السّياسة الجنائية في مواجهة جرائم الإنترنت
Cyber Crimes

أ.د.موسى مسعود ارحومة
أستاذ القانون الجنائي
كلية القانون ـ جامعة قاريونس

توطئة

ما من شكٍّ أن الحاسوب يُعدُّ من المتطلبات الأساسية في حياتنا المعاصرة، ولم يعد اقتناؤه أمراً ترفياً كما كان عليه الحال في بداية ظهوره . فقد بات من أهم لوازم الإنسان في الوقت الرّاهن ، ولم يعد ممكناً استغناؤه عنه سواء في منزله أو مكتبه ، بل حتى في ترحاله بالنّظر إلى الخدمات الجليلة التي يسديها في شتّى مناحي الحياة[1].

وببزوغ عصر الإنترنت ، نتيجة المزاوجة بين تقنيتي الحوسبة والاتصالات ، ازدادت أهمية المعلوماتية أو تقنية المعلومات ؛ إذ بفضل ذلك أضحى العالم قرية صغيرة ، مما يصح معه أن ينعت هذا العصر بعصر المعلومات .

فقد مكّنت شبكة المعلومات الدّولية (الإنترنت) ـ الواسعة بسعة هذا الكون الفسيح ـ من تيسير الاتصال بين الأفراد والمؤسسات في أية بقعة من هذا العالم المترامي الأطراف ، كما ساعدت على تدفق المعلومات وانسيابها عبر حدود الدّول والقارات ، وبفضل ذلك تذللت الصّعوبات في التّواصل بين بني البشر ، وفي تقريب الخدمات وإتقانها، وهو ما فتح آفاقاً رحبة في الاستفادة من هذه التّقنية العالية في ميادين شتّى كالتّعليم والصّحة والإدارة والأمن

والاتصالات والتّجارة والطّيران ، حتى إنه أخذت تبرز مصطلحات جديدة أفرزتها حقبة المعلوماتية كالحكومة الإلكترونية والتّوقيع الإلكتروني والجامعة الافتراضية والأرشيف الإلكتروني والسّيارة الإلكترونية ...إلخ . وهذا كله تطلّب إحداث ثورة في مجال القانون أيضاً بما يتواءم مع هذه المستجدات ويواكب تطورها .

غير أنه في المقابل ، فإن هذه الطّفرة اللامتناهية في مجال تقنية المعلومات صاحبها انعكاسات سلبية متمثلة في سوء استخدام هذه التّقنية الجديدة[2] بحيث أضحت المعلومات أو البيانات المخزنة بشبكة الإنترنت أو التي يتم انسيابها عبرها هدفاً للاعتداء سواء باختراق المواقع الخاصة أو بتدمير أو إتلاف البيانات ببث الفيروسات من قِبَل الحاقدين أو المتطفلين (الهاكرز Hackers) ، أو القرصنة المعلوماتية بالاستيلاء على تلك البيانات أو البرامج وتقليدها . كما توظف في كثير من الأحيان شبكة المعلومات (الإنترنت) في ارتكاب بعض الجرائم التّقليدية أو تسهيل ارتكابها ، كما في توجيه رسائل السّبّ أو القذف للآخرين عبر البريد الإلكتروني أو الاستيلاء على الأموال أو تحويلها . كذلك قد يكون الإنترنت مسرحاً للجريمة أو بيئة لها بإقامة المواقع المحظورة ، كالمواقع الإباحية أو التي تشجع على الدّعارة أو التّحريض على الإرهاب أو بإنشاء المواقع المعادية للآخرين وتوظيفها للنيل من الخصوم السّياسيين أو غيرهم .

أو بعبارة أخرى ، فإن بيئة الإنترنت تكون غالباً موئلاً لعصابات الإجرام والجريمة المنظمة بما تتيحه للجناة من سهولة الاتصال والتّخطيط دون إمكان كشفهم أو تحديد مكانهم لاسيّما مع قصور التّشريعات الجنائية لكثير من الدّول عن مواجهة الأفعال التي يساء فيها استخدام شبكة الإنترنت ، فضلاً عن

عجز الأجهزة العاملة في مجال مكافحة الجريمة عن التعامل مع جميع الصّور التي تدخل تحت ما يُسمى بالجرائم المعلوماتية أو جرائم الإنترنت Cyber Crimes.

وهذا كله أثار الجدل بشأن كيفية تحقيق التّوازن بين ضمان الاستخدام الحر لشبكة الإنترنت ، وفي الوقت ذاته تجنب المخاطر النّاجمة عن سوء استخدامها. أو بالأحرى كيف يمكن تنظيم التّعامل مع هذه التّقنية الجديدة بحيث يمكن الاستفادة المثلى منها مع الحدّ من الظواهر السّلبية المصاحبة لها ؟

فما هي الحلول الملائمة لمواجهة جرائم الإنترنت أو سوء استخدام الشبكة المعلوماتية سيّما وأن القواعد التّقليدية قد لا تكون ـ في كثير من الأحيان ـ كافية باعتبارها قد صيغت في زمن غير هذا الزّمن ؟

وباعتبار أن إساءة استخدام الإنترنت من الظواهر المستحدثة والخطيرة في آن معاً بما ينجم عنها من أضرار بالغة ، ونظراً لطبيعتها الخاصة ، فإن الأمر يتطلب التّصدّي لها بحزم للحد من مخاطرها من خلال تبني جملة من الآليات والتّدابير الفعّالة على الصّعيد الوطني بسنّ التّشريعات الجزائية الزّاجرة التي تكفل توفير الأمن المعلوماتي وضمان الحماية الكافية لنظم المعلومات وتطوير المنظومة الإجرائية فيما يخص قواعد الضبط والتّفتيش والتّحقيق والاختصاص وما إلى ذلك من الإجراءات التي يتطلبها تعقّب الجناة وملاحقتهم والتّحري عنهم بغية تقديمهم للعدالة وإنزال الجزاء المناسب بحقهم .

ولما كانت مخاطر هذه الجرائم تتعدى حدود الدّول (عابرة للحدود بل وللقارات) فقد أضحت مواجهتها على الصّعيد القطري قاصرة وغير ناجعة ما لم تعزّزها الجهود الدّولية في هذا المضمار من خلال إبرام الاتفاقيات الدّولية والإقليمية.

وعلى ضوء ما تقدَّم سنركز من خلال هذه الورقة على ثلاثة محاور ، نخصّص الأول للتعريف بجرائم الإنترنت وتحديد خصائصها والتّحديات التي تواجه القائمين على مكافحتها .

في حين نخصّص الثّاني لبحث آليات التّصدي لجرائم الإنترنت على الصّعيد الوطني .

أما الثّالث والأخير فسنخصّصه للجهود الدّولية والإقليمية لمواجهة جرائم الإنترنت ، وذلك كلّ في مطلب مستقل .

المطلب الأول

التّعريف بجرائم الإنترنت وتحديد خصائصها والتّحديات التي تواجه القائمين على مكافحتها

أولاً ـ التّعريف بجرائم الإنترنت :

نظراً لحداثة هذه الطّائفة من الجرائم فقد تباينت المصطلحات الدّالة عليها ، وذلك مرده تطور الإجرام المعلوماتي أو المرتبط بتقنية المعلومات تطوراً مذهلاً في أساليبه وأنماطه[3]. فتارة تُسمى بإساءة استخدام الحاسوب والإنترنت، كما يطلق عليها أحياناً جرائم الحاسوب أو الجرائم المرتبطة به ، أو جرائم الحاسب الآلي والإنترنت ، كذلك شاع مؤخراً استعمار مصطلح الجرائم المعلوماتية أو ذات التّقنية العالية Cyber Crimes ، إلى آخر ما هنالك من المسميات المتفاوتة في دلالتها كما يبدو ظاهرياً .

كما أن ثمة اختلافاً بشأن تعريفها أو تحديد مفهومها ، وذلك بحسب الزّاوية التي ينظر منها لهذه الجرائم أو بالأحرى وفقاً للمعيار أو الأساس الذي يستند إليه كل من حاول التّصدي لتعريفها[4]. فثمة من يقيم التّعريف على أساس موضوع الجريمة أو محلها، وهناك من يؤسسه على الأداة أو الوسيلة المستخدمة في ارتكابها . في حين يحاول البعض ربط التّعريف بشخص مرتكبها ، وفي مقابل هذا وذاك يذهب البعض إلى محاولة الجمع بين أكثر من معيار .

ووفقاً لما تقدَّم عرّفها جانب من الفقه بأنها الأنشطة غير المشروعة التي يكون فيها الحاسب الآلي أو الإنترنت موضوعاً للجريمة أو هدفاً لها . في حين يعرّفها جانب آخر بأنها الأفعال أو الأنشطة الإجرامية التي يكون الحاسوب أو

الإنترنت وسلة لارتكابها . وجرى تعريفها كذلك بأنها الأفعال التي يرتكبها شخص على دراية بتقنية المعلومات ، وقيل بأنها الأنشطة أو الأفعال غير المشروعة التي يتطلب ارتكابها أو متابعة فاعلها والتّحقيق فيها دراية بنظم المعلومات .

وكما هو ملاحظ من التّعريفات المتقدمة أن كلاًّ منها لا يخلو من القصور ، ومع ذلك فإن ثمة قاسماً مشتركاً بينها يتجلّى في أن ارتكاب هذه الأنشطة غير المشروعة يتم من خلال استخدام تقنية المعلومات وبواسطتها من قبل شخص لديه قدر من الدّراية بأصولها وقواعدها الفنية كي يمكنه بلوغ الغاية التي يسعى إليها عادة من وراء لجوئه إلى إساءة استخدام هذه التّقنية .

ومن ثم يمكننا تعريف جرائم الإنترنت بأنها الأنشطة أو الأفعال غير المشروعة التي يقوم بها شخص على دراية كافية بتقنية المعلومات متوسّلاً بشبكة المعلومات الدّولية في تحقيق مآربه الشريرة للإضرار بالآخرين .

فالحاسوب والإنترنت يلعب دوراً كبيراً في ارتكاب هذه الطّائفة من الجرائم ، فهو إما أن يكون هدفاً أو موضوعاً لها[5]، كما في حالة اختراق الأنظمة المعلوماتية أو الدّخول غير المصرح به إلى موقع ما ، وتدمير أو إتلاف المعطيات والبيانات والمعلومات المخزنة أو المنسابة عبر الإنترنت أو تحويرها أو تعديلها ، كما في زراعة الفيروسات أو الاستيلاء على تلك البيانات المنقولة عبر النّظم (القرصنة المعلوماتية) ، أو الاعتداء على الخصوصية والسّريّة .

كما قد يكون الحاسوب والإنترنت أداة لارتكاب بعض الجرائم التّقليدية كما في استغلاله في الاستيلاء على الأموال من خلال إساءة استخدام بطاقات الائتمان ، كذلك يستخدم أحياناً في ارتكاب جريمة القتل من خلال

الدّخول إلى البيانات المخزنة والتّلاعب ببرمجيتها ، ومن هذا القبيل إمكان التّحكم في الطّائرة أو السّفينة بشكل يؤدي إلى تدميرها وقتل ركابها ، أو تغيير البيانات المتعلقة بملفات المرضى أو تشخيص المرض .

فضلاً عن ذلك ، قد يكون الحاسب والإنترنت بيئة للجريمة ومسرحاً لها[6]، كما في توظيفه في نشر المواد غير القانونية مثل إنشاء المواقع الإباحية والتّحريض على الجريمة بجميع أنماطها كالتّرويج للمخدرات أو تجارة الأسلحة أو تجارة الرّقيق الأبيض ..إلخ .

ويصنّف الباحثون مجرمي المعلوماتية إلى مجموعة من الطّوائف والفئات ، فمنهم قراصنة الحاسوب أو من يمكن تسميتهم بالعابثين ، وهؤلاء قد يكونون مجرد هواة أو فضوليين (الهاكرز Hackers)[7]، ويهدفون عادةً إلى مجرد التّسلية واللهو وإظهار مقدرتهم على تحدي النّظام ، ويغلب على هؤلاء أنهم من صغار السّن أو المراهقين ممن نبغوا في هذا المجال أو على الأقل توافر لديهم قدر من المهارة في استخدام هذه التّقنية العالية ، وفي أغلب الأحيان لا يتوفر لدى هؤلاء أي دافع إجرامي بخلاف غيرهم من الطّوائف الأخرى .

وقد يكون القراصنة من أولئك المحترمين ، أو الذي يُطلق عليهم (Crakers) ، وهؤلاء يعدون أكثر خطورة من الفئة السّابقة ، وهم يتميزون بأن لديهم مهارة كبيرة وخبرة عالية بأنظمة الحاسوب والإنترنت ، وكثيراً ما ينجم عن أفعالهم أضرار بالغة بأنظمة المعلومات وبرامج الحاسوب ، وفي الغالب ما يكون هدفهم تحقيق الكسب المادي ، ومن هؤلاء من يسعى من وراء نشاطه غير المشروع إلى تحقيق أغراض سياسية أو غيرها .

وثمة فئة المحتالين (Fraudeurs)، الذين يتمتعون عادةً بقدر عالٍ من

المهارة ، وجلّ جرائمهم تتمثل في الاستيلاء على الأموال أو تحويلها بإساءة استخدام بطاقات الائتمان . إلى جانب هؤلاء توجد طائفة مجرمي المعلوماتية من الجواسيس (Espions)، والذين يهدفون عادةً إلى اختراق النّظم المعلوماتية من أجل الحصول على بعض المعلومات والبيانات لمصلحة بعض الجهات كالشركات أو لفائدة دول معينة .

كذلك من بين فئات المجرمين المعلوماتيين من يمكن أن نطلق عليهم المجرمين الحاقدين أو السّاخطين الذين تحركهم في العادة رغبة الانتقام من أرباب الأعمال الذين يعملون طرفهم .

ناهيك أن ثمة مجرمين في مجال الجريمة المنظمة الذين يستفيدون من أنظمة المعلومات في اقتراف جرائمهم وتسهيل ارتكابها والتّخطيط لها .

وعموماً يمكن القول بأن المجرم المعلوماتي قد يكون من الاختصاصيين في مجال الحاسبات الآلية ونظم المعلومات ، والذين يتمتعون بمهارات عالية ومعارف كبيرة ، وربما يكونون من الحاصلين على المؤهلات العلمية العالية ، الأمر الذي يتيح لهم ارتكاب جرائمهم وتحقيق غاياتهم بسهولة ويسر ودون ترك أي دليل . وقد يكون هؤلاء من أولئك الذين دأبوا على استخدام هذه التّقنية ، دون أن تتوافر لديهم الدّراية أو الخبرة الكافية ، كل ما في الأمر أنهم يملكون قدراً من المهارة بما يمكنهم من إساءة استخدام هذه التّقنية بأي وجه من الأوجه ، سواء بإتلاف بيانات معينة أو إضافة أخرى لما هو مخزن منها أو التّلاعب بها بصورة أو بأخرى .

أما الدّوافع المحركة للمجرم المعلوماتي ، فهي متباينة تختلف من مجرم إلى آخر[8]، ومن أبرزها :

1 ـ تحقيق الكسب المادي ، أو السّعي إلى الحصول على الأموال . فمثل هذه الجرائم كثيراً ما تغري مقترفيها بمكاسب وأرباح طائلة ، وينسحب هذا بوجه خاص على الاحتيال المعلوماتي .

2 ـ الانتقام : كما سبق القول أن بعض المجرمين يسعون إلى اقتراف جرائمهم بغية الانتقام من غيرهم سواء كانوا من المنافسين لهم أو من رجال الأعمال. ومن ذلك جرائم إتلاف البيانات والبرامج وتدمير نظم المعلومات بشتى الوسائل والطّرق بما في ذلك زرع الفيروسات .

3 ـ التّعبير عن التّفوق وقهر النّظام أو حب المغامرة والإثارة ، وثمة من يرى بأن هذا الدّافع يأتي في طليعة البواعث المحركة للمجرم المعلوماتي ، وهو يتمثل في قهر النّظام وإثبات القدرة على اختراق تعقيدات التّقنية أكثر من الرّغبة في كسب المال ، مثل اختراق مواقع الإنترنت والاستخدام غير المصرح به لأنظمة المعلومات . فمرتكبو هذه الجرائم يحاولون التّدليل على ما يتمتعون به من مقدرة على التّفوق وكسر كل الحواجز (مثل فكّ الشفرة أو الرّقم السّري)[9].

وبالإضافة إلى ما سبق فثمة دوافع أخرى ، سياسية أو أيديولوجية أو تنافسية أو إرهابية وما شاكل ذلك .

وفي واقع الأمر أن الجريمة الواحدة قد تتعدد البواعث لاقترافها ، فعلى سبيل المثال أن الإرهاب الإلكتروني ربما تقف وراءه دوافع سياسية أو عقائدية ، وإنكار الخدمة قد يكون الباعث إليه تحدي النّظام ، أو أن ثمة أحقاداً أو دوافعَ تنافسية تحرّكه . وبالنّسبة للاحتيال المعلوماتي فالدّافع إليه يكون في الغالب هو الاستيلاء على المال وتحقيق المكاسب المادية ، في حين أن الاستيلاء على

المعلومات أو البرامج قد يكون لتحقيق مآرب تنافسية أو سياسية أو بغية الابتزاز وتحقيق الكسب المادي . وفيما يتعلق بتدمير أو إتلاف المعطيات وتخريب الأنظمة فالباعث إليه قد يكون تنافسياً في المقام الأول أو لمجرد إخفاء أنشطة إجرامية أخرى ، وقد يكون الدّافع إليه الانتقام من الخصوم وغيرهم ممن يحقد عليهم مرتكبو هذه الفئة من الجرائم .

ثانياً ـ خصائص جرائم المعلوماتية والتّحديات التي تواجه القائمين بمكافحتها :

تتّسم هذه الجرائم المستحدثة عن سواها من الجرائم الأخرى بسمات تنفرد بها ، مما يضفي عليها طابعاً مميزاً[10]، الأمر الذي يثير جملة من الإشكاليات القانونية والتّحديات العملية أمام القائمين على مكافحتها ، ومن أبرزها :

1 ـ أن ثمة صعوبة في اكتشافها والاستدلال على مرتكبيها ، ومرد ذلك أنها تستهدف المعنويات (البرامج والمعلومات) لا المحسوسات أو الماديات؛ إذ لا يترك الجناة أثراً مادياً يمكن من خلاله التّعرّف عليهم بخلاف الجرائم التّقليدية . فضلاً عن أن مباشرة الاستدلال والتّحقيق فيها يتطلب دراية كبيرة بتقنية المعلومات مما يتعذر على الأجهزة الضبطية والتّحقيقية التّقليدية التّعامل معها[11].

ناهيك أن مرتكبيها يتّصفون بقدر عالٍ من الذكاء والمهارة ، ويعتمدون غالباً في اقترافها على التّضليل والخداع دون اللجوء إلى أسلوب العنف[12]، وهو ما يجعل إثباتها في كثير من الأحيان من الصّعوبة بمكان باستخدام الوسائل المتعارف عليها في إثبات الجرائم العادية .

2 ـ إن موضوع الضبط والتّفتيش في هذا النّمط من الجرائم هو النّظم المعلوماتية وقواعد البيانات في الغالب ، الأمر الذي يتطلب أحياناً امتداده إلى أنظمة أخرى تتعلق بغير المشتبه فيهم أو المتهمين ، مما يثير بعض الإشكاليات القانونية من حيث مشروعية ذلك الإجراء إذا كان من شأنه انتهاك الخصوصية المعلوماتية للأشخاص الذين يطالهم التّفتيش أو الضبط .

3 ـ إن الدّافع على ارتكاب هذه الجرائم في أغلب الأحيان هو إشباع الرّغبة في الانتقام أو من أجل إثبات القدرة على قهر النّظام والتّغلب على الأنظمة ، والقليل منها يكون المحرّك إلى اقترافه هو تحقيق الكسب المادي .

4 ـ إن التّطور المطّرد في مجال تقنية المعلومات وتضاعف أعداد المؤهلين في هذا الميدان ممن يملكون المهارة في التّعامل مع الحاسوب والإنترنت أدى إلى ازدياد نسبة ارتكاب هذه الجرائم عاماً بعد عام ، وشهراً بعد شهر ، ويوماً بعد يوم ، إن لم يكن ساعة بعد أخرى . ولعلَّ ذلك مبعثه أن جلَّ مقترفيها ينعدم لديهم الإحساس بعدم مشروعية ما يقدمون عليه ، أو بالأحرى تتداخل لديهم حدود الخير والشر ، بحيث يتلاشى أو على الأقل يضعف الشعور بالذنب عندهم فلا يرون في أفعالهم هذه ما يشكل انتهاكاً للقانون بحيث تستحق المؤاخذة عليها .

5 ـ ولعلَّ في مقدّمة التّحديات التي تواجه الجهات المعنية بالتّصدي لهذه الجرائم ـ بالإضافة إلى ما سبق ـ أن جلّها تتصف بأنها ذات بُعد دولي ، أي أنها عابرة للحدود Transnational Crimes بل وللقارات ، فهي تتجاوز الحدود الجغرافية للدول باعتبارها تنفذ عبر الشبكة المعلوماتية (الإنترنت)، وهو ما يخلق في كثير من الأحيان تحديات قانونية وإدارية في مواجهتها

لاسيما فيما يتعلق بإجراءات الاستدلال والتّحقيق والمحاكمة ، وعلى وجه الخصوص فيما يتصل بتحديد مكان وقوع الجريمة ، ومن ثم القانون الواجب التّطبيق . ذلك أن السّلوك الإجرامي قد يقع في أقصى الشرق والنّتيجة الضارة المترتبة عليه تقع في أقصى الغرب ، سيّما وأن التّشريعات التّقليدية غير ملائمة للتطبيق على مثل هذه الجرائم لصدورها في وقت مبكر قبل ظهور الإنترنت وأنظمة المعلومات . أي أنها سنّت في الأساس من أجل مكافحة الأنماط الإجرامية التّقليدية ، ولم يدر بخلد واضعيها عندئذ المخاطر النّاجمة عن إساءة استخدام التّقنية الحديثة[13].

المطلب الثّاني

آليات التّصدي لهذه الجرائم على الصّعيد الوطني

أمام المخاطر الجسيمة النّاجمة عن إساءة استخدام الحاسوب والإنترنت ، بادرت كثير من الدّول إلى تبني سياسة جنائية جديدة تتواءم مع هذا النّمط المستحدث من الإجرام (الإجرام المعلوماتي)، فذهبت بعض الدّول إلى إدخال تعديلات جزئية في التّشريعات الجنائية القائمة بما يكفل توفير الحماية المناسبة ضد التّحديات الجديدة التي برزت مع شيوع استخدام هذه التّقنية ، في حين خطا بعضها الآخر خطوات متقدمة في هذا المضمار بسنّ تشريعات خاصة تتعلق بجرائم المعلوماتية .

وفي المقابل ثمة طائفة أخرى من الدّول في طريقها إلى إصدار تشريعات في هذا الخصوص ، ويعمل القضاء فيها على تطويع قوانينها النّافذة بحيث يجري تطبيقها على الأفعال التي تمثل إساءة استخدام الحاسوب أو الإنترنت ، وهذه الطّائفة الأخيرة تشمل أغلب الدّول العربية وكذلك جلّ دول العالم الثّالث .

وحتى بالنّسبة للدول التي لم تواجه هذه الأفعال بقوانين خاصة ، فإن ثمة جهوداً تبذل من أجل تطوير الأجهزة العاملة في مكافحة هذه الجرائم .

وعلى ضوء ذلك سنعرض أولاً لموقف التّشريعات العربية ثم لموقف التّشريعات غير العربية بالخصوص ، مختتمين هذا المطلب بالوقوف على الجهود المبذولة لتطوير الأجهزة المناط بها مكافحة جرائم الإنترنت .

أولاً ـ موقف التّشريعات العربية :

لقد بدا لنا من مراجعة التّشريعات العقابية النّافذة في أغلب الدّول العربية أنها تخلو من إفراد نصوص خاصة لحماية نظم المعلومات في مواجهة إساءة استخدام الإنترنت ، وأمام هذا الفراغ التّشريعي يتجه القضاء ومعه بعض الفقه إلى تطويع النّصوص العقابية المتعلقة بالجرائم التّقليدية كالسّرقة والنّصب وخيانة الأمانة والتّزوير والإتلاف والتّجسس لكي يتم إعمالها بصدد إساءة استخدام تقنية المعلومات .

إلاّ أن هذه المحاولات واجهت من جهة أخرى معارضة من قبل جانب كبير من الفقه ، وقد أسفرت الدّراسات والأبحاث التي أجريت في هذا المقام بأن النّصوص التّقليدية غير كافية لمواجهة الجرائم المستحدثة ، ويصعب قبول تطبيقها بشأنها وذلك لأكثر من اعتبار : فمن ناحية أن جرائم الإنترنت تستهدف في المقام لأول المعطيات ، أو بالأحرى الكيان المنطقي المتمثل أساساً في البرامج والمعلومات والبيانات المخزنة في جهاز الحاسب الآلي أو المنقولة عبر الإنترنت منه أو إليه ، ومن ناحية ثانية أن مبدأ شرعية الجرائم والعقوبات يتنافى ومسألة إعمال القواعد المتعلقة بالجرائم التّقليدية على أنماط السّلوك المستحدثة دون النّص على تجريمها والعقاب عليها بصورة صريحة ، الأمر الذي يجعل الأفعال المذكورة بمنأى عن طائلة قانون العقوبات بالرّغم من خطورتها . ومن ناحية ثالثة أن القياس محظور في مسائل التّجريم والعقاب ، ومن ثم لا يسوغ قياس إساءة استخدام الحاسوب والإنترنت على الجرائم العادية[14].

ومع هذا ، فقد بادرت قلة من الدّول العربية إلى إدخال تعديلات طفيفة على قوانينها العقابية ، كما هو الحال في دولة عُمان ، حيث أضيفت إلى

قانون العقوبات مادة جديدة وهي المادة 276 مكرراً بموجب المرسوم السّلطاني رقم 2001/72م[15] التي تجرّم عشرة أفعال متى استخدم الحاسب الآلي في ارتكابها عن عمد وهي تشمل : الالتّقاط غير المشروع للمعلومات أو البيانات، الدّخول غير المشروع على أنظمة الحاسب الآلي ، التّجسّس والتّنصّت على البيانات والمعلومات، انتهاك خصوصيات الغير أو التّعدي على حقهم في الاحتفاظ بأسرارهم، تزوير بيانات أو وثائق مبرمجة أيّاً كان شكلها ، إتلاف وتغيير ومحو البيانات والمعلومات ، جمع المعلومات والبيانات وإعادة استخدامها، تسريب المعلومات والبيانات ، التّعدي على برامج الحاسب الآلي بالتّعديل أو الاصطناع، نشر واستخدام برامج الحاسبَ الآلي بما يشكل انتهاكاً لقوانين الملكية الفكرية والأسرار التّجارية .

كذلك جرَّم المشرع العماني بموجب المادة 276 مكرراً (1) المضافة بالتّعديل سالف الذكر الاستيلاء أو الحصول على نحو غير مشروع على بيانات تخص الغير تكون منقولة أو مختزنة أو معالجة بواسطة أنظمة المعالجة المبرمجة للبيانات.

وقد شدّد المشرع العقوبة في حالة ما يكون مرتكب الجرائم السّابقة من مستخدمي الحاسوب . ليس هذا فحسب ، بل جرّم التّعديل المشار إليه تقليد أو تزوير بطاقات الوفاء أو السّحب، واستعمال أو محاولة استعمال البطاقة المقلّدة أو المزوّرة مع العلم بذلك ، وقبول الدّفع ببطاقة الوفاء المقلدة أو المزوّرة مع العلم بذلك ، وذلك بمقتضى المادة 276 مكرراً (3). أضف إلى ذلك أن الفقرة 276 مكرراً (4) جرّمت استخدام البطاقة كوسيلة للوفاء مع العلم بعدم وجود رصيد ، واستعمالها بعد انتهاء صلاحيتها أو إلغائها مع العلم بذلك ، وأخيراً

استعمال بطاقة الغير دون علمه .

وهذه الخطوة من المشرع العماني جديرة بالتّنويه ، فهي وإن لم توفر الحماية الكافية لنظم المعلومات باعتبارها لا تواجه جميع صور إساءة استخدام تقنية المعلومات ، إلاّ أنها تعد محاولة جادة لبسط الحماية الجنائية للبيئة المعلوماتية مقارنةً بكثير من التّشريعات العربية التي لم يطرأ عليها أي تعديل بالخصوص حتى الآن ومنها القانون الليبي.

كما أقدم المشرع المغربي هو الآخر على إصدار تشريع مماثل ، ألا وهو القانون 03 . 07 المتمم لمجموعة القانون الجنائي بتجريم الأفعال التي تشكل اعتداءً على نظم المعالجة الآلية للمعطيات ، ومن صور الجرائم التي جاء بها القانون المذكور، الدّخول عن طريق الاحتيال إلى نظم المعلومات ، وتغلظ العقوبة في حالة ما يفضي ذلك إلى حذف أو تغيير أو اضطراب في المعطيات المدرجة فيها طبقاً للفصل 3 ـ 607 ، وكذلك جرّم المشرع المذكور عرقلة سير نظام المعالجة الآلية أو إحداث خلل فيه بصورة عمدية (الفصل 5 ـ 607) والمعاقبة على الدّخول عن طريق الاحتيال إلى مجموع أو بعض نظام المعالجة الآلية متى كان يفترض أن يتضمن معلومات تخص الأمن الدّاخلي أو الخارجي للدولة أو تهم الاقتصاد الوطني ، وتشدد العقوبة في حق الموظفين أو المستخدمين الذين يقدمون على ارتكاب هذا الفعل ، وكذلك يتم إعمال التّشديد في حق كل من يترتب على دخوله بواسطة الاحتيال للأنظمة المشار إليها حذف أو اضطراب في سير النّظام أو تغيير المعطيات المدرجة (الفصل 4 ـ 607) .

وإلى جانب ذلك جرّم المشرع المغربي بموجب القانون سالف الذكر بموجب الفصل (7 ـ 607) تزوير وتزييف وثائق المعلومات متى ترتب على

ذلك إلحاق ضرر بالغير ، وكذلك استعمال وثائق معلوماتية مع العلم بأنها مزوّرة أو مزيّفة .

غير أنه تجدر الإشارة إلى أن المشرع أغفل تجريم بعض الصّور التي جرّمتها تشريعات أخرى ، ومن ذلك التّحايل على الحاسب الآلي بتحويل الأموال وتبييضها بواسطة الحاسب الآلي[16].

ومن التجارب الرائدة في هذا المجال تجربة دولة الإمارات العربية المتحدة، فهي الدولة الوحيدة من بين الدول العربية التي أصدرت قانوناً خاصاً فيما يتعلق بهذه المسألة ، وهو القانون الاتحادي رقم (2) لسنة 2006م في شأن مكافحة جرائم تقنية المعلومات[17]، حيث أفرد لذلك 29 مادة ، حتى إنه يمكن القول بأنه جرّم كلّ صور إساءة استخدام الحاسب الآلي والإنترنت . وما يعنينا في هذا المقام أن هذا القانون ركّز بصورة واضحة على حماية الشبكات المعلوماتية مما قد يستهدفها من اعتداءات من قِبَل مستخدميها لتعطيلها أو اختراق البيانات أو المعلومات المخزنة بها أو التلاعب بها على أي وجه كان ، وتسخير تقنية المعلومات في ارتكاب الجرائم الخطيرة أو جعلها بيئةً حاضنةً للإجرام . لذا فقد جرّم القانون المذكور اختراق النظم المعلوماتية للوصول إلى البيانات أو المعلومات السرية بدون وجه حق ، وتزوير مستندات الحكومة الاتحادية والمتعلقة بالهيئات والمؤسسات العامة ، وإعاقة الوصول إلى الخدمة بتعطيل الشبكة أو تدمير أو إتلاف أو حذف أو تعديل البرامج أو البيانات أو المعلومات المخزنة بها .

وكان هذا القانون قد أفرد حكماً خاصاً لتعديل أو إتلاف الفحوص الطبية والتشخيص أو العلاج الطبي تقديراً من المشرع لما يمكن أن يترتب على

ذلك من أضرار فادحة بسلامة المرضى .

ولم يكتفِ بذلك ، بل حظر التنصت أو التقاط أو اعتراض كل ما هو مرسَل عبر الشبكة المعلوماتية بدون وجه حق . فضلاً عن أنه جرّم استخدام الشبكة المعلوماتية في ارتكاب بعض الجرائم الخطيرة ، كالتهديد أو ابتزاز الغير ، والاستيلاء على الأموال أو المستندات بطريقة احتيالية ، والوصول إلى أرقام أو بيانات البطاقات الائتمانية أو غيرها من البطاقات الإلكترونية ، وتوظيف الشبكة في عمليات غسل الأموال ، أو التحريض على الدعارة والفجور ، وكذلك الإساءة إلى المقدسات والشعائر الدينية الإسلامية أو المقررة في الأديان الأخرى المعترف بها ، والتحريض على المعاصي والحض عليها .

وقد شمل التجريم كلَّ فعل من شأنه أن يشكّل اعتداءً على القيم الأسرية أو حرمة الحياة الخاصة أو العائلية . ناهيك أن القانون سالف الذكر جرّم صوراً أخرى مثل : إنشاء المواقع أو نشر المعلومات على الشبكة بقصد تسهيل الاتجار بالأشخاص أو المخدرات والمؤثرات العقلية أو الترويج للأفكار التي من شأنها الإخلال بالنظام العام أو الآداب العامة ، أو لتمكين الجماعات الإرهابية من ترويج أفكارها أو الاتصال بقياداتها ، أو كيفية صنع المواد المتفجرة وكل ما يمكن أن يُستخدم في الأعمال الإرهابية .

وقد قرر هذا القانون مجموعة من الجزاءات من أجل زجر مرتكبي الأفعال المذكورة ، وهي تتراوح بين الحبس والغرامة أو الاكتفاء بأي منهما وذلك بالنّسبة لجل الجرائم الواردة به ، ومع ذلك فثمة طائفة أخرى من صور التّجريم واجهها المشرع الإماراتي بموجب القانون المذكور بعقوبات مغلّظة نوعاً ما حيث تصل إلى السّجن لوحده أو بإضافة الغرامة إليه ..

من ذلك ما تقضي به المادة (13) من هذا القانون ؛ إذ تعاقب على التحريض أو الإغواء لارتكاب الدّعارة أو الفجور أو المساعدة على ذلك بالسّجن والغرامة . وتشدد العقوبة إن كان المجني عليه حدثاً . وفي حالة استعمال الشبكة المعلوماتية في تهديد أو ابتزاز الغير تكون العقوبة السّجن مدة لا تزيد عن عشر سنوات (م 9)، وفي جريمة مناهضة الدّين الإسلامي تكون العقوبة السّجن مدة لا تزيد على سبع سنوات (م 15). وتبلغ العقوبة السّجن في حالة الدّخول بدون وجه حق إلى موقع أو نظام بقصد الحصول على بيانات أو معلومات حكومية سرية (م 22)، وإذا ما ترتب على الدّخول إلغاء تلك البيانات أو إتلافها أو تدميرها أو نشرها تشدد العقوبة لتصل إلى السّجن مدة لا تقل عن خمس سنوات . ولم يكتفِ المشرع الإماراتي بالعقوبات المذكورة ، بل عزّز حمايته لنظم المعلومات ببعض التّدابير والعقوبات التّكميلية الأخرى ، ومنها مصادرة الأجهزة أو البرامج أو الوسائل المستخدمة في ارتكاب أي من الجرائم المنصوص عليها في هذا القانون أو الأموال المتحصلة منها ، بل يصل الأمر إلى حد إغلاق المحل أو الموقع الذي يرتكب فيه أي من الأفعال المذكورة متى كانت الجريمة قد اقترفت بعلم مالكه ، وهذا الإغلاق إما كليّاً أو مؤقّتاً للمدة التي تقدرها المحكمة (م24) .

والأهم من ذلك كله ، أن القانون المذكور في سبيل تسهيل كشف الجرائم المنصوص عليها فيه وضبط مرتكبيها وتعقبهم يقضي في المادة (27 منه) بإضفاء صفة مأموري الضبط القضائي على بعض الموظفين الذين يصدر بتحديدهم قرار من وزير العدل والشؤون الإسلامية والأوقاف .

ويعد هذا القانون أنموذجاً ينبغي أن يُحتذى من باقي الدّول العربية

لاسيما مع التّوسع الملحوظ في الأعوام القليلة الماضية في استخدام الشبكة المعلوماتية ، وما قد ينجم عن ذلك من أفعال أو تعديات بجميع صورها وأشكالها . وهذا يتماشى مع التطور الذي بلغته دولة الإمارات في مجال تقنية المعلومات وبالذات بعد قيام الحكومة الإلكترونية .

وفي المقابل ثمة دول عربية أخرى في طريقها إلى إصدار قوانين مماثلة ، ومنها مصر، حيث أوكل لوزارة الاتصالات وتكنولوجيا المعلومات منذ يونيو 2006م بتشكيل لجنة قومية لوضع الملامح النّهائية لمشروع قانون الجرائم المعلوماتية تمهيداً لعرضه على البرلمان المصري ، كما أن السّودان قد أعدَّ مشروعاً مماثلاً لمكافحة جرائم المعلوماتية سنة 2006م ، ويذكر أنه تمّت إجازته مؤخراً (سنة 2007م) من قِبَل البرلمان السوداني مع قانون آخر وهو قانون المعاملات الإلكترونية[18].

وتجدر الإشارة في هذا الصدد إلى أن جامعة الدّول العربية قد وضعت مشروع قانون نموذجي بالخصوص لكي تتأسّى به الدّول العربية بإصدار تشريعات على منواله ، وهو يتفق إلى حدٍّ كبير مع القانون الإماراتي سالف الذكر باستثناء بعض الفروق الطّفيفة بينهما.

ورغبة من المشرع السّعودي هو الآخر في مكافحة هذه الجرائم ، صدر مؤخراً نظام الجرائم المعلوماتية ، الذي صار نافذاً مع مستهل شهر إبريل سنة 2007م وهو يقرر عقوبة السّجن مدة لا تزيد على سنة وبغرامة لا تزيد على (500 ألف) ريال أو بإحداهما على كل شخص يرتكب أيّاً من الجرائم المنصوص عليها في هذا القانون (النّظام) ، وهذه الجرائم تنحصر في الدّخول غير المشروع إلى موقع إلكتروني أو الدّخول إلى موقع إلكتروني لتغيير تصاميم

هذا الموقع أو إلغائه أو إتلافه أو تعديله أو شغل عنوانه أو المساس بالحياة الخاصة عن طريق إساءة استخدام الهواتف النّقالة المزوّدة بكاميرا أو ما في حكمها بقصد التّشهير بالآخرين وإلحاق الضرر بهم عبر وسائل تقنية المعلومات المختلفة .

كما يفرض هذا القانون عقوبة السّجن مدة لا تزيد على عشر سنوات وبغرامة لا تزيد على خمسة ملايين ريال أو بإحداهما على كل شخص ينشئ موقعاً لمنظمات إرهابية على الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي أو نشره لتسهيل الاتصال بقيادات تلك المنظمات أو ترويج أفكارها أو نشر كيفية تصنيع المتفجرات .

ليس هذا فحسب ، بل صدر كذلك نظام (قانون) المعاملات الإلكترونية[19].

وهكذا نلاحظ أن جل التّشريعات العربية ـ باستثناء النّماذج القليلة التي ألمحنا إليها ـ قاصرة عن مكافحة إساءة استخدام الحاسوب والإنترنت في الوقت الراهن مقارنةً بنظيراتها في الدول المتقدمة ، بل حتى بالنسبة لكثير من الدول النامية التي تسعى جاهدةً إلى تحديث تشريعاتها بما يواكب الطفرة التكنولوجية في مجال تقنية المعلومات .

ثانياً ـ في بعض التّشريعات غير العربية :

نتيجة لتفاقم هذه الظاهرة واستفحال خطرها في السّنوات الأخيرة بادرت عدّة دول ، وبالذات المتقدمة في مجال تكنولوجيا المعلومات، بسنّ تشريعات جديدة جرّمت بموجبها أغلب صور الاعتداء على نظم المعلومات . وتُعدّ دولة السّويد في طليعة الدّول الأوروبية التي أقدمت على إصدار تشريع في

هذا الخصوص منذ سنة 1973م ، وهو ما سُمِّيَ بقانون البيانات[20] الذي جرّم الاحتيال المعلوماتي وتزوير المعلومات الإلكترونية أو تحويلها أو الحصول عليها بطريقة غير مشروعة ، والدّخول غير المشروع على المعطيات أو البيانات الإلكترونية . ثم تلتها الولايات المتحدة الأمريكية التي سنّت هي الأخرى قانوناً خاصّاً بحماية أنظمة الحاسب الآلي، وهو ما جاء تحت مسمّى قانون التّحايل المعلوماتي سنة 1984م .

ولم يقف الأمر عند هذا الحد ، بل تلا ذلك صدور عدد من التّشريعات الخاصة بالولايات ـ كل على حدة ـ للتعامل مع هذه الأنماط الإجرامية النّاشئة عن إساءة استخدام تقنية المعلومات .

وفي سبيل تفعيل مكافحة هذه الجرائم منحت وزارة العدل الأمريكية سنة 2000م تفويضاً لخمس جهات حكومية للتعامل مع جرائم الحاسب الآلي والإنترنت ، من بينها مكتب التّحقيقات الفيدرالي (FBI)، فضلاً عن ذلك كله، فإن الولايات المتحدة الأمريكية عملت على تطوير نظامها الإجرائي فيما يتعلّق بالبحث عن الدّليل المستمد من شبكة المعلومات الدّولية (الإنترنت) من خلال إصدار قانون خصوصية الاتصالات الإلكترونية :

The electronic comunications privacy act of 1986
18 U.S.C. & 2522 2510 223321367

المعدل سنة 2001م ، والذي يُعرف اختصاراً بـ(ECPA) الذي ينظم أحكام الضبط والتّفتيش في نطاق الفضاء المعلوماتي أو في بيئة الحواسيب ، كما رسم القانون المشار إليه الآليات التي يستلزم اتخاذها من قبل مأموري الضبط القضائي أو المدعين العموميين ، وهذه المتطلبات تتفاوت بتفاوت المصالح المحمية ، بمعنى أن درجة الحماية تزداد وتتعاظم بزيادة خصوصية المصالح ذاتها ؛ فتارة يتطلب

الأمر مجرد مذكرة استدعاء للحصول على بعض المعلومات من مزودي الخدمات، وتارة أخرى يتعين ضرورة الحصول على إذن تفتيش[21].

وتجدر الإشارة إلى أن القانون المذكور يضع جملة من القيود على الكشف الإرادي بواسطة مزوّدي الخدمة للجمهور ، ومع ذلك فهو يورد بعض الاستثناءات على هذه القيود ، فالقسم usc sec 270218 من هذا القانون يسمح لمزود خدمة الحوسبة عن بُعد أو مزوّد خدمة الاتصالات الإلكترونية الكشف عن محتويات أو معلومات أخرى إرادياً لكل من الهيئات الحكومية وغير الحكومية.

وعموماً يمكن القول بأن هذه الاستثناءات تسمح بالكشف بواسطة مزود الخدمة للجمهور حينما تكون ثمة حاجة لحماية المجتمع ، ويرى مزود الخدمة أولوية هذا الأمر أو رجحانه على خصوصية العملاء ، أو عندما يكون الكشف منطوياً على تهديد للمصلحة في الخصوصية[22]. كذلك يمكن لرجال الضبط توجيه مزودي الخدمة للتحفظ على سجلات موجودة في انتظار اتخاذ إجراء قانوني إجباري ، فوفقاً لهذا القانون يتعيّن على مزود خدمة الاتصال السّلكي أو الإلكتروني أو خدمة الحوسبة عن بعد اتخاذ جميع الخطوات اللازمة للتحفظ على السّجلات وأدلة أخرى في حيازته إلى حين إصدار أمر محكمة أو أي إجراء آخر وذلك بناءً على طلب هيأة حكومية[23].

ومع هذا فإن عدم احترام القانون المذكور لا يترتب عليه بطلان الدّليل، وإن كان ذلك قد يرتب المساءلة المدنية بالإضافة إلى المسؤولية التّأديبية ضد الموظفين الذي ينتهكون أحكام القانون في سبيل الوصول إلى الدّليل[24].

بالإضافة إلى ما تقدم فثمة قانونان فيدراليان ينظمان المراقبة الإلكترونية

للاتصالات، وهما قانون المراقبة أو ما يُعرف بالباب الثّالثّ من قانون أمن الشوارع الصّادر سنة 1968م والمعدل سنة 1986م ، والثّاني قانون أجهزة التّسجيل والتّقصي ، وهذان القانونان يكمل كل منهما الآخر باعتبارهما ينظمان الاطلاع على أنواع مختلفة من المعلومات ، فالباب الثّالث يسمح للحكومة الحصول على محتويات الاتصالات السّلكية واللاسلكية والإلكترونية أثناء البث ، في حين يختص قانون التّسجيل والتّقصّي بتجميع العناوين في الزّمن الفعلي Real Time ، فقانون التّسجيل والتّقصي: The pen/Trap statute/18 usc.3121- 3127 يجيز للادعاء العام التّقدم للمحكمة بطلب لأجل الحصول على أمر يسمح بوضع أو إعداد تجهيزات وإمدادات جهاز التّسجيل والتّقصي طالما أن المعلومات المطلوبة تتعلق بتحقيق جنائي إجباري[25].

ويسمح الباب الثّالثّ للسلطات المختصة بمراقبة الاتصالات السّلكية والإلكترونية بناءً على أمر من المحكمة المقرر بالقسم (usc. sec. 2518 18) وذلك لمدة أقصاها 30 يوماً .

غير أن ثمة متطلبات يستلزم الوفاء بها قبل حصول المفتشين على أمر الباب الثّالث، من ذلك أنه يتعين تأسيس طلب الأمر على سبيل معقول يدعو للاعتقاد بأن المراقبة سوف تكشف عن دليل على جريمة متوقع حدوثها مقررة في القسم 2516[26].

ومن بين الدّول الأوروبية التي أولت اهتمامها بهذا الموضوع في وقت مبكر بريطانيا ، حيث أصدرت سنة 1981م قانوناً جرّمت بموجبه التّزوير والتّزييف باستخدام وسائط التّخزين الحاسوبية المتنوعة أو أي أداة أخرى يتم التّسجيل عليها سواء بالطّرق الإلكترونية أو التّقليدية . وفي وقت لاحق

أصدرت سنة 1990م قانوناً يعالج مسألة إساءة استخدام نظم المعلومات ، حيث جرّم الدّخول إلى البيانات المختزنة بالحاسب الآلي أو البرامج ، وكذلك إجراء أي تعديل عليها بصورة غير مشروعة أو محاولة فعل ذلك[27].

وبالمثل أقدمت كندا على خطوة مماثلة من خلال إدخال بعض التّعديلات على قانونها الجنائي سنة 1985م بحيث شمل ذلك سن قواعد خاصة بجرائم الحاسب الآلي والإنترنت وتحديد العقوبات على المخالفات الحاسوبية وجرائم تدمير أنظمة الحاسب الآلي أو الدّخول غير المشروع إليها .

وقد خوّل بموجب ذلك القانون مأموري الضبط القضائي حق تفتيش أنظمة الحاسب الآلي والتّعامل معها وضبطها في حالة الحصول على أمر قضائي بذلك .

وفي السّنة ذاتها نهجت الدّانمارك النّهج ذاته بإصدارها قانون أول يوليو سنة 1985م ، والذي يتعلق بمكافحة جرائم الحاسب الآلي والإنترنت بالنّص على تجريم الدّخول غير المشروع إلى أنظمة الحاسب أو التّزوير للبيانات أو التّلاعب بها بإتلافها أو تغييرها أو حذفها[28].

ومن بين الدّول التي عملت على تطوير قوانينها بما يتواءم مع الجرائم المعلوماتية فرنسا ، إذ سنّت سنة 1988م القانون رقم (19 ـ 88) الصّادر في 5 يناير 1988م المتعلق بجرائم معينة في المادة المعلوماتية ، حيث تمت إضافة جرائم الحاسب الآلي لقانونها العقابي، ثم صدر قانون جديد في 1994/3/1م تمَّ بموجبه تعديل بعض أحكام القانون السّابق الصّادر سنة 1988م[29].

وكذلك أضحت إساءة استخدام تقنية المعلومات مجرّمة في القانون الياباني، وقد أجازت قوانينها سنة 1991م التّنصت على شبكات الحاسب الآلي

من أجل البحث عن الأدلة الخاصة بالجرائم المذكورة .

والقائمة تطول بخصوص الدّول التي سنت تشريعات خاصة بهذه الجرائم ، ومنها على سبيل المثال لا الحصر دولة تشيلي بموجب القانون رقم (223 - 19) المؤرخ في 1993/6/7م في شأن جرائم المعالجة الآلية للمعلومات ، وجمهورية الصّين بموجب المرسوم رقم (147) بتاريخ 1994/4/18م ، والبرتغال من خلال القانون الخاص بجرائم المعلوماتية بتاريخ 1991/8/17م ، ودولة سنغافورة (قانون إساءة استعمال الحاسوب)، وبلجيكا حيث أضافت إلى المدوّنة العقابية أربع جرائم جديدة تتعلق بالمعلوماتية وهي جرائم الاحتيال المعلوماتي ، والنّصب والاختراق وتخريب البيانات المعلوماتية ، وكذلك أجرت عديد الدّول تعديلات مماثلة في قوانينها العقابية ، كما هو الحال في اليونان والمجر وأيسلندا وإيطاليا ولوكسمبرج (القانون المتعلق بتعزيز المكافحة ضد الجرائم المالية وجرائم الحاسوب المؤرخ في1993/7/15م)، والنّرويج[30].

ثالثاً ـ على صعيد تطوير الأجهزة المعنية بمكافحة جرائم الإنترنت :

فضلاً عن الجهود السّابقة التي تُبذل في مواجهة جرائم الإنترنت على الصّعيد التّشريعي ، فثمة آليات أخرى لمكافحة هذه الجرائم متمثلة في الأجهزة المعنية بضبطها والتّحري عن مرتكبيها وملاحقتهم ؛ إذ لا يكفي سن التّشريعات اللازمة ، فهذا الجهد رغم أهميته يظل في مهب الرّيح ما لم تدعمه جهود أخرى تُعنى بإعداد الأجهزة الضبطية القادرة على التّعامل مع هذه الجرائم ، وهي ما يُعرف بشرطة الإنترنت Internet Police وقد قطعت بعض الدّول المتقدمة شوطاً كبيراً في هذا المضمار ، من خلال قيامها بإنشاء إدارات أو وحدات أو

أقسام خاصة بشرطة الإنترنت . ومن الدّول ذات السّبق في هذا المجال الولايات المتحدة الأمريكية ، وتجلى ذلك في مبادرتها بإنشاء جهاز شرطة خاصة بجرائم الإنترنت سنة 1987م ، وهذا الجهاز تطوّر بحيث تحوّل إلى شرطة دولية للشبكة المعلوماتية International Web Police ، مهمتها السّهر على حماية مجتمع تكنولوجيا المعلومات في جميع أرجاء العالم ، وهذا الجهاز له اتصال بالأجهزة العاملة في ميدان مكافحة الجريمة ، كما له اتصال بالحكومات والمؤسسات المساعدة ، وأيضاً الجمعيات العاملة في حقل مكافحة الجريمة ، وهي كذلك على اتصال بأفراد متطوعين عديدين على مستوى العالم في حوالي (61) دولة[31].

ومن أبرز الخدمات التي تضطلع بها شرطة الإنترنت الأمريكية التّحري والتّتبع والقيام بالادعاء في بعض الأحيان وفض المنازعات ، ويأتي التّحري عن إساءة استخدام شبكة الإنترنت في مقدمة مهامها ، سواء في الجرائم البسيطة المتمثلة في المضايقات التي تتم من خلال البريد الإلكتروني أو بالنّسبة للجرائم الكبيرة والأكثر خطورة بما في ذلك الاستيلاء على الأموال وتسهيل الأعمال غير المشروعة بكافة أنماطها وصورها .

وجدير بالذكر في هذا المقام أن شرطة الإنترنت سالفة الذكر تعتمد على قاعدة بيانات كبيرة، بحيث يتم من خلالها تسجيل كافة الأنشطة غير المشروعة أو الإجرامية التي يتم الإبلاغ عنها . ويمارس هذا الجهاز العملاق عمله من خلال عدد من المنتسبين إليه والمدربين على أحدث تقنيات وأساليب مكافحة الجريمة الإلكترونية .

وهذه الفئة التي يعتمد عليها الجهاز المذكور تتميز بالتّخصص والمهارة العالية للقوى البشرية التي تنتمي إليه ، فضلاً عن استمرارية تقديم الخدمة

والإلمام بالقوانين الحاكمة ، وكذلك مجانية الخدمة.

وتعد هي الجهة الرّسمية لأمن الإنترنت ، وتربطها صلة بأكثر من (61) دولة حالياً من خلال ضباط اتصال ومنفذي القوانين[32].

كما قامت الصّين هي الأخرى باستحداث شرطة خاصة للإنترنت بمقاطعة (استهواي) سنة 2000م بهدف توفير الأمن المعلوماتي. ويعود لها الفضل في ضبط كثير من المخالفات كما هو الحال في المضايقات الشخصية والمواقع الإباحية . ولم يقف جهدها عند هذا الحد، بل تعدّى ذلك إلى قيامها بإعداد برامج تدريب لموظفي البنوك والبورصة بغية التّعريف بأهمية أمن المعلومات والاتصالات ، ناهيك عن قيامها بحملات توعية في وسائل الإعلام المختلفة عن مخاطر الجرائم المعلوماتية وكيف يمكن توقيها[33].

وفي الإطار ذاته أعلن الاتحاد الأوروبي عن مشروع إنشاء منظمة جديدة لتنسيق مكافحة الجريمة عبر الإنترنت والتي ستضطلع بنشر الوعي لدى المواطنين ومستخدمي الإنترنت بالمخاطر النّاجمة عن الفيروسات الإلكترونية وتبصيرهم بما قد يواجههم من مشكلات أمنية أثناء الإبحار في شبكة المعلومات (الإنترنت) ، وذلك من خلال برامج تدريبية وتوعوية للعاملين بالشركات والمؤسسات بأفضل الأساليب والوسائل التي يمكن الاستعانة بها لحماية شبكاتها وكذا العاملين بها ، ناهيك عن القيام ببعض الأبحاث بخصوص أمن الشبكات والإنترنت[34].

وبالنّظر إلى أهمية هذه المنظمة والدّور المعول عليه منها في تحقيق الأمن المعلوماتي رصد لها مبلغ يُقدر بحوالي 24 مليون يورو . وهذه المنظمة سيكون المقر المؤقت لها العاصمة البلجيكية ، وسيتم تقييم مدى جدواها خلال 4

سنوات .

أما بالنّسبة للدول العربية ، فقد اتجه بعضها إلى استحداث إدارات أو أقسام خاصة توكل لها مهام ضبط جرائم الحاسب الآلي والإنترنت والتّحري عنها وملاحقة مرتكبيها وتعقبهم . ومن بين الدّول التي نهجت هذا النّهج جمهورية مصر العربية ، حيث تمّ إنشاء إدارة لهذا الغرض بوزارة الدّاخلية ، وبفضلها أمكن كشف وضبط مرتكبي كثير من جرائم المعلوماتية كالابتزاز والتّشهير والاحتيال والدّعارة ، باستخدام شبكة الإنترنت .

ومن أبرز جهودها في هذا المضمار أنها قامت بشن حملات مداهمة لمقاهي الإنترنت وملاحقة الجهات القائمة على المواقع الإباحية .

ويذكر في هذا الصّدد أيضاً أن ثمة دولاً عربية أخرى أنشأت أقساماً أو وحدات من هذا القبيل تتعلق بمكافحة جرائم الحاسب الآلي والإنترنت ، كما هو الحال في السّعودية والإمارات المتحدة وتونس والأردن والمغرب .

وثمة دعوة إلى إنشاء شرطة إنترنت عربية تكون تابعة لجامعة الدّول العربية.

وفي إطار تطوير الأجهزة المعنية بمكافحة هذه الجرائم أنشأت ليبيا إدارة خاصة لمكافحة جرائم تقنية المعلومات تابعة للإدارة العامة للأدلة والبحث الجنائي وذلك بموجب قرار أمين (وزير) اللجنة الشعبية العامة للأمن العام رقم (63) لسنة 2005م بشأن تقرير حكم في القرار رقم (131) لسنة 2004م بشأن التّنظيم الدّاخلي للجهاز الإداري للجنة الشعبية العامة للأمن العام .

وقد تمّ تخويل الإدارة المشار إليها مجموعة من الاختصاصات ، أهمها مكافحة جرائم الحاسوب والإنترنت وجرائم تقنية المعلومات الأخرى ، فضلاً

عن تقديم الدّعم الفني للمؤسسات العامة في مجال الأمن المعلوماتي بالتّنسيق مع الجهات ذات العلاقة ، والقيام بأعمال البحث والتّحري وجمع الاستدلالات في الجرائم المذكورة . فضلاً عن أنه عهد إليها أمر وضع وتنفيذ برامج التّوعية في مجال الأمن المعلوماتي وجرائم الحاسوب والإنترنت والجرائم عالية التّقنية بالتّنسيق مع الجهات ذات العلاقة ، ووضع الأسس والضوابط لإدارة واستضافة مواقع المؤسسات العامة على الإنترنت والإجراءات الأمنية الواجب توافرها بما يكفل منع تشويهها أو إعلان محتوياتها أو اختطاف أسماء نطاقاتها ، كذلك إجراء البحوث وترجمة الدّراسات ونشر الإحصائيات ذات الصّلة بالأمن المعلوماتي وجرائم الحاسوب والإنترنت والجرائم عالية التّقنية . وبموجب ذلك يمكن إسناد أية اختصاصات أخرى إليها في هذا المجال وفقاً للتّشريعات النّافذة[35].

المطلب الثّالث

الجهود الدّولية والإقليمية لمكافحة جرائم الإنترنت

تظلّ الجهود الوطنية على مستوى كلّ دولة على حدة محدودة الأثر في مواجهة هذه الطّائفة من الجرائم ما لم تكملها جهود أخرى على الصّعيد الإقليمي والدّولي ، ذلك نظراً للطبيعة الخاصة لمثل هذه الجرائم باعتبارها عابرة للحدود بل وللقارات في كثير من الأحيان . فتأثيرها ليس قاصراً على دولة بعينها وإنما ترتكب عبر حدود الدّول ، الأمر الذي يتطلب مزيداً من التّعاون والتّنسيق بين الدّول في رسم سياسة جنائية أكثر شمولاً تتجاوز النّطاق الوطني الضّيق .

وشعوراً باتّساع رقعة هذه الجرائم وتعاظم مخاطرها فقد عملت كثير من الدّول على تجسيد التّعاون فيما بينها في التّصدي الجماعي لهذه الجرائم من خلال إبرام الاتفاقيات والمعاهدات الدّولية ، أو عقد المؤتمرات الدّولية ذات العلاقة .

ونحاول في هذا المقام سبر آفاق هذا التّعاون من خلال اتفاقية بودابست لمكافحة جرائم المعلوماتية ، ومؤتمر الأمم المتحدة الثّامن لمنع الجريمة ومعاملة السّجناء المنعقد بمدينة (هافانا سنة 1990م)، وأخيراً المؤتمر الخامس عشر للجمعية الدّولية لقانون العقوبات المنعقد في مدينة ريو دي جانيرو بالبرازيل سنة 1994م .

أولاً ـ الاتفاقية الأوروبية لمكافحة جرائم المعلوماتية

(اتفاقية بودابست نوفمبر 2001م)[36]:

لقد لعب المجلس الأوروبي دوراً كبيراً في هذا المضمار منذ ما يربو على عشرين سنة ، فقد بذلت محاولات عدة من أجل تكاثف الجهود لمكافحة جرائم المعلوماتية والتّصدي لها في نطاق الدّول المنضوية تحت مظلة المجلس المذكور والتي توّجت مؤخراً بإبرام الاتفاقية الأوروبية لمكافحة جرائم المعلوماتية ، أو ما أضحى يُعرف باتفاقية بودابست في 2001/11/23م ، والتي كانت ثمرة جهود متواصلة إلى أن بلغت الصّيغة النّهائية لها .

وقبل الوقوف على مضمون هذه الاتفاقية وأهدافها ، يقتضي تتبع الإرهاصات الأولية التي سبقت ميلادها . فالمجلس الأوروبي قد أقدم على عدة مبادرات مهّدت إلى عقد الاتفاقية المذكورة في نهاية المطاف[37]. ومن أهم هذه المبادرات في الاتجاه المذكور كانت الدّراسة التي أعدها المجلس الأوروبي مضمناً إياها جملة من التّوصيات تدعو إلى تفعيل دور القانون لمواجهة الأفعال غير المشروعة التي ترتكب عبر الحاسوب .

وفي عام 1995م تلتها دراسة أخرى تتعلق بالإجراءات الجنائية في مجال جرائم الإنترنت . وتأسيساً على ذلك انتهى المجلس إلى تشكيل لجنة لهذا الغرض سميت بلجنة خبراء الجريمة عبر العالم الافتراضي ، والتي أوكلت لها مهمة إعداد اتفاقية دولية ترمي إلى تسهيل التّعاون الدّولي في مجال الإجراءات الجنائية في الجرائم النّاشئة عن استخدام الحاسوب والإنترنت ، كما تمت في الوقت ذاته دعوة بعض الدّول من خارج المجلس الأوروبي للمساهمة في الإعداد لهذه الاتفاقية بصفة مراقب، والدّول التي وجهت إليها الدّعوة هي الولايات المتحدة

واليابان وكندا وجنوب أفريقيا .

وهذه الدّعوة لها أكثر من دلالة ، فمن ناحية أن بعض هذه الدّول المدعوة، والمتمثلة في الولايات المتحدة تحديداً لها صلة مباشرة بهذا الموضوع باعتبارها معنية أكثر من غيرها بمكافحة هذه الجرائم خاصة وأنها سنت تشريعات خاصة ، ومن ناحية ثانية أن دعوة مثل هذه الدّول للمشاركة في الإعداد لهذه الاتفاقية من شأنه أن يجعلها سارية في مفعولها على غير الدّول الأعضاء في المجلس الأوروبي ، أو بالأحرى ليكون باب الانضمام إليها مفتوحاً لغير الدّول الأعضاء ، وإن كانت المبادرة في أصلها أوروبية .

وكان عمل اللجنة سالفة الذكر قد أسفر عن صدور أول مشروع لهذه الاتفاقية وذلك في إبريل سنة 2000م تحت عنوان (اتفاقية الجريمة عبر العالم الافتراضي / الإنترنت) وهذا المشروع حظي بموافقة 43 دولة من الدول الأوروبية الأعضاء في المجلس الأوروبي .

ورغبة في تطوير هذه الاتفاقية ، فقد تمَّ تعميم المشروع سالف الذكر على ذوي الاختصاص من أجل إبداء الملاحظات بشأنه ، وتلقي الاعتراضات عليه إذا كان ثمة وجه للاعتراض قبل إصدارها في صورتها النّهائية .

ويبدو أن المشروع المذكور تخلله بعض القصور ، تجلّى في خلوه من النّص على بعض الجرائم كان يتعين تضمينها هذه الاتفاقية من وجهة نظر المختصين ، ومن ذلك جرائم الاختراق المعلوماتي . وعلى ضوء ذلك صدر المشروع المعدل الثّاني في شهر نوفمبر سنة 2000م مشتملاً على (48) مادة. وكان هذا المشروع محل خلاف ، وبالذات حول الإجراءات الجنائية ، ويتركز هذا الخلاف حول مسألة منح مزود خدمات الإنترنت الحق في الاحتفاظ

بالبيانات المطلوبة ، فذهب اتجاه إلى عدم منحه هذه الصّلاحية ، وكل ما يملكه لا يتعدى مجرد التّحفظ على الأدلة من أجل تمكين سلطات التّحقيق من القيام بعملها في تتبع وتعقب مرتكبي هذه الجرائم في أي مكان ، وهو الأسلوب الذي تبناه المشرع الأمريكي منذ خمس سنوات .

وثمة انتقادات وجهت إلى مشروع الاتفاقية المذكورة قبل أن تصل إلى صيغتها النّهائية بدعوى تهديدها للحقوق والحريات الأساسية، وتجسدت ردود الفعل السّلبية في مواجهة مشروع هذه الاتفاقية في بيان صدر سنة 2000م عن اثنتين وعشرين مؤسسة من المؤسسات الإقليمية والعالمية لحقوق الإنسان موجه إلى سكرتير المجلس الأوروبي ولجنة الخبراء في الجريمة عبر العالم الافتراضي والمجموعة العالمية لحريات الإنترنت ؛ بدعوى أن ثمة تعارضاً بين الالتّزام الذي تفرضه هذه الاتفاقية ومقتضيات حقوق الإنسان .

وقد بدا التردد في قبول هذه الاتفاقية في بادئ الأمر ؛ إذ كان ينظر إليها على أنها ليست نابعة من إرادة المجتمع الأوروبي ، وإنما هي ترديد لما أقره المشرع الأمريكي ، وإن تم تغليفها بالطّابع الدّولي من أجل منع تحرج الدّول الأوروبية من الانضمام إليها ، وحتى لا يقال بأن هذه الدّول ذات الماضي التّشريعي العريق تابعة للولايات المتحدة ، على اعتبار أن هذه الأخيرة هي صاحبة المبادرة في الدّعوة إلى التّعاون الدّولي في مكافحة جرائم الإنترنت لكي بتحقق الانسجام والتّوافق بين هذه الاتفاقية والتّشريع الأمريكي .

ولم يقف الأمر عند هذا الحد ، بل وُجّهت انتقادات أخرى لهذه الاتفاقية من أهمها ـ بالإضافة إلى ما سلف ـ مسألة التّعقب الدّولي للجريمة ، إذ من غير المسموح به إجراء تحقيقات للشرطة على إقليم دولة أخرى بدون أخذ

موافقتها المسبقة على ذلك .

والجدير بالذكر أن أبرز الانتقادات الموجهة لها كانت من منظمات حقوق الإنسان لما تتسم به من طابع بوليسي وما هو مخوّل لمأمور الضّبط القضائي من سلطات وصلاحيات واسعة . وقيل كذلك بأن مشروع هذه الاتفاقية يتنافى في جوهره مع المبادئ التي تضمنها الإعلان العالمي لحقوق الإنسان الذي يضع على عاتق الدّولة التّزاماً بحماية خصوصية الاتصالات .

وهكذا يمكن القول بأن هذه الاتفاقية قد مرّت بمخاض عسر قبل أن تأخذ طريقها إلى التطبيق .

وما يعنينا أن المشروع النّهائي للاتفاقية ضمَّ أربعة أقسام ، خُصِّصَ الأول لتحديد المفاهيم والمصطلحات ، أما القسم الثّاني فقد تضمن النّص على ما يتعين اتخاذه من خطوات في إطار التّشريعات الوطنية فيما يخصّ الأحكام الموضوعية والإجرائية ، أما القسم الثّالث فكان مخصصاً لموضوع التّعاون القضائي ، في حين أن القسم الرّابع والأخير يضم الشّروط النّهائية للانضمام للاتفاقية . وقد تمت الموافقة على المشروع النّهائي للاتفاقية في 2001/9/19م من قِبَل سفراء الدّول الأعضاء في مجلس أوروبا وذلك تمهيداً لعرضها على وزراء الخارجية . وفي 2001/11/23م خرجت إلى النور بالتّوقيع عليها في مدينة بودابست عاصمة المجر من قِبَل (30 دولة) من الدّول المنضوية تحت مظلة المجلس الأوروبي + الدّول الأربع من غير الأعضاء في المجلس المذكور ، وهي : الولايات المتحدة الأمريكية واليابان وكندا وجنوب أفريقيا .

وهي تتكون في صورتها النّهائية من (48 مادة) موزّعة على أربعة فصول، خُصِّصَ الفصل الأول منها لتحديد المفاهيم والمصطلحات ، في حين

خُصِّصَ الفصل الثّاني للتدابير التي يتعيّن على الدّول الأطراف اتخاذها على المستوى الوطني ، حيث أفردت الاتفاقية قسماً للقانون الجنائي الموضوعي وآخر للإجراءات الجنائية . وقد حدّدت مجموعة من الجرائم المعلوماتية متمثلة في الدّخول غير المشروع أو غير المصرّح به إلى شبكة المعلومات أو لأنظمة الحاسب الآلي ، والتّلاعب بالبيانات وتدميرها ، والاحتيال المعلوماتي ، والتّزوير ، ودعارة الأطفال، وإقامة المواقع الإباحية، وانتهاك حقوق الملكية والحقوق المجاورة .

وهي تُلقي على عاتق الدّول الأطراف سن التّشريعات اللازمة للتعامل مع طائفة جرائم المعلوماتية سالفة الذكر كلما كان ذلك ضرورياً واعتبارها جرائم في قوانينها الوطنية .

وفي الإطار ذاته خصصت الاتفاقية باباً مستقلاً للمساءلة القانونية والجزاءات التي يمكن للدولة الطّرف توقيعها حيال مرتكبي هذه الجرائم ، بما في ذلك مساءلة الشّخص الاعتباري .

فضلاً عن ذلك ، فقد أفردت أربعة أبواب للإجراءات الجنائية بما في ذلك إجراءات الضّبط والتّفتيش في نطاق بيئة المعلومات والحواسيب من خلال ضبط البيانات والمعلومات المخزنة ، واعتراض البيانات ، واتخاذ الإجراءات الوقائية المتمثلة في سرعة المحافظة على بيانات الحاسوب المخزنة وسرعة المحافظة على خط سير البيانات والكشف الجزئي عنها . ويشمل كذلك تفويض أو تخويل سلطان الدّولة الطّرف المختصة بإصدار الأوامر إلى الأشخاص الموجودين على إقليمها لتقديم بيانات مخزنة بالكمبيوتر تكون بحيازته أو تحت سيطرته ، وكذلك إصدار الأوامر إلى مجهزي الخدمة لتقديم معلومات أو بيانات تتعلق

بالمشترك صاحب الجهاز فيما يخص الخدمات الموجودة بحوزة أو تحت سيطرة مجهز الخدمة المعلوماتية .

أضف إلى ما تقدم أن هذه الاتفاقية تخول كل دولة طرف فيها كلما كان ذلك ضرورياً تفويض سلطاتها المختصة أو منحها حق أو صلاحية البحث في المنظومة المعلوماتية والدّخول إليها وإلى البيانات المخزنة بها ، بل ومصادرة البيانات، أو عمل نسخة من بيانات الحاسوب ، والمحافظة على وحدة وسلامة بيانات الحاسب الآلي المخزنة ذات الصّلة. وللدولة الطّرف الحق في تفويض سلطاتها المختصة بتجميع بيانات الحاسوب في الوقت الصّحيح ، وجمع أو تسجيل خط سير البيانات من خلال تطبيق الوسائل الفنية ، ولكل دولة طرف حق إلزام أحد مجهزي تقديم الخدمة المعلوماتية بالمحافظة على سريّة وقائع تنفيذ أية سلطات أو صلاحيات عن المعلومات المتعلقة بذلك .

ولم تغفل الاتفاقية تنظيم مسألة الاختصاص القضائي فيما يتعلق بالجرائم المنصوص عليها فيها ؛ إذ بمقتضاها يتحدد اختصاص قضاء الدّولة الطّرف في الأحوال التّالية :

1 ـ إذا كانت الجريمة مرتكبة على أراضيها .

2 ـ إذا كانت الجريمة مرتكبة على متن سفينة تحمل علمها .

3 ـ إذا كانت الجريمة مرتكبة على متن طائرة مسجلة وفقاً لقوانينها .

4 ـ إذا كانت الجريمة مرتكبة من قِبَل أحد مواطنيها إذا كان القانون يعاقب عليها في مكان ارتكابها ، أو إذا كانت قد ارتكبت خارج نطاق السّلطة القضائية الإقليمية لأية دولة.

ويجوز للدولة الطّرف أن تحتفظ بالحق في عدم التّطبيق أو التّطبيق فقط

في حالات أو ظروف معينة .

وفي حالة تنازع الاختصاص بين أكثر من دولة طرف فيما يتعلق بجريمة من الجرائم المنصوص عليها في هذه الاتفاقية ، فإن الدّول الأطراف المعنية يمكنها حل ذلك التّنازع بالتّشاور فيما بينها متى كان ذلك مناسباً بغية تحديد الاختصاص القضائي الأكثر ملاءمة .

في حين خصَّصت الاتفاقية المذكورة فصلاً مستقلاً للتعاون الدّولي في مواجهة جرائم المعلوماتية سالفة الذكر ، وهو الفصل الثّالث منها ، إذ تقضي بتعاون الدّول الأطراف فيها لأقصى حد ممكن من خلال تطبيق الاتفاقيات الدّولية ذات الصّلة أو القوانين المحلية أو وفقاً لمبدأ المعاملة بالمثل، وذلك فيما يخص عمليات التّحقيق والبحث أو جمع الأدلة الخاصة بالجرائم المعلوماتية أو فيما يخص الإجراءات أو التّدابير الخاصة بنظم وبيانات الحاسوب .

ومن أبرز أوجه التّعاون الدّولي التي نصت عليها هذه الاتفاقية والتي أفردت لها مساحة كبيرة ، مسألة تسليم المجرمين بين الدّول الأطراف بالنّسبة للجرائم سالفة الذكر من حيث ضوابط التّسليم وأحكامه (مادة 24) .

ودون الخوض في التّفاصيل ، فإن هذه الاتفاقية تعد بمثابة الإطار العام في تسليم المجرمين في الجرائم المذكورة في حالة عدم وجود اتفاقية خاصة بتسليم المجرمين بين الدّولتين طالبة التّسليم والمطلوب إليها التّسليم .

ليس هذا فحسب ، بل عنيت هذه الاتفاقية عناية كبيرة بموضوع المساعدة المتبادلة بين الدّول الأطراف فيما يخص تعقب الجناة والبحث عن الأدلة وتذليل كل ما من شأنه أن ييسر عملية الملاحقة القضائية وتفعيل هذه الاتفاقية وتحقيق أهدافها التي أبرمت من أجلها ، وقد أفردت لهذا الغرض 10

مواد من موادها الـ48 (المواد من 25 ـ 35) .

أما الفصل الرّابع والأخير ، والذي يضم باقي المواد (من 36 ـ 48) فقد خُصِّصَ للأحكام الختامية المتعلقة بالتّوقيع عليها ودخولها حيز التّنفيذ ، ومسألة الانضمام إليها ، والتّطبيق الإقليمي لها والتّحفظات المسموح للدولة إبداؤها أثناء التّوقيع أو الانضمام ، وآلية تعديل بعض بنودها ، وكيفية تسوية المنازعات النّاشئة عن تطبيقها بين الدّول الأطراف ، ومسألة فسخ الاتفاقية أو التّحلل منها وكيفية الإخطار .

ثانياً ـ موقف المؤتمرات الدّولية من إساءة استخدام الإنترنت :

لقد حظيت هذه المسألة باهتمام المؤتمرات الدّولية ، حيث تمَّ بحثها في مؤتمر الأمم المتحدة الثّامن لمنع الجريمة ومعاملة السّجناء المنعقد بـ(هافانا) بكوبا سنة 1990م ، كما أولتها الجمعية الدّولية لقانون العقوبات عنايتها في مؤتمرها الخامس عشر الذي عُقِد بعاصمة البرازيل آنذاك (ريو ديو جانيرو) ، ورغبة في الوقوف على جهودهما في هذا المضمار ، نحاول تسليط الضّوء على أهم التّوصيات التي انبثقت عن كلّ منهما ، والتي من شأنها تعزيز التّعاون الدّولي في التّصدي للجرائم النّاشئة عن إساءة استخدام الإنترنت .

أ ـ مؤتمر الأمم المتحدة الثّامن لمنع الجريمة ومعاملة السّجناء المنعقد بـ(هافانا عاصمة كوبا) سنة 1990م[38]:

إدراكاً من المؤتمر المذكور للمخاطر النّاجمة عن الجرائم ذات الصّلة بالحاسب الآلي، فإن القلق يساوره بشأن دور هذه التّقنية المتطورة في تيسير

اقتراف الجرائم محاولاً الرّبط بين الجريمة المنظمة وإساءة استخدام الحاسب الآلي والإنترنت ، ومن تم فإن المشاركين في أشغال هذا المؤتمر يؤمنون بضرورة تطوير سبل التّعاون الدّولي في هذا الميدان أخذاً في الاعتبار ما تتسم به هذه الجرائم من أبعاد دولية ، مما يتطلّب تطوير آليات مكافحتها والتّصدّي لها ، وعلى ضوء ذلك كله انتهى المؤتمر المذكور إلى جملة من التّوصيات بالخصوص ، والتي تمثل الإطار العام على المستوى الدّولي في مواجهة هذه الجرائم والحد من آثارها الضّارة ، ويمكن إجمال هذه التّوصيات في الآتي :

1 ـ أن تعمل الدّول الأعضاء على تكثيف جهودها في مواجهة عمليات إساءة استخدام الحاسب الآلي بتقرير جزاءات جنائية على الصّعيد الوطني .

2 ـ ينبغي أن يتخذ على الصّعيد الوطني جملة من التّدابير متى لزم الأمر، ومن ذلك:

أ ـ تحديث القوانين الرّاهنة فيما يخص سلطات التّحقيق وقبول الأدلة في الإجراءات القضائية وإدخال التّعديلات الملائمة كلما كان ذلك ضرورياً .

ب ـ العمل على مصادرة أو رد الأصول غير المشروعة النّاجمة عن ارتكاب الجرائم ذات الصّلة بالحاسوب .

جـ ـ العمل على تحسين التّدابير المتعلقة بالأمن والوقاية من مخاطر إساءة استخدام الحاسوب وحماية حقوق الإنسان وحرياته الأساسية بما في ذلك حماية الحق في الخصوصية .

د ـ تنمية الوعي لدى الجماهير والعاملين في الأجهزة القضائية وأجهزة إنفاذ القوانين بأبعاد المشكلة والتّحسيس بأهمية مكافحة الجرائم

ذات الصّلة بالحواسيب .

هـ ـ اعتماد تدابير مناسبة تستهدف تدريب رجال القضاء وكذلك الأجهزة المناط بها منع الجرائم الاقتصادية وتلك المرتبطة بالحاسوب فيما يخص التّحقيق فيها ومحاكمة مرتكبيها وإصدار الأحكام المتعلقة بها .

و ـ التّأكيد على ربط جسور التّعاون مع المنظمات المعنية بهذا الموضوع من أجل قواعد للآداب المرعية في استخدام أجهزة الحاسب الآلي وتضمين هذه الآداب في المناهج الدّراسية .

ز ـ اعتماد سياسات توفر الحماية لضحايا هذه الجرائم بحيث يراعى فيها أن تكون منسجمة مع إعلان الأمم المتحدة بشأن مبادئ العدل المتعلقة بضحايا الإجرام والتّعسف في استعمال السّلطة ، وبحيث تتضمن هذه السّياسات إعادة الممتلكات التي يتم الحصول عليها بطرق غير مشروعة ، واتخاذ التّدابير المناسبة التي من شأنها تشجيع الضّحايا على إبلاغ السّلطات المختصة بمكافحة هذا النّوع من الجرائم .

ح ـ كما يولي المؤتمر المذكور اهتماماً كبيراً بأهمية التّعاون الدّولي في ميدان مكافحة الجرائم المشار إليها باتخاذ التّدابير التّشريعية التي تكفل المشاركة في معاهدات تسليم المجرمين وكذلك التّعاون بين الدّول في إجراءات التّحقيق .

ط ـ فضلاً عن ذلك فإن المؤتمرين يهيبون بالأمين العام للأمم المتحدة والدّول الأعضاء توفير الميزانيات اللازمة لتمويل أنشطة مكافحة

هذه الجرائم المستحدثة.

ب ـ المؤتمر الدّولي الخامس للجمعية الدّولية لقانون العقوبات (4 ـ 1994/10/9) الذي عقدته في مدينة (ريو دي جانيرو بالبرازيل) بشأن جرائم الكمبيوتر[39]:

دأبت الجمعية الدّولية لقانون العقوبات منذ تأسيسها على عقد مؤتمرات تهتم بموضوعات السّياسة الجنائية سواء في شقها الإجرائي أو الموضوعي ، وكثيراً ما تفرد لكل مؤتمر من المؤتمرات التي تعقدها موضوعاً واحداً تراه جديراً بالدّراسة والبحث ، من أجل الوصول إلى حلول للإشكاليات التي يطرحها ، وسيراً على السّنة التي سارت عليها ، فقد جعلت مؤتمرها الخامس عشر الذي عُقِدَ في 4 ـ 1994/10/9م مكرّساً لجرائم الحاسوب (الكمبيوتر) ، بالنّظر إلى أهمية الموضوع وما تتطلبه مواجهة هذه الجرائم من جهود على المستويين الوطني والدّولي. وقد صدر عن المؤتمر المذكور عدة توصيات ، منها ما يتصل بالجانب الموضوعي (فيما يخص التّجريم) ، ومنها ما يتعلق بالجانب الإجرائي .

وعلى صعيد التّجريم أوصى المؤتمر بضرورة تجريم طائفة من الأفعال بوصفها من جرائم الحاسوب ، وهي تشمل الاحتيال أو الغش المرتبط بالحاسوب والتزوير بواسطة الحاسوب أو التّزوير المعلوماتي ، والإضرار بالبيانات والبرامج ، وتخريب وإتلاف الحاسوب، والدّخول غير المصرح به ، وأخيراً الاعتراض غير المصرح به .

أما بخصوص الجانب الإجرائي ، فإن المؤتمر المذكور يوصي بأن التّنقيب في جرائم المعلوماتية يتطلب وضع مكنات قسرية تحت تصرف سلطات التّحقيق والتّحري وبما يتلاءم مع الحماية الكافية لحقوق الإنسان وحرمة الحياة الخاصة ،

وألا يقبل تقييد حقوق الإنسان من قبل رجال السّلطة العامة إلاّ على أسس قانونية واضحة ودقيقة وبما ينسجم مع المعايير الدّولية لحقوق الإنسان .

وفي ضوء ما تقدم يتعين تحديد السّلطات التي يعهد إليها بإجراءات التّفتيش والضّبط في بيئة تكنولوجيا المعلومات ، وبصفة خاصة ضبط الأشياء غير المحسوسة وتفتيش شبكة المعلومات .

كما يوصي هذا المؤتمر بتخويل السّلطات العامة باعتراض الاتصالات داخل نظام الحاسب ذاته مع استخدام الأدلة التي يتم الحصول عليها في الإجراءات أمام المحاكم .

ويراعى أن يكون تنفيذ الإجراءات القسرية متناسباً مع الطّابع الخطير للانتهاكات، مع الأخذ في الاعتبار كل القيم المرتبطة ببيئة تكنولوجيا المعلومات مثل ضياع فرصة اقتصادية ، والتّجسّس ، وانتهاك حرمة الحياة الخاصة ، ومخاطر الخسارة الاقتصادية ، وتكلفة إعادة بناء البيانات كما كانت من قبل .

أضف إلى ذلك يوصي المؤتمر المذكور بوجوب تحديد القواعد التي يتعين العمل بها في قبول الأدلة تحديداً واضحاً ، وهو ما يتطلب إدخال بعض التّعديلات التّشريعية إذا لزم الأمر .

الخاتمـــــة

حاولنا من خلال هذه الورقة المتواضعة الوقوف على ملامح السّياسة الجنائية بشأن مكافحة جرائم الإنترنت ، والذي تطلّب الإحاطة بتعريف هذه الطّائفة من الجرائم والخصائص المميزة لها ، وما يمكن أن يواجه القائمين على مواجهتها من تحديات ، وإبراز الإشكاليات القانونية التي تثار في هذا الخصوص، كما وقفنا بإيجاز على الجهود المبذولة للتصدي لها ، سواء على الصّعيد الوطني أم على الصّعيدين الإقليمي والدّولي ، وقد خلصنا من كل ما تقدَّم إلى عدة نتائج يمكن إيجازها فيما يلي:

1 ـ إن هذه الجرائم تتسم بعدد من الخصائص التي تنفرد بها عن غيرها من الجرائم التّقليدية سواء من حيث أسلوب ارتكابها أو دوافعها أو من حيث الصّفات التي يتّصف بها مقترفوها ، وكذلك من ناحية آليات المواجهة ، وهذا كله أدى إلى أن القائمين على مكافحتها يواجهون جملة من التّحديات تتجلّى في المقام الأول في صعوبة إثبات هذه الطّائفة من الجرائم وتعقّب مرتكبيها وضبطهم . فضلاً عن أن هذه الجرائم ذات بُعد دولي لكونها عابرة لحدود الدّول والقارات ، الأمر الذي يثير إشكالية تحديد مكان وقوع الجريمة ومن ثم تحديد الاختصاص والقانون الواجب التّطبيق .

2 ـ عجز كثير من التّشريعات العقابية النّافذة في كثير من الدّول ، ومنها جلّ الدّول العربية ، عن مواجهة هذه الظاهرة ، إذ ظلّت على حالها ، ولم يطرأ عليها أي تعديل بما يتلاءم والتّصدّي لهذه الجرائم ، وفي المقابل سعت عدة دول إلى إجراء تعديلات على تشريعاتها بما يسمح بتوفير الحماية الجنائية

لنظم المعلومات . ولم يقف الأمر عند هذا الحد ، بل ثمة دول خطت خطوات متقدمة بإصدار تشريعات خاصّة .

3 ـ إن كثيراً من الدّول ـ حتى بالنّسبة للتي لم تتصدَّ لتجريم صور إساءة استخدام الإنترنت ـ عملت على استحداث أجهزة متخصصة يُناط بها مواجهة هذه الظاهرة المستحدثة بتكوين الأطر المؤهلة للتعامل معها فيما يتعلّق بكشف هذه الجرائم وتعقّب مرتكبيها وضبطهم ، وهو اتجاه يستحق التّنويه ، وينمّ عن شعور متزايد بالمخاطر المطّردة النّاجمة عن هذه الجرائم .

4 ـ في سبيل توسيع نطاق مكافحة هذه الجرائم على المستوى الإقليمي والدّولي اتجهت بعض الدّول إلى إبرام بعض الاتفاقيات فيما بينها ، ومن أبرزها اتفاقية بودابست الموقعة من دول المجلس الأوروبي وبعض الدّول الأخرى ، والتي رسمت استراتيجية واضحة المعالم للتعاون فيما بينها للحدّ من مخاطر هذه الجرائم بما فرضته من التّزامات على أطرافها سواء فيما يتعلق بضرورة تعديل تشريعاتها الوطنية أو فيما يخص قواعد تسليم المجرمين وتقديم أوجه المساعدة المتبادلة بينها.

ومع ذلك ، ورغم الجهود المبذولة على الصّعيدين الوطني والدّولي، فإنّ خطر هذه الظاهرة يتفاقم يوماً عن يوم ، لذا نقترح تضمين هذه الورقة بعض التّوصيات التي نراها قد تسهم في الحد من هذه الجرائم ، ومن ذلك :

1 ـ حث الدّول التي لم تبادر إلى رسم سياسة جنائية لمواجهة هذه الأفعال أن تسارع بسن تشريعات خاصة ، أو على الأقل العمل على تعديل قوانينها النّافذة بما يتّسع لتجريمها بدلاً من الرّكون إلى القواعد التّقليدية التي لم تعد كافية باعتبارها وضعت في زمن غير هذا الزّمن وذلك أسوة بغيرها من

الدّول المتقدمة التي انتهجت هذا النّهج منذ وقت مبكّر .

2 ـ التّأكيد على ضرورة استحداث أجهزة فاعلة يعهد إليها أمر ضبط جرائم الحاسوب والإنترنت والتّعامل معها ، وذلك بإعداد أطر مؤهلة في هذا الخصوص من أولئك الحاصلين على مؤهلات عليا في مجال الحاسوب .

3 ـ التّنسيق بين الدّول فيما يتعلّق بالتّصدي لهذه الجرائم ومكافحتها بإبرام اتفاقيات خاصة ، وتفعيل التّعاون الدّولي بخصوص تسليم المجرمين وتقديم المساعدات الممكنة لتيسير تعقب الجناة ، بما في ذلك تسهيل مهمة المحققين ورجال الضّبط القضائي بالقيام ببعض الإجراءات القانونية ذات العلاقة على أراضيها إذا اقتضى الأمر أو تفويض سلطاتها القضائية بهذا الأمر بموجب إنابات قضائية .

4 ـ العمل على رفع كفاءة رجال القضاء لتهيئتهم للتعامل مع هذه الجرائم سواء في مجال التّحقيق أو المحاكمة ، ويتأتى ذلك من خلال التّدريب أثناء الخدمة عن طريق معاهد القضاء وذلك من أجل تنمية الوعي لديهم بأبعاد المشكلة وبأساليب ارتكاب هذه الجرائم .

5 ـ ضرورة إجراء تعديل للقوانين الإجرائية القائمة بما يسمح بتفعيل مكافحة هذه الجرائم وتعقّب الجناة والتّحقيق معهم ، بما في ذلك السّماح بتفتيش الحواسيب الشّخصية والشّبكة المعلوماتية ، بشرط أن يتم ذلك تحت إشراف القضاء وبإذن منه ضماناً لعدم التّعسّف أو انتهاك حرمة الحياة الخاصّة ، ولو استلزم الأمر اعتراض الاتصالات التي تتم عبر شبكة المعلومات ، مع تحديد معايير واضحة لقبول الأدلة المستمدة من ذلك أمام القضاء .

6 ـ العمل على نشر الثّقافة المعلوماتية لدى طلاّب كليات القانون وكليات الشرطة ومعاهد القضاء من خلال إفراد بعض المقررات الدّراسية ذات العلاقة كمبادئ الحاسوب والتّجارة الإلكترونية وجرائم الحاسب الآلي والإنترنت .

7 ـ توجيه طلاب الدّراسات العليا في الجامعات العربية وتشجيعهم على تسجيل رسائل الماجستير وأطروحات الدّكتوراه في هذا المجال .

8 ـ تسخير وسائل الإعلام المختلفة لإرشاد مستخدمي شبكة المعلومات الدّولية (الإنترنت) وتوعيتهم بمخاطر إساءة استخدام هذه الشّبكة وما قد ينجم عن ذلك من أضرار فادحة ، وكيفية توقي ما يمكن أن يتعرضوا له من اعتداءات من قبل غيرهم من المستخدمين الآخرين والحيلولة دون وقوعهم ضحايا للإجرام المعلوماتي .

الهوامـــش

(1) ـ محمـد أمـين الرومـي ، جـرائم الكمبيـوتر والإنترنـت ، دار المطبوعـات الجامعيـة ـ الإسكندرية ، 2004م ، ص7 .

Voir : Dr. Mohammed Buzubar : "La Criminalité Informatique sur L'internet", Journal of Law , (Kwait University) , No. 1 , Vol. 26 , March 2002 , P. 21.

المحامي يونس عرب ، العالم الإلكتروني طريق المعلومات السريع ، مختارات من كتابه قانون الكمبيوتر ، منشورات اتحاد المصارف العربية ، 2001 ، على شبكة الإنترنت :

http://www.arablaw.org/Electronic%20world htm ;

د.جميل عبدالباقي الصغير ، القانون الجنائي والتكنولوجيا الحديثة ، الكتاب الأول : الجرائم الناشئة عن استخدام الحاسب الآلي ، دار النهضة العربية ـ القاهرة ، 1992م، ص4 ، 5 ؛ د.علي عبدالقادر القهوجي ، الحماية الجنائية لبرامج الحاسب ، دار الجامعة الجديدة للنشر ـ الإسكندرية ، 1997م ، مقدمة الكتاب ؛ د.محمد سامي الشوا ، ثورة المعلومات وانعكاساتها على قانون العقوبات ، الطبعة الثانية ، دار النهضة العربية ـ القاهرة ، 1998م ، ص3 ؛ د.محمد عبدالله القاسم، ود. رشيد بن مسفر الزهراني ، نموذج وطني مقترح للتعامل مع جرائم المعلوماتية بالمملكة العربية السعودية، الدليل الإلكتروني للقانون العربي ، على شبكة الإنترنت:

www.arablawinfo.com

Bart De Schutter , A Propos de la fraude Informatique , Rev . dr. Pén. crim . 1985 , P. 383 .

وانظر كذلك : عبدالله العلوي البلغيثي : "الإجرام المعاصر أسبابه وأساليب مواجهته"، ورقة مقدمة ضمن أشغال المناظرة الوطنية حول (السياسة الجنائية بالمغرب : واقع وآفاق) التي نظمتها وزارة العدل بمكناس أيام 9 و10 و11 دجنبر (ديسمبر) 2004م ، المجلد الأول ، (الأعمال التحضيرية) ، الطبعة الثانية ،

منشورات جمعية نشر المعلومة القانونية والقضائية ، سلسلة الندوات والأيام الدراسية، العدد (3) ، 2004م ، ص222 .

(2) ـ عقيد / محمد عبدالله المنشاوي ، دراسة جرائم الإنترنت ـ محاولة لتحديد جرائم الإنترنت في المجتمع السعودي ، موقع المنشاوي للدراسات والبحوث على شبكة الإنترنت :

http://www.minshawi.com/ginternet/interduse.htm

تاريخ الزيارة : 31 / 03 / 2007م .

د.جميل الصغير ، ص5 وما بعدها ؛ لواء/د. حسنين المحمودي بوادي ، إرهاب الإنترنت الخطر القادم ، الطبعة الأولى ، دار الفكر الجامعي ـ الإسكندرية، 2006م، ص49 وما بعدها؛ محمد أمين الرومي ، ص7.

(3) ـ د. عمر محمد بن يونس ، الجرائم الناشئة عن استخدام الإنترنت ، الطبعة الأولى ، دار النهضة العربية ـ القاهرة ، 2004م ، ص181 وما بعدها ؛ يونس عرب ، جرائم الإنترنت المعنى والخصائص والصور واستراتيجية المواجهة القانونية ، على الإنترنت :

http://www.arablaw.org/Download/Cybercrimes_General doc.

(4) ـ اللواء / محمد الرشيدي ، الجرائم الإلكترونية والتأمين الإلكتروني ، مجلة قضايا (تصدر عن المركز الدولي للدراسات المستقبلية والاستراتيجية) ، العدد (11) ، س1، نوفمبر 2005م ، ص22 ؛ محمد عبدالله المنشاوي ، جرائم الإنترنت من منظور شرعي وقانوني، موقع المنشاوي للدراسات والبحوث على شبكة الإنترنت:

http://www.minshawi.com/old/internetcrim-in%20 the %20 law.htm

تاريخ الزيارة : 17 / 03 / 2007م .

وانظر كذلك : د. محمد سيد أحمد الزغبي ، جرائم الإنترنت والمعلومات ، بحث مقدم إلى مؤتمر الأمن والتكنولوجيا الذي عقدته شرطة الشارقة خلال الفترة من 6 ـ 8 نوفمبر 2006م، الأبحاث الأكاديمية ، الطبعة الأولى ، منشورات أكسبو ،

ص54 ؛ وحول تعريف جرائم المعلوماتية انظر على شبكة الإنترنت :

Introduction on cyber crime

الموقع : http://cybercrime.planetindia.net/intro.htm

(5) ـ على شبكة الإنترنت انظر :

http://www.symantec.com/avcenter/cybercrime.index_Pag2.htm
cybercrime, cyberterrorist, and Digital Law Enforcement, NewYork
(http://cybercrime advanced studies.org)

وانظر كذلك : محمد أمين الرومي ، ص19 .

(6) ـ انظر : يونس عرب ، الخصوصية وأمن المعلومات في الأعمال اللاسلكية بواسطة الهاتف الخلوي ، ورقة مقدمة إلى منتدى العمل الإلكتروني بواسطة الهاتف الخلوي، اتحاد المصارف العربية ، 22 أيار 2001م ، عمان ـ الأردن ، ص19 .

(7) ـ وليد الزيدي ، القرصنة على الإنترنت والحاسوب (التشريعات القانونية) ، الطبعة الأولى ، دار أسامة للنشر والتوزيع ـ عمان ـ الأردن ، 2003م، ص39 ـ 41 ؛ محمد أمين الرومي ، ص23 ؛

Mohammed Buzubar , op. cit , PP. 43 - 49

(8) ـ انظر : د. عبدالله حسين علي محمود ، سرقة المعلومات المخزنة في الحاسب الآلي ، الطبعة الأولى ، دار النهضة العربية ـ القاهرة ، 2001م ، ص68 وما بعدها ؛ محمد أمين الرومي ، ص23 ـ 26 ؛

Mohammed Buzubar , op. cit , PP. 52, 53.

(9) ـ د. عبدالله حسين علي ، ص75 .

(10) ـ د. محمد رشيد أحمد الزغبي ، ص57 ؛ د. جميل الصغير ، ص10 ؛ لواء/د.حسنين المحمود بوادي ، ص75 ـ 77 .

وقارن : د. محمد سامي الشوا ، ص8 وما بعدها ؛ اللواء/ محمود الرشيدي ، ص23 ـ 24 ؛ د. عبدالله حسين علي محمود ، ص77 ؛ محمد محمد شتا ، فكرة الحماية الجنائية لبرامج الحاسب الآلي ، دار الجامعة الجديدة للنشر ـ الإسكندرية ، 2001م ، ص76 وما بعدها ؛ منير محمد الجنبيهي ، وممدوح محمد الجنبيهي،

جرائم الإنترنت والحاسب الآلي ووسائل مكافحتها ، دار الفكر الجامعي ـ الإسكندرية ، 2005م، ص13 وما بعدها ؛ وليد الزيدي، ص27 وما بعدها ؛ عبدالله العلوي البلغيثي ، ص224 .

(11) ـ محمد رشيد الزغبي ، ص56 ؛ عصام الدين الأمين ومحمد نور ، جرائم المعلوماتية، ورقة مقدمة إلى الندوة العلمية حول مشروع قانون مكافحة جرائم المعلوماتية (السوداني) لسنة 2006م، المنعقدة يوم الأحد الموافق 25 يونيه 2006م.

(12) ـ محمد محمد شتا ، ص103 .

(13) ـ د. محمد سامي الشوا ، ص87 ؛

Voir : Martine Briat, La Fraude Informatiquel une approche de droit comparé, Rev. dr. pén. crim. 1985 ; R. Gassin, La droit pénal de l'informatique,
D. 1988. chr., 35 . ; Françoise chamoux , La loi sur la Froude informatique, de nous elles incriminations, J.C.P.1988 -1- 13321 .

(14) ـ يونس عرب ، الخصوصية وأمن المعلومات ، ص20 .

(15) ـ انظر على شبكة الإنترنت :

www.omano.net

محمد أمين الرومي ، ص7 ، 8 .

(16) ـ عبدالله العلوي البلغيثي ، ص225 ، 226 .

(17) ـ القانون المذكور منشور على شبكة الإنترنت :

http://www.openarab.net/Laws/2006/Laws8.shtm.

(18) ـ انظر على شبكة الإنترنت :

http://Sudan_parliament.org/details.php?rsnType=18id=423

(19) ـ انظر على شبكة الإنترنت :

http://www.Swalif.net/softs/showthread.php?t=192022
http://www.alinqad.com/different/php?Filename=20070327 1244230

(20) ـ وهو القانون رقم (289) لسنة 1973م (انظر : د. محمد سامي الشوا، ص207؛ وكذلك صحيفة عكاظ في عددها الصادر يوم الخميس الموافق 27 ـ 1 ـ 1425هـ موقع المنشاوي على الإنترنت :

http://okaz.com.sa/okaz/Data/2004/3/18/Art_85170.XML
وانظر كذلك : د. عبدالله حسين علي محمود ، ص308 ، 309 .
تجدر الإشارة إلى أن القانون المذكور قد عُدّل أكثر من مرة في السنوات : 79 ، 82، 86 ، 90 ، 92 ، ثم حلَّ محله لاحقاً قانون البيانات الشخصية لسنة 1998م (انظر : منير الجنبيهي وممدوح الجنبيهي ، بروتوكولات وقوانين الإنترنت ، دار الفكر الجامعي ـ الإسكندرية ، 2005 ، ص65) .

(21) ـ انظر : الإجراءات الجنائية عبر الإنترنت في القانون الأمريكي ، (المرشد الفيدرالي الأمريكي لتفتيش وضبط الحواسيب وصولاً إلى الدليل الإلكتروني في التحقيقات الجنائية) ، ترجمة ودراسة وتحقيق : د. عمر محمد بن يونس ، الطبعة الأولى ، 2004 ـ 2005م ، ص275 .

(22) ـ المرجع السابق ، ص324 .

(23) ـ المرجع السابق ، ص329 .

(24) ـ المرجع السابق ، ص339 .

(25) ـ المرجع السابق ، ص349 .

(26) ـ المرجع السابق ، ص373 .

(27) ـ انظر : د. عبدالله حسين محمود ، ص317 . كما صدر قانون حماية المعطيات لسنة 1984م ، وتمَّ تعديله عام 1996م ، وقانون حماية البيانات لسنة 1998م الذي استحدث تعديلاً للقانون الصادر سنة 1984م ، ثم قانون حرية المعلومات لسنة 2000م (انظر : منير الجنبيهي وممدوح الجنبيهي ، بروتوكولات وقوانين الإنترنت ، ص70) .

(28) ـ د. محمد سامي الشوا ، ص207 .

(29) ـ انظر : د. هدى حامد قشقوش ، جرائم الحاسب الآلي في التشريع المقارن ، دار النهضة العربية ، القاهرة، 1992م ، ص8 ؛ د. محمد سامي الشوا ، ص208 ؛ د.عبدالله حسين علي محمود ، ص301 ؛ منير محمد الجنبيهي وممدوح محمد

الجنبيهي ، جرائم الإنترنت والحاسب الآلي ووسائل مكافحتها ، ص187 ؛ محمد أمين الرومي ، ص7 .

(30) ـ انظر : د. عمر بن يونس ، الجرائم الناشئة عن استخدام الإنترنت ، ص153.

(31) ـ لواء / محمد رضا عاشور ، الإنترنت والمجالات الأمنية ، بحث مقدَّم إلى مؤتمر الأمن والتكنولوجيا الذي عقدته شرطة الشارقة خلال الفترة 6 ـ 8 نوفمبر 2006م ، منشورات مركز إكسبو ـ الشارقة ، الطبعة الأولى 1427هـ ـ 2006م، ص106 .

(32) ـ المرجع السابق ، ص107 ، 108 .

(33) ـ المرجع السابق ، ص108 ، 109 .

(34) ـ المرجع السابق ، ص109 .

(35) ـ صدر هذا القرار بتاريخ 2005/04/2م .

(36) ـ Convention on cybercrime Budapest, 23. XI. 2001

على شبكة الإنترنت :

http://www.conventions.coe.int/Treaty/EN/Treaties/Html/185.htm
http://www. conventions.coe.int/Treaty/EN/cadreliste/Treaties/htm.

وانظر كذلك / منير الجنبيهي وممدوح الجنبيهي ، المرجع السابق ، ص180 ـ 185

(37) ـ انظر حول ذلك بتفصيل أكثر : د. عمر محمد بن يونس، جرائم الإنترنت ، ص198 ـ 216.

(38) ـ http://www.arabswata.org/Forums/archive/index.php/t-3201.html

(39) ـ انظر : د. هلالي عبداللاه أحمد ، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي ـ دراسة مقارنة ، الطبعة الأولى ، دار النهضة العربية ـ القاهرة ، 1997م، ص5، 6.