رؤية وتحليل للتحديات المستجدة للحق في الخصوصية الناتجة عن الثورة الرقمية وتطور الاتصالات والإنترنت

أ.د. سعيد عبد اللطيف إسماعيل

أستاذ القانون الجنائي بكلية القانون الكويتية العالمية

المحامي بالنقض والمحكمة الدستورية العليا – مصر

الملخص:

موضوع هذه الدراسة هو: رؤية وتحليل للتحديات المستجدة للحق في الخصوصية الناتجة عن الثورة الرقمية وتطور الاتصالات والإنترنت (دراسة تحليلية للموضوع ومشكلاته ومنهجية البحث فيه)

يعيش العالم الآن أزمة في احترام حقوق الإنسان والحق في الخصوصية، وأن الاعتداء المتكرر على تلك الحقوق قد صار وضعاً عالمياً جديداً ناجما عن وضع الحق في الخصوصية في مواجهة الثورة الرقمية والمعلوماتية والتطورات التكنولوجية لوسائل الاتصال والتواصل الاجتماعي، واستخدام معطيات تلك الثورة والوسائل التكنولوجية المتطورة في عمليات المراقبة والتجسس على الاتصالات والإنترنت، والانتهاكات الصارخة لخصوصية الأفراد وسيادة الدول، تلك الانتهاكات التي تهدر ضمانات حماية هذا الحق، وتمس سيادة الدول في غيبة من قوانين داخلية فعالة تحقق هذه الحماية، وقوانين دولية لا تشكل أي ردع للدول القوية التي تطمح للسيطرة على العالم، وتحقيق مصالحها على حساب الدول الأخرى.

ويتجه البحث في الموضوع إلى ـ وصف الموقف الراهن لموضوع الدراسة وصفاً يبرز مشكلاته كمقدمة أساسية لتقديم الحلول المناسبة لها، وتقديم رؤية جديدة للمعالجة المستقبلية الشاملة للموضوع ومشكلاته على كافة المستويات المحلية والدولية، ومن جميع الأبعاد الفنية، السياسية، الأمنية، القانونية، الحقوقية والاجتماعية.

تبدو أهمية الموضوع في أنه وصف وتحليل لموقف الأزمة الراهنة المتعلق بانتهاك حقوق الإنسان والخصوصية. ويزيد من أهمية الموضوع الشكاوى والدعاوي والإدانات بل والملاحقات القضائية من قبل الأفراد والدول المتضررين من جراء تلك الانتهاكات المرتكبة من قبل الأجهزة الأمنية والاستخباراتية، في غياب شبه تام للشرعية القانونية بحجة أو ذريعة الحفاظ على الأمن القومي للدول ومواجهة الإرهاب. ولئن كان حقاً أن للدول مصالح جديرة بالحماية ضد المخططات الإرهابية والإجرامية حفاظاً على أمنها القومي ومصالحها

الحيوية، فإن هذا لا يجوز أن يكون بإهدار سيادة الدول الأخرى وحق الأفراد في الخصوصية. إنها أوضاع ومواقف تخلق العديد من الأزمات على المستويات المحلية، الإقليمية والدولية، وتهدر الثقة بين الدول وتصيب العلاقات بينها بأضرار بالغة إن عاجلاً أو آجلاً.

تهدف هذه الدراسة إلى تحقيق هدفين:

الأول – تحليل وصياغة مشكلات الموضوع صياغة دقيقة، تمهيداً لبحثها بحثاً معمقاً.

الثاني – التعرف على أهم الفروض التي يمكن إخضاعها للبحث العلمي، لمحاولة التثبت من صحتها أو خطئها في بحوث معمقة.

بالإضافة إلى ما يلي:

1. التعرف المبدئي على المواقف والظواهر والمتغيرات والتحديات التي يرغب الباحثون بدراستها في المستقبل دراسة دقيقة ومتعمقة.
2. جمع بيانات ومعلومات عن الإمكانيات العملية لإجراء البحوث: استطلاع حقيقية التحديات والمتغيرات والمواقف التي تجري فيها الدراسة، ومدى الإمكانات المتاحة التي تيسر تنفيذ البحوث، أو الصعوبات التي تعوق تنفيذها.
3. الحصول على قائمة المشاكل التي يراها الأخصائيون والخبراء جديرة بالدارسة والبحث.

ونظراً لطبيعة هذه الدراسة «الاستطلاعية» Expiratory Study يستلزم تصميم هذا النوع من الدراسات قدراً كبيراً من المرونة والشمول.

ويهدف البحث من ناحية الدارسة الشاملة المتكاملة إلى المساهمة في تقديم رؤية جديدة وإطار جديد شامل ومتكامل لمعالجة الموضوع ومشكلاته، وأخيراً – بيان منهجية البحث في قضايا حقوق الإنسان والحق في الخصوصية.

المقدمة

أولاً: موضوع الدراسة وأهميته ومشكلاته الهدف من الدراسة وطبيعتها وحدودها

(1) الموضوع:

موضوع هذه الدراسة هو رؤية وتحليل للتحديات المستجدة للحق في الخصوصية الناتجة عن الثورة الرقمية وتطور الاتصالات والإنترنت (دراسة تحليلية للموضوع ومشكلاته ومنهجية البحث فيه)

- لقد كثر الحديث عن حقوق الإنسان وبصفة خاصة الحق في الخصوصية خلال النصف الأخير من القرن الماضي وحتى الآن، بشكل كبير وواضح، وزاد اهتمام المؤسسات التعليمية والحقوقية والسياسية والأمنية على المستويين الوطني (الرسمي والشعبي) والدولي بهذه الحقوق إلى درجة تكشف عن:

- حقيقة مفادها أن هناك، على المستويين الداخلي والدولي، «أزمة» في احترام حقوق الإنسان والحق في الخصوصية»[1]، وأن الاعتداء المتكرر على تلك الحقوق قد صار وضعاً عالمياً جديداً ناجماً عن وضع الحق في الخصوصية في مواجهة الثورة الرقمية والمعلوماتية والتطور في علوم ووسائل الاتصال والتواصل الاجتماعي»، واستخدام معطيات تلك الثورة والوسائل التكنولوجية المتطورة في عمليات المراقبة والتجسس على الاتصالات والإنترنت، والانتهاكات الصارخة لخصوصية الأفراد وسيادة الدول، تلك الانتهاكات التي تهدر ضمانات حماية هذا الحق وتمس سيادة الدول في غيبة من قوانين داخلية فعالة تحقق هذه الحماية، أو قوانين دولية لا تشكل أي ردع للدول القوية التي تطمح للسيطرة على العالم، وتحقيق مصالحها على حساب الدول الأخرى[2].

- إن الشعور المتزايد لدى الدول بفقدان القدرة على الحفاظ على سيادتها، وكذلك الشعور المتزايد لدى الناس بفقدان السيطرة على خصوصياتهم وأسرارهم وبياناتهم الشخصية، وعدم القدرة على الحفاظ على حياتهم الخاصة بعيداً عن تدخل الغير–أصبح يشكل هاجساً مستمراً للدول والأفراد على السواء، بات يؤرقهم ويسبب لهم القلق والخوف على حاضرهم ومستقبلهم وطريقة حياتهم في هذا الوضع الجديد في عصر الثورة الرقمية

(1) Thomas P. Ludwig, The Erosion of Online Privacy Rights in the Recent Tide of Terrorism, HEINONLINE, Citation: Computer Law Review and Technology Journal, (Vol. VIII) Page: 131 - 2003-2004.

(2) انظر: أحمد كمال أبو المجد، الإعلام وتدريس حقوق الإنسان، بحث مقدم إلى مؤتمر تعليم حقوق الإنسان، القاهرة 7/9/1987، ص 1

والتطور الهائل في وسائل الاتصال الحديثة، ومخاطرها المتجددة التي تهدد حقوق الدول في السيادة وحقوق الأفراد في الحرية الفردية والخصوصية وحرية التعبير، وفي هذا الوضع باتت الحماية (الفنية والقانونية) لهذه الحقوق أملاً بعيد المنال[1].

- فالرقابة الشاملة والمستمرة للاتصالات والإنترنت عبر عمليات التجسس والمراقبة والتسويق الإلكتروني للبيانات الشخصية للأفراد، وحجب ومطاردة المواقع الإلكترونية، سواء من قبل الحكومات أو أجهزة الاستخبارات أو بنوك المعلومات وشركات المواقع أو تطفل الأفراد وتجاوزاتهم، أصبحت تشكل اعتداءات صارخة على حقوق الدول والأفراد.
- ولهذا كثرت الاحتجاجات والدعاوي والإدانات على مستوى الدول والمنظمات الحقوقية والمؤسسات الأكاديمية، وكذلك على مستوى الصحافة والأفراد لكل هذه الانتهاكات، وأصبح كل ذلك من الجهد الإنساني المبذول إلى الإصلاح وتغيير الحال إلى وضع أفضل.

– ويتجه البحث في الموضوع إلى ـ وصف الموقف الراهن لموضوع الدراسة وصفاً يبرز مشكلاته كمقدمة أساسية لتقديم الحلول المناسبة لها، وتقديم رؤية جديدة للمعالجة المستقبلية الشاملة للموضوع ومشكلاته على كافة المستويات المحلية والدولية، ومن جميع الأبعاد الفنية والسياسية والأمنية والقانونية والحقوقية والاجتماعية.

(2) أهمية الموضوع:

لقد عرفت مراقبة المحادثات التليفونية التي تتم بأجهزة التليفون السلكي أو اللاسلكي منذ القرن الماضي[2]، فضلا عن ذلك فقد أدى التقدم التكنولوجي المستمر إلى إضافة وسائل أخرى بجانب التليفون للتنصت على المحادثات والأحاديث الخاصة، مما زاد من خطورة المراقبة على الحق في الخصوصية بسبب المد والانتشار الحالي للإرهاب[3]. ويثير هذا التطور مشكلات متعددة تقتضي البحث عن حلول تشريعية وقضائية ملائمة. ولم يعط موضوع

(1) There is one question that immediately arises in response to this shocking proposition: how could such a situation develop in a country that was built around the concept of individual freedom? While there are obviously many factors, two reasons stand out above the rest. First, the state of electronic privacy protection law has been unable to keep pace with the rapid development of modern wireless and online technology.
Thomas P. Ludwig, The Erosion of Online Privacy Rights in the Recent Tide of Terrorism, HEINONLINE, Citation: Computer Law Review and Technology Journal, (Vol. VIII) Page: 131 - 2003-2004.

(2) انظر: د. محمد أبو العلا، عقيدة مراقبة المحادثات التيلفونية: دراسة مقارنه في تشريعات الولايات المتحدة الأمريكية وانجلترا وإيطاليا وفرنسا ومصر، دار النهضة العربية، مصر، الطبعة الثانية 2008، ص 17.

(3) د. سعد صالح شكطي نجم الجبوري، الجرائم الإرهابية في القانون الجنائي، دار الجامعة الجديدة، سنة 2013، الإسكندرية، مصر.

تنظيم مراقبة المحادثات التليفونية في مصر ومعظم الدول العربية حتى الآن الاهتمام الذي يستحقه، ولم تخصص له دراسة شاملة وبصورة متعمقة، مما يبرز أهمية البحث في هذا الموضوع ويؤكد الحاجة إليه.

وتبدو أهمية الموضوع في أنه وصف وتحليل لموقف «الأزمة الراهنة» المتعلق بانتهاك حقوق الإنسان والخصوصية، ويزيد من أهمية البحث في الموضوع أن حقوق الإنسان لا تحظى باحترام كاف في عالمنا المعاصر، فهي تتعرض للاعتداء والانتهاك في صور وأوضاع شتى وعلى درجات متفاوتة من الخطورة. ولما كان من المتعين التصدي لرد هذا الاعتداء في صوره المتنوعة، فإن الوسيلة لذلك هي تعميق الفهم الاجتماعي لهذه الحقوق، وإبراز أهميتها وترسيخ احترامها، كي ينهض الناس، وبصفة خاصة رجال القانون، من تلقاء أنفسهم عن اقتناع بأهميتها من أجل مصالحهم ومصالح مواطنيهم للدفاع عنها حين تتعرض للاعتداء، وكي يحترمها رجال القانون[1].

ويزيد من أهمية الموضوع الشكاوى والدعاوي والإدانات، بل والملاحقات القضائية من قبل الأفراد والدول المتضررين من جراء تلك الانتهاكات المرتكبة من قبل الأجهزة الأمنية والاستخباراتية، في غياب شبه تام للشرعية القانونية بحجة أو ذريعة الحفاظ على الأمن القومي للدول ومواجهة الإرهاب. ولئن كان حقاً أن للدول مصالح جديرة بالحماية ضد المخططات الإرهابية والإجرامية حفاظاً على أمنها القومي ومصالحها الحيوية، فإن ذلك لا يمكن له أن يتم بإهدار سيادة الدول الأخرى وحق الأفراد في الحرية والخصوصية[2]. إنها أوضاع ومواقف تخلق العديد من الأزمات على جميع المستويات: المحلية والإقليمية والدولية،وتهدر الثقة بين الدول وتصيب العلاقات بينها بأضرار بالغة إن عاجلاً أو آجلاً.

ولعل الدراسات والأبحاث حول هذا الموضوع في جوانبه المختلفة، والدراسات حول حقوق الإنسان عموماً تصل إلى تحقيق «نقطة توازن» بين متطلبات الأمن من جهة وضمانات الحرية والسيادة من جهة أخرى، ولن يتحقق ذلك إلا من خلال دراسات جادة وتحليل دقيق

(1) انظر: د. محمود نجيب حسنى، تقرير مقدم إلى مؤتمر تعليم حقوق الإنسان الذي نظمته كلية الحقوق جامعة القاهرة في الفترة من 11/9 يونيه 1987 ، ص3.

(2) Thomas P. Ludwig, The Erosion of Online Privacy Rights in the Recent Tide of Terrorism, HEINONLINE, Citation: Computer Law Review and Technology Journal, (Vol. VIII) Page: 131 - 2003-2004.
Imagine a world where any idea or message communicated to another individual is subject to governmental scrutiny for possible criminal, subversive, or terroristic content. The current location of any individual, as well as the places that he or she commonly frequents, can easily be tracked through that person's phone calls, online activity, and financial records, which are all accessible to government agencies. By intercepting e-mails and tracking online browsing, shopping, and other activities, the most intimate details, habits, and preferences of the average individual are readily available to the prying eyes of cyber-criminals and law enforcement officials alike.

لموقف الأزمة الراهنة، والوصول إلى نتائج ومؤشرات علمية وواقعية تبنى عليها رؤى صائبة وإستراتيجيات وسياسات واضحة، وآليات قانونية موضوعية وإجرائية فعالة تحقق الحماية للمصالح المشتركة مجتمعة، وتحقق الشفافية لهذه العمليات والأنشطة، وتوفر الضمانات الكفيلة باحترام سيادة الدول وخصوصيتها وخصوصية الأفراد[1].

كما أن هذا الموضوع يثير العديد من المشكلات التي تحتاج إلى إدارة رشيدة وحلول ناجعة وفعالة للمشكلات، وتحقق في نفس الوقت الفاعلية لعمليات المراقبة في إطار المشروعية والشرعية القانونية والأخلاقية.

(3) التعريف العام بمشكلات الموضوع:

3-1 مشكلات الموضوع وخصائصها:

يثير موضوع هذه الدراسة مشكلات متعددة، كما يواجه عقبات منهجية وصعوبات عملية في تحديد شكل ومحتوى ونطاق البحث فيه. وتتنوع مشكلات موضوع الدراسة تنوعاً كبيراً، فثمة مشكلات: فنية وتقنية، اجتماعية وثقافية، سياسية وأمنية، وقانونية على كافة المستويات المحلية والإقليمية والدولية. ومن ثم تزيد هذه المشكلات تشابكاً وتركيباً بل وتعقيداً، وتتسم هذه المشكلات بالجدة والحيوية بفعل التقدم العلمي والتكنولوجي والتقدم في علم ووسائل الاتصال والثورة الرقمية، مما زاد من تنوع وتشابك وخطورة تلك المشكلات، كما تتسم تلك المشكلات بالأهمية بالنسبة لأجهزة الأمن والاستخبارات، وعدم حلها يمثل عقبة لهم وهم في سبيلهم لتحقيق الأمن، وكما تتسم بالخطورة – لاسيما عمليات المراقبة للاتصالات –على السيادة والخصوصية وحرية التعبير والصحافة.

3-2 تختلف هذه المشكلات بعضها عن البعض الآخر من حيث:

تحديد ماهيتها وخصائصها وأبعادها، وعلاقتها بغيرها من المشكلات، وعلاقتها بالوضع الراهن الذي يعيشه العالم في عصر الثورة الرقمية والتطور الهائل في تكنولوجيا المعلومات والاتصالات والإنترنت، ومن حيث استخدام تلك المعطيات الرقمية بمعرفة الأجهزة الأمنية والاستخباراتية في التجسس ومراقبة الاتصالات والإنترنت، ومخاطر تلك الانتهاكات والممارسات غير المشروعة على خصوصية وسيادة الدول وخصوصية وحرية الأفراد وحرية الصحافة والنشر. ومن جهة أخرى تستخدم تلك المعطيات والوسائل بمعرفة المنظمات الإرهابية والإجرامية والأفراد. كما أن كثرة الحديث في الآونة الأخيرة والاحتجاجات والشكاوى والدعوى والإدانات الدولية والفردية عن الانتهاكات اليومية المستمرة لأجهزة

(1) Lee A. Bygrave, Privacy Protection in a Global Context – A Comparative Overview, HEIN-ONLINE, Citation: 47 Scandinavian Stud. L, Page-319 - 2004.

الأمن والاستخبارات، وتقارير المنظمات الحقوقية الدولية والمحلية، كل ذلك يكشف عن أزمة في احترام سيادة الدول وحقوق الإنسان بصفة عامة وخصوصية الأفراد وحرية التعبير والصحافة بصفة خاصة».

3-3 **يشكل هذا الوضع تحديات ضخمة لأجهزة الأمن،** كما يثير العديد من الأزمات والتداعيات على سياسات الحكومات المحلية وعلى العلاقات الدولية، ويصيب الأفراد على المستوى الاجتماعي والشخصي بأضرار بالغة ناجمة عن انتهاك حقوقهم في الخصوصية والسرية نتيجة لعمليات المراقبة والتجسس غير المشروعة.

3-4 **إن الزيادة المخيفة لهذه الانتهاكات من قبل الأجهزة الأمنية والاستخباراتية تقابل الزيادة المرعبة في المخططات الإرهابية** والجريمة المنظمة عبر الحدود الدولية وجرائم الجاسوسية وسرقة الأسرار النووية العسكرية والصناعية من قبل التنظيمات الإرهابية والإجرامية المنظمة. وهذا الأمر هو في جزء كبير منه بسبب الثورة الرقمية وتطور علوم الاتصال في نقل المعلومات والأفكار والأخبار وتخزين واستخدام البيانات الشخصية للأفراد بطرق غير مشروعة.

3-5 ولمعالجة هذه المشكلات، وإصلاح الوضع الحالي وتغييره للأفضل، يقتضي الأمر **تحديد وتحليل تلك المشكلات بدقة وعناية وموضوعية،** كمقدمة ضرورية لتقديم أي تصورات لحلها بسياسات رشيدة وإستراتيجيات وآليات مناسبة وفعالة، سواء كانت فنية أم سياسية أم أمنية أم قانونية.

(4) أهداف البحث وطبيعة الدراسة وحدودها:

تهدف الدراسات والأبحاث التي تدور حول حقوق الإنسان، في جوانبها المختلفة، إلى تحقيق أكبر حماية ممكنة لهذه الحقوق والحريات وتوفير أعلى قدر من الضمانات العملية التي تتناسب مع قيمة تلك الحقوق، ووظيفتها الإيجابية الهامة في إدارة العلاقات بين الأفراد والجماعات داخل الدولة الواحدة، وعلى مستوى العلاقات التي تجاوز حدود الدول[1]. وقد كثر الحديث عن حقوق الإنسان خلال النصف الأخير من القرن الماضي وحتى الآن بشكل واضح، وزاد اهتمام المؤسسات التعليمية والسياسية على المستويين الرسمي والشعبي بهذه الحقوق إلى درجة تكشف عن حقيقتين[2]:

(1) د. أحمد كمال أبو المجد، الإعلام وتدريس حقوق الإنسان، بحث مقدم إلى مؤتمر تعليم حقوق الإنسان، القاهرة 1987، ص 1.

(2) انظر: د. أحمد كمال أبو المجد، المرجع السابق، ص 16.

الحقيقة الأولى: أن هناك على المستويين الداخلي والدولي «أزمة» في احترام حقوق الإنسان، وأن الاعتداء المتكرر على تلك الحقوق قد صار «وضعاً عالمياً جديداً»، ويهدف البحث إلى المساهمة في تنظيم الجهود وتنسيقها وتكثيفها لمقاومة ذلك الوضع والقضاء على أسبابه.

الحقيقة الثانية: أن كثرة الحديث عن تلك الحقوق قد صار جزءاً مهماً من الجهد الإنساني المبذول سعياً إلى تغيير الحال.

ويسعى البحث – في هذا الإطار – إلى المساهمة في تحقيق الأغراض الآتية:

1- التعريف بحقوق الإنسان وأساسها الأخلاقي وسندها الدستوري والقانوني، وبيان مفاهيمها وأبعادها، وهو الأمر الذي يغيب كثير منه عن وعي الناس، خصوصاً في أكثر دول العالم الثالث.

2- التعريف بالوسائل الفنية والتقنية وبرامج التجسس الحديثة التي تستخدمها أجهزة الاستخبارات في مراقبة الاتصالات والإنترنت وانتهاك خصوصية الأفراد وسيادة الدول.

3- التعريف بالممارسات والاستخدام غير المشروع للبيانات الشخصية وتأثيره على الخصوصية.

4- التعريف بالوسائل العملية التي يستطيع الفرد أن يدافع بها عن حقوقه من خلال النظام الدستوري والقانوني القائم في بيئته، وخصوصاً الضمانات القضائية التي يستطيع أن يحتمي بها لرد العدوان عن حقوقه الشخصية والعامة.

5- إذاعة أخبار حقوق الإنسان في العالم، وخصوصاً أخبار الانتهاكات التي تتعرض لها تلك الحقوق، بما يخلق وعياً متزايداً بالخطر على تلك الحقوق، وحافزاً إضافياً للحركة، طلباً لحمايتها.

يهدف البحث من الناحية الإجرائية إلى:

1 ـ وصف وتحليل البيانات والمعلومات المتاحة عن الموضوع، ثم استخلاص الحقائق والنتائج والمؤشرات عن اتجاهات الأحداث والظواهر واحتمالات حدوثها ونطاقها.

2 ـ بيان الأحداث والظواهر محل البحث، لفهم أبعادها وكيفية حدوثها (بيان علاقات السببية، أو الارتباط أو الاقتران)، وتحديد مدى الارتباط بينها (معاملات الارتباط)، والسعي إلى استخلاص مؤشرات تحدد حجمها واتجاهها.

3 ـ بيان ماهية المراقبات للاتصالات وبرامجها وآلياتها ووسائلها، وكيفية عملها ودورها وفاعليتها في تحقيق أهدافها والنتائج المرجوة منها في العمل.

4 ـ تفسير الظواهر والأحداث ببيان العوامل والأسباب التي تؤدي إلى حدوثها والظروف المرتبطة بذلك، وحجمها واتجاهها ونطاقها وآثارها، لبيان كيفية مواجهتها والمساهمة في تفعيل الإيجابي للاستفادة منه، وتقليل السلبي وتلافي مثالبه وأضراره.

5 ـ تحديد المخاطر التي تهدد الأمن القومي للدول ومصالحها الحيوية (وأهمها المخططات والعمليات الإرهابية والجريمة المنظمة)، والكشف عن حقائق الواقع والنظم والتشريعات والممارسات.

6- ويهدف البحث من الناحية الإستراتجية إلى بيان إستراتيجية معالجة المشكلات، وهي تتضمن إستراتيجية الأمن التقني للمعلومات، وتنظيم مراقبة الاتصالات وحماية الخصوصية.

7- ويهدف البحث من ناحية الدارسة الشاملة المتكاملة للموضوع إلى المساهمة في تقديم رؤية جديدة وإطار جديد شامل ومتكامل لمعالجة الموضوع ومشكلاته. ويرتكز هذا الإطار وتلك الرؤية على:

أ- تحديد المسائل الأساسية المحورية لتنظيم الموضوع ومعالجة مشكلاته الرئيسية، وتقديم تصورات لحلها بفاعلية تحقق التوازن المطلوب بين مقتضيات الأمن من جهة ومقتضيات العدالة من جهة أخرى، وتوفير أكبر قدر من الصيانة والحماية للسيادة والخصوصية والحرية بتقرير ضمانات حقيقية وآليات قانونية وقضائية تكرس احترامها وتفعيلها في الواقع والتطبيق العملي. مع أهمية التأكيد على لزوم أمرين معاً:

الأول ـ فاعلية الرقابة المشروعة لأداء دورها المرسوم وتحقيق أهدافها المنشودة.

الثاني ـ حماية وصيانة حقوق ومصالح الدول والأفراد والصحافة من أن تنتهك دون مقتضى أو سند من القانون.

وتعنى الدراسة ببيان الطبيعة القانونية والأخلاقية للتعارض بين الحق في الخصوصية ومصالح الأمن القومي بالتنبيه إلى ضرورة الوصول إلى «نقطة توازن بين الأمن القومي

في مقابل الحريات المدنية[1]، بين حق الدول في صيانة أمنها القومي ومصالحها الحيوية من مخاطر وأضرار الإرهاب والجرائم المنظمة والخطيرة، وكشفها ومعرفة مرتكبيها وملاحقتهم قضائياً لعقابهم والقصاص منهم، لتحقيق الأمن والاستقرار والعدالة. ومن جهة أخرى ضمان وصيانة سيادة الدول وحقوق وحريات الأفراد وحرية التعبير والصحافة من أن تنتهك بأنشطة وعمليات استخباراتية غير مشروعة، وممارسات خاطئة تخالف المعايير الدولية.

---

1 .

- **The Moral and Legal nature of the Clash Between the Right to Privacy and National Security Interests**

وانظر في الموضوعات الآتية:

A. The Right to Privacy
B. The National Security Interest
C. The Right to Privacy Versus the National Security Interest ...
II. Means of Infringing the Right to Privacy
A. Human Detectives
B. Technological Surveillance Measures
1. Technologies for Scanning Communications
2. Technologies for Enhancing the Quality of Information Obtained by Natural Senses
3. Technologies for Mapping Location
4. Identification Technologies
5. Technologies for Integrating Information
6. Terrorism Profiling

وكذلك الوضع القانوني للموضوع من وجه نظر إسرائيلية:

- The Legal Situation in Israel
A. Security Searches
1. The Technological Measures Which When Used May Be Regarded as Performing a Search
2. Manner of Implementing the Powers of Search-Profiling
3. The Constitutionality of the Search Arrangements …
B. Secret Monitoring Within the Framework of Security Investigations
C. Surveillance, Monitoring, and Photography
D. Data Bases

كذلك خروقات وانتهاكات أخرى للحق في الخصوصية

E. Other Infringements of Privacy
1. Opening Post
2. Entering Premises Without Search
3. Receipt of Communication Data

انظر: ورقة عمل بعنوان: مواجهة الإرهاب وحماية حقوق الإنسان – الحق في الخصوصية في مقابل المصلحة القومية (التوازن المطلوب)

Emanuel Gross, The Struggle of a Democracy Against Terrorism – Protection of Human Rights: The Right to Privacy Versus the National Interest – the Proper Balance, HEINON-LINE, Citation: Cornell International Law Journal (Vol. 37), 2004 Page: 27.

وتحاول الدراسة تقديم رؤية لحل صعوبة الوصول إلى نقطة التوازن المطلوبة من خلال الآتي:

أ- تحديد الإطار العام المرشد للحل باستلهام ما ورد من معايير دولية حاكمة في هذا الصدد بالإعلانات والمواثيق الدولية ودساتير وقوانين الدول- واستخلاص ما جاء في رؤى وسياسات الدول وعقيدة وإستراتيجيات أجهزة الأمن والاستخبارات، وما تقوم به من عمليات وممارسات في الواقع العملي لتحقيق أهدافها.

ب- ويساعد في تحديد هذا الإطار، بيان معايير تقييم الدول لأمنها ومصالحها، وفي المقابل أمن ومصالح الدول الأخرى، وكذلك حقوق ومصالح الأفراد وقيمتها الذاتية والاجتماعية والدولية، وبيان كيفية التوفيق بين المقتضيات والمصالح المتعارضة، بتحديد القواسم المشتركة بين جميع الدول والأطر القانونية (الحد المشترك من الأصول والمعايير الدولية) المتعارف عليها، والتي يمكن التوافق على إنفاذها في الحدود المشروعة، الأمن والعدالة والحرية معاً.

ت- وفي هذا الخصوص تعنى الدارسة بحل مشكلة اختلاف الرؤى والسياسات والإستراتيجيات والنظم الأمنية والقوانين في معالجة مشكلات الموضوع. ويمكن في هذا الشأن تحديد الإطار العام المرشد لتحقيق هذا التوازن بالتنسيق والتوافق والتعاون الدولي مهما اختلفت بعد ذلك نظم العمل الأمني والقانوني وآليات الممارسة في الواقع.

ث- ويساعد هذا الإطار في تحديد رؤية إستراتيجية دولية وإقليمية ومحلية موحدة، تحدد أولويات الاهتمام للوصول إلى حلول وعلاجات ناجعة للمشكلات استناداً إلى أسس ومعايير دولية مقبولة ومتوافق عليها تساهم في تغيير الأوضاع الحالية إلى الأفضل[1].

8- وأخيراً، تعميق الوعي بالحقوق وإبراز أهميتها وترسيخ احترامها.

9- منهجية البحث في قضايا حقوق الإنسان وأسلوب معالجة الموضوع ومشكلاته.

وأخيراً - بيان منهجية البحث في قضايا حقوق الإنسان والحق في الخصوصية.

(1) Lee A. Bygrave, Privacy Protection in a Global Context – A Comparative Overview, HEIN-ONLINE, Citation: 47 Scandinavian Stud. L.,2004, Page-319.

(5) طبيعة الدراسة وحدودها وإطارها المرجعي:

تهدف هذه الدراسة إلى تحقيق الأهداف الآتية:

أولاً– رصد المتغيرات والتحديات والمشكلات المستحدثة المترتبة على الثورة الرقمية وتطور تكنولوجيا الاتصال في مجالات حماية الأمن القومي والحماية الفنية والقانونية لتقنية المعلومات (إجرام تقنية المعلومات)، والمراقبة غير المشروعة للاتصالات وانتهاك سيادة الدول وخصوصياتها، وانتهاكات الحرية الشخصية وحرية التعبير والحق في الخصوصية.

ثانياً– رصد المشكلات الفنية والإدارية والأمنية والسياسية والحقوقية والقانونية للانسياب الدولي للمعلومات وأمن المعلومات والاتصالات والإنترنت.

ثالثاً– تحليل وصياغة مشكلات الموضوع الناجمة عن تلك المتغيرات والتحديات صياغة دقيقة، تمهيداً لبحثها بحثاً معمقاً.

رابعاً– التعرف على أهم الفروض التي يمكن إخضاعها للبحث العلمي، لمحاولة التثبت من صحتها أو خطئها في بحوث معمقة[1].

بالإضافة إلى ما يلي:

4– التعرف المبدئي على المواقف والظواهر والمتغيرات والتحديات التي يرغب الباحثون في دراستها في المستقبل دراسة دقيقة ومتعمقة.

5– جمع بيانات ومعلومات عن الإمكانيات العملية لإجراء البحوث: استطلاع حقيقية التحديات والمتغيرات والمواقف التي تجري فيها الدراسة، ومدى الإمكانات المتاحة التي تيسر تنفيذ البحوث، أو الصعوبات التي تعوق تنفيذها.

6– الحصول على قائمة المشاكل التي يراها الأخصائيون والخبراء جديرة بالدارسة والبحث.

7– إن المقصود بهذه الدراسة ليس شرح قانون معين، وإنما المقصود هو تحديد الأسس القانونية التي تنظم الموضوع وتعالج مشكلاته، سواء على مستوى القانون الجنائي الوطني أو القانون الإداري وعلوم الإدارة والاتصال التي يتم في ضوئها تحديد الآليات والوسائل القانونية لمعالجة الموضوع.

(1) من أهم أغراض هذه الدراسة تكوين انطباعات مبدئية وفهم، والتعرف على المسائل الآتية من وجهة نظر الباحثين المهتمين بدراسة الموضوع في القانون المقرر.

انظر في تفصيل الدراسة لهذه الأفكار:

Lee A. Bygrave. Privacy Protection in a Global Context – A Comparative Overview. HEIN-ONLINE. Citation: 47 Scandinavian Stud. L. Page-319 - 2004.

8- ونظراً لطبيعة هذه الدراسة الاستطلاعية يستلزم تصميم هذا النوع من الدراسات قدراً كبيراً من المرونة والشمول. ويهدف البحث من ناحية الدارسة الشاملة المتكاملة للموضوع إلى المساهمة في تقديم رؤية جديدة وإطار جديد شامل ومتكامل لمعالجة الموضوع ومشكلاته.

(6) تقسيم:

في ضوء ما سبق، تنقسم الدراسة إلى ثلاثة فصول يسبقها مبحث تمهيدي في تحليل المسائل الفنية والأمنية والسياسية للتحديات المستجدة للحق في الخصوصية الناتجة عن الثورة الرقمية والمعلوماتية وتطور تقنيات وعلوم الاتصال.

الفصل الأول: تحليل المسائل والمشكلات القانونية الناتجة عن الثورة الرقمية في مجال القانون الجنائي الوطني

الفصل الثاني: تحليل المشكلات القانونية الناتجة عن الثورة الرقمية في مجال القانون الدولي والقانون الإداري وعلوم الإدارة والاتصال

الفصل الثالث: تحليل المسائل المستقبلية في السياسة الجنائية والدولية المعاصرة فيما يتعلق بالقانون الجنائي المعلوماتي الإلكتروني.

مبحث تمهيدي
تحليل المسائل الفنية والأمنية والسياسية للتحديات المستجدة للخصوصية الناتجة عن الثورة الرقمية والمعلوماتية وتطور تقنيات وعلوم الاتصال

(7) التـحليل الفني والأمني والسياسي للموضوع ومـشكلاته:

يستلزم تعدد وتنوع مشكلات الموضوع وما تتسم به من أهمية وخطورة وتعقيد، تحليل تلك المشكلات إلى عناصرها، وتحديد العلاقات بينها تحديداً بما يمكّن من فهم أبعادها وحجمها وأسبابها ونطاقها وتأثيرها ومخاطرها، لمعرفة حجم التحديات والمخاطر الناجمة عنها أو المرتبطة بها وكيفية مواجهتها.

(8) أولاً- المشكلات الفنية:

يمكن تحليل هذا الجانب إلى المشكلات الفرعية الآتية:

8-1- مشكلة إدارة البنية التحتية لوسائل الاتصال الدولية والإنترنت:

تتمثل هذه المشكلة في تعدد وتنوع وسائل الاتصال والوسائط الإلكترونية «اللانهائية للمحتوى»، وعدم القدرة على السيطرة عليها، ويطلق على هذا الوضع «الانفجار المعلوماتي»[1]. وفي المقابل فإن وسائل التحكم والسيطرة على هذا المحتوى المعلوماتي محدودة، وهو ما يثير مشكلة حماية هذا المحتوى ومشكلة «صعوبة الرقابة على هذا المحتوى».

ويتعلق الشق الأول من المشكلة بأمرين: الأول -مبدأ الحرية الرقمية المعلوماتية. والأمر الثاني- «مبدأ الأمان الرقمي المعلوماتي»، ويتصل هذا المبدأ «بمدى كفاية الحماية الفنية وبرامج التأمين» للمعلومات والبيانات الشخصية والأسرار الخاصة بالدول والمؤسسات والأفراد ضد مخاطر الاختراق والتجسس والسرقة. ويتعلق الشق الثاني من المشكلة بمدى ضرورة الرقابة على المحتوى المعلوماتي من جهة، و«ضرورة حماية المستخدمين»من مطاردة مواقعهم وابتزازهم والاحتيال عليهم واستدراجهم إلى أنشطة غير مشروعة كالتجسس أو الدعارة وغيرها.

(1) Thomas P. Ludwig, The Erosion of Online Privacy Rights in the Recent Tide of Terrorism, HEINONLINE, Citation: Computer Law Review and Technology Journal. (Vol. VIII), 2003-2004. Page: 131.

8-2- مشكلة الرقابة الأخلاقية والمجتمعية على المحتوى المعلوماتي:

لهذه المشكلة بعد أخلاقي واجتماعي وثقافي لدى بعض المجتمعات، لاسيما المجتمعات الشرقية. وتتمثل في قيام بعض الدول بحجب المواقع الإباحية وبعض مواقع التواصل الاجتماعي على شبكة الإنترنت، ويستند هذا الحجب بالأساس إلى معايير أخلاقية وثقافية ومجتمعية تتعلق بحماية النظام العام والآداب العامة وثوابت المجتمع الثقافية والدينية. وهذه المعايير تتسم أحياناً بالعمومية وعدم التحديد.

8-3- مشكلة احتكار الدول المتقدمة للمعرفة والعلوم المتقدمة ووسائل الاتصال والتكنولوجيا الحديثة، وعدم قدرة الدول الأخرى على مواكبة هذا التقدم والمنافسة في هذا المجال:

وهذه المشكلة تستلزم وجود آلية معينة لتلافي الآثار السلبية لهذا الاحتكار، وتضييق الفجوة الرقمية بين الدول المتقدمة والدول النامية. وجدير بالذكر أن لهذا الاحتكار أبعاداً وجوانب علمية وفنية وسياسية وأمنية واقتصادية وصناعية وتجارية، وهي أبعاد تتصل بالضرورة بالتنمية والتقدم والاستقرار في جميع دول العالم، وبصفة خاصة في الدول النامية.

8-4- مشكلة بنوك وشركات المواقع وسماسرة المعلومات:

تتمثل هذه المشكلة في قيام شركات المواقع مثل: جوجل، وفيسبوك، وتويتر، وسماسرة المعلومات، بجمع معطيات رقمية ضخمة عن كل شيء في العالم: الدول، الجيوش، الأسلحة، المؤسسات، المنظمات، الأفراد، الأشياء وغيرها، إذ يتم تخزينها في بنوك معلومات عملاقة.

وتتحلل هذه المشكلة إلى عدة مشكلات فرعية:

8-4-1 **مشكلة الحماية الفنية للمعلومات:** نظراً لهذا الحجم الضخم من المعلومات العادية والسرية والشخصية عبر وسائل الاتصال والإنترنت، فثمة مشكلة فنية تتمثل في عدم قدرة برامج التأمين على توفير الحماية والتأمين الكافي لصون المعلومات والأسرار والمحافظة عليها وحمايتها، وهو ما يهدد أصحابها بإفشائها والإفصاح عنها أو الاستخدام غير المشروع لتلك المعلومات والأسرار. إن من شأن ذلك إهدار حقوق الدول والمؤسسات والأفراد في الحفاظ على خصوصيتهم وأسرارهم وبياناتهم الشخصية، إصابتهم في أمنهم الشخصي ومصالحهم الحيوية بأضرار بالغة.

8-4-1 **مشكلة التسويق الإلكتروني للمعلومات:** تقوم بعض شركات المواقع وسماسرة المعلومات بجمع وتخزين المعلومات والبيانات والأسرار الشخصية للمستخدمين

وبيعها للمستفيد، فيما يطلق عليه التسويق الإلكتروني للمعلومات، وهو ما يشكل عدواناً على المصالح الحيوية للدول والمؤسسات والأفراد، ويشكل انتهاكاً لخصوصياتهم وأسرارهم وأمنهم الشخصي.

(9) ثانياً- المشكلات الأمنية:

9-1- مشكلات الإرهاب والجريمة المنظمة والجرائم الجسيمة التي تهدد الأمن القومي للدول ومصالحها الحيوية:

منذ ظهور الشبكة العنكبوتية «الإنترنت» والتطور الهائل في علوم وتكنولوجيا الاتصالات، في النصف الثاني من القرن الماضي وحتى اليوم، أصبح العالم يعيش عصراً جديداً بمتغيراته وتحدياته هو عصر الثورة الرقمية (المعلوماتية) والثورة في علوم وتكنولوجيا الاتصال، وقد واكب ذلك - بفعل عوامل متعددة ومتنوعة - ظهور الإرهاب بأنواعه في موجات عاتية، بالإضافة إلى انتشار الإجرام المنظم في أشكاله المستحدثة، واجتاحت هذه الظواهر مناطق شاسعة من العالم، بل لم تسلم من ذلك دولة من الدول أو شعب من الشعوب، ولكن بدرجات متفاوتة.

لقد استفادت المنظمات الإرهابية والإجرامية من معطيات ووسائل الثورة الرقمية والمعلوماتية وتكنولوجيا الاتصال الحديثة في[1]: رسم المخططات الإرهابية والإجرامية، وتنفيذها بدقة متناهية وسرعة فائقة وأساليب مفاجئة غير متوقعة في أقصر وقت، مع تباعد واختفاء مرتكبيها في أماكن نائية أو عبر الحدود الدولية، وزادت من قدرتهم على طمس كل الآثار والأدلة التي يمكن أن ترشد عنهم أو تدل عليهم، فازدادت خطورة الإرهاب والجريمة المنظمة، وانتشر نطاقه، مما سبب ويسبب أضراراً بالغة للدول والأفراد على حد سواء، بل باتت تلك الظواهر تهدد بتقويض أركان الدول ذاتها[2].

(1) This explosive growth in technology has given criminals greater opportunity and an increasingly vast array of tools with which to commit their crimes, and has also forced law enforcement agencies to develop and utilize similarly advanced means to combat their commission. Meanwhile, innocent citizens are caught in the crossfire; the escalating crime jeopardizes the public's safety, while law enforcement's attempts to prevent such crime often results in the invasion of their privacy. The law has been unable to keep up in regulating this ongoing struggle.
Thomas P. Ludwig. The Erosion of Online Privacy Rights in the Recent Tide of Terrorism. HEINONLINE. Citation: Computer Law Review and Technology Journal. (Vol. VIII) Page: 131 - 2003-2004.

(2) د. محمد محي الدين عوض، مشكلات السياسة المعاصرة في جرائم نظم المعلومات (الكمبيوتر)، المركز العربي للدراسات الأمنية والتدريب بالرياض.

ويشكل هذا الوضع –بالغ الخطورة– تهديداً للأمن القومي للدول، ويصيب مصالحها الحيوية، ويصيب الشعوب والأفراد –وعلى كافة المستويات– بأبلغ الأضرار، وأصبح دور ووظيفة الأجهزة الأمنية بل وجيوش الدول على المحك، وبدأ عدم الثقة في قدرتها على محاربة الإرهاب والجريمة المنظمة يتطرق إلى نفوس الأفراد والشعوب التي تعيش الآن هاجس الخوف على حاضرها ومستقبلها[1].

9–2– حرب الجاسوسية:

– حرب الجاسوسية لا تنتهي، فالمال مقابل المعلومات، بالإضافة إلى الإغراءات الأخرى، هي المفاتيح التي تتسلل من خلالها أجهزة المخابرات إلى الجواسيس الذين يجمعون المعلومات عن الدول الأخرى وجيوشها وأجهزتها الأمنية وأوضاعها السياسية والاقتصادية والاجتماعية، سواء أكانت تلك الدول معادية أم صديقة. وهذا الأمر يقتضي من أجهزة المخابرات في الدول الأخرى أن تكثف جهودها الاستخباراتية لملاحقة عمليات التجسس ضدها والمتورطين فيها، سواء أكانوا شبكات تجسس أم أفراد، ويطلق على عمليات التجسس المتبادلة بين الدول لملاحقة التجسس ضدها «بالحرب الصامتة أو غير المعلنة» بين الدول وأجهزة الاستخبارات.

أشكال عمليات التجسس ومجالاتها:

– **تأخذ عمليات التجسس أشكالاً متعددة ومتطورة**، وقد ساعد على تعددها وتطورها وازدياد خطورتها واتساع نطاقها وتنوع أهدافها، ما توفر لأجهزة الاستخبارات حديثاً من معطيات ثورة المعلومات وتطور الاتصالات واستخدامها في التجسس، وكذلك كاميرات التصوير الإلكتروني ووسائل التصوير عن بعد بأقمار التجسس... الخ.

– **وقد اتسعت مجالات التجسس اتساعاً كبيراً بدء** من تجميع المعلومات العادية عن أحوال الدول المعيشية والاقتصادية والسياسية، إلى تجارة وتهريب السلاح، والعناصر النشطة في هذا المجال، والنزاعات الإقليمية والطائفية، وتجميع المعلومات عن الجيوش وتسليحها وميزانية التسليح والأسرار العسكرية، والأسلحة النووية والطاقة.

(1) The United States' responses to the past national security threats outlined in Part II with its present reactions to the threat of terrorism. Such an analogy provides practical lessons and warnings to those currently serving in each of this nation's three branches of government. This Part explores those safeguarding past situations to shed light on where to draw the line between protecting domestic security and individual liberties.
Thomas P. Ludwig, The Erosion of Online Privacy Rights in the Recent Tide of Terrorism, HEINONLINE, Citation: Computer Law Review and Technology Journal. (Vol. VIII) 2003-2004, Page: 131

- **ومن جهة أخرى تتزايد عمليات الجاسوسية بعد الثورات والفتن والقلاقل في مناطق وبؤر التوتر حول العالم**، واستغلال القوى الدولية الكبرى لكل ذلك في تحقيق مصالحها وتأمين حلفائها. كما تزيد بعد أي تغييرات سياسية في أي دولة، حيث يكون لدى أجهزة مخابرات الدول المختلفة نهم شديد للتعرف على أو التأثير فيما يدور بتلك الدولة، حتى تتمكن هذه الدول من وضع سياساتها تجاه تلك الدولة بالشكل المناسب. وفي الغالب تعمل أجهزة المخابرات المعادية بل والصديقة للدولة (محل التجسس) بهمة ونشاط لجمع المعلومات عنها وما يتبعها من تحولات سياسية داخلية. وأكثر من ذلك تتدخل أجهزة الاستخبارات –أحياناً واستغلالاً للظروف– بالتخطيط لقلب نظم الحكم في بعض الدول الرخوة أو غير الحليفة أو غير الموالية لها.

- **وتشكل الجاسوسية وعمليات التجسس مشكلة كبرى تواجه جميع أجهزة الاستخبارات في جميع الدول، وتمثِّل تحديات كبرى** يصعب ملاحقتها وتتبعها في كثير من الأحيان، كل ذلك بفعل معطيات العلم الحديث وعلوم الاتصال والإنترنت وأقمار التجسس وأدواته المستحدثة.

9–3– مشكلة مراقبة أجهزة الأمن والاستخبارات للاتصالات والإنترنت:

–تمثل مراقبة أجهزة الاستخبارات للاتصالات والإنترنت أهمية وضرورة للأمن القومي للدول، لأنها تؤمِّن مصالحها الحيوية من جهة، لكنها تشكل خطورة وانتهاكاً لسيادة الدول وخصوصية الأفراد وحرية التعبير من جهة أخرى. لقد اكتملت دوائر ووكالات الأمن القومي الأمريكي في الفترة من سنة 1945إلى 1978، ودأبت تلك الاستخبارات على انتهاك الحريات المدنية للمواطنين الأمريكيين بذريعة الحفاظ على الأمن القومي أثناء فترة الحرب الباردة. ونتيجة انتهاكات وخروقات وكالات الأمن القومي الأمريكي ومحصلة الانتقادات لهذا الوضع صدر قانون FISA لتقنين تلك السلطات، وبعد أحداث 11 سبتمبر 2001 صدر قانون مكافحة الإرهاب «USA Patriot Act»[1].

(1) American national security law has come full circle between 1945 and 1978, the intelligence community and the executive branch used the national security legal structure to monitor organizations and intrude on the civil liberties of American citizens. Critics argued that the executive branch abused its intelligence collection power during the Cold War in the name of national security. The Foreign Intelligence Surveillance Act ("FISA") was passed in 1978 after findings that intelligence agencies had abused the privacy rights of Americans. FISA was an attempt to provide greater protection of civil liberties by erecting a wall between intelligence collection and law enforcement. Civil liberties organizations now argue, however, that the wall is being eroded by the passage of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 ("USA Patriot Act"). Robert N. Davis, Striking the Balance: National Security vs. Civil Liberties, HEINONLINE, Citation: 29 Brook. J. Int'l L., 2003-2004, Page 175.

ورغم أهميتها وضرورتها، فإن أجهزة الاستخبارات تواجه مشكلات وتحديات وهي بسبيلها إلى تلك المراقبة. ويمكن تحليل هذه المشكلة إلى المشكلات الفرعية الآتية:

9-3-1- ضرورة المراقبة لدواعي أمنية:

تواجه أجهزة الأمن والاستخبارات في جميع الدول على حد سواء تحديات أمنية ضخمة لم يكن لها مثيل قبل ظهور الإنترنت وتطور علوم الاتصال وتقنياته:

- فهي تعمل على تأمين البلاد من أخطار التجسس الموجهة لها، وتحتاج في نفس الوقت إلى القيام بعمليات التجسس ضد الدول الأخرى لتحقيق أغراضها ومصالحها من تلك العمليات، سواء في أوقات الحرب الباردة أم الساخنة. وقد واكب ذلك - في العقود الأخيرة من القرن الماضي وبداية القرن الحالي وحتى اليوم- موجات عاتية من الإرهاب والجريمة المنظمة، وأصبحت الحرب على الإرهاب War on Terrorism ومواجهة تلك الموجات الإرهابية والإجرامية، وتتبع ومطاردة مرتكبيها وملاحقتهم أمنياً وقضائياً من الأمور العسيرة، بعد ازدياد قدرتهم ومهارتهم على استخدام وسائل الاتصال الحديثة ومعطيات الثورة المعلوماتية والإنترنت في تخطيط وتنفيذ مشروعاتهم الإرهابية والإجرامية بدقة وسرعة ومفاجأة غير متوقعة، واختفائهم في لحظات بعد طمس كل الأدلة والآثار التي تثبت جرائمهم أو ترشد عنهم. إن ذلك يعرض الأمن القومي للدول ومصالحها الحيوية لمخاطر وأضرار محققة [1].
- لكن رغم ذلك، فقد استطاعت أجهزة الأمن والاستخبارات في المقابل -باستخدام عمليات المراقبة والتجسس على الاتصالات والإنترنت واستخدام أقمار وبرامج التجسس والمراقبة- جمع معلومات ضخمة عن جميع الدول والأشخاص وفي شتى المجالات وتحليلها، تمهيداً لاستخدامها في وضع الخطط والإستراتيجيات الأمنية، كما تستخدم الدول الكبرى أقمار وبرامج التجسس والمراقبة، وترصد ميزانيات ضخمة لجمع

(1) يهتم الباحثون في الموضوع برصد وتحليل تلك العمليات أثناء الحرب العالمية الأولى والحرب العالمية الثانية والحرب الباردة واليوم الحرب على الإرهاب:

A. World War I
B. World War II
C. The Cold War
Today's "War on Terrorism"

لمزيد من التفصيل حول الموضوع انظر:

Thomas P. Ludwig, The Erosion of Online Privacy Rights in the Recent Tide of Terrorism, HEINONLINE, Citation: Computer Law Review and Technology Journal. (Vol. VIII) 2003-2004, Page: 131.

المعلومات والصور عن المخططات الإرهابية والإجرامية لدواعي حماية الأمن القومي والمصالح الحيوية لتلك الدول[1].

وتثير هذه المراقبة المشكلات الآتية:

1 – **مدى فاعلية تلك المراقبة في تحقيق أغراضها**، وهل تؤدي برامج التجسس واعتراض الاتصالات وتسجيلها، والتصوير عن بعد بأقمار التجسس والكاميرات الإلكترونية، الدور المنوط بها في مواجهة الإرهاب والجريمة المنظمة؟

2 – **المشكلات المتعلقة برصد ميزانيات ضخمة** للإنفاق على تلك العمليات.

3 – **مشكل المراقبة:** وتتعلق هذه المشكلة بأنشطة وعمليات أجهزة الاستخبارات من حيث طبيعتها، ونطاقها وأهدافها، ومدى إتاحة المعلومات ونشر التقارير الدورية عنها، وإخطار الجهات المعنية بها، سواء أكانت وزارات العدل أم محاكم الرقابة على أنشطة وعمليات الاستخبارات، للتأكد من مشروعيتها وسلامتها والتزامها بالضوابط والمعايير الدولية المقبولة أو المتفق عليها.

9–3–2– خطورة المراقبة:

–تشكل عمليات المراقبة الاستخباراتية للاتصالات والإنترنت انتهاكات لسيادة الدول الأخرى، وخصوصية المواطنين والأفراد الآخرين، ومخالفات للمعايير والإعلانات الدولية للحرية والأمن المعلوماتي وحقوق الإنسان، وخاصة حق الإنسان في الخصوصية وحرية التعبير والأمن المعلوماتي للدول والمؤسسات والأشخاص.

– ولعل أخطر جوانب هذه المشكلة هي ما أسفرت عنه تسريبات «مانينج» لموقع «ويكيليكس» وتسريبات «سنودن» لوثائق تكشف عمليات أجهزة الاستخبارات الأمريكية والغربية في التجسس على الاتصالات والإنترنت لسنوات طويلة، وعلى نطاق واسع، وفي شتى

(1) On December 16, 2005, the New York Times revealed that, shortly after the terrorist attacks of September 11, the White House surreptitiously authorized the National Security Agency ("NSA") to conduct surveillance on Americans inside the United States. This search for evidence of terrorist activity without first obtaining a court-approved warrant was in apparent violation of the Foreign Intelligence Surveillance Act ("FISA") and in possible abrogation of the Fourth Amendment.
Adam Burton, Fixing FISA for Long War: Regulating Warrantless Surveillance in the Age of Terrorism, HEINONLINE. Citation: Pierce Law Review (Vol. 4, No. 2), 2005-2006, Page: 381.

المجالات، وجمع معلومات ضخمة، سواء بطريق المراقبة المنتظمة أو العشوائية أو الاحتياطية للمحتوى المعلوماتي[1].

(10) ثالثاً ـ المشكلات السياسية لمراقبة الاتصالات وانتهاك خصوصية المواطنين:

- أثارت مشكلات التجسس والمراقبة للاتصالات الخاصة بالدول وقادتها ومواطنيها، وكذا تدخل أجهزة الاستخبارات في الشؤون الداخلية للدول وتدبير الفتن، والانقلابات والتغييرات السياسية، وخاصة من أجهزة الاستخبارات الأمريكية والبريطانية استهجان الدول المضارة في دول الشرق الأدنى والشرق الأوسط والدول الغربية مثل ألمانيا، ودول أمريكا اللاتينية، بل واستهجان وخوف المواطنين الأمريكيين أنفسهم من عمليات المراقبة الواسعة التي تنتهك خصوصيتهم بالمخالفة للمواثيق الدولية بل وللدستور الأمريكي ذاته.
- وقد نتج عن تلك العمليات أزمات وتداعيات سياسية على مستوى العلاقات الدولية بين الولايات المتحدة وروسيا والصين ودول أمريكا اللاتينية وإيران .... الخ بسبب انتهاك سيادة تلك الدول وخصوصيتها وخصوصية قادتها وانتهاك خصوصية مواطني تلك الدول، بل وصل الأمر إلى تقديم بعض الدول والمنظمات الحقوقية شكاوى ورفع دعاوى قضائية ضد الولايات المتحدة الأمريكية أمام المحاكم والمنظمات الدولية.

(1) لمزيد من التفصيل حول تسريبات وكيل المخابرات الأمريكية أدور سنودن فيما يتعلق بانتهاكات الخصوصية لتحقيق الأمن القومي الأمريكي انظر:

Zachary W. Smith, Privacy and Security Post-Snowden: Surveillance Law and Policy in the United States and India, HEINONLINE, Citation: 9 Intercultural Hum. Rts. L. Rev. 2014, Page: 137.

The June 2013 interview between Guardian journalist Glenn Greenwald and now famed National Security Agency (NSA) whistleblower Edward Snowden (Snowden) introduced the world to the NSA's data mining operation, known as "PRISM." Snowden showcased audacious undertakings occurring overseas, including spy games during diplomatic conferences with world leaders, and the storage of personal data at a one-million square foot site in the Utah Desert. By proffering these allegations to the world at a time when social media has developed into a popular mode of communication, and at a time when the amount of information traversing over the internet has never been higher, Snowden has refocused our attention on the state of informational privacy and the need for more transparency on privacy rules in the international arena. The opinion of this author is that despite the creation of privacy laws, the privacy laws that exist today across a large swath of the industrialized world are inherently inadequate to address the intrusive nature of communications technology, which has grown excessively under the vanguard of interconnectedness and openness

الفصل الأول
تحليل المشكلات القانونية الناتجة عن الثورة الإلكترونية وتطور تقنيات وعلوم الاتصال في مجال القانون الجنائي الوطني

(11) تعريف بالمشكلات القانونية في مجال فروع القانون العام:

- يتم مناقشة المشكلات القانونية للموضوع على مستوى القانون الدولي والقانون الوطني، حيث تدور التحولات القانونية لتنظيم الموضوع ومواجهة مشكلاته في دوائر القانون الدستوري والقانون الجنائي والقانون المدني والقانون الإداري وعلوم الإدارة والاتصال. وتتعدد وتتنوع المشكلات القانونية للموضوع سواء على مستوى القانون الدولي الإنساني، أو القانون الجنائي الدولي، أو القانون الدستوري، أو القانون الجنائي، سواء فيما يتعلق بالقانون الجنائي الموضوعي أو على مستوى القانون الجنائي الإجرائي، وكذلك فيما يتعلق بالقانون المدني والقانون الإداري وعلوم الإدارة والاتصال، وتبرز مشكلة مفاهيم القانون العام بفروعه وكذا تحديد المسائل محل التنظيم.

فإلى جانب الحكومة الإلكترونية ظهر التصويت الإلكتروني والعقود الإلكترونية (الإدارية والمدنية)، والتزوير الإلكتروني، والنقود الإلكترونية. ولذلك فإنه يجب في كل فرع من فروع القانون أن يحدد في البداية تلك المفاهيم، حتى يمكن تقديم تصور لآثار تطبيقها على النظام القانوني القائم. ثانياً: فبالنسبة للآثار، يمكن تصور هذا الأثر بالنسبة للقواعد القانونية المتصلة بالتجريم والعقاب والمسؤولية الجنائية، ومن جهة أخرى التنظيم الإجرائي من حيث الشكل وقواعد الاختصاص، بالإضافة لبعض المسائل الإجرائية. وإلى جانب قواعد القانون الإداري، فإن تطبيق الحكومة الإلكترونية يحتاج لموقف تشريعي واضح بالنسبة للتوقيع الإلكتروني[1].

- وسوف يقتصر التحليل على دوائر (محاور) القانون الجنائي الوطني، والقانون الإداري وعلوم الإدارة والاتصال، والقانون الدولي، نظراً للصلة الوثيقة بين تلك القوانين ودورها المتكامل في تنظيم الموضوع ومشكلاته باعتبارها فروعاً للقانون العام وعلوم الإدارة والاتصال. وسنخصص الدراسة في هذا الفصل لتحليل المشكلات القانونية في مجال القانون الجنائي الوطني، ثم في الفصل الثالث تحليل للمشكلات في فروع القانون العام

(1) انظر: د. محمد الفيلي، العلاقة بين القانون والحكومة الالكترونية، مؤتمر الكويت حول الحكومة الإلكترونية 13–15 اكتوبر 2003، ص 18

الأخرى، وكذلك مشكلات العلوم والإدارة والاتصال، وعلاقتها بالخصوصية وحقوق الدول في السيادة وعدم التدخل في شئونها الداخلية.

(12) المشاكل الأساسية المستحدثة في مجال القانون الجنائي الوطني:

يثير موضوع «التحديات المستجدة للحق في الخصوصية «العديد من المشاكل تتعلق بالقانون الجنائي الموضوعي، وأهمها مراقبة الاتصالات والإنترنت ومراقبة المحادثات التليفونية، حيث يتحدد مدى المسؤولية الجنائية لمن يتنصت على المحادثات الهاتفية للغير،فضلاً عن مشاكل أخرى تتعلق بتطبيق قواعد قانون الإجراءات الجنائية التي تحدد الحالات التي يجوز فيها مراقبة المحادثات والضمانات التي تحيط بها، فضلاً عن بيان مدى مشروعية الدليل المستمد منها. وحسبنا أن نبين في هذا الصدد ما يلي: أن قواعد القانون الجنائي الإجرائي المتعلقة بمشروعية المراقبة وحالاتها وشروطها وضماناتها تعد بمثابة الإطار الذي يحدد لنا مدى الخروج عن المشروعية في هذا المجال على النحو الذي يحدد النطاق الصحيح لتطبيق قواعد القانون الجنائي الموضوعي[1].

المبحث الأول

تحليل المشكلات المتعلقة بالقانون الجنائي الموضوعي

الحماية الجنائية للحق في المعلومات والخصوصية وسلامة شبكات الاتصال الدولية وتقنياتها

(13)– دور القانون الجنائي في التوفيق بين التدابير التشريعية وغير التشريعية:

يلعب قانون العقوبات (قانون الجزاء) دوراً هاماً في هذا الانسجام ما بين التدابير التشريعية وغير التشريعية، ولهذا السبب فإن الجزء التالي من هذا التحليل يعالج هذه المشاكل الجنائية.

أولاً– التحديات والمشكلات المواكبة لتقنية المعلومات في مجال قانون العقوبات «قانون الجزاء»(الحماية القانونية لتقنية المعلومات):

(14) المشكلات القانونية للانسياب الدولي للمعلومات:

لا شك أن تقنية المعلومات: مكوناتها، وملحقاتها، وبرامجها تعد كلها أموالاً متقومة

(1) انظر: د. محمد أبو العلا، عقيدة المحادثات التليفونية، مرجع سابق، ص 17

تتمتع بحماية القانون، فقد ظهرت حقوق ومصالح لم تكن موجودة من قبل، وظهرت اعتداءات عليها «جرائم تقنية المعلومات»، ومع ازدياد هذا النوع من الجرائم وانتشارها وما يتوقع لها من زيادة مطردة ومتصاعدة؛ فلا بد من إستراتيجية شاملة ومتكاملة لمواجهة هذا النوع المعقد من الإجرام. ومن أهم عناصر هذه الإستراتيجية آليات القانون وتدابير وأجهزة العدالة الجنائية.

ففيما يتعلق بمضمون وطبيعة المعلومات والاتصال، لوحظ أنه ولئن كان المبدأ هو «حرية انسياب المعلومات» ووضع نظام «معالجة المعلومات إلكترونيا» في خدمة كل مواطن، إلا أن هذه الحرية ترد عليها بعض القيود المتعلقة بمضمون وطبيعة هذه المعلومات، ذلك إنه – وفي المقام الأول:

أ) يجب ألا تتضمن مادة المعلومة أي مسخ للهوية والثقافة الإنسانية للشعوب، تشكل افتئاتاً على حقوق أفرادها، أو حياتهم الخاصة، أو حرياتهم الشخصية. ومن جهة ثانية، تثار مشكلة اللغة المستخدمة في بث المعلومات؛ حيث تثبت مشكلة البث باللغة الوطنية la langue national لمتلقي المعلومات، وأخيراً فيما يتعلق بسلطة الدولة في الرقابة على بث المعلومات باستخدام الكمبيوتر. فمن المؤكد عدم تخلي الدولة عن هذه السلطة، نظراً لما لها من دور في الحفاظ على السيادة الوطنية، ومن أهم مظاهرها تأمين مصالح الأفراد والدول والحفاظ على الحريات والمبادئ القانونية والدستورية العامة، فضلا عن النظام العام في هذه الدول. ولكن يثور التساؤل– في ظل النظام الدولي الجديد الذي أهدر في الواقع كثيراً من مظاهر سيادة الدول، خاصة الدول الصغرى ـ عن إمكانية التخلي عن الرقابة الصارمة التي تمارسها الدول اليوم على حقل المعلومات، كطريقة لكفالة قيم مشتركة تنزع إلى الحفاظ على المشكلات المجتمعية تحت السيطرة؟ وهل ثمة أساليب أخرى غير الرقابة على المعلومات للحفاظ على ثقافة تضحِّى بقسط من الحرية غربية الطابع في مقابل إحساس قوي بالجماعة؟!. في المقابل، فإنه من الواضح أن الحكومة في الصين مثلا، مقتنعة بإمكان الجمع بين الاثنين، فقد صرح «واجيشوان» وزير البريد والمواصلات الصيني بأن «اتصالنا مع الإنترنت لا يعني بالنسبة لنا الحرية المطلقة للمعلومات»، وأضاف أن بكين سوف تتبنى «تدابير إدارة» غير محددة من أجل ضبط عمليات تدفق البيانات في كل خدمات الاتصال عن بعد في مجرى تطورها في الصين. «فليس هناك تناقض على الإطلاق بين تطوير البنية الأساسية للاتصالات عن بعد وممارسة سيادة الدولة، والاتحاد الدولي للاتصالات عن بعد يقر بسيادة كل دولة على اتصالاتها».

ب) مشكلات جمع وتخزين واستغلال المعلومات الاسمية عن الأشخاص (الطبيعيين والاعتباريين) وما ينطوي عليه ذلك، بالنسبة للأشخاص الطبيعيين من انتهاك لحياتهم

الخاصة، وسرقة الأسرار التجارية والصناعية للمشروعات والشركات.

ت) ظهور بعض المصالح الجديرة بحماية القانون وبصفة خاصة «الحق في الخصوصية المعلوماتية» و«الحق في الوصول إلى المعلوماتية» وضرورة التوافق بينهما وبين مبدأ «حرية انسياب المعلومات».

ث) مشكلات الحماية الجنائية للحقوق والمصالح المستحدثة الجديرة بحماية القانون الجنائي بشقية الموضوعي والإجرائي في مجال الجرائم المعلوماتية وجرائم تقنية المعلومات، وضرورة ملاحقة القانون الجنائي للتطورات السريعة والمتلاحقة في هذا المجال.

(15) تعريف المعلومات والبيانات (موضوع المعالجة الإلكترونية):

يرى بعض الفقهاء أن المعلومة تعبير يستهدف جعل رسالة قابلة للتوصيل إلى الغير، ثم هي قابلية للتوصيل بفضل علامة أو إشارة من شأنها أن توصل المعلومة للغير، فالتعبير وتوصيله إلى الغير يحقق وظيفة المعلومات وهي انتقال أو نقل المعرفة[1]. ويتميز هذا التعريف بأنه يبرز أهمية التعبير في الانتقال الضروري من الواقع أو الفكرة إلى المعلومة، فواقعة معينة أو فكرة ما لا تعتبر معلومة طالما أنها لم تأخذ شكل إشارة ملموسة[2]، وكما يقال فإن المعلومة لا تصبح معرفة إلا باستخدامها. والمعلومة قد تكون موضوعية وقد تكون ذاتية: فالمعلومة الموضوعية تتعلق ببيانات مجردة مثل الاسم، والموطن، والحالة المدنية، والعقوبات، فهي لا تعكس آراء شخصية، ومن ثم تعتبر من مميزات الشخصية لمن تتعلق به المعلومة باعتبار أنه صاحب عناصر معلومة. أما المعلومة الذاتية فهي التي تحمل رأياً ذاتياً عن الغير مثل المقال الصحفي أو الملف الإداري، فمؤلفها هو من وضعها في القالب القابل للانتقال، ومن ثم يختلف شخص المؤلف عن الشخص موضوع المعلومة[3]. والمعلومة قد تكون اسمية أو مجهلة، فهي تعتبر اسمية إذا كانت تسمح –مباشرة أو بطريقة غير مباشرة وتحت أي شكل– بالتعرف على الشخص محل هذه المعلومات، أو تجعله قابلاً للتعرف عليه، والمعلومات الاسمية المخزنة في الحاسب الآلي هي التي تمس الحياة الخاصة أو الحق في الخصوصية المعلوماتية[4].

(1) انظر: د. حسام الدين كامل الأهواني، الحماية القانونية للحياة الخاصة في مواجهة الحاسب الآلي، بحث منشور بأعمال مؤتمر الكويت الأول للقانون والحاسب الإلكتروني، المنعقد في 4–7 نوفمبر 1989، كلية الحقوق، جامعة الكويت، منشورات مؤسسة الكويت للتقدم العلمي 1994، ص 100.

(2) انظر: د. حسام الدين كامل الأهواني، المرجع السابق، ص 100.

(3) انظر: د. حسام الدين كامل الأهواني، المرجع السابق، ص 100.

(4) انظر: د. حسام الدين كامل الأهواني، المرجع السابق، ص 100 – 101 .

ثانياً – رصد المتغيرات والتحديات المستحدثة للحق في الخصوصية والأمن القومي للدول:

(16) المشكلات المستحدثة في مجال قانون العقوبات المعلوماتي:

إن آثار إجرام تقنية المعلومات تحديات لها وزنها بالنسبة لقانون العقوبات في كل الأنظمة القانونية، وهو ما سنشرحه على الشكل التالي:

16–1– ظاهرة إجرام تقنية المعلومات:

ترجع الإرهاصات الأولى لموضوع الحماية الجنائية للمعلومات – والذي أصبح محلاً لأبحاث أكثر تفصيلاً في الآونة الأخيرة – إلى الستينيات – عندما طرحت بعض الصحف وبعض الكتب العلمية على بساط المناقشة، موضوع البيانات الأولية التي تتناول ما يطلق عليه «إجرام تقنية المعلومات» سواء الجرائم الإلكترونية Cyber Crime مثل غش الكمبيوتر Computer Fraud أو الجرائم التي يخطط لها أو ترتكب عن طريق الكمبيوتر والاتصالات الإلكترونية والإنترنت. وتعالج هذه البيانات الأولية عن الموضوع في غالبيتها التلاعب بالحاسب الآلي وتعطيله والتجسس عليه، والاستعمال غير المشروع له. وبالنظر إلى أن الكثير من هذه البيانات قد استند بصفة خاصة على تقارير الصحف، فكان من العسير جداً معرفة ما إذا كانت الظاهرة المستحدثة لإجرام تقنية المعلومات تعد من قبيل الحقيقة أم الخيال[1].

وقد أجريت أبحاث علمية وأخرى في مجال علم الإجرام منذ بداية السبعينات، وقد أمكن الكشف على إثر هذه الأبحاث على مقدار ضئيل من جرائم تقنية المعلومات، ولكن يتضح في نفس الوقت أن الرقم الرسمي الهام لهذه الجرائم لم يعلن عنه بعد. وقد لاحظت مع ذلك الأبحاث الميدانية أن هناك حالات من جرائم تقنية المعلومات جديرة بالنظر، وعلى سبيل المثال حالة الغش المعروف في الولايات المتحدة بمصطلح «Equity fading» والحالة الألمانية «HERSTATT» وطبقاً لها تم التلاعب ببيانات شركة «فولفو» بالسويد[2].

(1) "According to the FBI, there has been a steady rise in both cyber-crimes, such as computer fraud, and crimes planned or accomplished with the aid of electronic communication and the Internet", Published in Thomas P. Ludwig, The Erosion of Online Privacy Rights in the Recent Tide of Terrorism, HEINONLINE, Citation: Computer Law Review and Technology Journal. (Vol. VIII), 2003-2004, Page: 131

(2) عن Dr. UlrichSieber، تحليل لموضوع: جرائم الكمبيوتر والجرائم الأخرى في مجال تكنولوجيا المعلومات، نشر هذا التحليل بالمجلة الدولية لقانون العقوبات، 1991، ص 989، وقد ترجمه إلى اللغة العربية د. محمد سامي الشوا، كلية الحقوق بجامعة المنوفية، ونشرت الترجمة العربية في أعمال المؤتمر السادس للجمعية المصرية للقانون الجنائي الذي انعقد في القاهرة 25–28 أكتوبر 1993.

16-2- التغير الذي طرأ على المفهوم العام لإجرام تقنية المعلومات:

لقد طرأ منذ الثمانينات من القرن الماضي تغير عميق في المفهوم العام والعلمي لإجرام تقنية المعلومات، وقد ظهر ذلك لأول مرة ليس فقط في مجال الإجرام الاقتصادي الذي تأثر بإجرام تقنية المعلومات، ولكن أيضاً في مجال الاعتداءات الموجهة ضد مصالح أخرى كالتلاعب بالحاسب الآلي الخاص بأحد المستشفيات، أو انتهاكات الحياة الخاصة لشخص بمساعدة الحاسب الآلي. وقد بدأ حتمياً خلق إستراتيجيات مستحدثة سواء لمراقبة الأمن في مجال تقنية المعلومات أو للردع الجنائي، ومرد ذلك الانتشار الواسع لسرقة البرامج والتلاعب بالمنافذ البنكية وإساءة أنظمة الاتصالات البعدية والتي تعرف بـ Hacking [1]، والتي جعلت من الشائع - علاوة على ذلك - انتهاك أي مجتمع للمعلومات.

ويتركز الاهتمام اليوم في مجال انحراف تقنية المعلومات فيما يعرف على وجه الخصوص بعمليات اختراق شبكات الحاسبات الآلية، ومراقبة أجهزة الاستخبارات للاتصالات والإنترنت، والتجسس على مواقع التواصل الاجتماعي، وسوء استخدام البيانات الشخصية للمستخدمين، وحجب ومطاردة المواقع بشبكات الاتصال والإنترنت، بالإضافة إلى برامج الفيروسات[2] والديدان، والتلاعب بأنظمة التحويل الإلكتروني للأموال وخاصة التحويل لتمويل الإرهاب، وأيضاً فيما يقال عنه بالتزوير المتقن[3].

16-3 - مخاطر انتهاك شبكات الاتصال والإنترنت:

لقد تبلورت مخاطر انتهاك شبكات الحاسبات الآلية من قبل عامة الناس (الأفراد العاديين) عندما حركت إحدى الدعاوى الجنائية في ألمانيا الفيدرالية سنة 1989 ضد مجموعة من الألمان منتهكي شبكات الحاسبات الآلية، واتهمت إياهم باختراق الأنظمة التقنية للمعلومات، الخاصة بالولايات المتحدة وإنجلترا وغيرها من البلدان الأجنبية بواسطة شبكات تقنية للمعلومات، وقاموا ببيع الأسرار المتحصل عليها إلى إدارة المخابرات الروسية .K.G.B. وأصبحت مخاطر برامج الفيروسات والديدان واضحة بنفس الوقت في نوفمبر 1988،

(1) ظهر هذا المصطلح لأول مرة في الستينات، وشاع استخدامه بين الطلبة الجامعيين في الولايات المتحدة والذين يتمتعون بقدر كبير من الكفاءة والمعرفة بعلوم الحاسب الآلي، وبقدرتهم، على اختراق شبكات الحاسبات الآلية بمجهوداتهم الخاصة وبدون تعليمات، وذلك عن طريق إدخال مركبات أرقام وحروف مختلفة بصفة مستمرة في الحاسبات الآلية والموجودة بمنازلهم بغرض الولوج غير المسموح به إلى نظام تقني للمعلومات. انظر Dr. UlrichSieber، تحليل لموضوع جرائم الكمبيوتر والجرائم الأخرى في مجال تكنولوجيا المعلومات، المرجع السابق، ص 48.

(2) وهي مجموعة من التعليمات التي تنتشر سريعاً لدرجة تصيب النظام التقني للمعلومات بالشلل التام ويصعب اكتشافها.

(3) انظر: Dr. UlrichSieber، تحليل لموضوع جرائم الكمبيوتر والجرائم الأخرى في مجال تكنولوجيا المعلومات، المرجع السابق، ص48.

حيث ظهرت التقنية المعروفة بـ internet –worm أي الدودة التي تصيب الحاسب الآلي بالشلل، والتي عن طريقها تمكن طالب أمريكي من تعطيل 6000 حاسب آلي خلال بضعة أيام. ومن المؤكد أن مجال جرائم تقنية المعلومات سيتوسع أكثر فأكثر في المستقبل نظراً لاستحداث أفعال اعتداء في مجال تقنيات الاتصالات السمعية والبصرية مثل نظام الإرسال المرئي والتقني للمعلومات أو الإرسال عبر القمر الصناعي[1]، ومراقبة أجهزة الاستخبارات للاتصالات والإنترنت.

لقد أثار إحصاء إجرام تقنية المعلومات تحديات لها وزنها بالنسبة للقانون الجنائي في كل أنظمته القانونية، ويرجع السبب في ذلك إلى الحقيقة التي مؤداها أنه حتى هذه اللحظة فإن الأشياء المادية والمرئية هي التي تكون محمية بالقوانين الجنائية، وحماية المعلومات والقيم المعنوية الأخرى –وإن وجدت منذ فترة زمنية قصيرة– إلا أنها حتى منتصف القرن العشرين كانت أقل أهمية، وقد طرأ تغيير جوهري على هذا الموقف أثناء العشرين سنة من القرن الماضي وحتى الآن، فقد أدى تطور المجتمع من مجتمع صناعي إلى مجتمع ما بعد الصناعي، والقيمة المتنامية لتقنية المعلومات في غضون فترة زمنية قصيرة، والتطور الهائل في علوم وتكنولوجيا الاتصال، أدى ذلك كله إلى تحديات ضخمة ومقتضيات حديثة لمواجهتها والتغلب عليها.

16–4– تأثر القانون الجنائي بالثورة الرقمية والمعلوماتية والتقدم في علوم وتكنولوجيا الاتصال:

وقد تأثر القانون الجنائي نتيجة لتغير نموذج الأشياء من مادية إلى معنوية، إذ ظهر ذلك في العديد من موجات التعديل لقانون العقوبات (قانون الجزاء)[2]، وتبع ذلك تطور مواكب للحماية الجنائية الإجرائية والضمانات المقررة في هذا الخصوص[3].

الموجة الأولى من التعديلات التشريعية كانت تتعلق بحماية الحق في الخصوصية:

لقد حدثت الموجة الأولى لتعديل قانون العقوبات (قانون الجزاء) في شأن حماية المعلومات وتقنياتها في السبعينات والثمانينات في العديد من الأنظمة القانونية الغربية، وكانت تتعلق

(1) انظر: Dr. UlrichSieber، تحليل لموضوع: جرائم الكمبيوتر والجرائم الأخرى في مجال تكنولوجيا المعلومات، المرجع السابق، ص 48–49.

(2) انظر: Dr. UlrichSieber، تحليل لموضوع: جرائم الكمبيوتر والجرائم الأخرى في مجال تكنولوجيا المعلومات، المرجع السابق، ص 51–50

(3) انظر: Dr. UlrichSieber، تحليل لموضوع: جرائم الكمبيوتر والجرائم الأخرى في مجال تكنولوجيا المعلومات، المرجع السابق، ص 51.

بحماية الحياة الخاصة «الحق في الخصوصية»[1]، وكان هذا التشريع في بداية هذه السنوات بمثابة رد فعل إزاء التهديدات المستحدثة للحياة الخاصة (الخصوصية)، والتي تأثرت بالإمكانيات الحديثة للتجميع والتخزين ونقل البيانات السرية والشخصية بإحدى الوسائل التقنية للمعلومات[2].

وللتغلب على هذه المشكلة، عمدت العديد من الدول الأوروبية – على الرغم من أن حق الخصوصية نشأ في الولايات المتحدة لدى فقهاء القانون– إلى إصدار تشريعات لحماية البيانات الشخصية للأفراد، على نحو يكرِّس حماية الحياة الخاصة لهم، ففي عام 1970 سنت ولاية هيس الألمانية أول قانون لحماية المعلومات والبيانات. وفي عام 1973 تبعتها السويد بإصدار قانون البيانات الشخصية (الذي يطبق على جميع قطاعات المجتمع)، وقانون السرية (الذي يطبق على الإدارات الحكومية فقط)، وقانون البيانات للإدارات الخاصة (الذي يطبق فقط على عمليات محددة في إدارات معينة)، ثم تبعتها الدول الأوروبية الأخرى[3].

وإذا أخذنا فرنسا مثالاً لتلك الدول، نجد أن حماية الحياة الخاصة قد حظيت باهتمام المشرع الذي أصدر أول قانون لهذا الغرض في 6 يناير 1978 لتنظيم المعلومات الآلية والسيطرة على التطور السريع للتكنولوجيا المعلوماتية، دون إخلال بحماية الحياة الخاصة وتحقيق الشفافية في الحصول على المعلومات، ومبدأ الحق في النسيان أو السهو والسرية، وعرف في ذلك الوقت بـ(وضع المعلوماتية في خدمة المواطن). وتطبيقاً لهذا القانون أنشئ جهاز إداري يتمتع بالاستقلال، ويتصف بالحياد الإلكتروني – ويتبع اللجنة الوطنية للمعلومات والحرية – ويتكون مجلس إدارته من عدد من المختصين وثلاثة قضاة يمثلون مجلس الدولة ومحكمة التمييز ومحكمة المحاسبات، ويجب على الإدارات العامة أن تلجأ لهذا الجهاز لمعرفة

(1) لمزيد من التفاصيل حول التشريعات ذات الصلة بالموضوع:

A. Title III of the Omnibus Crime Control and Safe Streets Act of 1968

B. Electronic Communications Privacy Act (ECPA)

1. The New Wiretap Act

2. The Stored Communications Act

3. Pen Registers & Trap and Trace Devices

C. Federal Intelligence Surveillance Act (FISA)

انظر:

4. Thomas P. Ludwig, The Erosion of Online Privacy Rights in the Recent Tide of Terrorism, HEINONLINE, Citation: Computer Law Review and Technology Journal. (Vol. VIII), 2003-2004, Page: 131 -.

(2) انظر: Dr. UlrichSieber، تحليل لموضوع: جرائم الكمبيوتر والجرائم الأخرى في مجال تكنولوجيا المعلومات، المرجع السابق، ص51.

(3) غوستاف جونسون، المرجع السابق، ص 4 – 5

رأيه في كيفية التعامل مع المعلومات، على نحو يكفل أكبر ضمان لحماية البيانات الشخصية من خلال الأدوات القانونية التي يراها.

وفي ظل تطبيق الحكومة الإلكترونية يميل الرأي إلى الإبقاء على هذا الجهاز ومكناته القانونية، مع السماح بإجراء التعديلات اللازمة لأداء مهامه، وهذا ما حدث في 27 أغسطس 1998 بموجب المرسوم بقانون رقم 98 – 751 الذي أنشأ لجنة وزارية خاصة للدعم التقني من أجل تطوير تكنولوجيا المعلومات والاتصالات في الإدارة (M.T.I.C.).

وقد أعطيت اللجنة صلاحيات واسعة من بينها: ضمان التنسيق بين الإدارات والمرافق المختلفة، وتشجيع نقل وتحويل وتبادل البيانات والمعارف، واقتراح المعايير والمواصفات التقنية المشتركة، وإعداد الاقتراحات حول تبادل المعلومات والبيانات الممكنة فيما بين المرافق والإدارات[1].

(17) تطور الحماية الجنائية للمعلومات وتقنياتها:

ونظراً لأن المعلومة، وإن كانت شيئاً غير مادي، إلا أنها تصلح لأن تكون محلاً للحقوق المالية وعلى الأخص حق الملكية، فعلى سبيل المثال تقوم وكالات الأنباء ببيع ما تحصل عليه من معلومات أو أخبار[2]. والمعلومة قد تكون منتجاً أو سلعة مستقلة سابقة على الخدمة التي قد تكون المعلومة محلاً لها، فالمعلومة تتميز وتستقل عن الشكل المادي الذي تتمثل فيه، سواء كان كتابة أو صوتاً أو صورة، وتستقل عن الخدمة التي تكون محلاً لها، فهي بالضرورة سابقة في وجودها على لحظة تقديمها في شكل صورة أو خدمة، فالمعلومة شيء متميز ومستقل لا يختلط بشكل تقديم المعلومة ولا بالخدمة التي تكون محلاً لها[3].

ومن جهة أخرى، تختلف المعلومة عن الفكرة، فالفكرة (Idée) قد تصلح منهاجاً أو أساساً لوضع مؤلف أو مصنف أو برنامج للحساب الآلي، وهي بهذه المثابة يمكن أن تقوم باعتبارها مالاً، أما المعلومة (Information) فهي ثمرة للمؤلف أو المصنف أو البرنامج، ويمكن أن تقوم باعتبارها خدمة(Service) [4].

---

(1) انظر: د. داود عبد الرازق الباز، الإدارة العامة (الحكومة) الإلكترونية، وأثرها على النظام القانوني للمرفق العام وأعمال موظفيه، مجلس النشر العلمي – جامعة الكويت 2004، ص255–258

(2) انظرDr.UlrichSieber، تحليل لموضوع: جرائم الكمبيوتر والجرائم الأخرى في مجال تكنولوجيا المعلومات، المرجع السابق، ص51.

(3) انظر: د. حسام الدين كامل الأهواني، المرجع السابق، ص 100.

(4) انظر: د. عمر الفاروق الحسيني، تأملات في بعض صور الحماية الجنائية لبرامج الحاسب الآلي، منشور بأعمال مؤتمر الكويت الأول للقانون والحاسب الآلي، المنعقد في الفترة من 4–7 نوفمبر 1989 – كلية الحقوق، جامعة الكويت، منشورات مؤسسة الكويت للتقدم العلمي 1994، ص 88.

وقد انعكست تلك الأفكار على الموجة الثانية لإصلاح قانون العقوبات في بداية الثمانينات، كثمرة للكفاح ضد الإجرام الاقتصادي الخاص بتقنية المعلومات. وقد أصبحت هذه التعديلات التشريعية ضرورية، لأن الأشكال المستحدثة لإجرام تقنية المعلومات لم يقتصر اعتداؤها على القيم المادية، والتي كانت محمية حتى هذه اللحظة بقانون العقوبات (قانون الجزاء)، بل امتد أيضاً إلى القيم المعنوية «كالبرامج الخاصة بتقنية المعلومات»، ولأن الوسائل الحديثة لاقتراف الجريمة، على سبيل المثال، «التلاعب بالحاسبات الآلية بدلاً من «النصب على شخص ما» كانت قد استخدمت. وبدلاً من التوسع المغالى فيه لتحديد عناصر الجريمة، وهو أمر غير مرغوب فيه لدى فقه القانون الجنائي؛ لتناقضه مع مبدأ الشرعية وحظر القياس في مجال التجريم والعقاب، فقد أصدرت العديد من الدول قوانين لمكافحة الإجرام الاقتصادي الخاص بتقنية المعلومات والتي تشمل تحريم الولوج غير المسموح به إلى أي نظام تقني للمعلومات[1].

وفي تطور جديد، تعددت وسائل حماية برامج الكمبيوتر ضد خطر التقليد والقرصنة، بدء من بند السرية التعاقدي، ومروراً بقوانين براءات الاختراع، وحتى قوانين حماية الملكية الفكرية (حق المؤلف). ونقتصر على بيان المجالين الأخيرين[2].

(18) الحماية القانونية لبرامج الكمبيوتر:
برامج الكمبيوتر وقوانين براءات الاختراع

استبعدت التشريعات المعاصرة برامج الكمبيوتر من مجال الحماية بواسطة براءات الاختراع؛ لأحد سببين أساسيين وهما: إما تجرد برامج الكمبيوتر من أي طابع صناعي، وإما صعوبة البحث في مدى جِدَّة[3] البرنامج لتقدير مدى استحقاقه للبراءة[4].

برامج الكمبيوتر وقوانين حماية الملكية الفكرية (حق المؤلف):

تقوم حماية حقوق المؤلف على فكرة بسيطة مؤداها أن كل المصنفات الفكرية، أيا كان نوعها (أدبية أو فنية..الخ)، أو شكل التعبير عنها (إلقاء، تصوير، نحت، رسم، طباعة،..الخ)

(1) انظر: اولريش شيبية، المرجع السابق، ص 52، د. نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية دراسة نظرية وتطبيقية، منشورات الحلبي الحقوقية.

(2) لمزيد من التفصيل حول هذه الموضوعات، انظر: د. محمد حسام محمود لطفي، الحماية القانونية لبرامج الحاسب الآلي، المرجع السابق، ص 25 وما بعدها.

(3) وفقا لقاعدة شهيرة «إن كل جديد مبتكر وليس كل مبتكر جديد»، بمعنى أن الجدة خلق من العدم، في حين أن الابتكار هو استحداث من الوجود، فالجدة هي في كون الاختراع غير مسبوق، والابتكار ليس إلا في التميز في الشكل دون المضمون. فأول برنامج للحاسب الإلكتروني كان جديداً ومبتكراً، في حين أن البرامج الأخرى المنتمية لنفس مجاله تعد مبتكرة وليست جديد؛ لأنها مسبوقة بأخرى، راجع في ذلك: د. محمد حسام محمود لطفي، المرجع السابق، ص 29.

(4) انظر: د. محمد حسام محمود لطفي، المرجع السابق، ص 29.

وأهميتها(مصنفات أصلية، أو مشتقة من مصنفات أصلية)، أو الغرض منها (البحث العلمي، أو المتعة الفكرية، أو مجرد العبث..الخ) تتمتع بالحماية التشريعية مدى الحياة للمؤلف وخمسين سنة بعد وفاته كقاعدة عامة. وعلى هذا الأساس لا تتمتع الأفكار المجردة التي لم ترق إلى مستوى المصنف الفكري بهذه الحماية. وتطبيقاً لذلك، لا تتمتع الخوارزميات[1]– لأنها من قبيل الأفكار– بأية حماية تشريعية، ومن ثم تتمتع برامج الكمبيوتر بالحماية التشريعية بشرط أن تكون مبتكرة[2].

ولما كانت تشريعات حماية حق المؤلف (الملكية الفكرية) تكاد تتطابق في العالم أجمع بفضل انضمام معظم دول العالم إلى اتفاقية برن أو جنيف أو الاثنتين معاً، فقد أصبحت تشريعات حماية حقوق التأليف تتسم بالعالمية، وهي تحمي كل المصنفات المبتكرة أياً كان شكلها أو الغرض منها أو وسيلة التعبير عنها أو أهميتها، بشرط إثبات خاصية الابتكار. وقد جاءت النصوص النموذجية لحماية برامج الكمبيوتر الصادرة عن المنظمة العالمية للملكية الفكرية عام 1978، بأحكام لحماية حق المؤلف بعد تهذيب بعضها؛ حتى تتفق مع الطبيعة الخاصة لبرامج الكمبيوتر[3].

انطلقت الموجة الثالثة من التعديلات التشريعية خلال الثمانينات بغرض توفير حماية أفضل للملكية الذهنية في مجال تقنية المعلومات، وبعد أن استبعدت العديد من الدول في السبعينات برامج تقنية المعلومات من الحماية عن طريق قانون البراءات إلا أنها أصدرت قوانين أخرى لحماية برامج تقنية المعلومات عن طريق حقوق المؤلف، وفي نفس الوقت شددت العقوبات المعمول بها في العديد من الأنظمة القانونية، وقد أصدرت بعض الدول منذ عام 1984 قوانين خاصة لحماية المنتجات القابلة للانتقال عن طريق دوائر إلكترونية[4]. ولم يقف الأمر عند ذلك الحد، فقد حلت موجة رابعة لإصلاح التشريعات تدمج الابتكارات في مجال الإجراءات الجنائية، وتستجيب النصوص المستحدثة لاستقلال واحتياجات الشرطة القضائية بالنسبة للتحقيقات في مجال إجرام تقنية المعلومات.

ونحن حالياً بصدد موجة خامسة لإصلاح التشريعات التي صدر بعضها في الدول الغربية، خاصة في الولايات المتحدة الأمريكية وإنجلترا، والبعض الآخر من التشريعات في سبيل الإصدار لتنظيم مراقبة الاتصالات والإنترنت وضمان حماية الخصوصية وسيادة

(1) تستخدم كلمة logarithm خوارزمية، في لغة الكمبيوتر، للدلالة على "منهاج البرنامج" أو "خطوات الحل". أما في اللغة العادية فهي تعني نظام العد العربي أو العشري.
انظر: تعليق الأستاذ عبد السلام رضوان، ترجمة لمؤلف بيل جيتس، المعلوماتية بعد الإنترنت، المرجع السابق، ص 280.
(2) انظر: د. محمد حسام محمود لطفي، المرجع السابق، ص 32.
(3) انظر: د. حسام محمود لطفي، المرجع السابق، ص 37.
(4) انظر: اولريش شيبية، المرجع السابق، ص 51 – 52.

الدول، وفي نفس الوقت لمكافحة الموجات العاتية من الإرهاب والجريمة المنظمة التي تجتاح العالم الآن[1]. فقد اهتم المشرع الأمريكي بالتحايل المعلوماتي (الغش المعلوماتي)، فأصدر في 10 أكتوبر 1984 قانوناً مستقلاً للمعلوماتية حدد فيه كل ما يتعلق بالتحايل أو الغش المعلوماتي (Frauds and related activity connection with computers)[2]. كما اهتم المشرع الفرنسي بتجريم إتلاف المال المعلوماتي المعنوي «البرامج والمعلومات» وأيضاً المادي أي أجهزة وأدوات الحاسب، وذلك من خلال نصوص القانون رقم (19 – 88) في 5 يناير 1988 عن بعض جرائم المعلوماتية،حيث أفرد لها باباً مستقلاً في قانون العقوبات، وقد احتلت جريمة الإتلاف العمدي للأموال المعلوماتية مكاناً هاماً في هذا القانون، إذ أفرد نصين مستقلين لمعالجة مشاكل إتلاف برامج وأدوات الحاسب. وبالإضافة إلى ذلك، أورد المشرع الفرنسي نصاً مستقلاً يعالج جريمة التوصل بطريق التحايل لنظام المعالجة الآلية للبيانات، ويعتبر هذا التوصل لصيق الصلة بجريمة الإتلاف العمدي للأموال المعلوماتية المادية والمعنوية، إذ قد يترتب على ذلك إتلاف لهذا المال[3].

المبحث الثاني
النظرية العامة للحماية الجنائية للمعلومات:
أثر مكننة المعلومات وخدمات الإنترنت على الحق في المعلومات

(19) الخصوصية في إطار النظرية العامة للحماية الجنائية للمعلومات:

تشكل خدمات ومنتجات المعلومات أضخم وأسرع قطاع اقتصادي عالمي متنامي في الوقت الحالي، فعلى سبيل المثال، فإن الشبكة العالمية للإنترنت، وهي الأكثر انتشاراً وتواجداً بين أنظمة المعلومات العالمية، تعتبر أسرع وسيلة متنامية اقتصادياً في التاريخ المعاصر. وإن الدور غير العادي لمنتجات وخدمات المعلومات وأثرها التحويلي على كافة جوانب النشاط

(1) "This increase in criminal and terrorist activity and the public's resulting sense of vulnerability has shifted pressure on the government from privacy concerns to safety issues. Not surprisingly, the American public has implicitly conceded a measure of its privacy rights in order to regain some sense of security, and the legislative and executive branches have responded accordingly, most notably with the passage of the USA PATRIOT Act (hereinafter "Patriot Act"). The Patriot Act, quickly enacted after the September 11 attacks in an effort to prevent future attacks, further reduced the already insufficient statutory protection of electronic communications privacy", Published in: Thomas P. Ludwig, The Erosion of Online Privacy Rights in the Recent Tide of Terrorism, HEINONLINE, Citation: Computer Law Review and Technology Journal. (Vol. VIII), 2003-2004, Page: 131.

(2) انظر: د. هدى حامد قشقوش، المرجع السابق، ص 8.

(3) انظر: د. حسام الدين كامل الأهواني، المرجع السابق، ص 101، د. هدى حامد قشقوش، مرجع سابق، ص 8.

البشري قد طرح الكثير من المشكلات والقضايا القانونية الحديثة[1]. ووفقاً للأبحاث الأخيرة التي أجرتها الولايات المتحدة – كما يقول البروفيسور الفرنسي جون فريشيني – فقد لوحظ قلق المستفيدين من هذه الخدمات من جمع واستخدام المعلومات الشخصية التي تخصهم فيما يمس حقوقهم في «الخصوصية المعلوماتية»[2].

ويلاحظ بعض الفقهاء أن تحديد الأمور التي تدخل في نطاق الحياة الخاصة من الأمور المرنة التي يختلف فيها الفقه والقضاء المقارن. ولقد انتقلت فكرة الحياة الخاصة «الخصوصية» من القانون الأمريكي إلى قوانين البلاد الأوروبية. ويلاحظ أن الحق في الخصوصية في القانون الأمريكي يتسع مفهومة ليغطي فكرة «حقوق الشخصية» في مفهوم قوانين العائلة الرومانية الجرمانية، ولهذا فإن البحث في العلاقة بين الحياة الخاصة والحاسب الآلي وشبكات المعلومات الدولية يتأثر إلى حد كبير بمفهوم الخصوصية في القانون الأمريكي، ولا يخفى أن أول من تنبه إلى المشكلة هو القانون الأمريكي، نظراً لبدء تطور الحاسبات الآلية في الولايات المتحدة، ونقلت المشكلة إلى الفقه الأوروبي مع التأثر بصورة أو بأخرى بالمفهوم الأمريكي للحق في الخصوصية[3].

فإذا كانت شبكة المعلومات (Internet) قد أثارت مشكلة حماية المعلومات الشخصية، وخاصة في مجال الحياة الخاصة، فإن القلق الذي تثيره المعلوماتية قد بدأ منذ السبعينيات، مما جعل دولاً عديدة تنهض لوضع نظم قانونية ملائمة للحماية إلى جانب الحماية التقليدية، ولكن بمفهوم مختلف كما تظهره الحالات النموذجية في الاتحاد الأوروبي والولايات المتحدة التي تستند إليها كمرجع – حسب قول البروفيسور الفرنسي جون فريشيني. وتتزايد في الوقت المعاصر ضرورة حماية الأفراد من حيث المعلومات الخاصة بهم، مع تطور النظم المعلوماتية والشبكات مؤخراً[4].

إلى جانب الحرص على حماية الحياة الخاصة، والحق في الخصوصية (Privacy) تبدو أيضاً وعلى نفس المستوى، حماية الملكية الفكرية (Intellectual property)، والأمن (Security)، والسرية[5]، كما ظهرت مشكلات أخرى تتطلب حلاً أكثر شمولية،

(1) انظر:

Cate Fred H., legal controls of internet information, research presented on Kuwait, first conference in legal and judicial informatics, to modernize and develop the legal activities, organized by Ministry of Justice, State of Kuwait in cooperation with general secretarial of the Arab league, 15 – 17 Feb. 1999, Abstracts, P. 62.

(2) FRAYSSINET Jean: Effect of Information Automation on Privacy, Research Presented on Kuwait First Conference Noti`ced Above, p. 27.

(3) انظر: د. حسام الدين كامل الأهواني، المرجع السابق، ص 103.

(4) انظر: Frayssinet Jean، op. cit، p. 27.

(5) Lee A. Bygrave. Privacy Protection in a Global Context – A Comparative Overview. HEINONLINE. Citation: 47 Scandinavian Stud. L. Page-319 - 2004.

منها مشكلة التحكم في المعلومات الضارة (Control of Harmful Information)[1].

(20) الحاجة لوضع نظرية عامة للحماية الجنائية للمعلومات:

وقد أبان التحليل للقوانين في الدراسات المقارنة أن الحماية الجنائية للمعلومات والحق في الخصوصية وحرية التعبير وحرية الصحافة في كل دولة بحاجة ماسة لوضع نظرية عامة لها، ومرد ذلك أنه في غالبية الحالات فإن الحماية الجنائية لكل من الحياة الخاصة، والأموال والحقوق الذهنية وسوء استعمال البيانات الشخصية لمستخدمي شبكات الاتصال والإنترنت، إزاء إجرام تقنية المعلومات، قد تم مناقشتها كل على حدة، وأن الاقتراحات الإصلاحية المقدمة في هذا الشأن تتناسب دائماً وفقاً لكل حالة وبدون تمييز ما بين المسائل المتعلقة بالحماية العامة للمعلومات، والمسائل الخاصة بحماية المعلومات المخزَّنة في الحاسب الآلي، والحماية المتعلقة بالبيانات الشخصية والخصوصية، وعلى الرغم من أن حماية المعلومات تشهد تطوراً مستمراً بالمقارنة بحماية الأموال المادية، إلا أن ذلك يحدث دون الوضع في الاعتبار خصائص الأموال المعنوية، ويجب من الآن فصاعداً أن توجد استجابات قانونية حديثة للتحديات الحالية لمجتمع المعلومات وبخاصة التحديات المستحدثة للحق في الخصوصية، بل وأكثر من ذلك فمن الضروري أن نخلق فقهاً جديداً من أجل الحماية الجنائية للمعلومات[2].

(21) أسس وعناصر النظرية الحديثة للحماية الجنائية للمعلومات:

يجب أن تشيد النظرية الحديثة للحماية الجنائية للمعلومات على:

1- الحق في المعلومات وقانون تقنية المعلومات.

2- الحق في الخصوصية وقانون مراقبة الاتصالات والإنترنت.

وهي تشهد حالياً تطوراً في بعض الدول، ووفقاً لعلوم الحاسب الآلي وتقنية المعلومات،

---

(1) انظر:

Cate Fred H.: op. cit., p. 62, FrayssinetHean: op. citm p. 27.

(2) انظر Dr. UlrichSieber، تحليل لموضوع: جرائم الكمبيوتر والجرائم الأخرى في مجال تكنولوجيا المعلومات، المرجع السابق، ص 52. د. غنام محمد غنام، دور قانون العقوبات في مكافحة جرائم الكمبيوتر والإنترنت وجرائم الاحتيال المنظم باستعمال شبكة الإنترنت، دار الفكر والقانون، المنصورة، سنة 2013. د. علي عبدالقادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، دار الجامعة الجديدة، الإسكندرية، سنة 2010. أ. علي عدنان الفيل، الإجرام الإلكتروني، منشورات زين الحقوقية، مكتبة زين الحقوقية والأدبية ش.م.م، الطبعة الأولى، سنة 2011. د. عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية. د. محمد الشناوي، مكافحة جرائم النصب المستحدثة، الطبعة الأولى، دار البيان، سنة 2006. د. عبدالله حسين على محمود، سرقة المعلومات المخزنة في الحاسب الآلي، دار النهضة العربية، القاهرة، مصر.

تعترف النظرية الحديثة للحق في المعلومات بأن المعلومات عامل أساسي ثالث بجوار المادة والطاقة، وتنظر الأبحاث الميدانية إلى المعلومات ليس باعتبارها فقط قيمة اقتصادية وثقافية وسياسية مستحدثة، ولكن أيضاً بوصفها طاقة كامنة للمخاطر الاستثنائية (حيث تستخدم في الإرهاب والتجسس والمراقبات غير المشروعة للاتصالات وسائر الانتهاكات ضد المصالح المعتبرة).

(22) نقطة الانطلاق المستحدثة للحق في المعلومات:

بناءً على ما سبق، تعترف النظرية الحديثة للحق في المعلومات بحقيقة مفادها: أن التقنية المستحدثة للمعلومات قد عدلت من خصائص المعلومات، وعلى الأخص بتحسين أهميتها وبتحويل المعلومات إلى عامل ايجابي من شأنه أن يحدث تغييرات في أنظمة تقنية المعلومات بدون تدخل من أي فرد[1]، وأن يحمى بفاعلية الأمن القومي للدول، مع ضمان الحرية الفردية من أن تنتهك دون مبرر ودون سند من القانون. وهكذا تعكس نقطة الانطلاق المستحدثة للحق في المعلومات حقيقتين:

الأولى– حقيقة مضمونها أن التقدير القانوني للأموال المادية يجب أن يختلف عن نظيره بالنسبة للأموال المعنوية، ويتعلق أول مظهر للخلاف بحماية المالك أو الحائز للأموال المادية أو المعنوية، وفي حين أن الأموال المادية، –نظراً لطبيعتها– يستأثر بها شخص محدد على نحو مطلق، فإن المعلومات بالأحرى هي مال شائع، ومن ثم يجب أن تكون من حيث المبدأ حرة، ولا يجب أن تحمى بالحقوق الاستئثارية والتي تقتصر على الأموال المادية. ويعد هذا المبدأ الأساسي «حرية الوصول إلى المعلومات» شرطاً جوهرياً لأي نظام اقتصادي وسياسي حر، وعلاوة على ذلك فهو في غاية الأهمية من أجل تقدم الدول التي تكون في طريقها للتنمية.

الحقيقة الثانية – وترجع إلى الخاصية الثانية لتقدير الأموال المادية والمعنوية، وهي أن حماية المعلومات يجب ألا ينظر إليها بوصفها تمثل مصالح اقتصادية للملاك، ولكن أيضا تمثل مصالح الأشخاص الذين تأثروا بفحوى المعلومات، ويبرر هذا الوجه القيود المستحدثة في نطاق حماية الحياة الخاصة في مجال تقنية المعلومات. وقد صار من الواضح إذن أنه يستحيل تقليل القوانين التشريعية الخاصة بتقنية المعلومات قياساً على النصوص الخاصة بالأموال المادية، ولكن يجب زيادة الأسس الخاصة بها [2].

(1) انظر: Dr. UlrichSieber، تحليل لموضوع: جرائم الكمبيوتر والجرائم الأخرى في مجال تكنولوجيا المعلومات، المرجع السابق، ص 53–52

(2) انظر: Dr. UlrichSieber، تحليل لموضوع: جرائم الكمبيوتر والجرائم الأخرى في مجال تكنولوجيا المعلومات، المرجع السابق، ص 54–53.

(23) طبيعة الحق في المعلومات وأنواعه:

إن تحديد طبيعة الحق في المعلومات يستلزم تحليلاً أكثر تعمقاً لماهية الحق، وخصائصه القانونية التي تميزه عن غيره من الحقوق الأخرى التي قد تشتبه معه أو تختلط به، إلا أننا نحدد في عجالة –تقتضيها طبيعة الدراسة– طبيعة الحق في المعلومات وأنواعه، باعتباره من أهم المصالح التي ينبغي أن تحظى بالحماية القانونية، وعلى الأخص الحماية الجنائية، آخذين في الاعتبار جميع المؤشرات الحديثة الدالة على وجوده، بما يكفي لتحديد مفهومه العام ودلالته، وخصائصه. وبصفة عامة تعتبر المعلومات شيئاً غير مادي يصلح لأن يكون محلاً للحقوق الشخصية والمالية[1].

(24) أنواع الحق في المعلومات:

يندرج تحت الحق في المعلومات مجموعة من الحقوق، أهمها الحق في الخصوصية المعلوماتية، والحق في الملكية الفكرية للمعلومات، ومن أهم تطبيقاته الحق في ملكية برمجيات الكمبيوتر.

(25) التقنيات الجديدة للمعلوماتية وضرورة حماية المعلومات الشخصية:

في إطار مجتمع المعلومات الإلكترونية الرقمية، تتعرض بعض الحقوق والحريات للأفراد للانتهاكات من خلال المعلومات المخزنة عنها ببنوك المعلومات وشبكات الإنترنت. ويعزز ضرورة الحماية تطور المعلوماتية والشبكات وازدياد مخاطرها على الرغم من إيجابياتها[2]. وتبدو أهمية حماية الحياة الخاصة للأفراد المعنيين بالبيانات المختزنة، على سبيل المثال، في حالة التفتيش غير القانوني لحسابات بعض الأفراد الموجودة في الخارج من قبل سلطات بلادهم، وفي حالة المراقبة الشاملة للفرد عن طريق الجمع الموسع للبيانات الاسمية، وأيضاً في حالة إذاعة معلومات وهمية في شأن المنشآت وأوضاعها المالية، كإذاعة ديون مستحقة عليها. كذلك حالة الاستخدام التعسفي للبيانات الطبية، على سبيل المثال: «معلومات تتعلق بالإيدز».

(26) الحماية القانونية للحق في المعلومات:

تبرهن جميع الأمثلة السابقة على أن مجال خصوصية المواطن في مجتمع المعلومات يجب أن يحمى بقوانين حديثة في المجال المدني والقانون العام والجنائي، وينبغي التخلي، فيما يتعلق بالحماية الجنائية للحق في الخصوصية، عن حرفية النص الجنائي، وعن

(1) انظر: Dr. UlrichSieber، المرجع السابق، ص 53.

(2) انظر: Frayssinet Jean، op. cit، p. 27. وكذلك: د. أسامة عبد الله قايد، الحماية الجنائية للحياة الخاصة وبنوك المعلومات، ص 3 وما بعدها.

العناصر المبهمة المكونة للجريمة، والتي توجد حالياً – كما يقول – أولريتش – في كثير من الأنظمة القانونية[1]. كذلك أصدرت فرنسا في 6 يناير 1978 قانوناً خاصاً بالمعالجة الإلكترونية للبيانات الاسمية[2]، وطبقاً للمادة الرابعة من هذا القانون تعتبر المعلومات اسمية إذا كانت تسمح، مباشرة أو غير مباشرة، وتحت أي شكل بالتعرف على الشخص محل هذه المعلومات، أو تجعله قابلاً للتعرف عليه، والعبرة بأن تكون المعلومات اسمية وقت تسجيلها أو تخزينها في الحاسب الآلي. فإذا كانت المعلومات اسمية وقت الحصول عليها ولكن عند تخزينها تم محو كل ما يشير إلى شخصية صاحبها بحيث أصبح من غير الممكن التعرف عليها فإن المعلومات تكون غير اسمية. والمعلومة الاسمية هي التي يبدأ بتخزينها في الحاسب الآلي المساس بالحياة الخاصة، أما المعلومات المجهلة التي لا تدل على من تتعلق به فلا تثير أيه صعوبة، لأن المجهول لا خصوصية له[3]. ومقتضى الحماية أن تشمل المعلومات الاسمية حتى ولو لم تكن تتعلق بالحياة الخاصة، فالحماية تمتد إلى المعلومات الاسمية المتعلقة بالحياة العامة، وعدم قصر الحماية على المعلومات المتصلة بالحياة الخاصة يستهدف من جهة تفادي صعوبة التفرقة بين الحياة الخاصة والحياة العامة متى كانت المعلومات المختزنة في الحاسب الآلي ناقصة مما يستوجب تصحيحها، ولكن صور وأنواع الضمانات تختلف بحسب ما إذا كانت المعلومات الاسمية تتصل بالحياة الخاصة أو الحياة العامة، فبحسب الأصل، يحظر تخزين البيانات المتصلة بالحياة الخاصة دون تلك المتعلقة بالحياة العامة[4].

(27) المشكلة الأساسية للحماية الجنائية للحق في المعلومات:

يؤدي ظهور هذا «الحق في المعلومات» بالنسبة للقانون الجنائي الموضوعي إلى مشكلة أساسية، ويمكن تحليلها وتأصيلها إلى محورين رئيسين:

أولاً– بات من الضروري البحث عن مدى حماية المالك أو حائز المعلومات في الأنظمة القانونية الوطنية المختلفة.

ثانياً– يجب الإحاطة بتفاصيل حماية الحياة الخاصة (الحق في الخصوصية) للفرد والمعني بفحوى المعلومات وزيادة أسس تلك الحماية.

المحور الأول – يتعلق بحماية المالك أو الحائز للمعلومات:

ينبغي على القانون الجنائي أن يضع في الاعتبار أمرين أساسيين، **الأول:** من الضروري

(1) انظر: Dr. UlrichSieber، المرجع السابق، ص 56 – 57.
(2) انظر: د. هدى حامد قشقوش، المرجع السابق، ص 8.
(3) انظر: د. حسام الدين كامل الأهواني، المرجع السابق، ص 101.
(4) انظر: د. حسام الدين كامل الأهواني، المرجع السابق، ص 101.

أن يثير مسألة تتعلق بالحالات التي ينبغي فيها أن يحمي قانون العقوبات الاستخدام المطلق للمعلومات، والحالات التي ينبغي فيها أن يحمي بقاء المعلومات على سريتها.

الأمر الثاني– أن يقرر إلى أي مدى تحمى جنائياً «سلامة وصحة المعلومات وسلامة انتقالها»[1].

(28) أولاً– مجال الاستخدام المطلق للمعلومات ومجال بقاء المعلومات سرية:

من الضروري أن تثار مسألة تحديد الحالات التي ينبغي وفقاً لها أن يحمي قانون العقوبات «الاستخدام المطلق للمعلومات» بالتوازن مع مبدأ «حرية الوصول إلى المعلومات» وحق الناس في المعرفة «The People's Right to Know»[2].

(29) التوافق بين ضمان «مجال السرية المطلقة» و«مبدأ حرية الوصول إلى المعلومات»:

مبدأ حرية انسياب المعلومات من خلال تقنية المعلومات:

– المعلومات بالأحرى مال شائع؛ ومن ثم يجب أن تكون من حيث المبدأ حرة، ولا يجب أن تحمى بالحقوق الاستئثارية التي تقتصر على الأموال المادية. ويعد هذا المبدأ الأساسي (حرية الوصول إلى المعلومات) شرطاً جوهرياً لأي نظام اقتصادي وسياسي حر، وعلاوة على ذلك فهو في غاية الأهمية من أجل تقدم الدول في طريقها للنمو كما ذكرنا آنفاً.

– ومن تطبيقات هذا المبدأ في فرنسا القانون الذي اشتهر باسم قانون معالجة المعلومات والحريات «L'informatique et les libertes» الصادر بتاريخ 6 يناير 1987 وتنص المادة الأولى منه على أن معالجة المعلومات يجب أن تكون في خدمة كل مواطن، وقد تقرر المبدأ وتأيَّد في عدة قوانين لاحقة منها قانون 30 سبتمبر 1986 المعدل بالقانون

(1) انظر: Dr. UlrichSieber، تحليل لموضوع: جرائم الكمبيوتر والجرائم الأخرى في مجال تكنولوجيا المعلومات، المرجع السابق، ص54

(2) Along with restrictions on governmental invasion of privacy, restrictions exist which limit the type of information that can be withheld from the public. Recognizing that, if left unaccountable, the government may be prone to abuse its powers and then attempt to cover up any wrongdoing, Congress passed the Freedom of Information Act (FOIA) in 1966. This Act allows the public to have access to information regarding the government's activities and was designed to promote disclosure of, and prevent, "waste, fraud, abuse, and wrongdoing in the Federal Government. Technological advances have necessitated that the Act be amended to incorporate items such as the access to information stored in computers.

لمزيد من التفصيل حول حق الناس في المعرفة انظر:

Karen E. Jones,The Effect of the Homeland Security Act on Online Privacy and the Freedom of Information Act, HEINONLINE. Citation: University of Cincinnati Law Review (Vol. 72) Page: 787 - 2003-2004.

17يناير 1989، حيث تقرر مبدأ حرية المواطن في الإفادة من نظام معالجة المعلومات، فنصت المادة الأولى منه على مبدأ حرية الاتصال السمعي والبصري Liberte de communication audio visuelle[1].

- وقد اهتمت معظم الدول بتقرير هذا المبدأ منها الولايات المتحدة الأمريكية، التي تعد أولى الدول المسيطرة على تكنولوجيا المعلومات، إذ وضعت قانون الحق في الخصوصية Privacy Act في أواخر 1974 بسبب الانتشار الكبير للمعلومات وخشية استخدامها بالكمبيوتر شبكات المعلومات بصورة تستبيح انتهاك الأسرار[2].

- ولم يقتصر الاعتراف بحرية انسياب المعلومات باستخدام تقنية المعلومات على النطاق الوطني، وإنما امتد ليشمل النطاق الدولي، ففي عام 1985 تبنت منظمة التعاون والتقدم الاقتصادي (OCED)عدة توصيات تهدف إلى كفالة حرية الحياة الخاصة للأفراد، وضمان انسياب المعلومات المؤكدة والصحية من خلال تقنية المعلومات[3]، وأصدرت المنظمة تقريراً عن الجريمة المتعلقة بالكمبيوتر وتحليل السياسة القانونية الجنائية الذي استعرض القوانين الجنائية القائمة والمقترحات الخاصة بالتعديل في عدد من الدول الأعضاء، وتضمن التقرير قائمة بالحد الأدنى لأفعال سوء استخدام الكمبيوتر التي يجب على الدول أن تجرمها وتفرض لها عقوبات في قوانينها[4]. وقد صدرت اتفاقية المجلس الأوروبي لحماية الأشخاص في مواجهة المعالجة الآلية للمعلومات بهدف ضمان انسياب المعلومات عبر الحدود الدولية الأوروبية، إذ تعهدت تلك الدول بموجب هذه الاتفاقية بالتعاون على إزالة العوارض التي تحول دون هذا الانسياب، وضمان مرونة نقل المعلومات وتدفقها. كما أصدر المجلس الأوروبي توجيهات إلى المشرعين كي يساعدوا في بيان الأنشطة المتعلقة بالكمبيوتر التي يجب حظرها من الناحية الجنائية، وكيف يتم ذلك في مواجهة المصالح المتعارضة بين الحاجة للحماية الجنائية ضد هذه الأنشطة من ناحية، وحماية الحريات المدنية للأفراد من ناحية أخرى[5].

- وأخيراً فلا ريب في أن قيام مئة دولة بالاتفاق على إنشاء الاتحاد الدولي المعروف باسم

(1) انظر: Dr. UlrichSieber، المرجع السابق ، ص 54

(2) انظر: د. حسنى حسن المصري، المرجع السابق، ص 384

(3) انظر: د. حسنى حسن المصري، المرجع السابق، ص 384 – 385

(4) انظر: د . محمد محي الدين عوض، مشكلات السياسة الجنائية المعاصرة في جرائم نظم المعلومات (الكمبيوتر) ، بحث مقدم للمؤتمر السادس للجمعية المصرية للقانون الجنائي القاهرة 25–28 أكتوبر 1993 حول مشكلات المسؤولية الجنائية في مجال الإضرار بالبيئة، الجرائم الواقعة في مجال تكنولوجيا المعلومات، أعمال المؤتمر، دار النهضة العربية 1993.

(5) انظر: د. حسني حسن المصري، المرجع السابق، ص 284 – 285

«اتحاد القمر الصناعي الدولي للاتصال عن بعد» يعد اتفاقاً دولياً يتضمن الاعتراف بحرية هذه الاتصالات التي تضمن انسياب المعلومات عبر حدود الدول الأطراف[1].

- ولكن لا يخفى أن الاعتراف بحرية انسياب المعلومات بالوسائل التقنية الحديثة لا يعني الاستخدام المطلق للمعلومات؛ لأن هناك من يسيء لهذه الحرية، فيجنح بها بصورة أو بأخرى قد تصل إلى ارتكاب الجرائم، ومن ثم فلا مناص من تنظيم هذه الحرية بوضع الشروط القانونية التي تضمن صدق وسلامة المعلومات، وعدم الإضرار بمصالح الدول والأفراد.

- ومن ثم بات من الضروري، بالنسبة لقانون العقوبات، أن يحدد الحالات التي ينبغي وفقاً لها أن يحمي الاستخدام المطلق للمعلومات والإبقاء على سريتها. وينبغي على المشرع، عند تحديد مجال السرية المطلق وضمان حمايتها في مجال تقنية المعلومات وعلاقتها بمبدأ حرية الوصول إلى المعلومات أن يحدث نوعاً من التوازن والتوافق بينهما، بحيث يقتصر نطاق السرية في مجال تقنية المعلومات على المعلومات والبيانات الخاصة المختزنة في الحاسبات الآلية، وفضلا عن ذلك ينبغي على الشركات المنتجة للحاسبات الآلية وبرامجها أن توفر لها الأمن بوسائل تقنية عالية الفعالية، وهو ما تقوم به غالباً جميع الشركات المنتجة باعتبارها تخص جودة منتجاتها وأمانها من ناحية، وباعتبارها تدابير أمن للمستخدم أيضاً من ناحية أخرى.

(30) حماية الحق في ملكية المعلومات:

- تختلف حماية الحق في ملكية المعلومات (ملكية البرامج) ضِيقاً واتساعاً في الفقه المقارن بحسب التعريف «للبرنامج»، وهل يشمل فحسب مجموعة «التعليمات الموجهة إلى الحاسب الآلي» أو يضم إلى ذلك عناصر أخرى لا ينطبق عليها وصف البرنامج بالمعنى الفني الدقيق «مثل وصف البرنامج Discription de programe المستندات الملحقة documentation auxilaire». تبدو أهمية التفرقة بين تعريف ضيق وآخر واسع للبرنامج في تحديد محل الحماية ونطاقها، فالأخذ بالتعريف الضيق من شأنه أن يضفي الحماية الجنائية على التعليمات المجردة الموجهة إلى الحاسب الآلي، بينما الأخذ بالتعريف الواسع يضفي هذه الحماية على العنصرين الأخيرين أيضاً وهما وصف البرنامج وكذلك المواد المساعدة الرئيسية»[2].

- ولعل هذا الاختلاف هو السبب الذي من أجله اختار المشرِّع الفرنسي بحق أن يبسط

(1) انظر: د. حسني حسن المصري، المرجع السابق، ص 285

(2) انظر: د. عمر الفاروق الحسيني، المرجع السابق، ص 76 -78

حمايته الجنائية على «نظام المعالجة الآلية للبيانات» وليس على البرنامج فقط أو غيره من عناصر النظام الآلي[1].

– ويوضح الأستاذ أندريه لوكا Prof. Andre Lucas أن حماية البرامج المعلوماتية هي حماية شاملة، وترجع حماية الملكية المعلوماتية Protection of informatics Bases إلى تطبيق نظام الملكية الفكرية Intellectual Rights في قطاع المعلومات، والمقصود بها برامج الكمبيوتر، وبرامج لغة الكمبيوتر، ووسائط المعلومات، والاختراعات المساعدة للكمبيوتر[2].

(31) نماذج للتجريم وتطبيقات في مجال تحديد حالات سوء استخدام الكمبيوتر:

1. تطبيقات للحماية القانونية لبرامج الكمبيوتر:

بعد استبعاد نظام براءة الاختراع بالنسبة لبرامج الكمبيوتر من نطاق حماية قوانين براءة الاختراع، واللجوء إلى قوانين حقوق المؤلف (المخترع)، بات من الضروري أن تثار مسألة تحديد الحالات التي ينبغي فيها أن يحمي قانون العقوبات «الاستخدام المطلق للمعلومات».

أ) يمكن أن نوضح أهمية الاستخدام المطلق للمعلومات بمثال من ألمانيا للحادث المعروف ببرنامج انكاسو، وطبقاً لوقائع هذا الحادث فقد قام مبرمج يمارس مهنة حرة، بنسخ برنامج لحاسب آلي، يحوى العديد من الأسرار الهامة الخاصة بإحدى المنشآت، وذلك دون الحصول على إذن، وهيأ هذا الحادث الفرصة لأول مرة لمحكمة العدل الفيدرالية لكي تتصدى لمسألة حماية برامج المعلومات عن طريق حق المؤلف، وقد أظهر هذا الحادث أن الاستخدام المطلق للمعلومات لا يمكن إدراكه عن طريق العناصر التقليدية المكونة لجريمة السرقة أو خيانة الأمانة والتي خلقت من أجل حماية الأموال المادية، ولكن هناك حاجة لتشريعات مستقلة تتعلق «بالحقوق الأدبية والملكية الفكرية» وعلى وجه الخصوص «حق المؤلف والمبتكر»، وأيضاً ثمة حاجة لقوانين تتعلق بحماية «الأسرار والعلاقات التجارية»، ويبقى من الضروري – لتقدم ولتطوير تسويق أنظمة تقنية المعلومات – أن نضمن حماية فعالة «لبرامج الحاسب الآلي»[3].

(1) انظر: د. عمر الفاروق الحسيني، المرجع السابق، ص 87 –88

(2) LUCAS Andre : protection of informatics Bases , Research Presented on Kuwait First Conference on Legal and Judicial informatics to Modernize and develop the legal activities, organized by Ministry of Justice, State of Kuwait in cooperation with general secretarial of the Arab league, 15 – 17 Feb. 1999, Abstracts, P. 62.

(3) انظر: Dr. UlrichSieber، تحليل لموضوع: جرائم الكمبيوتر والجرائم الأخرى في مجال تكنولوجيا المعلومات، المرجع السابق، ص 54

وقد أشارت منظمة (OCED) إلى ضرورة أن يضم المشرِّعون إلى قوانين حماية تقنين المعلومات جرائم إعادة الإنتاج غير المرخص لبرنامج الكمبيوتر أو للطبوغرافيا «السمات والملامح الخارجية للأجهزة»[1]. وتتم جريمة النسخ غير المشروع أو الإنتاج غير المشروع للبرامج بعمل نسخة طبق الأصل من البرامج دون مقابل وبدون إذن أو تصريح من المالك، باستخدام أوامر النسخ المختلفة وأجهزته. ويتجاهل الجاني كل التحذيرات المكتوبة غالباً على البرامج بحقوق النسخ وإعادة الإنتاج، مخترقاً بذلك أساليب وقواعد الحماية المقررة قانوناً، وهذه العملية تكبد أصحاب الحقوق المعلوماتية على البرامج خسائر جسيمة[2].

ب) ويلي ذلك أن تضمن القوانين مجالاً من السرية المطلقة للمعلومات المختزنة بالحاسب الآلي، وذلك عن طريق النص على جزاء رادع للولوج غير المسموح به إلى المعلومات الخاصة. وقد أصبحت الحاجة ملحة لمثل هذا النص الجنائي لاسيما بالنسبة للحوادث الألمانية المعروفة بـ hacking أي اختراق شبكات الحاسبات الآلية، ويتوافق طلب ضمان «مجال السرية المطلق» في مجال تقنية المعلومات «ومبدأ حرية الوصول إلى المعلومات» المشار إليه سلفاً، وحيث يقتصر مجال السرية في مجال تقنية المعلومات على البيانات الخاصة والمختزنة في الحاسب الآلي، والتي غالباً ما تكون محمية بواسطة تدبير آمن للمستخدم ، كما يتطلب ذلك صراحة العديد من الأنظمة القانونية[3].

(32) جرائم اختراق شبكات المعلومات (جرائم الفيروسات) :

الفيروسات عبارة عن برامج وضعت من قبل أشخاص على علم متقدم بالبرمجة، واستعملوا فيها التقنيات المتطورة في وضع برامج من خصائصها الانتقال إلى جهاز الكمبيوتر والتكاثر والانتشار فيه، وهي برامج غير مرئية بالطرق العادية، فهي تحتاج للكشف عليها بأسلوب علمي أكثر تطوراً وطرق غير عادية .

اذاً فقضية الفيروس هي أولاً وأخيراً قضية أمنية، فالمعلومات الموجودة داخل الكمبيوتر مثل كل الوثائق الهامة يمكن أن تكون عرضة للعبث والتلاعب والتخريب.

قضية روبرت موريس:

تمكن الشاب الأمريكي «روبرت موريس» 24 سنة من إعطاب 6000 كمبيوتر يوم الأربعاء 2/9/1988، وذلك بتصميمه وإدخال برنامج بطريقة تجعله يقوم بنسخ المرة بعد

(1) انظر: د. محمد محي الدين عوض، المرجع السابق، ص 363. د. كامل السعيد، المرجع السابق.

(2) انظر: د. محمد محي الدين عوض، المرجع السابق، ص 363. د. كامل السعيد، المرجع السابق.

(3) انظر Dr. UlrichSieber ، تحليل لموضوع: جرائم الكمبيوتر والجرائم الأخرى في مجال تكنولوجيا المعلومات، المرجع السابق، ص 54

الأخرى، والتكاثر التلقائي داخل الأجهزة المتفرقة لشبكتين من أكبر شبكات الكمبيوتر في الولايات المتحدة الأمريكية، وهما شبكة «إنترنت Internet» وشبكة «اربانيت Arpanet». وقد تسبب هذا العمل في توقف الأجهزة المذكورة عن العمل لفترة زمنية تجاوزت الساعتين. وبالرغم من أن البرنامج الذي استخدمه (الفيروس) لم يؤد إلى إتلاف شيء من البيانات أو المعلومات التي تستخدمها تلك الأجهزة، إلا أن الذعر الذي سببه ترك آثاراً عامة على صناعة الكمبيوتر، التي أصبحت تواجه مخاطر أمنية جدية، بسبب الفيروسات، والتي تسببت في خسائر تقدر بملايين الدولارات.

وقد تم توجيه الاتهام ل «روبرت موريس» رسمياً أمام سلطات القضاء الأمريكي، إذ حاول المدعي العام إثبات أن العمل الذي قام به المتهم كان متعمداً ومخططاً، مما يمنحه صفة الإجرام الذي يستوجب العقاب بموجب القانون، وأمام المحكمة اعترف «موريس» أنه صمم «برنامج الدودة»، ثم أطلقها بعد ذلك ليرى كم عدد الكمبيوترات التي يمكن أن تصل إليها، لكن خطأ في برمجته تسبب في أن تتضاعف الدودة بسرعة أكبر بكثير مما توقعه. من جهة أخرى، حاول محامي المتهم إثبات أن نية «موريس» من وراء هذا العمل كانت تقتصر على إثبات أن الشبكة غير محصنة التحصين الكافي، وأن الأضرار التي سببها عمله يمكن إسنادها إلى سوء تقدير منه أو خطأ في التصرف، ولا يجب إلصاق صفة الجريمة به.

ومن الطريف، أن أعضاء هيئة المحلفين في هذه القضية قد أقروا أنهم لا يعرفون شيئا عن الكمبيوتر، إلا أن المحكمة أدانت «موريس» بتهمة انتهاك القانون الصادر سنة 1986، والمتعلق بالاحتيال وسوء الاستخدام في مجال الكمبيوتر، والتي تعد جريمة فيدرالية، يعاقب عليها القانون بالسجن لمدة لا تزيد على خمس سنوات أو استبداله بغرامة لا تزيد عن 250 ألف دولار، وقد عوقب المذكور بالسجن لمدة ثلاث سنوات مع وقف التنفيذ وإبقائه تحت المراقبة، وغرامة 10 آلاف دولار، و 400 ساعة عمل في الخدمة المجتمعية.

(33) ثانياً– حماية صحة المعلومات وسلامة انتقالها:

أ) وتبدو أهمية حماية سلامة وانتقال وصحة المعلومات من خلال الحادث المعرف بزيادة المرتب redoublement de salaire ، وطبقا لوقائع هذا الحادث فقد عمل المجرم كمبرمج بإحدى المنشآت الألمانية الكبرى، وقد أدخل بمساعدة برنامج تقني للمعلومات أعده لهذا الغرض خصيصاً، بيانات عن أشخاص وهميين في الذاكرة التي تحوي قائمة بمرتبات العاملين بالمنشأة. وقد سجل المبرمج حسابه الخاص على نفس الحساب الذي سيحول إليه مرتبات الأشخاص الوهميين، ونظراً لأن هذا التلاعب في المرتبات كان قد تم من قبل وبنجاح وبنفس الطريقة في العديد من المنشآت، وكان بالإمكان كشفه من قبل المنشأة المعنية عن طريق طبع وإعادة النظر في محتوى ذاكرة

الحاسب الآلي، فإن المجرم، من أجل منع كشف جريمته عن طريق طابعات الملاحظة– قد قام أولاً بتعديل برنامج دفع الأجور الخاصة بالمنشأة بحيث لا تظهر أيضاً هذه المبالغ في قوائم المراجعة، ثم حصل المبرمج بعد ذلك عن طريق إحداث تعديلات أخرى في برامج الميزانية وكشوف المصاريف على مبالغ تم تجنيبها على ذمة الضريبة قبل أن تسدد للخزينة العامة للدولة. ويشير هذا الحادث إلى أنه على قانون العقوبات– من أجل سلامة وصحة المعلومات – أن يحمي البيانات الخاصة بتقنية المعلومات ضد أي تعديل أو إتلاف غير مسموح به، وذلك عن طريق خلق حماية لنطاق السلامة.

ب) يجب علاوة على ذلك أن تحمى العناصر المكونة لجريمة تزوير الوثائق، ويصدق ذلك على الوثائق الخاصة بتقنية المعلومات المطبوعة، وكذلك استخدام المعلومات المزورة بواسطة المجرم للاعتداء على الأموال التقليدية المحمية، وعلى ذلك، فإنه لا يجب أن يستفيد إجرام تقنية المعلومات من أساليب التعبير الخاصة بالعناصر المكونة لجريمة النصب والتي تفترض صدور أفعال الاحتيال من إنسان بقصد الاحتيال على إنسان آخر.

المحور الثاني – يتعلق بالحماية الجنائية (الموضوعية) للخصوصية:

(34) تحليل المشكلات القانونية المتعلقة بالحماية الجنائية الموضوعية للحق في الخصوصية:

في هذا الجانب تثار مشكلات عديدة تتعلق بالآتي:

1– **النقص والقصور التشريعي:** يغلب على معظم التشريعات الحالية المنظمة للموضوع نقص الأحكام وقصورها عن حماية المصالح الجديرة بالحماية القانونية، كما أنها لا تواكب المستجدات والتحديات المتعلقة بالتجريم والمسؤولية والعقاب على[1]: الأعمال الإرهابية، والأنشطة الإجرامية المنظمة، والأفعال الخطيرة التي تمثل عدواناً على حقوق الإنسان بصفة عامة، وانتهاك حرية الصحافة في الإعلان والنشر، وإفشاء الأسرار، والاعتداء على الحياة الخاصة للأفراد، أو تمثل انتهاكات للخصوصية وحرية الاعتقاد وحرية التعبير وسوء استخدام وسائل الاتصال والإنترنت ومواقع التواصل الاجتماعي في التشهير بالأشخاص والتعريض بهم والمساس بسمعتهم وشرفهم وأعراضهم، والتسويق الإلكتروني للبيانات

(1)The USA Patriot Act was passed in the wake of the terrorist attacks of September 11, 2001. The USA Patriot Act is not perfect; no piece of legislation is. However, it is an effort to fix our structure in a way that is intended to make us all safe. The Act contains sunset provisions and will probably need future amendment
Robert N. Davis. Striking the Balance: National Security vs. Civil Liberties. HEINONLINE. Citation: 29 Brook. J. Int'l L. Page: 175 - 2003-2004.

الشخصية للأفراد وسوء استخدامها، واختراق المواقع الخاصة والتنصت على الأحاديث الشخصية وتسجيلها وإفشائها، وغيرها من الأنشطة الإجرامية الضارة المستحدثة التي تمثل عدواناً خطيراً على الحقوق والمصالح الجديرة بحماية القانون الجنائي، وتحتاج إلى سياسة جنائية وتشريعات فعالة لحمايتها من تلك الاعتداءات.

غياب الرؤية الشاملة لمخاطر تلك الاعتداءات، وعدم وضوح معايير تقدير الحقوق والمصالح، ومدى جدارتها بالحماية الجنائية في إطار سياسة جنائية رشيدة وفعالة لما ينبغي أن يكون عليه التجريم والعقاب حماية وصيانة لتلك الحقوق والمصالح، حتى تكون تلك السياسة إطاراً مرشداً للمشرع في وضع التشريعات الملائمة والفعالة لحمايتها.

مشكلة الصياغة التشريعية للجرائم الإرهابية ولجرائم تقنية المعلومات (الإجرام الإلكتروني) والجرائم الماسة بالأمن القومي والجرائم الماسة بالحق في الخصوصية وحرية التعبير: إن هذه المشكلة تمثل إحدى المعوقات لتأصيل هذه الجرائم وتحديد عناصرها التكوينية وشروط التجريم، وتحديد المصالح المحمية بالتجريم، وتصنيف تلك الجرائم وتأصيلها وفقاً لأسس قانونية محددة تساعد على تفسير أحكامها، وتسهل تطبيقها، وتقييم وتقدير الجزاءات القانونية التي ينبغي أن تتقرر لها في مرحلتي التشريع والتطبيق القضائي[1]. ويجب أن تتخلى فيما يتعلق بالحماية الجنائية للحق في الخصوصية عن حرفية النص الجنائي، وعن العناصر المبهمة المكونة للجريمة والتي نجدها حالياً في كثير من الأنظمة القانونية[2].

مشكلة استخدام المصطلحات المستحدثة في مجال الجرائم المعلوماتية والإلكترونية:

وضعت اتفاقية بودابست الصادرة عن المجلس الأوروبي بعض التعريفات المفيدة في هذا الخصوص:

مادة 1 – تعريفات:

لأغراض هذه الاتفاقية:

1- يقصد ب «منظومة الكمبيوتر» أي جهاز أو مجموعة من الأجهزة المتصلة أو المتعلقة ببعضها البعض، ويقوم واحد منها أو أكثر، تبعاً لبرنامج، بعمل معالجة آلية للبيانات.

(1) شامي الشوا، الغش المعلوماتي كظاهرة إجرامية مستحدث، بحث مقدم إلى المؤتمر السادس للجمعية المصرية للقانون الجنائي، القاهرة، مصر 25-28/10/1993، ص 516. نقلاً عن عبدالفتاح بيومي، مكافحة جرائم الكمبيوتر والإنترنت في القانون العربي النموذجي، جار الفكر العربي، الإسكندرية 2006، مصر، ص 18. د. هدى قشقوش، جرائم الحاسب الإلكتروني في التشريع المقارن، دار النهضة العربية، القاهرة، مصر 1992.

(2) انظر: Dr. UlrichSieber ، تحليل لموضوع: جرائم الكمبيوتر والجرائم الأخرى في مجال تكنولوجيا المعلومات، المرجع السابق، ص 57-56

2- يقصد ب «بيانات الكمبيوتر» أية عمليات عرض للحقائق أو المعلومات أو المفاهيم في قالب مناسب لعملية معالجة داخل منظومة الكمبيوتر، بما في ذلك برنامج مناسب لجعل منظومة كمبيوتر تؤدي وظائفها،

3- يقصد ب «مقدم الخدمة»:

- أي كيان عام أو خاص يقدم لمستخدمي الخدمة الخاصة به القدرة على الاتصال عن طريق منظومة كمبيوتر.

- وأي كيان آخر يقوم بمعالجة أو تخزين بيانات الكمبيوتر نيابة عن خدمة الاتصالات المذكورة أو مستخدمي هذه الخدمة.

4 - يقصد ب «بيانات المرور» أي بيانات كمبيوتر متعلقة باتصال عن طريق منظومة كمبيوتر، والتي تنشأ عن منظومة كمبيوتر تشكل جزءاً في سلسلة الاتصالات، توضح مصدر الاتصال، والواجهة المرسلة إليها، والطريق الذي تسلكه، ووقت وتاريخ وحجم ومدة ونوع الخدمة المذكورة.

وجاء القسم الثاني من الاتفاقية حاملاً عنوان «التدابير الواجب اتخاذها على الصعيد الوطني»، وخصص الباب الأول منه للقانون الجنائي الموضوعي، حيث جاء الفصل الأول منه ليعالج الجرائم التي تمس خصوصية وتجانس وتوافر بيانات الكمبيوتر ومنظوماته.

مادة 2 - الدخول غير مشروع:

تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم الفعل التالي في قانونها الوطني، إذا ما ارتكب عمداً، وبغير حق: الدخول على كامل أو جزء من منظومة كمبيوتر، يجوز لطرف أن يستلزم أن ترتكب الجريمة عن طريق مخالفة التدابير الأمنية، بقصد الحصول على بيانات كمبيوتر أو بقصد آخر غير أمين، أو فيما يتعلق بمنظومة كمبيوتر متصلة بمنظومة كمبيوتر أخرى.

مادة 3 - الاعتراض غير المشروع:

تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم الفعل التالي في قانونها الوطني، إذا ما ارتكب عمداً، وبغير حق: الاعتراض باستخدام وسائل فنية، لعمليات إرسال غير عمومية لبيانات كمبيوتر إلى أو من خلال منظومة كمبيوتر، بما في ذلك ما ينبعث من منظومة كمبيوتر من موجات كهرومغناطيسية تحمل هذه البيانات، يجوز لطرف أن يستلزم أن ترتكب الجريمة عن طريق مخالفة أو بقصد آخر غير أمين، أو فيما يتعلق بمنظومة كمبيوتر متصلة بمنظومة كمبيوتر أخرى .

مادة 4 – التدخل في البيانات:

تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم الأفعال التالية في قانونها الوطني، إذا ما ارتكبت عمداً، وبغير حق: إتلاف أو محو أو إفساد أو تعديل أو تدمير بيانات موجودة على كمبيوتر.

يجوز لطرف أن يحتفظ بحقه في أن يستلزم أن تتسبب الأفعال الموضحة بالفقرة(1) في ضرر جسيم.

مادة 5 – التدخل غير المشروع في المنظومة:

تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم الفعل التالي في قانونها الوطني، إذا ما ارتكب عمداً، وبغير حق: «الإعاقة الخطيرة لعمل منظومة الكمبيوتر عن طريق إدخال أو إرسال أو إتلاف أو محو أو تغير أو تبديل أو تدمير بيانات كمبيوتر».

مادة 6 – إساءة استخدام الأجهزة:

1– تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم الأفعال التالية في قانونها الوطني، إذا ما ارتكبت عمداً، وبغير حق:

2 – الإنتاج أو البيع، والحصول بغرض الاستخدام ، أو الجلب أو التوزيع أو بالأحرى التوفير لجهاز يشمل برنامج كمبيوتر، صمم أو طوع ابتداء، بغرض ارتكاب أي من الجرائم المنصوص عليها أعلاه في المواد من 2–5 ، لكلمة سر خاصة بكمبيوتر، أو كود دخول، أو بيانات مماثلة يمكن بواسطتها الدخول على كامل أو جزء من منظومة كمبيوتر، بغرض ارتكاب أي من الجرائم المنصوص عليها أعلاه في المواد من 2–5 .

3 – الحيازة لأحد الأشياء المشار إليها بالفقرة أ (1) أو (2) بعاليه، بغرض ارتكاب أي من الجرائم المنصوص عليها أعلاه في المواد من 2–5. يجوز لطرف أن يستلزم قانوناً أن تكون حيازة عدد من هذه الأشياء قد تمت لقيام المسئولية الجنائية.

4 – لا يجوز تفسير هذه المادة على أنها ترتب مسؤولية جنائية طالما أن الإنتاج أو البيع أو الحصول بغرض الاستخدام أو الجلب أو التوزيع أو بالأحرى التوفير، أو الحيازة المشار إليها بالفقرة 1 من هذه المادة، ليست بغرض ارتكاب جريمة من الجرائم المنصوص عليها في المواد من 2–5 من هذه الاتفاقية، كما في حالة اختبار منظومة كمبيوتر أو حمايتها بناء على تصريح يبيح ذلك.

5 – يجوز لكل طرف الاحتفاظ بالحق في عدم تطبيق الفقرة(1) من هذه المادة بشرط ألا يكون هذا التحفظ متعلقاً بعمليات بيع أو توزيع أو بالأحرى توفير هذه الأشياء المشار

إليها بالفقرتين أ(1) ، (2) من هذه المادة. وجاء الفصل الثاني ليعالج: الجرائم المتعلقة بالكمبيوتر

مادة –7 جريمة التزوير المتعلقة بالكمبيوتر:

تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم الأفعال التالية في قانونها الوطني، إذا ما ارتكبت عمداً، وبغير حق: إدخال، أو تبديل، أو محو أو تدمير بيانات كمبيوتر، ينتج عنها بيانات غير أصلية بقصد استخدامها أو التعويل عليها في أغراض قانونية كما لو كانت أصلية، بغض النظر عما إذا كانت هذه البيانات مقروءة ومفهومة بشكل مباشر من عدمه. يجوز لطرف أن يشترط وجود نية التدليس، أو قصد غير أمين مشابه، لقيام المسؤولية الجنائية.

مادة –8 جريمة النصب المتعلقة بالكمبيوتر:

تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم الأفعال التالية في قانونها الوطني، إذا ما ارتكبت عمداً، وبغير حق، وتسببت في إلحاق خسارة بملكية شخص آخر عن طريق: أي إدخال أو تبديل أو محو أو تدمير لبيانات كمبيوتر، أي تدخل في وظيفة منظومة كمبيوتر، بقصد احتيالي أو غير أمين للحصول وبدون وجه حق، على منفعة اقتصادية لصالح الشخص ذاته أو لصالح الغير.

وجاء الفصل الثالث ليعالج الجرائم المتعلقة بالمحتوى من خلال المادة التاسعة، وذلك على الشكل التالي:

مادة 9 – الجرائم المتعلقة بالصور الفاضحة للأطفال :

1– تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم الأفعال والسلوكيات التالية في قانونها الوطني، إذا ما ارتكبت عمداً، وبغير حق:

أ) إنتاج صور الأطفال الفاضحة بغرض توزيعها عبر منظومة كمبيوتر.

ب) عرض أو توفير صور الأطفال الفاضحة عبر منظومة كمبيوتر.

ت) توزيع أو بث صور أطفال الفاضحة عبر منظومة كمبيوتر.

ث) الحصول على صور الأطفال الفاضحة عبر منظومة كمبيوتر لصالح الشخص ذاته أو لصالح الغير.

ج) حيازة صور الأطفال الفاضحة داخل منظومة كمبيوتر أو بوسيط تخزين بيانات كمبيوتر.

2- لغرض الفقرة(1) بعالية، تشمل عبارة «صور الأطفال الفاضحة «على المواد الفاضحة التي توضح بالصورة: قاصر منشغل بارتكاب سلوك جنسي صريح، شخص يبدو أنه قاصر منشغل بارتكاب سلوك جنسي صريح، صور واقعية تظهر قاصراً منشغلاً بارتكاب سلوك جنسي صريح .

3- لغرض الفقرة(2) بعالية، يشمل تعبير «قاصر» كل من هو دون سن الثامنة عشرة. على أنه يجوز لأي طرف أن يشترط حداً عمرياً أقل، بما لا يقل عن سن السادسة عشرة .

4- يجوز لكل طرف أن يحتفظ بالحق في عدم تطبيق البندين «د» ، «هـ» من الفقرة (1)والبندين «ب» ، «ج» من الفقرة (2) كلياً أو جزئياً .

وجاء الفصل الرابع ليعالج: الجرائم المتعلقة بالانتهاكات الخاصة بحقوق الملكية الفكرية والحقوق المجاورة.

مادة 10- الجرائم المتعلقة بالانتهاكات الخاصة بحقوق الملكية الفكرية والحقوق المتعلقة بها:

تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم الفعل التالي في قانونها الوطني: انتهاك حقوق الملكية الفكرية، بحسب تعريفها وفقاً للقانون الخاص بهذا الطرف، وتبعاً لالتزاماتها بموجب وثيقة باريس الصادرة في 24 يوليو 1971، المنقحة لاتفاقية برن الخاصة بحماية الأعمال الأدبية والفنية، والاتفاقية الخاصة بالنواحي التجارية لحقوق الملكية الفكرية، ومعاهدة المنظمة العالمية للملكية الفكرية الخاصة بحقوق الملكية الفكرية، باستثناء أية حقوق معنوية تم التشاور بشأنها من خلال هذه الاتفاقيات، عندما ترتكب هذه الأفعال عمدا، وعلى نطاق تجاري، وبواسطة منظومة كمبيوتر.

تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم الفعل التالي في قانونها الوطني: انتهاك الحقوق المجاورة بحسب تعريفها وفقاً للقانون الخاص بهذا الطرف، وتبعاً لالتزاماتها بموجب الاتفاقية الدولية لحماية ممثلي ومنتجي الفونوغراف والهيئات الإذاعية (اتفاقية روما) والاتفاقية الخاصة بالنواحي التجارية لحقوق الملكية الفكرية، ومعاهدة المنظمة العالمية للملكية الفكرية الخاصة بالأعمال الإبداعية، والتمثيل، وأجهزة الفونوغراف، باستثناء أية حقوق معنوية تم التشاور بشأنها من خلال هذه الاتفاقيات، عندما ترتكب هذه الأفعال عمداً، وعلى نطاق تجاري، وبواسطة منظومة كمبيوتر.

يجوز لطرف الاحتفاظ بالحق في عدم فرض المسؤولية الجنائية بموجب الفقرتين 2،1 من هذه المادة في ظروف محددة، بشرط أن تتوافر وسائل علاجية فعالة أخرى، وألا يخل هذا التحفظ بالالتزامات الدولية للطرف بموجب الاتفاقيات الدولية المشار إليها بالفقرتين 2،1 من هذه المادة.

أما الفصل الخامس فينظِّم: (الأحكام العامة) للمسؤولية الإضافية (عن الشروع، والاشتراك في الجريمة) والعقوبات والتدابير.

مادة 11 – الشروع، والمساعدة، والتحريض:

تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم الأفعال والسلوكيات التالية في قانونها الوطني: إذا ما ارتكبت عمداً المساعدة، أو التحريض على ارتكاب أي من الجرائم المنصوص عليها في المواد من 2–10 من هذه الاتفاقية، وذلك بقصد ارتكاب مثل هذه الجريمة.

تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم الأفعال والسلوكيات التالية في قانونها الوطني: إذا ما ارتكبت عمداً: الشروع في ارتكاب أية جريمة من الجرائم المنصوص عليها في المواد من 3 وحتى 1–5،7،8،9 (أ)، (ج) من هذه الاتفاقية.

يجوز لكل طرف الاحتفاظ بالحق في عدم تطبيق الفقرة 2 من هذه المادة كلياً أو جزئياً.

مادة 12 – مسؤولية الهيئات الاعتبارية:

1– تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى، وذلك لإرساء مسؤولية الشخصيات الاعتبارية عن الجرائم المنصوص عليها في هذه الاتفاقية، والتي ترتكب لمصلحتها بمعرفة شخص طبيعي، سواء باشر ذلك بصورة فردية أو بصفته جزءاً من جهاز تابع للشخص الاعتباري، ويتبوأ منصباً قيادياً داخله، وذلك بموجب:

– سلطة تمثيل الشخص الاعتباري.

– تفويض قانوني باتخاذ القرارات نيابة عن الشخص الاعتباري.

– سلطة ممارسة التحكم داخل الشخص الاعتباري.

2– بالإضافة إلى الحالات المذكورة بالفقرة (1) من هذه المادة، يعتمد كل طرف الإجراءات الضرورية لإرساء المسؤولية الجنائية للشخص الاعتباري، وذلك في حالة ما إذا تسبب عدم الإشراف أو التحكم من قبل الشخص الطبيعي المشار إليه بالفقرة (1) في جعل ارتكاب جريمة منصوص عليها وفقاً لهذه الاتفاقية ممكناً لمصلحة الشخص الاعتباري عن طريق شخص طبيعي يعمل تحت سلطته.

3– وفقاً للمبادئ القانونية الخاصة بالطرف، يجوز أن تكون المسؤولية القانونية للشخص الاعتباري جنائية أو مدنية أو إدارية.

4- لا تؤثر هذه المسؤولية على المسؤولية الجنائية للأشخاص الطبيعيين الذين ارتكبوا الجريمة.

مادة 13 - العقوبات والإجراءات:

تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى للتأكد من أن الجرائم المنصوص عليها في المواد من 2-11 معاقب عليها بعقوبات فعالة ومتناسبة ورادعة، بما في ذلك تقييد الحرية.

يلتزم كل طرف بالتأكد من أن الأشخاص الاعتبارية الذين يقعون تحت طائلة المسؤولية وفقا للمادة 12 يخضعون لعقوبات أو تدابير فعالة ومتناسبة ورادعة، سواء أكانت عقوبات أم تدابير جنائية أم غير جنائية، بما في ذلك العقوبات المالية.

المبحث الثالث
الحماية الجنائية الإجرائية للحق في المعلومات والخصوصية وسلامة الاتصالات والإنترنت

الفرع الأول
تحليل المشكلات المتعلقة بالقانون الجنائي الإجرائي

(35) مشكلة إهدار مبادئ الإجراءات الجنائية:

تعد المشاكل الناجمة عن تطبيق قانون الإجراءات الجنائية من الأهمية بمكان على النحو الذي يستدعى تخصيص دراسة مستقلة لها، وحسبنا أن نشير- في حدود مقتضيات هذه الدراسة- إلى المشكلات الإجرائية الآتية:

1- إن وضع القوانين الإجرائية هو وفاء بالتزام طبيعي يقع على عاتق كل دولة لتحقيق الأمن، وإقامة العدل، وصيانة الحريات، وهي الدعامات الأساسية للمجتمع. والقانون الجنائي الإجرائي هو الآلية القانونية الوحيدة لتطبيق التشريعات الجنائية الأخرى. وينبغي أن يقرر هذا القانون الضمانات الأساسية لحقوق الشخصية وصيانة حق المتهم والأفراد الآخرين في الخصوصية من الانتهاك دون سند أو مقتضى، ويهم هذا القانون كل المواطنين أبرياء ومذنبين على السواء، إذ تتحدد من خلال الإجراءات الجنائية

مصير أي سياسة جنائية لمكافحة الجريمة، ويعتبر هذا القانون، بما يمثله من سلطة على الأفراد، هو أداة الدولة في ممارسة سيادتها داخلياً لتحقيق أمن المجتمع واستقراره وتوفير الطمأنينة لأفراده، ولذلك يعد قانون الإجراءات الجزائية في مجتمع ما، هو أخطر ما تمارسه الدولة باسم المجتمع ولحسابه في مواجهة الفرد ككائن اجتماعي، وهو ما يعبر في دولة ما عن الصورة الدقيقة لكفالة الحقوق والحريات فيها، وهو يتطور باستمرار ويتأثر بكل ما يصاحب الحضارة الإنسانية من تطور على مر السنين[1].

ويتأسس هذا القانون على مبادئ الشرعية الإجرائية (المتمثلة في: 1- القانون أصل الإجراءات 2 – أصل البراءة في الإنسان 3 – الرقابة القضائية على الإجراءات الجنائية وتفسير وتطبيق القوانين الإجرائية تطبيقاً سليماً بمعرفة الأجهزة الأمنية وأجهزة العدالة مع الالتزام بالخضوع إلى المبادئ والمعايير الأساسية للحقوق والحريات الشخصية).

2 – مشكلة تجاوز أهداف قانون الإجراءات الجزائية:

إن غاية قانون الإجراءات الجزائية هي حماية المجتمع من مخاطر الإجرام بكشف حقيقة الجريمة ومعرفة مرتكبيها، تمهيداً لملاحقتهم قضائياً لإنزال العقاب المقرر في قانون الجزاء بهم، وهي ذات الغاية التي يرمي إليها قانون الجزاء بتحديد الأفعال التي تعد جرائم وتقرير العقوبات لها، وذلك على اعتبار أن قانون الإجراءات الجزائية هو السبيل الوحيد لتطبيق قانون الجزاء، ومن ثم يتجه القانونان صوب غاية واحدة[2].

ويهدف قانون الإجراءات- وهو في سبيله لتحقيق تلك الغاية- إلى كشف حقيقة الجرائم ومرتكبيها تمهيداً لمحاكمتهم، وكفالة حقوق المتهم في الدفاع عن نفسه، وضمان الحقوق والحريات الشخصية للأفراد الآخرين أثناء ممارسة السلطات الأمنية والشرطية لوظيفتها المنعية الوقائية، وممارسة أجهزة العدالة الجنائية لإجراءات وسلطات كشف الجرائم وتحقيق أدلتها ومحاكمة مرتكبيها، في شأن جريمة ارتكبت بالفعل، مع عدم الإخلال بالحريات الشخصية للمتهم أو الأفراد دون مقتضى أو سند من القانون، فمن الخطأ أن ينظر إلى قانون الإجراءات الجنائية على أنه وضع للمجرمين دون غيرهم، إذ كثيراً ما يؤخذ بريء بشبهات تدفعه إلى قفص الاتهام. كما أن المجتمع ينشد الحقيقة، فلا يرغب في إفلات مجرم

(1) انظر: د. أحمد فتحي سرور، الوسيط في قانون الإجراءات الجزائية، دار النهضة العربية، الطبعة السابعة 1993، القاهرة، مصر، ص 20. د. عبد الأحد جمال الدين، في الشرعية الجنائية، بحث منشور بمجلة العلوم القانونية والاقتصادية، السنة 16، العدد الثاني، يوليو 1974، ص 359.

(2) انظر: د. محمود محمود مصطفى، شرح قانون الإجراءات الجزائية، الطبعة الحادية عشرة 1976، بند 6، ص 7. د. محمود نجيب حسني، بند 4، ص4

من العقاب، و لكن يثيره الحكم ظلماً على بريء[1]. قال تعالى: **(ومن يكسب خطيئة أو إثماً ثم يرمي به بريئاً فقد احتمل بهتاناً وإثماً مبيناً)**[2].

لذلك فإن القوانين الإجرائية المتوازنة لا توجد إلا لدى الشعوب المتمدنة التي تسير في تشريعاتها الإجرائية على هدى العدل والمنطق واحترام الحريات الفردية، وليس على أساس التحكم والاندفاع ورد الفعل الغريزي كما كان يجرى في المجتمعات البدائية[3].

وحتى يقوم هذا القانون بوظيفته ويصل إلى غايته، ينبغي أن يحقق التوازن المنشود بين مقتضيات كشف الجرائم ومرتكبيها وملاحقتهم، وضمان وكفالة الحريات وحقوق الشخصية وبصفة خاصة، الضمانات الأساسية للحق في الخصوصية للمتهمين وباقي الأفراد على حد سواء.

(36) وقد بات من الواضح في مجال الإجـراءات الجنائية المتعلقة بجرائم تقنية المعلومات الآتي:

أولاً- وجوب تأسيس قانون الإجراءات الجنائية على مبادئ الشرعية القانونية:

يجب أن يبقى قانون الإجراءات الجنائية على الرغم من هذه الاتجاهات العامة بمثابة الوثيقة الأساسية للمجرم التي تحمي المبادئ الأساسية المعترف بها في قانون الإجراءات كقرينة البراءة وإطلاق الاتهام الذاتي إزاء المخاطر المستحدثة والتي تنشأ من تقنية المعلومات. ولا يهدد فقط الحريات الفردية للمواطن التفسير عن طريق القياس أو التوسع في أذونات التدخل في قانون الإجراءات الجنائية، ولكن يؤثر ذلك أيضاً على مبدأ الفصل بين السلطات والذي بمقتضاه يستأثر البرلمان بتقرير قيود الحريات المستحدثة في الدعوى الجنائية[4].

ثانياً- وجوب أن تكون المحاكمة عادلة وناجحة:

ومن جهة الدعوى الجنائية، فإنها يجب أن تضمن محاكمة ناجحة في مجال تقنية المعلومات، لأن انتشار وتأثير هذه التقنية ينتشر بدون توقف في كل من الأوساط الاجتماعية والاقتصادية.

---

(1) تؤكد محكمة النقض المصرية هذا المعنى في قولها: «من المقرر أنه لا يضير العدالة إفلات مجرم من العقاب، بقدر ما يضيرها الافتئات على حريات الناس بدون وجه حق»، نقض 21/10/1958، مجموعة أحكام النقض، س 9، رقم 206، مجموعة د. المرصفاوي، ص 839، نقض 4/9/1973، س 24، رقم 105، ص 506. وأنظر د. محمود محمود مصطفى، مرجع سابق، ص 21.

(2) الخطيئة: الذنب الذي يحتمل الخطأ أو العمد، والإثم: المعصية التي لا تأتي إلا عن عمد (أوضح التفاسير لابن الخطيب، ص 213).

(3) د. أحمد فتحي سرور، الوسيط في قانون الإجراءات الجزائية، دار النهضة العربية، الطبعة السابعة 1993، القاهرة، مصر، ص 20. د. سعيد عبداللطيف إسماعيل، شرح قانون الإجراءات الجزائية الكويتي، مطبوعات أكاديمية سعد العبدالله للعلوم الأمنية، الكويت 2005، ص 27

(4) انظر: Dr. UlrichSieber ، تحليل لموضوع: جرائم الكمبيوتر والجرائم الأخرى في مجال تكنولوجيا المعلومات، المرجع السابق، ص 57

ثالثاً– يلزم لمجتمع المعلومات أن ينشئ قواعد قانونية حديثة، بحيث تضع معلومات معينة تحت تصرف الدولة والفرد، حيث نجد اليوم محترفي شبكات الحاسبات الآلية ومرتكبي الجرائم الاقتصادية وأيضاً تجار الأسلحة والمواد المخدرة والمنظمات الإرهابية، وهم يقومون بتخزين معلوماتهم في أنظمة تقنية المعلومات، وعلى نحو متطور. وتصطدم الإدارة العقابية بهذا التكنيك لتخزين المعلومات وهي التي تسعى إلى أدلة الإثبات، وتصادف صعوبات عندما يتعلق الأمر بتخزين بيانات في الخارج بواسطة شبكة الاتصالات البعدية، ويصعب حتى هذه اللحظة في غالبية الأنظمة القانونية أن نحدد إلى أي مدى تكفي الأساليب التقليدية للتفسير في قانون الإجراءات الجنائية من أجل تحقيقات ناجحة في مجال تقنية المعلومات[1].

الفرع الثاني
دور قانون الإجراءات الجنائية في مكافحة جرائم تقنية المعلومات وانتهاك الخصوصية

(37) إشكالية تعدد الاختصاص القضائي في مواجهة الأنشطة الجنائية عبر شبكة الإنترنت[2]:

يمكن التعبير ببساطة عن مشكلات تنظيم شبكة الإنترنت في ثلاث نقاط أساسية:

أولاً– أنها تسمح بأنشطة جديدة مثل البريد الإلكتروني والاطلاع على المعلومات...الخ، وهذه الأنشطة ربما تشكل جرائم.

ثانياً– أن نظام الإنترنت يعتبر نظاماً موزعاً يتعدى الحدود الجغرافية والقضائية، فقد يقع تنظيم الاختصاص القضائي بالنسبة لهذه الأنشطة الإجرامية ضمن اختصاص سلطتين قضائيتين محليتين أو أكثر، وبالتالي يصعب اختيار الاختصاص القضائي المناسب.

ثالثاً– أن الحاجة الحتمية لاختيار اختصاص قضائي سوف تعني أن القيم والمعايير المتعلقة

(1) أنظر: Dr. UlrichSieber ، تحليل لموضوع: جرائم الكمبيوتر والجرائم الأخرى في مجال تكنولوجيا المعلومات، المرجع السابق، ص 57

(2) Jones Richard, Legal Pluralism and Facing Criminal Acts of Internet, research presented on Kuwait, First conference in Legal and Judicial informatics, to modernize and develop the legal activities, organized by Ministry of Justice, State of Kuwait in cooperation with general secretarial of the Arabe League, 15-17 feb.1999, Abstracts, p 62.

بالتجريم التي يجب فرضها على النشاط سوف تكون نفس قيم النظام القانوني الذي ينتمي إليه الاختصاص القضائي المحلي، وهي قيم ومعايير ربما تكون مختلفة عن تلك التي تنتمي إلى نظام قانوني وقضائي آخر. وتصادف الباحثين القانونيين في مختلف الدول مشكلة اختيار الاختصاص القضائي الذي تنعقد له الأولوية، وهل ينبغي أن يبقى الاختصاص القضائي بجرائم تقنية المعلومات متفرداً أي منعقداً لجهة الاختصاص المحلية أم ينبغي البحث عن معالجة قانونية ضد تعددية المعالجة القضائية Pluralistic Approaches.

وقد ثبت بالدليل من القضايا الحديثة في الولايات المتحدة أن القضاة سوف يستخدمون تقنيات مشابهة لفرض القيم والمعايير الغربية على أنشطة شبكة الإنترنت، والمفهوم أن التعددية القانونية Legal Pluralism ليست معترفاً بها في الأنظمة القانونية الغربية، ومن ثم يتجه البحث في هذا المجال لدراسة ما إذا كانت هناك إستراتيجية أكثر تعددية يمكنها توفير طريقة معالجة أكثر قبولاً للتعامل مع تلك النزاعات على شبكة الإنترنت. وقد جاء الباب الثالث من الاتفاقية المتعلقة بالجريمة الإلكترونية بودابست 23/ 11/ 2001، مجموعة المعاهدات الأوربية بمجلس أوروبا رقم 185 تحت عنوان الاختصاص القضائي[1]:

وتنص المادة 22 من الاتفاقية على أن:

1- يعتمد كل طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى، وذلك لإقرار الاختصاص(سريان القانون الوطني) بشأن أي جريمة تنص عليها المواد من (2) إلى (11) من هذه الاتفاقية، وذلك عندما ترتكب الجريمة:

في إقليمه أو على متن إحدى السفن ترفع علم ذلك الطرف، أو على متن إحدى الطائرات المسجلة بموجب قوانين ذلك الطرف، أو من جانب أحد مواطنيه (مبدأ الشخصية الإيجابية)، إذا كانت الجريمة معاقباً عليها بموجب القانون الجنائي مكان ارتكابها، أو في حالة ارتكاب الجريمة خارج الاختصاص القضائي الإقليمي لأية دولة.

2- يجوز لكل طرف الاحتفاظ بالحق في عدم التطبيق أو التطبيق فقط في حالات أو بشروط معينة، قواعد الاختصاص القضائي المنصوص عليها في الفقرات من 1(ب) إلى 1(د) من هذه المادة أو أي جزء منها.

3- يعتمد كل طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى، وذلك لإقرار (سريان القانون الوطني) والاختصاص القضائي بشأن الجرائم المشار إليها في المادة (24) –

(1) انظر: د. إيهاب السنباطي، الترجمة الجديدة والكاملة للاتفاقية المتعلقة بالجريمة الإلكترونية (بودابست 2001)، والبروتوكول الملحق بها، دار النهضة العربية، 2009–2008.

الفقرة (1) من هذه الاتفاقية، في الحالات التي يكون فيها الجاني المزعوم موجوداً في إقليمه، ولا يقوم بتسليمه أو تسليمها لطرف آخر على سند وحيد من جنسيته أو جنسيتها، وذلك بعد طلب للتسليم .

4- لا تستبعد هذه الاتفاقية أي اختصاص جنائي يمارسه أحد الأطراف وفقاً لقانونه الوطني (مبدأ العينية – مبدأ العالمية).

5- في حالة مطالبة أكثر من طرف من الأطراف بالاختصاص القضائي بشأن جريمة ما تقرها هذه الاتفاقية، يقوم الأطراف المعنيون، متى كان ذلك ملائماً، بالتشاور بغرض تحديد الاختصاص القضائي الأكثر ملاءمة للمحاكمة.

(38) مدى جواز مباشرة إجراءات جمع الأدلة خارج إقليم الدولة:

نظراً للطبيعة العالمية لبعض جرائم تقنية المعلومات[1]، حيث ترتكب العديد من هذه الجرائم عبر شبكات الإنترنت وشبكات الاتصال السريع كجرائم التجسس واختراق شبكات المعلومات والتنصت، وإعاقة سلامة توصيل المعلومات والاستيلاء على الأموال عبر نظام التحويل الإلكتروني للأموال ...إلخ، يثور التساؤل عن مدى جواز مباشرة إجراءات جمع الأدلة وتحقيقها خارج إقليم الدولة؟

لقد انعكس الخلاف بين النظم الإجرائية الوضعية على نطاق مبدأ إقليمية قانون الإجراءات الجنائية وفقا للنظام الاتهامي المطبق في القوانين الأنجلو أمريكية، ذهب الفقه إلى السماح بالحصول على الأدلة التي تؤيد الاتهام أو تنفيه، ولو كان ذلك خارج إقليم الدولة، طالما أن أطراف الدعوى لا يحتاجون في سبيل جمع الدليل إلى استخدام أساليب القسر، فهم لا يقومون بعمل من أعمال السلطة. ويذهب الفقه الأنجلو أمريكي أيضاً إلى السماح بإجراء التحقيق خارج إقليم الدولة، طالما أن السلطة تنزل في هذا الصدد منزلة الخصوم طبقاً للنظام الاتهامي.

هذا بخلاف الحال في الدول الأوروبية حيث يسود نظام التحري والتنقيب والنظام المختلط فلا يجوز مطلقاً جمع الأدلة خارج إقليم الدولة، طالما أن الإجراءات الجنائية تباشرها سلطة التحقيق باسم الدولة، وهي إجراءات تتسم بالقهر بحكم طبيعتها[2].

وفي هذا المجال فإن التوافق بين مختلف سلطات التدخل الوطنية سيكون هاماً من أجل تيسير طلب المساعدة القانونية الوطنية، لأنه قد تلتمس إحدى الدول المساعدة القضائية من دول أخرى، ويلزم هذا التوافق حتى يمكن لهذه الأخيرة أن تباشر إجراءات تقديم تلك

(1) انظر: د. عمر الفاروق، المرجع السابق، ص 459 وما بعدها.

(2) انظر: د. أحمد فتحي سرور، المرجع السابق، ص 81

المساعدات، التي تكون مقبولة ومتاحة وفقاً لقوانينها الخاصة، وفي التجمعات الثقافية والاقتصادية كما هو الحال في أوروبا، فإنّ التوافق على المدى البعيد على أساليب القسر الإجرائية يمكن أن يسهل الإجراءات أمام قاضي أوروبا في المستقبل، أو لأي قاض دولي مماثل ومعترف به، والذي سيكون له نفس القيمة التي تكون للسلطة الوطنية[1].

ولكن خارج هذه التجمعات يتطلب الأمر عند ممارسة عمل من الأعمال المتعلقة بالبحث عن الأدلة وتحقيقها اللجوء إلى جهاز الدولة الأجنبية للقيام بهذا العمل في نطاق التعاون الدولي، ولا يكفي لذلك مجرد السماح لهم بممارسة اختصاصاتهم داخل إقليم الدولة الأجنبية.

وتنظم العلاقات الدولية كيفية ممارسة الإجراءات الجنائية خارج إقليم الدولة، وتحدد الاتفاقيات الدولية كيفية تقديم الدولة الأجنبية للمساعدة القضائية بناء على طلب الحكومة المعنية، وتنظم هذه الاتفاقيات الدولية الإنابة القضائية للدولة الأجنبية عن الدولة الوطنية في ممارسة الإجراءات الجنائية المتعلقة بالدولة الأخيرة، وتتعَلَّق هذه الإنابة إما بإجراء المعاينات المادية أو سماع الشهود أو القيام بالإعلانات الرسمية لأشخاص يقيمون على أرض الدولة الأجنبية، أو البحث عن الوثائق لوضعها تحت يد القضاء، وهناك بعض الاتفاقيات تنص أيضاً على إمكان إحضار بعض الأشخاص إلى الدولة الوطنية لسماعهم بواسطة المحكمة المختصة مع ضمان عودتهم في أقرب وقت[2].

(39)- الإصلاحات التشريعية الإجرائية الحديثة:

في مختلف الدول الآن تسود موجة لإصلاح التشريعات الإجرائية لكي تواكب المتغيرات والتطورات المطردة في جرائم تقنية المعلومات، والتعديلات المتلاحقة في نصوص قانون العقوبات، في شأنها وتفعيل الإجراءات الجنائية وخاصة إجراءات الإثبات في مجال تقنية المعلومات. وقد صدرت في المملكة المتحدة قوانين إثبات خاصة بجرائم الكمبيوتر، وأجريت عليها المزيد من التعديلات حتى تواكب التطورات المطردة في أساليب ارتكاب هذه النوعية من الجرائم[3].

(1) أولريش شيبيه، المرجع السابق، ص 60

(2) وهذه الاتفاقيات إما أن تكون ثنائية أو متعددة الأطراف. وينبغي تشجيع مثل هذه الاتفاقيات وإبرامها على غرار الاتفاقية الأوروبية للتعاون القضائي المبرمة سنة 1959. انظر: د. أحمد فتحي سرور، المرجع السابق، ص 80-79.

(3) Tapper Coline F., Evedence and Computer, Paper presented on Kuwait first conference in Legal and Judicial informatics, to modernize and develop the legal activities, organized by Ministry of Justice, State of Kuwait in cooperation with general secretarial of the Arabe League, 15-17 feb.1999, Abstracts, p 62.

وتميل الإصلاحات الإجرائية الحديثة إلى دمج جميع الابتكارات والتطبيقات الناتجة عن تقنية المعلومات. وتستجيب النصوص المستحدثة لاحتياجات الشرطة القضائية وإستقلالها بالنسبة للتحقيقات في هذا المجال. ولقد بات من الواضح الآن في مجال الإجراءات الجنائية أنه يلزم لمجتمع المعلومات، وضع قواعد قانونية حديثة تنظم استخدام المعلومات، وتمكن الدول والأفراد على السواء من الحصول على المعلومات، حتى تكون تحت تصرفهم عندما يريدون الحصول عليها بطريق قانوني، ذلك أن من حق الأفراد الوصول إلى المعلومات في نطاق الشرعية، كما أن للدولة أن تحصل على المعلومات لأغراض متعددة، ومن ذلك حق الدولة في كشف الحقيقة في جرائم تقنية المعلومات. غير أننا نجد اليوم محترفي استخدام شبكات الحاسبات الآلية جنائياً ومرتكبي الجرائم الاقتصادية وأيضاً الذين يباشرون الاتجار غير المشروع في الأسلحة والمخدرات... كل أولئك يقومون بتخزين معلوماتهم في أنظمة تقنية المعلومات عالية الكفاءة، وعلى نحو متطور باطراد، ومن ثم تصطدم أجهزة العدالة الجنائية بهذا «التكنيك المعلوماتي» وهي تسعى إلى ضبط الجرائم، وجمع أدلة الإثبات، وتصادف صعوبات كثيرة عندما يتعلق الأمر بمعلومات أو بيانات تم تخزينها في الخارج بواسطة شبكة الاتصالات عن بعدTelecommunication ويصعب، حتى هذه اللحظة، في غالبية الأنظمة القانونية أن نحدد إلى أي مدى تكفي الأساليب التقليدية للتفسير في قانون الإجراءات الجنائية، لضبط هذه المعلومات بحثاً عن الأدلة وتحقيقها من أجل تحقيقات ناجحة في مجال تقنية المعلومات، وكذا طرق تقديمها أمام القضاء وتحقيقها بمعرفته وتقديرها بما يساهم في توفير عقيدة صحيحة لدى القاضي[1].

ومن هذه الأساليب على سبيل المثال التحفظ على المعلومات والتفتيش في الحصول على الأدلة وإلزام الشاهد باسترجاع وكتابة المعلومات، والحق في مراقبة وتسجيل البيانات المنقولة بواسطة أنظمة الاتصال عن بعد، و جمعها وتخزينها، وضم المعلومات الاسمية إلى الدعوى الجنائية. ومن ثم يكون من الملائم إجراء أبحاث أكثر دقة لبيان مدى توافق تدابير إجراءات التفسير الموجود حالياً في قوانين الإجراءات الجنائية الوطنية، مع أغراض كشف الحقيقة لبيان مدى كفايتها لأغراض الاستدلال والتحقيق والمحاكمة في مجال جرائم تقنية المعلومات، خاصة أغراض الإثبات وطرح البدائل الأكثر ملاءمة لتحقيق هذه الأغراض مع تحقيق التوازن بين مصلحة الدولة في الوصول إلى الحقيقة، والحريات الفردية للمواطنين بهدف تحقيق محاكمة ناجحة وعادلة في مجال جرائم تقنية المعلومات[2].

وتنص المادة 14 من اتفاقية بودابست على أن:

(1) انظر: Dr. UlrichSieber، المرجع السابق، ص 57

(2) انظر: Dr. UlrichSieber، المرجع السابق، ص 58

«نطاق المواد الإجرائية:

1- تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لإقرار الصلاحيات والإجراءات الواردة بهذا القسم، وذلك لأغراض تحقيقات وإجراءات جنائية محددة .

2- فيما عدا ما ورد تحديداً بالمادة 21 ، يطبق كل طرف الصلاحيات والإجراءات المشار إليها بالفقرة (1) من هذه المادة على: الجرائم المنصوص عليها في المواد من 2 – 11 من هذه الاتفاقية، الجرائم الأخرى التي يتم ارتكابها بواسطة منظومة كمبيوتر، وجمع الأدلة الإلكترونية الخاصة بجريمة ما.

3- أ. يجوز لكل طرف أن يحتفظ بالحق في تطبيق الإجراءات المشار إليها بالمادة 20 على الجرائم أو أصناف الجرائم المحددة حصراً بالتحفظ، بشرط ألا تكون مرتبة هذه الجرائم أو أصناف الجرائم أغلظ وأشد من مرتبة الجرائم التي تطبق عليها الإجراءات المشار إليها بالمادة 21. على كل طرف النظر في أمر تقييد مثل هذا التحفظ حتى يمكن تطبيق الإجراء المشار إليه بالمادة 20 على أوسع نطاق.

4- في حالة ما إذا تعذر على طرف، بسبب قيود موجودة في تشريعاته السارية وقت التصديق على الاتفاقية الحالية، تطبيق الإجراءات المشار إليها بالمادتين 20،21 على اتصالات منقولة عبر منظومة كمبيوتر خاصة بمقدم خدمة، والتي منظومتها: يجري تشغيلها لصالح مجموعة مغلقة من المستخدمين، ولا تستخدم شبكات اتصال عمومية، وغير متصلة بأية منظومة كمبيوتر أخرى، سواء عامة أو خاصة، فإنه يجوز لهذا الطرف الاحتفاظ بالحق في عدم تطبيق الإجراءات المذكورة على مثل هذه الاتصالات. على كل طرف النظر في أمر تقييد مثل هذا التحفظ حتى يمكن تطبيق الإجراءات المشار إليها بالمادتين 20 – 21 على أوسع نطاق».

ومن جهة أخرى، يجب أن يبقى قانون الإجراءات الجنائية على الرغم من هذه الاتجاهات العامة المستحدثة، بمثابة الوثيقة الأساسية لحماية حقوق الإنسان والحريات، لاسيما بالنسبة للمتهم، حيث يجب أن تؤكد على احترام المبادئ الأساسية المعترف بها في قانون الإجراءات الجنائية، كقرينة البراءة، وأن يكون التشريع مصدر الإجراءات، وتأكيد الرقابة القضائية على ما تمارسه سلطات الاستدلال والتحقيق من إجراءات[1].

(1) Merle Roger et Vitu Andre, Traite de Droit Criminel, Procedure Penal, Edition Cujas, Deuxieme Edition, Paris 1973,p128 etc. Levasseuer George et Chavanne Albert, Edition Sirey, 6ieme Edition, Paris 1980, p 110 etc..

وانظر: د. محمود محمود مصطفى، شرح قانون الإجراءات الجنائية، مطبعة جامعة القاهرة والكتاب الجامعي، الطبعة الحادية عشرة، 1976، ص 414 وما بعدها. د. محمود نجيب حسني، شرح قانون الإجراءات الجنائية، دار النهضة العربية، الطبعة الثانية، 1988، ص 4-3 وما بعدهما.

وتنص المادة 15 من اتفاقية بودابست على أن:

«الشروط والضمانات:

على كل طرف أن يتأكد من أن إقامة، وتنفيذ، وتطبيق الصلاحيات والإجراءات الواردة بهذا القسم تخضع للضمانات والشروط المنصوص عليها في قانونه الوطني، الذي يتعين أن يوفر الحماية الكافية لحقوق الإنسان والحريات، بما في ذلك الحقوق الناشئة عن التزاماته بموجب اتفاقية مجلس أوروبا لعام 1950 الخاصة بحماية حقوق الإنسان والحريات الأساسية، والعهد الدولي للأمم المتحدة لعام 1966 الخاص بالحقوق المدنية والسياسية، وغيرها من الآليات الدولية الأخرى المنطبقة والخاصة بحقوق الإنسان، والتي تتضمن مبدأ الملاءمة.

تشمل هذه الشروط والضمانات، كلما كان الأمر ملائماً بالنسبة لطبيعة الإجراءات أو الصلاحيات ذات الصلة، الإشراف من قبل القضاء أو بواسطة إشراف محايد، ووضع مبررات للتطبيق وحدود ومجال ومدة هذا الإجراء أو الصلاحية. في حدود الصالح العام وبخاصة الإدارة السليمة للعدالة، يقوم كل طرف بدراسة تأثير الصلاحيات والإجراءات في هذا القسم على الحقوق والمسؤوليات، والمصالح المشروعة، والمصالح المشروعة للغير.

وقد جاء الفصل الثاني: «سرعة التحفظ على بيانات الكمبيوتر المخزونة»

والقول بغير هذا، إزاء المخاطر والأضرار التي تنجم عن جرائم تقنية المعلومات، بإطلاق الاتهام دون قيود تنظمه، أو التوسع في سلطات التحقيق التي تخول التدخل للحصول على المعلومات أو الترخيص بذلك لسلطات الاستدلال، أو التوسع في تفسير الإجراءات المقررة، لتلائم المستجدات، .....، فإن كل ذلك، لا يهدد فقط حقوق وحريات الأفراد بل أيضاً يخل بمبدأ الفصل بين السلطات والوظائف القضائية، والذي بمقتضاه يستأثر المشرع بسلطة فرض القيود المستحدثة على الحريات الفردية بمناسبة تحريك ومباشرة الدعوى الجنائية والفصل فيها[1].

(40) وجود مشاكل خاصة ومستحدثة :

لقد اقترن ظهور تقنية المعلومات بمشاكل خاصة ومستحدثة وعلى سبيل المثال:

(1) Merle Roger et Vitu Andre, Traite de Droit Criminel, Procedure Penal, Edition Cujas, Deuxieme Edition, Paris 1973,p128 etc. Levasseuer George et Chavanne Albert, Edition Sirey, 6ieme Edition, Paris 1980, p 110 etc..

أولريش شيبيه، المرجع السابق، ص 58. د. محمود نجيب حسني، المرجع السابق، ص 784–783. د. أحمد فتحي سرور، المرجع السابق، ص 48 وما بعدها، ص 66 وما بعدها.

أولاً- التحفظ على المعلومات:

وقد جاء الفصل الثاني من الاتفاقية تحت عنوان «سرعة التحفظ على بيانات الكمبيوتر المخزونة»:

وتنص المادة 16 من الاتفاقية على أن:

«سرعة التحفظ على بيانات الكمبيوتر المخزونة:

1. يعتمد كل طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى وذلك حتى يمكن لسلطاتها المختصة الأمر أو طلب التحفظ بصورة عاجلة على بيانات بعينها على كمبيوتر، بما في ذلك خط سير البيانات المخزنة بواسطة منظومة كمبيوتر، وخاصة في حالة وجود أسس للاعتقاد بإمكانية تعرض بيانات الكمبيوتر بصفة خاصة للفقد أو التعديل.
2. في حالة قيام طرف بتفعيل الفقرة(1) بعالية بواسطة إصدار أمر إلى شخص ما للتحفظ على بيانات كمبيوتر مخزنة بعينها، بحوزة الشخص أو تحت سيطرته، فإنه يتعين على هذا الطرف أن يعتمد ما قد يلزم من تدابير تشريعية وتدابير أخرى لإلزام ذلك الشخص بأن يحفظ ويتحفظ على سلامة بيانات الكمبيوتر المذكورة بالقدر اللازم، لفترة زمنية لا تزيد عن تسعين يوماً على الأكثر، حتى تتمكن السلطات المختصة من السعي لكشفها، ويجوز لطرف إصدار مثل هذا الأمر لتجديده بالتالي.
3. يعتمد كل طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى وذلك لإلزام المسؤول أو أي شخص آخر يتحفظ على بيانات كمبيوتر، بالمحافظة على سرية القيام بمثل هذه الإجراءات للفترة الزمنية المنصوص بها بموجب قانونه الوطني المحلي.
4. تخضع الصلاحيات والإجراءات المشار إليها بهذه المادة للمادتين 14 ، 15».

وتنص المادة 17 من الاتفاقية على أن:

«سرعة التحفظ على خط سير البيانات والكشف الجزائي لها:

1. يعتمد كل طرف، بالنسبة لخط سير البيانات المطلوب حفظها بموجب المادة 16، ما قد يلزم من تدابير تشريعية وتدابير أخرى وذلك:

أ- لضمان إمكانية سرعة التحفظ على خط سير البيانات المذكورة بصرف النظر عن مشاركة مقدم خدمة واحد أو أكثر في عملية نقل هذه الاتصالات.

ب- لضمان سرعة الكشف للسلطات المختصة بالطرف، أو للشخص الذي تعينه تلك السلطات، عن القدر الكافي من خط سير البيانات حتى يمكن للطرف تحديد مقدم

الخدمة والمسار الذي تم نقل الاتصال من خلاله.

2. تخضع الصلاحيات والإجراءات المشار إليها بهذه المادة للمادتين 14 ، 15» .

ثانياً– إصدار الأوامر لتقديم بيانات محددة داخل نظام الكمبيوتر أو على وسائط أخرى، وضبط وتأمين بيانات الكمبيوتر التي يتم الدخول عليها أثناء مباشرة الصلاحيات السابقة:

وقد جاء الفصل الثالث من الاتفاقية تحت عنوان «إصدار الأوامر»:

وتنص المادة 18 من الاتفاقية على أن:

1. يعتمد كل طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى وذلك لمنح سلطات ذلك الطرف صلاحية توجيه الأمر إلى:

أ. أي شخص في إقليمه لتقديم بيانات محددة موجودة على الكمبيوتر بحوزة ذلك الشخص أو تحت سيطرته، ومخزنة داخل نظام الكمبيوتر أو على أي وسيط تخزين بيانات آخر.

ب– أي مقدم خدمة يعرض خدماته في إقليم الطرف لتقديم معلومات للمشترك فيما يتعلق بتلك الخدمات الموجودة بحوزة أو تحت سيطرة مقدم الخدمة.

2. تخضع الصلاحيات والإجراءات المشار إليها في هذه المادة للمادتين (14) ،(15).

3. لغرض هذه المادة، فإن مصطلح «معلومات المشترك» يعني أية معلومات في صورة بيانات كمبيوتر أو أية صورة أخرى يتم حفظها من جانب مقدم الخدمة، والتي تتعلق بالمشتركين في الخدمات الخاصة به بخلاف خط سير البيانات أو مضمونها والتي بموجبها يمكن التوصل إلى:

أ– نوعية خدمة الاتصال المستخدمة، والشروط الفنية التي يتم اتخاذها في ذلك، والفترة الزمنية للخدمة.

ب– هوية المشترك، وعنوانه البريدي أو الجغرافي، ورقم تليفونه وغير ذلك من أرقام الدخول الأخرى الخاصة به، والبيانات الخاصة بالفواتير والدفع المتاحة بموجب اتفاق الخدمة أو الترتيبات الخاصة بذلك.

ج– أية معلومات أخرى خاصة بموقع تركيب أجهزة ومعدات الاتصالات، والتي تتوافر بموجب اتفاق الخدمة أو الترتيبات الخاصة بذلك».

ثالثاً – إلزام الشاهد باسترجاع وكتابة المعلومات:

رابعاً – تفتيش ومصادرة بيانات الكمبيوتر المخزنة:

وقد جاء الفصل الرابع من الاتفاقية تحت عنوان «تفتيش ومصادرة بيانات الكمبيوتر المخزنة»: وتنص المادة 19 من الاتفاقية على أن:

«تفتيش ومصادرة بيانات الكمبيوتر المخزنة:

1. يعتمد كل طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى وذلك لمنح سلطات ذلك الطرف صلاحية تفتيش أو الدخول على:

أ. أي نظام كمبيوتر أو أي جزء منه والبيانات المخزنة فيه.

ب. أي وسيط تخزين يجوز أن تكون البيانات مخزنة فيه في إقليم ذلك الطرف.

2. يعتمد كل طرف ما قد يلزم من تدابير تشريعية بعمليات البحث أو الدخول على نظام كمبيوتر بعينه أو على جزء منه، وفقاً للفقرة 1 (أ)، وقيام أسباب لديها للاعتقاد بأن البيانات المطلوبة مخزنة داخل نظام كمبيوتر آخر أو جزء منه في إقليم ذلك الطرف، وأن هذه البيانات يمكن الدخول عليها قانوناً أو متاحة على النظام الأصلي، يكون للسلطات توسيع عملية البحث أو الدخول المماثل بسرعة على النظام الآخر.

3. يعتمد كل طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى وذلك لمنح سلطاته المختصة صلاحية ضبط أو تأمين بيانات الكمبيوتر التي يتم الدخول عليها طبقا للفقرتين 1 أو 2، وتشمل هذه الإجراءات صلاحية:

أ. ضبط أو تأمين نظام الكمبيوتر أو جزء منه أو وسيط تخزين البيانات.

ب. عمل نسخة من هذه البيانات الكمبيوترية والاحتفاظ بها.

ج. المحافظة على تجانس بيانات الكمبيوتر المخزنة ذات الصلة.

د. جعل هذه البيانات الكمبيوترية غير قابلة للدخول عليها أو إزالتها على نظام الكمبيوتر الذي يتم الدخول عليه.

4. يعتمد كل طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى وذلك لمنح سلطاته المختصة صلاحية إصدار الأمر أو الإجراءات المطبقة لحماية البيانات الموجودة عليه من أجل أن يقدم– بالقدر المعقول– المعلومات اللازمة للتمكين من مباشرة الإجراءات المشار إليها في الفقرتين (1)، (2).

5. تخضع الصلاحيات والإجراءات المشار إليها في هذه المادة للمادتين (14)، (15)».

خامساً – الحق في مراقبة وتسجيل البيانات المنقولة بواسطة أنظمة الاتصالات البعدية وجمعها وتخزينها.

وقد جاء الفصل الخامس من الاتفاقية بشأن «التجميع الفوري لبيانات الكمبيوتر»، واعتراض محتوى البيانات. وتنص المادة 20 من الاتفاقية على أن:

« التجميع الفوري لبيانات الكمبيوتر:

1. يعتمد كل طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى وذلك لمنح سلطاته المختصة صلاحية:

أ. جمع أو تسجيل، من خلال تطبيق الوسائل الفنية، في إقليم ذلك الطرف،

ب. إجبار مقدم الخدمة في نطاق قدرته الفنية على:

1. جمع أو تسجيل، من خلال تطبيق الوسائل الفنية، في إقليم ذلك الطرف، أو
2. التعاون مع السلطات المختصة ومساعدتها في الجمع أو التسجيل بشكل فوري.
3. خط سير البيانات المرتبطة باتصالات معينة في إقليم ذلك الطرف التي تم نقلها بواسطة نظام الكمبيوتر.
4. في حالة تعذر تبني الطرف للإجراءات المشار إليه في الفقرة 1 (أ)، بسبب المبادئ القائمة في نظامه القانوني الوطني، يجوز له بدلاً من ذلك أن يعتمد ما قد يلزم من تدابير تشريعية وتدابير أخرى لضمان الجمع أو التسجيل الفوريين لخط سير البيانات المرتبطة باتصالات معينة تم نقلها في إقليمه، من خلال تطبيق الوسائل الفنية في ذلك الإقليم.
5. يعتمد كل طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى وذلك لإلزام مقدم الخدمة بالمحافظة على سرية وقائع تنفيذ أية صلاحيات تنص عليها هذه المادة وأية معلومات تتعلق بها.
6. تخضع الصلاحيات والإجراءات المشار إليها في هذه المادة للمادتين (14) ، (15) » .

وتنص المادة 21 من الاتفاقية على أن:

«اعتراض محتوى البيانات:

1. يعتمد كل طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى، وذلك فيما يتعلق بأنواع

الجرائم الجسيمة التي يقررها القانون الوطني، لمنح سلطاته المختصة صلاحية:

أ. جمع أو تسجيل، من خلال تطبيق الوسائل الفنية، في إقليم ذلك الطرف.

ب. إجبار مقدم الخدمة، في نطاق قدراته الفنية على:

2. جمع أو تسجيل، من خلال تطبيق الوسائل الفنية، في إقليم ذلك الطرف، أو

3. التعاون مع السلطات المختصة ومساعدتها في جمع أو تسجيل، بشكل فوري، لمحتوى البيانات المرتبطة باتصالات معينة في إقليم ذلك الطرف التي تم نقلها بواسطة نظام الكمبيوتر.

4. في حالة تعذر تبني الطرف للإجراءات المشار إليها في الفقرة 1(أ)، بسبب المبادئ القائمة في نظامه القانوني الوطني، يجوز له بدلاً من ذلك أن يعتمد ما قد يلزم من تدابير تشريعية وتدابير أخرى لضمان الجمع أو التسجيل الفوريين لمحتوى البيانات المرتبطة باتصالات معينة تم نقلها في إقليمه، من خلال تطبيق الوسائل الفنية في ذلك الإقليم.

5. يعتمد كل طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى وذلك لإلزام مقدم الخدمة بالمحافظة على سرية وقائع تنفيذ أية صلاحيات تنص عليها هذه المادة وأية معلومات تتعلق بها.

6. تخضع الصلاحيات والإجراءات المشار إليها في هذه المادتين (14)، (15) " .

سادساً – ضم المعلومات الاسمية إلى الدعوى الجنائية.

سابعاً– إيجاد «نقطة توازن» بين فاعلية الإجراءات وضمانات الحرية والخصوصية.

وسيكون من الملائم انتظارا لأبحاث أكثر دقة أن تتوافق تدابير القسر في القانون الداخلي للإجراءات الجنائية، بغرض إيجاد توازن عادل بين مصالح الدولة ممثلة في الدعوى الجنائية والحريات الفردية للمواطن.

وتدور هذه المشكلات الإجرائية الخاصة المستحدثة حول محورين، الأول: يتعلق بمراقبة الاتصالات والإنترنت، والثاني: يتعلق بضمانات أمن المعلومات و الأمن القومي والخصوصية.

وتوضح هذه المناقشات جميعها أن تحول المجتمع من صناعي إلى ما بعد الصناعي (عصر الثورة الرقمية وتكنولوجيا الاتصال) يستلزم تحليلاً أكثر تعمقاً للمؤشرات الحديثة للحق في المعلومات والحق في الخصوصية.

تؤدي مقتضيات حماية الأمن القومي والمصالح الحيوية للدول، ومقتضيات احترام

سيادة الدول الأخرى وعدم التدخل في شئونها الداخلية، وحماية الحق في الخصوصية إلى ضرورة الوصول إلى نقطة توازن بينها، ويؤدي ذلك كله إلى مشكلات قانونية إجرائية ، يمكن تأصيلها في محورين:

المحور الأول – متطلبات حماية حق الدول في الأمن القومي وحماية المصالح الحيوية

(41) تحليل المشكلات الإجرائية للأنشطة وعمليات مراقبة الاتصالات:

يواجه تقرير الضمانات الأساسية للحق في المعلومات وللحق في الخصوصية (الحماية الإجرائية للحق في الخصوصية) تحديات قانونية تتطلب بيان وتحليل المشكلات الإجرائية لعمليات مراقبة الاتصالات، حيث تثير تلك المراقبة المشكلات الفرعية الآتية:

1ـ طبيعة المراقبة:

وتثير التساؤلات الآتية حول: ماهية المراقبة من الناحيتين الفنية والقانونية؟ وما هي خصائصها التي تميزها عن الأوضاع الإجرائية الأخرى كالتفتيش؟، وماهي ضروراتها (مبرراتها وأسبابها) وأهميتها؟ وماهي وسائلها وبرامجها وحصيلتها (معلومات بيانات صور عن أشخاص و أوضاع وأنشطة)؟ وماهو الغرض الذي تستخدم فيه؟ (رسم خطط المكافحة والتتبع والملاحقة)؟ وما هو الهدف من ذلك (رسم خطط مكافحة الإرهاب والجريمة المنظمة والجرائم الخطيرة التي تهدد الأمن القومي والمصالح الحيوية، والنظام والآداب العامة والمصالح الاقتصادية والصناعية والتجارية)؟ وماهي الأجهزة التي تقوم بها وبأي صفة؟

2 ـ مظاهر خطورة المراقبة:

تتمثل خطورة مراقبة الاتصالات والإنترنت في أنها تعد عدواناً على سيادة الدول وخصوصيتها وأسـرارها، وعدواناً على حق الأفراد العاديين في الخصوصية، وإهداراً لمبادئ الحرية والأمان المعلوماتي الرقمي، وعدواناً على حرية التواصل الاجتماعي بين الأفراد وحقهم في سرية اتصالاتهم ومحادثاتهم عبر وسائل الاتصال، وحقهم في الحفاظ على أسرارهم الشخصية، وحريتهم في التعبير، وحقهم في التنقل بحرية.....، ويمثل هذا العدوان انتهاكاً خطيراً لأهم حقوق الإنسان اللصيقة بالشخصية التي تقررت في الإعلانات والمواثيق الدولية والدساتير والقوانين الوطنية في الدول الديمقراطية.

3 ـ مدى التوافق حول مشـــروعية المراقبة:

– نظراً إلى ضرورة عمليات المراقبة وأهميتها من جهة، وخطورتها من جهة أخرى تثور مشكلة مشروعية المراقبة وعدم مشروعيتها، وتثير هذه المشكلة التساؤل عن مدى

التوافق أو الانقسام بين الفقهاء والباحثين حول إقرار أو إنكار تلك العمليات:

(42) بيان مدى مشروعية المراقبة للاتصالات والإنترنت والممارسات الحالية:

– أثارت مراقبة أجهزة الاستخبارات للاتصالات والإنترنت، كما أثارت مراقبة المحادثات التليفونية منذ بداية ظهورها تساؤلاً حول مدى مشروعيتها[1]، بصورة انقسم معها الفقه والقضاء إلى فريقين: منهم المنكرون لمشروعيتها، ومنهم المؤيدون لها. وأخذ المؤيدون يبحثون عن أساس قانوني لمشروعيتها، وفي ظل غياب قانون منظم لها، بحثوا عن هذا الأساس إما في بعض النصوص القانونية أو ردوها لبعض النظم الإجرائية المطبقة. وسواء وجد قانون ينظم مراقبة المحادثات أم لم يوجد، فقد بحث الفقه والقضاء عن الضمانات الضرورية لمشروعية المراقبة باعتبارها استثناء يرد على الأصل العام وهو احترام حق الإنسان في الخصوصية. ويأتي البحث في القانون المقارن عن هذه الضمانات أمراً ضرورياً قبل دراسة الوضع في القانون المصري والقانون الكويتي وسائر القوانين العربية. وستكشف الدراسة في القانون المقارن سواء في النظام اللاتيني أو في النظام الأنجلو– ساكسوني عن نطاق مشروعية المراقبة وحدود الضمانات المقررة لها، بصورة سوف تترك بصماتها عند دراسة تنظيم القانون المصري والقانون الكويتي

(1) انظر: في ضمانات المراقبة قبل وبعد قانون سلطة وكالة الاستخبارات الأمريكية في مراقبة الأجانب:

Warrantless Surveillance Before and After FISA

Adam Burton. Fixing FISA for Long War: Regulating Warrantless Surveillance in the Age of Terrorism. HEINONLINE. Citation: Pierce Law Review (Vol. 4, No. 2) Page: 386-388 - 2005-2006.

Civil Rights Abuses, The Church Committee, and the Enactment of FISA

Electronic surveillance of private conversations for the purposes of national security and law enforcement is as old as telecommunications itself.

As evidence on the abuses of the surveillance program emerged in the shadow of Watergate, Congress initiated a formal investigation of the country's foreign intelligence practices, headed by Senator Frank Church. The voluminous reports of the Church Committee, published in 1975-76, concluded that the government's foreign intelligence program undermined the constitutional rights of citizens "primarily because checks and balances designed by the framers of the Constitution to assure accountability have not been applied.

In 1978, Congress enacted FISA as the "exclusive means" by which the President may conduct domestic surveillance for gathering foreign intelligence to address these concerns.

Procedure Under FISA

1. Electronic Surveillance Pursuant to a FISA Warrant

Congress enacted FISA to provide judicial scrutiny of the executive branch in foreign intelligence surveillance to ensure compliance with the Fourth Amendment, but without causing undue intrusion on executive branch discretion in matters of national security.

2. Warrantless Surveillance under FISA

FISA permits a federal agency to commence surveillance without first obtaining a warrant in only three circumstances.

لمراقبة المحادثات التليفونية[1] ومواقع التواصل الاجتماعي والاتصالات عبر الشبكات الدولية والإنترنت.

(43) الإطار العام لمشروعية ممارسة السلطات الإجرائية:

ويقتضي هذا التحليل تحديد الإطار العام لمشروعية ممارسة السلطات الإجرائية (العادية والاستثنائية)

– مبدأ المشروعية العام:

– يحكم الدولة المعاصرة مبدأ ذو أهمية خاصة، هو خضوع الدولة للقانون، ذلك أن الدولة حسبما استقر تعريفها في فقه القانون العام هي شخص من أشخاص القانون[2].

وترتيباً على ذلك فإن نشاط هيئاتها العامة، التشريعية والقضائية والتنفيذية، لا يكون صحيحاً ونافذاً وملزماً في مواجهة المخاطبين إلا إذا صدر طبقاً للقانون وبناء عليه، بل وأحياناً أخرى بالتطبيق الصحيح له، بحيث إذا صدر القرار أو النشاط على غير ذلك، فإنه يكون غير مشروع[3]، ويطلق على الدولة التي تلتزم بهذا المبدأ «الدولة القانونية».

ولكي يتحقق نظام الدولة القانونية الكامل، ينبغي توافر عناصر معينة وتقرير ضمانات محددة ، تتمثل فيما يلي[4]:

– وجود الدستور وهو القانون الأعلى للبلاد، تطبيق مبدأ الفصل بين السلطات، الاعتراف بالحقوق والحريات الفردية، خضوع الإدارة (أو الحكومة) للقانون، تنظيم رقابة قضائية فعالة على أعمال ممثلي السلطات العامة.

– وتثير مشكلة مشروعية تلك المراقبة مشكلة «مشروعية أدلة الإثبات المستمدة منها»[5] .

– مشكلة التفرقة بين المراقبة بمبادرات أمنية والمراقبة بإذن القضاء، ويتفرع عن ذلك مشكلة تقرير الرقابة القضائية الفعالة على أنشطة وعمليات المراقبة وممارستها والجزاءات القانونية لانتهاكها.

– صعوبة الوصول إلى تحديد معايير لعمليات ووسائل المراقبة السريعة والفعالة، تتسم بالمشروعية والتوافق مع المعايير الدولية، وصعوبة تحديد السياسات والإستراتيجيات

(1) انظر: الدكتور محمد أبو العلا، عقيدة، المرجع السابق، ص 8

(2) انظر: د. طعيمة الجرف، مبدأ المشروعية وضوابط خضوع الدولة للقانون، دار النهضة العربية، الطبعة الثالثة 1976، ص3.

(3) انظر: د. طعيمة الجرف، مرجع سابق، ص 3.

(4) انظر: د. ثروت بدوي، النظم السياسية، دار النهضة العربية، القاهرة، مصر، 1986، ص 173.

(5) د. مصطفى يوسف: مشروعية الدليل في المسائل الجنائية، سنة النشر 2010.

والآليات والضوابط التي تحكم الممارسات الفعلية في التطبيق العملي. وفي ذات الوقت صعوبة الوصول إلى ضمانات كافية للحقوق الشخصية وتفعيلها واحترامها من قبل الأجهزة الأمنية والاستخبارية، ومنع التجاوزات والانتهاكات في حق الدول والأفراد.

المحور الثاني – متطلبات الحماية الإجرائية للحياة الخاصة (الحق في الخصوصية):

تحديد معنى الحياة الخاصة: لم يهتم القانون ولا القضاء بتحديد معنى الحياة الخاصة بسبب صعوبة تعريفها من جهة، ونسبية فكرتها من جهة أخرى، حيث تتباين بتباين الناس وبيئاتهم وثقافاتهم وانتماءاتهم الدينية والسياسية والاجتماعية. ومع ذلك، فقد حاول جانب من الفقه الفرنسي تعريفها بأنها (كل ما ليس له علاقة بالحياة العامة، أو هي كل ما لا يعد من قبيل الحياة العامة للإنسان). ويركز هذا التعريف السلبي على الاهتمام بخصوصية الحياة في المقام الأول[1].

(44) حرمة الحياة الخاصة:

إن هذا الاختراق المذهل للحياة الخاصة في هذا العصر أمر لا تقِّره لا الشرائع السماوية ولا القوانين الوضعية، فلا خلاف بين فقهاء الشريعة الإسلامية على حرمة الحياة الخاصة؛ فحرمة المسكن وسرية الحديث تصونها الشريعة الإسلامية بآيات قرآنية وأحاديث نبوية غاية في الوضوح والدلالة. يقول تعالى في محكم التنزيل: **(يا أيها الذين آمنو لا تدخلوا بيوتا غير بيوتكم حتى تستأنسوا وتسلموا على أهلها)**2. ويقول أيضاً: **(يا أيها الذين آمنوا اجتنبوا كثيرا من الظن إن بعض الظن إثم ولا تجسسوا ولا يغتب بعضكم بعضا أيحب أحدكم أن يأكل لحم أخيه ميتا فكرهتموه واتقوا الله إن الله تواب رحيم)**[3]، ويقول ﷺ:«من اطلع في بيت قوم بغير إذنهم فقد حل لهم أن يفقئوا عينه، فإن فقأوا عينه فلا دية عليهم ولا قصاص»[4]. ويقول أيضا: «فمن استمع إلى حديث قوم صب في أذنه الآنك».

تبدو أهمية حماية الحياة الخاصة للأفراد المعنيين بالبيانات المختزنة على سبيل المثال في حالة التفتيش غير القانوني لحسابات بعض الأفراد الموجودة بالخارج من قبل سلطات بلادهم، وفي حالة المراقبة الشاملة للفرد عن طريق الجمع الموسع للبيانات الاسمية، وأيضا في حالة إذاعة معلومات وهمية عن المنشآت (كالإفلاس والديون)، وفي حالة الاستخدام التعسفي للبيانات الشخصية ومنها البيانات الطبية، وعلى سبيل المثال معلومات تتعلق

(1) انظر: د. داود عبد الرازق الباز، المرجع السابق، ص253.
(2) سورة النور، الآيات: 29–28–27
(3) سورة الحجرات، الآية: 12
4

بالإيدز. وتبرهن جميع هذه الأمثلة على أن مجال خصوصية المواطن في مجتمع المعلومات يجب أن يحمى بقوانين حديثة في المجال الجنائي والمدني والقانون العام[1].

الفرع الثالث
حق المتهم في الخصوصية

(45) أولاً – تعريف حق المتهم في الخصوصية وعناصره ونطاقه ومجالاته:

أولت الدول المتحضرة اهتماماً كبيراً بحقوق الإنسان، ومنها الحق في الخصوصية، غير أن مضمون هذا الحق قد يتسع أو يضيق تبعاً للنظام السياسي لهذه الدول، وما يقوم عليه من مبادئ وما يؤمن به من أسس في الفلسفة السياسية. فليس غريباً أن نرى مفهوم هذه الحقوق والحريات الشخصية يختلف اختلافاً كبيراً في الأنظمة الديمقراطية عنه في الأنظمة الدكتاتورية، كالأنظمة الماركسية والفاشية[2].

إن للمتهم بوصفه إنساناً الحق في أن يحيا حياته الخاصة، بعيداً عن تدخل الغير وبمنأى عن العلانية[3]. فالحق في الحياة الخاصة هو من حقوق الإنسان التي أكدها الإعلان العالمي لحقوق الإنسان، وقد أضفت كثير من الدول عليه قيمة دستورية، فنص على حمايته صراحة الدستور المصري الصادر سنة 1971 إذ أكد في المادة (45) على أن (لحياة المواطنين الخاصة حرمة يحميها القانون).

(46) مجالات حق المتهم في الخصوصية:

ويمارس الإنسان حياته الخاصة في مجالات متعددة يودع فيها أسراره الشخصية، وأهم هذه المجالات وأبرزها هو الشخص والمسكن والمراسلات، والمحادثات الشخصية[4].

(47) الإجراءات والسلطات القانونية الماسة بحق المتهم في الخصوصية :

وقد اقتضت سلطة الدولة في العقاب تخويل أجهزتها القائمة على التحقيق، الحق في مباشرة بعض الإجراءات الماسة بالحق في الحياة الخاصة لضبط أدلة الجريمة، وهي التفتيش وضبط المراسلات، ومراقبة المحادثات السلكية واللاسكية وتسجيل الأحاديث الشخصية.

(1) انظر: Dr. UlrichSieber ، تحليل لموضوع : جرائم الكمبيوتر والجرائم الأخرى في مجال تكنولوجيا المعلومات، المرجع السابق، ص 57–56

(2) د. كاظم السيد عطية، الحماية الجنائية لحق المتهم في الخصوصية، ص 22

(3) انظر د. أحمد فتحي سرور، الوسيط في قانون الإجراءات الجنائية، ص 542 .

(4) انظر د. أحمد فتحي سرور، المرجع السابق، ص 543

ولكن هذا الحق يجب أن يكون محدداً بالقدر اللازم للموازنة بين مقتضيات سلطة العقاب واحترام الحق في الحياة الخاصة. فلا يجوز أن ننسى مطلقاً أننا نتصرف تجاه شخص بريء لأن الأصل في المتهم البراءة، ولا يمكن أن يكون إجراء الاتهام أو بدء التحقيق إيذاناً بالفتك بحرية المتهم أو إهدار أسراره[1].

ومن ناحية أخرى، فإن التفتيش قد يمس حقوقاً أخرى يحميها القانون، كالحق في الحصانة (الدبلوماسية أو البرلمانية أو القضائية) أو (الحق في سر المهنة أو حقوق الدفاع). ولا بد من خلال شروط التفتيش تحقيق التوازن بين الحق في التفتيش وهذه الحقوق الأخرى[2].

(48) موقف التشريعات المقارنة من حق المتهم في الخصوصية:

وإذا كانت البشرية قد ارتقت في مجال احترامها لحقوق الإنسان بصفة عامة، والحق في الخصوصية بصفة خاصة، فإنه من الطبيعي أن تتقدم وبذات الخطى في مجال احترام حقوق المتهم، وعلى الأخصِّ حقه في الخصوصية، فقد تضمنت غالبية التشريعات المقارنة الحديثة نوعين من نصوص الحماية الجنائية لحق المتهم في الخصوصية، النوع الأول: وهو نصوص الحماية الجنائية الإجرائية لحق المتهم في الخصوصية، ويقصد بها أن الإجراءات الجنائية التي تباشر ضد المتهم خلال مراحل الخصومة الجنائية يجب أن تتسم بالمشروعية، وأن تراعى فيها الضمانات والقيود التي وضعها المشرع، فلا يجوز تفتيش مسكن المتهم والاطلاع على خصوصياته إلا في أحوال معينة وبشروط محددة، كما لا يجوز مراقبة أو تسجيل محادثاته الهاتفية أو الشخصية أو تصويره إلا وفق ضوابط معينة، كما لا يجوز فض مراسلاته الخاصة والاطلاع عليها إلا من قبل سلطة معينة وبشروط محددة . هذا عن النوع الأول من النصوص الجنائية، أمام عن النوع الثاني من نصوص الحماية الجنائية لحق المتهم في الخصوصية، فنعني به تلك النصوص التي تقرر الحماية الجنائية الموضوعية لحق المتهم في الخصوصية، إذ ليس كافياً أن يبطل الإجراء الجنائي الذي ينتهك الخصوصية، بل لابد من مجازاة القائم بهذا الإجراء متى توافرت في حقه أركان جرائم معينة، منها على سبيل المثال: جريمة انتهاك حرمة المسكن التي تقع من الموظف العام، وهو هنا غالباً ما يكون أحد مأموري الضبط القضائي، ومنها أيضاً جريمة استراق السمع أو اختلاس الصورة بغير رضاء صاحب الشأن، وفي غير الحالات المقررة قانوناً[3].

ثم مع استمرار التقدم العلمي والدخول في عصر الحاسبات الآلية، ظهرت بنوك المعلومات الحكومية ثم الخاصة وأودعت بها المعلومات والبيانات الشخصية الخاصة

(1) انظر: د. أحمد فتحي سرور، المرجع السابق، ص 543

(2) انظر: د. أحمد فتحي سرور، المرجع السابق، ص 543

(3) د. كاظم السيد عطية، الحماية الجنائية لحق المتهم في الخصوصية، ص 23

بالأفراد، فأصبحت حياتهم الخاصة معرضة أكثر من ذي قبل للانتهاك ، مما شكل تحدياً جديداً للمجتمعات المتحضرة في سبيل الحفاظ على حرمة الحياة الخاصة وحماية تلك البيانات والمعلومات من الإفشاء إلا في حالات معينة ووفق ضوابط محددة.

(49) تحديد الإطار الدستوري والقانوني المنظم لعمليات المراقبة للاتصالات والإنترنت وضمانات حقوق الإنسان والحق في الخصوصية:

ويتعرض هذا الإطار لبيان:

نطاق مشروعية المراقبة: وآلياتها القانونية، وضماناتها (برسم حدود للمراقبة، والحالات التي تجوز فيها، وشروطها، ووضع قيود على ممارستها حتى تبقى في إطارها المشروع، وبيان الاختلاف في صياغة الحقوق الشخصية للدول والأفراد، والضمانات الدستورية والقانونية لها في قوانين الدول، ومدى توافقها مع المعايير الدولية المقررة في الإعلانات والمواثيق الدولية [1].

وبناء على ذلك، تسعى الدراسة إلى تحديد الأصول والمبادئ (السياسية والقانونية والأخلاقية)، التي تحكم تنظيم سلطات وعمليات أجهزة الاستخبارات، لحماية الأمن القومي والمصالح الحيوية للدول. وكذلك الإطار القانوني العام لحق الدول في السيادة وحق الأفراد في الخصوصية والحق في حرية التعبير والصحافة والنشر(2)، ويتم ذلك بتحديد الآتي:

أ) تحديد الأصول والقيم والمعايير الدولية الحاكمة للتشريعات المنظمة لمراقبة الاتصالات، والحاكمة لممارسة السلطة في التطبيق العملي مع ضمان الحق في الخصوصية، حيث تنص المواثيق والمعاهدات الدولية على حماية حق الإنسان في حرمة حياته الخاصة، وهو ما أكدته المادة 12 من الإعلان العالمي لحقوق الإنسان الصادر عن الجمعية

(1) انظر: في تطور الوضع الدستوري والقانوني في الولايات المتحدة الأمريكية قبل وبعد إصدار قوانين المراقبة للاتصالات والإنترنت وضمانات حقوق الإنسان والخصوصية

Thomas P. Ludwig, The Erosion of Online Privacy Rights in the Recent Tide of Terrorism, HEIN-ONLINE, Citation: Computer Law Review and Technology Journal. (Vol. VIII), 2003-2004. Page: 131. "Imagine a world where any idea or message communicated to another individual is subject to governmental scrutiny for possible criminal, subversive, or terroristic content. The current location of any individual, as well as the places that he or she commonly frequents, can easily be tracked through that person's phone calls, online activity, and financial records, which are all accessible to government agencies. By intercepting e-mails and tracking online browsing, shopping, and other activities, the most intimate details, habits, and preferences of the average individual are readily available to the prying eyes of cyber-criminals and law enforcement officials alike".

(2) انظر: د. جعفر عبد السلام، الإطار التشريعي للنشاط الإعلامي، دار المنار للطبع والنشر والتوزيع، 1414 هـ، 1993 م، ص 215 وما بعدها

العامة للأمم المتحدة سنة 1948، والمادة 17 من الاتفاقية الدولية لحقوق الإنسان المدنية والسياسية الصادرة عن الجمعية العامة للأمم المتحدة في سنة 1966، والمادة 8 من الاتفاقية الأوروبية لحقوق الإنسان وحرياته الأساسية التي تم التوقيع عليها في روما سنة 19501.

ب) بيان الضمانات الدستورية والقانونية والقضائية لصيانة سيادة الدول والخصوصية وحرية التعبير والصحافة: تنص دساتير دول كثيرة على حرمة الحياة الخاصة وضرورة حمايتها بنصوص قانونية واضحة2، وهو ما تؤكده القوانين في البلاد المختلفة بوضع القواعد اللازمة لمشروعية التفتيش وضبط المراسلات والاطلاع عليها، أو لمراقبة المحادثات التليفونية مع إحاطتها بالضمانات التي تعمل على منع التعسف.

ت) تحديد الإطار العام لمشروعية عمليات أجهزة الأمن والاستخبارات لمراقبة الاتصالات والإنترنت، وشفافية تلك العمليات والأنشطة.

ث) تحديد الإطار العام للسياسات الأمنية والتشريعية للدول في تنظيم تلك العمليات والأنشطة، لضمان فاعليتها في تحقيق أهدافها.

ج) وسائل حماية حقوق الإنسان (إصلاح وتعديل التشريعات لمزيد من الضمانات وتقرير الجزاءات).

(1) The Role of United Nations in Protection and Enhancement of Human Rights.
Several Articles and the Preamble of the United Nations Charter deals with this matter as follows:
Preamble (2) Stated that:- to reaffirm faith in fundamental human rights, in the dignity and worth of the human person, in the equal rights of men and women and of nations large and small.
Article 12 (1b) The General Assembly shall initiate studies and make recommendations for the purpose of: b. promoting international co-operation in the economic, social, cultural, educational, and health fields, and assisting in the realization of human rights and fundamental freedoms for all without distinction as to race, sex, language, or religion.
Article (55) (c) Universal respect for, and observance of, human rights and fundamental freedoms for all without distinction as to race, sex, language, or religion.
The International Covenant on Civil and Political Rights (ICCPR) is a multilateral treaty adopted by the United Nations General Assembly on 1966, and enters into force on, 1976. It commits its Parties to respect the civil and political rights of individuals, including the right to life, freedom of religion, freedom of speech, freedom of assembly, electoral rights and rights to due process and a fair trial.
The ICCPR is part of the International Bill of Human Rights, along with the International Covenant on Economic, Social and Cultural Rights (ICESCR) and the Universal Declaration of Human Rights (UDHR).

د. محمد أبو العلا، عقيدة...، المرجع السابق، ص 8

(2) د. محمد أبو العلا، عقيدة...، المرجع السابق، ص8

وذلك بتحديد الآتي:

- نطاق ومجال المراقبة: حالاتها، وحدودها، وشروطها (الموضوعية والشكلية) ومدتها(بدايتها ونهايتها) وحصيلتها واستخدام تلك الحصيلة من المعلومات، ومشروعية أدلتها.
- بيان أهداف المراقبة، والوسائل والآليات المشروعة لتحقيقها.
- بيان شروط مشروعية المراقبة (من الناحيتين: الموضوعية والشكلية).
- بيان ضوابط ممارسة السلطة في التطبيق العملي.
- بيان آليات الرقابة الدولية والسياسة والبرلمانية والقانونية والحقوقية والقضائية، والجهات والأجهزة المنوط بها تلك الرقابة وضمانات حيادها واستقلالها.

وهو الأمر الذي يستهدف تحديد ومعالجة المشكلات التالية:

- مشكلة الوصول إلى «نقطة توازن» بين المصلحة العامة والمصلحة الخاصة (مقتضيات الأمن والعدالة وضمانات السيادة والحرية والخصوصية حال القيام بعمليات المراقبة، أي بين فاعلية المراقبة وضمانات الحرية)
- مشكلة «حرية المعلومات في مواجهة سرية البيانات والاتصالات الشخصية»، وحالات ومبررات وشروط الكشف عنها وإفشائها، ومعايير الإفصاح، والقيم الحاكمة للإفصاح والكتمان.
- مشكلة اختلاف النظم والدساتير والقوانين المقارنة في معالجة كل تلك المشكلات، لاسيما في تحديد نطاق مشروعية المراقبة وحدود الضمانات المقررة، وهو ما يلقي بظلاله ويترك بصماته في صعوبة الوصول إلى القواسم المشتركة والإطار العام للتنظيم والمعالجة[1].

(1) د. سعاد الشرقاوي، الاستفادة من تكامل مناهج تدريس حقوق الإنسان في كليات الحقوق، بحث مقدم إلى مؤتمر تعليم حقوق الإنسان، كلية الحقوق جامعة القاهرة من 9-11 يونيو سنة 1987، ص1.

المبحث الثالث
التحولات والمشكلات القانونية المتعلقة بالقانون الإداري والقانون الدولي وعلوم الإدارة والاتصال الحديثة في علاقتها بالقانون الجنائي

(50) رؤية الخيارات التنظيمية الإستراتيجية:

إن تحقيق مشروع الحكومة الإلكترونية أو الإدارة الإلكترونية يحتاج إلى توفير البيئة القانونية والتنظيمية الملائمة التي من شأنها أن توفر لتطبيقات تكنولوجيا المعلومات والاتصالات في العمل الإداري المستوى اللازم من الأمان والموثوقية والسرية والإثبات، وأن تقلِّص من حجم المخاطر المحتملة[1]. وتحتاج هذه العملية من الدولة المعنية أن تحسم العديد من الخيارات الإستراتيجية على الصعيد التنظيمي وذلك بصورة مسبقة (أولاً) قبل التصدي للمسائل القانونية والتنظيمية الجديدة التي تطرحها الإدارة الإلكترونية (ثانياً).

ومن أهم الركائز القانونية والتنظيمية للإدارة الإلكترونية ما يلي:

وضع تعريف قانوني وتقني موحد للمصطلحات: إن من أبرز هذه الخيارات التنظيمية الإستراتيجية وجوب وضع تعريف قانوني وتقني موحد للمصطلحات وللمفردات الحديثة المتداولة، وإقرار الطابع الإلزامي أو الاختياري للإدارة الإلكترونية (بالنسبة للمواطنين والإدارات على حد سواء)، واتخاذ القرار المناسب إما باعتماد تنظيم مستقل للخدمات الإدارية الإلكترونية أو جعله مشتركاً مع الخدمات التقليدية، وكيفية ضمان مبدأ المساواة بين المواطنين في الاستفادة من الخدمات العامة[2]. ومن بين المسائل القانونية والتنظيمية الجديدة التي تطرحها الإدارة الإلكترونية – والتي يقتضي التصدي لها من خلال استحداث تشريعات ونظم خاصة – صعوبات التعريف بهوية المواطنين لدى القيام بالمعاملات الإلكترونية مع الإدارات، وتحديد أصول وأساليب الاستعانة بالتوقيع الإلكتروني في المعاملات الإدارية، وطرق معالجة البيانات الشخصية، والمبادئ الواجب مراعاتها في هذا

(1) د. طوني ميشال عيسى، الركائز القانونية والتنظيمية للإدارة الإلكترونية، مؤتمر الكويت حول الحكومة الإلكترونية 13–15 أكتوبر 2003، ص 15.

(2) د.طوني ميشال عيسى، المرجع السابق، ص 15.

المجال، والتصدي للاعتداءات على المعلومات والمعاملات الإلكترونية، وتنظيم أساليب حل النزعات والشكاوى الإدارية بالوسائل الإلكترونية[1].

(51) الدائرة الثانية للتحولات القانونية تحتوى بقية فروع القانون في علاقتها بالقانون الجنائي، لاسيما القانون الإداري وعلوم الإدارة والاتصال الحديثة،

ذلك أن تطبيق مفاهيم الحكومة الإلكترونية يرتبط بالضرورة بمعالجة أشكال جديدة للجريمة المرتكبة بالوسائل الإلكترونية، وأيضاً فإن مثل هذا التطبيق يعني مواجهة أشكال جديدة من حماية الحياة الخاصة وسرية الاتصالات، بالإضافة لوجوب متابعة الآثار القانونية للتعاملات التجارية والمدنية بالوسائل الإلكترونية، بكل بساطة يجب أن نتصور الآثار القانونية في كل اتجاه ومنحى من مناحي وظائف الدولة وحركة المجتمع[2].

وبالنسبة للدائرة الثانية من التحولات لا تستطيع أن تقدم دراسة معمقة، لكن الهدف من العرض هو لفت نظر المشرع إلى اتساع دائرة التحولات القانونية في كل المجالات.

ومن بعد التعامل مع المحاور الإستراتيجية المذكورة، فإن الورقة تحاول أن تقدم رؤية وعدداً من التوصيات في هذا المجال، مثل أن تطبيق الحكومة الإلكترونية يرتب التزاماً قانونياً على الدولة بتيسير استخدام الإنترنت للمواطنين، وأن نجاح الحكومة الإلكترونية يرتبط بحد كبير بالقدرة على تطوير العقلية الإدارية، ففي نهاية المطاف نحن أمام إدارة تقدم إمكانيات النجاح وليس النجاح ذاته[3]، مع تقديم تصورات لحل المشكلات الملحة القانونية والأمنية على وجه الخصوص.

المطلب الأول
مشكلات الحوكمة في المؤسسات الحكومية والحق في الخصوصية

(52) مشكلات الحوكمة في المؤسسات الحكومية الاقتصادية

سنعرض في هذا المطلب لمشكلات الحوكمة في عدد من المؤسسات الحكومية الاقتصادية والخدمية الكويتية، وهي المؤسسة العامة للبترول ومؤسسة الخطوط الجوية الكويتية وهيئة المعلومات المدنية.

(1) د.طوني ميشال عيسى، المرجع السابق، ص 15.

(2) انظر: د. محمد الفيلي، العلاقة بين القانون والحكومة الإلكترونية، مؤتمر الكويت حول الحكومة الإلكترونية 13–15 أكتوبر 2003، ص 17–18

(3) انظر: د. محمد الفيلي، المرجع السابق، ص 19.

وفيما يلي نتعرض بالتحليل للمسائل الآتية:

– الأولى: قواعد الحوكمة.

– الثانية: تأثير الحوكمة على الحق في الخصوصية.

– الثالثة: الحق في المعرفة وتقويض السرية في الإدارة.

(53) أولاً– قواعد الحوكمة في ظل عصر المعلوماتية

– **الارتقاء بكفاءة أداء الإدارات الحكومية:** أضحى من المسلمات أن الإدارة الحديثة عنصر من عناصر التنمية. وسيفرض المستقبل على الإدارات الحكومية وغيرها، العمل على تنمية قدرات المجتمع في العالم والتقنية وتسخير ثورة المعلومات والاتصالات للارتقاء بخدمات الأفراد، وأوضح مظهر للرقي الإداري أن تبدو الخدمات العامة شاملة ومحكمة الأداء، وإن استلزم ذلك حدوث تغيير جذري في آليات تقديم الخدمات العامة بشكل يواكب التطورات السريعة في ميدان المعلوماتية والاتصال عن بعد، وما يترتب عليه من ضرورة التنسيق والتكامل بين الإدارات في تقديم الخدمات والشفافية في الأداء، على نحو يحمي المعلومات والخصوصية والبيانات الشخصية للأفراد في الوقت نفسه[1].

وسوف نوضح ذلك من خلال ما يلي:

1. الارتقاء بالأداء من خلال التكامل بين الجهات الحكومية:

– إن نجاح الإدارة الإلكترونية يتوقف على رأي المستفيد من الخدمة، والذي تتطلع الحكومة الإلكترونية إلى نيل رضائه وكسب ثقته وتحقيق رغباته.

– وسوف تؤدي تكنولوجيا المعلومات إلى تغيير نظرة الإدارات الحكومية إلى المتعامل معها ليتحول إلى (زبون) – بدلاً من مراجع – تحرص الإدارات على راحته ورضاه، على اعتبار أن المستفيد من خدمات الحكومة الإلكترونية يشكل المحور الرئيسي في عملية تيسير الإجراءات وتكامل الخدمات.

– إن المأمول من الحكومة الإلكترونية أن تحسن العلاقة بين الجمهور والمرافق العامة، على نحو يجعل الإدارات الحكومية أكثر تجاوباً مع المتطلبات الجديدة للمواطنين.

– ولعل أفضل طريقة للوصول إلى ذلك هي التكامل والتنسيق والتواصل والتفاعل بين الإدارات، وتبادل المعلومات والبيانات المخزنة لديها بصورة تظهر للعميل، وكأنه يتعامل

(1) انظر: د. داود عبد الرازق الباز، المرجع السابق ص241.

مع إدارة واحدة، أو لا يحتاج إلى الذهاب إلى جهة إدارية أخرى، أو يجد معاملته موزعة على دوائر عديدة.

- وسوف يؤدي هذا التكامل إلى وضع العميل في مكان السائق الذي يقود آله المعاملة مع الإدارة، وعندما يكون طالبو الانتفاع بخدمات المرافق في مكان السائق، فهم الذين يحددون الهدف وكيفية الوصول إليه.
- وبالتالي فإن الحكومة الإلكترونية تعد فرصة للارتقاء بأداء الخدمات الحكومية وتحسين مستواها، بتقليل نسبة الأخطاء والإهمال الناشئ عن الكم الهائل من الوثائق والملفات، وكسب ثقة الجمهور من خلال منهج علمي متطور لتوظيف تكنولوجيا المعلومات والاستفادة من معطيات ثورة الاتصالات والنظم الإلكترونية في تقديم الخدمات المطلوبة للمواطنين بسهولة ويسر، وبشكل راق وأسلوب حضاري.

أ. إصدار التشريعات التي تنظم التوقيع الإلكتروني في القطاع العام: لا يوجد في السويد تشريع عام يتعلق بصلاحية التواقيع الإلكترونية، إلا أن هناك بعض الجوانب ينظمها قانون التوقيع الإلكتروني، وهي عبارة عن التطبيق السويدي لنظم الاتحاد الأوروبي بشأن التوقيع الإلكتروني[1].

ب. النصوص والمستندات القانونية الجديدة: يبدو أن استخدام تكنولوجيا المعلومات يشجع استخدام المستندات والنصوص القانونية غير التقليدية، حيث أن بعض هذه المستندات إنما هو عبارة عن ترجمة إلكترونية لمستندات قديمة شبة قانونية، على سبيل المثال النماذج الإلكترونية، ومن الأمثلة الأخرى مستندات سياسة استخدام التواقيع الإلكترونية مثل ما يسمى بيانات سياسة التوثيق (CPS)، ومثال آخر ما يسمى بالمواثيق حيث تتعهد الإدارات بمستوى معين من الخدمات. وقد تم طرح هذه المواثيق من قبل الإدارات السويدية كنوع جديد من التفاعل الديمقراطي بين الإدارات والمواطنين[2]. ولبيان ذلك بصورة أوضح نأخذ البطاقة الشخصية أو المدنية مثالاً، فاستخراج هذه البطاقة يستلزم وجود إيصال كهرباء أو مياه لإثبات محل الإقامة، ولا شك أن بيانات صاحب البطاقة تكون موجودة من قبل لدى شركة الكهرباء، كما يمكن الحصول على بياناته الوظيفية إن كان موظفاً من قاعدة البيانات الموجودة في مؤسسة التأمينات الاجتماعية من خلال الدخول على شبكتها الإلكترونية. وقامت وزارة التنمية الإدارية بتعميم نموذج موحد لطلب الخدمة، ليكون وسيلة معتمدة في التعامل بين الفرد وجهة الإدارة، وتحدد فيه كل البيانات المطلوبة للخدمة، من مستندات

(1) غوستاف جونسون، المرجع السابق، ص 5.
(2) غوستاف جونسون، المرجع السابق، ص 35.

ورسوم وتوقيتات لتبصير المواطن بحقوقه، ويكون هذا النموذج ملزماً للجهة التي يتعامل معها الفرد، بالإضافة إلى تحديد مسئولية الموظفين القائمين على أداء الخدمة، وإيضاح الجهة التي يتقدم إليها الفرد بشكواه إذا تطلبت الضرورة ذلك.

ومن جهتها، أطلقت دولة الكويت في 14 / 01 / 2003 موقع بوابة حكومتها الإلكترونية، ليكون المدخل الرئيسي نحو تقديم جميع الخدمات الحكومية في شتى المجالات للمواطن والمقيم على حد سواء.

صفوة القول: إن التنسيق بين الإدارات الحكومية والمرافق العامة وتشجيع نقل وتحويل وتبادل المعلومات، والسعي إلى توحيد النماذج التقنية المعتمدة، واقتراح المواصفات الموحدة يؤدي إلى الارتقاء في أداء خدماتها لجمهور المتعاملين معها، بأسلوب متطور ويرفع كفاءة أدائها، للوصول إلى شعور العميل أو طالب الخدمة بالرضا عن الخدمات التي يطلبها من الجهاز الإداري، من ناحية حصوله على الخدمة بسرعة ومرونة في الإجراءات، وجودة وكفاءة عالية في نوعية الخدمة بصورة تكفل الارتقاء بالخدمات وتساعد على توفير الثقة لدى الجمهور في استخدام وسائل التعامل مع الحكومة الإلكترونية (Customer Loyalty)[1].

2. الارتقاء من خلال تحقيق الشفافية الإدارية:

تعمل الإدارة العامة الإلكترونية على إرساء قواعد الشفافية في توفير المعلومات بسهولة، وكذلك في الحصول عليها، وهذا أمر يؤدي إلى تعزيز روح الديمقراطية الإدارية، ويساهم في تطوير العلاقة بين سلطات الدولة وإداراتها العامة، كما أن من شأنه أن يؤدي إلى تعاون أفضل في نشر المعلومات التي تساعد المختصين على إصدار القرارات السليمة. وتعمل الشفافية في مجال المعلومات على تجاوز المفاهيم القديمة التي تنطلق من قاعدة أن كل معلومة سرية ما لم يشر إليها بغير ذلك، وأن الملفات والوثائق الإدارية تعد مملوكة للإدارة ملكية خاصة، ومن ثم لا يجوز لأحد أن يطلع عليها ، إمعاناً في الالتزام بعدم إفشاء المعلومات السرية التي يحصل عليها الموظف بمناسبة وظيفته. وقد أطلق على هذا الالتزام بالفرنسية La discretion professionnelle أي: الالتزام بالكتمان الذي يمنع الموظفين من نشر بيانات عن أعمالهم دون تصريح بذلك. بيد أن ثورة المعلومات والاتصالات أدت إلى اعتبار السرية مجرد ميراث تاريخي للإدارة، وأن مواكبة هذه الثورة تستدعي العمل من خلال إدارة من زجاج Administration de Verre تتحول فيها العلاقة بين الإدارات العامة والجمهور إلى علاقة شفافية ونقاء بدلاً من السرية والعتامة واللاشفافية.

(1) انظر: د. داود عبد الرازق الباز، المرجع السابق ص241.

إن الشفافية تعد مبدأ أساسياً في إتمام كل المعاملات الحكومية، وهي من المزايا المهمة التي يوفرها نظام الحكومة الإلكترونية، ومعنى ذلك أن علاقة الإدارة الحكومية بالجمهور تتحول في ظل الشفافية إلى علاقة تشاور وتناغم، ترسي دعائم الديمقراطية الإدارية التي تتيح للجمهور مشاركته للإدارة فيما تقوم به من أعمال، وحقه في فهم تصرفاتها ما دام بإمكانه الاطلاع على وثائقها وأسباب قراراتها التي يسوغها انفتاح الإدارة على الجمهور، ولكن مع احترام الحق في الحياة الخاصة للأفراد وعدم نشر المعلومات المتعلقة بأسرارهم الفردية وقضايا أحوالهم الشخصية وسندات الملكية للأراضي، وهذه الفكرة يصبح طرحها في ظل تطبيق الإدارة العامة الإلكترونية أكثر حضوراً في أذهان رجال القانون ولدى الجمهور الواعي المتعامل مع الإدارات الحكومية[1].

(54) ثانياً – تأثير الحوكمة على الحياة الخاصة والشفافية:

لم يهتم القانون ولا القضاء بتحديد معنى الحياة الخاصة بسبب صعوبة تعريفها من جهة ونسبية فكرتها من جهة أخرى، حيث تتباين بتباين الناس وبيئاتهم وثقافاتهم وانتماءاتهم الدينية والسياسية والاجتماعية. ومع ذلك فقد حاول جانب من الفقه الفرنسي تعريفها بأنها (كل ما ليس له علاقة بالحياة العامة، أو هي كل ما لا يعد من قبيل الحياة العامة للإنسان). ويركز هذا التعريف السلبي على الاهتمام بخصوصية الحياة في المقام الأول[2]. وقد أدى التطور العلمي والتكنولوجي في عصرنا الحاضر إلى حدوث قلق متزايد بشأن الخصوصية ومدى تهديد حرمة الحياة الخاصة في ظل عصر المعلومات، ووسائل الاتصالات المتقدمة ولاسيما الإنترنت، وينطوي ذلك القلق على تساؤلات عديدة أهمها، مدى التعارض بين المزيد من الشفافية الذي يتوقع من الحكومة الإلكترونية مع حماية الخصوصية أو البيانات السرية للأفراد والمعلومات المالية والوظيفية وما يماثلها، كالسيرة الاجتماعية والصحية والسياسية.

إن الحاسوب الذي لا يمكن وضع حد لشراهته في جمع المعلومات، وما عرف عنه من دقة وعدم نسيان، قد تنقلب معه الحياة رأساً على عقب، بحيث يخضع الأفراد فيه لنظام رقابي مشدد، ويتحول المجتمع بواسطته إلى عالم شفاف، تصبح فيه بيوت الناس ومعاملاتهم اليومية وحالتهم العقلية والجسمانية عارية لأي مشاهد. وكما قيل، فقد أصبح الفرد أمام تقنية الاتصالات والمعلومات كتاباً مفتوحاً، وهذا قد يؤدي إلى إساءة استخدام المعلومات الشخصية على نحو يجعل الخصوصيات محلاً للإشاعات والثرثرة.

(1) انظر: د. داود عبد الرازق الباز، المرجع السابق ص252–249.

(2) انظر: د. داود عبد الرازق الباز، المرجع السابق، ص253.

الآثار القانونية قصيرة وطويلة المدى لاستخدام تكنولوجيا المعلومات في الإدارة:

سياسة الإدارة وتكنولوجيا المعلومة:

يتمثل الهدف الأبرز لتطوير خدمات الحكومة الإلكترونية بالسويد في جعل الإدارة أكثر تمركزاً حول المواطن، وتتضمن الأهداف الأخرى أشكالاً جديدة من التفاعل الديمقراطي للمواطنين.

حماية السرية للبيانات الشخصية:

تتمتع السرية من الناحية الإدارية بحماية بموجب قانون البيانات الشخصية، الذي ينطبق على جميع قطاعات المجتمع. وبشكل عام فإن السويديين لا يهتمون كثيراً بمخاطر السرية، ولم تكن المخاوف المتعلقة بالسرية عائقاً أمام تقدم الحكومة الإلكترونية، إلا أن هناك بعض المشاكل في نظم السرية التي تمت مواجهتها لعدم توافق الأنواع المختلفة لقوانين السرية، فبعضها يتعلق بالإدارات والبعض الآخر يتعلق بالمعلومات نفسها. ومن أجل تسهيل الخدمات المتقدمة بين الإدارات المختلفة، سيكون من الضروري إصلاح قوانين السرية، إذ يجب أن تقوم نظم جديدة بتحديد الإدارة المسؤولة عن معلومات معينة، وكيفية المشاركة في هذه المعلومات[1]. ومن بين أحد المجالات التي تحدث فيها مثل هذه المشاكل هو موضوع السرية، وفقاً لقانون السرية الرسمي، فإن المعلومات السرية في إحدى الإدارات ستكون بالضرورة سرية عندما تنتقل إلى إدارة أخرى، وبالتالي فإنه يمكن أن يكون هذا البند والبنود المشابهة عوائق أمام استخدامات تكنولوجيا المعلومات المرغوبة تكنولوجياً وسياسياً[2].

وفي القرن الحادي والعشرين ستكون الخصوصية بالنسبة لمجتمع المعلومات مصدر إلحاح في طلب حمايتها، وعلى الرغم من الحماس الذي يحيط بمناقشة موضوع الخصوصية، وعلى الرغم من أن المعلومات قد أضحت هي شريان الحياة في عصرنا الحالي، فإن الحكومة الإلكترونية يصعب – إن لم تنعدم – الاستفادة منها أو تحقيق أهدافها دون إمكانية تبادل البيانات والمعلومات بين إدارات المرافق العامة وغيرها من الإدارات الخاصة[3]. لكن موضوع الحماية والسرية للبيانات الخاصة يبدو أكثر طلباً عندما يعهد إلى غير الموظفين في الإدارات الحكومية بإدارة الأنظمة المعلوماتية– إدارة غير مباشرة لمرفق عام – التي تجمع البيانات والمعلومات الشخصية عن الأفراد، مما يزيد من دواعي القلق والتهديد للحياة الخاصة. وفي رأي بعض الفقهاء، فإن مقتضيات تطبيق نظام الحكومة الإلكترونية سوف تفرض

(1) غوستاف جونسون، الحكومة الإلكترونية والقانون الإداري، مؤتمر الكويت حول الحكومة الإلكترونية 13–15 أكتوبر 2003 ، ص 4 – 5

(2) غوستاف جونسون، المرجع السابق، ص 6.

(3) انظر: د. داود عبد الرازق الباز، المرجع السابق ص254–253

إصدار قوانين تحكم نشاطات الحكومة الإلكترونية، وتجيز التعامل بها في إطار قانوني مضمون للمعاملات الإلكترونية على نحو يوفِّر الثقة واليقين، ويضمن أن تعمل التطورات التكنولوجية على خدمة المستفيدين من المرافق العامة أو طالبي الاستفادة، على أن تكفل هذه القوانين حماية الحياة الخاصة بشكل حازم وفعال، وتتسم بالصرامة والشدة في هذا المجال[1].

(55) ثالثاً– الحق في المعرفة وتقويض السرية في الإدارة:

الحقيقة أن التفاعل بين الواقع والقانون واستجابة النظام القانوني لأصداء التطور التكنولوجي الهائل هو الذي ألقى بظلاله ونتائجه على علاقة الإدارات الحكومية بالجمهور، وتبديلها من علاقة سرية إلى علاقة شفافية، إذ من الثابت أن نجاح النظام القانوني إنما يكون رهيناً بمدى استجابته لأصداء ذلك التطور. ولا شك أن هناك متطلبات خاصة من القانون إزاء الإجراءات الإدارية المتعلقة بتكنولوجيا المعلومات من أجل ضمان توفير الشفافية الكافية لعل أهمها:

أ) الحق في المعرفة الذي يركز على حق المواطنين في معرفة ما تنوي حكومتهم عمله عن طريق كفالة حرية المعلومات، وإتاحة أنشطة الحكومة بصورة مفتوحة أمام العين الثاقبة للتدقيق العام. ويعد انفتاح المعلومات عرفاً قديماً في السويد، وقد تم سن القانون الأول الخاص بإمكانية الاطلاع على المستندات العامة في عام 1766، وعلى مر السنين تم تعديل البنية القانونية التي تحكم الانفتاح والوصول إلى المستندات العامة بشكل فاعل لتلائم التكنولوجيا الحديثة، وليواكب التطور القانوني التطور التكنولوجي من أجل تحقيق الشفافية في الإدارات، وتأهيل المواطنين وإمدادهم بالمعرفة ليحيوا حياة ديمقراطية.

وفي فرنسا، يعود بداية التحول نحو شفافية الإدارة في فرنسا إلى عهد الرئيس فاليري جيسكار ديستان، الذي كان يضمر عداء للسرية في أعمال الإدارة على نحو جعل من هدف تحسين العلاقة بين الإدارة والجمهور محلاً لاهتمام كبير في سياسة الحكومة وأعمالها. ورويداً رويداً ومن خلال السلطة التشريعية الفرنسية، تم تقويض مجتمع السرية وإحلال الشفافية محل مبدأ السرية، وقلب القاعدة التقليدية بجعل العلم أو الحق في المعرفة أو المعلوماتية Droit a I'information هو المبدأ الرئيسي الذي يحكم علاقة الإدارة بالجمهور، ويجعلها إدارة تعمل في وضح النهار، حتى يتسنى للمواطنين المشاركة فيما تتخذه الإدارة من قرارات تمس مصالحهم، فضلاً عن تمكينهم من الدفاع عن حقوقهم، والاعتراض على ما يعد انتهاكاً لحرمة حياتهم الخاصة.

(1) انظر: د. داود عبد الرازق الباز، المرجع السابق ص258–255

ب) الحق في رقابة الحكومة ومن خلال مشاركة الجمهور في الحصول على المعلومات والاطلاع على سير العمل في الإدارات: يتضح بجلاء أثر الحكومة الإلكترونية في القضاء على السرية التي جذَّرت البيروقراطية في أعمال الإدارة، وفوَّتَت على الشعوب حقها في فرض رقابتها على حكوماتها، فمن خلال الحكومة الإلكترونية يمكن لأي متعامل مع الإدارات أن يدخل إلى الموقع الإلكتروني للحكومة، الذي يوفر له المعلومات بسهولة تأكيداً لعلاقة الانفتاح بين الإدارة والجمهور التي تجعل الإعلام هو الأصل أو القاعدة، والسرية وانعدام الشفافية هي الاستثناء.

ت) معرفة سير إجراءات إنجاز المعاملات: كما يمكن للمتعامل مع الإدارة أن يعرف أين تقف معاملته ؟ وما الإجراءات التي مرت بها ؟ وهل توجد صعوبات في تنفيذها أم لا ؟

وأخيراً– الشفافية تطبيق لمبادئ العدالة والمساواة وتكافؤ الفرص: إن الحكومة الإلكترونية تكفل درجة عالية من الشفافية إن لم تكن الشفافية بعينها على حد تعبير البعض، وذلك بتعزيزها لتطبيق مبدأ العدالة أو المساواة وتكافؤ الفرص، فالجميع متساوون في اتباع إجراءات الحصول على الخدمات الحكومية، ومن ثم يتم القضاء على الواسطة والمحسوبية والفساد والرشوة، أو التقليل من آثارها وخاصة في مجال التعيين والترقية. وتحرص الدول المتقدمة على الأخذ بالوسائل التي تكفل المساواة في شغل الوظائف العامة إدراكاً منها لحقيقة أن هذا المبدأ يعد أساس الديمقراطية الإدارية، كما يعد الاقتراع العام أساس الديمقراطية السياسية. أما الدول النامية، فعليها توجيه اهتماماتها الجدية نحو الإدارة العامة الإلكترونية، لا لغرض تحسين الخدمات الحكومية فقط، بل للقضاء على الفساد من خلال زيادة الشفافية وإرشاد الجمهور للتعامل السليم مع المرافق العامة. ولا شك أن ذلك يدعم الاتجاه المتزايد نحو تطبيق نظام الصلاحية والجدارة في شغل الوظائف والقيام بأداء مهامها المتغيرة باستمرار نتيجة ثورة الاتصالات التي يمر بها عالمنا اليوم، والتي تستلزم الاستعانة بموظفين ذوي عقول مفكرة، يمكنها أن تواجه تحديات التطور التكنولوجي الديناميكي[1].

(1) انظر: د. داود عبد الرازق الباز، المرجع السابق، ص259 وما بعدها .

المطلب الثاني
التحولات والمشكلات المتعلقة بالقانون الدول في علاقته بالقانون الجنائي والحق في المعلومات والحق في الأمن والخصوصية

الفرع الأول
التنسيق على مستوى القانون الدولي

(56) رؤية المجلس الأوروبي في شأن الجريمة الإلكترونية:

قدم مجلس أوروبا مجموعة من المعاهدات الأوروبية من أهمها الاتفاقية المتعلقة بالجريمة الإلكترونية بتاريخ 23/11/2001، وقد عبرت ديباجة الاتفاقية عن رؤية المجلس في هذا الخصوص كما يلي:

«إن الدول الأعضاء بمجلس أوروبا وغيرها من الدول الأخرى الموقعة على هذه الاتفاقية:

أخذاً في الاعتبار أن هدف مجلس أوروبا هو تحقيق الوحدة الكبرى بين أعضائه، واعترافاً بقيمة دعم التعاون مع الدول الأخرى أطراف هذه الاتفاقية، واقتناعاً بضرورة الحاجة إلى اتباع سياسة جنائية مشتركة كمسألة أولوية – تهدف إلى حماية المجتمع ضد الجريمة الإلكترونية، وذلك من خلال عدة أمور منها: إقرار التشريع الملائم ودعم التعاون الدولي، وإدراكاً لعمق التغييرات التي أحدثتها عمليات الترقيم والتقارب واستمرار عولمة شبكات الكمبيوتر، واهتماماً بمخاطر إمكانية استخدام شبكات الكمبيوتر والمعلومات الإلكترونية كذلك في ارتكاب جرائم جنائية، وأن الأدلة المتعلقة بمثل هذه الجرائم يمكن تخزينها ونقلها عبر هذه الشبكات، واعترافاً بالحاجة إلى التعاون بين الدول والكيانات الصناعية الخاصة في مكافحة الجريمة الإلكترونية، والحاجة لحماية المصالح المشروعة في استخدام وتطوير تكنولوجيا المعلومات، وإيمانا بأن المكافحة الفعالة للجريمة الإلكترونية تستلزم زيادة وسرعة وتفعيل التعاون الدولي في المسائل الجنائية، واقتناعاً بأن هذه الاتفاقية لازمة لردع أعمال الاعتداء الموجهة ضد سرية وسلامة وإتاحة نظم الكمبيوتر، والشبكات، وبيانات الكمبيوتر، وكذلك ردع إساءة استخدام مثل هذه النظم، والشبكات والبيانات، وذلك بالنص على تجريم مثل هذا السلوك كما هو مبين بهذه الاتفاقية، وإقرار الصلاحيات الكافية من أجل مكافحة فعالة لمثل هذه الجرائم الجنائية، عن طريق تسهيل كشفها، والتحقيق فيها والمحاكمة

بشأنها على المستويين المحلي والدولي، وكذلك عن طريق توفير الترتيبات من أجل تحقيق التعاون الدولي العاجل والموثوق به،

وحرصاً من جانبها على ضرورة ضمان وجود توازن ملائم بين مصالح تنفيذ القانون واحترام حقوق الإنسان الأساسية، كما هو منصوص عليه في اتفاقية مجلس أوروبا لعام 1950 بشأن حماية حقوق الإنسان والحريات الأساسية، والعهد الدولي للأمم المتحدة لعام 1966 بشأن الحقوق المدنية والسياسية، والمعاهدات الدولية الأخرى واجبة التطبيق بشأن حقوق الإنسان، التي تؤكد على حق كل فرد في التعبير عن رأيه دون أي تدخل، وكذلك الحق في حرية التعبير – بما في ذلك حرية البحث، وتلقي ونقل المعلومات والأفكار في شتى المجالات، بغض النظر عن الحدود والحقوق المتعلقة باحترام الخصوصية. وحرصاً من جانبها كذلك على حق حماية البيانات الشخصية، مثلما تم التباحث بشأن ذلك – على سبيل المثال – بموجب اتفاقية مجلس أوروبا لعام 1981 بشأن حماية الأفراد عند المعالجة الآلية للبيانات الشخصية، واهتماماً من جانبها باتفاقية الأمم المتحدة لعام 1989 بشأن حقوق الطفل، واتفاقية منظمة العمل الدولية لعام 1999 بشأن أسوأ صور عمل الأطفال.

وأخذاً في الاعتبار اتفاقيات مجلس أوروبا القائمة بشأن التعاون في المجال الجنائي، وكذلك المعاهدات المماثلة القائمة فيما بين الدول الأعضاء بمجلس أوروبا والدول الأخرى، وتركيزاً من جانبها على أن الاتفاقية الحالية الغرض منها استكمال تلك الاتفاقيات من أجل جعل التحقيقات والإجراءات الجنائية المتعلقة بالجرائم الخاصة بنظم وبيانات الكمبيوتر أكثر فعالية، والتمكين من جمع أدلة الجرائم الجنائية التي تمت في شكل إلكتروني، وترحيباً من جانبها بالتطورات الأخيرة التي تدفع بالتفاهم والتعاون الدوليين في مجال مكافحة الجريمة الإلكترونية – بما في ذلك الإجراءات التي تتخذها الأمم المتحدة ، ومنظمة والتعاون الاقتصادي والتنمية ، والاتحاد الأوروبي، ومجموعة الدول الصناعية الثمانية، وإحياء لتوصيات لجنة الوزراء رقم (R (85) 10) الخاصة بالتطبيق العملي للاتفاقية الأوروبية بشأن المساعدة المتبادلة في المسائل الجنائية فيما يتعلق بالإنابة القضائية بشأن اعتراض الاتصالات السلكية واللاسلكية، ورقم (R (88) 2) بشأن القرصنة في مجال حقوق النشر والتأليف والحقوق المجاورة، ورقم (R (87) 15) التي تنظم استخدام البيانات الشخصية في قطاع الشرطة، ورقم (R (95) 4) بشأن حماية البيانات الشخصية في مجال خدمات الاتصالات، وتشير بصفة خاصة للخدمات التليفونية، وكذلك رقم (R (89) 9) بشأن الجرائم المتعلقة بالكمبيوتر التي تقدم الإرشادات للهيئات التشريعية الوطنية، فيما يتعلق بتعريف جرائم معينة تتعلق بالكمبيوتر، ورقم(R (95)13) التي تتعلق بمشكلات قانون الإجراءات الجنائية ذات الصلة بتكنولوجيا المعلومات.

وبعد النظر في القرار رقم (1) الذي أقره وزراء العدل الأوروبيون في مؤتمرهم الواحد والعشرين (براغ 10 – 11 يونيو 1997) الذي أوصى بقيام لجنة الوزراء بدعم العمل الخاص بالجريمة الإلكترونية، والذي تتولى اللجنة الأوروبية القيام به وتنفيذه فيما يتعلق بالمشكلات الخاصة بالجريمة، وذلك لجعل نصوص القوانين الجنائية المحلية أكثر قرباً من بعضها البعض، والتمكن من استخدام الوسائل الفعالة للتحقيق والبحث في مثل هذه الجرائم، وكذلك القرار رقم (3) الذي أقره المؤتمر الثاني والعشرون لوزراء العدل الأوروبيين (لندن 8– ، 9 يونيو 2000) الذي شجع أطراف المفاوضات على متابعة جهودهم بغرض إيجاد الحلول الملائمة، حتى يتمكن أكبر عدد ممكن من الدول أن تصبح أطرافاً في الاتفاقية، وأقر بضرورة الحاجة إلى منظومة تعاون دولي تتسم بالمرونة والفعالية، وتأخذ على عاتقها – على نحو ملائم – النصوص المحددة بشأن مكافحة الجريمة الإلكترونية.

وبعد النظر كذلك في خطة العمل التي أقرها رؤساء دول وحكومات الدول الأعضاء بمجلس أوروبا بمناسبة عقد القمة الثانية لهم (ستراسبورج 10–11 أكتوبر 1997) لإيجاد استجابات مشتركة التطوير تكنولوجيا المعلومات الحديثة وفقاً لمعايير وقيم مجلس أوروبا، قد اتفقت على ما يلي (نصوص الاتفاقية).

(57) ضرورة وجود توافق دولي محكم في مجال الحق في المعلومات:

– تنشأ ضرورة وجود توافق دولي محكم في مجال الحق في المعلومات، على وجه الخصوص من سهولة حركة المعلومات في أنظمة تقنية المعلومات، وتجعل هذه السهولة لحركة المعلومات بالإمكان ارتكاب جريمة عن طريق حاسب آلي موجود في دولة معينة، بينما يتحقق نجاح الفعل الإجرامي في دولة أخرى، وتستلزم مثل هذه الجرائم تعاوناً دولياً فعالاً– والذي يعد ضرورياً – من أجل حماية حقيقية لأنظمة الاتصالات البعدية من الاستخدام غير المشروع في التجسس والإرهاب والجريمة المنظمة التي تعبر العديد من الدول، ويبرر أيضاً وجود قانون دولي ينظم تصدير برامج تقنية المعلومات إلى الخارج[1].

– وينشأ حتماً عن أوجه الخلاف بين القوانين الوطنية والخاصة بإجرام تقنية المعلومات ما يعرف بـ «المعلومات المختبئة» أو «جرائم الكمبيوتر المختبئة»، والتي ستكون لها نتيجة عكسية في صورة قيود وطنية على حرية حركة المعلومات، ولن تقتصر هذه العقبات الوطنية على المنشآت فقط، والتي تريد إعاقة تصدير برامج تقنية المعلومات إلى الدول،

(1) انظر: Dr. UlrichSieber، تحليل لموضوع: جرائم الكمبيوتر والجرائم الأخرى في مجال تكنولوجيا المعلومات، المرجع السابق، ص 58

والتي لا توجد بها أي حماية قانونية للبرامج، وسيكون أيضاً لأوجه الخلاف بين القوانين الوطنية نتيجة أخرى مؤداها أن الدول التي تتمتع بمستوى أعلى من الحماية سوف تحد من تدفق البيانات إلى الدول ذات نظام حماية أقل تطوراً[1].

– وتوجد اليوم قيود في العديد من الأنظمة القانونية على «تصدير المعلومات الاسمية»، ومع ذلك فإن مثل هذه القيود، وكذلك تدابير المراقبة الوطنية تعرض للخطر الحق في احترام الحياة الخاصة وأسرار الصفقات التجارية للمنشآت، وأيضاً النمو الاقتصادي للسوق الدولي للمعلومات، ويمكن أن تؤدي أيضاً إلى تفاوت في المنافسة[2].

(58) القيود الوطنية على نقل المعلومات وعلى مواقع التواصل الاجتماعي ومواقع شبكات الاتصال الدولية:

تظل الحلول والقيود الوطنية محكوماً عليها بالفشل، حيث يمكن نقل البيانات المرقمة عالمياً في بضعة ثواني عن طريق شبكات الاتصالات البعدية والتليفونية، ويبقى أيضاً من المستحيل إجراء مراقبة عبر الحدود لكل الشرائط المغنطة والاسطوانات ودوائر المعالجة الميكروية والتي تكون مخصصة لدولة أجنبية، وحركة تحرير دول أوروبا الشرقية في السنوات الماضية والتي حدثت على نطاق واسع عن طريق نقل المعلومات من الغرب، تشير بوضوح جداً إلى «حرية المعلومات»، والتي قليلاً ما تخضع لرقابة الدولة. ولا يمكن لأي مجتمع حر أن يتخلى عن الاتفاقات الدولية في مجال الحق في المعلومات، ومرد ذلك سهولة حركة المعلومات وعدم التحكم في مراقبتها[3].

(59) في مجال الإجراءات على المستوى الدولي:

فإن التوافق بين مختلف سلطات التدخل الوطنية، سيكون هاماً من أجل تيسير طلب المساعدة القانونية الوطنية، لأنه قد تلتمس إحدى الدول المساعدة القضائية من دولة أخرى، بحيث يمكن لهذه الأخيرة أن تباشر التدابير التي تكون مقبولة طبقاً لقوانينها الخاصة، وفي التجمعات الثقافية والاقتصادية كما هو الحال في أوروبا، فان التوافق على المدى البعيد على أساليب القسر الإجرائية يمكن أن يجعل الإجراءات المعقدة لقاضي

(1) انظر: Dr. UlrichSieber، تحليل لموضوع: جرائم الكمبيوتر والجرائم الأخرى في مجال تكنولوجيا المعلومات، المرجع السابق، ص 59

(2) انظر: Dr. UlrichSieber ، تحليل لموضوع : جرائم الكمبيوتر والجرائم الأخرى في مجال تكنولوجيا المعلومات، المرجع السابق، ص 59

(3) انظر: Dr. UlrichSieber ، تحليل لموضوع: جرائم الكمبيوتر والجرائم الأخرى في مجال تكنولوجيا المعلومات، المرجع السابق، ص 60–59

أوروبا في المستقبل أو لأي قاضى دولي مماثل ومعترف به غير مجدية [1] والذي سيكون له نفس القيمة التي للسلطة الوطنية[2].

وجاءت المادتان (23 – 24) من الفصل الأول «مبادئ عامة تتعلق بالتعاون الدولي» والباب الأول في «مبادئ عامة»– القسم الثالث من الاتفاقية تحت عنوان «التعاون الدولي». وتنص المادة 23 على أن :«مبادئ عامة تتعلق بالتعاون الدولي: يتعاون الأطراف مع بعضهم البعض، وفقاً لنصوص هذا الباب، ومن خلال تطبيق الاتفاقيات الدولية ذات الصلة والخاصة بالتعاون الدولي في الشؤون الجنائية والترتيبات المتفق عليها بمقتضى التشريعات الموحدة والمتبادلة بالمثل، والقوانين الوطنية، لأقصى درجة ممكنة لأغراض إجراءات التحقيقات التي تتعلق بجرائم نظم وبيانات الكمبيوتر، أو من أجل تجميع أدلة الجريمة الجنائية في شكل إلكتروني». وجاء الفصل الثاني في: «مبادئ تتعلق بتسليم المجرمين»[3]:

(60) دور المنظمات الدولية في تحقيق التوافق الدولي في مجال الحق في المعلومات والحق في الخصوصية:

لقد بلغ التوافق الدولي للحق في المعلومات اليوم مرتبة عليا، وذلك بفضل المبادرات المبكرة لمختلف المنظمات الدولية كمنظمة التعاون والتنمية الاقتصادية، والجماعة الأوروبية، والمجلس الأوروبي، والمنظمة الغربية للمعلومات المعالجة، وقد ساهمت المنظمات سالفة الذكر كثيراً على وجه الخصوص في رقي مستوى التوافق حتى اليوم في مجال الحماية المدنية لبرامج تقنية المعلومات وللطبوغرافيا وفي مجال حماية الحياة الخاصة عن طريق القانون العام والقانون المدني، وأيضاً في مجال تدبير النصوص الجنائية الخاصة بالدعاوى المقامة ضد إجرام تقنية المعلومات[4]، وانتهاك الخصوصية وسيادة الدول.

(1) (Article (9), recognizes the rights to liberty and security of the Person. It prohibits arbitrary arrest and detention, requires any deprivation of liberty to be according to law, and obliges States Parties to allow those deprived of their liberty to challenge their imprisonment through the Courts. These provisions apply not just to those imprisoned as part of the criminal process, but also to those detained due to mental illness, drug addiction, or for educational or immigration purposes.
Article (9/3 and 9/4), impose procedural safeguards around arrest, requiring anyone arrested to be promptly informed of the charges against them, and to be brought promptly before a judge. It also restricts the use of pre-trial detention, requiring it to be imposed only in exceptional circumstances and for as short a period of time as possible.

(2) انظر: Dr. UlrichSieber، تحليل لموضوع: جرائم الكمبيوتر والجرائم الأخرى في مجال تكنولوجيا المعلومات، المرجع السابق، ص 60

(3) انظر: د. إيهاب السنباطي، الترجمة الجديدة والكاملة للاتفاقية المتعلقة بالجريمة الإلكترونية (بودابست 2001) والبروتوكول الملحق بها ، دار النهضة العربية ، 2008 – 2009

(4) انظر: Dr. UlrichSieber، تحليل لموضوع: جرائم الكمبيوتر والجرائم الأخرى في مجال تكنولوجيا المعلومات، المرجع السابق، ص 60

(61) ضرورة إحداث توافقات جديدة في المستقبل بشأن الحق في الخصوصية:

وسيكون من الضروري إحداث توافقات جديدة في المستقبل بشأن الحق في الخصوصية، وعلاوة على ذلك فإن الأنشطة الدولية الموجودة من قبل، والتدابير المستقبلية، يجب أن تركز كل منها على المحاور الثلاثة الآتية:

أولاً: من الأهمية بسط التعاون الدولي إلى المجالات المستحدثة[1]، والتي على وشك أن يبدأ فيها فقط التعاون الدولي ودراسات القانون المقارن، وعلى وجه الخصوص الحماية الجنائية للحق العام في الشخصية (والحقوق اللصيقة بالشخصية)، وأيضاً المسائل الخاصة بتقنية المعلومات في قانون الإجراءات[2].

ثانياً: يجب توسيع أساس التوافق الدولي، والذي سبق الحصول عليه، ويلاحظ أنه وإلى وقتنا الحالي، فإن المبادرات من أجل توافق الحق في المعلومات تصدر عن الأمم الصناعية، وعلى وجه الخصوص في مجال المنظمة الأوروبية للتعاون والتنمية الاقتصادية، والمجلس الأوربي، والتجمعات الأوروبية، وبالنظر إلى أن «المعلومات المختبئة» و«جرائم الكمبيوتر المختبئة» يمكن أن يكون مصدرها الدول التي في طريقها للتنمية، وأن البراهين من أجل توافق الحق في المعلومات تنطبق على جميع الدول، لذا يجب توسيع دائرة الأمم المساهمة، وهذا يمكن تحقيقه عن طريق عمل الأمم المتحدة في مجال الكفاح والوقاية من الجريمة، وقد سبق للمؤتمر الدولي الخاص بمنع ومحاكمة إجرام تقنية المعلومات، والذي انعقد بالاشتراك مع المؤتمر الدولي الثامن للأمم المتحدة في سبتمبر 1990 بهافانا، والخاص بالوقاية من الجريمة ومعاملة المذنبين[3]، أن منح دفعات قوية في هذا الشأن.

(وللبحث بقية)

(1) Article 1 (3) To achieve international co-operation in solving international problems of an economic, social, cultural, or humanitarian character, and in promoting and encouraging respect for human rights and for fundamental freedoms for all without distinction as to race, sex, language, or religion;

(2) انظر: Dr.UlrichSieber، تحليل لموضوع: جرائم الكمبيوتر والجرائم الأخرى في مجال تكنولوجيا المعلومات، المرجع السابق، ص 61–60.

(3) انظر: Dr.UlrichSieber، تحليل لموضوع: جرائم الكمبيوتر والجرائم الأخرى في مجال تكنولوجيا المعلومات، المرجع السابق، ص 61.

المراجع:

المراجع العربية:

1- د. أحمد فتحي سرور، الوسيط في قانون الإجراءات الجزائية، دار النهضة العربية، الطبعة السابعة 1993، القاهرة، مصر.

2- د. أحمد كمال أبو المجد، الإعلام وتدريس حقوق الإنسان، بحث مقدم إلى مؤتمر تعليم حقوق الإنسان، القاهرة 9/7/1987.

3- د. أسامة محمد محي الدين عوض، جرائم الكمبيوتر والجرائم الأخرى في مجال تكنولوجيا المعلومات، بحث مقدم إلى المؤتمر السادس للجمعية المصرية للقانون الجنائي، القاهرة 25-28 أكتوبر 1993، مصر.

4- د. إيهاب السنباطي، الترجمة الجديدة والكاملة للاتفاقية المتعلقة بالجريمة الإلكترونية (بودابست 2001) والبروتوكول الملحق بها، دار النهضة العربية 2008 - 2009، القاهرة، مصر.

5- د. ثروت بدوي، النظم السياسية، دار النهضة العربية، طبعة 1986 القاهرة، مصر.

6- د. جعفر عبد السلام، الإطار التشريعي للنشاط الإعلامي، دار المنار للطبع والنشر والتوزيع، 1414 هـ، 1993 م.

7- د. حسام الدين كامل الأهواني، الحماية القانونية للحياة الخاصة في مواجهة الحاسب الآلي، بحث منشور بأعمال مؤتمر الكويت الأول للقانون والحاسب الإلكتروني، المنعقد في 4-7 نوفمبر 1989، كلية الحقوق، جامعة الكويت، منشورات مؤسسة الكويت للتقدم العلمي 1994.

8- د. داود عبد الرازق الباز، الإدارة العامة (الحكومة) الإلكترونية، وأثرها على النظام القانوني المرفق العام وأعمال موظفيه، مجلس النشر العلمي - جامعة الكويت 2004.

9- سعاد الشرقاوي، الاستفادة من تكامل مناهج تدريس حقوق الإنسان في كليات الحقوق، بحث مقدم إلى مؤتمر تعليم حقوق الإنسان، كلية الحقوق جامعة القاهرة من 9-11 يونيو سنة 1987.

10- د. سعد صالح شكطي نجم الجبوري، الجرائم الإرهابية في القانون الجنائي، دار الجامعة الجديدة 2013، الإسكندرية، مصر.

11- د.سعيد عبد اللطيف إسماعيل، الحماية الجنائية للسرية المصرفية في القانون المقارن،

دار النهضة العربية 1999، القاهرة، مصر.

12- د. طعيمة الجرف، مبدأ المشروعية وضوابط خضوع الدولة للقانون، دار النهضة العربية، الطبعة الثالثة 1976، القاهرة، مصر.

13- د. طوني ميشال عيسى، الركائز القانونية والتنظيمية للإدارة الإلكترونية، مؤتمر الكويت حول الحكومة الإلكترونية 13-15 أكتوبر 2003، الكويت.

14- د. عبد الأحد جمال الدين، في الشرعية الجنائية، بحث منشور بمجلة العلوم القانونية والاقتصادية، السنة 16، العدد الثاني، يوليو 1974، جامعة القاهرة، مصر.

15- بيل جيتس، المعلوماتية بعد الإنترنت، ترجمة عبد السلام رضوان، الإصدار 231 من سلسلة عالم المعرفة، الكويت.

16- عبدالله حسين علي محمود، سرقة المعلومات المخزنة في الحاسب الآلي، دار النهضة العربية، القاهرة، مصر.

17- د. عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية، بدون سنة نشر، القاهرة، مصر.

18- د. علي عبدالقادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، دار الجامعة الجديدة، سنة 2000، الإسكندرية، مصر.

19- علي عدنان الفيل، الإجرام الإلكتروني، منشورات زين الحقوقية، مكتبة زين الحقوقية والأدبية، الطبعة الأولى، سنة 2011، بيروت، لبنان.

20- د.عمر الفاروق الحسيني، تأملات في بعض صور الحماية الجنائية لبرامج الحاسب الآلي، منشور بأعمال مؤتمر الكويت الأول للقانون و الحاسب الآلي، المنعقد في الفترة من 4-7 نوفمبر 1989، الكويت.

21- د. غنام محمد غنام، دور قانون العقوبات في مكافحة جرائم الكمبيوتر والإنترنت وجرائم الاحتيال المنظم باستعمال شبكة الإنترنت، دار الفكر والقانون، سنة 2013، المنصورة، مصر.

22- غوستاف جونسون، الحكومة الإلكترونية والقانون الإداري، مؤتمر الكويت حول الحكومة الإلكترونية 13-15اكتوبر 2003 ، الكويت.

23- د. كاظم السيد عطية، الحماية الجنائية لحق المتهم في الخصوصية: دراسة مقارنة بين القانون المصري والفرنسي والإنجليزي، دار النهضة العربية، سنة 2007، القاهرة، مصر.

24– د. محمد أبو العلا، عقيدة مراقبة المحدثات التيلفونية، دراسة مقارنه في تشريعات الولايات المتحدة الأمريكية وإنجلترا وإيطاليا وفرنسا ومصر، دار النهضة العربية، الطبعة الثانية، سنة 2008، القاهرة، مصر.

25– د. محمد الشناوي، مكافحة جرائم النصب المستحدثة، الطبعة الأولى، دار البيان، سنة 2006

26– د. محمد الفيلي، العلاقة بين القانون والحكومة الإلكترونية، مؤتمر الكويت حول الحكومة الإلكترونية 13–15 أكتوبر 2003.

27– د. محمد حسام محمود لطفي، الحماية القانونية لبرامج الحاسب الآلي، دار النهضة العربية، القاهرة، مصر.

28– د. محمد محمد محمد عنب، استخدام التكنولوجيا الحديثة في الإثبات الجنائي، دار النهضة العربية سنة 2007، القاهرة، مصر.

29– د. محمد محي الدين عوض، مشكلات السياسة الجنائية المعاصرة في جرائم نظم المعلومات (الكمبيوتر)، بحث مقدم للمؤتمر السادس للجمعية المصرية للقانون الجنائي القاهرة 25–28 أكتوبر 1993، منشور في : مشكلات المسؤولية الجنائية في مجال الإضرار بالبيئة والجرائم الواقعة في مجال تكنولوجيا المعلومات، أعمال المؤتمر، دار النهضة العربية 1993، القاهرة، مصر.

30– د. محمود محمود مصطفى، شرح قانون الإجراءات الجنائية، مطبعة جامعة القاهرة والكتاب الجامعي، الطبعة الحادية عشرة 1976، القاهرة، مصر.

31– د. محمود نجيب حسني، تقرير مقدم إلى مؤتمر تعليم حقوق الإنسان الذي نظمته كلية الحقوق جامعة القاهرة في الفترة من 9/ 11 يونيه 1987.

32– د. نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية دراسة نظرية وتطبيقية ، منشورات الحلبي الحقوقية، بيروت، لبنان.

المراجع الأجنبية:

1. Adam Burton, Fixing FISA for Long War: Regulating Warrantless Surveillance in the Age of Terrorism, HEINONLINE, Citation: Pierce Law Review (Vol. 4, No. 2) - 2005-2006.
2. Cate Fred H., legal controls of internet information, research presented on Kuwait, first conference in legal and judicial

informatics, to modernize and develop the legal activities, organized by Ministry of Justice, State of Kuwait in cooperation with general secretarial of the Arab league, 15 – 17 Feb. 1999, Abstracts.

3. Emanuel Gross, The Struggle of a Democracy Against Terrorism – Protection of Human Rights: The Right to Privacy Versus the National Interest – the Proper Balance, HEINONLINE, Citation: Cornell International Law Journal (Vol. 37) 2004.
4. Frayssinet Jean, Effect of Information Automation on Privacy, Research Presented on Kuwait First Conference in legal and judicial informatics, to modernize and develop the legal activities, organized by Ministry of Justice, State of Kuwait in cooperation with general secretarial of the Arab league, 15 – 17 Feb. 1999, Abstracts.
5. Jones Richard, Legal Pluralism and facing Criminal Acts of internet , research presented on Kuwait, first conference in legal and judicial informatics, to modernize and develop the legal activities, organized by Ministry of Justice, State of Kuwait in cooperation with general secretarial of the Arab league, 15 – 17 Feb. 1999, Abstracts.
6. Karen E. Jones, The Effect of the Homeland Security Act on Online Privacy and the Freedom of Information Act, HEINONLINE, Citation: University of Cincinnati Law Review (Vol. 72) 2003-2004.
7. Lee A. Bygrave, Privacy Protection in a Global Context – A Comparative Overview, HEINONLINE, Citation: 47 Scandinavian Stud. L2004.
8. Lucas Andre, Protection of informatics Bases, Research Presented on Kuwait First Conference on Legal and Judicial informatics to Modernize and develop the legal activities, organized by Ministry of Justice, State of Kuwait in cooper-

ation with general secretarial of the Arab league, 15 – 17 Feb. 1999, Abstracts.

9. Merle Roger et Vitu Andre, Traite de Droit Criminel, Procedure Pénale, Edition CUJAS, Deuxieme Edition, Paris 1973, LEVASSEUER George et CHAVANNE Albert, Edition SIREY, 6e Edition Paris 1980
10. Robert N. Davis, Striking the Balance: National Security vs. Civil Liberties, HEINONLINE, Citation: 29 Brook. J. Int'l L.2003-2004
11. Tapper Coline F., Evedence and Computer, Paper Presented on Kuwait First Conference on Legal and Judicial informatics to Modernize and develop the legal activities, organized by Ministry of Justice, State of Kuwait in cooperation with general secretarial of the Arab league, 15 – 17 Feb. 1999, Abstracts
12. Thomas P. Ludwig, The Erosion of Online Privacy Rights in the Recent Tide of Terrorism, HEINONLINE, Citation: Computer Law Review and Technology Journal. (Vol. VIII).
13. Zachary W. Smith, Privacy and Security Post-Snowden: Surveillance Law and Policy in the United States and India, HEINONLINE, Citation: 9 Intercultural Hum. Rts. L. Rev. 2014.

المحتوى: