء القانون الجديد ليعدل كثيراً مما ورد فى القانون الاتحادى رقم ٢ لسنة ٢٠٠٦ فى شأن مكافحة جرائم تقنية المعلومات والذى تم إنهاء العمل به فور نشر القانون الجديد فى الجريدة الرسمية، وجرم القانون كافة الممارسات غير الشرعية على شبكة الإنترنت، كذلك نشر أى أفكار يرى المسئولون أنها تضر بأمن الوطن حتى وإن كانت رسوم كرتونية. (العربية، ٢٠١٣: ١)

وتم الإعلان عبر **"البوابة الرسمية لحكومة دبى" عن المواقع المحظورة** والتى قامت الحكومة بحجبها منذ عام ٢٠١٠ وحتى يناير ٢٠١٣، ويمكن توضيحها على النحو التالى:

جاء فى المرتبة الأولى (محتوى الإنترنت الذى يتعارض مع القيم والأخلاق من دولة الإمارات العربية المتحدة بما فى ذلك التعرى والمواعدة) بنسبة بلغت (٨٨%) فى عام٢٠١١، (٧٩%) فى عام ٢٠١٣. يليها فى المرتبة الثانية (محتوى الإنترنت الذى يحتوى على المواد التى تعبر عن الكراهية للأديان) بنسبة بلغت (٧%) لعام ٢٠١٠، و (٥%) لعام ٢٠١٢، ثم جاء فى المرتبة الثالثة (محتوى الإنترنت الذى لا يتوافق مع قوانين دولة الإمارات العربية المتحدة) بنسبة بلغت (١١%) لعام ٢٠١٠، و(٧%) لعام (٢٠١٣)، يليها فى المرتبة الرابعة (محتوى الإنترنت الذى يسمح أو يساعد المستخدمين على الوصول إلى المحتوى المحظور) بنسبة بلغت (١%) لعام ٢٠١١، يليها (محتوى الإنترنت الذى يشكل بشكل مباشر أو غير مباشر خطراً على مستخدمى الإنترنت فى الإمارات العربية المتحدة مثل مواقع التصييد، أدوات القرصنة وبرامج التجسس) فى المرتبة الخامسة بنسبة بلغت (١١%) لعام ٢٠١٣، ثم (محتوى الإنترنت التى يوفر معلومات حول شراء أو تصنيع أو ترويج أو استخدام الأدوية غير المشروعة) فى المرتبة السادسة بنسبة بلغت (١%)، وأخيراً جاء(محتويات الإنترنت ذات الصلة بالميسر والقمار والتى توضح كيفية المقامرة وتروج له) . وذلك وفقاً لما تم نشرة فى البوابة الرسمية لحكومة دبى . (البوابة الرسمية لحكومة دبى ،٢٠١٣: ١)

كما قامت هيئة تنظيم الاتصالات بدولة الإمارات بإنشاء مركز يسمى "مركز الاستجابة لطوارئ الحاسب الآلى qe cert"، وذلك بهدف تحسين معايير وممارسات أمن المعلومات وحماية البنية التحتية لتقنية المعلومات بدولة الإمارات من مخاطر واختراقات الإنترنت. (مركز الاستجابة لطوارئ الحاسب الآلى، ٢٠١٣: ١)

وسحب البرلمان **العراقى** يوم ١١ فبراير ٢٠١٣ مشروع "قانون جرائم المعلوماتية" الذى أثار جدلاً واسعاً على الصعيد الداخلى والدولى، لما يحتويه من مواد مقيدة للحق فى حرية الوصول للمعلومات ونشرها، وفرض عقوبات تصل إلى السجن المؤبد. (الشبكة العربية لمعلومات حقوق الإنسان ،٢٠١٣: ١)

كما قامت وزارة الداخلية فى **البحرين** من خلال موقعها الإلكترونى بتلقى البلاغات وإستقبال الشكاوى عن المشاركات المسيئة التى يتعرض لها الأفراد عبرالإنترنت بحيث يتيح هذا الموقع إمكانية تقدم أى شخص ببلاغ عن أية مخالفة يراها فى أحد المواقع أو المنتديات الإلكترونية وذلك بإرسال عنوان الموقع الإلكترونى المسئ إلى موقع وزارة الداخلية لتقوم بعد ذلك بإتخاذ الإجراءات القانونية تجاه الموقع ومن قام بارتكاب الفعل الإجرامى. (صحيفة الوسيط البحرينية،٢٠١٣: ١-٢)

وفى الندوة التى نظمتها شركة آيتكس للحلول التقنية بالتعاون مع جامعة الملكة اروى باليمن، بعنوان "أمن المعلومات والأمن السيبرانى" والذى عقد فى ٢٦ مارس ٢٠١٣، أوضح أحد الخبراء فى مجال تقنية المعلومات، أن **اليمن** تُعد من الدول التى لم تهتم بعد بأمن المعلومات، وقد يرجع ذلك إلى : قلة الوعى المعلوماتى والأمنى، وعدم وجود جهاز حكومى متخصص فى تقديم خدمات الدفاع والأمن للفضاء السيبرانى، وأيضاً عدم وجود أطر وتشريعات قانونية متكاملة وحديثة لتؤسس لقاعدة وطنية

فاعلة للأمن السيبرانى الوطنى. لذا أوصت الندوة بضرورة إصدار قوانين وتشريعات وسياسات شاملة تنظم الأمن المعلوماتى وتجرم جرائم الإنترنت،و المطالبة بإنشاء مجلس قومى لحماية اليمن من جرائم الإنترنت والمعلومات على أن تقوم وزارة الاتصالات وتكنولوجيا المعلومات بالتعاون مع المركز الوطنى للمعلومات والأمن القومى بشكيل هذا المجلس. (أنور حيدر، ٢٠١٣: ١)

وعلى الرغم من أن وزارة الداخلية **اللبنانية** استحدثت قسماً خاصاً بجرائم الإنترنت تابعاً لقوى الأمن الداخلى يتعقب عناوين المجرمين من خلال استخدام أدوات متقدمة للعثور على أدلة رقمية متصلة بجرائم شبكة الإنترنت، إلا أن التشريعات القانونية فى لبنان لا يزال يعتريها قصور شديد، فلم تصدق لبنان على الاتفاقية المتعلقة بجرائم المعلوماتية الإلكترونية حتى عام (٢٠١٣) – والذى لا يزال معلقاً منذ عام (٢٠٠٥). (جورج لبكى، مرجع سابق : ٧)

وتم إطلاق حملة بإسم **"الحملة الوطنية لأمن الإنترنت فى لبنان"** بالتعاون مع وزارة الاتصالات، من خلال إطلاق حملة رسائل قصيرة خلال أسبوع ٥ شباط ٢٠١٣ لجميع المشتركين بخدمة الهاتف النقال، وكتابة الرابط الذى يؤدى إلى الموقع الإلكترونى الوطنى National Internet Safety Lebanon، ويهدف هذا الموقع إلى مساعدة المواطنين اللبنانيين ليتصرفوا بمسئولية أكبر فى الفضاء السيبرانى ويقدم نصائح مفيدة ومبسطة ومعلومات مكثفة للأهل والمراهقين والمدرسين، لمساعدتهم على مواجهة مخاطر الإنترنت. وقد تم إطلاق هذا الموقع باللغتين الإنجليزية والعربية. (منال شهاب ،٢٠١٣: ١-٥)

وقد ولج **السودان** – كغيره من بلدان العالم الثالث – مجال التقنية وفضاءاتها متأخراً جداً، ويرجع ذلك لعدة أسباب منها الاقتصادى والسياسى والاجتماعى، وقد مارست تلك الأسباب أحد المعوقات الأساسية لبرامج التحديث والعولمة الشاملة للمجتمع السودانى. وعلى الرغم من وجود قانون للمعاملات الإلكترونية وقانون للجرائم المعلوماتية وما يشتملان عليه من عقوبات رادعة لمن يرتكب جريمة إلكترونية، إلا أن الأمر يتطلب تطوير السياسات الوطنية لكى تواجه مخاطر جرائم الإنترنت، وتخصيص نيابة كاملة للجرائم الإلكترونية وذلك لرصد الشبكات الإجرامية على الإنترنت. (الموقع الرسمى لوزارة الدفاع بجمهورية السودان،٢٠١٣: ١-٢)

والجدير بالذكر أنه بعد قرار وزير الداخلية التونسى بإنشاء هيئة حكومية لمكافحة "الجرائم الإلكترونية"، حذرت مجموعة "أنونيموس – تونس"* من عودة الرقابة على الإنترنت فى تونس، وقالت المجموعة فى رسالة صوتية باللغة الفرنسية موجهة إلى "الشعب التونسى" أن (الحكومة التى تقودها حركة النهضة الإسلامية تريد استغلال أنشطتنا الإلكترونية لإعادة إرساء وسائل رقابة على الإنترنت بهدف سجن الناس فى أفكار مخالفة لايديولوجياتهم .. تريد الحكومة هذه المرة فرض رقابة على كل شئ، ستبدأ بالإنترنت ثم تمر إلى تكميم الصحافة وهذا قد حصل، وغداً (تكميمكم) أنتم مواطنينا الأعزاء). (موقع France 24، ٢٠١٣: ١-٢)

من العرض السابق للجهود المبذولة من قبل الدول العربية لمكافحة جرائم الإنترنت يتبين ما يلى :

تنوعت طرق المكافحة وتعددت صورها ما بين: **إنشاء إدارة متخصصة معنية بمكافحة جرائم الإنترنت** ،حيث إتجهت بعض الدول العربية إلى إنشاء إدارة أو وحدة خاصة معنية بمكافحة جرائم الإنترنت مثل (الأردن ٢٠٠٨ – الكويت ٢٠٠٩ – فلسطين ٢٠١٣– أما دولة البحرين فقد اكتفت بتلقى البلاغات عن مثل تلك الجرائم واستقبال الشكاوى على موقع وزارة الداخلية الخاصة بها).وأيضاً**عقد العديد من المؤتمرات والندوات سواء على الصعيد الوطنى أو الدولى** هذا فضلاً عن عقد العديد من الدورات لتخريج ضباط قادرة على التعامل مع هذه النوعية من الجرائم، وكذلك مشاركة الإنتربول الدولى فى الحملات التى يشنها وخاصة على المواقع الإباحية المتاحة على شبكة الإنترنت، واستغلال الأطفال جنسياً عبر الإنترنت، و**كذلك إصدار بعض التشريعات القانونية للحماية من جرائم الإنترنت :**

* أونيموس – تونس : هى مجموعة متخصصة فى القرصنة واختراق مواقع الإنترنت فى تونس، وفى عام (٢٠١٢) قرصنت مجموعة أنونيموس البريد الإلكترونى لرئيس الحكومة السابق (حمادى الجبالى) الأمين العام لحركة النهضة ولأعضاء فى حكومته، رداً على ما اعتبرته محاولات من الإسلاميين للتضييق على الحريات فى البلاد، كما اخترقت الموقع الإلكترونى الرسمى (لراشد الغنوشى) رئيس حركة النهضة الذى وصف عمليات القرصنة بأنها "حرب إلكترونية".

ومن أمثلتها : (تشريع القانون الجزائرى لسنة ٢٠٠٩ المتعلق بجرائم الإنترنت، فرض نظام لمكافحة الجرائم المعلوماتية فى السعودية عام ٢٠٠٨، تشريع القانون الإماراتى لسنة ٢٠١٢ المتعلق بمكافحة جرائم تقنية المعلومات). هذا فضلاً عن قيام بعض الدول بحجب بعض المواقع المحظورة مثل دولة الإمارات، أو حجب المواقع الاباحية عن الظهور فى شبكة الإنترنت المحلية لها مثل ليبيا .

وأخيراً قامت بعض الهيئات – بالدول العربية – بإطلاق حملات أو إنشاء مراكز للحماية من اختراقات الإنترنت بهدف مساعدة المواطنين وتقديم نصائح هامة عن كيفية استخدام شبكة الانترنت بشكل آمن .

وعلى الرغم من الجهود التى بُذلت من قبل الدول العربية، إلا أنها تُعد غير كافية- من وجهه نظر الباحثة- لمكافحة هذا النوع المستحدث من الجرائم، وقد يرجع ذلك إلى :

١- عدم اتفاق الدول العربية على وضع مسمى محدد للجريمة التى تحدث فى بيئة تكنولوجيا المعلومات والاتصالات، فمنهم من أطلق عليها جرائم تكنولوجيا المعلومات والاتصالات والإنترنت مثل الأردن، ومنهم من يصنفها ضمن الجرائم المستحدثة مثل قطر، ومنهم من أطلق عليها الجرائم المعلوماتية مثل السعودية، والعراق، والسودان، ومنهم من أطلق عليها مسمى الجرائم الإلكترونية مثل الكويت، وفلسطين، وتونس، ومنهم من أطلق عليها جرائم تقنية المعلومات مثل الإمارات، ومنهم من أسماها جرائم المعلوماتية الإلكترونية مثل لبنان، وأخيراً من أطلق عليها مسمى جرائم الإنترنت مثل الجزائر.

٢- ثمة قصور تشريعى واضح فى الكثير من الدول العربية، والتى تحول دون مكافحة جرائم الإنترنت، فمثلاً لبنان لم تصدق على الاتفاقية المتعلقة بالجرائم المعلوماتية الإلكترونية منذ عام (٢٠٠٥) وحتى عام (٢٠١٣)، أما العراق فقامت بسحب مشروع "قانون الجرائم المعلوماتية" فى فبراير ٢٠١٣، الذى آثار جدلاً واسعاً على الصعيد الداخلى والدولى. أما فى فلسطين فمازال مشروع قانون "الإنترنت والمعلوماتية" تحت الإعداد فى ديوان الفتوى والتشريع بوزارة العدل.

٣- هذا فضلاً عن تركز سياسات الدول العربية والأفريقية لمواجهة جرائم الإنترنت* فى مجال : غسل الأموال، والتجارة الإلكترونية، والاعتداء على أنظمة الشبكة والحاسوب.(فايز الشهرى ،٢٠٠٥ : ١٧٠)

ولهذا اتجهت بعض الدول إلى تطبيق النصوص القانونية التقليدية لمواجهة الجرائم الناشئة عن استخدامهم شبكة الإنترنت، إلا أن ثمة عقبات عديدة تقف أمام تطبيق النصوص القانونية التقليدية، نذكر منها :

- أن القواعد الموجودة فى القوانين القائمة سُنت للتعامل مع المجتمع التقليدى، ولم يكن للكمبيوتر والإنترنت أى دور فيه.
- التقسيم الثلاثى للجرائم المنصوص عليه فى قانون العقوبات لا يجدى مع جرائم الإنترنت، وذلك لعدم استطاعته الفصل بين الحقوق المعتدى عليها بسبب تداخلها بنسب متفاوتة فى هذه الجرائم.
- ظهور أفعال إجرامية لا ينطبق عليها أى نص من قانون العقوبات.
- البعد الدولى الذى تتصف به جرائم الإنترنت وإمكانية تحقيق النتيجة فى أكثر من دولة، ووجود الجانى فى الخارج قد يكون عائقاً أمام النصوص التقليدية القائمة. (محمد الكعبى ،٢٠٠٥: ٦٤-٦٦)

ثالثاً: الجهود المحلية (المصرية) لمكافحة جرائم الانترنت

اما فى جمهورية مصر العربية فقد استحدثت وزارة الداخلية إدارة جديدة لمكافحة جرائم الحاسبات وشبكات المعلومات*، لتتولى تأمين الشبكات الخاصة بالوزارة، وتتبع المواقع الإلكترونية

* والجدير بالذكر توجد بعض التشريعات فى العالم العربى التى تتعلق بالجرائم المعلوماتية والحاسب خاصة فى مصر، وسوريا، والأردن، والإمارات العربية المتحدة، وعمان، وقطر ... ونظراً لاختلاف جرائم الإنترنت عن الجرائم المعلوماتية من حيث طبيعتها وأنواعها، ومكان ارتكاب الجريمة، فقد ركزت الباحثة على التشريعات الخاصة بجرائم الإنترنت فقط نظراً لارتباطها المباشر بموضوع الدراسة.

المشبوهة وغير الشرعية، وتلقى البلاغات من الأفراد أو الجهات، والعمل على مكافحة جرائم الانترنت بعد تقنين الإجراءات والعرض على النيابة المختصة. .(محمد سعد،٢٠٠٣: ١٠١)

وتُعد إدارة مكافحة جرائم الحاسبات وشبكات المعلومات Cyber crime combat Department هى الإدارة المعنية بمكافحة كافة الجرائم المتعلقة بالاستخدام غير المشروع والمخالف وغير المرخص به للحاسبات الآلية وشبكات المعلومات والاتصالات فى المجتمع المصرى. وقد صدر قرار من وزارة الداخلية برقم ١٣٥٠٧ لسنة ٢٠٠٢ بإنشاء إدارة مكافحة جرائم الحاسبات وشبكات المعلومات بالإدارة العامة للمعلومات والتوثيق، وذلك للأخذ بزمام المبادرة لمواجهة تلك الجرائم، والحد من خطورتها وضبط مرتكبيها وتقديمهم للعدالة.

ويتمثل **الهدف الأساسى** لإنشاء تلك الإدارة* فى : "توفير الاستخدام الآمن للحواسيب الآلية وشبكات المعلومات، تحقيقاً للأمن العام بمدلولاته المختلفة".وتعمل الإدارة من خلال **رؤية محددة** تتبلور فى الآتى: "إن الحد من مخاطر وسلبيات الاستخدام غير الأمن لتكنولوجيا المعلومات.. يحض على تعظيم الاستفاذات الإيجابية من تكنولوجيا المعلومات فى جميع مناحى حياتنا".

وبالنسبة **لإختصاص إدارة مكافحة جرائم الحاسبات وشبكات المعلومات**: فقد تم وضع خطة عمل للإدارة، كان من أهم بنودها:

- ضبط ومكافحة جرائم الانترنت بشتى صورها وأنماطها.
- تقديم المساعدات الفنية والأدلة المادية لضبط جرائم الانترنت لأجهزة الشرطة النوعية.
- حصر ومتابعة مقاهى الانترنت ووضع الضوابط لها لتسجيل بيانات مستخدمى الشبكة العالمية وإعداد قاعدة بيانات لخدمة أغراض المتابعة.
- إعداد البحوث الفنية والقانونية فى مجال جرائم الحاسبات مع الأجهزة المختصة بوزارة الداخلية.
- وضع خطة تأمين ووقاية نظم وشبكات المعلومات لأجهزة وزارة الداخلية.
- إعداد أرشيف متكامل للمعلومات التى تخدم أعمال الإدارة وإنشاء الملفات والسجلات والبطاقات اللازمة لذلك.
- إعداد قاعدة بيانات بجرائم المعلومات التى تدخل فى نطاق اختصاص الإدارة.

كما تختص إدارة مكافحة جرائم الحاسبات وشبكات المعلومات بالإدارة العامة للمعلومات والتوثيق بالتعامل مع كافة الجرائم التى ترتكب عن طريق شبكة الانترنت ومن ضمنها جرائم الصور الفاضحة للأطفال. حيث يتم التحقيق فى جرائم الصور الفاضحة باعتبارها أحد الجرائم المنصوص عليها فى قانون العقوبات، فيُجرم قانون العقوبات المصرى رقم ٩٥ لسنة ١٩٩٦ مادة (١٧٨) كافة الأفعال المنافية للأداب العامة والتى تتضمن الصور الفاضحة.

والجدير بالذكر أنه يتم الاتصال دولياً بإدارة مكافحة جرائم الحاسبات وشبكات المعلومات من خلال إدارة الشرطة الجنائية الدولية** والعربية "انتربول القاهرة – قطاع مصلحة الأم العام". وتلتزم مصر بالوثائق الدولية والإقليمية الموقع عليها والقوانين الوضعية المصرية.

---

* وأستطاعت الباحثة الحصول على تلك البيانات من الإداره العامة لمكافحة الحاسب وشبكات المعلومات بوزارة الداخلية بعد الحصول على موافقة أمنية .

** وحصلت الباحثة على بعض من نماذج التعامل مع الانتربول الدولى فى مكافحة الاستغلال الجنسى للأطفال من إدارة مكافحة جرائم الحاسب وشبكات المعلومات، وجاء ذلك كالتالى:

أولاً: انتربول لندن:

١- عملية مازارد (عام ٢٠٠٤):

تم القبض على أحد الأشخاص بالمملكة المتحدة ووجهت إلهي تهمة حيازة وإنشاء وتوزيع صور استغلال جنسى للأطفال وتبين أنه مرتبط بمجموعات بريدية على شبكة الياهو وإن الاشتراك بتلك المجموعات من خلال إرسال صور أطفال جنسية لأعضاء المجموعات. وأثبت الفحص الفنى وجود أرقام تعريفية خاصة بدولة مصر حيث تبين من فحصها أنها مستخدمة من دائرة قسم المعادى وأنها خاصة بمقاهى إنترنت بتلك المنطقة وأن أصحاب تلك المقاهى لم يقوموا بتسجيل بيانات المترددين عليهم سواء من المصريين أو الأجانب المقيمين بتلك المنطقة وأنهم

يستخدمون برامج Deep freeze لإرجاع حالة الأجهزة إلى ما كانت عليه قبل التشغيل. وتم اتخاذ الإجراءات القانونية حيال أصحاب تلك المقاهى لعدم قيامهم بتسجيل المترددين ومخالفتهم لشروط التراخيص.

٢- بث معلومات على شبكة الانترنت (عام ٢٠٠٨):

وردت معلومات من انتربول لندن تفيد بأن أحد الأشخاص يستخدم عنوان بريد الكترونى قام بالدخول على موقع للمحادثة على شبكة الانترنت وعرض فيه صورة طفلة تبلغ من العمر ثلاث سنوات وأنه يعرضها لممارسة الجنس مع شخص آخر وأنه قد تم رصد تلك المحادثة من رقم تعريفى بمصر. وبتكثيف التحريات وجمع المعلومات أمكن التوصل لمرتكب الواقعة والذى قام بعرض صورة طفلة أدعى أنها نجلته والتى تبلغ من العمر ثلاث سنوات لممارسة الجنس مع كل من يرغب من خلال إقامة محادثات على شبكة الانترنت باستخدام نفس عنوان البريد الالكترونى الذى تم رصده بمعرفة انتربول لندن. وتم القبض على مرتكب الواقعة حيث اعترف بارتكابه لها وعلل ذلك بأنه قام بارتكابها بدافع الفضول والتسلية وتم تقديمه للنيابة العامة التى قررت إحالته لمحاكمة عاجلة. وتم إخطار انتربول لندن بما تم من إجراءات.

ثانياً: انتربول روما:

١- عملية "كانال جراند" CANAL GRAND (عام ٢٠٠٥):

أفادت التحريات السرية وفرق مكافحة جرائم الحاسب الألى بمدينة فيينا قيام مواطنون إيطاليون وأجانب باستخدام برامج المشاركة للملفات file– Sharing وبخاصة برنامج يسمى "كازا" Kazaa وكذلك شبكة "فاست تراك" Fast treck بتوزيع مواد وصور إباحية للأطفال على شبكة الانترنت. واثبت الفحص الفنى للأرقام التعريفية الواردة بالأسطوانة المرفقة أن التوقيتات غير متوافقة مع استخدامات تلك الأرقام على مدار اليوم المحدد لكل رقم تعريفى الأمر الذى أدى إلى عدم التوصل إلى مستخدمى تلك الأرقام وتحديد المشاركين فى توزيع المواد والصور الإباحية للأطفال. وتم مخاطبة انتربول روما بما تم التوصل إليه لمراعاة تحديد وقت استخدام الرقم التعريفى بتوقيت جرينتش لإمكانية تحديد التوقيت المحلى بكل دقة.

ثالثاً: انتربول ألمانيا (فسبادن):

١- عملية (افرى ستار) Every Star (عام ٢٠٠٥):

قامت شركة ميكروسوفت بإبلاغ مكتب المدعى العام بميونخ بأنها أغلقت المواقع الخاصة بمجموعة يطلق عليها اسم Every Star حيث كان يتم توزيع صور إباحية للأطفال داخل نطاق هذه المجموعة. وأثبت الفحص الفنى إن الأرقام التعريفية التى تم استخراجها مر عليها أكثر من عام– أى أنها تعدت المدة القانونية للحفظ– الأمر الذى أدى إلى عدم التوصل لمستخدميها. وتم مخاطبة انتربول فسبادن بمراعاة المدد القانونية المتفق عليها دولياً والواردة باتفاقية بودابست (٩٠ يوماً).

رابعاً: انتربول باريس (فرنسا):

١- ارتافنان Artafnan (عام ٢٠٠٥):

ورد من انتربول باريس أنه تم العثور على مجموعتين بشبكة الياهو تتضمن صور شرائط فيديو للأعمال الإباحية للأطفال وأن عدد الأعضاء المسجلين على تلك المجموعات ١٣٠٠ عضو من مختلف دول العالم مستخدمين عناوين أجنبية. وأثبت الفحص الفنى للأرقام التعريفية الواردة بالأسطوانة المرفقة بكتاب الجهة أنها قد استخدمت من خطوط تليفونية منزلية بمدينة الإسكندرية ومدينة ٦ أكتوبر. وأكدت التحريات السرية أن أصحاب تلك المنازل قد قاموا باستئجارها لأجانب أثناء إقامتهم بمصر. وتم مخاطبة انتربول باريس ببيانات الأجانب الذين قاموا باستئجار تلك الشقق خلال الفترة التى تم فيها ارتكاب الواقعة.

خامساً: انتربول أوسلو (النرويج):

١– رسائل بريد الكترونى (عام ٢٠٠٥)

ورد من انتربول أوسلو أنه تم القبض على شخص نرويجى بتهمة حيازة وترويج صور فاضحة للأطفال من خلال إنشاء مجموعة ضمت أشخاص من عدة دول على شبكة الانترنت تتراسل فيما بينها من خلال رسائل البريد الالكترونى. وأثبت الفحص الفنى أن الرقم التعريفى الصادر من مصر خاص بأحد الأشخاص بمصر بمنطقة المعادى. وبسؤاله أفاد بأنه قام بتأجير مسكنه منذ عام ٢٠٠٢ لشخص بريطانى الجنسية يعمل مدرس بالقاهرة. وتم إخطار انتربول أوسلو بما تم التوصل إليه من بيانات الشخص الأجنبى مستأجر العقار الذى ارتكبت من خلاله الواقعة.

سادساً: انتربول برازيليا (البرازيل):

١- نشر صور إباحية للأطفال من خلال تبادل الملفات (عام ٢٠٠٨):

ورد من انتربول برازيليا إن عمليات البحث التى تقوم بها وحدة الإجرام السيبرى بالشرطة الفيدرالية البرازيلية بالتعاون مع خبراء من الجمعية الوطنية لعلوم الطب الشرعى والأدلة الجنائية قد أسفرت عن التوصل إلى مواد تتضمن صور إباحية للأطفال وعمليات استغلال جنسى لهم تبث عبر شبكة الانترنت من خلال استخدام برنامج حاسب آلى يسمى Emule. وأثبت الفحص الفنى للأسطوانة المرفق بها بيانات المستخدمين من مصر أنهم قد قاموا بالدخول على هذا الموقع باستخدام أرقام بطاقات ائتمان مملوكة لأجانب من خلال أرقام تعريفية بمصر ولم يتوصل الفحص الفنى لتحديد مستخدمى تلك الأرقام نظراً لمضى أكثر من عام على تاريخ استخدامها الأمر الذى يعنى استحالة وجود بيانات يمكن من خلالها تحديد المستخدمين. وتم إخطار انتربول برازيليا بمراعاة المدد القانونية المتفق عليها دولياً والواردة باتفاقية بودابست (٩٠يوماً).

والجدير بالذكر فى إطار الخطة الاستراتيجية للإدارة العامة للمعلومات والتوثيق لمكافحة الجريمة المعلوماتية بشتى أشكالها وأنواعها، فتعمل الإدارة من خلال خطة متكاملة الأبعاد، وتتمثل فى عدة محاور جاءت كالتالى :

المحور الأول: فى مجال بناء القدرات والتمكين (التدريب):حيث يتم تدريب عدد من الضباط على أحدث أساليب مكافحة الجرائم الحديثة، سواء كان تدريب داخلى(بالجهات الشرطية المختلفة)، أو جهات محلية (وزارة الاتصالات وجهات متخصصة)، أو تدريب دولى.

المحور الثانى: فى مجال الافصاح والإتاحة (توفير البيانات والإحصاءات) : حيث يتم إعداد قواعد المعلومات تتيح توافر كافة البيانات، سواء تم تقديم البلاغ فى الإدارة، او من خلال الخط الساخن، أو بلاغات واردة على الموقع الاليكترونى للوزارة. كما تقوم الإدارة بإصدار إحصائية فى مطلع كل عام عن عدد القضايا فى العام المنصرم، إلا انه حالياً يتأخر هذا الاصدار لمده عام تقريباً .

المحور الثالث: فى مجال المشاركة والتعاون: حيث تتعاون الإدارة مع كافة الأطراف الفاعلة فى عملية المكافحة، سواء كانت أطراف محلية (حكومية، منظمات مدنية، مقدمى الخدمة) او أطراف دولية، هذا فضلا عن تقديم الدعم الفنى لعدد من الجهات (القضائية والأمنية، والقوات المسلحة، وجهات أخرى).

المحور الرابع : فى مجال السيطرة والتحكم: حيث تقوم الإدارة بمتابعة سير العمل بمقاهى الانترنت للتأكد من توفيرها لضوابط الاستخدام الأمن للانترنت وقد تم ضبط عدد من القضايا خلال الحملات المستمرة التى تمت بمعرفة الإدارة على مقاهى الانترنت.

المحور الخامس : فى مجال التوعية: فى إطار جهود الإدارة للتوعية بمخاطر الاستخدام غير الآمن للانترنت تقوم الإدارة بعدد من الأنشطة التوعوية مثل : اللقاءات التليفزيونية، والأحاديث صحفية، وندوات التوعية، وأيضاً المشاركات فى مؤتمرات دولية ومحلية، وأخيراً توعية للسادة الضباط بمختلف المعاهد الأمنية.

وبإستقراء تقارير الأمن العام الصادرة من وزارة الداخلية الخاصة بأعداد جرائم الحاسبات وشبكات المعلومات المبلغ عنها فى المجتمع المصرى منذ عام (٢٠٠٢) وحتى عام (٢٠١٦) **تبين ما يلى :

- تم الإبلاغ عن هذة الجرائم **لأول مرة فى المجتمع المصرى** عام (٢٠٠٢) بعدد (٧) بلاغات، وظلت هذه الجرائم فى تزايد مستمر، لتصل عام (٢٠١٣) الى (٢٣٤٤) بلاغاً ،ثم واصلت فى الزيادة لتصل عام (٢٠١٥) الى (٥٠٥١) جريمة، و(٦٧٠٩) فى عام (٢٠١٦)* . ولعل هذه المؤشرات تشير إلى ضرورة مواجهة تصاعد هذه الجرائم، ويتم ذلك من خلال العمل بقانون الجرائم الالكترونية الجديد الذى تم التصديق علية من قبل مجلس الشعب، ولم يتم العمل به حتى الأن (٢٠١٨) ،هذا فضلاً عن ضرورة إيجاد آليات للتعاون الدولى فى الجرائم المرتكبة عن طريق حاسبات خادمة خارج البلاد. (تقرير الأمن العام، ٢٠٠٣: ٧٩٤)
- وصل إجمالى أعداد الجرائم المبلغ عنها فى إدارة مكافحة جرائم الحاسب وشبكات المعلومات الى **(أثنين وعشرون الف ومائة وأربعة وستون جريمة)** وذلك منذ عام ٢٠٠٢ وحتى عام ٢٠١٦ . **ولعل هذا يُعد** مؤشر هام على دور إدارة مكافحة جرائم الحاسبات وشبكات المعلومات فى تتبع مرتكبى هذه الجرائم وإستحداث اساليب جديدة تتناسب مع حجم التغيرات التقنية والتكنولوجية الحادثة فى العالم أجمع للتوصل إلى فاعليها، كما يعُد أيضاً دليلاً واضحاً فى زيادة وعى أفراد المجتمع بأهمية عمل بلاغات فى الجهة المختصة بذلك، وإلى انه يحقق الغاية المبتغاة منه، وبتغيير الفكرة السائدة لدى بعض أفراد المجتمع فى انه يصعب الوصول الى مرتكبى هذه الجرائم، وقد يشير أيضاً الى حجم المعاناة النفسية للخسائر الناجمة عن مثل تلك الجرائم وخاصة ان الغالبية العظمى منها هى جرائم أخلاقية (إساءة سمعة،سب وقذف وتشهير) تلك الجرائم التى تهدف فى المقام الأول الى التأثير على سمعة صاحبها وتشوية سمعته الاجتماعية والمهنية والأخلاقية من خلال شبكة الانترنت مما يضطر ضحاياها إلى الإبلاغ عن مثل تلك الجرائم .

---

* أستطاعت الباحثة الحصول على تلك البيانات الاحصائية من ادراة مكافحة جرائم الحاسب وشبكات المعلومات بوزارة الداخلية بعد الحصول على موافقة أمنية وأشتملت تلك البيانات الفترة منذ عام ٢٠١١ وحتى عام ٢٠١٦.

- **وبالنسبة لأنواع الجرائم :** فتتنوع جرائم الحاسب وشبكات المعلومات فى المجتمع المصرى ما بين جريمة إساءة سمعة فى المرتبة الأولى بنسبة بلغت (٣٥.١٣%)، يليها جريمة سب وقذف وتشهيرفى المرتبة الثانية بنسبة بلغت (٢٧.٢٨%)، وجاءت جريمة ابتزاز وتهديد فى المرتبة الثالثة بنسبة بلغت (١٠.٦٤%)، ثم جريمة انتحال صفة فى المرتبة الرابعة بنسبة بلغت (٨.١٧%)، يليها جريمة استيلاء على بريد الكترونى فى المرتبة الخامسة بنسبة بلغت (٧.٨٠%)، كما جاءت جريمة نصب واحتيال فى المرتبة السادسة بنسبة بلغت (٤.٦٧%)،اما جريمة اختراق وقطع اتصال فجاءت فى المرتبة السابعة بنسبة (١.٥٦%)، فجريمة سرقة بنسبة بلغت (١.٢٦%)، يليها جريمة التحريض بنسبة (١.٢١%)، كما جاءت جرائم أخرى بنسبة أقل من (١%) وتمثلت تلك الجرائم فى: (شبكات، تهديد بالقتل، إعادة بث قنوات فضائية، ملكية فكرية،كروت ائتمان،غياب،اثبات حالة،ازدراء الأديان، تعذيب حيوانات) وذلك من إجمالى اعداد جرائم الحاسب وشبكات المعلومات فى المجتمع المصرى منذ عام ٢٠١٢ وحتى عام ٢٠١٦ . (تقارير الأمن العام، ٢٠٠٣، ٢٠٠٤، ٢٠٠٥، ٢٠٠٦، ٢٠٠٧، ٢٠٠٨، ٢٠٠٩، ٢٠١٠ : ٧٩٥، ٨٦٠، ٨٦٢، ٨٧٢، ٨٠١، ٩١٥، ٩١٩، ٩٣١)

- **وبالتحليل السوسيولوجى لتلك الجرائم،** يتضح ان الجرائم الأخلاقية كما مثلتها(جريمتى إساءة سمعة، سب وقذف وتشهير) جاءت فى المرتبة الأولى من بين أنواع جرائم الانترنت، ولعل هذا يشير إلى ان هناك تغييراً جذرياً فى منظومة القيم الاجتماعية والأخلاقية فى المجتمع فبات من اليسير أختلاق اكونت وهمى أو سرقة بريد إلكترونى أو أنتحال صفة المجنى عليه ،وتركيب بعض مقاطع الصوت والصورة ورفعها على وسائل التواصل الاجتماعى حتى يراها كل المقربين من المجنى عليه وكل الاعضاء على صفحتة الشخصية، فيزداد الضرر النفسى والاجتماعى له، ويصبح التشهير فى اسوء صوره اذا لصق الجانى صورة إباحية للمجنى علية أو استغل اسمه وصفته للدخول لأحد المواقع المشبوهة فيسهل على الأخرين تصديق الأمر. وبالتالى نجد انتشار للعديد من القيم السلبية كعدم احترام خصوصية الأخر، والرغبة فى الانتقام لأتفه الاسباب ،وإبداء الرأى بطريقة غيرلائقة لدرجة تصل إلى تشوية السمعة وإلصاق التهم بالأخرين .

المحور السادس: آليات مكافحة جرائم الانترنت بين الوضع الراهن والنظرة الإستشرافية

سيتم عرض آليات المكافحة وفقاً لمرحلتين هما : **المرحلة الوقائية والمرحلة العلاجية،** وفيما يلى إستعراض ذلك على النحو الآتى:

أولاً: المرحلة الوقائية

تُعد المرحلة الوقائية من أهم مراحل المواجهة التى ينبغى أن تكرس لها كل الجهود عملاً بالمقولة القائلة إن " الوقاية خير من العلاج"، وتتسم أدوات الحماية والأمن فى هذه المرحلة بإنها عبارة عن مجموعة من البرامج يتم تثبيتها أو تحميلها على الحاسبات حتى تكون النظم المعلوماتية بمأمن من مخاطر واختراقات هذة النوعية من الأنشطة الإجرامية، مثل : برامج الحماية من الفيروسات، وبرامج الجدران النارية، وبرامج تشفير المعلومات. (هلالى عبد اللاة، ٢٠١٥: ٢٢٦-٢٢٧)

وتوصلت نتائج أحدى الدراسات التى طُبقت فى المجتمع المصرى عام (٢٠١٦) : إلى تنوع الأساليب الوقائية التى يتبعها المبحوثين لعدم تعرضهم لجرائم الإنترنت وفقاً للنوع، حيث جاء الذكور أكثر استخداما لبرامج حمايه وعمل فحص شامل ودورى على جهاز الحاسب الآلى، بينما جاءت المبحوثات الإناث الأكثر حرصاً فى عدم الاستجابه لأى طلب من أشخاص بدون سابق معرفة بهويتهم الحقيقيه . (رانيا حاكم، ٢٠١٦: ٢١٤-٢١٥)

ولعل هذا يؤكد على ضرورة الإلتزام ببعض الاساليب الوقائية عند إستخدام شبكة الانترنت حتى لا نكون عرضة لهذة النوعية من الجرائم، إلا أن الواقع يكشف لنا العديد من الممارسات التى تتم عبر الشبكة، كإدخال المعلومات الشخصيه (الاسم وأرقام التليفونات ومكان العمل ...وغيرها) بشكل يومى عبر مواقع التواصل الاجتماعى ، وأيضاً تحميل الصور الشخصية والعائليه ومشاركة الأحداث الهامة،

وبالتالى أصبحت الأسرار الشخصية معلنة للجميع بكل ما تحملة من أفراح وأتراح، مما قد تكون عرضه للاستغلال من قبل البعض فيما بعد، حيث تُعد هذة البيانات مجالاً خصباً وبيئة ثرية يستغلها البعض فى الإساءة أو إحداث أضرار بالآخرين .

وإستناداً لما سبق : فلابد من إتباع بعض الأساليب الوقائية عند التعامل مع شبكة الأنترنت، نذكر منها على سبيل المثال وليس الحصر: إستخدام برامج حماية وعمل فحص شامل ودورى على جهاز الحاسب الآلى، تغيير كلمة السر بشكل دورى، الحرص فى عدم الاستجابه لأى طلب من أشخاص بدون سابق معرفة بهويتهم الحقيقيه، عدم فتح إيميلات من شخصيات مجهولة، الحرص فى إرسال البيانات الشخصية الحقيقة لأى موقع، عدم المبالغة فى تحميل الصور الشخصية والعائلية عبر مواقع التواصل الاجتماعى، عدم وضع بيانات وأرقام الكروت الائتمانية دون التأكد من جدية الموقع، وأخيراً الحرص عند تبادل أجهزة الهواتف المحمولة أو الحاسب الشخصى "اللاب توب" مع آخرين لإحتوائهم على بيانات هامة وشخصية.

ثانياً : المرحلة العلاجية

من المنطقى والبديهى انه لكى يتم مواجهة جرائم الانترنت فى -المرحلة العلاجية- لابد أولاً من وضع تعريف واضح ومحدد لما يشكل الجريمة السيبرانية أو جرائم الإنترنت، وبالرغم من المحاولات العديدة التى قامت بها الدول المتقدمة وعلى رأسها الولايات المتحدة الأمريكية، والدول العربية إلا أنها ما زالت تطبق بعض النصوص القانونية التقليدية على الجرائم التى تحدث فى بيئة تكنولوجيا المعلومات، ومن المعلوم أن الجريمة الإلكترونية بصفة عامة تحدث فى بيئة إفتراضية أى واقع إفتراضى بما يتيحة هذا العالم من تغيير مكان وزمان وطريقة إرتكاب الجريمة ،هذا فضلاً عن استحداث أساليب جديدة بإستمرار فى إرتكاب الجرائم، والوصول إلى أكبر عدد من الضحايا فى وقت وجيز، وإمكانية إرتكاب الجريمة عن بعد، وهو الأمر الذى أدى إلى صعوبة تعقب الجانى ومن ثم الوصول إلية خاصة إذا أرتكبت الجريمة من خلال حواسيب خارج البلاد .

ومما يزيد من صعوبة الأمر إعتماد هذه الجرائم على التطور التكنولوجى الحادث والمستمر فى العالم أجمع، حيث يلجأ الجناة إلى استغلال القدرات التكنولوجية الهائلة التى تتيحها شبكة الانترنت فى ارتكاب بعض الأفعال غير المشروعة والمجرمة قانوناً عبر الفضاء الالكترونى، وبالتالى فلابد من تدخل القانون بشكل سريع حتى يتواكب مع حجم هذة التغيرات . هذا إلى جانب ضرورة الاهتمام بسن تشريعات ونصوص قانونية تجرم جميع أشكال الأفعال الاجراميه التى تتم عبر الشبكة، مع تشديد العقوبات بشكل يتناسب مع نوعية كل جريمة والضرر الناتج عنها .

ومما يزيد من تفاقم المشكلة هو إختلاف البيئات والعادات والتقاليد والثقافات والديانات بين الدول المرتبطة بالإنترنت بما يستتبعه ذلك من اختلاف التشريعات فى مسائل أساسية بين دول الشرق والغرب والعالم الإسلامى، ولذلك فإنه من الطبيعى أن نجد أن بعض المعلومات أو الصور التى تبث على الإنترنت قد تكون مشروعة فى بلد المنشأ ولكنها قد تكون مستهجنة أو غير مشروعة فى بلد آخر (جميل عبد الباقى،٢٠٠٢: ٧٢).

بالإضافة إلى أن تأثير هذه الجرائم يمتد ليشمل العالم بأسره وفقاً لأننا نعيش فى عصر العولمة، العصر التى ذابت فية الحدود بين الدول، فأصبح من السهل واليسير التواصل والأتصال بين شعوب العالم المختلفة ،وهنا تكمن الخطورة على اعتبار أن هذه النوعية من الجرائم لم يقتصر تأثيرها على المجتمع المحلى الذى أفرز هذه النوعية من الجرائم وإنما تأثيرها سيكون ممتد وأشمل وأكثر ضراوة وقسوة لأنها سوف تنتشر على مستوى العالم بأسره. لذا فإن مواجهة هذه الجرائم لا تقتصر على الدولة التى أفرزتها بل لابد أن يكون هناك تعاون دولى بين مختلف دول العالم، مما يعنى أن النتائج المأساوية لانتشار جرائم الإنترنت لا تقتصر على دولة دون الأخرى فهى بمثابة وباء حقيقى يحتاج إلى تحرك عالمى.

لذا بات من الضرورى أن نخلص إلى مجموعة من المقترحات المستقبلية المأمولة فيما يتعلق بآليات مكافحة جرائم الانترنت :

١- تنسيق الجهود الدولية والعربية والمحلية لوضع تصور محدد لجرائم الإنترنت، ومن ثم وضع الأساليب الملائمة لمواجهة تلك الجرائم، مع ضرورة إسراع الدول – وخاصة الدول العربية – بسن بعض النصوص القانونية نظراً لعدم كفاية النصوص التقليدية فى شكلها الحالى، هذا بالإضافة إلى ضرورة تعزيز التعاون الدولى والانضمام إلى الاتفاقيات والمعاهدات الدولية لمواكبة التطورات المتلاحقة فى هذه النوعية من الجرائم.

٢- تكثيف الجهود لتوعية الأطفال والمراهقين والشباب - فلم يعد استخدام الانترنت يقتصر على فئة عمرية دون أخرى -، وذلك بكيفية الأستخدام الأمن لشبكة الانترنت وأن الحل ليس فى عدم استخدام الانترنت نهائياً كما يفعل بعض الآباء، ولكن بتعليم الأولاد والأطفال منذ الصغر كيفية الأستفادة بالمعلومات والبيانات الهائلة على الشبكة ،وكيف يمكن توظيف طاقاتهم بشكل صحيح، وكيفية إبداء أرائهم بطريقة لائقة، وكيفية قضاء أوقات فراغهم بطريقة أمنة . ولعل هذا الدور يقع على عدة مؤسسات وتأتى الأسرة فى مقدمتها حيث أنها تعد أول وأعمق مؤسسة تقوم بعملية التنشئة الاجتماعية للصغار وبث القيم الايجابية وروح التعاون والمساندة والعطاء والبعد عن القيم السلبية كالحقد والبغض والانانية وحب الذات .

٣- أهمية التوعية الاعلامية عبر وسائل الإعلام التقليدية، وعبر وسائل الاعلام الحديثة بضرورة الإبلاغ فى حالة التعرض لجريمة الكترونية، وتغيير الفكرة السائدة أن الابلاغ عن الجريمة يضر بسمعة الفتاة حتى وإن كانت ضحية لمرتكبها .

٤- ضرورة الإعلان عن حجم جرائم الانترنت والبلاغات المقدمة إلى إدارة مكافحة جرائم الحاسب وشبكات المعلومات بوزارة الداخلية، وإتاحتها للباحثين والمهتمين بهذة القضايا حتى يتسنى وضع الخطط الاجتماعية والثقافية والقانونية والإدارية والتكنولوجية لمكافحتها. مع ضرورة الأعلان عن جهود مباحث الإنترنت فى التوصل إلى مرتكبى هذة الجرائم وتقديمهم للعدالة .

وإنطلاقاً من أهمية دور التوعية بخطورة جرائم الانترنت فقد أنطلقت أحدى الدراسات إلى تقديم رؤية مقترحة من منظور تربوى لتفعيل دور أعضاء هيئة التدريس بكليات التربية لزيادة الوعى بمكافحة الجرائم المعلوماتية، وتوصل البحث إلى إطار مقترح لدور أعضاء هيئة التدريس بكليات التربية من خلال تفاعلهم مع الكيانات التى تشمل وحدات ومراكز ونظم الكلية المختلفة، وأوصى البحث بضرورة الاهتمام بالبرامج التعليمية والتدريبية للتوعية بقضايا امن المعلومات وأهمية التعاون الجاد مع أعضاء هيئة التدريس من مختلف القطاعات للحد من انتشار الجرائم المعلوماتية (أحمد حسنى، ٢٠١٥ : ١٨٤) .

قائمة المصادر

أولاً : المراجع العربية

١- أحمد حسنى صالح متولى : **الجرائم المعلوماتية (٢.٠) – رؤية مقترحة من منظور تربوى لدور أعضاء هيئة التدريس بكليات التربية لزيادة الوعى بمكافحة الجرائم المعلوماتية،** المؤتمر الدولى الأول لمكافحة الجرائم المعلوماتية ICACC ، جامعة الإمام محمد بن سعود الإسلامية ، المملكة العربية السعودية ، ٢٠١٥.

٢- أحمد يوسف وهدان : **تقييم فعاليات المواجهة التشريعية لجرائم الإنترنت،** مجلة الفكر الشرطى، المجلد الثالث عشر ، العدد الأول ، مركز بحوث شرطة الشارقة ،الإمارات العربية المتحدة ، ٢٠٠٤.

٣- أنور حيدر: **سجل اليمن فى أمن المعلومات متدنى،** صنعاء – اليمن ،http://www.felixnews.com/news-21847.html ، ٢٠١٣/١٠/٣٠ .

٤- أيمن الدسوقى : **الوقوف ضد الإخلال بإتفاقيات وتراخيص بعض المواقع،** ندوة جرائم الإنترنت ودور الأجهزة الأمنية للتصدى لها، ندوة نظمتها اللجنة الوطنية للتربية والعلوم والثقافة "يونسكو" بالتعاون مع اللجنة الفنية لبرنامج المعلومات للجميع "ايفاب"، القاهرة، ٤ مارس ٢٠٠٨.

٥- بسمة الشريفى : **قانون جرائم الإنترنت فى الجزائر،** متاح فى موقع زوايا – مغاربية، http://zawaya.magharebia.com/ar/zawaya/opinion,664 ، ٢٠١٣/٣/١١ .

٦- البوابة الرسمية لحكومة دبى : **إحصائيات النفاذ إلى الإنترنت – المواقع التى تم الإبلاغ عنها للحجب،** هيئة تنظيم الاتصالاتtRA، www.dubai.ae/ar/pages/default.aspx ، ٢٠١٣/٣/١١ .

٧- جامعة الدول العربية : **الاتفاقية العربية لمكافحة جرائم تقنية المعلومات،** الأمانة العامة لجامعة الدول العربية، **الشبكة القانونية العربية،** www.arablegalnet.org، ٢٠١٨/٧/١٧.

٨- جعفر حسن جاسم : **جرائم تكنولوجيا المعلومات - رؤية جديدة للجريمة الحديثة،** عمان- الأردن ، الطبعة الأولى، دار البداية للنشر والتوزيع ، ٢٠١٢.

٩- جميل عبد الباقى الصغير : **الجوانب الإجرائية للجرائم المتعلقة بالإنترنت،** القاهرة ، الطبعة الأولى، دار النهضة العربية ، ٢٠٠٢.

١٠- جورج لبكى : **المعاهدات الدولية للإنترنت – حقائق وتحديات،** مجلة الدفاع الوطنى، الموقع الرسمى للجيش اللبنانى، متاح فى http://www.lebarmy-gov.ib/ar/news/?33995، ٢٠١٣/١٠/٣٠ .

١١- حسين بن سعيد الغافرى : **السياسة الجنائية فى مواجهة جرائم الانترنت "دراسة مقارنة"،** رسالة دكتوراة، كلية الحقوق، جامعة عين شمس ، ٢٠٠٧ .

١٢- خالد المختار الفار؛ اسماعيل بابكر محمد : **التحقيق الجنائى فى جرائم الحاسوب (سيكولوجيته – أساليبة القانونية - أدواته العلمية)،** الخرطوم- السودان، الطبعة الأولى، دار عزة للنشر والتوزيع، ٢٠١٠ .

١٣- رانيا حاكم كامل : **جرائم الانترنت فى المجتمع المصرى (دراسة ميدانية بمدينة القاهرة)،** رسالة دكتوراة، كلية البنات جامعة عين شمس ، ٢٠١٦.

١٤- سليمان بن عبد الرزاق الغديان وآخرون : **صور جرائم الابتزاز الإلكترونى ودوافعها والآثار النفسية المترتبة عليها من وجهة نظر المعلمين ورجال الهيئة والمستشاريين النفسيين**، مجلة البحوث الأمنية، العدد (٦٩)، المملكة العربية السعودية ، ٢٠١٨.

١٥- سهير عادل العطار : **الجرائم المستحدثة ضد الأطفال عبر النظم المعلوماتية**، المؤتمر الإقليمى الأول عن الطفل العربى فى ظل المتغيرات المعاصرة ، مركز الدراسات والبحوث المتكاملة، كلية البنات، جامعة عين شمس، ٢٠٠٤ .

١٦- الشبكة العربية لمعلومات حقوق الإنسان :**العراق .. ترحب بسحب مشروع "قانون جرائم المعلوماتية"**، http://www.anhri.net/?p=70284، ٢٠١٣/١٠/٣٠ .

١٧- شمسان ناجى صالح : **الجرائم المستخدمة بطرق غير مشروعة لشبكة الإنترنت – دراسة مقارنة**، القاهرة ، الطبعة الأولى، دار النهضة العربية ، ٢٠٠٩ .

١٨- صباح محمد عبد الكريم : **أخلاقيات مجتمع المعلومات فى عصر الانترنت** ، مجلة مكتبة الملك فهد الوطنية ، مجلد (١٣) ، العدد(١) ، المملكة العربية السعودية ، ٢٠٠٧.

١٩- صحيفة الوسيط البحرينية **: الداخلية تُعلن عن ملاحقة جرائم التشهير والإساءة فى الإنترنت**، العدد (٣٦٥٦)، الأثنين ١٠ سبتمبر ٢٠١٢، http://www.alwasatnews.com/3656/news/read/700371/1.html ، ٢٠١٣/١٠/٣٠ .

٢٠- الصفحة الرسمية للأمم المتحدة : **مؤتمر الأمم المتحدة الثانى عشر لمنع الجريمة والعدالة الجنائية**، سلفادور – البرازيل من ١٢ : ١٩ نيسان ٢٠١٠، متاح فى : http://www.un.org/ar/conf/crimecongress2010/

٢١- الصفحة الرسمية لمديرية الأمن العام بالإردن :**الجرائم المستحدثة**، إدارة البحث الجنائى، المملكة الأردنية الهاشمية، متاح فى:

http://www.cdd.psd.gov.jo/index.php?option=com_content&task=view&id=263 ,

٢٢- الصفحة الرسمية لوزارة الداخلية بدولة الكويت : **تنسيق على أعلى مستوى مع الانتربول**، http://www.moi.gov.kw/portal/vArabic/pressrel.asp

٢٣- عبد الله عبد الله سيف : **الجريمة المنظمة**، رسالة دكتوراة، كلية الحقوق، جامعة القاهرة ، ٢٠٠٣.

٢٤- العربية : **نشر قانون جرائم الإنترنت الإماراتى**، http://www.arabia.com/tech/details/13976

٢٥- على إسماعيل مجاهد : **تطوير أساليب التدريب لتحقيق الأمن الرقمى فى ظل الجريمة المعلوماتية**، ندوة المواجهة الأمنية للجريمة المعلوماتية تحت شعار نحو استخدام أمن لتكنولوجيا المعلومات، مركز بحوث الشرطة، وزارة الداخلية ، جمهورية مصر العربية ، ٢٠٠٩.

٢٦- عمر محمد أبوبكر: **الجرائم الناشئة عن استخدام الانترنت – الأحكام الموضوعية والجوانب الإجرائية**، القاهرة، الطبعة الأولى، دار النهضة العربية ، ٢٠٠٤ .

٢٧- فايز عبد الله الشهرى : **التحديات الأمنية المصاحبة لوسائل الاتصال الجديدة – دراسة الظاهرة الإجرامية على شبكة الإنترنت**، المجلة العربية للدراسات الأمنية والتدريب، المجلد (٢٠) ، العدد (٣٩) ، أكاديمية نايف العربية للعلوم الأمنية، السعودية ، ٢٠٠٥.

٢٨- محمد سعد ابراهيم : **تشريعات الإعلام فى إطار تكنولوجيا الاتصال والمعلومات**، القاهرة ، الطبعة الأولى، دار الكتب العلمية للنشر والتوزيع ، ٢٠٠٨.

٢٩- محمد سعد أحمد : **التشهير على الانترنت وإشكاليات التنظيم القانونى لحرية التعبير (دراسة مقارنة للتشريعات الأمريكية والبريطانية والاسترالية والكندية)** ، المجلة المصرية لبحوث الإعلام، العدد (١٩) ،القاهرة ، كلية الإعلام، جامعة القاهرة ، ٢٠٠٣.

٣٠- محمد عبد المنعم عبد الخالق : **جرائم الإنترنت**، القاهرة ،الطبعة الأولى، دار النهضة العربية ،١٩٩٨.

٣١- محمد عبيد الكعبى : **الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الإنترنت – دراسة مقارنة**، القاهرة ، الطبعة الأولى، دار النهضة العربية ، ٢٠٠٥.

٣٢- محمد فتحى عيد : **الإنترنت ودوره فى انتشار المخدرات**، الرياض، الطبعة الأولى، أكاديمية نايف العربية للعلوم الأمنية ، ٢٠٠٣.

٣٣- محمد محمد الألفى : **المسئولية الجنائية عن الجرائم الأخلاقية عبر الانترنت**، القاهرة ، الطبعة الأولى، المكتب المصرى الحديث ، ٢٠٠٥ .

٣٤- محمود الرشيدى : **الجرائم الإلكترونية والتأمين الإلكترونى**، المركز الدولى للدراسات المستقبلية والإستراتيجية، العدد (١١)، الطبعة الاولى ، ٢٠٠٥.

٣٥- مركز الاستجابة لطوارئ الحاسب الآلى: **تعزيز الوعى حول أمن المعلومات على مستوى الدولة- نحو ثقافة إلكترونية آمنة**،http://www.aecert.ae/about-us-ar.php ، ٢٠١٣/١٠/٣٠ .

٣٦- منال شهاب : **الحملة الوطنية لأمن الإنترنت فى لبنان، الهيئة المنظمة للاتصالات**، ١٥ نيسان ٢٠١٣، بيروت – لبنان، www.tra.gov.ib، ٢٠١٣/١٠/٣٠ .

٣٧- موقع France 24 : **أنونيموس – تونس تحذر الحكومة من قانون قد يعيد الرقابة على الإنترنت**، http://www.france24.com، ٢٠١٣/١٠/٣١ .

٣٨- الموقع الرسمى لوزارة الدفاع بجمهورية السودان : **الجريمة الإلكترونية .. الخطر داخل البيوت**، نشر بتاريخ ٢ نوفمبر ٢٠١٠http://mod.gov.sd/portal/section-blog، ٢٠١٣/١٠/٣٠ .

٣٩- هلالى عبد اللاه أحمد : **جرائم الحاسب والانترنت بين التجريم الجنائى وآليات المواجهة**، القاهرة ، دار النهضة العربية ، ٢٠١٥ .

٤٠- وزارة الداخلية : **تقرير الأمن العام (٢٠٠٣)** ، القاهرة ، مطابع الشرطة للطباعة والنشر والتوزيع .

٤١- وزارة الداخلية : **تقرير الأمن العام (٢٠٠٤)** ، القاهرة ،مطابع الشرطة للطباعة والنشر والتوزيع.

٤٢- وزارة الداخلية : **تقرير الأمن العام (٢٠٠٥)** ، القاهرة ،مطابع الشرطة للطباعة والنشر والتوزيع.

٤٣- وزارة الداخلية : **تقرير الأمن العام (٢٠٠٦)** ، القاهرة ، مطابع الشرطة للطباعة والنشر والتوزيع.

٤٤- وزارة الداخلية : **تقرير الأمن العام (٢٠٠٧)** ، القاهرة ، مطابع الشرطة للطباعة والنشر والتوزيع.

٤٥- وزارة الداخلية : **تقرير الأمن العام (٢٠٠٨)** ، القاهرة ، مطابع الشرطة للطباعة والنشر والتوزيع.

٤٦- وزارة الداخلية : **تقرير الأمن العام (٢٠٠٩)**، القاهرة ، مطابع الشرطة للطباعة والنشر والتوزيع.

٤٧- وزارة الداخلية : **تقرير الأمن العام (٢٠١٠)** ، القاهرة ، مطابع الشرطة للطباعة والنشر والتوزيع.

٤٨- وزارة الداخلية. : **تقرير الأمن العام (٢٠١١)** ، القاهرة ، مطابع الشرطة للطباعة والنشر والتوزيع.

٤٩- وائل إسماعيل عبد البارى : **أسس مجتمع المعلومات العربى – قراءة للأبعاد المعرفية والتقنية فى المجتمع المصرى** ،٢٠٠٢، متاح فى http://www.mafhoum.com/press4/123T44.htm

٥٠- وكالة الأنباء الكويتية (كونا Kuna) ٢٠١٣. خبراء .. القانون الكويتى بحاجة إلى سن تشريعات وقوانين لمكافحة الجرائم الإلكترونية ،- http://www.kuna.net.kw/articleDetails-aspx?id=2300965&language-ar, 28/10/2013.

٥١- يوسف المصرى : **الجرائم المعلوماتية والرقمية للحاسوب والإنترنت**، القاهرة ، الطبعة الأولى، دار العدالة للنشر ، ٢٠١١.

ثانياً :المراجع الإنجليزية

52- A.S.Duff : **Daniel Bell Theory of the Information Society** ، Journal Of Information Science ، 1998، https: //journals.sagepub.com/doi/.

53- Burns, Ronald G.; Whitworth, Keith H ;Thompson, Carol Y: **Assessing law enforcement preparedness to address internet fraud**, Journal of criminal Justice , Vol. (32), N. (5), 2004.

54- Brad Smith : **The Best VPN: Cyber Security Statistics**, Honest, In-Depth & Transparent VPN Reviews from Real Users,2018 https://thebestvpn.com/cyber-security-statistics-2018.

55- **Bell's 'post-industrial society'**, criticisms of his analysis of the role of information and knowledge in relation to contemporary social change and the extent of these changes. (2005) http://samba.fsv.cuni.cz/~soukp6as/OLD/Bell.doc.

56- Cooper, Sharon W ; Estes, Richard J ; Giardino, Angelo p; Kellogg, Nancy D; Vieth, Victor : **Medical, Legal, Social Science aspects of Child**

sexual exploitation –A comprehensive review of pornography, prostitution, and internet crime, GW Medical publishing , Vol (1) , United Kingdom, 2005.

57- Center For Strategic And International Studies : **The Economic Impact Of Cyber Crime And Cyber Espionage** , Report International, Mc afee An Intel Company, 2013.

58- Center For Cyber Victim Counselling : **"Helping Cyber Crime Vicitims"**, www.cyber victims.org , 18/10/2013.

59- Cullen, Thomas : **keeping children safe – OJJDP'S child protection Division**, Office of Juvenile Justice and Delinquency prevention, Juvenile Justice clearing house publisher, Washington, 2001, Retrieved from http://www.ojjdp.ncjrs.org.

60- Daniel Bolotsky: **Daniel Bell** , Encyclopaedia Britannica , http: // Britannica.com ,2018 .

61- D.A.Akopyan and A.D.Yelyakov: **Cybercrimes in the Information Structure of society: a Survey**, Scientific and Technical Information Processing, Allerton Press , Vol. (36), N. (6 (, 2009.

62- David L. speer : **Redefining borders – the challenges of cyber crime, crime**, Law & Social change, Vol. (34), Kluwer Academic publisher, Netherlands , 2000.

63- FBI National Press Office : **FBI Releases The IC3 2017 Internet Crime Report and Calls for Increased Public Awareness**, Washington,2018,https://www.fbi.gov/news/pressrel/press-releases/fbi-releases-the-ic3-2017-internet-crime-report-and-calls-for-increased-public-awareness.

64- Frank Webster : **What Information Society**? , The Information Society, Vol. 10(1), http://www.artefaktum.hu/it/Webster.htm.

65- Fausto Pocar : **New challenges for international rules against cyber crime**, European Journal on Criminal policy and Research ,Kluwer Academic Publishers, Netherlands, 2004.

66- John Herhalt : **Cyber Crime - A growing challenge for Governments**, Issues Monitor, Volume Eight, KPMG International , 2011.

67- Liang Bin and Lu,Hong : **Internet development ,censorship ,and cyber crime in china** , Journal of contemporary criminal Justice , Vol. 26(1), N. (2 (, 2010

68- Marco Gercke : **Europé's Legal approaches to cyber crime**, ERA Forum published , Germany, 2009.

69- Min Jae Lee and Jinkyu lee : **The Impact Of Information Security Failure On Customer Behaviors - A Study On a Large - scale Hacking Incident On The Internet** , Springer Science &Business Media, 2010.

70- Nhan, Johnny : **Policing cyber space – the compatibility of the internet with traditional forms of law enforcement, law and policy**, Humanities and social sciences, Vol. (69), N . (7-A), 2009.

71- Peter Grabosky : **Requirements Of Prosecution Services To Deal With Cyber Crime**, Crime Law Soc Change, No. (47) , Springer Science And Business Media, Australia, 2007.

72- Ponemon Institute : **Cost Of Cyber Crime Study**, Research Report, United State, 2012.

73- Rohini Tendulkar : **Cyber Crime, Securities Markets And Systemic Risk, Survey World Federation Of Exchanges Office**, world federation of exchanges , 2013.

74- Steve Morgan : **2017 Cyber crime Report**, Cyber Security Ventures, HERJAVEC GROUP, 2017.

75- Susan J. Drucker : **Cyber crime and punishment**, Critical Studies in Media communication, Vol. (17), N. (2), 2000.

76- Sylvia Kierkeygaard : **Cybercrime convention: narrowing the cultural and privacy gap ?,** Intercultural information Management, Vol. (1), No. (1), Inderscience Enterprises Ltd, 2007 .

77- Wilson, David L : **Senate Approves Measure Making obscenity on the internet a crime**, chronicle of Higher Education ,Vol. (41), N. (41) , 1995.

78- Yar, Majid: **the private policing of internet crime**, Handbook of internet crime, Willan Publishing, United Kingdom , 2010 .

Mechanisms of Countering the Internet Crimes Between Theoretical Concepts and Practical Applications

By

Dr. Rania Hakim Camille

Lecturer, Department of Sociology, Girls College Ain-Shams University

ABSTRACT :

This present study purpose is to: discuss and analyze the mechanisms of "countering and combating the internet crimes" on the overall three levels, the global, Arab, and local level; shedding light on the definition of the internet crimes, their evolution history, and risks on victims. The study comes to several results that: A- there is no specific deal or agreement between the European and the Arab states to set a specific label or name for a crime that occurs with the information technology and communication setting. B- There is a remarkable legislative gap or shortness in so many of the world's states that cripple countering the internet crimes. C- Finally, the study indicates that since tragic outcomes of such crimes of the internet are not limited on one state but extends to affect others, becoming as an epidemic that should be removed by a world activity and motion.

Keywords: Countering the internet crimes – Information Society – world states – Arab states – Egyptian Community.