ملخص عن البحث الموسوم

المواجهة التشريعية لجرائم المعلوماتية في النظام البحريني على ضوء اتفاقية بودابست

تأليف

أ.د. هلالى عبداللاه أحمد

أستاذ القانون الجنائي

كلية الحقوق – جامعة البحرين

١- تقديم:

تدور فكرة البحث[1] حول كيفية المواجهة التشريعية لجرائم المعلوماتية على ضوء اتفاقية بودابست، وذلك بغرض أن نقدم للمشرع البحريني نموذجا يحتذي في تقنين هذه النوعية من الجرائم.

وتحقيقاً لهذه الغاية التى نهفو إليها فقد قسمنا هذا البحث إلى خمسة فصول يسبقها فصل تمهيدى ويتبعها خاتمة.

٢- موضوع البحث:

فلقد قمنا فى الفصل التمهيدى بتحديد موضوع البحث وأهميته وموقف التشريعات منه. كما صغنا مشكلة البحث الرئيسة والإجراءات المنهجية المتبعة فى حلها.

٣- الجذور التاريخية والتعريفات:

وفى الفصل الأول تناولنا الجذور التاريخية لفكرة المعلومات وأوعية التدوين الخاصة بها، وكيف تطورت إلى أن أصبح لها علم مستقل بها ينتظم جزئياتها ويلملم محتوياتها، يطلق عليه علم المعلومات information science. ويقصد به ذلك العلم الذى يهتم بدراسة خصائص وسلوك المعلومات، وإنشائها واستخدامها والقوى التى تتحكم فى انسيابها وإدارتها ووسائل معالجتها وتجهيزها لأقصى درجة من الوصول والاستخدام ويشمل التجهيز إنتاج المعلومات وبثها وتجميعها وتنظيمها واختزانها واسترجاعها وتفسيرها واستخدامها.

وعلم المعلومات بهذا المفهوم يرادف – وفقاً لرأى جانب كبير من العلماء والباحثين – المعلوماتية informatics وذلك على أساس أن جوهر المعلوماتية هو تقنيات المعلومات من عتاد وحاسبات وبرمجيات وشبكات ومزودات قواعد البيانات ومحطات اتصال.

[1] يقع اصل هذا البحث في ٣٨٦ صفحة وهو بحث ممول من عمادة البحث العلمي بجامعة البحرين. وقد تم تحكيمه عن طريق محكمين مشهود لهم بالتبحر في العلم والمعرفة والتعمق في البحث والتفنيد. ونظرا لضخامة عدد صفحاته فقد كلفت المجلة الباحث بإعداد هذا الملخص.

وبتحليل مصطلح المعلوماتية informatics يتبين أنه عبارة عن موضوع ومجموعة من العمليات الآلية التى يخضع لها هذا الموضوع. فموضوع المعلوماتية يتمثل فى البيانات والمعلومات. أما مجموعة العمليات الآلية التى يخضع لها هذا الموضوع فتتمثل فى عمليات الجمع والتحليل والمعالجة والصياغة والنقل والتداول وغيرها، والتى تتم من خلال الحاسبات أو ما يقوم مقامها من النظم المطمورة Embedded systems وشبكات الاتصال.

وبناء على ذلك قمنا بوضع التعريف الاشتراطى الآتى للمعلوماتية: "أنها ذلك العلم الذى يهتم بالبيانات والمعلومات ومجموعة العمليات الآلية التى تخضع لها من جمع وتحليل وتخزين ومعالجة وصياغة واسترجاع ونقل وتداول وفقاً للتقنيات الحديثة لنظام معلوماتى معين يتمثل فى نظم الحاسبات الآلية وما يقوم مقامها من النظم المطمورة وشبكات الاتصال".

وحتى نزيد هذا التعريف وضوحاً وجلاء ألقينا مزيداً من الضوء على ثلاثة اصطلاحات وردت به. أولها الحاسبات، ويقصد بالحاسب جهاز اليكترونى يستطيع ترجمة أوامر مكتوبة بتسلسل منطقى لتنفيذ عمليات إدخال بيانات، أو إخراج معلومات، وإجراء عمليات حسابية أو منطقية، وهو يقوم بالكتابة على أجهزة الاخراج أو التخزين الرئيسة أو الثانوية، التقليدية أو المستحدثة كالذاكرة الوميضية Flash memory. والبيانات يتم إدخالها بواسطة مشغل الحاسب عن طريق وحدات الإدخال التقليدية أو المستحدثة كتقنيات القياس الحيوى Biometric Technologies أو استرجاعها من خلال وحدة المعالجة المركزية التى تقوم بإجراء العمليات الحسابية والمنطقية. وبعد معالجة البيانات تتم كتابتها على أجهزة الإخراج التقليدية أو المستحدثة كسبورة الشرح التفاعلية أو السبورة الذكية Smart Board.

ثانيها : النظم المطمورة Embedded systems وهى عبارة عن وسيلة تستخدم فى التحكم أو فى مراقبة أو فى مساعدة تشغيل معدة أو آلة أو مصنع، بحيث تصبح جزءاً لا يتجزأ منها. وهى تتكون من معالج دقيق أو جهاز تحكم دقيق أو دوائر متكاملة ذات تطبيق خاص. فالنظم المطمورة مبرمجة لأداء منظومة ثابتة من المهام.

وثالثها: شبكات الاتصال Communication networks ويقصد بها مجموعة من الحاسبات متصلة بعضها ببعض بخطوط اتصالات سلكية أو لاسلكية لتتقاسم العمل فيما بينها أو لتبادل المعلومات. وتقوم شبكات الاتصال بدور بالغ الأهمية بالنسبة لنقل وتداول المعلومات وإتاحتها على نطاق واسع وكبير شمل أرجاء المعمورة بأسرها. فلقد تعاظم فى

الآونة الأخيرة دور هذه الشبكات فى الربط بين النظم المعلوماتية داخل المصالح والشركات والمؤسسات المختلفة، أو الربط بين الأشخاص بعضهم بعضا. بل لقد ازداد هذا الدور تعاظماً من خلال التطوير الدائم والتحديث المستمر للخدمات التى تقدمها شبكة المعلومات الدولية الإنترنت Internet مثال ذلك خدمات الويب Web الشهيرة وعلى رأسها خدمة هاتف الإنترنت Internet Telephony والتى قد يطلق عليها هاتف عبر بروتوكول الإنترنت IP Telephony أو فى تسمية ثالثة "خدمة الصوت عبر بروتوكول الإنترنت" Voice Over Internet Protocol VOIP كذلك يضاف إلى الخدمات السابقة التى أتاحتها الشبكة الدولية للمعلومات خدمة الرسائل القصيرة لأجهزة الهاتف الجوال Short Message Service SMS.

والذى نود أن نخلص إليه من تحليل مفردات النظام المعلوماتى هو أن هذا المصطلح لا يقتصر فقط على الحاسبات بل يشمل أيضاً النظم المطمورة ،ولذلك يعد قصر نطاق النظام المعلوماتى على الحاسبات الآلية خطأ من الناحية التقنية وقصورا في التعريف من الناحية القانونية. هذا بالإضافة إلى أنه يمكن الآن الاستغناء عن الحاسبات الآلية والاتصال مباشرة بشبكة الانترنت عن طريق الهاتف الجوال بعد تزويد الجيل الثالث من هذه الهواتف بخاصية الويب Web. ليس هذا فحسب بل يمكن تحميل down load بعض المواقع على الهاتف الجوال مثال ذلك www. facebook.com [2] وكذلك موقع عنكبوت www.join3ankaboot.com وعنكبوت هو أول شبكة خدمات من نوعها فى العالم العربى تعرض مجاناً من خلال الهواتف الجوالة. ويحتوى عنكبوت على مجموعة من التصنيفات والخدمات والبرامج التى تلبى الاهتمامات لكل من الأفراد والهيئات.

وعلى ضوء هذه المعطيات مجتمعة عرفنا جرائم المعلوماتية بأنها: فعل أو امتناع يأتيه شخص طبيعي أو معنوي عن طريق ممثليه، باستعمال نظام معلوماتي معين يتمثل في الحاسبات أو ما يقوم مقامها من نظم مطمورة، وشبكات الاتصال، إضراراً بمصلحة أو حق يحميه القانون من خلال جزاء جنائي، سواء كانت هذه المصالح أو الحقوق المحمية تمثل نماذج معلوماتية مستحدثة، أو كانت تدخل في نطاق المصالح أو الحقوق التى كان يحميها مسبقاً قانون العقوبات بالطرق التقليدية، وسواء كان الاعتداء واقعاً داخل حدود الدولة أو كان يمس أقاليم عدة دول.

[2] للمزيد عن هذا الموقع راجع : د. جمال مختار: "حقيقة الفيس بوك" مصر، شركة متروبول للطباعة، الطبعة الأولى، ٢٠٠٨.

ويتضمن هذا التعريف الذى قلنا به خمسة عناصر أساسية نرى أنها ضرورية فى أى تعريف لجرائم المعلوماتية أولها الوسيلة المستخدمة فى ارتكاب الجريمة المعلوماتية ولابد أن تكون نظاماً معلوماتياً. وثانيهاً : شخص مرتكب الجريمة ويمكن أن يكون شخصاً طبيعياً أو معنوياً. وثالثها محل الجريمة المعلوماتية ويمكن أن يكون نماذج معلوماتية مستحدثة أو حقوقا تقليدية. رابعها مراعاة مبدأ الشرعية الجنائية إذ لا جريمة ولا عقوبة إلا بنص. خامسها نطاق تطبيق الجريمة المعلوماتية إذ يمكن أن تقع داخل حدود الدولة ويمكن أن تمس أقاليم عدة دول. وفى هذه الحالة الأخيرة تثير مجموعة من المسائل القانونية أوردناها في حينها.

٤- المواجهة الموضوعية لجرائم المعلوماتية :

وبعد إيراد هذه التحليلات والتعريفات والتعليقات التي قيلت بصددها شعرنا أن الطريق قد أصبح واضحاً وممهداً لدراسة كيفية المواجهة الموضوعية لجرائم المعلوماتية، وهذا ما خصصنا له الفصل الثانى من دراستنا.

وينقسم هذا الفصل إلى أربعة مباحث رئيسة أولها يضم جوهر جرائم الحاسب أو جرائم المعلوماتية تلك الجرائم التى تعرف بالجرائم ضد سرية البيانات وسلامة البيانات والنظم وإتاحة البيانات والنظم وهذه الجرائم تمثل التهديدات الرئيسة التى تؤثر على نظم المعالجة الآلية وإرسال البيانات. ويمكن حصر هذه الجرائم في

١- الولوج غير المصرح به.

٢- الإتلاف غير المشروع للنظم، أو البرامج، أو البيانات.

وتشتمل مباحث هذا الفصل على نوعية أخرى من جرائم الحاسب أو جرائم المعلوماتية، وهى التى تلعب دوراً أكبر فى الممارسة العملية حيث يتم استخدام أجهزة الحاسب والاتصالات كوسيلة للهجوم على بعض المصالح القانونية، والتى كقاعدة عامة، يحميها مسبقاً قانون العقوبات من هذه الهجمات، عن طريق استخدام الوسائل التقليدية.

وقد تمت إضافة جرائم المبحث الثانى وهى:

- الغش المعلوماتى Les fraude informatiques.

- والتزوير المعلوماتى La falsification informatique.

من خلال الاقتراحات الواردة فى توصية مجلس أوروبا رقم ٩ لسنة ١٩٨٩.

ويعالج المبحث الثالث الشروع والاشتراك فى الجرائم المعلوماتية.

وأخيراً، يشتمل المبحث الرابع على الجزاءات والإجراءات. وذلك طبقاً للمعايير الحديثة بالنسبة لمسئولية الأشخاص المعنوية.

وإذا كانت نصوص قانون العقوبات تنطبق على الجرائم المرتكبة عن طريق تكنولوجيا المعلومات. فإن المذكرة التفسيرية حرصت على إيضاح أن الاتفاقية تستخدم مصطلحات تكنولوجية محايدة neuter بطريقة يمكن معها تطبيق جرائم قانون العقوبات على كل من التكنولوجيات الحالية والمستقبلية.

ومن النقاط المهمة التى ركزت عليها المذكرة التفسيرية أيضاً ضرورة أن يكون ارتكاب الجرائم المحصاة في هذه الاتفاقية "دون حق sans droit". ويتجلى ذلك فى قولها : "يشترط فى تجريم الأفعال المذكورة فى هذه الاتفاقية أن يكون القيام بالفعل قد تم دون حق".

وهذا المصطلح الأخير يأخذ فى الاعتبار أن السلوك قد لا يعاقب عليه دائماً فى حد ذاته، إذ يمكن أن يكون سلوكاً شرعياً أو مُبرّراً ليس فقط عن طريق الاستثناءات القانونية التقليدية، كالرضاء والدفاع الشرعى وحالة الضرورة ،ولكن أيضاً فى الحالات التى يمكن أن تؤدى فيها مبادئ أو مصالح أخرى إلى استبعاد كل المسئولية الجنائية.

٥- المواجهة الإجرائية لجرائم المعلوماتية :

وبعد أن فرغنا من تناول الأحكام الخاصة بكيفية المواجهة الموضوعية لجرائم المعلوماتية، واجهنا بالبحث كيفية المواجهة الإجرائية لهذه الجرائم وهو موضوع الفصل الثالث من هذه الدراسة، والذى يضم المواد ١٤-٢٢ من الاتفاقية. وقد تم توزيع هذه المواد على ستة مباحث: أولها: نطاق تطبيق الإجراءات الجنائية الشروط والضمانات. وفى هذا المبحث تناولنا نصين من النصوص ذات الطابع العام الذى ينطبق على كل المواد التى تمس قانون الإجراءات الجنائية وهما نص المادة ١٤ المتعلق بنطاق تطبيق الإجراءات الجنائية، والذى يشمل الجرائم الجنائية المنصوص عليها وفقاً للمواد ٢-١١ من الاتفاقية، والجرائم الأخرى المرتكبة عن طريق نظام معلوماتى وكذلك

جمع الأدلة الإليكترونية لكل جريمة جنائية، وذلك مع جواز إجراء بعض التحفظات بالشروط التى أوردناها فى حينها. أما النص الثانى فهو نص المادة ١٥ الخاص بالشروط والضمانات. ومدار هذا النص إقامة موازنة إجرائية عادلة بين حقوق المجتمع والمتمثلة فى السلطات والإجراءات المنصوص عليها فى هذا الباب وحقوق الإنسان وحرياته الأساسية الواردة فى المواثيق الدولية وإعلانات الحقوق والدساتير والقوانين وغيرها. كما تضمن هذا النص ضمانا مهما بتقريره أن السلطات والإجراءات يجب أن تتكامل مع مبدأ التناسب بمعنى آخر أن هذه السلطات والإجراءات يجب أن تكون متناسبة مع طبيعة وظروف الجريمة.

وفى المبحث الثاني تناولنا التحفظ العاجل على البيانات المعلوماتية المخزنة فبدأنا بإقامة عتبة فارقة بين مصطلحي "التحفظ على البيانات"، و"الاحتفاظ أو أرشفة البيانات"، على أساس أن المصطلح الأخير يعنى الاحتفاظ بالبيانات في أرشيف، أي وضعها في ترتيب معين وفقاً لقواعد معينة لدى حائزها وذلك بالنسبة للبيانات المستقبلية التى فى طور الإنتاج أو التوالد. وهى عملية روتينية تقوم بها المنشأة أو الشركة أو أى كيان آخر أياً ما كانت تسميته من تلقاء نفسه وفقاً للنظام السائد أو المتعارف عليه دون تكليف أو أمر صادر له من الخارج.

وذلك على خلاف التحفظ على البيانات الذى لا يكون إلا عن طريق إصدار أمر من السلطة المختصة. وأنه لا يكون إلا بصدد تحقيق جنائى معين وفى قضية معينة. وهو إجراء يتم اتخاذه لحماية البيانات من كل شىء يمكن أن يؤدى إلى إتلافها أو تجريدها من صفتها أو حالتها الراهنة. وهو لا يرد إلا على بيانات تم تخزينها بالفعل عن طريق نظام معلوماتى، أى أنه لا يتخذ إلا إذا كانت البيانات "موجودة من قبل وفى طور التخزين" وبمفهوم المخالفة لا يسرى التحفظ على بيانات مستقبلية أو سيتم إنتاجها فى المستقبل.

وعمدة القول أن المادتين ١٦ و١٧ تقرران فقط سلطة طلب التحفظ على بيانات موجودة ومخزنة في انتظار الكشف عن محتواها للسلطات القانونية بمناسبة التنقيبات والتحقيقات الجنائية النوعية.

وإذا كان التحفظ العاجل على البيانات المعلوماتية المخزنة أداة جديدة ومستحدثة فى مجال مكافحة جرائم المعلوماتية، وبالأخص فى مواجهة الجرائم المرتكبة بواسطة شبكة الإنترنت. فإن هناك العديد من المبررات التى تزكى الأخذ بها واللجوء إليها. ومن ذلك :

- **قابلية البيانات المعلوماتية للتلاشى:** بالإضافة إلى أنها لا تبقى داخل النظام إلا لفترة قصيرة، فإنه من السهل أن تخضع للتلاعب أو التغيير. وهكذا يسهل فقدان عناصر إثبات الجريمة من خلال الإهمال وممارسات التخزين غير الدقيقة، أو التغيير العمدى لها أو محوها من أجل تدمير كل عنصر للإثبات أو محو هذا العنصر فى إطار العمليات العادية أو الروتينية لمحو البيانات التى لم تعد فى حاجة إليها. وإحدى وسائل المحافظة على سلامة البيانات وسريتها هو قيام السلطات المختلفة بالتحفظ عليها لدى حائزها. خاصة إذا كان حارس البيانات جديرا بالثقة. كما فى حالة شركة تجارية ذات سمعة طيبة، فإن سلامة البيانات يمكن ضمانها بطريقة أسرع عن طريق إصدار أمر بالتحفظ على البيانات لديها. وبهذا يمكن أن يكون الأمر بالتحفظ على البيانات أقل قلقاً أو إخلالاً بالنظام بالنسبة للأنشطة وأقل ضرراً على سمعة الشركة الأمينة من عملية تفتيش الأوعية المعلوماتية بغرض الضبط.

- إن الجرائم المعلوماتية أو الجرائم المتصلة بالحاسب غالباً ما يتم ارتكابها عن طريق نقل الاتصالات التى يتم من خلالها تبادل البيانات والمعلومات عبر النظام المعلوماتى. هذه الاتصالات يمكن أن تشتمل على محتوى غير مشروع مثال ذلك مواد إباحية، فيروسات معلوماتية أو تعليمات أخرى، تحمل اعتداء على البيانات أو تعوق حسن أداء النظام المعلوماتى. كما يمكن أيضاً أن تشتمل على عناصر يمكن من خلالها إثبات أن جرائم أخرى قد تم ارتكابها. مثال ذلك الاتجار بالمخدرات أو النصب.

فالتحفظ العاجل على البيانات في كل هذه الحالات يمكن أن يساعد على تحديد هوية مرتكبى هذه الجرائم.

- عندما تقدم هذه الاتصالات محتوى غير مشروع أو دليل إثبات أفعال جنائية، فإن صوراً من هذه الاتصالات يتم الاحتفاظ بها لدى مقدمى الخدمات على سبيل المثال البريد الإليكترونى التحفظ على هذه الاتصالات يكون مهماً من أجل عدم فقد عناصر الاثبات الجوهرية. فلا مراء فى أن إعطاء صور من هذه الاتصالات الخارجية على سبيل المثال البريد المخزَّن يمكن أن يكشف عن الجرائم التى تم ارتكابها.

وفى كل الحالات فإن إجراء التحفظ العاجل على البيانات المعلوماتية المخزنة موقوت بحد أقصى ٩٠ يوماً، قابلة للتجديد وفقاً لمقتضيات الحال.

وفى المبحث الثالث تعرضنا للأمر بإنتاج أو تقديم البيانات المعلوماتية المنصوص عليها فى المادة ١٨ من الاتفاقية، حيث ناقشنا ماهية هذا الأمر، والسلطات التى تصدره وإلى من يوجه، ونوعية البيانات المعلوماتية التى يأمر بإنتاجها، والشروط والضمانات الواجب توافرها. وخلصنا من كل ذلك إلى أن الأمر بإنتاج البيانات يعنى أن يقوم شخص أو مقدم خدمات بتقديم البيانات الإليكترونية المخزنة فى نظام معلوماتى والتى فى حيازته أو تحت سيطرته إلى السلطات المختصة. ويشير تعبير "فى حيازة أو تحت السيطرة" إلى الحيازة المادية للبيانات المعنية داخل حدود هذا الطرف، كما يشير أيضاً إلى الحالات التى تكون فيها البيانات المراد تقديمها خارج الحيازة المادية للشخص لكن بمقدوره السيطرة عليها من خلال مرورها داخل حدوده.

والأمر بهذا المفهوم لا ينطبق إلا على الشخص أو مقدم الخدمات الذى يحتفظ بهذه البيانات وبهذه المعلومات. ويستوى بعد ذلك أن تكون البيانات المطلوب تقديمها بيانات معلوماتية أو بيانات متعلقة بالمشترك. وتفيد هذه الأخيرة فى حالتين جوهريتين أولاهما أن هذه المعلومات ضرورية من أجل تحديد الخدمات والإجراءات الفنية المرتبطة التى استخدمت أو التى من شأنها أن تستخدم بواسطة المشترك مثل نوع الخدمة التليفونية المستخدمة كأن يكون تليفوناً محمولاً ونوع الخدمات المرتبطة المستخدمة مثل النداء الآلى والبريد الصوتى ، ورقم التليفون، أو أى عنوان إليكترونى آخر، كعنوان البريد الإليكترونى.

أما الحالة الثانية فتبدو عندما يكون العنوان التقنى معروفاً، فإن المعلومات المتعلقة بالمشتركين يتم حيازتها من أجل المساعدة فى تحديد هوية الشخص المطلوب. وهناك معلومات أخرى متعلقة بالمشتركين كالمعلومات التجارية التى تتمثل فى دوسيهات الفواتير ودفع الاشتراك يمكن أن تكون ذات فائدة كبيرة للتحقيقات والتنقيبات الجنائية وبالأخص عندما يكون موضوع التحقيق أو التعقيب جريمة غش معلوماتى أو جريمة أخرى اقتصادية.

وتأسيساً على ما تقدم فإن المعلومات المتعلقة بالمشتركين تشتمل على أنواع مختلفة من المعلومات بالنسبة لاستخدام الخدمة ومستخدم الخدمة على النحو الذى أوردناه تفصيلاً فى هذا الفصل.

وفى كل الحالات، لا يصدر الأمر بإنتاج البيانات إلا عن طريق سلطة قضائية من أجل الحصول على أنواع معينة من البيانات، فى قضايا فردية، تتعلق بمشترك معين. مع مراعاة مبدأ التناسب الذى يستوجب استبعاد هذا الإجراء بالنسبة للقضايا عديمة الخطورة. كذلك يجب مراعاة السرية فى العلم الإليكترونى كما يجب تحديد الفترة الزمنية التى يجب فى خلالها إفشاء البيانات، أو

النص على وجوب تقديم هذه البيانات التى تم إفشاؤها فى شكل معين كأن يكون نصاً واضحاً على الهواء، أو مُخرجاً مطبوعاً، أو قرصاً.

وفى المبحث الرابع بحثنا تفتيش وضبط البيانات المعلوماتية المخزنة المنصوص عليه فى المادة ١٩ من الاتفاقية. والحق يقال إن هذا الموضوع ينبغى أن ينال عناية ملحوظة خاصة إذا وضعنا فى الحسبان الاعتبارات التالية:

- أوصى المؤتمر الدولى الخامس عشر للجمعية الدولية لقانون العقوبات والذى عقد فى ريودى جانيرو بالبرازيل فى الفترة من ٤-٩ سبتمبر سنة ١٩٩٤ فيما يتعلق بالقانون الإجرائى بما يلى[3] :

١- يتطلب التنقيب بالنسبة لجرائم الحاسب الآلى، والجرائم الأكثر تقليدية فى بيئة تكنولوجيا المعلومات - لمصلحة الدفاع الاجتماعى الفعال - أن نضع تحت تصرف سلطات التحقيق والتحرى مكنات قسرية كافية تتعادل مع الحماية الكافية لحقوق الإنسان وحرمة الحياة الخاصة.

٢- لتجنب تعسف السلطات الرسمية، فإن القيود التى ترد على حقوق الإنسان عن طريق رجال السلطة العامة، لا يمكن أن تكون مقبولة إلا فى الحالة التى تكون فيها مرتكزة على قواعد قانونية واضحة ودقيقة ومتماشية مع المعايير الدولية لحقوق الإنسان. الانتهاكات غير المشروعة لحقوق الإنسان التى يرتكبها رجال السلطة العامة، يمكن أن تبطل الدليل المتحصل عليه، بالإضافة إلى تقرير المسئولية الجنائية لرجل السلطة العامة الذى انتهك القانون.

٣- على ضوء هذه المبادئ العامة يجب أن يحدد بوضوح ما يلى:

أ - السلطات التى تقوم بإجراء التفتيش والضبط فى بيئة تكنولوجيا المعلومات، وخاصة ضبط الأشياء غير المحسوسة وتفتيش شبكات الحاسب.

ب - واجبات التعاون الفعال من جانب المجنى عليهم ، والشهود ، وغيرهم من مستخدمى تكنولوجيا المعلومات، فيما خلا المشتبه فيه (خاصة لكى تكون المعلومات متاحة فى صورة

(3) XV eme congrès international de droit penal. Rio de Janeiro. Bresil. 4-10 septembre 1994. Association internationale de droit penal. R.I.D.P.. let et 2e trimesters 1995. PP. 32-33

يمكن استخدامها للأغراض القضائية).

جـ- السماح للسلطات العامة باعتراض الاتصالات داخل نظام الحاسب ذاته، أو بينه وبين نظم الحاسبات الأخرى. مع استخدام الأدلة التى يتم الحصول عليها فى الإجراءات أمام المحاكم.

٤- نظراً لتعدد وتنوع البيانات المدرجة فى نظم معالجة البيانات ، فإن تنفيذ المكنات القسرية (المنوطة برجال السلطة العامة) يجب أن يكون متناسباً مع الطابع الخطير للانتهاك، ولا يسبب سوى الحد الأدنى من إعاقة الأنشطة القانونية للفرد. كما يجب عند بدء التحريات أن يوضع فى الاعتبار - بالإضافة إلى القيم المالية التقليدية - كل القيم المرتبطة ببيئة تكنولوجيا المعلومات. مثل ضياع فرصة اقتصادية، التجسس، انتهاك حرمة الحياة الخاصة، فقد أو مخاطرة الخسارة الاقتصادية، كلفة إعادة بناء تكامل البيانات كما كانت من قبل.

٥- القواعد القائمة فى مجال قبول ومصداقية الأدلة، يمكن أن تثير مشاكل عند تطبيقها، نظراً لتقييم تسجيلات الحاسبات فى الإجراءات القضائية لذا ينبغى إدخال بعض التغييرات التشريعية فى حالة الضرورة.

وقد سبق للحلقة التمهيدية التى عقدت على المستوى الدولى فى فريسبورج WURZBOURG بألمانيا لبحث "جرائم الحاسب والجرائم الأخرى فى مجال تكنولوجيا المعلومات" فى الفترة من ٥-٨ أكتوبر سنة ١٩٩٢، والتى كانت تمهد لهذا المؤتمر[4] أن أوصت بما يقارب من هذه التوصيات آنفة الذكر فى مجال التقنين الإجرائى[5].

كذلك أوصى المؤتمر الدولي الخامس عشر سالف الذكر في مجال حركة إصلاح الإجراءات الجنائية وحماية حقوق الإنسان بمجموعة من التوصيات بلغت الثلاثين، يهمنا منها التوصيات أرقام ١، ٢، ٣، ١٠، ١١، ١٢، ١٣، ١٤، ١٥، ١٦، ١٧، ١٨، ١٩، ٢٠. وفيما يلى نورد مضمون هذه التوصيات على النحو التالى[6]:

---

(4) ومن هنا جاء تسميتها بالحلقة التمهيدية. وقد مهد لهذا المؤتمر أيضاً المؤتمر السادس للجمعية المصرية للقانون الجنائى الذى أقيم فى الاهرة فى الفترة من ٢٥-٢٨ أكتوبر ١٩٩٣.

(5) راجع فى هذا الخصوص

- Delits informatiques et autres infractions à la technologie de l'information", colloque" préparatoire. Section I. WURZBOURG. Allmagne 5-8 Octobre 1992. Association internationale de droit penal. R.I.D.P le 2e trimesters. 1993. P. 678.

(6) راجع:

- XV em congrés international de droit penal. op. cit. pp. 36-40.

• **التوصية رقم ١**

إن حماية حقوق الإنسان يجب أن تكون مكفولة فى كل مراحل الدعوى الجنائية، بل حتى لو لم تكن الدعوى قد بدأت بقرار صريح من القاضى أو من موظف عام آخر. ولتحديد لحظة بداية الدعوى، فإن أى إجراء يتخذ من جانب رجال الضبطية القضائية يعتبر كافياً.

• **التوصية رقم ٢**

يستفيد المتهم من قرينة البراءة في كل مراحل الإجراءات، حتى صدور حكم يحوز قوة الشىء المقضى فيه.

• **التوصية رقم ٣**

فى مرحلة التحقيق الابتدائى، وهي التى تسبق مرحلة المحاكمة، فإن قرينة البراءة تتطلب – إذا ما اتخذت وسائل قسرية تطبيق مبدأ التناسب الذى يقيم علاقة معقولة بين جسامة الإجراء القسرى في مساسه بالحقوق الأساسية من ناحية، وبين مدى تناسب هذا الإجراء وفقاً للقصد المتوخى منه من ناحية أخرى.

• **التوصية رقم ١٠**

كل إجراء يتخذ بواسطة سلطة رسمية ويمس الحقوق الأساسية للمتهم – ومنها الإجراءات التى تتخذها الضبطية القضائية – يجب أن يكون مسموحاً به عن طريق القاضى أو خاضعاً لرقابته.

• **التوصية رقم ١١**

بغض النظر عن التوصية رقم ١٠، فإن كل إجراء قسرى يتم اتخاذه أو الأمر به من جانب سلطة التحرى أو الشرطة، يجب أن يكون مصدقاً عليه من القاضى فى خلال ٢٤ ساعة.

• **التوصية رقم ١٢**

وسائل الإثبات التى تمس بطريقة خطيرة – وخاصة – الحق فى الخصوصية ، مثل التنصت على المحادثات التليفونية لا تكون مقبولة إلا بقرار سابق من القاضى وفى الحالات التى قررها

المشرع بطريقة واضحة.

- **التوصية رقم ١٣**

مجرد البحث عن الأدلة فى المرحلة الابتدائية لا يصلح أن يستخدم أساسا للإدانة.

- **التوصية رقم ١٤**

مجرد اعتراف المتهم لا يقود بالضرورة إلى الإدانة الجنائية دون فحص صدقه.

- **التوصية رقم ١٥**

حالات قبول .. نتائج المراقبة الإلكترونية عن بعد يجب أن تكون منظمة بواسطة القانون.

- **التوصية رقم ١٦**

إن منح الإعفاء من العقاب أو تخفيف العقوبة لبعض الشهود ولبعض المرشدين السريين، لا يكون مقبولاً إلا بصفة استثنائية فى القضايا الخطيرة أو الجريمة المنظمة. وإذا لم يعلن عن هوية هؤلاء الأشخاص فإن إقراراتهم لا تكون لها أى قوة فى الإثبات، ولا يمكن أن تكون أساساً للإجراءات القسرية.

- **التوصية رقم ١٧**

البحث عن الأدلة، لابد أن يحترم فى كل الفروض، السر المهنى.

- **التوصية رقم ١٨**

كل الأدلة التى يتم الحصول عليها عن طريق انتهاك حق أساسى للمتهم، والأدلة المستمدة منها، تكون باطلة، ولا يمكن مراعاتها فى أى لحظة خلال الإجراءات.

- **التوصية رقم ١٩**

الحق فى الدفاع يكون مكفولاً فى كل مراحل الدعوى.

- **التوصية رقم ٢٠**

لا يجبر أحد على أن يساعد بأسلوب إيجابى، مباشرة أو بطريقة غير مباشرة، فى اتهام نفسه جنائياً. المتهم له الحق فى الصمت... وصمته لا يستخدم ضده [7].

واستلهاماً من هذه التوصيات سالفة الذكر. ومحاولة متواضعة من جانبنا لإقامة موازنة بين حق المجتمع فى العقاب بالنسبة لجرائم الحاسب الآلى والجرائم الأخرى فى مجال تكنولوجيا المعلومات، وبين المحافظة على حقوق الإنسان فى مجال الإجراءات الجنائية وبالأخص فى مواجهة التفتيش والضبط، نطرح على بساط البحث الإشكالية التالية :

"ما مدى حجم ما يتمتع به المتهم المعلوماتى من ضمانات فى حالة التفتيش والضبط فى مجال نظم الحاسب الآلى وجرائم المعلومات؟ وما الكيفية التى يمكن أن تؤدى بها هذه الضمانات؟ ويتفرع من هذا السؤال الرئيس مجموعة من التساؤلات الفرعية من أهمها :

- ما مدى خضوع مكونات شبكات الحاسب الآلى أو ما يقوم مقامه لفكرتى التفتيش والضبط؟
- هل التعريف التقليدى لهاتين الفكرتين بسماته المعروفة أمر مقبول فى مجال تقنية المعلومات؟
- هل هناك إصلاحات حتمية ينبغى أن ترد على القواعد الإجرائية الخاصة بهما؟
- هل من شأن هذه الإصلاحات أن تؤثر على التوازن العام ما بين الحريات الفردية وحق الدولة فى ملاحقة الجرائم والمجرمين؟

وعلى ضوء هذه المعطيات ينبغى فهم الأفكار التى تناولها هذا الفصل، وأول هذه الأفكار أن الغاية من التفتيش هو تجميع الأدلة أو ضبط الأدلة المادية التى تفيد فى كشف الحقيقة. وعلى ذلك يكون ضبط الأشياء المتعلقة بالجريمة هو الأثر المباشر للتفتيش. والضبط كإجراء من إجراءات التحقيق هو وضع اليد على الشىء وحبسه والمحافظة عليه لمصلحة التحقيق. والضبط المقصود هنا هو الضبط القضائى الذى يهدف إلى الحصول على دليل مادى لمصلحة التحقيق. فهل التفتيش والضبط بالمعنى التقليدى يسرى على الأوعية المعلوماتية وعلى البيانات المخزنة بها؟

---

(7) ومما تجدر الإشارة إليه أنه قد تم عقد حلقة تمهيدية حول "حركات إصلاح الإجراءات الجنائية وحماية حقوق الإنسان" فى مدينة توليد Toléde بأسبانيا فى الفترة من ١-٤ أبريل سنة ١٩٩٢. وقد كانت هذه الحلقة أيضاً تمهد لعقد هذا المؤتمر الدولى الخامس عشر سالف الذكر. لمزيد من التفصيل حول هذه الحلقة راجع :
- "Les mouvements de réforme de la procedure pénale et la protection des droits de l'Homme" colloque préparatoire. Section III. Toléde. Espagne. 1-4 Avril 1992 - Association internationale de droit penal. R.I.D.P. 3e et 4e trimesters 1993.

تذهب المذكرة التفسيرية إلى أن البيانات المعلوماتية لا تعتبر فى حد ذاتها أشياء مادية وبالتالى لا يمكن الحصول عليها أو ضبطها لأغراض التنقيب أو كإجراء جنائى بنفس طريقة الأشياء المادية، لكن على الأقل يمكن ضبط حاملة البيانات، أى الدعامة التى تم تخزين البيانات عليها.

وإذا كان التفتيش التقليدى يستوجب توافر مجموعة من الشروط أو الضوابط الموضوعية والشكلية، فإنه فيما يتعلق بعملية البحث عن البيانات المعلوماتية تبقى كثير من عناصر التفتيش التقليدى مستمرة فى البيئة التكنولوجية الجديدة. ومن ذلك أن جمع البيانات يتم خلال الفترة الزمنية للتفتيش، وأنه يعتمد على بيانات موجودة فى هذه الفترة. كما أن الشروط الخاصة من أجل الحصول على إذن قانونى لمباشرة التفيتش تظل كما هى. وأن درجة الاقتناع المطلوبة من أجل الحصول على هذا الإذن القانونى لا تختلف سواء اتخذت تلك البيانات الشكل المادى أو الشكل الإليكترونى وكذلك فإن الاقتناع والتفتيش يتعلقان ببيانات موجودة من قبل وأنها تسمح بإثبات جريمة معينة قد تم ارتكابها.

وهناك مع ذلك ضرورة لوجود نصوص إجرائية تكميلية بالنسبة للتفتيش المعلوماتى المتعلق بالبحث عن بيانات معلوماتية. وهذه الضرورة تفسرها أسباب معينة أوردناها فى حينها.

أما بالنسبة لمحل التفتيش المعلوماتى فإن المادة ١/١٩ من الاتفاقية تلزم الأطراف بتخويل السلطات المختصة صلاحيات التفتيش والولوج إلى البيانات المعلوماتية التى تم احتواؤها سواء فى داخل نظام معلوماتى أو فى جزء منه أو على دعامة مستقلة، كما يشمل التفتيش أيضاً المكونات المتصلة بالنظام كما فى حالة الحاسب المحمول والطابعة وأجهزة التخزين المتصلة، والشبكة المحلية. وفى بعض الأحيان قد تكون البيانات مخزنة مادياً فى نظام آخر أو فى جهاز تخزين آخر، لكن يمكن الوصول إليها بطريقة قانونية من خلال النظام المعلوماتى الذى يتم تفتيشه. وذلك بعمل اتصال مع النظم المعلوماتية المنفصلة الأخرى.

وإذا كان إجراء التفتيش المعلوماتى لا يقتصر فقط على تفتيش النظم بل يشمل أيضاً كل دعامة تخزين مشتركة كالأقراص التى تكون مجاورة مباشرة لهذا النظام المعلوماتى، فإن المادة ١/١٩ تحرص على تخويل السلطات المختصة من الصلاحيات ما يتناول الموقفين.

وفيما يتصل بالبيانات المعلوماتية المخزنة يمكن أن يثار سؤال مهم في هذا الخصوص هو: ما حكم الرسالة الإليكترونية المغلقة والموجودة في صندوق خطابات مقدم خدمة الإنترنت حتى يقوم المرسل إليه بإدخالها في نظامه المعلوماتى، هل تعد من قبيل البيانات المعلوماتية المخزنة وبالتالى

يطبق عليها حكم المادة ١٩ من الاتفاقية أو أنها تعتبر من قبيل البيانات التى فى مرحلة النقل أو التحويل وبالتالى يطبق عليها حكم المادة ٢١ الخاصة باعتراض البيانات المتعلقة بالمحتوى؟

تترك المذكرة التفسيرية حكم هذه الحالة للتشريع الداخلى. على أساس أن بعضاً من التشريعات يعتبر هذه الرسالة جزءاً من الاتصال وأن محتواها لا يمكن الحصول عليه إلا عن طريق سلطة الاعتراض فى حين أن بعض التشريعات الأخرى تعتبر هذه الرسالة مشابهة للبيانات المخزنة التى ينطبق عليها نص المادة ١٩ من هذه الاتفاقية.

وتخول الفقرة ٢ من المادة ١٩ السلطات المختصة مكنة توسيع نطاق التفتيش أو الولوج بطريقة مشابهة ليشمل نظاماً معلوماتياً آخر أو جزءاً منه، إذا كانت هناك أسباب تدعو للاعتقاد بأن البيانات المطلوبة مخزنة فى هذا النظام المعلوماتى أو فى أجزاء منه. ويتم هذا التوسيع وفقاً لمجموعة من الخيارات التى ينتقى منها القانون الداخلى على النحو الذى بيناه فى موضعه من الدراسة.

هذا فيما يتعلق بالتفتيش المعلوماتى وأحكامه المختلفة أما فيما يتعلق بصلاحيات الضبط أو الحصول بوسيلة مشابهة على البيانات المعلوماتية التى كونت موضوع التفتيش أو الولوج بطريقة مشابهة فقد ناقشتها الفقرة الثالثة من المادة ١٩، ونصت على أن نطاق الضبط يشمل ضبط الأجزاء المادية للحاسب ودعامات التخزين المعلوماتية خاصة فى الحالات التى لا يمكن فيها الحصول على نسخة من البيانات أو المعلومات، وكذلك ضبط البرامج الضرورية من أجل الولوج إلى البيانات وضبطها.

وبالإضافة إلى استخدام المصطلح التقليدى "يضبط" فقد تم استخدام مصطلح "الحصول بطريقة مشابهة" وذلك من أجل الأخذ فى الاعتبار طرقاً أخرى كرفع البيانات غير المادية أى جعلها غير قابلة للوصول إليها ، إما عن طريقة ترميزها أو تقييدها عن طريق أية وسيلة إليكترونية أخرى تمنع الدخول إلى هذه البيانات. لكن ذلك لا يعنى تدميرها. فالضبط ليس معناه المحو النهائى للبيانات المضبوطة. بل تستمر فى الوجود مع حرمان المشتبه فيه من الولوج إليها.

وفى كل الحالات ينبغى المحافظة على سلامة البيانات، والتى تعنى أن البيانات المنسوخة أو المرفوعة يجب أن تكون متحفظاً عليها فى الحالة التى تم العثور عليها لحظة الضبط.

ثم أثارت الفقرة الرابعة من المادة ١٩ مسألة غاية فى الأهمية تتمثل فى إلزام مديرى النظام بالتعاون أو تقديم المساعدة اللازمة بحكم اللزوم العقلى والمنطقى للقيام بعملية التفتيش والضبط. إذ إنه بدون تأكيد هذا التعاون فإن السلطات المختصة يمكن أن تمكث فى المواقع المراد تفتيشها ومع الوصول إليها عبر النظام المعلوماتى فترة طويلة من الزمن وهذا الوضع يمكن أن يخلق عبئاً اقتصادياً بالنسبة للشركات الشرعية أو لعملائها وكذلك للمشتركين الذين يجدون أنفسهم فى حالة استحالة للوصول إلى البيانات أثناء عملية التفتيش.

والمعلومات التى يمكن إلزام مديرى النظام بتقديمها هى المعلومات الضرورية التى تسمح بتطبيق إجراء التفتيش والضبط أو تطبيق طريقة مشابهة للدخول والحصول على البيانات. كأن يتعلق الاتصال بكلمة مرور أو إجراء أمنى آخر.

وأخيراً تناولت الفقرة الخامسة من المادة ١٩ مدى إمكانية إخطار الأطراف المعنية بإجراء التفتيش المعلوماتى. وخلصنا إلى أنه حتى إذا كانت بعض الدول ترى فى الإخطار عنصراً جوهرياً فى إجراء التفتيش على أساس أنه يسمح بإقامة تفرقة بين البحث عن بيانات معلوماتية مخزنة تدخل فى إطار التفتيش – والذى لا يقصد منه بصفة عامة أن يكون إجراء سرياً، وبين اعتراض البيانات فى فترة نقلها – والذى يقصد منه أن يكون إجراءً سرياً، فإن الراجح هو عدم الالتزام بالإخطار على النحو الذى أوضحناه فى موضعه من الدراسة.

وفى المبحث الخامس بحثنا مسألة التجميع – فى الوقت الفعلى – للبيانات المعلوماتية المنصوص عليها فى المادتين ٢٠، ٢١ من الاتفاقية. ونقطة البدء فى هذا الفصل هى إماطة اللثام عن مصطلح جديد من مصطلحات المعلوماتية التى ظهرت فى الجيل الرابع من أجيال الحاسبات، وهو ما يعرف بنظام الوقت الفعلى أو الحقيقى الذى يهدف إلى الوصول الفورى إلى البيانات ومعالجتها ثم استرجاعها فى الوقت نفسه عن طريق حاسب مركزى له طاقة تخزينية هائلة متصلة بوحدات طرفية يمكنها التعامل المباشر مع الحاسب[8].

---

[8] كما هو الحال فى أعمال البنوك وفى حجز التذاكر بشركات الطيران وحجز الغرف بالفنادق. راجع:
– د. لنده سامى اسخارون: "أساسيات علوم الحاسب وتطبيقاتها" جامعة جنوب الوادى، كلية التجارة سوهاج ١٩٩٧/ ١٩٩٨ ص ١٢٧.

وعلى ذلك تعني "عبارة فى الوقت الفعلى" أن هذا العنوان يطبق على تجميع أدلة المحتويات المتعلقة بالاتصالات فى فترة الإنتاج وتجميعها لحظة الفعل عبر الاتصال.

وتنص المادتان ٢٠، ٢١ من هذه الاتفاقية على التجميع فى الوقت الفعلى لبيانات المرور والاعتراض فى الوقت الفعلى لبيانات المحتوى المشاركة فى اتصالات معينة للنقل عبر نظام معلوماتى، وذلك عن طريق سلطات مختصة، أو عن طريق مقدمى الخدمات.

فالبيانات التى يتم تجميعها تنقسم إلى نوعين: البيانات المتعلقة بالمرور والبيانات المتعلقة بالمحتوى، وبالنسبة للنوع الأول فإن المادة الأولى من الاتفاقية سبق أن عرفت البيانات المتعلقة بالمرور على النحو الذى بيناه سلفاً. أما بالنسبة للنوع الثانى: البيانات المتعلقة بالمحتوى فإنه لم يأت تعريف لها فى هذه الاتفاقية، لكنها تشير إلى المحتوى الإخبارى للاتصال، بمعنى مضمون الاتصال أو الرسالة أو المعلومات المنقولة عن طريق الاتصال، فيما عدا البيانات المتعلقة بالمرور.

والواقع أن هذه البيانات سواء أكانت متعلقة بالمرور أم بالمحتوى لها أهميتها من الناحية الجنائية. فالتجميع فى الوقت الفعلى للبيانات المتعلقة بالمرور يعد إجراءً مهما للتنقيب والتحرى. ذلك أن تجميع بيانات المرور المتعلقة بالاتصالات عن بعد كالمحادثات التليفونية تعد دائماً أداة تنقيب مفيدة من أجل تحديد مصدر الاتصال ومآله عن طريق أرقام التليفون كما توفر بيانات مرتبطة بالساعة، والتاريخ، والمدة المتعلقة بمختلف أنواع الاتصالات غير المشروعة. كذلك توفر هذه الاتصالات أدلة على جرائم وقعت فى الماضى أو جرائم مستقبلية كما هو الحال فى جرائم الاتجار بالمخدرات وجرائم القتل.

وكما أن تجميع بيانات المرور بالنسبة للاتصالات التقليدية عن بعد لها أهميتها، فكذلك تجميع بيانات المرور المتعلقة بالاتصالات المعلوماتية قد يكون أكثر أهمية. وخاصة فى حالة البث غير المشروع للمواد الإباحية، والولوج غير القانونى لنظام معلوماتى، وإعاقة حسن أداء وظيفة نظام معلوماتى، أو الاعتداء على سلامة البيانات. فى كل تلك الأمثلة يكون من الضرورى إذا كانت الجريمة مرتكبة من خلال شبكة الإنترنت، تتبع مسار الاتصالات بين الضحية وفاعل الجريمة.

ولا مراء فى أن هذه التقنية للتنقيب والتحرى تسمح بعمل مقارنات بين ساعة وتاريخ ومصدر ومآل اتصالات المشتبه فيه وساعة التدخلات غير القانونية فى نظم الضحايا، وهوية الضحايا الآخرين، أو ببيان روابطه مع شركاء آخرين.

ونفس الأهمية تتجلى فى حالة اعتراض البيانات الخاصة بالمحتوى سواء تعلق الأمر بتجميع بيانات تخص محتوى الاتصالات التقليدية عن بعد أم تخص محتوى الاتصالات المعلوماتية. ففى الحالتين إذا لم يكن من الممكن الاعتراض فى الوقت الفعلى للاتصالات التقليدية عن بعد، أو إذا لم يكن من الممكن منع هذه الاتصالات المعلوماتية عن طريق اعتراض محتوى الرسالة، فإن الجرائم ستقع والأضرار سوف تتحقق.

وتتخذ الدول أحد مسلكين بالنسبة لشروط اتخاذ هذين الإجراءين. فالبعض يفرق بين اتخاذ إجراء الاعتراض فى الوقت الفعلى لبيانات المحتوى، حيث يشترط لاتخاذه شروطاً أشد صرامة من تلك المتطلبة فى البيانات المتعلقة بالمرور، هذا من ناحية، ومن ناحية أخرى من حيث نوعية الجرائم التى ينطبق عليها كلٌ منها. فيكون بالنسبة لبيانات المحتوى الجرائم الأشد خطراً من تلك المتعلقة ببيانات المرور.

أما البعض الآخر من الدول فإنها تسوى بين الإجراءين سواء بالنسبة للشروط التى ينبغى توافرها أو بالنسبة للجرائم التى يمكن اللجوء لمثل هذه الإجراءات حيالها.

وفى كل الحالات يمكن إلزام مقدم الخدمات على تجميع أو تسجيل بيانات المرور، أو البيانات المتعلقة بمحتوى اتصالات معينة، أو أن يتعاون مع السلطات المختصة ويساعدهم من أجل تجميع وتسجيل هذه البيانات. ويلاحظ أن هذا الالتزام المفروض على مقدمى الخدمات لا يتم تطبيقه إلا فى حدود عملية التجميع أو التسجيل أو التعاون والمساعدة. وأن يكون ذلك فى نطاق الإمكانيات الفنية المتوفرة لدى مقدم الخدمات. بيد أن النصوص الحالية لا تلزم مقدمى الخدمات بضمان أن يكون بحوزتهم إمكانات فنية لمباشرة عملية التجميع أو التسجيل أو منح العون والمساعدة. كما أنها لا تفرض عليهم حيازة تجهيزات جديدة، أو أن يكلفوا خبراء لمساعدتهم، أو أن يتم مباشرة هذا الإجراء بشكل باهظ لنظمهم المعلوماتية.

أما إذا كان لدى نظمهم المعلوماتية وموظفيهم الذين يعملون فيها الامكانات الفنية اللازمة لمباشرة هذا التجميع أو التسجيل أو منح العون والمساعدة، فإن هذه النصوص تلزمهم باتخاذ الإجراءات الضرورية من أجل تطبيق هذه الإمكانات الفنية.

ونظراً لخطورة هذين الإجراءين ومساسهما بالحقوق والحريات الفردية، فإن الشروط والضمانات الخاصة بالسلطات والإجراءات المرتبطة بهما تخضع للمادتين ١٤، ١٥ من الاتفاقية، بالإضافة إلى الضمانات التى أوردتها المذكرة التفسيرية، والتى أوردناها فى حينها.

وفى المبحث السادس والأخير عالجنا مسألة الاختصاص بجرائم المعلوماتية، حيث وضعت المادة ٢٢ من اتفاقية بودابست مجموعة من المعايير، والتى تصوغ وفقاً لها، الأطراف المعنية نطاق اختصاصها القضائى بالنسبة للجرائم الجنائية الوارد ذكرها فى المواد ٢-١١ من هذه الاتفاقية.

٦- التعاون الدولي في مواجهة جرائم المعلوماتية:

وبعد أن وضعنا أسس المواجهة الموضوعية والإجرائية لجرائم المعلوماتية بصفة عامة والتى تقع عادة داخل الحدود الاقليمية للدولة وتخضع لاختصاصها القانونى طبقاً لمبدأ الاختصاصى الاقليمى لقانون العقوبات. ألفينا أنفسنا على عتبة الانتقال إلى الفصل الرابع من دراستنا لنتلمس الأحكام المتعلقة بكيفية مواجهة جرائم المعلوماتية عن طريق التعاون الدولى.

وأول هذه الأحكام يتجلى فى التعاون الدولى بين الدول لأغراض التنقيب والتحرى أو الإجراءات الجنائية المرتبطة بنظم وبيانات معلوماتية أو لجمع أدلة ذات شكل اليكترونى للجريمة الجنائية. وقد أوجبت المادة ٢٣ على الدول الأطراف أن تتعاون فى أوسع نطاق ممكن، وأن تقلل ما استطاعت من العقبات التى ربما تعوق التدفق السريع للمعلومات والأدلة الاليكترونية على المستوى الدولى. كما أوجبت أن يمتد الالتزام بالتعاون ليشمل كل الجرائم الجنائية المرتبطة بنظم وبيانات معلوماتية وبالأخص تلك المشار إليها فى المادة ٢/١٤ من هذه الاتفاقية.

وبعد أن انتهينا من تحليل فكرة الالتزام بالتعاون قادنا منطق الحديث إلى دراسة أحكام تسليم المجرمين المعلوماتيين بالنسبة للجرائم الجنائية الواردة فى المواد من ٢ إلى ١١ من الاتفاقية. وبالنسبة لهذا الالتزام لاحظنا مدى عناية اتفاقية بودابست بتفصيل أحكامه وقواعده فى المادة ٢٤ بصورة تضمن المحافظة على حقوق المطلوب تسليمه وحقوق الدولة طالبة التسليم حيث لا إفراط ولا تفريط. فالتسليم لا يكون إلا فى الجرائم المعاقب عليها من كلا الطرفين بعقوبة سالبة للحرية لا تقل عن سنة. كما أن الالتزام بالتسليم لابد أن يراعى أحكام المادة الثالثة من الاتفاقية الأوربية لتسليم المجرمين والتى تنص على رفض التسليم إذا كانت الجريمة سياسية أو كان الطلب المقدم للملاحقة الجنائية أو العقاب مبنياً على أساس الجنس أو العقيدة أو الآراء السياسية.

وبعد أن فرغنا من تناول الالتزام بالتسليم وقيوده دلفنا إلى دراسة الالتزام بتوفير المساعدة القضائية المتبادلة لأغراض التحقيقات أو الاجراءات بالنسبة للجرائم الجنائية المرتبطة بنظم وبيانات معلوماتية أو بغرض تجميع الأدلة الاليكترونية للجريمة الجنائية. حيث أقامت المادة ٢٥

عتبة فارقة بين الحالات العادية وحالة الاستعجال فخصت هذه الأخيرة ببعض الأحكام منها – كما نصت الفقرة الثالثة من هذه المادة – أن يتم تقديم طلب المساعدة المتبادلة عن طريق وسائل سريعة للاتصال كالفاكس أو البريد الاليكترونى. وذلك لما تقدمه هذه الوسائل من شروط كافية للأمن والتوثيق بما فى ذلك التشفير إذا كان ضرورياً. ويجب على الدولة المقدم إليها الطلب أن ترد بإحدى الوسائل العاجلة للاتصال أيضاً.

وتجد هذه التفرقة مبرراتها في أن البيانات المعلوماتية سريعة الزوال أو التبخر. إذ يكفى مجرد الضغط على بعض المفاتيح أو تشغيل برنامج أوتوماتيكى من أجل محوها. مما يؤدى إلى استحالة تتبع مرتكب الجريمة أو تدمير أدلة إجرامه. كذلك هناك بعض أشكال من بيانات الحاسب يتم تخزينها لفترات زمنية قصيرة ثم يتم محوها. ولذا يمكن في بعض الحالات إذا لم يتم تجميع الأدلة بسرعة أن يلحق أشخاصا أو أشياء ضرر جسيم.

وفى كل الحالات تخضع المساعدة المتبادلة للشروط الواردة فى الاتفاقيات وتلك الواردة فى القانون الداخلى. ولا مراء فى أن هذه الشروط تضمن حقوق الأفراد الموجودين على أرض الطرف المطلوب منه المساعدة والذين يمكن أن يكونوا موضوعاً لطلب المساعدة. وهكذا على سبيل المثال فإنه بالنسبة للالتزامات الاجرائية التى يخضع لها المتهم المعلوماتى مثل التفتيش والضبط. فإنه لا يتم إجراؤه نيابة عن الطرف مقدم الطلب، إلا إذا كانت الشروط الأساسية للطرف المقدم إليه الطلب التى يتم تطبيقها فى القضايا المحلية قد تم استيفاؤها. كذلك يمكن للأطراف ضمان حماية حقوق الأفراد الذين لهم علاقة بالأشياء التى يتم ضبطها وتوفيرها من خلال المساعدة القضائية المتبادلة.

واستكمالاً لهذه الأحكام قد يحدث أن يكون لدى أحد الأطراف معلومات مهمة. ويعتقد هذا الطرف أن تقديم هذه المعلومات يمكن أن تحقق فائدة من أجل التنقيب والتحرى أو الاجراءات المفتوحة والتى لا يعلم بوجودها الطرف صاحب الشأن. فى مثل هذه الحالات تجيز الفقرة الأولى من المادة ٢٦ للدولة التى تحوز معلومة أن تقوم بالاتصال بالدولة الأخرى المعنية دون انتظار لتقديم طلب مسبق. بيد أنه بمقدور الطرف الذى لديه معلومات حساسة أن يشترط أن تظل سرية أو أن تستخدم وفقاً لشروط معينة.

غير أنه إذا كان الطرف المرسل إليه لا يستطيع تلبية تلك الشروط أو المحافظة على طابع السرية الذى يشترطه الطرف المرسل، كأن تكون تلك المعلومات لازمة بوصفها أدلة فى دعوى

عمومية، فإنه يجب عليه فى هذه الحالة إخطار الطرف المرسل بذلك. على أنه إذا قبل الطرف المرسل إليه المعلومات تحت شروط معينة فإنه يصبح مقيداً بهذه الشروط ويجب عليه الوفاء بها.

وإذا كانت اتفاقية بودابست قد عنيت بموضوع الالتزام بتوفير المساعدة القضائية المتبادلة والذى يخضع للشروط الواردة فى الاتفاقيات وتلك الواردة فى القانون الداخلى. فإنها عنيت أيضاً ببيان الاجراءات المتعلقة بطلبات المساعدة القضائية المتبادلة بين الأطراف فى ظل غياب اتفاقيات دولية مطبقة. إذ تلزم المادة ٢٧ الأطراف بتطبيق اجراءات وشروط معينة بالنسبة للمساعدة القضائية المتبادلة فى حالة عدم وجود معاهدة أو اتفاقية تستند إليها التشريعات الموجودة أو المتماثلة وتكون سارية المفعول بين الطرف مقدم الطلب والطرف المقدم إليه الطلب. وهذه الإجراءات والشروط هى تلك المنصوص عليها فى الفقرات من ٢-٩ من هذه المادة.

وتختلف هذه الاجراءات والشروط فى الحالات العادية عنها فى حالة الاستعجال تماماً كما هو الحال فى المادة ٢٥ آنفة الذكر. فأما الحالات العادية فإنها تخضع لمجموعة من القواعد من أهمها ما تنص عليه الفقرة الثانية من المادة ٢٧ من ضرورة إنشاء هيئة مركزية أو أكثر تناط بها مسئولية الرد الفورى على الطلبات الخاصة بالمساعدة القضائية المتبادلة. كما تلزم الفقرة الثالثة من هذه المادة الطرف المقدم إليه الطلب بتنفيذ الطلبات وفقاً للإجراءات المحددة بواسطة الطرف مقدم الطلب، إلا إذا كانت هذه الاجراءات لا تتوافق مع قانونه. فعلى سبيل المثال لا يستطيع الطرف المقدم للطلب إلزام الطرف المقدم إليه الطلب تنفيذ عمليات التفتيش والضبط التى لا تستوفى الشروط القانونية الجوهرية الخاصة بالطرف المقدم إليه.

كما تنص الفقرة الرابعة من المادة ٢٧ من هذه الاتفاقية على امكانية رفض طلبات المساعدة القضائية المتبادلة المقدمة وفقاً لهذه المادة؛ إذا كان الطلب يحتوى على جريمة يعتبرها الطرف المقدم إليه هذا الطلب جريمة سياسية أو جريمة تتصل بجريمة سياسية. أو إذا كان الطرف المقدم إليه الطلب يعتقد أن تنفيذ الطلب يمكن أن ينتهك سيادته أو نظامه العام أو مصالحه الأخرى الأساسية.

وتجيز الفقرة الخامسة للطرف المقدم إليه الطلب أن يقوم بتأجيل طلب المساعدة القضائية بدلاً من رفضه. وذلك فى حالة ما إذا كان التنفيذ الفورى للبنود المشار إليها فى هذا الطلب سوف تلحق ضرراً بتنقيبات أو اجراءات تحقيق تقوم بها سلطاته.

وتنص الفقرة السادسة على أنه فى حالة رفض طلب المساعدة أو تأجيله أن باستطاعة الطرف المقدم إليه الطلب أن يقوم بتنفيذ هذه المساعدة بشروط معينة وذلك بعد التشاور مع مقدم الطلب.

وتلزم الفقرة السابعة الطرف المقدم إليه الطلب إعلام الطرف مقدم الطلب بنتيجة طلب المساعدة الذى قدمه، مع إبداء أسباب الرفض أو التأجيل. وتعزى الغاية المتوخاه من هذا التسبيب إلى مساعدة الطرف مقدم الطلب على فهم كيفية تفسير متطلبات تلك المادة لدى الطرف المقدم إليه الطلب. مما يعمل على إنشاء قاعدة للتشاور بغرض تحسين فعالية المساعدة القضائية وتزويد الطرف مقدم الطلب بمعلومات تتعلق بالواقعة محل البحث لم تكن معلومة له مسبقاً بشأن وجود أو وضع الشهود أو الأدلة.

لكن قد يحدث أن طرفاً ما يقدم طلباً للمساعدة القضائية فى قضية ذات خطورة، أو أن قضية معينة يترتب على الافصاح المبكر عن محتوياتها نتائج خطيرة. فى مثل هذه الحالات ترخص الفقرة الثامنة للطرف مقدم الطلب أن يطلب من الطرف المقدم له الطلب أن يظل محل أو موضوع الالتماس سرياً. كأن يكون الطرف المقدم إليه الطلب ليس فى مقدوره المحافظة على سرية الطلب، فيجب عليه إخطار مقدم الطلب بذلك. ولهذا الأخير إمكانية سحب طلبه أو تعديله.

وإذا كانت الهيئات المركزية المعنية وفقاً للمادة ٢/٢٧ هى التى تتصل مباشرة بعضها ببعض فى الحالات العادية، فإنه فى حالات الاستعجال يقوم القضاة والمدعون العموميون للطرف المقدم للطلب بإرسال طلبات المساعدة القضائية لنظرائهم لدى الطرف المقدم إليه الطلب مع إرسال نسخة أخرى من هذه الطلبات لكل من الهيئة المركزية التابعة لهم والهيئة المركزية التابعة للطرف المقدم إليه الطلب. كما يمكن إرسال الطلبات عن طريق الانتربول.

وكما هو الحال بالنسبة للمادة ٢٧ يتم تطبيق المادة ٢٨ فقط عندما لا يكون هناك معاهدات واتفاقيات خاصة بالمساعدة القضائية. إذ تنص هذه المادة على أحكام استخدام المعلومات أو الأشياء المادية من حيث القيود المتعلقة بالسرية، وأوجه الاستخدام، والاستثناءات المقررة فى هذا الخصوص. إذ تسمح الفقرة الثانية من هذه المادة للطرف المقدم إليه الطلب عند الرد على طلب المساعدة القضائية المتبادلة أن يضع نوعين من الشروط: أولهما أن يطلب الحفاظ على سرية المعلومات والأشياء المادية التى يقوم بتقديمها ثانيهما عدم استخدام المعلومات والأشياء المادية التى يقوم بتقديمها فى تحقيقات أو اجراءات قضائية غير تلك الواردة فى الطلب. ومن ثم يكون

استخدام هذه الأمور لأغراض أخرى بدون موافقة الطرف المقدم إليه الطلب غير جائز.

ومع ذلك يوجد استثناءان يردان على امكانية تحديد استخدام المعلومات وفقاً للمبادئ الأساسية للعديد من الدول الأعضاء فى مجلس أوربا وهى. الأول: إذا كانت الأشياء المادية التى تم تقديمها يمكن أن تشكل عناصر أدلة براءة لأحد المتهمين المعلوماتيين. ففى هذه الحالة يجب الكشف عنها للدفاع أو للسلطة القضائية المختصة. والثانى: طالما أن معظم الأشياء المادية التى يتم تقديمها وفقاً لنظم المساعدة القضائية المتبادلة سيتم استخدامها فى الدعاوى فإنه بحكم اللزوم العقلى والمنطقى ستكون فى إجراءات علنية، بما يتضمن الافشاء الإجبارى لسريتها. وعند حدوث هذا الإفشاء تكون هذه الأشياء المادية قد خرجت إلى نطاق العلانية. وفى مثل هذه الحالات لا يكون فى الامكان ضمان سرية التحقيقات أو اجراءات التقاضى التى من أجلها تم طلب المساعدة القضائية المتبادلة.

وتنص الفقرة الثالثة من المادة ٢٨ على أنه إذا كان الطرف الذى سيتم إمداده بالمعلومات لا يستطيع الإذعان لأحد الشروط الواردة فى الفقرة الثانية من المادة نفسها، فعليه إخطار الطرف المانح لهذه المعلومات. ولهذا الأخير حرية الاختيار فى أن يمنح أو يمنع تقديم هذه المعلومات.

وأخيراً تنص الفقرة الرابعة من هذه المادة على أنه يمكن الاستفسار من مقدم طلب المساعدة القضائية عن أوجه استخدام المعلومات والأشياء المادية التى يطلبها حتى يتحقق الطرف المقدم إليه الطلب – فيما بعد – أن هذه الأمور قد تم استخدامها بالفعل فى الأغراض المحددة فى الطلب.

وبعد دراستنا لهذه الأحكام العامة شرعنا فى دراسة مجالات المساعدة القضائية المتبادلة لمكافحة جرائم المعلوماتية المنصوص عليها فى المواد ٢٩ –٣٥.

وفى هذا الخصوص تركز جل اهتمامنا على مجالين : الأول المساعدة المتبادلة فى مجال الإجراءات الوقتية العاجلة. والثانى المساعدة المتبادلة فى مجال سلطات التحقيق.

وبالنسبة للمجال الأول أتاحت لنا الدراسة أن ندفع إلى دائرة الضوء أحكام التحفظ العاجل على البيانات المعلوماتية المخزنة المنصوص عليها فى المادة ٢٩ من الاتفاقية، والتى تنص على آلية معينة على المستوى الدولى تعادل تلك المنصوص عليها فى المادة ١٦ على المستوى القومى. فالفقرة الأولى من هذه المادة تجيز لكل طرف أن يطلب من الطرف الآخر التحفظ العاجل على

البيانات المخزنة بواسطة نظام معلوماتى يوجد داخل أراضى ذلك الطرف؛ حتى لا يتم تغيير هذه البيانات أو نقلها أو حذفها خلال الفترة الزمنية اللازمة لإعداد ونقل وتنفيذ طلب المساعدة المتبادلة بخصوص الحصول على هذه البيانات.

إن عملية التحفظ عبارة عن إجراء محدود ذى طبيعة وقتية معينة تتطلب التدخل بطريقة أكثر سرعة من مجرد تنفيذ التماس أو طلب المساعدة المتبادلة التقليدى. إذ أن البيانات المعلوماتية – كما أشرنا آنفاً – تتسم بأنها سريعة الزوال. إذ يكفى بعض نقرات على مفاتيح الحاسب أو استخدام بعض البرامج الآلية، حتى يتم حذف هذه البيانات أو تغييرها أو نقلها مما يؤدى إلى استحالة تتبع مرتكب الجريمة، أو تدمير الأدلة القاطعة على إجرامه. كذلك هناك بعض أشكال للبيانات المعلوماتية لا يتم تخزينها إلا لفترات قصيرة من الزمن قبل محوها. لهذه الأسباب مجتمعة تم الاتفاق على وجود آلية تضمن توافر هذه البيانات أثناء الفترة الطويلة والمعقدة لتنفيذ الالتماس الرسمى للمساعدة والذى قد يمتد لعدة أسابيع أو شهور.

وإذا كان هذا الاجراء يعد أكثر سرعة من إجراء المساعدة المتبادلة التقليدى، فإنه يمكن أيضاً أن يعد أقل تدخلاً. فهو لا يتطلب من مسئولى المساعدة القضائية المتبادلة للشخص المقدم إليه الطلب الاستحواذ على بيانات من الجهة القائمة عليها. إنما كل ما هنالك هو أن الطرف المقدم إليه الطلب يضمن أن هذه الجهة – وغالباً ما تكون مورد خدمات أو شخصا ثالثا – تتحفظ على البيانات ولا تقوم بمحوها، انتظاراً لصدور أمر بتحويلها إلى السلطات المكلفة بتطبيق القانون فى مرحلة لاحقة. كذلك يتسم هذا الإجراء بكونه عاجلاً ويحترم حق الإنسان المعنى بهذه البيانات فى الخصوصية. لأن تلك البيانات لا يتم كشف سريتها أو فحصها من قبل أى أحد من الموظفين الحكوميين إلا بعد استيفاء المعايير المطبقة بالنسبة لكشف السرية وفقاً لمعاهدات المساعدة المتبادلة متعددة الأطراف.

ومن ناحية أخرى يكون الطرف المقدم إليه الطلب مسموحاً له استخدام إجراءات أخرى لضمان التحفظ العاجل على البيانات. بما في ذلك التنفيذ العاجل لأمر تفتيش هذه البيانات. فالشرط الأساسى في كل هذا هو تسريع الإجراءات إلى أقصى حد ممكن لمنع البيانات من الضياع بشكل يتعذر معه استردادها.

وتحدد الفقرة الثانية محتوى الطلب الخاص بالتحفظ، مع الأخذ فى الاعتبار أن الأمر يتعلق بإجراء وقتى. وأن مثل هذا الطلب ينبغى أن يتم إعداده ونقله بسرعة. كما أن المعلومات التى

يتم تقديمها تحت شكل ملخص لا تحتوى إلا على الحد الأدنى من المعلومات اللازمة التى تسمح بالتحفظ على البيانات. بالإضافة إلى تحديد هوية السلطة التى تطلب التحفظ والجريمة التى من أجلها تم اتخاذ هذا الاجراء. كما يجب أيضاً أن يحتوى هذا الطلب على ملخص مختصر للوقائع والمعلومات بشكل يكفى لتحديد البيانات الواجب التحفظ عليها ومكانها، مع توضيح أن هذه البيانات وثيقة الصلة بالتحقيق أو بالدعوى الخاصة بالجريمة المعنية، كذلك يجب بيان أن عملية التحفظ عملية ضرورية.

وتشير الفقرة الثالثة من هذه المادة إلى عدم لزومية اشتراط مبدأ التجريم المزدوج كقاعدة عامة. وذلك على أساس أن تطبيق مبدأ التجريم المزدوج يكون غير منتج فى مواد التحفظ. إذ كما يرى واضعو الاتفاقية أن التحفظ على البيانات لا يعد فى هذا الخصوص من قبيل التدخل فى الحياة الخاصة. فكل ما يفعله الحارس على البيانات أو القائم عليها هو المحافظة على أن تبقى هذه البيانات فى حيازته بشكل قانونى. و ألا يتم كشفها أو فحصها من قبل مسئولى الطرف المقدم للطلب إلا بعد تنفيذ المساعدة المتبادلة التى تهدف إلى كشف سرية هذه البيانات. كذلك غالباً ما يستغرق التأكد من وجود مبدأ التجريم المزدوج فترة زمنية طويلة للحصول على التوضيحات اللازمة لاثبات وجود هذا المبدأ بشكل قاطع لا يقبل العكس. الأمر الذى قد ينجم عنه أن البيانات المهمة سوف يتم محوها بشكل آلى بواسطة موردى أو مزودى الخدمات الذين يحتفظون بها فقط لعدة ساعات أو أيام بعد عملية الإرسال.

بيد أنه استثناء من هذه القاعدة تجيز الفقرة الرابعة من هذه المادة رفض طلب التحفظ تمسكاً بمبدأ التجريم المزدوج وذلك بالنسبة لغير الجرائم الواردة فى المواد من ٢-١١ من هذه الاتفاقية.

كذلك يمكن رفض طلب التحفظ على البيانات المعلوماتية وفقاً للفقرة الخامسة إذا كان الطلب يتعلق بجريمة يعتبرها الطرف الذى قدم له هذا الطلب جريمة سياسية أو جريمة تتصل بجريمة ذات طبيعة سياسية. أو إذا اعتقد أن تنفيذ هذا الطلب فيه إضرار بسيادته أو أمنه أو نظامه العام أو أية مصالح أخرى جوهرية.

وقد يحدث فى بعض الأحيان أن يدرك الطرف المقدم إليه الطلب أن حارس البيانات أو القائم على البيانات قد يخاطر بالتدخل بطريقة قد تهدد سرية تنقيبات أو تحقيقات الطرف الملتمس، أو أنها تضر به بأية طريقة كانت. على سبيل المثال إذا كانت البيانات المراد التحفظ

عليها تحت حراسة مزود خدمات يأتمر بأمر منظمة جنائية أو يأتمر بواسطة الشخص المستهدف من التحقيقات ذاته. فى مثل هذه الحالات، وبمقتضى الفقرة السادسة لابد أن يتم إخطار الطرف الملتمس على وجه السرعة حتى يمكنه تقدير ما إذا كان عليه أن يخاطر بتنفيذ طلب التحفظ أم أن يبحث عن شكل آخر من أشكال المساعدة القضائية المتبادلة يكون أكثر تدخلاً ولكن أكثر أمناً كالتفتيش والمصادرة.

وأخيراً تلزم الفقرة السابعة كل طرف بضمان أن تظل البيانات التى يتم التحفظ عليها وفقاً لهذه المادة متحفظاً عليها لمدة لا تقل عن ٦٠ يوماً فى انتظار تلقى طلب المساعدة المتبادلة الرسمى الذى يطلب بمقتضاه كشف سرية هذه البيانات. وتستمر عملية التحفظ على البيانات حتى بعد استلام طلب المعاونة وذلك حتى يتم البت فى شأنه.

واستكمالاً لأحكام المادة ٢٩ المتعلقة بالتحفظ العاجل على البيانات المعلوماتية المخزنة قمنا بعرض وتحليل أحكام المادة ٣٠ بشأن الإفشاء العاجل لسرية بيانات المرور المتحفظ عليها باعتبارها تتمة طبيعية ومنطقية لمفردات المجال الأول الخاص بالمساعدة القضائية المتبادلة فى مجال الاجراءات الوقتية العاجلة فهذه المادة تنشئ مستوى دوليا من السلطات يعادل السلطات التى أنشئت على المستوى القومى وفقاً للمادة ١٧ من هذه الاتفاقية. وبناء على ذلك تنص الفقرة الأولى من هذه المادة على أنه إذا اكتشف الطرف المقدم إليه الطلب أثناء تنفيذ طلب مقدم تطبيقاً للمادة ٢٩ للتحفظ على بيانات المرور المتعلقة باتصال معين، أن مزود خدمة فى دولة أخرى ساهم فى نقل الاتصال، فإنه يجب عليه أن يقوم بالافشاء الفورى عن قدر كاف من البيانات المتعلقة بالمرور للطرف الملتمس بغية التعرف على هذا المزود للخدمة وعلى المسار الذى تم عبره هذا الاتصال. كذلك إذا كان الاتصال قد تم نقله عبر دولة فإن هذه المعلومات تسمح للطرف الملتمس أن يصدر لهذه الدولة طلب تحفظ من خلال المساعدة المتبادلة العاجلة لتلك الدولة الأخرى كى تتبع المصدر الحقيقى للاتصال. وإذا كان الاتصال قد تم نقله إلى الطرف الملتمس فسيكون بمقدوره التحفظ وإفشاء البيانات الجديدة المتعلقة بالمرور عن طريق مجموعة الإجراءات الداخلية.

كما تؤكد الفقرة الثانية من هذه المادة على أن الطرف المقدم له الطلب لا يمكنه رفض الإفشاء العاجل أو الفورى للبيانات المتعلقة بالمرور إلا إذا وجد هذا الطرف أن من شأن هذا الافشاء أن يحدث ضرراً بسيادته، أو أمنه أو نظامه العام، أو بأية مصلحة أخرى من مصالحة الأساسية. وكذلك إذا اعتبر هذا الطرف أن الجريمة المقدم بخصوصها الطلب جريمة سياسية أو أنها تتصل بجريمة سياسية.

وكما هو الحال فى المادة ٢٩ فإنه فى غير هذه الأسباب لا يحق لأى طرف التذرع بأسباب أخرى لرفض طلب الإفشاء العاجل لسرية بيانات المرور.

وبعد أن انتهينا من دراسة المجال الأول بمادتيه، واجهنا بالبحث والتحليل المجال الثانى المتعلق بالمساعدة المتبادلة فى مجال سلطات التحقيق والتى تنظم أحكامها المواد ٣١-٣٤.

فلقد أباحت الفقرة الأولى من المادة ٣١ لكل طرف أن يطلب من الطرف الآخر أن يفتش أو يقوم بالولوج إلى البيانات المعلوماتية المخزنة فى نظام معلوماتى موجود على أرض هذا الطرف الآخر لضبطها أو الحصول عليها أو الكشف عنها، بما فى ذلك البيانات التى تم التحفظ عليها تبعاً للمادة ٣٠.

والفقرة الثانية تتطلب من الطرف المقدم إليه الطلب أن تكون لديه المقدرة على تلبيته من خلال تطبيق المعاهدات والاتفاقيات الدولية والتشريعات الوطنية المطبقة والخاصة بالمساعدة المتبادلة فى المواد الجنائية.

كما توجب الفقرة الثالثة الرد بصفة عاجلة فى حالتين الأولى إذا كان هناك اعتقاد بأن البيانات المتعلقة بالقضية محل البحث يمكن أن يتم ضياعها أو تعديلها. والحالة الثانية إذا كانت المعاهدات والاتفاقيات والتشريعات تقرر هذا التعاون العاجل أو الفورى.

أما المادة ٣٢ المتعلقة بكيفية الوصول إلى البيانات المعلوماتية المخزنة على أرض طرف آخر. فقد نصت على نوعين من الحالات التى اتفق واضعو هذه الاتفاقية على الولوج إليها، أولهما عندما تكون البيانات المعلوماتية التى تم الوصول إليها متاحة للجمهور، وثانيهما عندما يتم الوصول إلى هذه البيانات المخزنة خارج النطاق الإقليمى لطرف معين أو تلقيها من خلال نظام معلوماتى يقع على إقليمه بناء على موافقة قانونية إرادية من شخص يملك سلطة قانونية للكشف عنها. وتتنوع طبيعة هذا الشخص بتنوع الظروف والحالات. فبالنسبة لحالة البريد الاليكترونى لأحد الأشخاص يمكن أن يتم تخزينه فى دولة أخرى عن طريق مورد أو مزود خدمات. كما يمكن لشخص ما أن يقوم بتخزين البيانات الخاصة به عمداً فى اقليم دولة أخرى. فى مثل هذه الحالات بمقدور هؤلاء الأشخاص استعادة هذه البيانات شريطة أن يكون لديهم سلطة قانونية للقيام بهذا الاجراء. كما يكون بمقدورهم أيضاً أن يقوموا بالكشف عن هذه البيانات بمحض إرادتهم للسلطات المكلفة بتنفيذ القانون. أو أن يسمحوا لهذه السلطات بالولوج أو بالدخول إلى هذه البيانات.

ثم عرجنا إلى تناول أحكام المادتين ٣٣ و٣٤ بشأن المساعدة القضائية المتبادلة فى الوقت الفعلى للبيانات المعلوماتية سواء أكانت بيانات تتعلق بالمرور أم بالمحتوى. وقد خلصنا على ضوء الفروق بين الإجراءين إلى أن المادة ٣٣ أوجبت فى فقرتها الأولى على الأطراف أن تقدم المساعدة المتبادلة بعضها إلى بعض بالنسبة لجمع بيانات المرور فى الوقت الفعلى، والتى تكون مرتبطة باتصالات معينة على أرضهم ومرسلة عن طريق نظام معلوماتى.

ويحكم هذا النوع من المساعدة المتبادلة الشروط والاجراءات المنصوص عليها فى القانون الداخلى حسبما تنص الفقرة الثانية من هذه المادة.

أما بالنسبة للمادة ٣٤ المتعلقة بالمساعدة المتبادلة فى مسألة اعتراض بيانات المحتوى، فقد أوجبت على الأطراف تقديم المساعدة المتبادلة بعضها لبعض إلى المدى المسموح به فى معاهداتهم وقوانينهم الداخلية المطبقة، فيما يتصل بجمع أو تسجيل بيانات المحتوى فى الوقت الفعلى للمساعدة القضائية المتبادلة المتعلقة باعتراض بيانات المحتوى الذى له تداعياته. فقد تم اتخاذ قرار بخصوص هذا الإجراء. وذلك بأن يتم تنظيمه وفقاً للقوانين الداخلية المعمول بها من المساعدة والقيود التى ترد عليه.

٧- المواجهة التقنية لجرائم المعلوماتية:

واختتمنا فصول الدراسة بالفصل الخامس الذى عالجنا فيه كيفية المواجهة التقنية لجرائم المعلوماتية. وكنا نقصد بهذه النوعية من المواجهة تلك التى ترتكز على التقنية الرقمية التى تساهم فى رسم سياسة وقائية تحد من وقوع الجرائم المعلوماتية من ناحية وفى تقديم معالجة ناجعة لآثارها إذا كانت فى طور الشروع أو أنها قد وقعت بالفعل من ناحية أخرى. وهو ما خصصنا له المبحثين الأول والثانى. أما المبحث الثالث والأخير فقد خصصناه لمسألة تدعيم هذه المواجهة التقنية عن طريق إنشاء شبكة طوارئ دائمة تعمل على مدار الساعة بغرض التدخل السريع والمساعدة الفورية من أجل التجميع الفعال للأدلة الإليكترونية وعمل التحقيقات واتخاذ الإجراءات المنصوص عليها فى هذا الفصل. ويعتبر إنشاء هذه الشبكة من أهم الطرق المنصوص عليها فى اتفاقية بودابست لأنها ليست فقط تضمن أفضل الوسائل الناجعة فى مواجهة مشكلات الإجرام المعلوماتى بل السلطات المناط بها تنفيذ القانون.

٨- ملاحظات ختامية نضعها أمام أعين المشرع البحريني

وأخيراً بالإضافة إلى الملاحظات والتعليقات التى أوردناها فى حينها نشير إلى بعض الملاحظات الختامية التى نود أن نضعها أمام أعين المشرع البحرينى وهى على النحو الآتى :

أولاً : أن مصطلح النظام المعلوماتى لا يقتصر فقط على الحاسبات الالية والشبكات المتصلة بها، بل يجب أن يضاف إليها ما يقوم مقام هذه الحاسبات وهى النظم المطمورة على النحو الذى بيناه تفصيلاً فى موضعه من الدراسة.

ومن ثم نهيب بالمشرع البحرينى إذا أراد أن يضع تعريفاً تشريعياً للنظام المعلوماتى ألا يقصره على الحاسبات، بل أن يضاف إليه النظم المطمورة. والقول بغير ذلك يعتبر خطأ من الناحية التقنية وقصورا فى التعريف من الناحية التشريعية.

ثانياً : أن اتفاقية بودابست أغفلت جرائم الخطأ غير العمدى التى تقع فى هذا المجال.

إذ يشترط فى كل الجرائم الواردة فى هذه الاتفاقية ركن العمد إذ تقرر المذكرة التفسيرية أن كل الجرائم المدرجة فى هذه الاتفاقية يجب أن تكون مرتكبة بطريقة عمدية... من أجل تقرير المسئولية الجنائية.

ولا مراء فى أن هذا يعد - فى تقديرنا - قصوراً يعتور هذه الاتفاقية خاصة بعد استفحال ظاهرة أخطاء الحاسبات وتكنولوجيا المعلومات. ويكفى للتدليل على ذلك أن نذكر بعضاً من الأمثلة التالية[9] :

- فى فبراير من عام ١٩٨٢م دخل عامل صيانة فى مصنع "كاواساكى" فى مدينة "اكيسكى" باليابان التاريخ من أبشع أبوابه. وأصبح "كينجى أورادا" أول إنسان يقتله الروبوت Robot، بعد أن حاول "كينجى" أن يفتح بوابة الأمان فى "الروبوت" لقطع الطاقة عنه ولكن زميله ضغط على زر التشغيل عن طريق الخطأ، فألقى الروبوت نظرة عليه، واعتبره أحد المكونات الصناعية، وأمسك بتلابيب الرجل وعصره، وقطعه قطعاً صغيرة، وحوَّله فى النهاية إلى سجق".

[9] راجع للاستزادة : "برامج الكمبيوتر فى دور القاتل الندل" ٢٠٠٢/٧/٢٣ متاح فى :
- http://www.islamoline.net/completesearch/arabic/.

- وفى عام ١٩٨٣م تسبب الحاسب فى إحداث فيضان كبير على طول نهر "كولورادو" بالولايات المتحدة الأمريكية، وهو ما تسبب فى حدوث أضرار بالغة وخسائر جسيمة تعدت قيمتها ملايين الدولارات بالإضافة إلى وفاة ستة أشخاص. واعترف حاكم "نيفادا Nivada" بأن المتسبب فى هذا الفيضان هو: "خطأ ارتكبته الحاسبات الاتحادية". فقد قرر الحاسب إهمال نسبة ذوبان الجليد فى ربيع عام ١٩٨٣، لأنه فضل التعامل بالمعدلات التى سجلها فى السنوات السابقة بناء على قراره الناتج عن التغيير المنطقى.

ولذلك تدفقت كمية هائلة من الماء من فوق السد، وتسبب هذا الفيضان الناجم عن خطأ إليكترونى فى موت ستة أشخاص كما أشرنا سلفاً.

- وفى مايو ١٩٨٧ وفى أحد مراكز علاج الأورام السرطانية فى كندا، وأثناء قيام الحاسب بعلاج بعض المرضى عن طريق قصف الأورام بموجات مشعة تسمى موجات "ثراك - ٢٥/٢٥ - Therac" لكن فجأة قرر الحاسب زيادة الجرعة إلى ١٠٠ مرة مما تسبب فى قتل مريضين فى الحال كما توفى عدد آخر بعد ذلك.

- وفى عام ٢٠٠٠ أسقط النظام الدفاعى لروسيا الاتحادية طائرة ركاب كورية وتسبب فى قتل جميع ركابها، بعد أن دخلت الطائرة إلى المجال الجوى الروسى نتيجة لحدوث خطأ فى برمجيات الطيار الآلى، واعتبر الكمبيوتر الروسى أن الطائرة الكورية المدنية هدف عسكرى عدائى، وأهمل الاتصالات اللاسلكية والقراءات الرادارية والصور التى تؤكد عكس ذلك تماماً.

ومن أجل هذه الأمثلة ونظائرها كثير توصى سلطات السلامة الدولية بإجراءات وقائية صارمة لمواجهة "الروبوتات Robots" والحاسبات القاتلة. لكن عدداً قليلاً جداً من المصانع فى العالم الصناعى هو الذى اتخذ مثل هذه الإجراءات الوقائية على أرض الواقع.

وهناك أمثلة أخرى لأخطاء الحاسبات - قد تكون أقل وطأة من سابقتها - نذكر منها :

- خطأ فى برمجيات الحاسب يتسبب فى وقوع أخطاء فى اختبارات ألف مرشح للجامعة فى اسكتلندا A computer programming error may have caused an exams blunder affecting 1000 candidates in Scotland[10].

(10) - "Computers suspected over exam errors", available at: http: // news.bbc.co.uk/2/hi/Scotland/2192433.stm.

– فوضى فى امتحانات الطلاب بسبب خطأ كمبيوتر أدى إلى حذف النتائج فى إنجلترا.

فلقد واجهت الاختبارات المدرسية لأكثر من مليون طفل حالة من الفوضى فى صيف ٢٠٠٢ "بعد أن تسبب خطأ الحاسب فى حذف نتائج آلاف الطلاب ... after a computer error wiped out the records of thousands of pupils"[11].

– خطأ كمبيوتر يؤدى إلى تحميل نفقات رعاية صحية زائدة للطلاب فى أمريكا. فلقد تسبب خطأ كمبيوتر فى نظام المركز الصحى بالجامعة فى تلقى حوالى ٥٠ طالباً لفواتير تحتوى على بيانات غير صحيحة.

A computer malfunction in the university health center's system caused about 50 students to receive incorrect billing statements[12].

– خطأ كمبيوتر يؤدى إلى دفع ٨٠ مليون جنيه استيرلينى فى إنجلترا. فلقد أدى خطأ كمبيوتر إلى قيام إدارة الريع الداخلى بدفع أكثر من ٨٠ مليون جنيه استيرلينى خطأ إلى الآف الأشخاص من أصحاب المعاشات A computer error led the Inland Revenue to wrongly pay out more than £80 million to thousands of pension scheme members[13].

– خطأ كمبيوتر يؤدى إلى سحب سيارة إحدى السيدات فى واشنطون computer error leads trooper to seize woman's car in Washington[14].

إذا أظهرت السجلات خطأ أن رخصة قيادتها موقوفة.

---

(11) – "Exam chaos as computer error wipes outrecords" Macer Hall: Available at: http://www. Telegraph.co.uk/news/main.Jhtmp?xml=/news/ 2002/05/19/nwipe 19-xml.

(12) – Erin HEALTH: "computer malfunction overcharges students' accounts", available at: http://www. Inform. Umd.edu/News/Diamondback/1999-editions/02-feb/03-wednes day/News4-htm.

(13) – "L 80 million taxman blunder hits pension savers", available at: http://www. Ananova.com/news/story/sm.705547.html?menu.

(14) – SCOTT SUNDE: "computer error leads trooper to seize woman's car", available at : http:// seattlepi.nwsource.com/Local/imp 01.shtml.

- خطأ كمبيوتر يتسبب فى إحداث فوضى فى المجال الجوى للملكة المتحدة Computer fault causes chaos in UK Airpace British Airways فقد ألغت الخطوط الجوية البريطانية Britich Airways ٦٠ رحلة من رحلاتها فى مطارى هيثرو Healthrow وجاتويك Gatwick يوم ١٧ يونية سنة ٢٠٠ بسبب عطل فى نظام الحاسب فى المركز الطبى لمراقبة خدمات الحركة الجوية a computer system breakdown at the National Air Traffic services control center[15].

- خطأ كمبيوتر يعطل الرحلات الجوية فى شمال شرق أمريكا Compuer fault hits Northeast flights فلقد تعطلت حركة الطيران فى شمال شرق الولايات المتحدة الأمريكية فى ٢٢ نوفمبر سنة ٢٠٠٢ لمدة ساعتين "بسبب مشكلة فى كمبيوتر الطيران الفيدرالى because of a federal aviation authority computer problem"[16].

- خطأ كمبيوتر يؤثر على إشارات مرور لندن Computer fault affects London traffic lights فلقد أثر خطأ الحاسب على حوالى ٨٠٠ إشارة مرور فى وسط لندن يوم ٢٤ يوليو ٢٠٠٢ خلال ساعة الذروة[17].

- خطأ فى تصميم أنظمة الأمن العاملة بالكمبيوتر يمكن أن يعرِّض ٤٠ مطاراً فى العالم وأهدافاً فى مواقع أخرى لخطر الاختراق A design flaw in computer controlled security of the world's airports and scores of other ٤٠ systems could make at lest sites vulnerable to intruders"[18].

- خطأ فى برنامج مستكشف الإنترنت يجعل القراصنة قادرين على اختراق كمبيوتر المستخدم IE flaw lets hackers take over user's computer.

---

(15) – "Computer fault causs chaos in UK Air space", Jun 17, 2000, available at: http:// news.airwise.com/stories/2000/06/96/278654.html.

(16) – "Computer fault hits Northeast flights", Jan. 6.2000, available at: http:// news.airwise.com/stories/2000/01/947177014.html.

(17) – "Computer fault affects London Traffic lights", London, July 25 2002, available at: http://www. Theage com.au/aricles/2002/07/25/ 1027497369917.html.

(18) – "A design flaw in computer-controlled security systems could mnake at least 40 of the world's airports and seores of other sites vulnerable to intruders" The New York, Times reported Sunday, available at: http://www. Infowar.com/CLASS-٣٠٢٢٥٩٨a.html-ssi.

فلقد اعترفت شركة ميكروسوفت Microso corp فى ٢٣ مارس سنة ٢٠٠١ أنها اكتشفت وصّنعت رقاقة إليكترونية لمواجهة عدم مناعة مستكشف جديد للإنترنت a new Internet (Explorer (IE.

والذى من الممكن أن يسمح للقراصنة بإدارة برنامج من اختيارهم على جهاز مستخدم آخر. فلقد كان البرنامج يسمح للمهاجمين بالسيطرة على جهاز المستخدم وإضافة أو تغيير أو محو البيانات، والاتصال بالشبكة اعادة تشكيل قرص التشغيل الصلب الخاص بالجهاز. وذكرت الشركة أن النسخ التى تاثرت تراوحت بين ٠١ , ٥٪ و٥ , ٥٪[19].

ويلاحظ على هذه الأمثلة السابقة أنها تشمل كل أنواع الأخطاء الكمبيوترية: سواء أكانت أخطاء بسبب المكونات المادية للحاسب الهاردوير Hard ware، أو أخطاء بسبب المكونات المنطقية السوفت وير So ware وتشمل أخطاء نظم التشغيل operating systems وأخطاء البرامج programs وأخطاء الشبكات Networks. و أخيراً أخطاء بشرية Human error وتشمل أخطاء مشغل operator أو مستخدم user الحاسب، أو المبرمج programmer أو المصنّع Manufacturer.

ولا أظن أننى فى حاجة إلى الاستطراد فى تسجيل حيثيات دوافعى إلى المطالبة بتجريم أخطاء الحاسبات وشبكات المعلومات، بعد إيراد هذه الأمثلة الدامغة التى تشهد بذاتها على ضرورة تقنين جرائم المعلوماتية غير العمدية، وأن عدم النص على جرائم الخطأ فى اتفاقية بودابست يعد قصوراً ينبغى على المشرع البحرينى أن يتفاداه.

ثالثاً: أما الملحوظة الثالثة فتتعلق بوضع السؤال الآتى والإجابة عليه: هل التقاعس فى الإبلاغ عن حالات الاختراق التى تقع على الحاسبات وشبكات المعلومات يعد من قبيل الامتناع عن التبليغ عن الجرائم؟

لم تتعرض اتفاقية بودابست لهذه المسألة ولكن أثير هذا الموضوع فى ولاية كاليفورنيا California بخصوص واقعة مفادها قيام بعض مجرمى المعلوماتية Cyber criminals فى أبريل ٢٠٠٢ باختراق broke into قاعدة بيانات المرتبات لولاية كاليفورنيا The Payroll

(19) – "IE flaw lets hackers take over user's computer". March 30. 2001. available at: Fere = http % 3A %2 F% 2 f search % 2 Eyahoo % 2 Fsearch % 3 f p% Domputer % 2 B flaw & sud=1.

Database for the State of California وقد استطاع هؤلاء القراصنة Hackers على مدار أكثر من شهر من الوصول إلى المعلومات الشخصية The personal information لحوالى ٢٦٥ ألف عامل وموظف. وأن مكتب مراقبة كاليفورنيا The California Controller's Office الذى يدير قاعدة البيانات The database لم يقم بإخطار موظفى الولاية لمدة تزيد على أسبوعين بعد اكتشاف هذا الاختراق. الأمر الذى أثار موجة من الغضب والاستياء، بعد أن أصبحت أرقام الضمان الاجتماعى Social security numbers وبيانات الحاسبات البنكية bank account information وعناوين المنازل home addresses لهؤلاء الضحايا مرتعاً للقراصنة.

ولذا "قامت ولاية كاليفورنيا بسن قانون يلزم بالكشف الفورى عن أى اختراقات لأمن الكمبيوتر يتم فيها الوصول إلى معلومات سرية. ولا يغطى هذا القانون فقط وكالات الولاية، بل أيضاً يشمل المشروعات الخاصة التى تعمل فى كاليفورنيا. وعندما يأتى أول يوليو ٢٠٠٣ سوف يتعرض أولئك الذين يتقاعسون عن الإبلاغ عن أى اختراق يحدث، للحكم عليهم بالتعويضات المدنية أو رفع الدعاوى الجنائية فى مواجهتهم"[20].

ونرى تأسيساً على ما تقدم اعتبار الإهمال أو إرجاء الإبلاغ للسلطات المختصة عن حالات الاختراق التى تقع على الحاسبات وشبكات المعلومات من قبيل الامتناع عن التبليغ عن الجرائم. ويجب على المشرع البحرينى أن يضع ذلك فى الحسبان عند تقرير هذه النوعية من الجرائم.

رابعاً: تتمثل الملحوظة الرابعة فى الطبيعة القانونية لالتزام مديرى النظام ومقدمى الخدمات بالتعاون أو تقديم المساعدة المنصوص عليها فى المواد ١٩-٢١ من هذه الاتفاقية. هل هو التزامهم بأداء الشهادة؟

---

[20] وفيما يلى نورد العبارات الدالة على هذا المعنى:
California enacted a Sweeping measure that mandates public discloure of computer - ..." - security breaches in which comfidential information may have been compromised. Thw law covers not just state a gencies but private enterprises doing business in California. Those who fail to disclose that a breuch has occurred cold be liable for ،٢٠٠٣ ،١ Come july ."civil damages or face class actions

لمزيد من الاستفاضة راجع:
abailable ،٢٠٠٢ ،١٢ Alex SALKEBER: "Computer break - Ins: Your right to know", November - at: http://biz.yahoo. Com/bizwk/ 021112/tc 2002 11112402-1.html

بعبارة أكثر تفصيلاً، هل الالتزام بتأدية الشهادة يشمل التعاون أو تقديم المساعدة التى تتمثل فى القيام بطبع الملفات والإفصاح عن كلمات المرور والشفرات أو تجميع وتسجيل البيانات المتعلقة بمحتوى اتصالات معينة؟ أو أن هذا الالتزام يزيد عن نطاق الشهادة الأمر الذى يوجب البحث عن وسيلة قانونية جديدة تحقق ما لم يستطع الالتزام بأداء الشهادة أن يؤديه؟ الواقع أن الوسيلة القانونية الجديدة التى أتينا بها لتجشيم الشاهد بهذا الالتزام تكمن فى فكرة الالتزام بالإعلام المعروفة فى القانون المدنى. على أن أمراً مهما لابد أن نشير إليه منذ البداية وهو أننا فى استعارتنا للالتزام بالإعلام السائد فى القانون المدنى، سوف نأخذ الإطار الخارجى لهذا الالتزام دون المحتوى والمضمون. إذ إننا سنفرغ هذا الالتزام من مضمونه المدنى الخاص بالإعلام قبل التعاقد لنصب فيه مضموناً جديداً يتعلق بالإعلام بالبيانات والمعلومات الجوهرية والمهمة لولوج نظام المعالجة الآلية للبيانات أو تجميع وتسجيل البيانات المتعلقة بالمحتوى إذا كانت مصلحة التحقيق تقتضى ذلك.

وأحسب أن استعارة مصطلح من مصطلحات القانون المدنى ليحل مشكلة من مشاكل القانون الجنائى ليست بدعة. فلقد سبق أن أخذ الأستاذ جارسون GARÇON – على سبيل المثال – فكرة الحيازة من القانون المدنى وطوعها لتتلاءم وتتواءم مع مواد السرقة فى القانون الجنائى. إذ كان فى نظره – كما هو معلوم – أن بيان ماهية الاختلاس Soustraction فى جريمة السرقة VOL يجب أن يبحث عنه فى نظرية الحيازة Théorie de Possession المقررة فى القانون المدنى.

وقد يتوهم البعض أن فى النصوص الخاصة بالتزامات الشاهد، ما يغنى عن البحث عن وسيلة قانونية جديدة. بيد أن هذا الظن سرعان ما يتبين خطؤه. إذ إن الالتزام بتأدية الشهادة لا يشمل أو يتضمن التعاون والمساعدة الممثلة فى القيام بطبع ملفات البيانات المخزنة فى ذاكرة الحاسب أو الإفصاح عن كلمات المرور السرية أو الكشف عن الشفرات المدونة بها الأوامر الخاصة بتنفيذ البرامج أو تجميع وتسجيل البيانات المتعلقة بمحتوى اتصالات معينة. كل أولئك يزيد على نطاق الشهادة، الأمر الذى يوجب البحث عن وسيلة قانونية جديدة تتدارك أوجه القصور والعجز الذى يعتور تلك الوسيلة التقليدية. ومن هنا تبدو ضرورة الأخذ بفكرة الالتزام بالإعلام فى جرائم المعلوماتية[21].

[21] راجع للمؤلف: "التزام الشاهد بالإعلام فى الجرائم المعلوماتية دراسة مقارنة" القاهرة، دار النهضة العربية ١٩٩٧.

وبعد هذا الذى أسلفناه من قول يبدو لنا ضرورة تدخل المشرع الإجرائى البحرينى، على النحو الذى يقر فيه مبدأ الالتزام بالإعلام فى جرائم المعلوماتية. فلا مراء فى أن وجود نص قانونى يقرر هذا الالتزام سيترتب عليه الكثير من المزايا لبيئة تكنولوجيا المعلومات، لعل من أهمها تجنب ضبط شبكات الحاسب الآلى الممتد WAN. فمن الملاحظ أن الشكوى قد تثور فى الحالات التى تكون فيها البيانات مخزنة فى وحدة معالجة مركزية فى حاسب ضمن شبكة معلومات ممتدة. ففى هذه الحالة فإن صياغة شرط يعطى للمحقق إمكانية ضبط هذا النظام الشبكى بأكمله وعزله عن البيئة المعلوماتية لا يعد شرعياً طبقاً لمبدأ التناسب Le principe de proportionnalité لما فيه من مساس بحقوق الغير فى النظام المعلوماتى محل الضبط.

وهكذا يلعب الالتزام بالإعلام فى جرائم المعلوماتية دوراً وقائياً Rôle Préventif. ولذا أشارت التوصية الرابعة للمؤتمر الدولى الخامس عشر للجمعية الدولية لقانون العقوبات فيما يتعلق بالقانون الإجرائى[22] إلى أن تنفيذ المكنات القسرية المنوطة برجال السلطة العامة يجب أن يكون متناسباً مع الطابع الخطير للانتهاك، ولا يسبب سوى الحد الأدنى من إعاقة gênante الأنشطة القانونية للفرد. كما يجب عند بدء التنقيبات Investigations أن يوضع فى الاعتبار – بالإضافة إلى القيم المالية التقليدية – كل القيم المرتبطة ببيئة تكنولوجيا المعلومات. مثل ضياع فرص اقتصادية، التجسس انتهاك حرمة الحياة الخاصة، مخاطر الخسائر الاقتصادية، كلفة Le coût إعادة بناء تكامل البيانات كما كانت من قبل.

خامساً : لوحظ فى بعض الدول الأوروبية أن تشريعاتها – وقت تقنين هذه الاتفاقية – لا تقيم أية تفرقة بين تجميع البيانات المتعلقة بالمرور واعتراض البيانات المتعلقة بالمحتوى وذلك لعدم تقرير أية تفرقة فى القانون الداخلى بالنسبة للفروق المتعلقة بالمصالح ذات الطبيعة الخاصة أو لأن تقنيات التجميع المتعلقة بالإجراءين تتماثل إلى حد كبير. وهكذا تكون الشروط القانونية الواجب توافرها لتطبيق الإجراءين والجرائم التى يتم استخدام هذين الإجراءين بصددها متماثلة. وقد أقرت الاتفاقية هذا الوضع بعمل نفس الاستخدام التشغيلى لمصطلح "يجمع أو يسجل" فى نص المادتين.

---

[22] الميجابايت وحدة من وحدات قياس سعة الذاكرة أو سعة وسائط التخزين المختلفة. وهى تعادل مليون كلمة من كلمات الذاكرة وهو ما يساوى ١٠٢٤ كيلوبايت (الموسوعة الشاملة ص ٢٩٤).

ولما كان الإجراء الأخير، أى اعتراض البيانات المتعلقة بالمحتوى، أشد خطورة وتدخلاً فى الحياة الخاصة للإنسان، فينبغى أن يحاط بمجموعة من الشروط والضمانات التى تحقق توازنا مناسبا بين مصالح العدالة والحقوق الأساسية للإنسان. إذ الملاحظ أن اتفاقية بودابست لا تذكر ضمانات معينة لهذا الإجراء ما خلا التصريح بأن إجراء اعتراض بيانات المحتوى يقتصر على التحقيقات المتعلقة بالجرائم الجنائية الخطيرة كما يعرِّفها القانون الداخلى. ولذا ينبغى بالإضافة إلى ذلك النص على مجموعة من الشروط والضمانات منها:

- الإشراف القضائى أو أى إشراف آخر مستقل.
- ضرورة أن يتم صراحة تحديد الاتصالات المراد اعتراضها أو الأشخاص المعنيين بهذا الاعتراض.
- الضرورة، والمساعدة والتناسب ، على سبيل المثال الشروط القانونية التى تبرر تطبيق هذا الإجراء، وعدم فعالية الوسائل الأخرى الأقل تطفلاً.
- تحديد مدة الاعتراض.
- الحق فى الطعن.

وجدير بالذكر أن العديد من هذه الضمانات يعكس ما نصت عليه الاتفاقية الأوربية لحقوق الإنسان وقضائها اللاحق[23].

وآخر دعوانا أن الحمد لله رب العالمين،

[23] راجع على سبيل المثال القضايا التالية والتى سميت بأسماء أصحابها :
- قضية كلاس Klass
- قضية كورسلين Kruslin
- قضية أوفيج Huving
- قضية مالون Malone
- قضية الفورد Halford
- قضية لمبرت Lambert

المذكرة التفسيرية ص ٦٧