العنوان:	قانون دولى موحد لمكافحة الجرائم الإلكترونية
المصدر:	المجلة العربية للدراسات الأمنية
الناشر:	جامعة نايف العربية للعلوم الأمنية
المؤلف الرئيسي:	الشهري، حسن بن أحمد
المجلد/العدد:	مج 27, ع 53
محكمة:	نعم
التاريخ الميلادي:	2011
الشهر:	رجب
الصفحات:	5 - 54
رقم MD:	466944
نوع المحتوى:	بحوث ومقالات
قواعد المعلومات:	EcoLink
مواضيع:	أمن المعلومات ، القوانين والشتريعات ، الإنترنت ، تكنولوجيا المعلومات ، الحاسبات الإلكترونية ، تكنولوجيا الاتصالات ، جرائم المعلومات ، فيروسات الحاسب
رابط:	http://search.mandumah.com/Record/466944

قانون دولي موحد لمكافحة الجرائم الإلكترونية

(تصور مقترح)

اللواء د. حسن بن أحمد الشهري(*)

مستخلص الدراسة

من أهم إنجازات العلم الحديث في هذا العصر وأعظمها جدوى للإنسان ظهور الحاسب الآلي والإنترنت، اللذين قدما خدماتهما للإنسانية في أغلب مناحي الحياة الاقتصادية والتعليمية والطبية والعديد من المجالات الأخرى. ولكن رافق هذه الانجازات بروز خبراء جدد لم تعهدهم الإنسانية من قبل، يتمتعون بالخبرة والحرفية في تطويع هذه التقنية للقيام بأعمال إجرامية أفرزت 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.

وهذه الأعمال الإجرامية لفتت أنظار الدول والهيئات الدولية التي أدركت خطورتها وسهولة ارتكابها وتأثيرها المباشر، لتجعل مكافحتها من أولى أولويات المجتمع الدولي

(*)وكيل مركز الدراسات والبحوث بجامعة نايف العربية للعلوم الأمنية.

والحكومات ما حتم أهمية الحماية القانونية لمواجهة هذه الأفعال الإجرامية، وانبرت العديد من دول العالم في إصدار التشريعات والأنظمة لمكافحة هذه الجريمة (الملط، ٢٠٠٦) . وبخلاف ما يتصوره الكثير من الباحثين والمختصين في مجال مكافحة الجريمة المعلوماتية، فإن ظاهرة انتشار التشريعات والقوانين للحد من هذه الآفة أخذت في الازدياد في الكثير من دول العالم . وأغلب هذه القوانين لم تأخذ في الاعتبار عند إنشائها أن الجريمة المعلوماتية تنشأ في بلد ليحدث أثرها في بلد آخر، وأدلتها منتشرة عبر بلدان أخرى، فأي قانون يحكم هذه الجريمة؟

سيقوم الباحث باستعراض وتحليل القوانين الوطنية الخاصة بالجرائم المعلوماتية لكل من دولة الإمارات العربية المتحدة وسلطنة عمان والمملكة العربية السعودية وكيفية معالجة كل منها لهذه الجريمة داخل حدودها وآلية التعاون الدولي ووجود إطار قانوني يجمعها، كما هو حاصل لاتفاقية مجلس أوروبا للتصدي للجرائم المعلوماتية والذي سيتم استعراض هذه الاتفاقية وإمكانية اعتبارها أساساً لمشروع قانون دولي موحد لمكافحة الجريمة المعلوماتية.

مقدمـــــة

بقدر ما حققته تكنولوجيا المعلومات والاتصالات من فوائد عديدة في مجال الرقي والتقدم الإنساني، فإنها في الوقت ذاته مهدت السبيل إلى بروز أنماط جديدة من الجرائم بالغة الخطورة، وذلك بعد أن تم ربط الحواسب الآلية بالشبكة العالمية للإنترنت، حيث وجد مجرم تقنية المعلومات، تقنية عالية وأساليب حديثة تساعده في ارتكاب ما يحلو له من الجرائم، دون أن يترك أثراً ملموساً لملاحقته ومعرفة مصدرها. والجاني يستطيع بواسطة هذه التقنيات العالية أن يصل إلى أي مكان يرغب فيه، عبر الإبحار في الشبكة المعلوماتية وأن يتصل ويتفاعل مع من يشاء في أي مكان. فلا مكان ولا زمان يستطيع وضع حدود لهذه الشبكة. ولاشك انه من الضروري أن تواكب التشريعات المختلفة هذا التطور الملحوظ في جرائم المعلوماتية، فالمواجهة التشريعية ضرورية للتعامل من خلال قواعد قانونية غير تقليدية لهذا الإجرام غير التقليدي، هذه المواجهة تتعامل بشكل عصري متقدم مع جرائم الكمبيوتر المختلفة، والتي يأتي في مقدمتها الدخول غير المشروع

على شبكات الحاسب ونظم المعلومات، والتحايل على نظم المعالجة الآلية للبيانات ونشر الفيروسات وإتلاف البرامج وتزوير المستندات، ومهاجمة المراكز المالية والبنوك وتعدتها إلى الحروب الإلكترونية، والإرهاب الإلكتروني، ونشر الشائعات والنيل من هيبة الدول، إضافة إلى نشر الرذيلة والإباحية وغيرها من الجرائم الإلكترونية.

وبخلاف تصور العديد من الكتاب والباحثين في مجال الجريمة الإلكترونية بقلة قوانين مكافحة الجريمة المعلوماتية في العالم، فإن إصدار القوانين الوطنية للحد منها آخذ في الازدياد إلا أن مبدأ الإقليمية هو المبدأ المهيمن على تطبيق قوانين الجريمة المعلوماتية من حيث المكان، غير أن هذا المبدأ يفقد صلاحيته للتطبيق بالنسبة للجرائم المعلوماتية، التي تتجاوز حدود المكان. 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، لقد تنبه لذلك القصور دول مجلس أوروبا التي اتفقت على إعداد إطار قانوني للتعاون الدولي في التحقيقات في الجرائم المعلوماتية كان من أهم أهداف هذا الإطار (الاتفاقية) وضع سياسة جنائية مشتركة ضد الجرائم المعلوماتية وإيجاد انسجام تام بين القوانين المحلية والإطار القانوني المتفق عليه، كما أنه ألزم الدول الأعضاء في الاتفاقية بالعمل على إصدار قانون محلي لمكافحة الجرائم المعلوماتية يتسم بالكفاءة في التحقيق والملاحقة القضائية للمخالفات التي ترتكب بواسطة نظام معلوماتي بالإضافة إلى إيجاد تصور لنظام تعاون دولي لمحاربة مثل هذه الجرائم (العبابنة، ٢٠١٠) ولأهمية هذا الموضوع والحاجة إلى معرفة إمكانية إصدار قانون دولي موحد يحاربها على المستوى الدولي، فقد تم إعداد هذا البحث الذي سيلقي الضوء على القوانين الوطنية المتعلقة بالجرائم المعلوماتية، لكل من دولة الإمارات العربية المتحدة وسلطنة عمان، والمملكة العربية السعودية، وإجراء تحليل لهذه القوانين ومقارنتها لاستنتاج درجة التشابه والاختلاف، وإبراز قصورها وتمسكها بمبدأ السيادة الوطنية الأساسي، الذي بمقتضاه لا يمكن إجراء تحقيق في هذه الجرائم خارج حدودها، وعدم وجود إطار يجمع هذه القوانين بموجبه يتم تحديد نقطة اتصال دائمة للاستجابة لطلب المساعدة، كما هو معمول به في اتفاقية مجلس أوروبا ما حدا بالباحث إلى القيام باستعراض القانون الاسترشادي الأوروبي لمكافحة الجرائم المعلوماتية، وإمكانية اعتباره أساساً للقانون الدولي المقترح.

١ . الإطار العام للدراسة

١ . ١ مشكلة الدراسة

تعد وسائل التقنية الحديثة من أهم ما أفرزته الثورة المعلوماتية في الزمن الحاضر، والتي تزايد الاعتماد عليها في مجالات الحياة كافة، ما جعلها عرضة لارتكاب الجرائم التي تقع عليها مباشرة، أو ترتكب من خلالها أو استخدامها كبيئة لارتكاب الجرائم. ولخصوصية هذه الجريمة وتميزها ظهرت الحاجة لسن قوانين لمعاقبة مرتكبيها، إلا أنه برز وبشكل واضح قصور القوانين الوطنية للجريمة المعلوماتية، لمحدودية نطاق تطبيقها باعتبارها محلية لا أثر لها خارج حدودها، وبرزت الحاجة لإصدار قانون عالمي وشامل يواكب تطور هذه الجريمة ويتناسب مع طبيعتها ويحيط بكافة أبعادها.

١ . ٢ التساؤل الرئيس للدراسة

تتبلور مشكلة الدراسة في السؤال الرئيس التالي: ما مدى فعالية القوانين الوطنية للجرائم المعلوماتية في نطاقها المحلي في التصدي للجريمة المعلوماتية، ومعرفة أثر هذه القوانين لردعها خارج حدودها؟ وتفرع عنه سؤال فرعي: ما أهمية إيجاد قانون دولي موحد للجرائم المعلوماتية؟

١ . ٣ 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 وثمانمائة مليون مستخدم(www.vsdoj.gov). وأصبحت هذه الوسيلة مكاناً ملائما لارتكاب أنواع الجرائم المعلوماتية الحديثة التي لم تكن معروفة للبشرية قبل اختراع هذه التقنية، لقد تنوعت جرائمها وأثرت على جل جوانب الحياة. حيث بلغ الضرر درجة لا يمكن تجاهلها وأصبحت ظاهرة معروفة دعت على إثرها العديد من دول العالم إلى سن قوانين وأنظمة وتشريعات لمكافحة الجريمة المعلوماتية، وقد

خصصت هذه القوانين لتخدم كل دولة على حدة 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 (حجازي، ٢٠٠٧) . لقد انحصر تطبيق هذه القوانين كقوانين محليه لا أثر ولا فائدة لها خارج حدودها . وبحكم ذكاء المجرم المعلوماتي ومعرفته لهذه القوانين التي أعطته خيارات متعددة لارتكاب جريمته في دولة لا قوانين لمكافحة هذه الجريمة فيها أو دولة تتسم عقوباتها بالتخفيف. ولقد عقد الكثير من المؤتمرات والندوات ونشر العديد من الأبحاث نوقشت فيها هذه الظاهرة محاولة الإجابة على العديد من التساؤلات المعقدة للبحث عن حلول للقضاء على هذه الجريمة. والباحث لا يميل إلى ترك إيجاد حلول جذرية لها للصدفة للبحث والباحثين، وعلى حد علمه فإنه لا يوجد قانون دولي موحد متفق عليه زماناً ومكاناً للتصدي لهذه الآفة، لذا فان الوقت قد حان لإيجاد آلية دولية . تقترح الآليات والوسائل التي تجيب على التساؤلات المطروحة ولربما يجد الحلول المناسبة وإيجاد تشريع دولي موحد لمواجهة هذه الجرائم وهو ما سيتم إيضاحه من خلال هذا البحث.

١ . ٤ أهداف الدراسة:

١ ـ دراسة وتحليل ثلاثة من قوانين مكافحة الجرائم المعلوماتية والخاصة بكل من سلطنة عمان ودولة الإمارات العربية المتحدة والمملكة العربية السعودية.

٢ ـ معرفة التشابه والاختلاف بين هذه القوانين الثلاثة وقصور هذه القوانين في التصدي للجرائم المعلوماتية خارج حدودها.

٣ ـ استعراض القانون الاسترشادي الأوروبي لمجلس أوروبا لمكافحة الجرائم المعلوماتية وإمكانية أخذه كأساس للقانون الدولي المقترح.

١ . ٥ منهجية الدراسة

المنهج المتبع في هذا البحث، هو المنهج الوصفي الذي يقوم على تحليل المضمون والمقارنة ، حيث سيتم وصف القوانين الوطنية لمكافحة الجريمة المعلوماتية لكل من دولة الإمارات العربية المتحدة وسلطنة عمان والمملكة العربية السعودية، واستعراض جميع

موادها ثم يصار إلى تحليل مضمونها ومقارنتها وإبراز الفوارق بينها لمعرفة مدى قصورها في التصدي للجريمة المعلوماتية والوصول للنموذج المقترح.

١ . ٦ مصطلحات وتعاريف متغيرات الدراسة

قبل البدء في تعريف الجريمة المعلوماتية لابد من الإشارة إلى أن الجريمة المعلوماتية مثلها مثل الجريمة الإرهابية ليس لها تعريف محدد متفق عليه من جميع دول العالم، وإذا سمح لقضية الجريمة المعلوماتية ان تسلك طريق ملف الإرهاب نفسه، فسوف يشهد العالم فوضى معلوماتية، وتخريباً شاملاً لا يستثنى منه أحد. وللمضي قدما في التصدي لهذه الجريمة، لابد من الاعتراف بعالميتها حيث لا حدود ولا دين لها، والاعتراف بشمولها العالم دون استثناء، ووضع التعريف العالمي الحقيقي المتفق عليه دوليا، وفيما يلي استعراض لعدد من التعريفات الحالية لهذه الجريمة:

- الجريمة المعلوماتية هي : كل فعل أو امتناع يأتيه الإنسان ويحدث أضرارا بمكونات الحاسب المادية والمعنوية وشبكات الاتصال الخاصة به (فتوح، ٢٠٠٣).
- وعرفها (العبابنة، ٢٠١٠) بأنها كل فعل أو امتناع عمدي ينشأ عن الاستخدام غير المشروع للتقنية المعلوماتية ويهدف إلى الاعتداء على الأموال المادية أو المعنوية.
- عرف المرشد الفيدرالي الأمريكي منتهك الحاسوب بأنها: الشخص الذي يخترق حاسوبا محميا (مشمولاً بالحماية) دون أن يكون مصرحا له بذلك (البقمي، ٢٠٠٧).
- عرفها قانون مكافحة الجريمة المعلوماتية السعودي: على انه أي فعل يرتكب متضمنا استخدام الحاسب الآلي أو الشبكة المعلوماتية بالمخالفة لأحكام هذا النظام . (www.mcit.gov.sa)
- عرفتها الشرطة البريطانية بأنها: استعمال شبكة الحاسوب لعمل إجرامي (خليفة، ٢٠٠٧).

- عرفهـا مجلس أوروبا(www.gocsi.com) بأنها: أي مخالفة جرمية ترتكب ضد أو باستعمال شبكة الحاسب الآلي.
- أمـا تعريـف الأمـم المتحدة فيقـول: أي جريمة يمكن ارتكابها بواسـطة نظام حاسـوبي أو شبكة حاسوبية أو داخل نظام حاسوبي، وتشمل تلك الجريمة من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في بيئة إليكترونية (الشـوابكة، ٢٠٠٤) .
- تعريف إجرائي: الدخول بغير وجه حق إلى جهاز حاسب آلي مستقل أو مرتبط بجهاز آخر مماثل، بواسـطة شبكة محلية أو دولية كشبكة الإنترنت أو الإنترانت وغيرها من الشبكات بغرض ارتكاب فعل ما يحرمه الشرع و القانون.
- **البيانـات** : هـي المعلومـات، والأوامر، أو الرسـائل ، أو الأصـوات، أو الصور التي تعد ، أو التي سبق إعدادها لاستخدامها في الحاسب الآلي ، وكل ما يمكن تخزينه، ومعالجته ، أو نقله، أو إنشاؤه بواسطة الحاسب الآلي كالأرقام والحروف والرموز وغيرها (الصغير، ٢٠٠١).
- المعلومـات : كل مـا يمكـن تخزينـه ومعالجتـه وتوليـده ونقلـه بوسـائل تقنية المعلومـات وبوجـه خـاص الكتابـة والصـور والصـوت والأرقـام والحروف والرموز والإشارات وغيرها (سرحان، ٢٠٠١).
- نظـام المعلومـات : مجموعـة برامج وأدوات معدة لمعالجـة وإدارة البيانات أو المعلومات أو الرسائل الإلكترونية أو غير ذلك (مدني، ٢٠٠٧).
- الدخول غير المشروع لنظام معلوماتي: دخول شخص بطريقة متعمدة إلى حاسب آلى، أو موقع إلكتروني، أو نظام معلوماتي ، أو شبكة حاسبات آلية غير مصرح لذلك الشخص بالدخول إليها (خليفة، ٢٠٠٧).

١ . ٧ مصطلحات الجريمة المعلوماتية

عندما ظهرت شبكة الإنترنت ودخلت جميع المجالات وتضاعف استعمالها بين أفراد ومؤسسات، وشركات، وحكومات كوسيلة مساعدة في تسهيل حياتهم اليومية، انتقلت

جرائـم الكمبيوتـر لتدخل فضاء الإنترنـت، وظهر تبعا لذلك ما يعـرف اليوم بالجرائم المعلوماتية وتعددت أسماؤها، نورد فيما يلي بعضا من هذه المصطلحات:

الاحتيال المعلوماتي، الغش المعلوماتي، التعسف في استعمال الحاسب الآلي، الجرائم المرتبطة بالحاسـب الآلي، جرائم الحاسـب الآلي، جرائم المعلوماتية، احتيال الكمبيوتر، جرائم التقنية العالية، جرائم الهاكرز، الاختراقات، جرائم الإنترنت، جرائم الحاسـب والإنترنـت، الجرائـم الاقتصادية المرتبطة بالكمبيوتر، السـيبر كرايـم، جرائم أصحاب الياقات البيضاء (الملط، ٢٠٠٦).

١ . ٨ صفات المجرم المعلوماتي

هناك صفات مشتركة لمجرمي المعلومات منها:

- أعمارهم تتراوح عادة بين ١٨ إلى ٤٦ سنة .
- المعرفة والقدرة الفنية الهائلة.
- الحرص الشديد وخشية الضبط وافتضاح الأمر.
- ارتفاع مستوى الذكاء ومحاولة التخفي (الشوابكة،٢٠٠٤).

١ . ٩ أقسام الجريمة المعلوماتية

ان أكثر الجرائم المعلوماتية التي يتم ارتكابها يكون الهدف الأساس لها هو الحصول على المعلومات التي تكون اما محفوظة على أجهزة الحاسـبات الآلية أو تلك المنقولة عبر شـبكة الإنترنـت ، إلا أن ذلك لا يعني أن هناك جرائـم أخرى يكون لها هدف آخر غير الحصـول على المعلومـات، مهما كانت أهمية تلك المعلومات، وكـما اختلف الباحثون في تسـمية الجرائم الإلكترونية فقد اختلفوا أيضا في تقسـيمها وتصنيفها فمنهم من قسـمها إلى ثلاث مجموعات :

- جرائم تسـتهدف النظام والمعلومات كهـدف : هناك العديد من الجرائم التي يكـون ارتكابها لهدف يتعلق بالمعلومات، ويتمثل هذا الهدف إما بالحصول على

المعلومـات أو تغييرهـا أو حذفها . ومعظم تلك الجرائم التي يكون الهدف منها المعلومات، هي في الأغلب من الحالات تكون جرائم اقتصادية للحصول على مزايا أو مكاسب اقتصادية.

- جرائـم تسـتخدم الكمبيوتر وسـيلة لارتـكاب جرائم أخـرى : في هذه الحالة يكـون الهدف من ارتكاب الجرائم الإلكترونية عبر شـبكة الإنترنت هو أجهزة الكمبيوتـر فالغالـب يكـون الهـدف هو تخريـب تلـك الأجهزة نهائيـا، أو على الأقل تعطيلها لأطول فترة ممكنة، ومعظم تلك الجرائم تتم بواسـطة اسـتخدام الفيروسات.

- جرائـم تتعلـق بمحتوى مواقـع المعلوماتيـة وبيئتها. كجرائم إتلاف وتشـويه البيانـات والمعلومات وبرامج الحاسـب وجرائم الغش للحصول على الأموال (مدني،٢٠٠٧).

وقسمها آخرون) إلى ما يلي:

- جرائم تصنف حسب المعطيات ومحل الجريمة كجرائم إتلاف وتشويه البيانات والمعلومات وبرامج الحاسب وجرائم الغش للحصول على الأموال ، وجرائم تسـتهدف المواضيـع الخصوصية ، وكذلك جرائم الاعتـداء على حقوق الملكية الفردية لبرامج الحاسوب ، كالنسخ والتقليد والاعتداء على العلامات التجارية.

- جرائم تصنف تبعا لدور الحاسب في الجريمة كالجرائم التي تستهدف عناصر السريـة والسـلامة كالدخـول غـير القانـوني ، واعـتراض وتدمـير البيانـات ، وإساءة استخدام الأجهزة. والجرائم المرتبطة بالحاسوب والتي تشمل التزوير، والاحتيال ، والأعمال المخلة بالآداب كالإباحية والنشر الفاضح الخادش للحياء، وجرائم مرتبطة بحق المؤلف وحقوق منتجي البرامج.

- جرائـم تصنـف تبعا لمساسـها بالأشـخاص والأمـوال كالجرائم التي تتسـبب بالوفـاة، والتحريض عـلى الانتحار، والمضايقة والتهديـد، والملاحقة، وانتهاك خصوصية البريد الإلكتروني. وكذلك الجرائم الجنسية الواقعة على الاحداث،

كإفسادهم والتحرش بهم، ونشر المواد الفاضحة ومواقع الدعارة. كما أنها تشمل الجرائم التي تستهدف الأموال كغسل الأموال، واستخدام النطاقات، والعلامات التجارية، وجرائم الاحتيال والسرقة كاستخدام أنظمة المعلومات للحصول على البطاقات الائتمانية، والاختلاس من الحسابات البنكية، وقرصنة البرامج، وسرقة الهويات الوطنية، وجرائم التزوير للبريد الإلكتروني، وتزوير الوثائق والسجلات، وجرائم القمار والابتزاز، وجرائم مخلة بأمن الدولة كتعطيل الحكومة، ونشر الإشاعات المغرضة والمضللة والشائعات الكاذبة والفتن بقصد النيل من هيبة الدولة، وجرائم المخدرات والتجسس الإلكتروني والإرهاب والقرصنة الإلكلترونية (يونس،٢٠٠٢).

مما سبق نرى أن جرائم الحاسوب لا تختلف عن الجرائم التي توالى حدوثها عبر التاريخ ولكنها اليوم ترتكب في بيئات جديدة ووسائل حديثة وضحايا من نوع جديد وأضيف إلى ما سبق عدد من الجرائم المستحدثة والتي أصفها بالجرائم الأشد قسوة.

١ . ١٠ أنواع الجريمة المعلوماتية الأشد قسوة

- 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 الفساد في التجارة الإلكترونية.
- إنشاء مواقع إباحية والترويج للإباحية الجنسية من خلال نشر الصور والأفلام الهابطة.
- تملك وإدارة مشروع مقامرة على الإنترنت.
- سرقة أدوات التعريف والهويات الوطنية.
- القتل بالحاسب والتسبب في الوفاة.
- التحريض على القتل عبر الإنترنت.
- جرائم تتعلق بأمن الدول كبث الشائعات وتعطيل الحكومة .

١ . ١١ خصائص الجريمة المعلوماتية

تعد الجرائم التي ترتكب من خلال شبكة الإنترنت ، جرائم ذات خصائص منفردة خاصة بها، لا تتوفر في أي من الجرائم التقليدية في أسلوبها ، وطريقة ارتكابها ، أورد فيما يلي بعضا من هذه الخصائص:

- من خصائص هذه الجريمة أنها ليست عادية أو تقليدية ترتكب بصورة عشوائية أو غير مدروسة.
- سهولة ارتكاب الجريمة الإلكترونية ، وذلك باستخدام الوسائل التقنية.
- صعوبة تتبع مرتكبي هذه الجريمة وسهولة إخفاء معالمها.
- سرعة ارتكاب هذا النوع من الجرائم.
- إنها جريمة تنفذ بواسطة مجرمين 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، ما يدعو إلى القـول بـأن مرتكبي هذه الجرائم غالبا ما يكونـون من المتخصصين في مجال الحاسب والمعلومات (الملط، ٢٠٠٦).

- من خصائصها أيضا أنها من الجرائم العابرة للحدود 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.
- الحاسب الآلي هو أداة ارتكاب الجريمة.
- ترتكب أغلب تلك الجرائم عبر شبكة الإنترنت (خليفة، ٢٠٠٧).

١ . ١٢ أركان الجريمة المعلوماتية

اتفقـت جميع القوانين عـلى ضرورة توافر أركان الجريمة الثلاثة: الشرعي، المادي، المعنوي في كل الجرائم بدون اسـتثناء، ذلك لأنها سـلوك إرادي مصدره الإنسان . وهي كأي سلوك إنساني لها جانبان ، جانب مادي خارجي نلمسه في الكون المحيط ، وجانب باطني داخلي يعبر عن نفسـية مرتكبها. هذان الجانبان ليسـا سوى الركن المادي والركن المعنـوي ومـن ثم لابـد من توافرهمـا واجتماعهما معا حتـى تقوم الجريمـة ، وتخلفهما أو تخلف احدهما يترتب عليه تخلف الجريمة . أما الركن الشرعي سـواء تمثل في الصفة غير المشروعـة للفعـل أو النص الشرعي المجرم، أي القاعـدة الجنائية ، فيعد ركنا في الجريمة الإلكترونية، لان الجريمة لا توجد أصلا دون توافر القاعدة الجنائية ، التي تحدد الجريمة وترسم حدودها. وفيما يلي بعض التفصيل لهذه الأركان:

أولاً: الركن الشرعي

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 إنجاز 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 عرضة للاعتداءات. ويذكر (الشوابكة ، ٢٠٠٤) أن النصوص التقليدية تقف عاجزة أمام هذه الاعتداءات على الخصوصيات الفردية وأسرارها . لذا فإن الحاجة تغدو ملحة لسد فراغ تشريعي في حماية ما يتم تداوله من معلومات وأسرار على هذه الشبكة ، ولحماية الاتصالات والمراسلات بين الناس.

ثانياً: الركن المعنوي

هو الحالة الذهنية والعقلية للجاني ، أي وجود سوء نية ، وإرادة حرة وواعية للولوج في الشبكة، وإحداث إضرار أو الولوج بقصد السرقة وتدمير البيانات وغيرها من الجرائم. كالاعتداء على المعلومات الخاصة بالمنظمات الحكومية أو الخاصة أو المملوكة للأفراد بقصد إتلافها كليا أو جزئيا أو تقليل منفعتها ما يؤدي إلى إلحاق الضرر بمالكي المعلومات وتعد من الجرائم العمدية في حالة تحقق عنصري العلم بملكيتها للغير والإرادة في تدميرها ما له الأثر السلبي في تنفيذ أنشطة المنظمة جزئيا أو كليا (قشقوش،١٩٩٢). ويقسم الشوابكة الركن المعنوي إلى محورين هما:

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

٢ ـ الدخول غير المرخص إلى أنظمة المنظمة الإلكترونية ، ويتم في هذه الحالة تدمير البيانات والمعلومات كليا والموجودة في النظام أو التعديل والتشويه للبيانات

والمعلومات ما يكون عائقا أمام المنظمة للاستمرار في تنفيذ عملياتها أو الحد من اتخاذ القرارات السليمة (الشوابكة، ٢٠٠٤).ويذكر مدني 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. (مدني، ٢٠٠٧).

ثالثاً: الركن المادي

يتمثل هذا الركن بالنشاط الايجابي والسلوك المادي، المرتبط ببيئة رقمية واتصال بالشبكة، ومعرفة هدف هذا النشاط وأسلوبه ونتائجه، كأن يقوم المجرم بتشغيل الحاسب ووصله بالإنترنت، وإعداد البرامج للاختراق للأجهزة الهدف، أو إعداد وضخ فيروسات مدمرة بهدف الإضرار بهذا الهدف، كما انه 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 (قشقوش، ١٩٩٢).

١ . ١٣ خسائر الجريمة المعلوماتية

أورد أسعد خليل انه بعد ازدياد الخطر من استخدام الإنترنت بدأت العديد من المنظمات والهيئات في إطلاق الدعوات والتحذيرات من خطورة هذه الظاهرة التي تهدد كل مستخدمي الإنترنت خاصة بعد تقرير برلماني في مجلس اللوردات البريطاني أظهر أن شبكة الإنترنت تحولت إلى حلبة يرتع فيها المجرمون، وتنفذ فيها العصابات سرقة الأموال من الحسابات المصرفية ، محذرا الحكومات للتدخل لتنظيم عملها قبل فوات الأوان. وأضاف التقرير أن خسائر بريطانيا في العام ٢٠٠٩ جراء الجرائم الإلكترونية بلغت ٧٦ مليون دولار. (مدني، ٢٠٠٧). وتشير تقارير موثقة أن خسائر المصارف الأمريكية الناجمة عن جرائم الإنترنت في العام ٢٠٠٩ م بلغت ملياري دولار، وفي عام ٢٠٠٧ م ارتكبت جريمة إلكترونية في بريطانيا كل عشر ثوان، وبلغت جرائم التحرش بالأطفال والنساء فيها أكثر من ٨٥٠ ألف حالة، وأكثر من ٩٢ ألف حالة سرقة للهوية الوطنية، و١٤٥ ألف حالة اختراق لأجهزة حواسب وسرقة معلوماتها، وسجلت كذلك

٢٠٧ آلاف حالة سطو على الأموال من خلال سرقة أرقام البطاقات الائتمانية (www.alarabaialyawm.net).

وفي دراسة لرئيس المجمع العربي للملكية الفردية أن الجرائم الإلكترونية باتت تشكل تحديا كبيرا للاقتصاد العالمي ، حيث يشهد العالم جريمة إلكترونية كل ثلاث دقائق للملكية الفكرية، وتجاوزت خسائرها أكثر من ٤٨ مليار دولار (www.uaew.maktoob. com). وفي الإمارات العربية المتحدة تم التحقيق في ٢٢٢ قضية قرصنة إلكترونية (www.uaew.maktoob.com).

وفي الولايات المتحدة الأمريكية أعلنت السلطات الاتحادية الأمريكية تزايد جرائم الاحتيال عبر الإنترنت بنسبة ٣٣٪ في عام ٢٠٠٨ م عنه في العام الذي قبله، وبحسب التقارير فالأعوام منذ ٢٠٠٩ م وما بعده تتجه لأن تكون أعواما مزدحمة في مجال الجريمة المعلوماتية . كما ان التوقعات بان الجرائم الإلكترونية قد تتسبب بخسارة دول مجلس التعاون الخليجي بين ٥٥٠ مليوناً و٧٣٥ مليون دولار أمريكي سنويا. ومن المتوقع أن ترتفع هذه الأرقام نظرا لتزايد استخدام الإنترنت على نطاق واسع للتواصل وعقد المعاملات والصفقات التجارية (www.neelwafurat.com).

٢ . مراجعة عدد من القوانين والمعاهدات السابقة

٢ . ١ معاهدات واتفاقيات ودعوات لمكافحة الجرائم المعلوماتية:

- دعا خبراء جزائريون إلى نشوء تعاون دولي وثيق لمحاربة الجريمة المعلوماتية ورأى هؤلاء الخبراء أن ظاهرة الإجرام المعلوماتي تقتضي محاربة فاعلة لهذه الجريمة، وأشار المدير العام للمدرسة الجزائرية العليا للقضاء أن التشريع الدولي في مجال الجريمة المعلوماتية سائر نحو مزيد من التعزيز مشيرا إلى عدة دول مثل كندا وأمريكا وكوريا واليابان وجنوب أفريقيا انضمت إلى الاتفاقية الدولية لمجلس أوروبا وأضاف أن هذه الدول استلهمت من هذه الاتفاقية وضع 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 (خليفة، ٢٠٠٧).

- أكثر من ٥٠٠ مؤتمر دولي في العشر السنوات الماضية تتعلق بالجرائم المعلوماتية (www.elaf.com).
- أهاب مؤتمر الأمم المتحدة الثامن لمنع الجريمة ومعاملة المجرمين الذي عقد في هافانا عام ١٩٩٠م، في قراره المتعلق بالجرائم الإلكترونية بالدول الأعضاء ان تكثف جهودها لمكافحة إساءة استعمال الحاسب الآلي. كما حث الدول الأعضاء على مضاعفة الأنشطة التي تبذلها على الصعيد الدولي من اجل مكافحة هذه الجرائم، بما في ذلك الدخول حسب الاقتضاء أطرافا في المعاهدات المتعلقة بتسليم المجرمين، وتبادل المساعدة الخاصة بهذه الجرائم وفتح آفاق جديدة للتعاون الدولي لوضع معايير دولية لأمن المعالجة الآلية للمعلومات، ووضع التدابير الملائمة لحل مشكلات الاختصاص القضائي، التي تثيرها الجرائم المعلوماتية العابرة للحدود، أو ذات الطبيعة الدولية، وإيجاد الآليات الدولية لتنظيم إجراءات التفتيش والضبط المباشر الواقع عبر الحدود على الأنظمة المعلوماتية(البقمي،٢٠٠٧).
- معاهدة حماية الأفراد المتعلقة بالمعالجة الآلية للبيانات الشخصية(www.c /cisac.html).
- تعديلات حول معاهدة حماية الأفراد المتعلقة بالمعالجة الآلية للبيانات الشخصية (www.c /cisac.html).
- بروتوكول إضافي حول حماية الأفراد المتعلقة بالمعالجة الآلية للبيانات الشخصية (www.c /cisac.html).
- معاهدة حول جريمة الفضاء التخيلي (www.c /cisac.html).
- بروتوكول إضافي حول المعاهدة حول جريمة الفضاء السيبراني المتعلق بتجريم أعمال كره الأجانب المرتكبة عبر أنظمة الكمبيوتر (www.c /cisac.html).
- إعلان بوخارست حول مكافحة التزوير والقرصنة (www.c /cisac.html).
- حماية تقنية المعلومات ووسائل منع الجرائم الخاصة بالإنتربول (خليفه، ٢٠٠٧).
- قرار إطار العمل الصادر عن مجلس الاتحاد الأوروبي حول الجريمة المعلوماتية (العبابنة، ٢٠٠٦).

- دعا مؤتمر مكافحة الجرائم الإلكترونية لدول مجلس التعاون الخليجي إلى عقد معاهدة على مستوى المجلس على غرار الاتفاقية الأوروبية للجريمة الإلكترونية تشكل نواة لمعاهدة عربية في مجال مكافحة الجريمة الإلكترونية (الملط، ٢٠٠٦).
- اتفاقية مجلس أوروبا ـ الذي يشرف على الكثير من المعاهدات القانونية ـ أول معاهدة دولية حول الجرائم المرتكبة بواسطة شبكة الإنترنت والتي يعود تاريخها إلى عام ٢٠٠١ (العبابنة، ٢٠٠٦).
- يأمل الإتحاد الدولي للاتصالات الدولية الذي يضم جميع دول العالم التي تستخدم نظام الهاتف العالمي في أن يأخذ زمام المبادرة للمطالبة بمعاهدة عالمية ضد الجريمة الإلكترونية(www.c /cisac.html) .

٢ . ٢ الجهود العلمية العربية في مجال رصد وتتبع الظواهر الأمنية المصاحبة لانتشار الحاسبات والإنترنت ومنها:

- أمن المعلومات في الحاسبات الآلية والاتصالات ١٩٨٦، نظمها مركز المعلومات الوطني السعودي (الرياض، ١٩٨٦).
- ندوة حول الجرائم الناجمة عن التطور التكنولوجي، (الأردن ١٩٩٨) .
- ندوة المواجهة الأمنية للجرائم المعلوماتية ، (دبي ١٩٩٩) .
- مؤتمر جرائم الإنترنت ، (دبي ٢٠٠٠) .
- ندوة دراسة الجرائم المستحدثة ، أكاديمية نايف العربية للعلوم الأمنية، (الرياض ٢٠٠٠).
- المؤتمر الخليجي الثاني لأمن الإنترنت (مسقط ٢٠٠١) .
- مؤتمر امن المعلومات العربية ، (القاهرة ٢٠٠٢).
- ندوة الجرائم الإلكترونية، (مسقط ٢٠٠٢) .
- ندوة الاحتيال الإلكتروني، (الأردن ٢٠٠٣).

- ندوة الإنترنت وامن المعلومات، (ليبيا ٢٠٠٢).
- مؤتمر الجوانب الأمنية لأمن المعلومات، (دبي ٢٠٠٣).

٢ . ٣ منظور مبدئي لقانون دولي موحد لمكافحة الجرائم المعلوماتية

- مشروع قانون عربي للجرائم الإلكترونية: قدم يونس عرب مشروعه لسن قانون عربي موحد للجريمة الإلكترونية، وقد برر ذلك إلى أن جميع التشريعات الحالية متباينة، وعدم كفاية نصوص التجريم السائدة عن الإحاطة بهذه الجرائم، وأضاف أن الغالبية من دول العالم قد أطلقت على قوانينها وتشريعاتها الخاصة بمكافحة الجريمة الإلكترونية، مسميات مختلفة مثل جرائم الكمبيوتر، جرائم الكمبيوتر والمعلومات، جرائم الكمبيوتر والإنترنت، جرائم إساءت استخدام الكمبيوتر، جرائم السايبر وغيرها من المسميات، وبرغم انه قد يتبادر للذهن للوهلة الأولى ، انها تعطي نفس المعنى ، إلا أننا وجدنا من استعراضنا لبعض هذه القوانين انها تتفاوت في تحديد الجرائم والعقوبات لنفس الجريمة الواحدة. وقدم مشروعه العربي (جرائم الكمبيوتر والإنترنت) المكون من ١١ مادة ، غطت تقريبا مفردات جميع القوانين العربية الحالية بعد استبعاد التكرار ومساواة العقوبات للجرائم المتساوية(يونس، ٢٠٠٦) .
- واعتمدت الجامعة العربية ما سمي بقانون الإمارات العربي الاسترشادي لمكافحة الجريمة المعلوماتية حيث اعتمده وزراء العدل العرب في دورته التاسعة عشرة بالقرار رقم ٤٩٥- د١٩- ٨/ ١٠/ ٢٠٠٣ م ومجلس وزراء الداخلية العرب في القرار رقم ٤١٧- د٢١/ ٢٠٠٤ م.
- وافق مجلس وزراء العدل العرب على مشروع الاتفاقية العربية حول مكافحة جرائم تقنية المعلومات واحالته لمجلس وزراء الداخلية العرب لاعتماده (الشهري، ٢٠٠٧).
- مركز الشكاوى الخاصة بجرائم الإنترنت (IC٣) : نظام تبليغ وإحالة شكاوى الناس في الولايات المتحدة الأمريكية والعالم اجمع ضد جرائم الإنترنت.

ويتعامل المركز بواسطة استمارة للشكاوى مرسلة على الإنترنت وبواسطة فريق من الموظفين والمحللين ، وكذلك الجمهور ووكالات فرض و تطبيق القوانين الأمريكية والدولية التي تحقق في جرائم الإنترنت. وقد تم تأسيس أول مكتب للمركز سنة ١٩٩٩ م في الولايات المتحدة ، وسمي مركز شكاوى الاحتيال على الإنترنت . وفي العام ٢٠٠٢ م ، وبغية توضيح نطاق جرائم الإنترنت التي يجري تحليلها، بدءا من الاحتيال البسيط إلى تشكيلة من النشاطات الإجرامية التي أخذت تظهر على الإنترنت، بعدها دعا مكتب التحقيقات الفيدرالي الأمريكي ووكالات فدرالية أخرى للمساعدة في تزويد المركز بالموظفين وللمساهمة في العمل ضد الجرائم الإلكترونية. وبإمكان الناس من كافة أنحاء العالم تقديم شكاوى بواسطة موقع المركز على الإنترنت(www.gocsi.com).

- الاتفاقية الأوروبية لجرائم الحاسب الآلي: ست وأربعون دولة أوروبية إضافة إلى الولايات المتحدة الأمريكية ، وقعت على الاتفاقية الأوروبية لمكافحة الجرائم الإلكترونية في العام ٢٠٠١م. الهدف من هذه الاتفاقية ، تحسين قدرات الدول الموقعة عليها للتعامل مع الجريمة الإلكترونية، وفي وقت لاحق انضم إلى هذه الاتفاقية كل من كندا واليابان والجبل الأسود وجنوب إفريقيا . وضع المجلس النموذج العام لاتفاقية مكافحة الجريمة المعلوماتية كنموذج وإطار تستفيد منه الدول في تحسين وتطوير أنظمتها في مكافحة هذه الجريمة ، وتلزم هذه الاتفاقية الدول الموقعة عليها بالإفصاح عن الجرائم الإلكترونية التي يوجد ضحاياها في هذه الدول ، وتفصح كذلك عن الإجراءات المتخذة في الضبط والتحقيق ونشر النتائج ، وخصوصا ما يتعلق بجرائم الغش والتزوير وهتك أعراض الأطفال ونشر الإباحية والتعدي على حقوق المؤلفين وجرائم القرصنة والإرهاب الإلكتروني(www.c\cisac.stanford.edu).
- توصيات المؤتمر الخامس عشر للجمعية الدولية لقانون العقوبات الذي انعقد في البرازيل ١٩٩٤م بشأن جرائم الكمبيوتر ووضع حدود دنيا لعقوبات جرائم الحاسب (www.conventions.coe).

- توجد تشريعات وطنية تختص بجرائم الحاسب الآلي بشكل عام مابين ٥٠ إلى ٦٠ بلدا ، إلا أن أكثر من ١٠٠ بلد أخرى ليس لديها شيء من هذه القوانين (خليفة، ٢٠٠٧).

- توصيات وزراء العدل والداخلية للدول الثماني الكبرى، في اجتماعهم في فرنسا العام ٢٠٠٢م بتكثيف التعاون الدولي لمواجهة الجريمة الإلكترونية (www.gocsi.com).

٢ . ٤ بعض دول العالم التي سنت قوانين وطنية للتصدي للجريمة المعلوماتية

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 (تمام، ٢٠٠٠). وفيما يلي بيان بالدول التي لديها قوانين محلية للتصدي للجريمة المعلوماتية:

١ ـ السويد: السويد هي أول دولة تسن تشريعات خاصة بجرائم الحاسب الآلي والإنترنت، حيث صدر قانون البيانات السويدي عام ١٩٧٣ الذي عالج قضايا الاحتيال عن طريق الحاسب الآلي، إضافة إلى شموله فقرات عامة تشمل جرائم الدخول غير المشروع على البيانات الحاسوبية أو تزويرها أو تحويلها أو الحصول غير المشروع عليها(يونس، ٢٠٠٢) .

٢ ـ الولايات المتحدة الأمريكية: بعد السويد أصدرت الولايات المتحدة تشريعات لمكافحة الجريمة الإلكترونية عام ١٩٧٣ م هذا القانون يسمح للأشخاص أو المؤسسات التي تم الاعتداء على 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:

- تخويل كتابي من المعتدى عليه.
- يجب أن يكون المراقب لتلك الاتصالات عضوا في لجنة التحقيق.

- يجب أن تتوافر لدى مراقب الاتصالات المعرفة لمراقبة الاتصالات التي لها علاقة بالجريمة.
- مراقبة اتصالات منتهك الحاسوب الخاصة بالجريمة فقط وقدر الإمكان.
- عندما يسفر التحقيق عن وجود الدليل الإلكتروني خارج حدود الولايات المتحدة فإن الولايات المتحدة تسعى للحصول على الدليل من الدول على النحو التالي:
  - موافقة الدولة الأجنبية.
  - موافقة مكتب الشؤون الدولية مع وزارة العدل (البقمي، ٢٠٠٧).

كما أصدرت الولايات المتحدة عدداً من القوانين المتعلقة بالجرائم الإلكترونية منها قانون الخصوصية لعام ١٩٧٤ م ،تلا ذلك أن قام معهد العدالة القومي في العام ١٩٨٥ م بتحديد خمسة أنواع رئيسة للجرائم الإلكترونية، وهي جرائم الحاسب الآلي وجرائم الاستخدام غير المشروع عن بعد، وجرائم التلاعب بالحاسب الآلي، ودعم التعاملات الإجرامية وسرقة البرامج الجاهزة ، والمكونات المادية للحاسب، وفي العام ١٩٨٦م صدر قانون تشريعي عرف جميع المصطلحات الضرورية لتطبيق القانون على الجرائم المعلوماتية ووضعت المتطلبات القانونية اللازمة لتطبيقه ومن ثم تبعته بقانون المعاملات الموحد في العام ١٩٩٩م ، وعلى ذلك قامت الولايات الداخلية بإصدار القوانين المحلية الخاصة بكل ولاية (عبدالكريم، ٢٠٠٧).

٣ ـ استراليا: 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 ومخزنة في حاسبات أخرى لا تنتمي لهذه الدول يعد هذا الشخص متهما ومنتهكا للقوانين ويستحق عقوبة السجن لمدة ستة أشهر إلى جانب مواد أخرى (البقمي، ٢٠٠٧).

٤ ـ كندا: تطبق كندا قوانين متخصصة ومفصلة للتعامل مع جرائم الحاسب الآلي والإنترنت، حيث عدلت في العام ١٩٨٥م قانونها الجنائي بحيث يشمل قوانين خاصة بجرائم الحاسب الآلي والإنترنت، كما يشمل القانون الجديد تحديد عقوبات المخالفات الحاسوبية ، وجرائم التدمير او الدخول غير المشروع لأنظمة الحاسب الآلي فعلى سبيل المثال 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 يعد مدانا ويستحق عقوبة السجن لمدة لا تتعدى عشر سنوات (البقمي، ٢٠٠٧).

٥ ـ الصين: أصدرت الصين أنظمة حماية أمن المعلومات وتشمل معاقبة الشخص بمبلغ ٥٠٠٠ يوان عند استخدامه الفيروسات لتدمير المعلومات أو قام بالتأثير على نظام المعلومات أو باع أنظمة معلومات بدون ترخيص. كما أنها أصدرت لاحقا قانون مكافحة الإباحية على المواقع الإلكترونية. حدد هذا القانون معايير معاقبة القائمين بإنتاج أو نشر أو نسخ المعلومات الإباحية على الإنترنت، أو الهاتف النقال أو أي وسائل أخرى، وقد وسع هذا القانون مجال مراقبة المواقع على شبكة الإنترنت (خليفة، ٢٠٠٧).

٦ ـ مقاطعة (هونج كونج التابعة للصين) يعاقب من يصل للمعلومات المخزنة بالحاسب الآلي من غير إذن شرعي بدفع غرامة قدرها ٢٠٠٠٠ دولار أمريكي ، وبالسجن خمس سنوات لمن يتسبب في خسارة الآخرين وحصوله على دخل غير شرعي (خليل، ٢٠٠٧).

٧ ـ مملكة الدنمارك: سنت القوانين الدنماركية قانون مكافحة الجريمة في العام ١٩٨٥ م الأول الخاص بجرائم الحاسب الآلي والإنترنت والتي شملت في فقراتها العقوبات المحددة لجرائم الحاسب الآلي كالدخول غير المشروع للحاسبات أو التزوير أو أي كسب غير مشروع فعلى سبيل المثال ينص على

الغرامة والسجن لمده تصل ستة أشهر لأي شخص يدخل على المعلومات الآلية بدون إذن شرعي (البقمي، ٢٠٠٧).

٨ ـ فرنسا: من الدول التي اهتمت بتطوير قوانينها الجنائية للتوافق مع المستجدات الإجرامية ، حيث أصدرت في العام ١٩٨٥ م قانونا يضيف إلى قانون العقوبات الجنائي ، جرائم الحاسب الآلي والعقوبات المقررة لها. فعلى سبيل المثال ينص نظام مكافحة الجريمة المعلوماتية في فرنسا على معاقبة أي شخص لقيامه بنشاط من شأنه التحايل على النظام الآلي بالسجن لمدة تصل إلى سنة وغرامة تصل ١٠٠٠٠٠ فرنك فرنسي (عبدالكريم، ٢٠٠٧).

٩ ـ ألمانيا: في ألمانيا يحق للقاضي إصدار أوامره بمراقبة اتصالات الحاسبات الآلية وتسجيلها والتعامل معها ومن أمثلة العقوبات في هذا القانون ان القانون الألماني الخاص بأنظمة المعلومات ينص 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(عبدالكريم، ٢٠٠٧).

١٠ ـ جمهورية إيرلندا: يعاقب منتهك الأنظمة المعلوماتية بدون إذن بغرامة ٥٠٠ جنيه أو السجن لمدة لا تتجاوز ثلاثة أشهر(البقمي، ٢٠٠٧).

١١ ـ الهند: تخضع الجرائم الإلكترونية كالسرقة والاحتيال والتشهير والأذى لقانون العقوبات الهندي وعلى سبيل المثال ينص نظام الاعتداء على أنظمة المعلومات بالسجن لمدة تصل إلى ثلاث سنوات وبغرامة لا تتعدى ٢٠٠٠٠ روبية أو بهما معا (البقمي، ٢٠٠٧).

١٢ ـ اليابان: يعاقب منتهك أنظمة المعلومات بغرامة تصل ٥٠٠٠٠ ين أو السجن خمس سنوات كحد أقصى (Lilley, 2002)، ولكن القانون الياباني لا يلزم مالك الحاسب الآلي المستخدم في جريمة ما ، التعاون مع جهات التحقيق أو إفشاء كلمة السر التي يستخدمها إذا ما كان ذلك سيؤدي إلى إدانته (عبدالكريم، ٢٠٠٧). كما صدرت تشريعات مشابهة في كل من أيسلندا ولكسمبورغ و مالطا

والنرويج وبولندا والبرتغال و سـنغافورة وجنوب أفريقيا واسبانيا وسويسرا وتركيا. وبلجيكا واستونيا وفنلندا وألمانيا واليونان(الشهري، ٢٠٠٧).

١٣ ـ المملكـة العربيـة السـعودية: نظام التعاملات الإلكترونيـة ، وقانون مكافحة الجرائم المعلوماتية (١٤٢٩هـ).

١٤ـ الإمارات العربية المتحدة: قانون مكافحة جرائم تقنية المعلومات (٢٠٠٦ م) .

١٥ ـ سلطنة عمان: قانون مكافحة الجرائم الإلكترونية (٢٠٠١ م) .

١٦ ـ لبنان: قانون التجارة الإلكترونية (٢٠٠٠م) .

١٧ ـ البحرين: قانون التجارة الإلكترونية ، ومرسوم بشأن المعاملات الإلكترونية (٢٠٠٣م) .

١٨ ـ قوانين ومراسيم مماثلة في الجزائر والمغرب وتونس (٢٠٠٧ م) .

١٩ ـ الأمـم المتحـدة: الاونيسـيترال حـول منـع ومراقبـة الجرائـم المرتبطـة بالكمبيوتر(٢٠٠٧) م. (www.uaew.maktoob.com).

٣ . قوانين مكافحة الجرائم المعلوماتية في كل من المملكة العربية السعودية ودولة الإمارات العربية المتحدة وسلطنة عمان

تمهيد

سـوف يتناول هذا الجزء تعريف وتصنيف الجرائم المعلوماتية وتحديد عقوباتها في كل مـن نظـام مكافحة الجرائم المعلوماتيـة الخاص بالمملكة العربية السـعودية، وقانون الإمارات العربية المتحدة وقانون سلطنة عمان الخاص بجرائم الحاسب الآلي، ثم نتطرق إلى استعراض القانون الاسترشادي الأوروبي الخاص بمكافحة الجرائم المعلوماتية، يلي ذلك تحليل ومقارنة لمضامين هذه القوانين .

١.٣ الجرائم المعلوماتية في النظام السعودي http: / /www.mcit.gov.sa /arabic

صدر في المملكة العربية السعودية نظام مكافحة الجرائم المعلوماتية بالمرسوم الملكي رقم م- ١٧ في ٧/ ٣/ ١٤٢٨ هـ الذي يهدف إلى مواجهة جرائم الحاسب الآلي والإنترنت والحد منها، وإلى حماية المصالح العامة، والأخلاق، والآداب العامة، وحماية الاقتصاد الوطني .

ويعرف هذا النظام الجريمة المعلوماتية بأنها : أي فعل يرتكب متضمنا استخدام الحاسب الآلي أو الشبكة العنكبوتية بالمخالفة لأحكام هذا النظام (الفقرة ٨ ، المادة ١) .

وقد تضمن هذا النظام المكون من ست عشرة مادة تصنيفاً للجرائم المعلوماتية إلى (٥) فئات حسب العقوبات المقررة لها .

وتتراوح هذه العقوبات المقررة بين السجن مدة لا تزيد على سنة أو غرامة لا تزيد على خمسمائة ألف ريال، وبين السجن مدة لا تزيد على عشر سنوات أو غرامة لا تزيد على خمسة ملايين ريال ، وفيما يلي تفصيل لذلك:

١.١.٣ الفئة الأولى : (المادة ٣)

وتشمل هذه الفئة مجموعة الجرائم المعاقب عليها بالسجن مدة لا تزيد على سنة وبغرامة لا تزيد على خمسمائة ألف ريال ، أو بإحدى هاتين العقوبتين وهي :

- التقاط أو اعتراض ـ دون مسوغ نظامي صحيح ـ ما هو مرسل عن طريق الشبكة المعلوماتية أو أحد أجهزه الحاسب الآلي ، أو التنصت عليه .
- الدخول غير المشروع لتهديد أو ابتزاز شخص ، أو لحمله على القيام بفعل أو الامتناع عنه ، ولو كان القيام بهذا الفعل أو الامتناع عنه مشروعاً .
- الدخول غير المشروع إلى موقع إلكتروني أو الدخول إليه بقصد الإتلاف أو التعديل أو شغل عنوانه أو تغيير تصاميم هذا الموقع .
- إساءة استخدام الهواتف النقالة المزودة بالكاميرا ، أو ما في حكمها بما فيه مساس بالحياة الخاصة .

• استخدام وسائل تقنيات المعلومات المختلفة من اجل التشهير بالآخرين وإلحاق الضرر بهم .

٣ . ١ . ٢ الفئة الثانية (المادة ٤)

يندرج تحت هذه الفئة الجرائم المعاقب عليها بالسجن مدة لا تزيد على ثلاث سنوات وبغرامة وهي:

• الاحتيال ، أو اتخاذ اسم كاذب أو انتحال صفة غير صحيحة ، للاستيلاء لنفسه أو لغيره على مال منقول أو على سند أو على توقيع لهذا السند .

• الوصول غير المشروع أو بدون مسوغ نظامي صحيح إلى بيانات بنكية ، أو ائتمانية، أو بيانات متعلقة بملكية أوراق مالية للحصول على بيانات أو معلومات، أو أموال، أو ما تتيحه من خدمات .

٣ . ١ . ٣ الفئة الثالثة (المادة ٥)

وتضم هذه الفئة الجرائم المعاقب عليها بالسجن مدة لا تزيد على أربع سنوات وبغرامة لا تزيد على ثلاثة ملايين ريال ، أو بإحدى هاتين العقوبتين وهي :

• الدخول غير المشروع بقصد إلغاء أو حذف أو تدمير أو تغير أو تسريب بيانات خاصة أو إعادة نشرها .

• تعطيل أو إيقاف الشبكة المعلوماتية عن العمل ، أو تدمير ، أو مسح ، أو حذف، أو تسريب أو إتلاف أو تعديل البرامج أو البيانات أو المستخدمة فيها .

• تعطيل أو تشويش أو إعاقة الوصول إلى الخدمة بأي وسيلة كانت .

٣ . ١ . ٤ الفئة الرابعة (المادة ٦)

وينضوي تحت هذه الفئة الجرائم المعاقب عليها بالسجن مدة لا تزيد على خمس سنوات وبغرامة لا تزيد على ثلاثة ملايين ريال ، أو بإحدى العقوبتين وهي :

- إنتاج أو إعداد أو إرسال أو تخزين عن طريق الشبكة المعلوماتية ما من شأنه المساس بالنظام العام ، أو القيم الدينية ، أو الآداب العامة أو حرمة الحياة الخاصة .
- إنشاء أو نشر موقع على الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي لغرض الاتجار في الجنس والمواد الاباحية .
- إنشاء أو نشر أو ترويج المواد والبيانات المتعلقة بالشبكة الإباحية، أو الأنشطة المخلة بالآداب العامة.
- إنشاء أو نشر موقع على أجهزة الحاسب الآلي، أو على الشبكة المعلوماتية بقصد الاتجار بالمخدرات أو المؤثرات العقلية، أو ترويجها، أو طرق تعاطيها، أو تسهيل التعامل بها .

٣ . ١ . ٥ الفئة الخامسة (المادة ٧)

ويندرج تحت هذه الفئة الجرائم المعاقب عليها بالسجن مدة لا تزيد على عشر سنوات وبغرامة لا تزيد على خمسة ملايين ريال، أو بإحدى هاتين العقوبتين، وهي :

- إنشاء أو نشر موقع على احد أجهزة الحاسب الآلي أو على الشبكة المعلوماتية لمنظمات إرهابية يقصد تسهيل الاتصال بقيادات تلك المنظمات، أو أي من أعضائها، أو تمويلها، أو ترويج أفكارها، أو نشر كيفية تصنيع الأجهزة الحارقة، أو المتفجرات، أو أي أداة تستخدم في الأعمال الإرهابية .
- الدخول غير المشروع عن طريق أحد أجهزة الحاسب الآلي أو الشبكة المعلوماتية إلى موقع إلكتروني، أو نظام معلوماتي مباشرة لغرض الحصول على بيانات تخص الأمن الداخلي والخارجي للدولة، أو اقتصادها الوطني .

٣ . ٢ قانون مكافحة جرائم المعلومات في دولة الإمارات العربية المتحدة

تمهيد

صدر في دولة الإمارات العربية المتحدة أول قانون مختص في مكافحة جرائم تقنية المعلومـــات في الـدول العربيـة فقـد صدر القانون الاتحـادي رقم ٢ السـنة ٢٠٠٦ م . http: / /uaew.maktoobblog.com

وقد تضمن هذا النظام المكون من سبع وعشرين مادة تصنيفاً للجرائم المعلوماتية إلى (٣) فئات حسب العقوبات المقررة لها وتتراوح هذه العقوبات بين السجن والغرامة او بهما معا:

٣ . ٢ . ١ الفئة الأولى : المواد ((٢ فقرة ١) ، ٤ ، ٥ ، ٧ ، ٨ ، ١٤)

وتشمل هذه الفئة مجموعة الجرائم المعاقب عليها بالسجن أو بالغرامة غير المحددتين أو بإحدى هاتين العقوبتين والمتروك للقضاء تحديدها وهي :

- الدخول بغير وجه حق إلى موقع أو نظام معلوماتي .
- تزويـر مسـتند اتحادي أو محلي أو هيئة أو مؤسسـة اتحاديـة معترف بها قانوناً في نظام معلوماتي .
- إعاقـة الوصـول إلى الخدمـة أو الدخـول إلى الأجهـزة أو البرامـج أو مصـادر البيانـات أو المعلومـات بـأي وسـيلة كانـت عن طريـق الشـبكة المعلوماتية أو إحدى وسائل التقنية .
- إتـلاف الفحـوص الطبيـة أو التشـخيص الطبـي أو العلاج الطبـي أو الرعاية الطبيـة، أو مـن سـهل للغير فعل ذلك باسـتعمال الشـبكة المعلوماتية أو إحدى وسائل تقنية المعلومات .
- إنشـاء موقع أو نشر معلومات على الشـبكة المعلوماتية أو إحدى وسـائل تقنية المعلومات بقصد الاتجار بالبشر.

- إنشـاء موقع أو نشر معلومات على الشـبكة المعلوماتية أو إحدى وسـائل تقنية المعلومات بقصد ترويج المخدرات أو المؤثرات العقلية .
- الدخـول بغـير وجـه حق إلى موقع في الشـبكة المعلوماتيـة، لتغيير تصاميم هذا الموقع أو إلقائه أو إتلافه او تعديله أو شغل عنوانه .
- التنصت أو الالتقاط أو الاعتراض عمداً من دون وجه حق على ما هو مرسل عن طريق الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات .

٣ . ٢ . ٢ الفئة الثانية: المواد ((٢ فقرة ٢ / فقرة ٣) ، ٦ ، ٩ ، ١٠)

وتشـمل هذه الجرائم مجموعة الجرائم المعاقب عليها بالسجن مدة لا تقل عن ستة أشـهر ولا تزيد على سـنتين وبغرامة غير محددة أو غرامة لا تقل عن عشرة آلاف درهم ولا تزيد على خمسين ألف درهم أو بإحدى هاتين العقوبتين وهي :

- الدخول إلى موقع أو نظام معلوماتي بغير وجه حق وترتب عليه إلغاء أو حذف أو تدمـير أو إنشـاء أو تغيير أو إعادة نشر بيانـات أو معلومات (الحبس مدة لا تقل عن سـتة اشـهر وبالغرامة أو إحدى هاتين العقوبتين) فإذا كانت البيانات شـخصية تكون العقوبة حبسـاً لا يقل عن سنة وغرامة لا تقل عن عشرة آلاف درهـم ، فإذا وقعت هذه الجريمة بسـبب تأدية العمـل أو أثناءه فيعاقب بحبس سنة وغرامة لا تقل عن عشرين ألف درهم أو بإحدى هاتين العقوبتين .
- إيقـاف الشـبكة أو تعطيلهـا أو تدمـير أو نسـخ أو حذف أو إتـلاف أو تعديل البرامـج أو البيانات أو المعلومات بواسـطة الدخول غير المشروع على الشـبكة أو إحدى وسائل تقنية المعلومات فيعاقب عليها بالسجن المؤقت وبالغرامة التي لاتقل عن خمسين ألف درهم أو بإحدى هاتين العقوبتين .
- اسـتخدام الشـبكة المعلوماتيـة أو إحـدى وسـائل تقنيـة المعلومـات في إيـذاء الأشـخاص لحملهـم عـلى القيـام بأفعـال أو الامتنـاع عنها يعاقـب على ذلك بالحبس مدة لا تزيد على سـنتين وبالغرامة التي لا تزيد على خمسـين ألف درهم أو بإحدى هاتين العقوبتين .

- استخدام الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات في الوصول من دون وجه إلى الاستيلاء لنفسه أو لغيره على مال منقول أو على سند أو توقيع هذا السند ، وذلك بالاستعانة بطريقة احتيالية أو باتخاذ اسم كاذب أو انتحال صفة الغير متى كان ذلك من شأنه خداع المجني عليه يعاقب بالسجن مدة لا تقل عن سنة وبالغرامة التي لا تقل عن ثلاثين ألفاً أو بإحدى هاتين العقوبتين .
- استخدام الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات في الوصول دون وجه حق ، إلى أرقام أو بيانات بطاقة ائتمانية أو غيرها من البطاقات الإلكترونية يعاقب بالحسب وبالغرامة فإن قصد الحصول على أموال الغير أو ما تتيحه من خدمات يعاقب بالحبس مدة لا تقل عن ستة أشهر وبالغرامة أو بإحدى هاتين العقوبتين، وتكون العقوبة الحبس مدة لا تقل عن سنة والغرامة التي لا تقل عن ثلاثين ألف درهم أو إحدى هاتين العقوبتين إذا توصل من ذلك إلى الاستيلاء لنفسه أو لغيره على مال الغير .
- إنتاج أو إعداد أو تهيئة أو إرسال أو تخزين مواد بقصد الاستغلال أو التوزيع أو العرض على الغير عن طريق الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات، من شأنه المساس بالآداب العامة أو أدار مكاناً لذلك، يعاقب بالحبس وبالغرامة أو بإحدى هاتين العقوبتين، فإذا كان الفعل موجهاً إلى حدث فتكون العقوبة الحبس مدة لا تقل عن ستة أشهر والغرامة لا تقل عن ثلاثين ألف درهم .
- الاعتداء على المبادئ والقيم الأسرية أو نشر أخبار تتصل بحرمة الحياة الخاصة أو العائلية للأفراد ولو كانت صحيحة عن طريق شبكة المعلومات أو إحدى وسائل تقنية المعلومات يعاقب بالحبس مدة لا تقل عن سنة وبالغرامة التي لا تقل عن خمسين ألف درهم أو بإحدى هاتين العقوبتين .

٣ . ٢ . ٣ الفئة الثالثة : المواد (٩ ، ١٣ ، ١٥)

وتشمل هذه الجرائم مجموعة الجرائم المعاقب عليها بالسجن مدة لا تقل عن خمس سنوات والغرامة وهي .

- يعاقب بالسجن وبالغرامة من حرض ذكراً أو أنثى أو أغواه لارتكاب الدعارة أو الفجور أو ساعده على ذلك باستخدام الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات. فإذا كان المجني عليه حدثاً كانت العقوبة بالسجن مدة لا تقل عن خمس سنوات .
- يعاقب بالسجن وبالغرامة أو بأحدهما من أساء إلى المقدسات الإسلامية، أو الإساءة إلى المقدسات الأخرى، سب الأديان السماوية المعترف بها أو روج لها وتشدد العقوبة مدة لا تزيد على سبع سنوات إذا تضمنت الجريمة مناهضة للدين الإسلامي أو بشر لغيره .
- تحويل الأموال غير المشروعة أو نقلها أو تمويه المصدر غير المشروع لها أو إخفائه أو استخدام الشرب أو حيازة الأموال مع العلم أنها غير مشروعة أو تحويل الموارد والممتلكات غير المشروعة وذلك باستخدام الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات بقصد إخفاء الصفة المشروعة على تلك الأموال أو إنشاء أو نشر معلومات أو موقع لارتكاب أي من هذه الأفعال كل هذا عقابه مدة لا تزيد على سبع سنوات وبالغرامة التي لا تقل عن ثلاثين ألف درهم ولا تزيد على مائتي ألف درهم .
- السجن مدة لا تزيد على خمس سنوات لكل من أنشأ موقعاً أو نشر معلومات على الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات لأي مجموعة تدعو لتسهيل وترويج برامج وأفكار من شأنها الإخلال بالنظام العام والآداب العامة .
- قيام جماعة إرهابية تحت مسميات تمويهية بإنشاء مواقع أو نشر معلومات على الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات لتسهيل الاتصال بقياداتها، أو أعضائها أو ترويج أفكارها أو تمويلها أو نشر كيفية تصنيع الأجهزة الحارقة، أو المتفجرة، أو أي أدوات مستخدمة في الأعمال الإرهابية، فالعقاب الحبس مدة لا تزيد على خمس سنوات .
- السجن للدخول بغير وجه إلى موقع أو نظام مباشرة أو عن طريق الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات بقصد الحصول على بيانات أو

معلومـات حكومية سرية إما بتطبيقها أو بمقتضى تعليمات صادرة بذلك ، فإذا ترتـب عـلى الدخول إلغاء تلك البيانات أو المعلومات أو إتلافها أو تدميرها أو نشرها تكون العقوبة السجن مدة لا تقل عن خمس سنوات ، ويسري ذلك على البيانات والمعلومات الخاصة بالمنشآت المالية والمنشآت المالية الأخرى التجارية والاقتصاديـة . حدد النظـام كذلك الإجراءات لمصادرة الأجهزة أو الوسـائل المستخدمة في ارتكاب الجريمة المستعرض عليها بهذا القانون أو الأموال المتصلة بهـا ، وكذلـك الحكـم بإغلاق المحلات أو المواقع التـي يرتكب بها أي من هذه الجرائم ، وكما حدد النظام انه بالإضافة إلى العقوبات المسـتعرض عليها في هذا القانون تقضي المحكمة بإبعاد الأجنبي الذي يحكم عليه بالسجن . وحدد النظام كذلك انه لا يخل تطبيق العقوبات المستعرض عليها في هذا القانون بأي عقوبة اشد ينص عليها في قانون العقوبات أو أي قانون آخر .

٣ . ٣ قانون سلطنة عمان لمكافحة جرائم الحاسب الآلي

تمهيـــــد

أصـدرت سـلطنة عمان جملة مـن التشريعات لمكافحـة الجريمـة المعلوماتية قانون سلطنة عمان لمكافحة جرائم الحاسب الآلي ، فقد صدر المرسوم السلطاني رقم (٧٢) لسنة ٢٠٠١م بشأن تعديل بعض أحكام قانون الجزاء العماني ليشمل معالجة جرائم الحاسب الآلي (الكمبيوتـر) وذلـك بإضافة فصل في الباب السـابع من قانون الجزاء العماني تحت عنوان [جرائم الحاسب الآلي] واشتمل هذا الفصل على خمس مواد [٢٦٧ مكررة، ٢٦٧ مكرر١، ٢٦٧ مكرر٢، ٢٦٧ مكرر٣ و ٢٦٧ مكرر٤] وهي جميعا مستحدثة . وكذلك أضيفت مواد إلى قانون الاتصالات العماني تحرم تبادل رسائل تخدش الحياء العام وتحرم استخدام أجهزة الاتصالات للإهانة أو الحصول على معلومات سرية أو إفشاء الأسرار أو إرسال رسائل تهديد ، وأسست السلطنة قانوناً ينظم المعاملات الحكومية الإلكترونية والتوقيع الإلكتروني وحوادث اختراق الأنظمة وفيما يلي بيان لما ورد في المادة (٢٧٦) من قانون الجزاء العماني فيما يتعلق بعقوبات جرائم الحاسب الآلي والشبكة العالمية :

٣ . ٣ . ١ الأعمال المجرمة في هذا القانون: جرم القانون العماني ١٠ جرائم في المادة ٢٦٧ مكرر ١ هي :

الالتقاط غير المشروع للمعلومات أو البيانات، والدخول غير المشروع على أنظمة الحاسب الآلي ، والتجسس والتنصت على البيانات والمعلومات، وانتهاك خصوصيات الغير أو التعدي على حقهم في الاحتفاظ بأسرارهم، وتزوير بيانات أو وثائق مدمجة أياً كان شكلها . وإتلاف وتغيير ومحو البيانات أو استخدامها وتسريب المعلومات والبيانات والتعدي على برامج الحاسب الآلي بما يشكل انتهاكاً لقوانين حقوق الملكية والأسرار التجارية ، كما جرمت المادة ٦٧٢ مكرر ١ الاستيلاء على البيانات المنقولة أو المخزنة أو المعالجة بواسطة أنظمة المعالجة المبرمجة للبيانات. ومما بحثت المادة ٦٧٢ مكرر ٤ ثلاث صور من صور إساءة استخدام بطاقة الوفاء الإلكترونية وجرمت عمليات سيول الدفع ببطاقة مزورة أو مسروقة واستخدام بطاقات بعد انتهاء صلاحيتها، تزوير البطاقات الائتمانية وبطاقات السحب الآلي، استعمال بطاقة في غير المراد عمله وتصل عقوبة مثل هذه الجرائم إلى غرامة تصل إلى خمسمائة ريال عماني كما جاء في الفصل التاسع من نظام التعاملات الإلكتروني .

كما صدر قانون المعاملات الإلكتروني لسلطنة عمان وفق المرسوم السلطاني رقم ٢٠٠٨/٦٩م وقد شمل الفصل التاسع عقوبات لعدد من جرائم الحاسب الآلي كما يلي:

٣ . ٣ . ٢ المادة(٥٢)

مع عدم الإخلال بأي عقوبة أشد ينص عليها قانون الجزاء العماني أو أي قانون آخر، يعاقب بالسجن لمدة لا تتجاوز سنتين وبغرامة لا تتجاوز – ٥٠٠٠ر.ع (خمسة آلاف ريال عماني) أو بإحدى هاتين العقوبتين كل من:

تسبب عمداً في تعديل غير مرخص به في محتويات أي حاسب آلي بقصد إضعاف أو منع أو تعويق الدخول إلى أي برنامج أو بيانات محفوظة فيه أو إضعاف فاعلية ذلك البرنامج أو إضعاف الاعتماد على تلك البيانات إذا تم ذلك التعديل بإحدى الطرق الآتية:

أ ـ شطب أي برنامج أو بيانات محفوظة في الحاسب الآلي.

ب ـ إضافة أي برنامج أو بيانات إلى محتويات الحاسب الآلي.

ج ـ أي فعل يسهم في إحداث ذلك التعديل.

اخترق جهاز حاسب آلي أو منظومة حاسبات آلية أو موقع على الإنترنت أو شبكة إنترنت وترتب على ذلك:

١ ـ تعطيل أنظمة تشغيل جهاز الحاسب الآلي أو منظومة الحاسبات الآلية.

٢ ـ إتلاف برامج الحاسب الآلي أو الحاسبات الآلية وما تحتويه من معلومات.

٣ ـ سرقة المعلومات.

٤ ـ استخدام المعلومات التي تتضمنها مخرجات الحاسبات الآلية في أغراض غير مشروعة.

٥ ـ اختراق نظام معلوماتي والقيام بما يلي:

أ ـ دخل بطريق الغش إلى نظام معلومات أو قاعدة بيانات بغرض العبث بالتوقيعات الإلكترونية.

ب ـ قام بطرق غير مشروعة بكشف مفاتيح لفض التشفير أو فض تشفير معلومات مودعة لديه.

ج ـ استعمل بصفة غير مشروعة عناصر تشفير شخصية متعلقة بتوقيع غيره.

د ـ اخترق أو اعترض معلومات أو بيانات مشفرة أو قام بفض شفرتها عمداً دون مسوغ قانوني، وتضاعف العقوبة إذا كانت المعلومات أو البيانات تتعلق بسر من أسرار الدولة.

هـ ـ قام عمداً بفض معلومات أو بيانات مشفرة بأي طريقة في غير الأحوال المصرح بها قانونا.

و ـ قام عمداً بإنشاء أو نشر شهادة زور بمعلومات إلكترونية غير صحيحة لغرض غير مشروع.

ز ـ قـدم بيانات غير صحيحة عـن هويته أو تفويضه لمقدم خدمات التصديق بغرض طلب إصدار أو إلغاء أو تعليق شهادة.

ح ـ قام عمداً ـ بغير سند قانوني ـ بكشف بيانات سرية تمكن من الوصول إليها بما له من سلطات بموجب هذا القانون أو أي قانون آخر.

ط ـ مارس نشاط مقدم خدمات تصديق بدون ترخيص.

ي ـ استعمل بصفة غير مشروعة أداة إنشاء توقيع متعلقة بتوقيع شخص آخر.

ك ـ قام بالدخول غير المشروع إلى حاسب آلي بقصد ارتكاب جريمة أو تسهيل ارتكاب جريمة أو بواسطة شخص آخر.

ل ـ زور سجلاً إلكترونيا أو توقيعا أو استعمل أيا من ذلك مع علمه بتزويره.

م ـ قـام عمـداً بطريقة غير مشروعة بنشر أو تسـهيل نشر أو اسـتعمال سـجل إلكـتروني أو فض شـفرته. وتضاعف العقوبـة إذا كان مرتكب الجريمة أميناً على ذلك السجل أو التوقيع بمقتضى مهنته أو وظيفته.

٣ . ٣ . ٣ المادة (٥٣)

مـع عدم الإخلال بأي عقوبة أشـد ينص عليها قانـون الجزاء العماني أو أي قانون آخر يعاقب بالسجن لمدة لا تتجاوز سنة واحدة وبغرامة لا تتجاوز-١٥٠٠ر.ع. (ألف وخمسمائة ريال عماني) أو بإحدى هاتين العقوبتين.

كل من صنع أو حاز أو حصل على نظام معلومات أو برنامج لإنشاء توقيع إلكتروني دون موافقة صاحب ذلك التوقيع صراحة.

كل صاحب مفتاح تشـفير رفض تسـليمه للموظف الذي تحدده السلطة المختصة بعد الإفصاح عن هويته.

كل مقدم خدمات تصديق أو أحد العاملين لديه رفض تقديم تسـهيلات للسـلطة المختصة أو لأي من موظفيها للقيام بالمراقبة أو الإشراف أو التفتيش على أي نظام حاسب

آلي أو جهاز بيانات أو مواد أخرى متصلة بنظام الحاسب الآلي بمقر خدمات التصديق. وأشـارت المادة ٤٥ إلى أنه في حالة الإدانة بموجب أحكام هذا القانون، تحكم المحكمة بالإضافة إلى أي عقوبة أخرى بمصادرة الأدوات التي استعملت في ارتكاب الجريمة.

٤ . القانون الدولي المقترح

يتناول هذا الجزء مكونات القانون الدولي المقترح في هذه الدراسة مستفيدا في ذلك مـن المصادر التالية : مفردات وبنود ومواد مختـارة من القوانين الوطنية لمكافحة الجرائم المعلوماتيـة في بلـدان العالم التي سـنت قوانين في هذا الصدد، المصدر الثاني هو ما يمكن الاسـتفادة منـه من مواد مختارة مـن الاتفاقيات والمعاهدات الاقليميـة والدولية التي لها علاقـة وثيقـة بمكافحة الجرائم المعلوماتية، فضلا عما يمكن ان يسـهم به خبراء القانون الـدولي وخـبراء قوانين مكافحـة الجرائم المعلوماتية المنوط بهم صياغـة هذا القانون من قبـل هيئـة الامم المتحده كمصدر ثالـث، أما المصدر الرئيس والاهـم وهو ما يمكن ان يكـون الإطار الرئيس لهذا القانون المقترح فهو اتفاقية مجلس اوروبا لجرائم الحاسـوب. صحيح ان هناك مصادر متعددة لسن مثل هذا القانون ، الاانني في بلورة مقترحي هذا، كان اعتمادي على اتفاقية مجلس اوروبا لجرائم الحاسوب كان أكبر من غيره لاسباب لعل أهمها: يمثل هذا القانون ست واربعين دولة أوروبية، وهي تمثل ٢٥٪ من عضوية هيئة الامم المتحدة، كما انها كانت الاسبق لجميع دول العالم في سنها لقانون اطاري موحد لهذه الظاهرة. ليس ذلك فحسب بل انها متقدمة على سواها تاريخيا وحضاريا في صياغة قوانين مماثلـة والتعامـل القانوني مع قضايا من هذا القبيل ، لربما بسـبب ثراء تجربتها وتعرضها لمشكلات ومعضلات مثل الحرب العالمية الاولى والثانية ، ما أذكى عندها الحس القانوني المبكر لمثل هذا النوع من الجرائم. وبالرغم من ان المجلس يحمل اسـم مجلس أوروبا بيد أن باب العضوية مفتوح لأي دولة من القارات المختلفة بدلالة أن اليابان وامريكا وكندا وبعـض دول امريكا الجنوبية وافريقيا قد حصلـت على عضوية المجلس. ويجدر بالذكر ان القانون الاسترشـادي الاوروبي لمجلس أوروبا وفر إطاراً قانونياً ملزماً لكافة الدول الاعضاء شريطة أن يراعى في سن تلك القوانين الحد الادنى من العقوبة. ولافت للانتباه ان المجلس قد نجح في توحيد مصطلحات الجريمة المعلوماتية وتعريفاتها ما يعد خطوة متقدمة في سبيل مكافحة الجريمة المعلوماتية.

٤ . ١ اتفاقية مجلس أوروبا لجرائم الحاسوب http: / /www.c /cisac.html

تأسس مجلس أوروبا في العام ١٩٤٩ م ويتكون من ٤٦ دولة ، من دول الاتحاد الأوروبي وعدد آخر من الدول من خارج القارة ، الولايات المتحدة وكندا واليابان وغيرها من دول أمريكا اللاتينية مراقبين. يقوم هذا المجلس بدور مهم في محاولة الحد من جرائم الحاسب الآلي من خلال إقراره للعديد من التوصيات الخاصة لحماية البيانات من سوء الاستخدام وكذلك حماية تدفق المعلومات وحماية الأشخاص في مواجهة المعالجة الإلكترونية للبيانات ذات الصفة الشخصية ، واصدر هذا المجلس العديد من القواعد التوجيهية في جرائم الحاسب الآلي و جرمت العديد من السلوكيات كالغش وتزوير المعلومات وسرقة الأسرار المخزنة والدخول غير الشروع لسرقة منافع الحاسب الآلي وغيرها (عبابنة، ٢٠٠٦).

صادقت دول مجلس أوروبا على اتفاقية بودابست للجرائم الإلكترونية في عام ٢٠٠١م . والتي تعد أول اتفاقية دولية شاملة تتعلق بجرائم الحاسب الآلي ، والجرائم التي ترتكب عبر شبكة الإنترنت وأجهزة تقنية المعلومات الأخرى، وكان الهدف من هذه الاتفاقية وضع سياسة جنائية مشتركة بين دول المجلس تهدف إلى حماية ممتلكاته من الجريمة الإلكترونية من خلال اعتماد التشريعات الملائمة وتقرير التعاون الدولي، آخذة بعين الاعتبار جميع التوصيات السابقة لهذه الاتفاقية والمتعلقة بجرائم الحاسب الآلي وبالمشاكل التي تعيق قوانين الإجراءات الجنائية في مجال جرائم الحاسب الآلي، كما أخذت بعين الاعتبار مؤتمر براغ في العام ١٩٩٧ م الذي دعا إلى ضرورة دعم اللجنة الأوروبية المختصة بمشاكل جرائم الحاسب الآلي (CDPC) وكذلك ما صدر عن قمة ستراسيورغ في نفس العام وما صدر عنها فيما يتعلق بمدى التجاوب العام بين دول المجلس مع تكنولوجيا المعلومات الحديثة المؤسسة على معايير ومقاييس المجلس وتتكون هذه الاتفاقية من ٤٨ مادة في أربعة فصول نستعرضها كما يلي :(www.stanford.edu)

٤ . ١ . ١ الفصل الأول

ويتكون من مادة واحدة حدد فيها عدد من المصطلحات الواردة في هذه الاتفاقية

كتعريف نظام الحاسب الآلي بأنه : أي جهاز أو مجموعة من الأجهزة ذات العلاقة والمرتبطة ببعضها والذي يعالج واحدة منها أو أكثر البيانات وتشغيل البرامج ، كما أنها تطرقت إلى بيانات الحاسب الآلي بأنها أي تمثيل للحقائق والمعلومات جهزت بطريقة ملائمة للمعالجة في أي نظام حاسب آلي وعرج كذلك على تعريف مقدمي الخدمة بأنها هيئة عامة أو خاصة تزود مستخدميها بخدمة تبادل الاتصالات الإلكترونية عبر شبكة الإنترنت، وتطرق كذلك لتعاريف الشبكة المعلوماتية وحركة البيانات فيها .

٤ . ١ . ٢ الفصل الثاني : التدابير المستخدمة على الصعيد الوطني لدول المجلس

يتكون هذا الفصل من ٧ أقسام تحتوي على سبع وعشرين مادة، خصص هذا الفصل من الاتفاقية للإجراءات الواجب اتخاذها من قبل أعضاء المجلس على المستوى الوطني، القسم الأول من هذا الفصل يتعلق بالتأكيد على بناء قوانين وتشريعات وأنظمة رادعة لمنع الاعتداءات على أنظمة وشبكات الحاسب وذلك على المستوى الوطني لكل دولة ، كما أشارت الاتفاقية إلى وجوب إضافة نصوص قانونية للقوانين الوطنية لمحاربة اعتراض البيانات عبر شبكات الحاسب وكذلك اعتراض البث الكهرومغناطيسي للبيانات أو إتلافها وإتلاف أنظمة الحاسب الآلي وتعطيل أنظمته . وفي القسم الثاني أوجب على دول المجلس أن تدرج في تشريعاتها ما يحدد عقوبة لجريمتي التزوير والاحتيال عن طريق الحاسب الآلي وترك الباب مفتوحاً لكل دولة في حرية تنظيم مسألة القصد الجرمي بخصوصه . أما القسم الثالث من هذا الفصل فخصص لجريمتي الاعتداء على محتويات الحاسب الآلي وشبكات المعلومات والإنترنت وكذلك الاعتداءات بواسطة الحاسب الآلي وشبكات الإنترنت وتقنية المعلومات على الأحداث من نشر صور إباحية أو إغواء ووجوب تجريم مثل هذه الأفعال في كافة قوانين دول المجلس ويترك تعريف سن الحدث لكل دولة حيث إنه لا يتجاوز الثامنة عشرة .

وخصص القسم الرابع من هذا الفصل لحقوق النسخ والاعتداءات المتصلة بها ووجوب تبني دول المجلس في تشريعاتها نصوصاً رادعة لإعادة إنتاج وتوزيع أي مواد محمية بقوانين حماية الملكية من خلال الاعتداءات التي يمكن أن تقع عليها بواسطة الحاسب الآلي .

وخصص القسم الخامس من هذا الفصل للمساهمة والمسؤولية والعقوبات [Ancillary, Liability and Sanction] . حيث ركز هذا القسم على وجوب معاقبة الشروع في هذه الجرائم وعقاب المساهم في ارتكابها ، وكذلك مسؤولية المساهمة حيث يتوجب معاقبة الأشخاص أو المؤسسات التي ترتكب الجريمة لمصلحتهم ويشرط أن يكون مرتكب الجريمة ممثلاً قانونياً للمؤسسة ، ويملك سلطة اتخاذ القرار ، إذا تم ارتكاب الجريمة بتكليف منهم ، وبالنسبة للعقاب على هذه الجرائم أشارت إلى أن العقوبات التي تفرض على مرتكبي الجرائم يتوجب أن تكون من العقوبات السالبة للحرية والغرامات .

أما نهاية هذا الفصل من الاتفاقية فلقد تم تخصيصها لقانون الإجراءات (Procedural Law) حيث نظمت أحكام التفتيش ومصادرة معلومات الحاسب الآلي المخزنة التي تفيد في التحقيق، ونظمت الأحكام الخاصة بالتعاون مابين دول المجلس في مجال التحقيق وتبادل المعلومات وتقديم المساعدة .

٤ . ١ . ٣ الفصل الثالث : التعاون الدولي

خصص هذا الفصل من الاتفاقية للتعاون الدولي (International Cooperation) حيث تم استعراض عدة مبادئ تلزم دول المجلس بوجوب التعاون في اتخاذ الإجراءات والتشريعات الكفيلة بتحقيق التعاون الكامل وتطبيق التشريعات الدولية فيما يتعلق بمجالات التحقيق في الجرائم الإلكترونية كسرقة البيانات واعتراضها وإتلافها وتعطيل أنظمة الحاسب وتدمير المواقع ومهاجمتها على الإنترنت، وكافة جرائم الحاسب المعروفة والمصنفة قانونياً لدى كل دولة، كما الزم دول المجلس بجمع وتبادل الأدلة الإلكترونية وكذلك الالتزام بمعاهدات تسليم المجرمين، وركزت كذلك على حتمية التعاون المتبادل وتبادل المعلومات إذا كانت تحت سلطة دولة من دول المجلس ومخزنة ضمن نطاقها وتسليم المعلومات عند طلبها .

ووجوب التزام كل طرف بتعيين نقطة اتصال على مدار الساعة وفي أيام العطل لاستقبال طلبات التحقيق في الاعتداءات التي تطال معطيات الحاسب الآلي والمعلومات أو لجمع الأدلة الإلكترونية . تعد هذه الاتفاقية بمثابة القانون بين الدول الأعضاء والتي

وبموجبها تلتزم الدول الأعضاء في المجلس بضرورة العمل على تنفيذ أحكامها والخضوع لها واحترام تنفيذها وتطويع النصوص القانونية بالشكل الذي يضمن عدم التعارض مع أحكامها وتلزم هذه الاتفاقية لسن الحد الأدنى من القوانين الضرورية للتعامل مع جرائم التقنية العالمية وجميع جرائم الحاسب الآلي المعروفة .

٤ . ١ . ٤ الفصل الرابع : أحكام ختامية للاتفاقية

خصص هذا الفصل لتحديد قواعد وإجراءات التوقيع على الاتفاقية واعتبارها مفتوحة لغير الأعضاء للانضمام إليها ، كما حددت نطاق تطبيق هذه الاتفاقية والآثار المترتبة عليها . كما أوضحت بشكل لا يقبل الشك مواضيع التحفظات وسحبها من قبل أعضاء المجلس ، وكذلك التعديلات المراد إجراؤها على الاتفاقية ، حددت كذلك إجراءات تسوية المنازعات ، والانسحاب من هذه الاتفاقية ، وقد اعتمد المجلس اللغتين الإنجليزية والفرنسية واعتماد النصين متساويين في الحجية ، في نسخة واحدة تودع في محفوظات مجلس أوروبا ، وترسل نسخة لكل عضو في مجلس أوروبا وكذلك الدول غير الأعضاء المنظمة للاتفاقية وتركت الباب مفتوحاً للانضمام لأي دولة من دول العالم .

٥ . خلاصة الدراسة وأهم نتائجها وتوصياتها

٥ . ١ خلاصة الدراسة

اشتملت هذه الدراسة على خمسة أجزاء بالإضافة الى المراجع ، وغطى الجزء الاول كمدخل للدراسة،أسباب اختيارموضوع الدراسة، ومشكلة الدراسة واهميتها واهدافها والتساؤلات التي تجيب عنها، واهم المصطلحات التي استخدمها الباحث في دراسته ومنهجية الدراسة، وعرض الباحث في الجزء الثاني الإطار النظري المشتمل لبعض القوانين والمعاهدات والاتفاقيات الدولية التي دارت حول موضوع الدراسة. أماالجزء الثالث فقد تناول فيه الباحث قوانين مكافحة الجريمة المعلوماتية لثلاث دول هي المملكة العربية السعودية ودولة الإمارات العربية المتحدة وسلطنة عمان. تم عرض هذه القوانين الثلاثة وايضاح أوجه التشابه والاختلاف بينها.أما الجزء الرابع فقد تناول الباحث

مكونـات النظـام الدولي المقترح، والذي حدد مكوناته بأربعة مصادر رئيسـة هي اتفاقية مجلس أوروبا لجرائم الحاسـوب، ومواد مختارة من قوانين وطنية تم سـنها والعمل بها من قبل بعض دول العالم، إضافة الى مواد مختارة ومناسـبة وذات علاقة بالموضوع وردت في المعاهدات والمواثيق الدولية الخاصة بمكافحة جرائم المعلومات، يضاف الى هذه المصادر مايمكن أن يقدمه خبراء الفريق المتخصص بسن هذا القانون. أما الجزء الخامس والأخير في هذا فيه البحث فيعرض فيه الباحث خلاصة الدراسة وأهم نتائجها وتوصياتها.

٥ . ٢ النتائج

اسـتنتج الباحـث وجود قوانين وطنية لمكافحة الجرائـم المعلوماتية ، هذه القوانين حديثة ومستقلة ،وليست جزءا من قوانين أخرى. واستنتج كذلك وجود قوانين وطنية لمكافحـة الجرائم المعلوماتيه عبـارة عن قوانين جزئية من قوانين مكافحة الجريمة وهذه هي الغالبية العظمى من قوانين مكافحة هذه الجريمة. واسـتنتج الباحث وجود تفاوت بين هذه القوانين من دولة لاخرى. فقوانين مملكة الدنمارك تنص على الغرامة والسـجن لمدة تصل إلى سـتة أشـهر لمنتهك أنظمة المعلومات بدون إذن شرعي، بينما تعاقب قوانين مكافحة الجريمة الإلكترونية في جمهورية أيرلندا منتهك أنظمة المعلومات بدون إذن بغرامة ماليه قدرها ٥٠٠ جنيه أو السجن لمدة لا تتجاوز ثلاثة اشهر، وفي اليابان يعاقب منتهك أنظمة المعلومات بغرامة تصل ٥٠٠٠ ين أو السـجن خمس سـنوات، وفي هونج كونج يعاقـب مـن يصل للمعلومات المخزنة بالحاسـب الآلي من غير إذن بدفـع غرامة قدرها ٢٠٠٠٠ دولار أمريكي ، والسـجن خمس سنوات . وفي أستراليا سنت قوانين لمكافحة الجريمـة الإلكترونية لحماية المعلومات عبر الشـبكة ، وعاقبت منتهك أنظمة المعلومات من غير إذن بالسـجن لمدة سـتة أشهر. وينص نظام مكافحة الجريمة المعلوماتية الكندي عـلى معاقبـة منتهك أنظمة المعلومات بعقوبة السـجن لمدة لا تتعدى عشر سـنوات . في حين نجد في القوانين الأمريكية يقترن فعل الاتصال بدون تصريح مع تحقيق نتائج محددة كالحصـول على المعلومات أو اسـتخدام النظام أو إتـلاف المعطيات، أما قانون مكافحة الجريمـة الإلكترونية الفرنسي فيعاقب من قام بالتحايل على أنظمة المعلومات بالسـجن لمـدة تصـل للسـنة وغرامة قدرهـا ١٠٠٠٠٠ فرنك فرنـسي، ويجرم هـذا القانون مجرد

التوصل مع نظام الحاسوب أو البقاء فيه . 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 الاعتداء على أنظمة المعلومات بالسجن لمدة تصل إلى ثلاث سنوات ، وبغرامة لا تتعدى ٢٠٠٠٠ روبية أوبهما معا. مثل هذه التناقضات وجدت في قوانين دول أخرى مثل اليونان ، وجنوب أفريقيا ، وسنغافورة واسبانيا وسويسرا والنرويج وبولندا والبرتغال. وتنص المادة الخامسة من نظام مكافحة الجرائم المعلوماتية في المملكة العربية السعودية على أنه يعاقب بالسجن مدة لا تزيد على أربع سنوات وبغرامة لا تزيد على ثلاثة ملايين ريال أو بإحدى هاتين العقوبتين لكل شخص يرتكب الجريمة المعلوماتية التالية: الدخول غير المشروع لإلغاء بيانات خاصة أو حذفها أو تدميرها أو تسريبها، أو إتلافها أو تغييرها أو إعادة نشرها. القوانين الوطنية السابقة سن أغلبها 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 جسيمة . 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، وبرغم صدور عدد من التشريعات بشأن حماية الملكية الفردية والصناعية التي تضمنت النص على برامج الحاسب الآلي وعدتها من ضمن المصنفات.

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 ، وتعد أول ثلاثة قوانين عربية تصدر بشكل مستقل لمواجهة الجرائم المعلوماتية وتميزت بما يلي:

- 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 ثلاث دول من دول الخليج العربي وما به من مميزات، لم يمنع من وجود عيوب وقصور يتمثل 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. فعلى سبيل المثال قانون المعاملات الإلكتروني العماني تعامل مع ١٦ نمطاً من الجرائم المعلوماتية وقرر لها عقوبة سالبة للحرية وهي السجن لمدة لا تتجاوز سنتين وبغرامة لا تتجاوز خمسة آلاف ريال عماني ، أو بإحدى هاتين العقوبتين وهي الاعتداء على النظم المعلوماتية، الاختراق، الاعتداء على التوقيع الإلكتروني، إفشاء الأسرار، الاعتداء على البيانات والتزوير الإلكتروني، سرقة المعلومات. أما القانون الإماراتي لمكافحة الجرائم المعلوماتية وفي المادة (٢٢) يعاقب بالسجن كل من دخل وبغير وجه حق موقعاً أو نظاماً مباشرة أو عن طريق الشبكة المعلوماتية أو إحدى وسائل حكومية سرية إما بطبيعتها أو بمقتضى تعليمات صادرة بذلك، فإذا ترتب على الدخول إلغاء تلك البيانات أو المعلومات أو إتلافها أو تدميرها أو نشرها، تكون العقوبة السجن مدة لا تقل عن خمس سنوات ويسري حكم هذه المادة على البيانات والمعلومات الخاصة بالمنشآت المالية والمنشآت الأخرى والتجارية والاقتصادية يقابل هذه المادة المادتان الرابعة والخامسة من نظام مكافحة الجرائم المعلوماتية السعودي، الجرائم المعاقب عليها بالسجن مدة لا تزيد على ثلاث سنوات وبغرامة لا تزيد على مليوني ريال، أو بإحدى هاتين العقوبتين لجرائم الاحتيال أو اتخاذ اسم كاذب أو انتحال صفة غير صحيحة،

للاستيلاء لنفسه أو لغيره على مال منقول أو على سند وكذلك الوصول غير المشروع أو بدون مسوغ نظامي صحيح إلى بيانات بنكية، أو ائتمانية، أو بيانات متعلقة بملكية أوراق مالية للحصول على بيانات أو معلومات أو أموال، أو ما تتيحه من خدمات، أما المادة الخامسة فيندرج تحتها الجرائم المعاقب عليها بالسجن مدة لا تزيد على أربع سنوات وبغرامة لا تزيد على ثلاثة ملايين ريال أو بإحدى هاتين العقوبتين لجرائم الدخول غير المشروع بقصد إلغاء أو حذف أو تدمير أو تقصير أو تسريب بيانات خاصة وتعطيل الشبكة المعلوماتية أو تدمير أو خرق أو تسريب أو إتلاف أو تعديل البرامج أو إعاقة الوصول إلى الخدمة.

أما في قانون مكافحة الجرائم المعلوماتية الاماراتي فتنص المادة ٢١ على ان كل من أنشأ موقعاً أو نشر معلومات على الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات لجماعة إرهابية تحت مسميات تمويهية لتسهيل الاتصال بقياداتها، أو أعضائها، أو ترويج أخطارها، أو تمويلها، أو نشر كيفية تصنيع الأجهزة الحارقة، أو المتفجرة، أو أي أدوات تستخدم في الأعمال الإرهابية يعاقب بالحبس مدة لا تزيد على خمس سنوات، يقابلها المادة السابعة من قانون مكافحة الجرائم المعلوماتية السعودي والتي تعاقب بالسجن مدة لا تزيد على عشر سنوات وبغرامة لا تزيد على خمسة ملايين ريال، أو بإحدى هاتين العقوبتين، وهي إنشاء أو نشر موقع على أحد أجهزة الحاسب الآلي أو على الشبكة المعلوماتية لمنظمات إرهابية بقصد تسهيل الاتصال بقيادات تلك المنظمات أو أي من أعضائها، أو تمويلها، أو ترويج أخطارها أو نشر كيفية تصنيع الأجهزة الحارقة، أو المتفجرات أو أي أداة تستخدم في الأعمال الإرهابية. بقراءة هذه المواد في القانونين السعودي والإماراتي لمكافحة الجرائم المعلوماتية يلاحظ أن صياغتها متشابهة الى حد كبير والاختلاف الوحيد هو في العقوبة حيث إن العقوبة في النظام السعودي هي ضعفا نفس العقوبة في نفس المادة في قانون الإمارات، كما انه لا يوجد أي تنسيق أو إطار قانوني يجمع هذه القوانين الثلاثة، و ليس هناك مكاتب ارتباط لجهات التحقيق في هذه الجرائم ولا تبادل معلومات أو تبادل مجرمين من هذا النوع، كما اتضح عدم وجود أي مواد تحث على التنسيق والتعاون الدولي.

٥ . ٣ التوصيات

خلص الباحث إلى أن مجلس أوروبا المكون من ست وأربعين دولة هو التجمع الأكبر في العالم بأسره الذي استطاع التوصل الى اتفاقية إطارية موحدة لمكافحة الجريمة المعلوماتية، تحت مسمى الاتفاقية الاسترشادية لمجلس أوروبا (اتفاقية مجلس أوروبا لجرائم الحاسب)، وأصبحت هذه الاتفاقية مظلة للقوانين الوطنية في هذا الجزء من العالم، وحتى تلك الدول الأعضاء في الاتحاد والتي لم يتسن لها وضع قوانينها الخاصة، طلب إليها سن قوانين لمكافحة الجريمة المعلوماتية الخاصة بها وملزمة لشروط الانضمام إلى اتفاقية مجلس أوروبا الذي أرتأته دول المجلس. كما ظهر جلياً قلة الدول التي نجحت في سن قوانين وطنية لمكافحة الجريمة الإلكترونية ولا أدل على صحة ما أوردناه من أن هناك ثلاث دول عربية فقط (السعودية، الإمارات وعمان) من بين ٢٢ دولة عربية هي التي سنت قوانين من هذا النوع. وكما جاء بيانه من أن هذه القوانين مستقلة وتفتقر إلى إطار يجمعها، وما يؤسف له أن كل دولة من هذه الدول الثلاث سنت قوانينها بمعزل عن الأخرى فهي قوانين محلية وتفتقر إلى إطار يجمعها، وعلى الموال نفسه قس على ذلك دول العالم المختلفة التي وضعت قوانين لمجابهة هذا النوع من الجرائم.

وهذه الاستقلالية في وضع القوانين برهنت بوضوح على الغياب التام للتنسيق وتبادل الخبرات وبلورة أنجع الأفكار في هذا المجال الحيوي.

وبالطبع لو كان هناك وجود ــ ارتباط واتصال بين الدول أو أن تعاوناً دولياً كان قائماً بين الدولة التي سنت قانوناً وبقية دول العالم ــ لأضحى ذلك القانون أكثر فعالية وذا إمكانية تطبيقية أكبر، ويعود هذا في المقام الأول إلى الطبيعة الخاصة للجريمة المعلوماتية إذ أنها عالمية الطبع وعابرة للحدود (Transnational) والحال هذا فلا مناص من سن قانون دولي موحد ملزم لكافة الدول إذا كان للعالم أجمع أن يكافح هذا النوع الخطير من الجرائم.

والحق يقال أن مثل هذا القانون الدولي الموحد لو كتب له أن يصبح واقعاً فإنه سوف يمثل إطاراً قانونياً عاماً يستوعب قوانين وطنية أو حتى إقليمية تشمل كافة الدول

ومنظومات الدول (الجامعة العربية) (الاتحاد المغاربي)، (الاتحاد الإفريقي)، (مجلس التعاون الخليجي) ...إلخ).

وترتيباً على ما سبق فإن الباحث في سعيه لتحقيق الهدف الرئيس لعمله هذا ألا وهو سن قانون دولي موحد رأى أن لا ضرورة لأن تكون البداية من الصفر وإنما يتوجب على كل الدول ولربما تحت راية الأمم المتحدة قبول القانون الاسترشادي لمجلس أوروبا وتوسيعه والتأسيس عليه بحيث يتم التوصل للقانون الدولي الموحد الملزم للجميع. وبالطبع فإن التطبيق السليم والشفاف للقانون المذكور سوف يقلص أعداد الجرائم الإلكترونية على آثارها السالبة. فإذا وضعنا في الاعتبار كل المزايا التي سبق ذكرها لتأكد لنا سلامة المقترح الذي أكد عليه الباحث آنفاً ألا وهو تبني القانون الاسترشادي لمجلس أوروبا كأساس لقانون دولي موحد لمكافحة الجريمة المعلوماتية تحت مظلة الأمم المتحدة. هذا وقد توصل الباحث إلى هذا المقترح الذي هو أيضاً نتيجة رئيسة لهذه الدراسة من خلال عرضه ومناقشته لثلاثة محاور أساسية ألا وهي:

١ ـ المسح والعرض بصورة عامة لعدد من القوانين الوطنية والاتفاقيات والمعاهدات الخاصة بمكافحة الجريمة المعلوماتية.

٢ ـ المسح والعرض المفصل لقوانين ثلاث دول عربية لمكافحة الجريمة المعلوماتية والدول الثلاث هي: دولة الإمارات العربية المتحدة، المملكة العربية السعودية، سلطنة عمان.

٣ ـ عرض ومناقشة للقانون الاسترشادي لمجلس أوروبا.

المراجع

المراجع العربية:

أحمد، هلال(١٩٩٧).تفتيش نظم الحاسب الآلي، دار النهضة العربية ،القاهرة.

البقمي، ناصر (٢٠٠٧) فاعلية التشريعات العقابية في مكافحة الجرائم المعلوماتية.

تمام، احمد (٢٠٠٠). الحماية الجنائية للحاسب الآلي، دار النهضة العربية، القاهرة.

حجازي، عبد الفتاح (٢٠٠٦). مكافحة جرائم الكمبيوتر والإنترنت، دار الفكر الجامع، الإسكندرية.

حجازي، عبدالفتاح (٢٠٠٧). الإثبات الجنائي في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية القاهرة.

خليفة،محمد(٢٠٠٧). الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، دار الجامعة الجديدة، الجزائر.

الرومي،محمد(٢٠٠٣). جرائم الكمبيوتر والإنترنت، دار المطبوعات الجامعية، الإسكندرية.

سرحان والمشهداني (٢٠٠١). أمن الحاسوب والمعلومات، دار وائل للطباعة والنشر، الأردن، عمان.

الشاذلي، فتوح (٢٠٠٣) جرائم الكمبيوتر، منشورات الحلبي الحقوقية، بيروت.

الشهري، حسن والعطيوي، صالح (٢٠٠٧). دراسة الوضع الحالي لتدريس وتطبيق أنظمة وتشريعات الجريمة الإلكترونية في المملكة، ورقة عمل مقدمة إلى ندوة المجتمع والأمن: الجرائم الإلكترونية .. الملامح والأبعاد، الرياض.

الشوابكة، محمد (٢٠٠٤). جرائم الحاسوب والإنترنت الجريمة المعلوماتية، عمان، الأردن: مكتبة دار الثقافة للنشر والتوزيع.

الصغير، جميل (١٩٩٤). الإنترنت والقانون الجنائي، دار النهضة العربية، القاهرة، مصر.

الصغير، جميل (٢٠٠١). الأحكام الموضوعية للجرائم المتعلقة بالإنترنت، دار النهضة العربية، القاهرة.

عبابنة، محمود (٢٠٠٥). جرائم الحاسوب وأبعادها الدولية، دار الثقافة، عمان، الأردن.

ـــــــــــــ (٢٠١٠). جرائم الحاسوب وأبعادها الدولية، دار الثقافة، الأردن، عمان.

عبدالكريم، عبدالله (٢٠٠٧). جرائم المعلوماتية والإنترنت، منشورات الحلبي الحقوقية،بيروت.

عبد المطلب،ممدوح(٢٠٠٦). البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، القاهرة.

عرب، يونس (٢٠٠٢). جرائم الكمبيوتر والإنترنت، ورقة عمل مقدمة إلى مؤتمر الأمن العربي، المركز العربي للدراسات والبحوث الجنائية، أبو ظبي.

العريان، محمد (٢٠٠٤). الجرائم المعلوماتية. الإسكندرية، مصر: دار الجامعة الجديدة للنشر.

عيد، محمد (١٩٩٩). الإجرام المعاصر، مركز الدراسات والبحوث بأكاديمية نايف العربية للعلوم الأمنية، الرياض، الطبعة الأولى.

قشقوش، هدى (١٩٩٢). جرائم الحاسب الإلكتروني في التشريع المقارن، القاهرة: دار النهضة العربية.

مدني، سالم (٢٠٠٧). مدى إمكانية تطبيق الحدود على الجرائم الإلكترونية، ورقة عمل مقدمة إلى ندوة المجتمع والأمن: الجرائم الإلكترونية..الملامح والأبعاد، الرياض.

الملط، احمد (٢٠٠٦). الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية.

موسى، مصطفى(٢٠٠٣). أساليب إجرامية بالتقنية الرقمية، سلسلة اللاء الأمنية، القاهرة.

نماذج تشريعات الفضاء السيبراني في الدول الأعضاء بالاسكو، الأمم. المتحدة، نيويورك، ٢٠٠٧.

المراجع الأجنبية:

Cate, F (1997), privacy in the information age. Washington: The Brookings Institution.

Lilley, P (2002), hacked attacked& abused digital crime exposed, London, Kogan Page Limited.

Laura Quarntile, Cyper Crime: how to protect your self from computer crime, Limelight Books, Tier Publications, 1997.

John Kntile, The Danger of Computer Hacking,The Rosen Publishing Group, New York,2000.

Gina Angelis, Cyper Crimes, Chelsa Housing Publishers, NY,2000.

Deon Parker, Fighting Computer Crime, John Wiley Publishing, UK, 1988.

David Johnson. Cipher Law, Stoddert Publishing, Toronto, Canada, 1977.

مواقع الإنترنت

http://www.alarabalyawm.net

ttp://www.saudir2.com/vb/showthread.php?t=6829

http://www.neelwafurat.com/itempage.aspx?id=lbb163532-126150&search=books

http://www.al-jazirah.com.sa/digimag/07032004/maaa42.htm

http://www.muslm.net/vb/showthread.php?t=202754

http://uaew.maktoobblog.com/

http://www.mcit.gov.sa/arabic/

http://www.elaph.com/web/politics/2008/12/391129.html

http://www.alyaum.com/issue/page.php?IN=12423&P=15

http://forum.stop55.com/47089.html

http://www.gocsi.com/prelea.html.

http://biz.yahoo.com/st/html.

http://www.vsdoj.gov/criminal/cyper.

http://www.c/cisac.html