نحو قانون دولي موحد لمكافحة الجرائم المعلوماتية

الدكتور/ حسن بن أحمد الشهري[1][1]

مستخلص الدراسة:

من اهم إنجازات العلم الحديث في هذا العصر واعظمها جدوى للانسان ظهور الحاسب الآلي والإنترنت، اللذين قدما خدماتهما للانسانية في أغلب مناحي الحياة الاقتصادية والتعليمية والطبية والعديد من المجالات الأخرى. ولكن رافق هذه الانجازات بروز خبراء جدد لم تعهدهم الانسانية من قبل ، يتمتعون بالخبرة والحرفية في تطويع هذه التقنية للقيام بأعمال إجراميةافرزت إلى جانب الجريمة التقليدية الجرائم المعاصرة، بل حولت هذه الجريمة من صفتها العادية وأبعادها المحدودة إلى أبعاد جديدة تعتمد التقنية في تنفيذ الفعل المجّرم وبأساليب مبتكرة وطرق جديدة لم تكن معروفة من قبل. وساعد هؤلاء المجرمين ما يشهده العصر من تطور الوسائل المعلوماتية الحديثة، في زيادة سرعة نشر جرائمهم حتى أصبحت تهدد النظام المعلوماتي، بل أصبح في إمكانهم التسبب في خلق شلل كامل للأنظمة المدنية والعسكرية، الأرضية والفضائية، وتعطيل المعدات الإلكترونية ، واختراق النظم المصرفية، وإرباك حركة الطيران وشل محطات الطاقة وغيرها بواسطة قنابل معلوماتية ترسلها لوحة مفاتيح الكمبيوتر من على مسافات تتعدى عشرات الآلاف من الأميال (1).

وهذه الأعمال الإجرامية لفتت أنظار الدول والهيئات الدولية التي أدركت خطورتها وسهولة ارتكابها وتأثيرها المباشر ، لتجعل مكافحتها من أولى أولويات المجتمع الدولي والحكومات مما حتم أهمية الحماية القانونية لمواجهة هذه الأفعال الإجرامية، وانبرت العديد من دول العالم في إصدار التشريعات والأنظمة لمكافحة هذه الجريمة (7) . وبخلاف ما يتصوره الكثير من الباحثين والمختصين في مجال مكافحة الجريمة المعلوماتية، فإن ظاهرة انتشار التشريعات والقوانين للحد من هذه الآفة أخذت في الإزدياد في الكثير من دول العالم .

وأغلب هذه القوانين لم تأخذ في الاعتبار عند أنشائها أن الجريمة السيبرانية تنشأ في بلد ليحدث أثرها في بلد آخر، وأدلتها منتشرة عبر بلدان أخرى، فأي قانون يحكم هذه الجريمة؟

سيقوم الباحث في هذه الورقة – نحوقانون دولي موحد لمكافحة الجرائم المعلوماتية – المقدمة إلى مؤتمر التنظيم القانوني للإنترنت والجريمة الإلكترونية المقام في جامعة الجلفة بكلية الحقوق والعلوم السياسية في الجمهورية الجزائرية الديمقراطية الشعبية، بدراسة

[1][1] **الدكتور حسن بن أحمد الشهري، وكيل مركز الدراسات والبحوث ، جامعة نايف العربية للعلوم الأمنية**

وتحليل عدد من الأنظمة الدولية لمكافحة الجرائم المعلوماتية لدولتين من دول العالم، لإستنتاج درجة التشابة والاختلاف وإمكانية مزجها في نظام موحد، بعدها سيقدم الباحث مقترحا يوصي بقيام الأمم المتحدة ممثلة في جهاز الأنتربول الدولي بدراسة وتحليل جميع الأنظمة الدولية التي أصدرتها دول العالم في مكافحة الجريمة الإلكترونية والخروج بنظام دولي موحد يمكن تطبيقه على هذه الجرائم في أي دولة عضو في هيئة الأمم المتحدة.

مقدمة:

دخلت البشرية عصر المعلومات منذ عقود قليلة، ومن أهم معالم هذا العصر انتشار الحواسيب الشخصية منذ ثمانينيات القرن العشرين، ثم شبكة الويب العالمية خلال التسعينيات، واليوم تعتمد معظم قطاعات الاقتصاد والمجتمع على تقنيات المعلومات والاتصالات على نحو لم يسبق له مثيل (8).

ولقد أضحى من الصعوبة بمكان الاستغناء عن خدماتهما اللامحدودة وكطبيعة النفس البشرية استغلت الشريرة منها هذه المخترعات لارتكاب العديد من الجرائم المرتبطة بهذه التقنيات وتزايدت معدلات هذه الجرائم في العقدين الأخيرين على وجه الخصوص بصورة أدت إلى بزوغ ظاهرة إجرامية جديدة تعرف بالإجرام المعلوماتي أو الإجرام الإلكتروني. واقع الأمر اثبت أن زيادة نسبة هذه الجرائم وتنوع أساليبها وتعدد اتجاهاتها زاد من أخطارها على الأمن القومي للدول مما يستدعي التعامل معها جماعيا لا فرديا(9).

وبخلاف تصور العديد من الكتاب والباحثين في مجال الجريمة الإلكترونية، فإن ظاهرة انتشار التشريعات والقوانين الوطنية للحد منها آخذة في الازدياد في الكثير من دول العالم. ولعل أبرز العوائق التي تواجه الحد من انتشار هذه الجريمة ضعف التعاون الدولي لمواجهة هذه الجرائم والاكتفاء بسن قوانين وطنية محلية ، يقتصر أثرها في داخل حدودها ، ولأهمية هذا الموضوع والحاجة إلى معرفة إمكانية سن قانون دولي يحاربها على المستوى الدولي ، فقد تم إعداد هذا البحث الذي سيلقي الضوء على بعض التشريعات الوطنية المتعلقة بالجرائم المعلوماتية وإبراز قصورها في تطبيق أنظمتها خارج حدودها وضعف تبادل المعلومات بشأنها.

مشكلة الدراسة:

تعد وسائل التقنية الحديثة من أهم ما أفرزته الثورة المعلوماتية في الزمن الحاضر ، والتي تزايد الاعتماد عليها في كافة مجالات الحياة ، مما جعلها عرضة لارتكاب الجرائم التي تقع عليها مباشرة ، أو

ترتكب من خلالها واستخدامها كبيئة لارتكاب الجرائم. ولخصوصية هذه الجريمة وتميزها ظهرت الحاجة لسن تشريعات وقوانين لمعاقبة مرتكبيها ، إلا أنه برز وبشكل واضح قصور الأنظمة والتشريعات الوطنية لمحدودية نطاق تطبيقها بإعتبارها محلية لا أثر لها خارج حدودها ، وبرزت الحاجة لسن تشريع إليكتروني عالمي وشامل يواكب تطور هذه الجريمة ويتناسب مع طبيعتها ويحيط بكافة أبعادها.

التساؤل الرئيس للدراسة:

تتبلور مشكلة الدراسة في السؤال الرئيس التالي: ما مدى توافق الأنظمة والتشريعات والقوانين الوطنية لمكافحة الجريمة الإلكترونية ومدى تطبيقها خارج حدودها. وتفرع عنه سؤال فرعي : ما اهمية ايجاد بدائل اخرى للحد من هذه الجريمه .

أهمية الدراسة:

تتمثل أهمية الدراسة في أنها تتصل بموضوع ذي درجة عالية من الأهمية نتج من التوسع الكبير في استخدام الشبكة العنكبوتية التي ازداد مستخدموها حيث وصل تعدادهم ما يقارب المليار وستمائة مليون مستخدم(11). وأصبحت هذه الوسيلة وسطا ملائما لارتكاب أنواع الجرائم السيبرانية الحديثة التي لم تكن معروفة للبشرية قبل اختراع هذه التقنية ، لقد تنوعت جرائمها وأثرت على جل جوانب الحياة. حيث بلغ الضرر درجة لايمكن تجاهله وأصبحت ظاهره معروفة دعت على إثرها العديد من دول العالم إلى سن قوانين وأنظمة وتشريعات لمكافحة الجريمة المعلوماتية، وقد صممت هذه القوانين لتخدم كل دولة على حده ويتم تطبيقها داخل حدودها، برغم معرفة طبيعة هذه الجريمة التي لا وطن ولا حدود لها ، فالجاني يرتكبها في بلد والمجني عليه في بلد آخر وأركان الجريمة منتشرة في بلدان أخرى(4) . لقد أنحصر تطبيق هذه القوانين كقوانين محليه لا أثر ولا فائدة لها خارج حدودها . وبحكم قوة ذكاء المجرم الإلكتروني ومعرفته لهذه القوانين التي اعطته خيارات متعددة لارتكاب جريمته في دولة لا قوانين لمكافحة هذه الجريمة فيها أو دولة تتسم عقوباتها بالتخفيف. فقد عقد الكثير من المؤتمرات والندوات ونشر العديد من الأبحاث نوقشت فيها هذه الظاهرة محاولة الاجابه على العديد من التساؤلات المعقدة للبحث عن حلول للقضاء على هذه الجريمة. والباحث لا يميل إلى ترك ايجاد حلول جذرية لها للصدفة للبحث والباحثين، وعلى حد علمه فإنه لا يوجد قانون دولي لمكافحة هذه الآفة ، لذا فان الوقت قد حان للتخطيط لمؤتمر دولي يقترح الآليات والوسائل التي تجيب على التساؤلات المطروحة و لربما يجد الحلول المناسبة وإيجاد تشريع دولي موحد لمواجهة هذه الجرائم وهو ما سيتم إيضاحه من خلال هذا البحث.

أهداف الدراسة:

1: تحليل ووصف بعض قوانين الجريمة الإلكترونية الوطنية، في عدد من بلدان العالم المختلفة.

2: اقتراح توحيد هذه الأنظمة وإعادة صياغتها والتنسيق فيما بينها ، ليشمل تطبيقها على المجرم الإلكتروني في أي بلد يرتكب جريمته فيها.

منهجية الدراسة:

المنهج المتبع في هذا البحث، هو المنهج الوصفي الذي يقوم على تحليل المضمون والمقارنة ، حيث سيتم وصف لبعض القوانين الوطنية لمكافحة الجريمة الإلكترونية التي تم جمعها وتلخيصها ثم يصار إلى تحليل مضمونها ومقارنتها وابرز ألفوارق بينها لمعرفة مدى قصورها في معاقبة المجرم الإلكتروني.

أدبيات الدراسة:

تعريف الجريمة الإلكترونية:

الجريمة المعلوماتية هي : كل عمل أو امتناع يأتيه الأنسأن ويحدث أضرارا بمكونات الحاسب المادية والمعنوية وشبكات الاتصال الخاصة به (10).

وتعرف كذلك على انها كل فعل أو امتناع عمدي ينشأ عن الاستخدام غير المشروع للتقنية المعلوماتية ويهدف إلى الاعتداء على الأموال المادية أو المعنوية (6).

ويعرفه المرشد الفيدرالي الأمريكي منتهك الحاسوب أنه : الشخص الذي يخترق حاسوبا محميا (مشمول بالحماية) دون أن يكون مصرحا له بذلك (2).

أما تعريف الأمم المتحدة فيقول المحامي محمد أمين الشوابكة إنها أي جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية أو داخل نظام حاسوبي، وتشمل تلك الجريمة من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في بيئة إليكترونية(10) .

أسماء الجريمة الإلكترونية:

الاحتيال المعلوماتي ، الغش المعلوماتي ، التعسف في استعمال الحاسب الآلي ، الجرائم المرتبطة بالحاسب الآلي ، جرائم الحاسب الآلي ، جرائم المعلوماتية ، احتيال الكمبيوتر ، جرائم التقنية العالية، جرائم الهاكرز ، الاختراقات ، جرائم الإنترنت ، جرائم الحاسب والإنترنت ، الجرائم الاقتصادية المرتبطة بالكمبيوتر ، السيبر كرايم ، جرائم أصحاب الياقات البيضاء(7).

أقسام الجريمة الإلكترونية:

قسمها (ابوبكر،2007) إلى ثلاثة أقسام:

جرائم تستهدف النظم والمعلومات كهدف

جرائم تستخدم الكمبيوتر وسيلة لارتكاب الجريمة

جرائم تتعلق بمحتوى مواقع المعلوماتية وبيئتها.

أشكال وأنماط الجريمة الإلكترونية :

الإرهاب الإلكتروني يتمثل في اتخاذ الجماعات الإرهابية مواقع لها على الإنترنت لتمارس أعمالها كالتحريض على القتل وتعليم صنع القنابل والمتفجرات ونشر الأفكار الإرهابية.

تدمير اقتصاديات المؤسسات التجارية ومؤسسات الدول والمجتمعات .

الجرائم الدولية المنظمة .

تدمير وتعطيل القواعد الأمنية للبيانات.

جرائم غسل الأموال .

الاستغلال الجنسي للنساء والأطفال.

جرائم القذف والسب والكذب والتعدي وتشويه السمعة.

الاعتداء على حقوق المؤلفين ونسخ البرامج من الإنترنت وبيعها في السوق السوداء.

جرائم التعدي على المؤسسات المصرفية وتخريب الحسابات وتحويل الأموال من حساب لآخر.

سرقة أرقام البطاقات الائتمانية وبث ألفساد في التجارة الإلكترونية.

إنشاء مواقع إباحية والترويج للإباحية الجنسية من خلال نشر الصور والأفلام الهابطة(13).

خصائص الجريمة الإلكترونية:

من خصائص هذه الجريمة أنها ليست عادية أو تقليدية ترتكب بصورة عشوائية أو غير مدروسة.

إنها جريمة تنفذ بواسطة خبراء على درجة عالية من التخصص والكفاءة في استخدام الحاسب الآلي والإنترنت وسعة الأفق والحيلة . يتمتع هؤلاء الخبراء بمكانة اجتماعية ولديهم قدر من العلم والتقنية التكنولوجية ومهارات ومعارف فنية في مجال الكمبيوتر والإنترنت وكيفية التعامل معهما بحرفية عالية، مما يدعو إلى القول بإن مرتكبي هذه الجرائم غالبا ما يكونون من المتخصصين في مجال الحاسب والمعلومات (4).

من خصائصها أيضا أنها من الجرائم السيبرانية التي تنشأ في بلد وأثرها في بلد آخر وأدلتها منتشرة عبر بلدان أخرى.

إنها أشد تأثيرا وأوسع انتشارا وأكثر تنوعا.

سهولة تخلص المجرم الإلكتروني من أدلتها الرقمية المستخدمة في الجريمة.

تدخل في أغلب أنواع الجرائم التقليدية (10).

أركان الجريمة الإلكترونية:

الركن المعنوي:

الاعتداء على المعلومات الخاصة بالمنظمات الحكومية أو الخاصة أو المملوكة للأفراد بقصد إتلافها كليا أو جزئيا أو تقليل منفعتها مما يؤدي إلى إلحاق الضرر بمالكي المعلومات وتعتبر من الجرائم العمدية في حالة تحقق عنصري العلم بملكيتها للغير والإرادة في تدميرها مما له الأثر السلبي في تنفيذ أنشطة المنظمة جزئيا أو كليا (3).

يقسم الشوابكة الركن المعنوي إلى محورين هما:

1: الاعتداء على نظام تشغيل بخلق مشكله تؤدي إلى تباطؤ النظام في تنفيذ العمليات المطلوبة مثل معالجة المعلومات واسترجاعها وإرسالها، مما يكون له الأثر السلبي على أداء المنظمة.

2: الدخول غير المرخص إلى أنظمة المنظمة الإلكترونية ، ويتم في هذه الحالة تدمير البيانات والمعلومات كليا والموجودة في النظام أو التعديل والتشويه للبيانات والمعلومات مما يكون عائقا أمام المنظمة للاستمرار في تنفيذ عملياتها أو الحد من اتخاذ القرارات السليمة (قشقوش،1992).

وتذكر(قوره ، 2005) أن الاعتداء على المعلومات من جرائم النصب ومن الجرائم العمدية ويكون الركن المعنوي في هذا النوع من الجرائم القصد الجنائي الذي يجب أن يتحقق في الجريمة(5).

الركن المادي:

يتعلق بالإتلاف الجزئي أو الكلي للجانب المادي من نظم المعلومات الذي يفقده القدرة على تأدية أعمال المنظمة ومن ثم لا يحقق المنفعة التي أوجد من أجلها هذا النظام الإلكتروني (9).

الركن القانوني:

اهتمت الشريعة الإسلامية والقوانين الوضعية بحماية الحقوق الخاصة بالأفراد والمجتمعات . ويتميز هذا العصر بالسرعة المذهلة في تطور تقنية المعلومات واعتماد جل المجالات عليها وبما تحققه للفرد والمجتمع من توفير للوقت والسرعة في أنجاز الأعمال. أن هذه المميزات

فرضت على كافة مكونات المجتمع من أفراد ومنظمات عامة وخاصة استخدام تلك التقنية . ويذكر (Cate ,1997)

أن الاستفادة من الشبكة العالمية للمعلومات والتقنية المصاحبة لها من الحاسبات والشبكات الأخرى أصبحت عرضه للاعتداءات. ويذكر (الشوابكة ، 2004) أن النصوص التقليدية تقف عاجزة أمام هذه الاعتداءات على الخصوصيات ألفردية وأسرارهم . لذا فإن الحاجة تغدو ملحة لسد فراغ تشريعي في حماية ما يتم تداوله من معلومات وأسرار على هذه الشبكة ، ولحماية الاتصالات والمراسلات بين الناس(19).

خسائر الجريمة الإلكترونية:

في عام 2007 ارتكبت جريمة إليكترونية في بريطانيا كل عشر ثوان ، وبلغت جرائم التحرش بالأطفال والنساء فيها أكثر من 850 ألف حاله ، وأكثر من 92 ألف حالة سرقه للهوية الوطنية ، و145 ألف حالة اختراق لأجهزة حواسب وسرقة معلوماتها ، وسجلت كذلك 207 ألف حالة سطو على الأموال من خلال سرقة أرقام البطاقات الائتمانية (2).

وفي دراسة لرئيس المجمع العربي للملكية الفردية أن الجرائم الإلكترونية باتت تشكل تحديا كبيرا للاقتصاد العالمي ، حيث يشهد العالم جريمة إليكترونية كل ثلاث دقائق للملكية الفكرية ، وتجاوزت خسائرها أكثر من 48ألف مليار دولار (13).

وفي الإمارات العربية المتحدة تم التحقيق في 222 قضية قرصنة إلكترونية (14) .

وفي الولايات المتحدة الأمريكية أعلنت السلطات الاتحادية الأمريكية تزايد جرائم الاحتيال عبر الإنترنت بنسبة 33% في عام 2008 عنه في العام الذي قبله ، وبحسب التقارير فإن العام 2009 يتجه لأن يكون عاما مزدحما في مجال الجريمة الإلكترونية(16) .

معاهدات واتفاقيات ودعوات لمكافحة الجرائم المعلوماتيه:

دعى خبراء جزائريين الى نشوء تعاون دولي وثيق لمحاربة الجريمة المعلوماتية ورأى هؤلاء الخبراء أن ظاهرة الإجرام المعلوماتي تقتضي محاربة فعالة لهذه الجريمة، وأشار المدير العام للمدرسة الجزائرية العليا للقضاء أن التشريع الدولي في مجال الجريمة المعلوماتية سائرا نحو مزيدا من التعزيز مشرا إلى عدة دول مثل كندا وأمريكا وكوريا واليابان وجنوب أفريقيا إنضمت إلى الإتفاقية الدولية لمجلس أوروبا وأضاف أن هذه الدول إستلهمت من هذه الإتفاقية لوضع تشريعها الوطني الخاص بها لمواجهة الجريمة المعلوماتية وأضاف أن الجزائر بصدد التحضير لمشروع قانون خاص بمحاربة الجريمة المعلوماتية. واقترح ضرورة توحيد التشريعات الخاصة بالجريمة المعلوماتية (18).

دعا مؤتمر مكافحة الجرائم الإلكترونية لدول مجلس التعاون الخليجي إلى عقد معاهدة على مستوى المجلس على غرار الإتفاقية الأوروبية للجريمة الإلكترونية تشكل نواة لمعاهدة عربية في مجال مكافحة الجريمة الإلكترونية (19).

تعد إتفاقية مجلس أوروبا –الذي يشرف على الكثير من المعاهدات القانونية– أول معاهدة دولية حول الجرائم المرتكبة بواسطة شبكة الإنترنت والذي يعود تاريخها إلى عام 2001 . الموافقة على هذه الإتفاقية جزئية واختيارية انضم إليها من خارج أوروبا كندا وأمريكا وكوريا واليابان وجنوب أفريقيا (20).

يأمل الإتحاد الدولي للإتصالات الدولية الذي يضم جميع دول العالم التي تستخدم نظام الهاتف العالمي في أن يأخذ زمام المبادرة للمطالبة بمعاهدة عالمية ضد الجريمة الإلكترونية (20).

التشريعات الوطنية لمكافحة الجريمة الإلكترونية

اعتبر القانون الوضعي في بعض دول العالم التعدي على الآخرين وعلى الممتلكات العامة والأنظمة بواسطة استخدام الوسائل التقنية جريمة يعاقب عليها فاعلها، لما في ذلك من إخلال بالأمن بمختلف مستوياته، من أمن الفرد وأمن المجتمع وأمن الدولة بل الأمن العالمي(3).

فيما يلي بعض مواد عدد من القوانين والتشريعات الوطنية لمكافحة الجريمة الإلكترونية :

1:الولايات المتحدة الأمريكية: أصدرت الولايات المتحدة تشريعات لمكافحة الجريمة الإلكترونية عام 1973 هذا النظام يسمح للأشخاص أو المؤسسات التي تم الاعتداء علي حواسبهم بتفويض السلطات لمراقبة تحرك المعتدين وبالتالي تتولى السلطة متابعة اتصالات المعتدي التي يبثها إلى تلك الأجهزة المحمية وعند طلب التفتيش لابد من توافر الآتي:

1: تخويل كتابي من المعتدى عليه.

2: يجب أن يكون المراقب لتلك الاتصالات عضوا في لجنة التحقيق.

3: يجب أن تتوافر لدى مراقب الاتصالات المعرفة لمراقبة الاتصالات التي لها علاقة بالجريمة.

4: مراقبة اتصالات منتهك الحاسوب الخاصة بالجريمة فقط وقدر الإمكان. (يونس، 2004).

عندما يسفر التحقيق عن وجود الدليل الإلكتروني خارج حدود الولايات المتحدة فإن الولايات المتحدة تسعى للحصول على الدليل من الدول على النحو التالي:

1: موافقة الدولة الأجنبية.

2: موافقة مكتب الشئون الدولية مع وزارة العدل(1).

أستراليا

سنت أستراليا قوانين لمكافحة الجريمة الإلكترونية لحماية تدفق المعلومات عبر الشبكة العالمية وحددت الجرائم الإلكترونية بواسطة المشرع ومنها أن الشخص الذي يدخل لأنظمة الحاسب الآلي من غير إذن شرعي ويتمكن من الوصول إلى البيانات الموجودة في الحاسبات الخاصة بدول الكومنولث أو البيانات الخاصة بدول الكومنولث ومخزنه في حاسبات أخرى لا تنتمي لهذه الدول يعتبر هذا الشخص متهما ومنتهكا للقوانين ويستحق عقوبة السجن لمدة ستة أشهر إلى جانب مواد أخرى(2).

كندا

ينص نظام مكافحة الجريمة المعلوماتية الكندي على أن أي فرد يحتال وبدون وجه حق على الحصول على خدمات الحاسب الآلي بواسطة أدوات إلكترومغناطيسية أو سمعية أو ميكانيكية أو أي أدوات تعترض أو تسبب خللا لوظائف نظام الحاسب أو استخدام رقم سري لشخص آخر، فإنه يعتبر مدانا ويستحق عقوبة السجن لمدة لا تتعدى عشر سنوات (2).

الصين

أصدرت الصين أنظمة حماية أمن المعلومات وتشمل معاقبة الشخص بمبلغ 5000 ين عند استخدامه الفيروسات لتدمير المعلومات أو قام بالتأثير على نظام المعلومات أو باع أنظمة معلومات بدون ترخيص (1).

هونج كونج

يعاقب من يصل للمعلومات المخزنة بالحاسب الآلي من غير إذن شرعي بدفع غرامة قدرها 20000 دولار أمريكي ، وبالسجن خمس سنوات لمن يتسبب في خسارة الآخرين وحصوله على دخل غير شرعي(2).

الدنمارك

سنت القوانين الدنماركية قانون مكافحة الجريمة الذي ينص على الغرامة والسجن لمده تصل ستة أشهر لأي شخص يدخل على المعلومات الآلية بدون إذن شرعي (11).

فرنسا

ينص نظام مكافحة الجريمة المعلوماتية في فرنسا على معاقبة أي شخص لقيامه بنشاط من شأنه التحايل على النظام الآلي بالسجن لمدة تصل إلى سنه وغرامة تصل 100000 فرنك فرنسي (1).

ألمانيا

ينص القانون الألماني الخاص بأنظمة المعلومات على معاقبة أي شخص يدخل للنظام الآلي بدون إذن بالغرامة والسجن لمدة لا تتجاوز ثلاث سنوات وبخمس سنوات سجن إذا كانت الضحية من قطاع الأعمال والشركات(2).

أيرلندا

يعاقب منتهك الأنظمة المعلوماتية بدون إذن بغرامة 500 جنيه أو السجن لمدة لا تتجاوز ثلاثة أشهر(1).

الهند

ينص نظام الاعتداء على أنظمة المعلومات بالسجن لمدة تصل إلى ثلاث سنوات وبغرامة لا تتعدى 20000 روبية أو بهما معا (11).

اليابان

يعاقب منتهك أنظمة المعلومات بغرامه تصل 50000 ين أو السجن خمس سنوات كحد أقصى (Lilley,2002)، كما صدرت تشريعات مشابهة في كل من أيسلندا ولكسمبورغ و مالطا والنرويج وبولندا والبرتغال و سنغافورة وجنوب أفريقيا واسبانيا وسويسرا وتركيا (الماكب) . وبلجيكا واستونيا وفنلندا و المانيا واليونان(1).

أما الدول العربية بشكل عام وبحكم تأخرها في مجالات التقنية فلقد إتسمت الاتفاقيات والمعاهدات في هذه الدول بأنها فضفاضة و بقصورها الشديد ولم تعط الجريمة الإلكترونية ما تستحقه من اهتمام وبقيت عاجزة عن مواجهة خطر جرائم الكمبيوتر والمعلومات.

برزت دول الخليج العربي بشكل خاص بالتصدي لهذه الجريمة بسن التشريعات والقوانين ، فأصدرت عمان أول قانون عربي يتطرق لمواجهة هذه الجرائم، تبعتها دولة الإمارات العربية المتحدة ثم المملكة العربية السعودية. جميع هذه القوانين مختصة في مكافحة جرائم المعلومات، وتعد هذه القوانين نموذجية حيث تطرقت إلى غالبية الجرائم المعلوماتية ، وتعتبر أول ثلاثة قوانين عربية تصدر بشكل مستقل لمواجهة الجرائم المعلوماتية(17).

التحليل و المقارنه:

بدراسة وتحليل هذه المواد من التشريعات السابقة والخاصة بمكافحة الجريمة الإلكترونية، لاحظ الباحث وجود تناقض بين هذه التشريعات من دولة لأخرى. فقوانين الدنمارك تنص على الغرامة والسجن لمدة تصل إلى ستة اشهر لمنتهك أنظمة المعلومات بدون إذن شرعي،

بينما تعاقب قوانين مكافحة الجريمة الإلكترونية في أيرلندا منتهك أنظمة المعلومات بدون إذن بغرامة ماليه قدرها 500 جنيه أو السجن لمدة لا تتجاوز ثلاثة اشهر، وفي اليابان يعاقب منتهك أنظمة المعلومات بغرامة تصل 5000 ين أو السجن خمس سنوات، وفي هونج كونج يعاقب من يصل للمعلومات المخزنة بالحاسب الآلي من غير إذن بدفع غرامة وقدرها 20000 دولار أمريكي ، والسجن خمس سنوات . وفي أستراليا سنت قوانين لمكافحة الجريمة الإلكترونية لحماية المعلومات عبر الشبكة ، وعاقبت منتهك أنظمة المعلومات من غير إذن بالسجن لمدة ستة اشهر . وينص نظام مكافحة الجريمة المعلوماتية الكندي على معاقبة منتهك أنظمة المعلومات بعقوبة السجن لمدة لا تتعدى عشر سنوات . أما نظام مكافحة الجريمة الإلكترونية ألفرنسي فيعاقب من قام بالتحايل على أنظمة المعلومات بالسجن لمدة تصل للسنة وغرامة قدرها 100000 فرنك فرنسي . وفي القانون الألماني الخاص بأنظمة المعلومات يعاقب بالسجن منتهك النظام المعلوماتي بدون إذن بالغرامة والسجن لمدة لا تتجاوز ثلاث سنوات وبخمس سنوات إذا كانت الضحية من قطاع الأعمال والشركات.

وفي الهند ينص نظام ألاعتداء على أنظمة المعلومات بالسجن لمدة تصل إلى ثلاث سنوات ، وبغرامة لا تتعدى 20000 روبية أوبهما معا. مثل هذه التناقضات وجدت في قوانين دول أخرى مثل اليونان ، وجنوب أفريقيا ، و سنغافورة واسبانيا وسويسرا والنرويج وبولندا والبرتغال. وتنص الماده الخامسه من نظام مكافحة الجرائم المعلوماتيه في المملكه العربيه السعوديه على أنه يعاقب بالسجن مدة لاتزيد على اربع سنوات وبغرامة لاتزيد على ثلاثة ملايين ريال اوباحدى هاتين العقوبتين لكل شخص يرتكب الجريمه المعلوماتيه التاليه:

الدخول غير المشروع لالغاء بيانات خاصه اوحذفها او تدميرها اوتسريبها، او اتلافها او تغييرها اواعادة نشرها.

اما الماده الثانيه من نظام مكافحة الجرائم المعلوماتيه لدولة الامارات العربيه المتحده ، فينص على ان كل فعل عمدي يتوصل فيه بغير وجه حق الى موقع اونظام معلوماتي سواء بدخول الموقع او النظام ، يعاقب بالسجن والغرامه اوبهما معا ، فاذا ترتب على الفعل الغاء اوحذف اوتدمير او افشاء او اتلاف او تغيير او اعادة نشر بيانات او معلومات فيعاقب بالحبس مدة لاتقل عن ستة اشهر وبالغرامه او بإحدى هاتين العقوبتين (17).

النتائج والتوصيات

بعد التحليل و المقارنة لبعض مواد قوانين الجرائم الإلكترونية لعدد من دول العالم تم التوصل للنتائج التالية:

أولا: النتائج

التشريعات الوطنية السابقة تمت عن طريق الإضافة أو التعديل لقوانينها القائمة، هدفت منه إلى مواجهة جرائم لم يعهدها المشرعون القدامى ، مشرعو هذا العصر وخصوصا في مجتمع الدول المتقدمة نشأوا في بيئة متقدمة وتعاملوا معها وتأثروا بما أفرزه العصر من تقدم في جميع المجالات ومنها تقنية المعلومات والاتصالات، وما أفرزته من سلبيات سببت أضرارا وخسائر جسيمه . سن هؤلاء المشرعون أنظمة وطنية تخدم كل دولة على حدة لا علاقة لها بما يدور في الدول المجاورة برغم أن هذه الجريمة لا يحدها حدود ولا يمنع من أن يكون المجرم في بلد وضحيته في بلد مجاور لا يبعد عنه إلا مسافة قصيرة ولكنه يعرف تماما أنه لن يطبق عليه إلا نظام بلده. أما الدول العربية بشكل عام وبحكم تأخرها في مجالات التقنية فلقد إتسمت الاتفاقيات والمعاهدات في هذه الدول بأنها فضفاضة و بقصورها الشديد ولم تعط الجريمة الإلكترونية ما تستحقه من اهتمام وبقيت عاجزة عن مواجهة خطر جرائم الكمبيوتر والمعلومات.

برزت دول الخليج العربي بشكل خاص بالتصدي لهذه الجريمة بسن التشريعات والقوانين ، فأصدرت عمان أول قانون عربي يتطرق لمواجهة هذه الجرائم، تبعتها دولة الإمارات العربية المتحدة ثم المملكة العربية السعودية. جميع هذه القوانين مختصة في مكافحة جرائم المعلومات، وتعد هذه القوانين نموذجية حيث تطرقت إلى غالبية الجرائم المعلوماتية ، وتعتبر أول ثلاثة قوانين عربية تصدر بشكل مستقل لمواجهة الجرائم المعلوماتية وتميزت بمايلي:

وضوح المصطلحات المستخدمة عن طريق وضع تعريف لكل مصطلح.

الدقة في صياغة النصوص ووضوح عناصر الجريمة وتحديد عقوبتها.

الالتزام بمبدأ الشرعية الجنائية بمعناها الدقيق الذي يقضي بأن لا جريمة ولا عقوبة إلا بنص.

اشتمالها على أغلب الجرائم المعلوماتية المتصور حدوثها.

ما ذكرناه عن قوانين الخليج العربي الثلاثة مميزات، أما عيوب وقصور هذه الأنظمة فيتمثل في محليتها وتطبيقها داخل الدولة فقط. فالمجرم الإلكتروني السعودي أو المقيم داخل السعودية لا يطبق عليه نظام عمان أو الإمارات عندما يكون الضحية في عمان أو الإمارات .

النتيجة الرئيسية التي استنتجتها في هذا البحث مايلي:

1. اختلاف عقوبات جرائم الكمبيوتر والمعلومات من بلد لآخر.
2. لا تطبق هذه القوانين في غير بلدها باستثناء ما اتفقت عليه دول مجلس اوروبا.
3. ضعف التعاون الدولي في مجال مكافحة الجريمة المعلوماتية.
4. لجوء المجرم الإلكتروني إلى استغلال الثغرات القانونية للإفلات من العقوبة.

5. الوضع الجغرافي الواحد للعالم الغربي يمثل أيضا الوحدة القانونية لمثل هذه الجرائم.

ثانيا: التوصيات

كشفت الدراسة أن الكثير من القوانين الوطنية لمكافحة الجريمة الإلكترونية تعاملت مع المجرم الإلكتروني على أنه مجرم محلي يطبق عليه قانون الدولة التي ارتكب جريمته على أرضها . وكشفت أيضا أن طبيعة الجريمة الإلكترونية كجريمة عابرة للحدود ، لم تؤخذ في الاعتبار عند سن قوانين مكافحة الجريمة الإلكترونية، ولم يتم التنسيق فيما بينها – باستثناء ماتم الاتفاق عليه بين دول المجلس الاوروبي _ وظهر ذلك من خلال وجود عقوبات مختلفة بين الشدة والسهولة لجريمة من نوع واحد.

وبناء على النتائج السابقة توصل الباحث إلى التوصيات التالية:

1. زيادة التعاون الدولي لمواجهة الجرائم المعلوماتية.
2. عقد مؤتمر دولي يتم التركيز فيه على اقتراح سن قانون دولي يعتبر الجريمة الإلكترونية جريمة دولية لا دين ولا حدود ولا وطن لها. وقيام الأمم المتحدة ممثله في الإنتربول الدولي باتخاذ الوسائل والآليات لتحقيق ذلك.
3. إيجاد قاعدة بيانات دولية لمرتكبي الجرائم الإلكترونية.
4. تكريس البحث العلمي العربي نحو سن قوانين دولية لمكافحة الجريمة الإلكترونية.
5. إدراج المحاور السابقة في الإستراتيجية الأمنية العربية للوصول إلى حل عربي موحد.

المراجع:

المراجع العربية:

1. البقمي، ناصر (2007) فاعلية التشريعات العقابية في مكافحة الجرائم المعلوماتية.
2. الشهري، حسن والعطيوي، صالح (2007). دراسة الوضع الحالي لتدريس وتطبيق أنظمة وتشريعات الجريمة الإلكترونية في المملكة، ورقة عمل مقدمة إلى ندوة المجتمع والأمن: الجرائم الإلكترونية..الملامح والأبعاد، الرياض.
3. الشوابكة، محمد (2004). جرائم الحاسوب والإنترنت الجريمة المعلوماتية، عمان، الأردن: مكتبة دار الثقافة للنشر والتوزيع.
4. الصغير، جميل (1994). الإنترنت والقانون الجنائي، دار النهضة العربية، القاهرة، مصر.

5. العريان، محمد (2004). الجرائم المعلوماتية. الإسكندرية، مصر: دار الجامعة الجديدة للنشر.
6. عباينه، محمود (2005). جرائم الحاسوب وأبعادها الدولية، دار الثقافة، عمان، الأردن.
7. عرب، يونس (2002). جرائم الكمبيوتر والإنترنت، ورقة عمل مقدمة إلى مؤتمر الأمن العربي، المركز العربي للدراسات والبحوث الجنائية، أبوظبي.
8. عيد، محمد (1999). الإجرام المعاصر، مركز الدراسات والبحوث بأكاديمية نايف العربية للعلوم الأمنية، الرياض، الطبعة الأولى.
9. قشقوش، هدى (1992). جرائم الحاسب الإلكتروني في التشريع المقارن، القاهرة: دار النهضة العربية.
10. مدني، سالم (2007). مدى إمكانية تطبيق الحدود على الجرائم الإلكترونية، ورقة عمل مقدمة إلى ندوة المجتمع والأمن: الجرائم الإلكترونية..الملامح والأبعاد، الرياض.
11. http://www.alarabalyawm.net
12. http://www.saudir2.com/vb/showthread.php?t=6829
13. http://www.neelwafurat.com/itempage.aspx?id=lbb163532-126150&search=books
14. http://www.al-jazirah.com.sa/digimag/07032004/maaa42.htm
15. http://www.muslm.net/vb/showthread.php?t=202754
16. http://uaew.maktoobblog.com/
17. http://www.mcit.gov.sa/arabic/
18. http://www.elaph.com/web/politics/2008/12/391129.html
19. http://www.alyaum.com/issue/page.php?IN=12423&P=15
20. http://forum.stop55.com/47089.html

المراجع الأجنبية:

21. Cate, F (1997), privacy in the information age. Washington: The Brookings Institution.
22. Lilley, P (2002), hacked attacked& abused digital crime exposed. London, Kogan Page Limited.