التَّهْدِيدَاتُ الِافْتِرَاضِيَّةُ لِلْأَمْنِ «السَّيبرَانيِّ» في الـمُناسَباتِ الرِّياضِيَّةِ

د. ياسر محمد عبد السلام رجب

أستاذ القانون العام المساعد - كلية الحقوق- جامعة القاهرة
المستشار القانوني بوزارة التنمية الإدارية والعمل والشؤون الاجتماعية -دولة قطر

التَّهْدِيدَاتُ الِافْتِرَاضِيَّةُ لِلْأَمْنِ «السَّيبَرانيّ» في المُناسَباتِ الرِّياضِيَّةِ

د. ياسر محمد عبد السلام رجب أستاذ القانون العام المساعد - كلية الحقوق- جامعة القاهرة
المستشار القانوني بوزارة التنمية الإدارية والعمل والشؤون الاجتماعية -دولة قطر

المُلخَّص

يُعد الأمن «السَّيبرانيّ» خيارًا حتميًا لجهة الإدارة، لا سيما في ظل تنامي التهديدات الأمنية «الإلكترونيّة»، سواء من جهة ارتفاع عدد الهجمات، أو الأضرار الناجمة عنها،وتتزايد أهمية التأمين «السَّيبرانيّ» في المناسبات الرياضيّة التي تتسم بزخم في الأعداد البشرية، وزخم في الفعاليات والمباريات، وتتعدد صور التهديدات «السَّيبرانيّة» في المناسبات الرياضية؛ كجرائم الاختراقات «الإلكترونيّة»، والجرائم المالية والاقتصادية «الإلكترونيّة»، وجرائم الإرهاب «الإلكترونيّ»، وجرائم اختراق النُّظم الأمنية لأغراض اقتصادية عبر «الإنترنت»؛ ومنها: استهداف محطات توليد الطاقة والماء،واستهداف البنية التحتية الاقتصادية،ونظم المواصلات، والاتصالات، والتهديد والترويع «الإلكترونيّ»،والاستيلاء على المعلومات التي يتم نقلها عبر شبكات المعلومات،وجرائم الاعتداء على بيانات الحكومة « الإلكترونيّة»،مما يستدعي مواجهة تلك التهديدات كلها أو جلها من خلال المواجهة الإدارية للتهديدات «السَّيبرانيّة» من جهة، و المواجهة التشريعية خلال تشريعات مستحدثة،وتفعيل ما يسمى باستراتيجية أمن المعلومات من جهة أخرى.

وعلاوة على ما تقدم من وسائل مواجهة تلك التهديدات مواجهة شاملة، هناك وسائل حديثة للضبط الإداري منها : تأمين الشّبكات على نحو يمنع من اختراقها، و تأهيل رجال الضبط والتحقيق الجنائي والمحاكمة في مكافحة جرائم «الإنترنت»، وثالثا: تأمين بيانات الحكومة «الإلكترونيّة» فنّيًا، من خلال وسائل الحماية الفنية لبيانات الحكومة «الإلكترونيّة»، كالجدار الناري أو حوائط المنع (Fire Walls)، ومكافحة الفيروس المعلوماتي.

الكلمات المفتاحية: الأمن السيبراني – الأمن المعلوماتي – الضبط الإداري الالكتروني– التهديدات السيبرانية – الجريمة السيبرانية – البيانات والمعلومات.

ABSTRACT

Potential threats to cybersecurity at sporting events

Dr. Yasser Mohammed Abdelsalam Ragab

Cyber security is an inevitable choice for the administration, especially in light of the growing electronic security threats, whether in terms of the high number of attacks or the damage caused by them. , And the importance of cybersecurity is increasing in sporting events that are characterized by momentum in human numbers and momentum in events and matches, and there are many forms of cyber threats in sporting events Such as cyber intrusion crimes, cyber financial and economic crimes, cyber terrorism crimes, breaches of security systems for economic purposes via the Internet such as targeting power and water plants, targeting economic infrastructure, transportation systems, communications, electronic threat and intimidation, and seizing information that is transmitted over networks Information and crimes against the government's electronic data, which necessitates facing all or all of these threats through administrative confrontation with cyber threats on the one hand, and besides that it is necessary to Legislative interface threats through innovative cyber legislation, and to activate the so-called information security strategy in terms .

In addition to what has been presented to confront these threats comprehensively, there are modern means of administrative control, including: securing networks in a way that prevents penetration, qualification of officers, criminal investigation and trial in combating cybercrime, and thirdly, securing e-government data technically through technical protection means for e-government data as an example Firewall or FireWall Prevention walls.

Key words: Cyber security - information security - electronic administrative enforcement authority - cyber threats - cyber crime - data and information

مقدمـة

إن تزايد حجم المعلومات المنتشرة على ساحة « الإنترنت»، وتصاعُد قيمتها بوصفها مصدرًا معرفيًا، واقتصاديًا، و سياسيًا، قد ألقى بظلاله على ميدان الأمن «السَّيبرانيّ»،مما نجم عنه حصول تغيير في أهداف عملية القرصنة المعلوماتية، التي كانت في بداياتها مجرد نزعة فضولية للوصول إلى معرفة جديدة، أو تحدي العقبات الأمنية التي تضعها الجهات الأخرى؛ لغرض الإحساس بنشوة النصر، ثم توجهت صوب استثمار هذه القدرات، وترجمتها إلى مكاسب مادية، أو سياسيَّة موجهة؛ حيث أضحت عملية الاختراق التي يقوم بها قرصان المعلومات تتسم بسوء قصد وتعمد .

من ناحية أخرى يُعد الأمن «السَّيبرانيّ» خيارًا حتميًا لجهة الإدارة؛ لا سيما في ظل تنامي التهديدات الأمنية « الإلكترونيّة» على مستوى الدول والمؤسسات العامة والحكومية والخاصة سواء من جهة ارتفاع عدد الهجمات أو الأضرار الناجمة عنها، وقد شهدت بلدان المنطقة بما في ذلك في دولة قطر في الآونة الأخيرة اختراقات مقلقة، وتتزايد أهمية التأمين «السَّيبرانيّ» في المناسبات الرياضية التي تتسم بزخم في الأعداد البشرية المتمثلة في جنسيات دولية من ناحية، وزخم في الفعاليات والمباريات من ناحية أخرى

وتتعدد صور التهديدات «السَّيبرانيّة» في المناسبات الرياضية، كجرائم الاختراقات «الإلكترونيّة»، وجرائم التجسس «الإلكترونيّ»، والجرائم المالية والاقتصادية «الإلكترونيّة»، وجرائم الإرهاب « الإلكترونيّ»،وجرائم الإرهاب والفتن الداخلية عبر «الإنترنت»،والجرائم العسكرية، وجرائم اختراق النظم الأمنية لأغراض اقتصادية عبر «الإنترنت»؛ ومنها: استهداف محطات توليد الطاقة والماء،واستهداف البنية التحتية الاقتصادية، ونظم المواصلات، والاتصالات، والتهديد والترويع «الإلكترونيّ»، والاستيلاء على المعلومات التي يتم نقلها عبر شبكات المعلومات،وجرائم الاعتداء على بيانات الحكومة «الإلكترونية»،مما يستدعي مواجهة تلك التهديدات كلها أو جلها من خلال المواجهة الإدارية للتهديدات «السَّيبرانيّة» من جهة، والمواجهة التشريعية للتهديدات «السَّيبرانيّة» و استراتيجية أمن المعلومات من جهة أخرى.

ويَستدعي ما تقدم التعرّض إلى الوسائل الحديثة للضبط الإداري؛ إذ أن هناك العديد من الوسائل الحديثة لمواجهة تلك التهديدات ومنها: تأمين الشّبكات على نحو يمنع من اختراقها،وتأمين بيانات الحكومة «الإلكترونيّة» فنيًّا، من خلال وسائل الحماية الفنية لبيانات الحكومة «الإلكترونيّة»، كالجدار الناري أو حوائط المنع (Fire Walls)، ومكافحة الفيروس المعلوماتي، وإلى جانب ذلك: لا بد من المواجهة التشريعية للتهديدات «السَّيبرانيّة»، من خلال تشريعات مُستحدثة،وتفعيل ما يسمى استراتيجية أمن المعلومات.

الدراسات السابقة:

تكاد تنعدم الدراسات السابقة في مجال الأمن «السَّيبرانيّ» من وجهة نظر القانون الإداري، وبخاصة في مجال الضبط الإداري والنشاط الإداري، إلا أنه قد توجد دراسات مُقارِبة، ولكن بشكل جزئي لمجال البحث، ومنها:

1- مُظفّر حسن الرزو :- الأمن المعلوماتي، معالجة قانونية أولية، مجلة الأمن والقانون، أكاديمية شرطة دبى، السنة (12)، العدد (1)، (2006).

2- يونس عرب،: قانون الكمبيوتر-موسوعة القانون وتقنية المعلومات، اتحاد المصارف العربية (2001).

أهمية البحث:

[1] على الصعيد العلمي

أولًا: النظر في مدى ملاءمة المفاهيم التقليدية للضبط الإداري للوسائل الحديثة في مجال الأمن «السَّيبرانيّ»؛ كتأمين الشبكات، وتأهيل رجال الضبط والتحقيق الجنائي، والمحاكمة، وتأمين بيانات الحكومة «الإلكترونية».

ثانيًا: النظر في مدى سد الفراغ التشريعي، الناتج عن تطوُّر وظهور الجرائم المستحدثة، وعابرة الدول، عن طريق الضبط التَّشريعي، وتأهيل رجال الضبط الإداري لمواجهة التهديدات «السَّيبرانيّة».

ثالثا: إثبات تطوُّر وتحوُّل مفاهيم الضبط الإداري لمفاهيم مستحدثة، ومجالات أرحب، كمجالات الاقتصاد، والسياحة، والبيئة، والرياضة، وعدم انحصارها في المفاهيم التقليدية(الأمن العام، والسكينة العامة، والصحة العامة)، وأهمية الضبط الإداري بمفهومه المستحدث في المناسبات الرياضية العالمية، على وجه الخصوص.

[2] على الصعيد العملي:

أولًا: أهمية الأمن «السَّيبرانيّ» ، لاسيما في ظل تنامي التهديدات الأمنية « الإلكترونيّة»، على مستوى الدول، والمؤسسات العامة والحكومية، والخاصة، سواء من جهة ارتفاع عدد الهجمات، أو من جهة الأضرار الناجمة عنها.

ثانيا: أهمية التأمين «السَّيبرانيّ» في المناسبات الرياضية التي تتسم بزخم في الأعداد، من خلال التعرُّض إلى الوسائل الحديثة للضبط الإداري، كتأمين الشبكات،

و تأهيل رجال الضبط، و تأمين بيانات الحكومة «الإلكترونيّة».

ثالثا: توقيت البحث، وبخاصة أن دولة قطر مُقبِلة على استضافة أهم حدث رياضي - عالميًا - وهو كأس العالم لكرة القدم (2022).

صعوبات البحث:

أولًا: قلة المراجع الفقهية والقضائية، في مجال الأمن «السَّيبرانيّ» من وجهة نظر القانون العام.

ثانيًا: تعدُّد صور التهديدات «السَّيبرانيّة» في المناسبات الرياضية، كجرائم الاختراقات «الإلكترونيّة»، وجرائم التجسس «الإلكترونيّ»، والجرائم المالية والاقتصادية «الإلكترونيّة»، وجرائم الإرهاب «الإلكترونيّ»، وجرائم الإرهاب والفتن الداخلية عبر «الإنترنت»، والجرائم العسكرية، وجرائم اختراق النظم الأمنية لأغراض اقتصادية عبر «الإنترنت»، والتهديد والترويع «الإلكترونيّ»، والاستيلاء على المعلومات التي يتم نقلها عبر شبكات المعلومات، وجرائم الاعتداء على بيانات الحكومة «الإلكترونيّة».

منهج البحث:

تشترك في هذا البحث عدة مناهج، أحدها: الاستقرائيّ، عن طريق رد الفروع إلى أصولها، والثاني: الاستنباطي، بتحليل نصوص القوانين، بالإضافة إلى المنهج المقارن، في تناول العديد من القوانين المواجهة للتهديدات «السَّيبرانيّة» من خلال ما يسمى استراتيجية أمن المعلومات.

خطة البحث:

ستكون المعالجة البحثية على النحو التالي:

المبحث الأول: صور التهديدات «السَّيبرانيّة» في المناسبات الرياضيّة، والمواجهة الإدارية لها.

المبحث الثاني: المواجهة التشريعية للتهديدات « السَّيبرانيّة»، واستراتيجية أمن المعلومات.

توصيات البحث

المبحث الأول

صور التهديدات «السَّيبرانيّة» في المناسبات الرياضية والمواجهة الإدارية لها

تتعدد صور التهديدات «السَّيبرانيّة» في المناسبات الرياضية، كجرائم الاختراقات «الإلكترونيّة»، وجرائم التجسس «الإلكترونيّ»، والجرائم المالية والاقتصادية « الإلكترونيّة»، وجرائم الإرهاب «الإلكترونيّ»، وجرائم الإرهاب والفتن الداخلية عبر «الإنترنت»، والجرائم العسكرية، وجرائم اختراق النظم الأمنية لأغراض اقتصادية عبر «الإنترنت»، كاستهداف محطات توليد الطاقة والماء، واستهداف البنية التحتية الاقتصادية، ونظم المواصلات والاتصالات، والتهديد والترويع «الإلكترونيّ»، والاستيلاء على المعلومات التي يتم نقلها عبر شبكات المعلومات، وجرائم الاعتداء على بيانات الحكومة الإليكترونية، مما يستدعي مواجهة تلك التهديدات كلها أو جلها من خلال المواجهة الإدارية للتهديدات «السَّيبرانيّة»، ولحسن العرض سوف تكون المعالجة كالتالي:

المطلب الأول: صور التهديدات «السَّيبرانيّة» في المناسبات الرياضيّة.

المطلب الثاني: المواجهة الإدارية للتهديدات «السَّيبرانيّة» في المناسبات الرياضية (الضبط الإداري).

المطلب الأول

صور التهديدات «السَّيبرانيّة» في المناسبات الرياضية

تتنوع صور التهديدات «السَّيبرانيّة» في المناسبات الرياضية، ما بين ما يتعلق بالتهديدات «السَّيبرانيّة» في المناسبات الرياضية في الظروف العادية، ومنها ما يتعلق بالتهديدات «السَّيبرانيّة» في المناسبات الرياضية في الظروف الاستثنائية، وحريٌّ بنا – قبل التعرُّض لكليهما – أن نعالج الإطار العام لفكرة التهديدات «السَّيبرانيّة»، مع تعريف الأمن «السَّيبرانيّ» .

ولحسن العرض سوف تكون المعالجة كالتالي:

الفرع الأول: الإطار العام لفكرة التهديدات «السَّيبرانيّة»، وتعريف الأمن «السَّيبرانيّ» .

الفرع الثاني: التهديدات «السَّيبرانيّة» في المناسبات الرياضية في الظروف العادية.

الفرع الثالث: التهديدات «السَّيبرانيّة» في المناسبات الرياضية في الظروف الاستثنائية.

الفرع الأول

الإطار العام لفكرة التهديدات «السَّيبرانيّة» مع تعريف الأمن «السَّيبرانيّ»

أولا: الإطار العام لفكرة التهديدات « السَّيبرانيّة»:

بدأ استعمال مصطلح «الشبكة العنكبوتية» في الأمور العسكرية في الولايات المتحدة، عام (1969م)، وبدأ العالم يتعرف عليها منذ أواخر ثمانينيَّات القرن الماضي تدريجيًّا(1)، ولم يعد اعتراض المعلومات، والتطفل عليها، والعبث بها، حِكرًا على الجواسيس والخبراء العسكريين، بل أصبح هواية للأشخاص العاديّين، مما شكل في حد ذاته تهديدًا حقيقيًّا للمُنظَّمات الحكومية والخاصة، ولمواجهة التهديدات «السَّيبرانيّة» لتلك الشبكة نُظِّمت عدة مؤتمرات محلية ودولية، بعضها كان في دولة قطر (2).

ومما يزيد الإشكالية تعقيدًا: «الاستخدام العام للبريد «الإلكترونيّ»، ووصول الجمهور لمواقع «الويب»"web sites" عبر «الإنترنت»، وسهولة الوصول إلى المعلومات في النظم المعلوماتية، مع الإمكانيات اللامحدودة لتبادلها وإرسالها، بصرف النظر عن بُعد المسافات الجغرافيّة، مما مكَّن المستخدمين من اصطناع فضاء جديد، يسمى «الفضاء «السَّيبرانيّ» ، والذي يُستعمل أساسًا لأغراض شرعية، ولكن يمكن أن يخضع لسوء الاستخدام»(3).

«إن الحديث عن أمن المعلومات، يُملي ضرورة الحديث – كمقدِّمة ضرورية ولازمة – عن فكرة الوجود القانوني لغايات الدولة، ذلك أن بعضًا ينكر هذا الوجود، من منظور أن الحديث

---

1 ()انظر:د. الديربي: عبد العال، والاستاذ اسماعيل: محمد صادق: الجرائم « الإلكترونيّة» دراسة قانونية قضائية مقارنة – الطبعة الأولى- المركز القومي للإصدارات القانونية، القاهرة 2012، ص(8). و في ذلك المعنى انظر:-العقيد الحقوقي: عبد الله جعفر كوفلي: مراقبة الاتصالات في التنظيم الدولي والداخلي، المركز القومي للإصدارات القانونية، الطبعة الأولى، 2017. حيث يؤكد ذلك الرأي أن استراتيجية أمن المعلومات تهدف إلى: تعريف المستخدمين والإداريين بالتزاماتهم وواجباتهم المطلوبة لحماية نظم الحاسوب والشبكات، وكذلك حماية المعلومات بكافة أشكالها، وفي مراحل إدخالها، ومعالجتها، وخزنها، ونقلها، وإعادة استرجاعها، وتحديد الآليّات التي يتم من خلالها تحقيق وتنفيذ الواجبات على كل من له علاقة بالمعلومات ونظمها، وتحديد المسؤوليّات عند حصول الخطر، وبيان الإجراءات المتَّبعة لتجاوز التهديدات والمخاطر والتعامل معها، والجهات المنوط بها القيام بها بذلك.

2() الرزو،مظفر حسن، الأمن المعلوماتي، معالجة قانونية أولية، مجلة الأمن والقانون، أكاديمية شرطة دبي، السنة (12)، العدد (1)، 2006، ص(68 – 93). وفي ذلك المعنى انظر للمزيد: ياسين،السيد:- شبكة الحضارة المعرفية من المجتمع الواقعي إلى العالم الافتراضي – الهيئة المصرية العامة للكتاب – 2009. حيث يؤكد ذلك الرأي أنه توجد عدة أسباب لدى قراصنة المعلومات لمباشرة الجرائم المعلوماتية على النظام الحاسوبي:

١- تراكم أحقاد، أو إحداث أي نوع من التخريب؛ لتحقيق نوازع غير متزنة، على مستوى الأشخاص، أو المؤسسات، أو النظم الحاكمة.

٢- وجود إغراءات ماديّة، توفرها حكومات، أو مؤسسات، أو شركات، أو أفراد؛ لاستحصال معلومات وبيانات مهمة من نظام معلوماتي، يكمن وراءها غايات سياسيَّة، أو يَقْنِيَّة، أو اقتصادية بحتة.

٣- وجود أغراض سياسية، تستهدف مباشرة أنشطة مخابراتيّة، على نظم أو مؤسسات في بلدان أخرى.

في السياق ذاته، انظر: تعليقًا قاله الدكتور «عميد كلية الهندسة بجامعة قطر»، في جريدة الشرق القطرية بتاريخ: (26/4/2017)، وتاريخ: (28/10/2019): «يعتبر الأمن «السَّيبرانيّ» أولوية وطنيَّة لدول المنطقة؛ لتطوير معرفة الأفراد بهذا النوع من الأمن؛ للاستفادة من التقنية المتوفرة، كما أنه يعتبر جزءًا أساسيًّا من استراتيجيات الأمن «السَّيبرانيّ» الوطني والإقليمي، وفيه: تم التوصل إلى أنه «لا يمكن ضمان حماية الأمن «السَّيبرانيّ» من خلال نشر أحدث وسائل التكنولوجيا فقط، بل يجب أن يؤخذ في الاعتبار أيضًا: الأشخاص، والعمليات التي تتفاعل مع النظم؛ فالأمن «السَّيبرانيّ» منظومة تتركز حول عناصر أساسيّة؛ منها : نشر الوعي بين الأفراد، وإبراز أفضل الممارسات، ومعرفة أفضل الوسائل لمشاركة المعلومات. لقد أصبح العامل البشري أكثر أهمية عند الحديث عن حلول الأمن «السَّيبرانيّ». تفصيلاً لذلك: يُعد تزايد حجم المعلومات المنتشرة على ساحة «الإنترنت»، وتصاعُد قيمتها بوصفها مصدرًا معرفيًّا، واقتصاديًّا، و سياسيًّا، قد ألقى بظلاله على ميدان القرصنة المعلوماتية، مما نجم عنه حصول تغيير في أهداف عملية القرصنة المعلوماتية التي كانت في بداياتها مجرد نزعة فضولية للوصول إلى معرفة جديدة، أو تحدي العقبات الأمنية التي تضعها الجهات الأخرى لغرض الإحساس بنشوة النصر فتوجهت صوب استثمار هذه القدرات، وترجمتها إلى مكاسب مادّيّة أو سياسيَّة موجهة، وبذلك أضحت عملية الاختراق التي يقوم بها قرصان المعلومات تتسم بسوء قصد، وتعمّد، وقد ينشأ الدافع لديه ذاتيًّا، أو بناءً على حافز خارجي من جهة أخرى، فيباشر عملية اعتراض سبيل المعلومات المتدفقة في الشبكة، ويحولها إلى جعبته الشخصية؛ لكي يحقق أغراضًا مرسومة مسبقًا.

3 () د. عطية، طارق إبراهيم الدسوقي: «الأمن المعلوماتي» (النظام القانوني لحماية المعلومات) دار الجامعة الجديدة، 2009، ص(14).

عن مهام الدولة هو الحديث عن وجهة نظر متجاوزة للقانون»(4)؛ فالأمن – بصفة عامة – من بين الغايات الأساسيّة للدولة، ويستقر الفقه على تعريفه – بصفة عامة – بأنه: عبارة عن «الإجراءات والتدابير الوقائية، التي تراعى بقصد الحفاظ على الدولة، ورقابة نظامها العام المجتمعي، وحماية الأشخاص والممتلكات والأموال، فضلًا عن المنشآت العامة والخاصة ناهيك عن المعلومات المحفوظة بل وأيضًا المتداولة»(5).

ثانيا: تعريف الأمن «السَّيبرانيّ»

بَداءَةً – قبل تعريف الأمن «السَّيبرانيّ» – يجدر بنا أن نقوم بتعريف الخطر «السَّيبرانيّ» ؛ فقد قام البعض بتعريفه بأنه: خطر جديد يواجه المؤسَّسات، وجهات الإدارة، ويكون مرتبطًا بالتطوُّر التكنولوجي، وتدفقات المعلومات (6)، وفي اعتقادنا، أن الخطر «السَّيبرانيّ» يمكن تعريفه بأنه: تهديد إلكتروني مُحتمَل يتعلق بالمعلومات، والبيانات الرسمية وغير الرسمية، للمؤسَّسات، والأفراد، والجهات الإدارية والحكومية، ومجاله: احتمال التغيير، أو التأثير في صورة، أو في نشاط، أو في سلوك، بإرادة مصدر الخطر.

إذن فجملة المخاطر «السَّيبرانيّة» تتلخص في عملية جمع المعلومات وتخزينها وتوزيعها (7)، وهو ما يتطلب القيام باتخاذ تدابير وإجراءات معيَّنة، يُطلَق عليها الأمن «السَّيبرانيّ»، وتجدر الإشارة إلى أن للأمن «السَّيبرانيّ» مفهومًا أوسع من أمن المعلومات، فالأمن «السَّيبرانيّ» يهتم بأمن كل ما هو موجود على الفضاء «الإلكترونيّ»، باستثناء أمن المعلومات، بينما أمن المعلومات لا يهتم بذلك، كما أن أمن المعلومات يهتم بأمن المعلومات الفيزيائية «الورقية»، بينما لا يهتم الأمن «السَّيبرانيّ» بذلك.

4 () د. فوزي، صلاح الدين، الإدارة العامة بين علم متغير ومتطلبات التحديث - دار النهضة العربية 1998، ص(388).

5 () تفصيلًا لذلك انظر: مرجع سابق، ص(388).

في السياق ذاته، أكد تقرير مجلة «انترناشيونال بوليسي دايجست»: الدوحة مركز دولي للأمن «السَّيبرانيّ»، المنشور في (31ديسمبر 2019) بجريدة الشرق القطرية، أن دولة قطر تبذل جهودًا كبيرة؛ لتحديد الخطوط العريضة لاستخدام الوسائط الرقمية وتأثيرها على الأفراد والدول، من خلال استخدام الوسائل الدبلوماسيَّة؛ للاستجابة للتحديات في الفضاء «الإلكترونيّ».

وفي ذلك المعنى، أورد التقرير أن الدوحة عملت على جذب الانتباه، في جميع أنحاء العالم، إلى المخاطر المرتبطة بالبيئة الرقمية اليوم، وأوضح التقرير أن الدوحة، المقبلة على استضافة كأس العالم (2022)، على وعي تام بالحاجة إلى الاستعداد لمواجهة التهديدات الافتراضية لحماية الفضاء «الإلكترونيّ»، لذلك أطلقت عددًا من المبادرات والسياسات، بما في ذلك الإستراتيجية الوطنية للأمن «السَّيبرانيّ» التي انطلقت في عام (2014).

وذكر التقرير أنه في إطار جهود دولة قطر للحفاظ على سلامة أفراد المجتمع على «الإنترنت» وحماية شبكات البنية التحتية ومجابهة المخاطر والتهديدات الحالية والناشئة، قامت «اللجنة الوطنية لأمن المعلومات»، بإشراف وزارة الاتصالات وتكنولوجيا المعلومات، بوضع «الإستراتيجية الوطنية للأمن «السَّيبرانيّ»»، انطلاقًا من أهداف الإستراتيجية الوطنية للاتصالات وتكنولوجيا المعلومات، الرامية إلى حماية البنية التحتية للمعلومات الحيوية الوطنية، وتوفير بيئة آمنة لمختلف القطاعات؛ لتقديم خدمات إلكترونية متكاملة وآمنة، وهي هيئة رسمية مُكلَّفة بتحديد الهجمات « السَّيبرانيّة» ومنعها. كما تم وضع قواعد الإشراف المصرفي، التي بدأها بنك قطر المركزي بالتنسيق مع اللجنة الوطنية لأمن المعلومات لحماية المؤسسات المالية، حيث تقوم وزارة المواصلات والاتصالات إجراء تدريبات سنوية، فريدة من نوعها في البلاد، وتُشرك المؤسسات العامة والخاصة في مجموعة من الأنشطة الفنية والتعليمية، مما يزيد من الاستعداد والوعي بكيفية إدارة الهجمات «الإلكترونيّة». وواصل التقرير أنه: في أكتوبر (2019)، استضافت قطر النسخة الثانية من منتدى الأمن العالمي، الذي نظمه كل من «مركز صوفان» الاستشاري للشؤون الأمنية، وأكاديمية قطر الدولية للدراسات الأمنية (قياس)، وحضره مسئولون حكوميون، وخبراء من أكثر من خمسين دولة؛ للمشاركة في مجموعة متنوعة من الجلسات، ألقى الضوء على التحديات الأمنية التي يفرضها انتشار الحروب الحديثة للمعلومات في المجتمعات المترابطة رقميًّا، بل و أشار التقرير إلى أن قطر أدركت على وجه الخصوص أهمية التعليم والعلوم والبحث في تعزيز الأمن «السَّيبرانيّ»، وتوطيد مكانتها بوصفها مركز لتحقيق الأمن « السَّيبرانيّ» الدولي.

6 () انظر: د / الزغبي، محمد علي فارس:الحماية القانونية لقواعد البيانات وفقا لقانون حق المؤلف -دراسة مقارنة ما بين النظام اللاتيني والنظام الأنجلوأمريكي، ص (85).

7 () تفصيلا لذلك انظر: بوقرة، سامية: المخاطر المعلوماتية لنظم المعلومات وآليات مواجهتها، مجلة صوت الجامعة 2015 - تصدر عن الجامعة الإسلامية في لبنان، ص(229).

اصطلاحيًّا هناك العديد من التعاريف التي قُدِّمت لمفهوم الأمن «السَّيبرانيّ» ، حيث يُعرّف بأنه: "مجموعة من الإجراءات المتَّخَذة، في مجال الدفاع ضد الهجمات «السَّيبرانيّة»، ونتائجها، التي تشمل تنفيذ التدابير المضادة المطلوبة". وهذا ما ذهب إليه الكاتبان: "Lehto Martti"، "Neittaanmäki Pekka"، في كتابهما الموسوم: «Cyber Security: Analytics, Technology and Automation"، حيث جعلا الأمن «السَّيبرانيّ» : "عبارة عن مجموعة من الإجراءات، التي اتُّخذت في الدفاع ضد هجمات قراصنة الكمبيوتر وعواقبها، ويتضمن تنفيذ التدابير المضادة المطلوبة..(8)

وقد عُرّف الأمن «السَّيبرانيّ»، في التقرير الصادر عن الاتحاد الدولي للاتصالات، حول اتجاهات الإصلاح في الاتصالات، لعام (2010–2011)، بأنه: «مجموعة من المُهِمَّات، مثل تجميع وسائل وسياسات وإجراءات أمنية، ومبادئ توجيهية، ومقاربات لإدارة المخاطر، وتدريبات وممارسات فُضْلى، وتِقْنيات يمكن استخدامها لحماية البيئة « السَّيبرانيّة»، وموجودات المؤسَّسات والمستخدِمين».(9)

من ناحية أخرى، يذهب البعض لتعريف الأمن «السَّيبرانيّ» (أو السَّيبَري) بأنه: «مجموعة الأطر التنظيمية، والإجراءات العملية، والتِّقْنيات التي تهدف إلى منع الاستعمال غير المُصرَّح به للمعلومات، مع الأخذ في الاعتبار تأمين استمرارية الخدمة، وخُصوصيَّة المعطَيات والمعلومات، وكذلك الحرص على إيجاد السبل الكفيلة بحماية المستخدم لتلك التقنيات من كافة المخاطر (10).

ويذهب البعض الآخر إلى تعريفه بأنه: «كيفية حماية البيانات والنُّظُم « الإلكترونيّة» من الهجمات «attack»، أو الفقد «loss»، أو التداخل «compromise».(11)

8 ()تفصيلا لذلك انظر: https://political-encyclopedia.org/dictionary/الأمن%20» السَّيبرانيّ» الموسوعة السياسية،موقع على شبكة « الإنترنت» -آخر تحديث (17/4/2020).
إجرائيًا: يمكن القول بأن الأمن « السَّيبرانيّ» هو: مجموعة الآليات، والإجراءات، والوسائل، والأطر، التي تهدف إلى حماية البرمجيات، وأجهزة الكمبيوتر (الفضاء « السَّيبرانيّ» بصفة عامة)، من مختلف الهجمات والاختراقات (التهديدات السَّيبرانيّة) التي قد تُهدِّد الأمن القومي للدول.
9 () https://political-encyclopedia.org/dictionary/الأمن%20» السَّيبرانيّ»
الموسوعة السياسية،موقع على شبكة «الإنترنت» آخر تحديث (17/4/2020)
في السياق ذاته، قدّمت وزارة الدفاع الأمريكية «البنتاغون» تعريفًا دقيقًا لمصطلح الأمن « السَّيبرانيّ»، على أنه: «جميع الإجراءات التنظيمية اللازمة لضمان حماية المعلومات بجميع أشكالها، المادية، و» الإلكترونيّة»، من مختلف الجرائم: الهجمات، التخريب، التجسس والحوادث". في حين رأى الإعلانُ الأوروبي الأمنَ « السَّيبرانيّ» أنه يعني: «قدرة النظام المعلوماتي على مقاومة محاولات الاختراق، التي تستهدف البيانات.
10 ()في ذلك المعنى انظر: د. حب الله،عماد يوسف: ورشة عمل حول «بناء القدرات في مجال الحماية القانونية على «الإنترنت» (5-4 شباط 2009)- الهيئة المنظمة للاتصالات في لبنان - أمن الفضاء « السَّيبرانيّ» ص(2)، في إشارة إلى الجهود في مجال الأمن المعلوماتي، من خلال لجنة الاتصالات وتكنولوجيا المعلومات، التابعة لجامعة الدول العربية، ومثال تلك الجهود: القانون الاتّحادي لمكافحة الجرائم المعلوماتية، الصادر في الإمارات العربية المتحدة، في (شباط 2006)، وقانون سعودي صادر في عام (2006) يُجرِّم التنصُّت، والاعتراض، أو الاستفادة من البيانات «الإلكترونيّة» دون مسوغ قانوني .
11 () The Emergence of cyber security law, prepared for the Indiana university -Maurer school of law by Hanover Research, February,2015 p. 11.

وفي اعتقادنا أن الأمن «السَّيبرانيّ» أحد محددات الأمن القومي، وإذا كانت فكرة الأمن القومي أكثر غموضًا فإن الأمن «السَّيبرانيّ» يعد أكثر تحديدًا لكنّه أوسع نطاقًا. (12)

مؤدَّى ما سبق: أن الأمن – بوصفه أحد مكوِّنات النِّظام العام – لم يعد يقتصر على لون واحد فقط، بل تعدَّدت صوره؛ ما بين الأمن العسكري، والأمن الاجتماعي، والأمن السياسي، والأمن الفكري، والأمن الاقتصادي، وأمن الجهاز الإداري الحكومي، والأمن العقائدي، والقيمي، والأخلاقي (13).

أضف الى ذلك أن مفهوم الأمن لم يعد يقتصر على تأمين المواطن ضد المخاطر التقليدية المحتملة، أو الوجود المادي للدولة وسيادتها الكاملة على أراضيها، لكنّه توسَّعَ نحو آفاق جديدة، أهمها: صيانة أمن الفرد، والجماعات، والدولة، والحفاظ على كيانها ووجودها المادي والافتراضي. (14)

12 (12) تأكيدًا على ذلك: يحيط الأمنَ القومي تساؤلاتٌ وتحديدات عديدة، ما بين التحديد السياسي والتحديد القانوني، ويعزِّز وجهة النظر هذه: أن أهمية المعلومات تتعدى الأمن «السَّيبرانيّ» إلى الأمن القومي، فإذا كانت الدول النامية من أكثر المستفيدين من الطفرة « السَّيبرانيّة» إلاّ أنها تبنَّت آراء مقيِّدة لجمع المعلومات أو نشرها، لذا تُطالب دومًا بالحصول على المعلومات الخاصة بأراضيها، حتى لا يمكن استغلال ثرواتها دون علمها أو باتفاقيات غير متكافئة.

13 () في ذلك المعنى انظر للمزيد: غطاس، جمال محمد: أمن المعلومات والأمن القومي- مكتبة نهضة مصر، دون سنة نشر، ص(2). وكذلك -م.د. حجازي،عبد الفتاح بيومي:- مكافحة جرائم الكمبيوتر و» الإنترنت» في القانون العربي النموذجي «دراسة متعمقة في القانون المعلوماتي» - دار الكتب القانونية – 2007،8، 29.

فالأمن العسكري هو: قواعد بيانات ونظم المعلومات، العسكرية والحربية، والمحتوى «السَّيبرانيّ» الرقمي العسكري . والأمن الاجتماعي هو: قواعد بيانات ونظم المعلومات، المخصَّصة للتعامل مع الحالة الاجتماعية للمجتمع، كإحصاءات ودراسات السكان.

والأمن السياسي هو: قواعد بيانات ونظم المعلومات، والمحتوى الرقمي للأحزاب، والبرلمان، ورئاسة الدولة، والجماعات السياسية المختلفة، وأجهزة الأمن السيادية.

والأمن الفكري هو: قواعد بيانات ونظم المعلومات، والمحتوى الخاص بالإنتاج الفكري والفني والثقافي.

والأمن الاقتصادي هو: قواعد البيانات ونظم المعلومات، والمحتوى الرقمي لدى البنوك، والبورصة، والجمارك، والضرائب، والمالية، وغيرها من المؤسسات الاقتصادية الكبرى.

أما أمن الجهاز الإداري الحكومي، فهو: قواعد البيانات ونظم المعلومات، والمحتوى الرقمي الخاص بالخدمات الحكومية المقدمة للجماهير، وبخاصّة مشروعات الحكومة « الإلكترونيّة».

أما الأمن العقائدي والقيمي والأخلاقي، فهو: قواعد بيانات ونظم المعلومات، لدى المؤسسات الدينية، كالأزهر، والأوقاف، والمجلس الأعلى للشئون الإسلامية ... الخ.

14 () تفصيلا لذلك: "إذا أردت أن تعرف سمات نموذج الأمن القومي الجديد ،فلا تناقش كبار الجنرالات، أو أبرز خبراء الدفاع، ولكن ناقش خبراء التكنولوجيا والاتصالات». مرجع سابق ص (12)، في إشارة إلى المفكر الاستراتيجي الأمريكي Thomas Barner)).

وتجدر الإشارة إلى عقد مركز قطر للاستجابة لطوارئ الحاسبات «كيوسرت»، التابع للمجلس الأعلى للاتصالات وتكنولوجيا المعلومات (أي سي تي قطر)، مؤتمرًا بعنوان «تحديات الأمن « السَّيبرانيّ» في القطاع المالي" fin.INFOSEC " ، وذلك بحضور نخبة من أبرز الخبراء والمتخصّصين في الأمن المعلوماتي، حيث تناول أحدث الأساليب للهجمات «السَّيبرانيّة» وكيفية التصدي لها، وأهمية الشراكات بين مؤسسات القطاع العام والخاص؛ لمحاربة الجريمة «الإلكترونيّة»؛ فضلاً عن إيجاد حلول تقنية جديدة؛ لتعزيز حماية الأنظمة الحيوية، وتشكيل خريطة طريق وطنية للأمن المعلوماتي.

يُذكر أن الأعلى للاتصالات كان قد أنشأ مركز «كيوسرت» في عام (2005)؛ بغية تعزيز الأمن « السَّيبرانيّ» في الدولة. ومنذ إنشائه، عمل المركز على تأمين البِنية التحتيّة للمعلومات الحيوية لدولة قطر. وأصبح المركز نموذجًا وطنيًّا للإيفاء بكافة متطلبات الأمن « السَّيبرانيّ»، وحماية الأفراد والأنظمة التكنولوجية من التهديدات « السَّيبرانيّة» بشكل استباقي، وذلك من خلال الممارسات الآمنة والسياسات التوجيهية، بالإضافة إلى التركيز على سبل إدارة المخاطر « الإلكترونيّة»، وتبادل المعلومات بشكل موثوق وآمن.

كما يقوم المركز باتخاذ كافة الإجراءات الاحترازية التي تُمكّنه من التصدي لمخاطر التهديدات « السَّيبرانيّة» على الصعيد الوطني، ويعمل «كيوسيرت» علي الإبلاغ السريع والفعال للتهديدات والمخاطر «الإلكترونيّة»، واتخاذ الإجراءات اللازمة لتعزيز الأمن « السَّيبرانيّ» في دولة قطر.

الفرع الثاني

التهديدات «السَّيبرانيّة» في المناسبات الرياضية في الظروف العادية

هناك العديد من صور التهديدات «السَّيبرانيّة» في المناسبات الرياضية، في الظروف العادية، والتي يمكن أن تواجه نظام المعلومات « الإلكترونيّة» في تلك الشبكة، أو من خلالها، وأبرز هذه المخاطر ما يلي:

أولًا: اختراق الأنظمة: ويتحقق ذلك بدخول شخص غير مُخوَّل بذلك، إلى نظام الكمبيوتر، والقيام بأنشطة غير مصرح له بها، كتعديل البرمجيات التطبيقية، وسرقة البيانات السرية، أو تدمير الملفات، أو البرمجيات أو النظام، أو لمجرد الاستخدام غير المشروع، ويتحقق الاقتحام بشكل تقليدي من خلال أنشطة (التَّقنُّع والتخفي)، ويراد به: تظاهر الشخص المخترق بأنه شخص آخر مصرح له بالدخول، أو من خلال استغلال نقاط الضعف في النظام، كتجاوز إجراءات السيطرة والحماية، أو من خلال المعلومات التي يجمعها الشخص المخترق من مصادر مادية أو معنوية، كالتنقيب في قمامة المنشأة للحصول على كلمات السر، أو معلومات عن النظام، أو عن طريق الهندسة الاجتماعية، كدخول الشخص إلى مواقع معلومات حساسة داخل النظام، ككلمات السر أو المكالمات الهاتفية.

ثانيًا: الاعتداء على حق التخويل: ويتم ذلك من خلال قيام الشخص المُخوَّل له باستخدام النظام لغرض ما، باستخدامه في غير هذا الغرض، دون أن يحصل على التخويل بذلك، وهذا الخطر يُعد من الأخطار الداخلية في حق إساءة استخدام النظام من قبل موظفي المُنشأة، وهو أيضًا قد يكون من الأخطار الخارجية، كأن يستخدم مخترق حساب شخص مخول له باستخدام النظام، عن طريق تخمين كلمة السر الخاصة به، أو استغلال نقطة ضعف في النظام؛ للدخول إليه بطريق مشروع أو من جزء مشروع، ومن ثَمَّ القيام بأنشطة غير مشروعة.

ثالثًا: زراعة نقاط الضعف: عادةً ينتج هذا الخطر عن اقتحام من قِبَل شخص غير مصرح له بذلك، أو من خلال مستخدِم مشروع، تجاوز حدود التخوِّيل الممنوح له، بحيث يقوم الشخص بزرع مدخل ما، يحقق له الاختراق فيما بعد. ومن أشهر أمثلة زراعة المخاطر حصان طروادة، وهو عبارة عن برنامج يؤدي غرضًا مشروعًا في الظاهر، لكنه يُمكِن أن يُستخدم في الخفاء للقيام بنشاط غير مشروع، كأن يَستخدم برنامج معالجة كلمات لتحرير وتنسيق النصوص ظاهريًا، في حين يكون غرضه الحقيقي نسخ كافة ملفات النظام، ونقلها إلى ملف مخفي، بحيث يمكن للمخترِق طباعة هذا الملف، والحصول على محتويات النظام.

رابعًا: مراقبة الاتصالات: ويتم ذلك من خلال قيام الجاني بالحصول على معلومات سريِّة – دون اختراق حاسوب المجني عليه – غالبًا ما تكون المعلومات التي تُسهِّل له مستقبلًا اختراق النظام، وذلك بسهولة من خلال مراقبة الاتصالات، من إحدى نقاط الاتصال أو حلقاتها.

خامسًا: اعتراض الاتصالات: ويتم ذلك – أيضًا – دون اختراق النظام، حيث يقوم الجاني في هذه الحالة باعتراض المعطيات المنقولة خلال عملية النقل، ويُجري عليها التعديلات التي تتناسب مع غرض الاعتداء، ويشمل اعتراض الاتصالات: قيام الجاني بخلق نظام وسيط وهمي، بحيث يكون على المستخدم أن يمُرَّ من خلاله، ويزوّدَ النظام بمعلومات حساسة بشكل طَوْعي.

سادسًا: إنكار الخدمة: ويتم ذلك من خلال القيام بأنشطة تمنع المستخدم الشرعي من الوصول إلى المعلومات، أو الحصول على الخدمة،وأبرز أنماط إنكار الخدمة: إرسال كمية كبيرة من رسائل البريد «الإلكترونيّ» دفعةً واحدة إلى موقع معين؛ بهدف إسقاط النظام المستقبل؛ لعدم قدرته على احتمالها، أو توجيه عدد كبير من عناوين «الإنترنت»، على نحو لا يتيح عملية تجزئة حِزَم المواد المرسَلة؛ فتؤدي إلى اكتظاظ الخادم وعدم قدرته على التعامل معه.

سابعًا: عدم الإقرار بالقيام بالتصرف: ويتمثل هذا الخطر في عدم إقرار الشخص المرَسل إليه، أو المرسِل بالتصرف الذي صدر عنه، كأن ينكر أنه ليس هو شخصيًّا الذي قام بإرسال طلب الشراء عبر «الإنترنت»..(15)

ثامنًا: جرائم الاختراقات « الإلكترونيّة»: يرتبط الاختراق «السَّيبرانيّ» بالمستوى المتقدم للغاية، الذى باتت وسائل الاتصالات وتقنية المعلومات تلعبه في جميع مجالات الحياة وفى العالم بأسره، ومن خلال الأنظمة «الإلكترونيّة»، والشبكات المعلوماتية، اتخذ الاختراق أبعادًا جديدة، وازدادت خطورته على المجتمعات الدولية، وينطلق الاختراق «الإلكترونيّ» من عالمين: العالم المادي (Physical World)، والعالم الافتراضي (Virtual World) الذى من خلاله تتم عمليات الإرهاب «الإلكترونيّ» والتدمير والتخريب.

ويشير العالم المادّي إلى قضايا وظواهر متعددة مثل: الطاقة، والضوء والظلام، والبرودة والحرارة، وجميع الأمور المادِّية والحيّز الذى يعيش فيه المجتمع، ويمارِس الوظائف والأدوار من خلاله، أما العالم الافتراضي فيشير إلى التمثيل الرَّمزي والمجازي للمعلومات، وهو

15 () في ذلك المعنى انظر: عرب، يونس: قانون الكمبيوتر-موسوعة القانون وتقنية المعلومات اتحاد المصارف العربية، 2001 ،ص (281) وما بعدها.
تفصيلا لذلك: تهدف استراتيجية أمن المعلومات إلى: تعريف المستخدمين والإداريين بالتزاماتهم، وواجباتهم المطلوبة لحماية نظم الحاسوب والشبكات، وكذلك حماية المعلومات بكافة أشكالها، وفي مراحل إدخالها، ومعالجتها، وخزنها، ونقلها، وإعادة استرجاعها، وتحديد الآليّات التي يتم من خلالها تحقيق وتنفيذ الواجبات، على كل من له علاقة بالمعلومات ونظمها، وتحديد المسؤوليّات عند حصول الخطر، وبيان الإجراءات المتّبعة لتجاوز التهديدات والمخاطر والتعامل معها، والجهات المنوط بها القيام بها بذلك.

المكان الذى تعمل به البرامج والأنظمة «الإلكترونيّة» وتنتقل فيه البيانات، كما تتعدد صور جرائم الاختراقات (16).

تاسعًا: الجرائم المالية والاقتصادية « الإلكترونيّة»: تتمثل هذه الجرائم فيما يلى:

- الاحتيال والاستيلاء على المعلومات البنكية لعملاء البنوك عبر «الإنترنت»، واستغلالها في الشراء.
- الوصول إلى البيانات التفصيلية للبطاقات الائتمانية عبر «الإنترنت»، والاستيلاء عليها، واستغلالها في الشراء.
- إنشاء مواقع إلكترونية وهمية على «الإنترنت»، مُقلِّدة للمواقع «الإلكترونيّة»الرسمية للبنوك على «الإنترنت»؛ بهدف الاحتيال على عملاء تلك البنوك، والاستيلاء على بياناتهم البنكية.

عاشرًا: جرائم غسل الأموال عبر «الإنترنت»: وهى عبارة عن استخدام الأموال غير مشروعة (المُحرَّمة محليًا وعالميًا)، أو غير النظامية (المخالفة للأنظمة المحليَّة) وتمريرها، أو تحويلها، أو نقلها، أو استبدالها، أو الاتجار بها عبر « الإنترنت»، وقد أسهمت التجارة «الإلكترونيّة»في انتشار جرائم غسل الأموال بشكل كبير.

الفرع الثالث

التهديدات «السَّيبرانيّة» في المناسبات الرياضية في الظروف الاستثنائية

هناك العديد من صور التهديدات «السَّيبرانيّة» في المناسبات الرياضية، في الظروف الاستثنائية، وأبرز هذه المخاطر ما يلي:

أولا: جرائم التجسس «الإلكترونيّ»: ويتمثل هذا النوع من الجرائم فيما يلي:

- اختراق المواقع والصفحات «الإلكترونيّة»على «الإنترنت» بغرض التجسس،أو التنصُّت على ما تحتويه من بيانات ومعلومات (نصية، أو صوتية، أو مرئية) تُهِمُّ الجهة

16 () في ذلك المعنى انظر: الرزو، 2006، مرجع سابق ص (68 – 93).
استثناءً من ذلك: اختلفت الآراء في تحديد نقطة بداية الهجمة المعلوماتية ص (89)، و متى يمكن اعتبار النظام يعاني من عملية اختراق أمني؟ فذهب البعض الى اعتبار بدء محاولة الغير الدخول الى ساحة النظام، ممن لا يمتلكون ترخيصًا للعمل على نظام بذاته، أو محاولة إحباط نشاط ما في بقعة من بقاع النظام، نقطة البداية للهجمة المعلوماتية. بينما يذهب البعض إلى عدم اعتبار النشاط «السَّيبرانيّ» اختراقًا مالم يبدأ بعملية قرصنة المعلومات بكامل تفاصيلها الدقيقة. و يبدو أن كلا الطرفين لم ينجح في الصياغة الدقيقة؛ لأن محاولة الدخول لنظام معلوماتي لا يلزم أن تنجح؛ لذا لا يصح وصفها بالاختراق، و لكن بالهجمة المعلوماتية، كما أن ربط الاختراق بتحقُّق هدفه يُعد تساهلًا واضحًا؛ لأن الدخول إلى الحِمَى هو اختراق لحرمة النظام، سواء تحققت غايته أم لم تتحقق، من اجل ذلك فإن عملية دخول غير مشروع، يمارسها الغير على نظام معلوماتي، دون وجود حساب ترخيص قانوني، بصورة مباشرة او غير مباشرة، يُعدّ اختراقًا معلوماتيًا يضع صاحبه تحت المساءلة قانونيًا.
تتعدد صور جرائم الاختراق، كالتالي:
- اختراق المواقع والصفحات «الإلكترونيّة» على «الإنترنت» وتدميرها، أو إلغائها، أو إتلافها، أو التعديل والعبث بالبيانات والمعلومات المتوفرة عليها.
- شغل العنوان (الرابط) «الإلكترونيّ» للموقع، أو تحويله لعنوان موقع آخر على « الإنترنت».
- اختراق البريد «الإلكتروني» للآخرين، والاستيلاء عليه، واستخدامه في انتحال شخصية الغير.
-اختراق قواعد البيانات، وحذف أو تعديل المعلومات الموجودة عليها، أو الاستيلاء على المعلومات المتوفرة عليها، كأسماء المستخدمين، وأرقامهم السرية، وعناوين الاتصال الخاصة بهم، واستخدامها لأغراض غير مشروعة، أو ببيعها إلى جهات مستفيدة (جهات اقتصادية وتجارية، أو سياسية، أو أمنية).

المستفيدة من التجسُّس (جهات اقتصادية وتجارية، أو سياسية، أو أمنية).

- إرسال رسائل بريد إلكترونية لمستخدمي «الإنترنت»، تتضمن ملفات برمجيّة لديها القدرة على الإرسال بشكل آلي للمعلومات المتوفرة على جهاز المستخدم، من ملفات (نصية، أو صوتية، أو مرئية)، كما أن لديها القدرة على إرسال أي معلومات تتعلق بمستخدم «الإنترنت»، مثل سجل زياراته لمواقع «الإنترنت»، والبيانات التي يدخلها المستخدم فى مواقع « الإنترنت»، كاسم المستخدم، وكلمة السر، بالإضافة إلى كلمات البحث التي يُدخلها المستخدم في محركات البحث العالمية.

- استخدام البرامج المتخصصة باختراق أجهزة الحاسبات الآلية المرتبطة بـ« الإنترنت»؛ بهدف التجسس على ما تحتويه من معلومات وبيانات، وهناك الكثير من الأمثلة على هذه البرامج، أشهرها برنامج يسمى (Subseven).

أضف إلى ذلك أيضًا: أنه مع تزايد اعتماد المؤسسات والشركات الحكومية الكبرى على الحاسب الآلي، في جمع وتخزين البيانات الخاصة بأفرادها، المتعلقة بأوضاعهم المادية والصحية والعائلية والتعليمية... إلخ، يمكن أن يُسهِّل ذلك للبعض الحصول على هذه البيانات الخاصة على نحو غير مأذون به،ومن ثَمَّ إمكانية إساءة استخدامها وتوجيهها توجيهًا منحرفًا، أو خاطئًا، كقيام بعض الجماعات الإرهابية، المدرَّبة تدريبًا جيدًا، بالتغلغل في مجتمع ما، وتهديد أمن المطارات، والمصانع الكيمائية، ومحطات الطاقة النووية فيه، وغيرها من المؤسسات التي تسير بنظم الحاسب، ولا تُطبِّق إجراءات أمنية بشكل كافٍ.

ثانيًا: جرائم الإرهاب « الإلكترونيّ»: ويتمثل هذا النوع من الجرائم فيما يلى:

- إنشاء أو استضافة المواقع والصفحات على «الإنترنت» التي تدعو للإرهاب، والعنف، والتطرف، والتفرقة بين أفراد المجتمع بمختلف فئاته.

- إنشاء أو استضافة مواقع إلكترونية على «الإنترنت»، تحتوي على دروس (نصية، أو مرئية، أو مسموعة) لتعليم صناعة المتفجرات، وطرق استخدامها في تنفيذ العمليات الإرهابية.

- إنشاء مواقع إلكترونية على «الإنترنت» تُسهم في دعم المنظمات الإرهابية، وترويج أفكارها، وتُسهِّل الاتصال بقياداتها وأعضائها.

ثالثًا: جرائم الإرهاب والفتن الداخلية عبر «الإنترنت»:

تستخدم الجماعات الإرهابية الشبكات في تبادل المعلومات الإرهابية ونشرها، وتبادل الآراء والأفكار والمعلومات إذا كان صعبًا في الواقع، فإنّ الشبكات المعلوماتية تُسهِّل هذه العملية كثيرًا.

رابعًا: الجرائم العسكرية وجرائم اختراق النظم الأمنية لأغراض اقتصادية عبر «الإنترنت»:

تقوم التنظيمات الإرهابية بشن هجمات إلكترونية من خلال الشبكة المعلوماتية؛ بقصد تدمير المواقع والبيانات «الإلكترونيّة»والنظم المعلوماتية، وإلحاق الضرر بالبنية المعلوماتية التحتية وتدميرها، وتستهدف الهجمات الإرهابية في عصر المعلومات ثلاثة أهداف أساسية – غالبًا – وهى: الأهداف العسكرية، والسياسية، والاقتصادية، ويستطيع قراصنة الحاسب الآلي (Hackers) التوصل إلى المعلومات السرية والشخصية، واختراق الخصوصية وسرية المعلومات بسهولة.

خامسًا: استهداف محطات توليد الطاقة والماء:

يشمل هذا مباشرة سلسلة من الهجمات المعلوماتية على نظم الحواسيب والشبكات المعلوماتية، التي تنهض بمهام التحكُّم في شبكات توزيع الطاقة الكهربائية الوطنية، وينشأ عن مثل هذه الهجمات تعطيل العديد من مرافق الحياة في البلاد، ولا يتوقف الأمر عند هذا الحد، حيث إن هنالك الكثير من الأهداف الأخرى، التي يمكن بواسطتها للقراصنة المتمكِّنين أن يشيعوا الفوضى في الحياة المدنية؛ فهنالك مثلاً: شبكات المعلومات الطبية.

سادسًا: استهداف البنية التحتية الاقتصادية:

أصبح الاعتماد على الشبكات المعلوماتية شبه مُطلَق في عالم المال والأعمال، مما يجعل هذه الشبكات هدفًا سهلاً؛ نظرًا لطبيعتها وانفتاحها على العالم، ومما يزيد من إغراء الأهداف الاقتصادية والمالية: أنها تتأثر بشكل ملموس بالانطباعات السائدة والتوقعات، والتشكيك في صحة هذه المعلومات أو تخريبها يمكن أن يؤدى إلى إضعاف الثقة في النظام الاقتصادي.

سابعًا: استهداف نظم المواصلات:

يتضمن هذا النوع اختراق نظم التحكم بخطوط الملاحة الجويّة، والبرّيّة، والبحريّة، وإحداث خلل في برامج هبوط الطائرات وإقلاعها، مما قد ينجم عنه حصول تصادم فيما بينها.

ثامنا - استهداف نظم الاتصالات:

ويشمل هذا النوع اختراق الشبكات المعلوماتية، والشبكة الهاتفية الوطنية، وإيقاف محطات توزيع الخدمة الهاتفية، وقد تمارَس سلسلة من الهجمات على خطوط الهواتف المحمولة، ويُمنع الاتصال بين أفراد المجتمع ومؤسساته الحيوية، الأمر الذي ينشر حالة من الرعب والفوضى، وعدم القدرة على متابعة تداعيات الهجمات الإرهابية المعلوماتية.

تاسعًا: التهديد والترويع « الإلكترونيّ»:

تقوم المنظمات والجماعات الإرهابية بالتهديد عبر وسائل الاتصالات، ومن خلال الشبكة العالمية للمعلومات (Internet)، وتتعدد أساليب التهديد وتتنوع طرقه؛ وذلك من أجل نشر الخوف والرعب بين الأشخاص.

عاشرًا: الاستيلاء على المعلومات التي يتم نقلها عبر شبكات المعلومات:

يتم نقل كَمِّيات هائلة من المعلومات عبر شبكات المعلومات بصورة يومية، وتتميز كثير من هذه المعلومات بكونها على درجة كبيرة من الأهمية. وعلى الرغم من استخدام أجهزة تشفير تتولى تشفير الرسائل والمعلومات المهمة عند إرسالها وفك شفرتها عند استقبالها، إلا أن الاستيلاء على المعلومات، التي يتم نقلها عبر شبكات المعلومات، قد أصبح يشكِّل خطرًا كبيرًا يهدد أمن وسلامة هذه المعلومات.

حادي عشر: جرائم الاعتداء على بيانات الحكومة «الإلكترونية»:

تقع هذه الجرائم في نطاق الاعتداء على نظام معالجة البيانات، أو شبكات المعلومات التي تؤدَّى من خلالها خدمات الحكومة «الإلكترونية» (17).

17 () د. خشبة،محمد سعيد– نظم المعلومات – المفاهيم والتكنولوجيا – دون ناشر – 1990، ص(101).
في ذلك المعنى انظر: للمزيد البروفيسور. كير،أورين: - نطاق الجريمة الافتراضية – الأكاديمية الدولية للتجارة «الإلكترونيّة» – مؤسسة آدم للنشر والتوزيع (مالطا)، 2008.
يمكن تقنين جريمة الاعتداء على البيانات «الإلكترونيّة» للحكومة، عن طريق الركن المادّي، الذي يشمل صور عديدة وهي:
-1 الدخول غير المشروع لمواقع الحكومة الإليكترونية.
-2 التعدي على البيانات الشخصية في نطاق الحكومة الإليكترونية.
-3 انتهاك سرية وخصوصية البيانات.
-4 جرائم الاعتداء على التوقيع الإليكتروني.
-5 جرائم الاعتداء على البيانات المشفرة.
في ذلك المعنى انظر: للمزيد د. عبادة، عبادة أحمد:- التدمير المتعمد لأنظمة المعلومات الإليكترونية – بحث منشور لدى مركز البحوث والدراسات، الإدارة العامة لشرطة دبي – مارس 1999.
تفصيلًا لذلك: وحتى تقوم هذه الجريمة، فإنه يجب ألا يكون نظام المعالجة الآلية للبيانات أو المعلومات مفتوحًا للجمهور، ولذلك فإن هذه الجريمة لا تقوم في شأن مواقع الحكومة الإليكترونية المفتوحة للمستخدمين – ومنهم الجمهور – لكنها تقوم في حق من يدخل إلى موقع غير مخصص للجمهور.
والمواقع المفتوحة للجمهور إن تم الاعتداء عليها، يمكن العقاب على ذلك كما في صورة إتلاف الموقع معلوماتيًّا عن طريق الفيروس المعلوماتي، وقد سبق بيان ذلك – في شأن الإتلاف المعلوماتي – ومن وسائل التعييب أو الإفساد: استخدام القنبلة المعلوماتية، أو البرنامج الذى يحمل «حصان طروادة»، وغير ذلك من الفيروسات التي كان يجب عليه أن يُخرجها، بل أن الإفساد يمكن أن يتحقق عن طريق إتلاف أو تخريب العناصر المادِّية في النظام.

المطلب الثاني

المواجهة الإدارية للتهديدات «السَّيبرانيّة» في المناسبات الرياضية

(الضبط الإداري)

تستدعي معالجة المواجهة الإدارية للتهديدات «السَّيبرانيّة» في المناسبات الرياضية، التعرض أولًا لمفهوم الضبط في المدلولين: اللغوي، والاصطلاحي، ثم نُتبع ذلك بفرع ثانٍ، نتطرق فيه إلى الوسائل الحديثة للضبط الإداري لمواجهة تلك التهديدات، ومنها تأمين الشبكات على نحوٍ يمنع من اختراقها، وفي الثالث: نتناول تأمين بيانات الحكومة «الإلكترونية» فنيًّا، من خلال وسائل الحماية الفنية لبيانات الحكومة «الإلكترونية»، ومنها: الجدار الناري أو حوائط المنع (Fire Walls)، ومكافحة الفيروس المعلوماتي، ولحسن العرض سوف تكون المعالجة كالتالي:

الفرع الأول

مفهوم الضبط في المدلولين: اللغوي، والاصطلاحي

من ناحية أولى: للضَّبْط لُغةً عدة مفاهيم، فهو يعنى أولًا: دقة التحديد، فيقال: ضُبِطَ ٱلأَمْرَ، بمعنى: أنه حُدِّد على وجه الدقة، وهو يعنى ثانيًا: وُقوعُ العَيْنين، ثم إلقاء اليدين على شخص كان خافيًا، ويجرى البحث عنه، والمعنى الثالث للضبط يُفهم منه العَوْد بالأمور إلى وضعها الطبيعي، المنسجم مع القانون الحاكم لها، وذلك عقب خلل أو اضطراب أصابها، منُحرفًا بها عن حكم هذا القانون(18).

ويقال أيضا في تعريف الضَّبْط لُغةً، (ضَبْطُ) الشَّيْءِ حِفْظُه بِالْحَزْم، وبابه: (ضَبَطَ)، ورَجُلٌ (ضابِطٌ)، أي: حازِمٌ(19)، ويقال أيضًا: الضَّبْطُ: لُزُومُ الشَّيْءِ وحَبْسُه لاَ يُفَارِقُهُ فِي كُلِّ شَيْءٍ (20).

ومن ناحية أخرى – فيما يتعلق بالمدلول الاصطلاحي–: تباينت وجهات النظر بشأن تحديد ماهية الضّبط الإداري وتعريفه، فذهب البعض إلى أن الضّبط الإداريَّ مهمته وقائية، تنحصر في المحافظة على النظام العام، والحيلولة دون وقوع الجرائم، ومن ثم يُعرَّف بأنه: حق الإدارة في أن تفرض على الأفراد قيودًا تَحُدُّ بها من حرياتهم؛ بقصد حماية النظام العام(21)، و أيضًا، يُعرِّف هذا الرأي الضبط الإداري بأنه: «مجموعة ما تفرضه السلطة العامة، من أوامر ونواه وتوجيهات ملزمة للأفراد؛ بغرض تنظيم حرياتهم العامة، أو بمناسبة ممارستهم لنشاط معين؛ بهدف صيانة النظام العام في المجتمع»(22).

18 () انظر الدكتور بهنام، رمسيس: علم النفس القضائي، الاسكندرية، منشأة المعارف، سنة النشر غير مذكورة، ص(15).
19 () قاموس مختار الصحاح، الطبعة الثالثة، ص(400).
20 () قاموس لسان العرب، الجزء التاسع، القاهرة، الدار المصرية للتأليف والترجمة، ص(214) فصل الضاد، حرف الطاء.
21 () انظر الدكتور الطماوى،سليمان محمد: الوجيز في القانون الإداري «دراسة مقارنة»، القاهرة، دار الفكر العربي، 1979، ص(574).
22 () انظر الدكتور الجرف،طعيمة: القانون الإداري والمبادئ العامة في تنظيم ونشاط السلطات الإدارية، القاهرة، دار النهضة العربية، 1978، ص(487).

ويرى البعض أن وظيفة الضبط الإداري تعدُّ وظيفةً تتسم بخصائص متميزة؛ فهي ضرورية، ومحايدة، وهادفة إلى وقاية النظام العام في المجتمع، في ظل سيادة القانون، وبوسائل السلطة العامة(23)، ولذا يُعرِّف البعض الضبط الإداري بأنه: «النشاط الذى تتولاه الهيئات الإدارية، ويتمثل في تحديد النشاط الخاص بهدف صيانة النظام العام»(24)، ويرى البعض – في تعريفه للضبط الإداري – ضرورة التركيز على الهدف منه، وهو صيانة النظام العام، دون اشتراط أن يكون الإجراء الضبطي ماسًّا بالحريات؛ لأنه قد لا يمس إلا مجرد رُخَص، فيُعرَّف الضبط الإداري – تبعًا لذلك – بأنه: «مجموع الأنشطة التي تتخذها الإدارة منفرِدَة؛ بهدف المحافظة على النظام العام، أو إعادة هذا النظام في حالة اضطرابه.»(25)

وذهب البعض إلى أن وظيفة السُّلطة التنفيذية هي السَّهَر على تنفيذ القوانين، ولا يقتصر ذلك على المعنى الحرفي للتنفيذ، بل يتناول أيضًا وقاية وحماية النظام الاجتماعي، فالسلطة التنفيذية لها بحكم وظيفتها ما يشبه التفويض العام في المحافظة على النظام العام(26).

الفرع الثاني

الوسائل الحديثة للضبط الإداري لمواجهة التهديدات «السَّيبرانيّة» في المناسبات الرياضية

هناك العديد من الوسائل الحديثة التي على أجهزة الضبط الإداري أن تتغياها للوصول إلى مواجهة شاملة للجرائم المعلوماتية ومنها:

أولًا: تأمين الشبكات على نحو يمنع من اختراقها:

لعل في محاولة الشركات والمؤسسات الخاصة والحكومية تأمين شبكاتها الخاصة بالكومبيوتر ضد الاختراق، ما يكون وسيلة تحُدُّ – إن لم تمنع مطلقًا – من عملية الاختراق لهذه الشبكات، ومن ثم فهي تؤدِّى – بطريقة غير مباشرة – إلى منع الأحداث من الانحراف بطريق اختراق هذه الشبكات.

وجدران النار عبارة عن برامج تقوم بصدِّ محاولات الاختراق، أو الهجوم الوافد من شبكة «إنترنت» لتهديد الشبكة الداخلية أو النظام المعلوماتي، وتوجد برامج كثيرة لجدران النار، من ذلك: برنامج شبكة (DAN) والذى يتضمن مزايا أمنية عديدة عبارة عن برامج جدران النار (Firewalls)، ومزوّدات «بروكسى» (Proxy servers)، التي تحتفظ بصفحات الشبكة – للويب – على القرص الصلب، ومرشحات عناوين (arl filters).

23 () انظر الدكتور الشريف، محمود سعد الدين: النظرية العامة للضبط الإداري، مقالة منشورة بمجلة مجلس الدولة، السنة الحادية عشرة، 1962، ص(112).
24 () انظر الدكتور البنا، محمود عاطف: الوسيط في القانون الإداري، القاهرة، دار الفكر العربي، 1984، ص(337).
25 () انظر الدكتورة الشرقاوي، سعاد: القانون الإداري، القاهرة، دار النهضة العربية، 1983، ص(13).
26 () انظر الدكتور جعفر، محمد أنس قاسم: الوسيط في القانون العام «أسس وأصول القانون الإداري»، دار النشر غير مذكورة، سنة النشر غير مذكورة، ص(163).

ثانيًا: تأهيل رجال الضبط الإداري في مكافحة جرائم « الإنترنت»:

من الأهمية بمكان، تأهيل رجال الضبط الإداري في مكافحة جرائم « الإنترنت»، وبخاصَّة فيما يتعلق بكشف الثغرات المعلوماتية، ويعتمد البعض تعريف الثغرة المعلوماتية بأنها عبارة عن: هيئة، أو خاصّية تقْنية يتصف بها عتاد الحاسوب، أو برمجياته التطبيقية، التي تتيح للمستخدم غير المرخَّص إمكانية اقتناص فرصة الدخول إلى النظام «السَّيبرانيّ»، أو زيادة مستوى الدخول إلى حدود غير متاحة له بدون وجود هذه الثغرة، وتشمل الثغرة المعلوماتية مساحة واسعة في ميدان الأمن «السَّيبرانيّ»، مثال العتاد (hard) أو البرمجيات (software).(27)

وتأسيسًا على ما تقدم، فلابد – عند مكافحة جرائم «الإنترنت» – من وضع سياسة جنائية رشيدة، تستند على تدريب أجهزة العدالة الجنائية للأحداث، لمكافحة الجريمة، بما فيها الجريمة المعلوماتية، ويمتد التدريب إلى العاملين في الشرطة كما القضاء و التنفيذ، وقد تنبهت الدول إلى أهمية هذا التدريب، وظهر هذا الاهتمام جليا في توصيات العديد من المؤتمرات الدولية الخاصة بمنع الجريمة ومعاملة المجرمين، منها: ما جاء في القاعدة (1–22) من (قواعد بكين)، من التأكيد على الحاجة إلى التخصص المهني والتدريب، وورد فيها أنه: «يُستخدم التعليم المهني، والتدريب أثناء الخدمة، ودورات تجديد المعلومات، وغيرها من أساليب التعليم المناسبة، من أجل تحقيق واستمرار الكفاءة المهنية اللازمة، لجميع الموظفين الذين يتناولون قضايا الأحداث». (28).

وليس بالضرورة أن يكون المحقق خبيرًا في الحاسب الآلي، لكن لابد له من الإلمام ببعض المسائل الأولية، التي تمكنه من مسايرة التعاون مع رجال الضبط الإداري، أو الخبراء من موظفي الجهات الإدارية، ويشاطرنا الرأي في ذلك جانب من الفقه (29). ونحن نرى

27 () الرزو ،2006مرجع سابق ص 70
حيث يؤكد ذلك الرأي أنه يمكن تعريف الأدوات المعلوماتية التخريبية، بأنها عبارة عن: «برمجيات، أو وسائط تقنية، قابلة للتوظيف مع عتاد الحاسوب وبرمجياته؛ لتحقيق الأهداف الرئيسية التالية:
١- مضايقة، وإنهاك مستمر لموارد النظام المعلوماتي.
٢- تدمير قواعد البيانات والمعلومات والمعارف، وموارد البرمجيات والنظم التطبيقية.
٣- إحداث ثغرات في النظام « السَّيبرانيّ»، أو التمهيد لها، من خلال الكشف عن مواطنها.
في السياق ذاته، تُستغَل هذه الأدوات من قبل قراصنة المعلومات؛ لضمان سهولة اختراق الشبكات، عن طريق استثمار الامكانيات المتاحة في هذه الأدوات؛ للوقوف على طبيعة الثغرات الأمنية الموجودة على الشبكة، والاستفادة منها لفك الرموز، والشفرات التي قد يُشكل عليهم حلها بأدواتهم الشخصية.
28 () د. منصور،محمد حسين– المسؤولية «الإلكترونيّة» – دار الجامعة الجديدة للنشر- الاسكندرية 2007 ص (202)،. وفي السياق ذاته، انظر: للمزيد د. خليل،عزة محمود أحمد:- مشكلات المسئولية المدنية فى مواجهة فيروس الحاسب – دراسة مقارنة في القانون المدني والشريعة الإسلامية – دار النهضة العربية – القاهرة – 1994. و د. القهوجي،علي عبد القادر: - الحماية الجنائية لبرامج الحاسب الآلي – دار الجامعة الجديدة – الإسكندرية – 1997.
د. أبو صديق،فوزي: - إشكالية المعلوماتية بين حق الخصوصية وإفشاء الأسرار المهنية – مؤتمر الأعمال المصرفية الإليكترونية – كلية الشريعة والقانون – الإمارات.
وتأكيدًا على ذلك، يتعرض د. منصور – فيما يخص الضبط القضائي – إلى أنه يجب على مورِّد الخدمة أن يلتزم بتقديم البيانات الخاصة بالعملاء للسلطات التحقيقية، وله الدخول لتلك البيانات الموجودة على الأجهزة، والاطلاع على مواقع البريد «الإلكترونيّ»، وعلى جميع الملفات المخزونة على وحدة الأقراص الصلبة، وذلك أيًّا كانت درجة السرية التي يتخذها المستخدم، ولهذا يجب إعداد المحققين، ورجال الضبط في جرائم الحاسب الآلي و» الإنترنت»؛ لأنهم يواجهون أنشطة إجرامية معقدة، تُنفَّذ بطريقة دقيقة وذكية، من الكبار والأحداث على حد سواء.
29 () راجع د. البشرى،محمد الأمين في «التحقيق في جرائم الحاسب الآلي» بحث مقدم إلى مؤتمر القانون والكمبيوتر و»الإنترنت». مقدم إلى كلية الشريعة والقانون – جامعة الإمارات العربية المتحدة – الفترة من (1-3 مايو 2000م).
تفصيلاً لذلك: يذهب هذا الرأي إلى أهمية التفاهم مع خبراء الحاسب الآلي، وحسن استغلالهم في كشف الجرائم وجمع الأدلة، كما أنه من الضروري أن يكون المحقق مُلمًّا بالإجراءات الاحتياطية التي ينبغي اتخاذها على مسرح الجريمة في جرائم الحاسب الآلي، والتدابير اللازمة لتأمين الأدلة ومعلوماتها الممغنطة، بصورة علمية وسليمة.

أهمية مواجهة الجرائم المعلوماتية من خلال اتخاذ إجراءات قد تتجاوز المفاهيم والمبادئ المستقرة، بأن يكون هناك تعاون بين العاملين فى تطبيق القانون والخبراء المتخصِّصين في نطاق القطاع الخاص. (30)

ويجب أن تشمل خطة التدريب والتأهيل أولئك القائمين على جمع الاستدلالات، والتحقيق الابتدائي، والحكم في هذه الجرائم(31).

ثالثا- تأمين بيانات الحكومة الإليكترونية فنيًا:

تخلص وسائل الحماية الفنية لبيانات الحكومة الإليكترونية في الآتي:

1- الجدار الناري أو حوائط المنع (Fire Walls):

الجدار الناري عبارة عن مجموعة أنظمة معلوماتية (برامج)، توفر سياجات أمنية ما بين شبكة إنترنت وشبكة المؤسسة – أو الحكومة الإليكترونية – حتى يتم إجبار جميع عمليات الخروج من الشبكة والدخول إليها، بأن تمر من خلال هذا الجدار الناري، والذى يمنع أي مخترق أو متطفل من الوصول إلى الشبكة.

2- مكافحة الفيروس المعلوماتي:

ويُعرف الفيروس المعلوماتي بأنه «برنامج للحاسب الآلي، مثل أي برنامج آخر، لكنه يهدف إلى إحداث أكبر ضرر بنظام الحاسب الآلي، وله القدرة على ربط نفسه بالبرامج الأخرى، وكذلك إعادة إنشاء نفسه حتى يبدو كأنه يتكاثر ويتوالد ذاتيًّا، ويقوم الفيروس بالانتشار بين برامج الحاسب الآلي المختلفة، وبين مواقع مختلفة فى الذاكرة»(32)، ومشكلة الفيروس المعلوماتي: قدرته على الاختفاء، وعلى الانتشار والتدمير، وتتم مواجهته ببرامج حماية (anti-virus).

30 () في اعتقادنا، أن التقدم المتواصل في تكنولوجيا الحاسب الآلي و» الإنترنت»، جعل الشركات الخاصة تستعين بمحققين خبراء في الحاسب الآلي؛ فالجهات الحكومية أولى بإعداد كوادرها للضبط والتحقيق في جرائم المعلوماتية و» الإنترنت»، ويُفترض أن من الواجب على جهات تطبيق القانون أن تسير في خطوات متناسقة مع التطورات السريعة التي تشهدها هذه التقنيات، وهذا الأمر يتطلب الإلمام بالتقنيات الجديدة. وهذا الأمر واضح في مؤسسات القطاع الخاص؛ نظرًا للأجور العالية التي يقبل هذا القطاع أن يدفعها لهم.

31 () د. الصغير،جميل عبد الباقي، أدلة الإثبات الجنائي والتكنولوجيا الحديثة، دار النهضة العربية، القاهرة، 2001، ص(118).

تعزيزًا لذلك: ليس من المطلوب أن ينفرد رجل الضبط القضائي، أو خبير الحاسب الآلي، بتحقيق الجريمة المعلوماتية كاملة، لكن كلاهما يكمل دوره دور الآخر، فكل منهما له خبرات ومعارف يجب أن تُسخَّر لمصلحة التحقيق في مثل هذه الجرائم، وهناك محققون متمرسون في جرائم الحاسب الآلي، ولم تكن دراستهم الأولى في هذا المجال، وهناك مجموعة من صغار المحققين لديهم الإلمام بعلوم الحاسب الآلي، الأمر الذى يقتضى التعاون بين هؤلاء لمصلحة العمل، عن طريق تبادل المعرفة والخبرة بأسلوب علمي،وفي اعتقادنا يتطلب أن نعهد بتحقيق هذه الجرائم إلى بيوت خبرة متخصصة في هذا المجال، خاصة أن هناك شركات عالمية حققت نجاحًا في بعض الحالات.

ويتعلق منهج التدريب والتأهيل – كذلك – بتدريس الأساليب الفنية المستخدمة في ارتكاب الجريمة، أو الأساليب التي تتعلق بالكشف عنها والجرائم والأدلة المستخدمة في ارتكاب هذه الجرائم، وكيفية إثباتها ومعاينتها والتحفظ عليها، وكيفية فحصها فنيًّا، وتدريب القضاة على معالجة هذا النوع من القضايا التي تحتاج إلى خبرات عالية، وذلك حتى يمكن قبول الأدلة الناشئة عنها في الإثبات وتقديرها، وحتى يمكنهم في النهاية الفصل – بجدارة – في هذا النوع من الجرائم. وينظم البوليس الدولي – كذلك – دورات تدريبية، في مجال شبكات الحاسبات الآلية؛ من أجل تحسين أداء الأعضاء – من رجال الضبط القضائي – في مجال الكشف عن الجريمة، وجمع المعلومات، ومتابعة الجناة، وإقامة الدليل في الجرائم التي تُرتكب في هذا المجال.

32 () د. عبادة أحمد عبادة،1999، مرجع سابق (56). وفي ذلك المعنى، انظر: د. هدى قشقوش – جرائم الحاسب الآلى في التشريع المقارن، دار النهضة العربية، القاهرة، 1992، ص(99). و انظر: للمزيد م.د. حجازي،عبد الفتاح بيومي: مكافحة جرائم الكمبيوتر و» الإنترنت» في القانون العربي النموذجي «دراسة متعمقة في القانون المعلوماتي» ، دار الكتب القانونية، -2007 نحو صياغة نظرية عامة في علم الجريمة والمجرم المعلوماتي ، دار النهضة العربية ، الطبعة الأولى، 2009.

رابعًا: دور الشراكة المعلوماتية في تطوير أساليب الضبط الإداري:

تُعد الشراكة المعلوماتية بين القطاعين العام والخاص أحد أهم وسائل تعزيز الأمن «السَّيبرانيّ» ، فضلًا عن ضرورة التعاون الدولي لتوفير الحلول؛(33)فالتقنيات المستعملة في الاختراقات المعلوماتية، لا بد أن تُواجَه بطرق جديدة للتعامل؛ لإدارة تلك الاختراقات، من خلال وجود قواعد معلوماتية واستخباراتية تحدد نوع التهديدات، فضلًا عن التنسيق بين العديد من القطاعات على مستوى التشريع القانوني والرقابي. (34)

ومن أهم المنظمات التي تولت الاهتمام بالأمن المعلوماتي دوليًا: الاتحاد الأوروبي، وحلف الناتو، الذى اعتمد في ذلك على الشراكات بين مختلف الأجهزة، الحكومية وغير الحكومية، ومن الدول الرائدة في ذلك: الولايات المتحدة الأمريكية، وألمانيا، وإستونيا(35).

ويرى البعض أن الاحتمال الأبرز – بالنسبة للأمن المعلوماتي – سيكون بلجوء جهات الإدارة، على المستوى العالمي، لتأسيس شبكات محلية أو إقليمية، والاستغناء عن الشبكة الموحَّدة للإنترنت، وذلك كي يتم الحد من تدفق البيانات والمعلومات، ولكن يعيب ذلك التدبير الاحترازي الإداري: أنه يطغى على عدة أمور:

أولها: حرية تداول المعلومات.

وثانيها: ازدياد قدرة الحكومات على مراقبة ما يُنشر على الشبكة؛ لصغر حجمها. وثالثها: ارتفاع تكلفة البنية التحتية لإنشاء هذه الشبكات، بسبب تكرار بنائها في كل دولة أو إقليم. (36)

33 () في السياق ذاته، تطرق المؤتمر السنوي الثالث لأمن المعلومات، المنعقد بالدوحة في (نوفمبر 2016)، إلى ضرورة التعاون الدولي، وأعرب الرئيس السابق لأسكوتلانديارد، «اللورد ستيفنز» عن أن جميع القطاعات أصبحت معنية بتأمين معطياتها وبياناتها، حيث عمد بعض القراصنة إلى الاستحواذ على بيانات وملفات اللاعبين المشاركين في الأولمبياد.

وفي السياق ذاته، أكد تقرير لمجلة «انترناشيونال بوليسي دايجست»، أن الشراكات الدولية لعبت – أيضًا – دورًا رئيسًا في تعزيز الدبلوماسية «السَّيبرانيّة»، حيث تتبادل الدول الصديقة المعرفة والخبرة، ويساعد بعضها البعض في أوقات الأزمات، وتطبيقًا لذلك، فقد طورت قطر العديد من الشراكات الثنائية؛ لتعزيز قدراتها في مجال الأمن «السَّيبرانيّ» وتبادل المعرفة على الصعيد الدولي، وتم إطلاق مبادرة مشتركة، «التعاون الأكاديمي الصناعي في مجال الأمن «السَّيبرانيّ»، والتي يطلق عليها «دبلوماسية العلوم» بين الصندوق القطري لرعاية البحث العلمي ومجلس البحوث العلمية والتكنولوجية في تركيا (TÜBİ-TAK)، في عام 2017، بهدف تطوير استجابات مبتكرة لسد احتياجات الأمن « السَّيبرانيّ».

وجاء في ختام التقرير: تمكنت قطر من تقديم نفسها بوصفها حليفًا عالي المستوى على المسرح الدبلوماسي، رغم أنه لا يمكن أن يكون هناك أي شك في النفوذ الاقتصادي للبلد؛ فإن استجابة الدوحة المدروسة بشكل ملحوظ، ودبلوماسية الأمن «الإلكترونيّ»، تُسهِّل إقامة شراكات إضافية، مع مؤسسات دولية رائدة، تُعد حيوية لنقاش الأمن «السَّيبرانيّ» الشامل، بعد أن وضعت نفسها في طليعة هذه القضية.

ومع وجود بيئة تهديد رقمية ومعقدة بشكل متزايد، والتي تشكل اليوم خطرًا على جميع البلدان، فمن المحتمل أن يتحول مركز القيادة في مجال الأمن « السَّيبرانيّ» إلى قطر باعتبارها من اهم الدول التي تمتلك القوة الناعمة في المنطقة.

34 ()تفصيلا لذلك، من أمثلة قطاعات البنية التحتية المعلوماتية: القطاعات المالية، والطاقة، والرعاية الصحية، والاتصالات، والاستخبارات، ووزارة الداخلية... الخ.

35 (35) PETA،Cezar: cyber security – current topic of National security Public security studies, volume II, Issue 3)7) / 2013, p. 67 “cyber security is challenge that must be tackled through cooperation between various national actors, and institutions, private companies and non-governmental organizations, and international level through cooperation among states, regional and global organizations.

وفي اعتقادنا: أن الاتفاقيات الدولية، ومذكرات التفاهم، أحد أنجع الوسائل لتبادل الخبرات، ومثال ذلك: ما نادى به البعض من عقد اتفاقيات دولية رقمية، ومن ذلك: دعوة شركة (MICROSOFT) الى عقد «اتفاقية جنيف الرقمية»، التي تتطلب من الحكومات الإبلاغ عن ثغرات الأجهزة الحاسوبية للبائعين، بدلا من تخزينها، أو بيعها، أو استغلالها.

36 () مجلة حالة العالم، مرجع سابق ص(17، 18)، نقلًا عن تقرير «جايسون هيلي»، مدير مبادرة ”cyber state craft initiative“ بمركز (Atlantic council). ومن أمثلة ذلك: اتجاه بعض الدول إلى إنشاء ما يسمى (حائط النار) ”fire wall“؛ لحماية الشبكات الوطنية، والتحكم في تدفق المعلومات والبيانات منها وإليها، ومن تلك الدول: الصين، وروسيا، وقد تقود الجهود المبذولة لتقنين « الإنترنت»، تحت إشراف الاتحاد الدولي للاتصالات، التابع للأمم المتحدة، إلى الدفع نحو ذلك التدبير المستحدث.

أما الفقه المقارن فهو يفضل الأساليب العملية في تحقيق الأمن المعلوماتي، وذلك عن طريق التعاون الدولي قانونيًّا وقضائيًّا، كالاتفاق في مجال الاختصاص القضائي، والقانون الواجب التطبيق في بيئة منازعات «الإنترنت»، وأما الوسائل الافتراضية، ومثل: دعوات إنشاء حكومة «الإنترنت» أو بوليس « الإنترنت»، أو معايير الاستخدام الموحد، أو سياسات التنظيم الذاتي للالتزامات، فلن تجدي؛ وذلك لأن « الإنترنت» يتصف (باللامركزية)، وغياب السلطة التحكمية(37).

ويشكل التعاون الدولي في مجال الأمن المعلوماتي ركنًا أساسيًّا لتعزيز الأمن المعلوماتي الداخلي، من خلال مدّ رجال الضبط الإداري بالوسائل المستحدثة، والاستراتيجيات الجديدة لمكافحة الإرهاب «الإلكترونيّ» بصفة خاصة، وانتهاكات الأمن المعلوماتي بصفة عامة. (38)

ويرى الفقه المقارن أن مسألة الأمن المعلوماتي أصبحت مسألة قانونية أكثر منها مسألة تِقْنيّة؛ لتعلقها بمجالات الخصوصية (Privacy) وأمن المعلومات (Data security)، فلا بد أن تُعد المنظمات حزمة القوانين المنظمة للأمن المعلوماتي، وأن يكون للقانونيين دور في تصميم الإجراءات والتدريب وتقديرات المخاطر(39).

علاوة على ما سبق، يمكن الاستفادة من خبرات القطاع الخاص في مجال الأمن «السَّيبرانيّ» ، ومن نماذج ذلك: إطار "NIST" (المعهد الوطني للمعايير والتكنولوجيا) لحماية البنية الأساسية الحيوية المحلية، Domestic critical Infrastructure ، في الولايات المتحدة الأمريكية(40).

ويرى الفقه المقارن إمكانية لجوء جهة الإدارة إلى إجراء برامج لتطوير برامج حيازة البيانات، من خلال تِقْنيّات أكثر سرعة، وبشكل قابل لتحمل التكلفة، على أن تسمح تلك التقنيات لجهة الإدارة بالتحرك في الفترة ما بعد الجريمة بالبحث عن بيانات الأفراد

37 ()Ulrich، Sieber, computer crimes and other crimes related to information technology. I.R.P.. 1994. Vol. 62 p. 1033 seq. .

38 () شارك (700) خبير أمني أوروبي، في تدريبات أمنية على حدوث هجوم افتراضي واسع على الفضاء «الإلكترونيّ»، بوصفه جزءًا من مشروع دفاعي أوروبي عن الأمن «الإلكترونيّ»، يحمل اسم "cyper Europe2016"، ويضم المشروع التدريب على العديد من السيناريوهات المظلمة لبعض صور الإرهاب «الإلكترونيّ»، وتشمل: قطع الكهرباء، والسيطرة على أنظمة الملاحة الجوية، واستغلال ذلك في تعطيل الطائرات، وطلب الضريبة، وذلك بحسب صحيفة «ديلي ميل» البريطانية، في الفترة من (أبريل 2016) وحتى (ديسمبر 2016)، نقلًا عن صحيفة الوطن في العدد (7780)، السنة (22)، بتاريخ السبت (21 ديسمبر 2016).

39 (39) The Emergence of cyber security law, prepared for the Indiana university Maurer school of law by Hanover Research, February, 2015.,3

"Lawyers must play a role in designing the procedures, training and risk assessments required to implement managerial operational and technical controls needed to protect data".

40 () Scott J. Shackelford, JD, PhiD, scott Russell, JD & Andreas juehn, Defining cybersecurity Due Diligence under International law: lessons from the private sector. 15.

Electronic copy available at: http://ssrn.com/abstract =2594323

موضوعي البحث عن البيانات، (41) لذا يؤكد الفقه المقارن أن على الولايات المتحدة الأمريكية – في مجال تعزيز الأمن المعلوماتي – أن تستعين بالقطاع الخاص واستثماراته في الوقاية ووضع تدابير احترازية للأمن المعلوماتي، وتستعين بالقطاع العام واستثماراته في العلاج، وتلافى آثار الانتهاكات المعلوماتية (42).

ويساير ما سبق، ما يميل إليه الفقه الأمريكي من تعزيز الأمن المعلوماتي بصورة شاملة، في كل من القطاعين العام والخاص، ولكن لابد من الأخذ في الاعتبار أن المؤسسات العامة وشركات الطاقة أقل في القدرة الوقائية في مجال الأمن المعلوماتي من الشركات التجارية التنافسية(43)، لذا يرى البعض أن التشفير يُعد وسيلة مهمة لحماية الإدارة من المخاطر المعلوماتية، خاصة في حالة تداول البيانات والمعلومات بين جهات إدارة مختلفة، في صورة قرارات أو أوامر أو تعاقدات إدارية. (44)

وفي اعتقادنا أنه قد يكون التشفير، و تأمين الشبكات المعلوماتية، حلَّين مؤقتين لجهة الإدارة، إلا أن مراعاة حصر الاختصاصات، للموظفين الذين يتعاملون مع البيانات و المعلومات الحكومية وغيرها، يُعد حلًا دائمًا.

41 () See: task force on national security in the information Age, Markle found creating AA Trusted Network for Homeland security (2003): Task force on National security in the information age, Markle found, Mobilizing information to prevent terrorism (2006); protecting America's freedom in the information age.
في السياق ذاته، أسهمت تلك التقنيات بقوة، خاصة بعد الهجمات الإرهابية في (11 سبتمبر)، حيث كشفت جهة الإدارة فى الولايات المتحدة الأمريكية بيانات هائلة حول الأفراد، مستمَدّة من القطاع الخاص، مما يعني أن الكونجرس قد أخفق في الموازنة بين الخصوصية (privacy) والأمن القومي (National security).
For more – the Cantigny principles on technology terrorism, and privacy, National security law Report, feb. 2005, at 14. "The Cantigny" conference on counter terrorism technology and privacy organized by the standing committee on law and Nation security of the American Bar Association".
42 ()sales، Nathan Alexander: Regulating cyper security – Northwestern university law Review 2013 vol., 107, No 4, p. 1506 "According to Brace smith, the united states follows a "bifurcated approach to network security prevention and public investment in prosecution".
43 ()smith، Bruce P., Hacking, Poaching, and counterattacking: Digital counterstrikes and the contours of self-Help, I J.L Econ, & Pol'Y 171, 173 (2005),p.32
44 () د. باز، بشير على: دور الحكومة «الإلكترونيّة» في صناعة القرار الإداري والتصويت « الإلكترونيّ»، مجلة روح القانون، كلية الحقوق جامعة طنطا، 2007، ص(35، 36).

المبحث الثاني

المواجهة التشريعية للتهديدات «السَّيبرانيّة» واستراتيجية أمن المعلومات

تعتمد جهة الإدارة – عامَّة – على الضبط الإداري في مواجهة التهديدات «السَّيبرانيّة»، كما تُقدِم على تهيئة أدوات البيئة المعلوماتية الآمنة، وأولها: الإدارة «الإلكترونيّة»، والحكومة «الإلكترونيّة»، لكن القضية تتطلب إلى جانب ذلك ضرورة المواجهة التشريعية للتهديدات «السَّيبرانيّة»، من خلال تشريعات مستحدثة،وتفعيل ما يسمى «استراتيجية أمن المعلومات». ولحسن العرض سوف تكون المعالجة كالتالي:

المطلب الأول

المواجهة التشريعية للتهديدات «السَّيبرانيّة»

لحسن العرض سوف تكون معالجة هذا المطلب كالتالي:

الفرع الأول :المواجهة التشريعية للتهديدات «السَّيبرانيّة» بشكل عام.

الفرع الثاني: المواجهة التشريعية الأمريكية والفرنسية للتهديدات « السَّيبرانيّة».

الفرع الأول

المواجهة التشريعية للتهديدات «السَّيبرانيّة» بشكل عام

إن المواجهة التشريعية للتهديدات «السَّيبرانيّة»، يُفترَض أن تؤسَّس على أن المصلحة التي يحميها القانون هي: الحق في المعلومات، وفق توازن يراعي كفالة تدفُّقِها، وتنظيم معالجتها واستخدامها ونقلها، حيث إنه في التعامل مع «المعلوماتية» يتعين إدراك ما يحصل من تحوُّل في السلوكيات من مادِّية إلى معنوية، وما نشهده من تحول من اقتصاد الموجودات إلى اقتصاد المعلومات، وإذا كانت جدلية مدى إمكان انطباق نصوص القوانين الجنائية التقليدية على الجرائم التي تستهدف الاعتداء على معطيات الكمبيوتر أو المعلومات، قد خلقت مواقف فقهية ترفض ذلك، أو تؤيده، أو ترى عدم كفايته من جهة وإمكان تحققه من نواحٍ أخرى، فقد امتدت تلك الجدلية إلى القضاء، وحتى جهات التشريع (45).

أما فيما يتعلق بالمعلومات، ونظمها، وسبل معالجتها آليًّا، فالأيسر والأصوب بشأنه أن يلتفت المُشرِّع إلى هذه المشكلة بتشريع خاص، ينص على تجريم صور العدوان المتصوَّرة على المعلومات، ونظمها، وبرامجها، وسبل معالجتها (46).

45 () في السياق ذاته يقول الفقيه (Huet) «أنه من الصعوبة بمكان، أن توفر الجرائم التقليدية (والأدق نصوص التجريم التقليدية) - المرتكزة على التفكير في تحقيق ثروة فعلية أو إتلاف مستندات مادية – حماية فعالة لهذه القيم المعنوية التي تمخضت عنها المعلوماتية»، حيث إن الطبيعة المادّية للحقوق المالية التي يحميها القانون الجنائي، والطبيعة المعنوية لمعطيات الحاسوب، خلقتا اتجاهات متباينة في تحديد الطبيعة القانونية للمعلومات (معطيات الحاسوب)،

46 () في السياق ذاته يقول الفقيه الألماني «Ulrich sieber»: «تعكس نقطة الانطلاق المستحَدَثة للحق في المعلومات حقيقة مضمونها، أن التقدير القانوني للأموال المادية يجب أن يختلف عن نظيره بالنسبة للأموال المعنوية، ويتعلق مظهر الخلاف بحماية المالك، أو الحائز للأموال المادية أو المعنوية، ففي حين أن الأموال المادية – نظرًا لطبيعتها – يستأثر بها شخص محدَّد على نحو مطلق، فإن المعلومات بالأحرى هي مال شائع، ومن ثَمَّ يجب أن تكون من حيث المبدأ حرة، ولا يجب أن تُحمى بالحقوق الاستئثارية التي تقتصر على الأموال المادية، ويُعد هذا المبدأ الأساس (حرية الوصول للمعلومات) شرطًا جوهريًّا لأي نظام اقتصاديّ وسياسيٍّ حُرّ، وعلاوة على ذلك، فهو في غاية الأهمية من أجل تقدم الدول التي في طريقها للتنمية. وترجع الخاصية الثانية لتقدير الأموال المادية والمعنوية؛ فالحاجة إلى حماية المعلومات يجب أن لا يُنظر إليها بوصفها تمثِّل مصالح الأشخاص الذين تأثروا بفحوى المعلومات، ويبرِّر هذا الوجه القيود المستحدثة في نطاق حماية الحياة الخاصة في مجال تقنية المعلومات، وقد صار من الواضح إذن، أنه يستحيل تقليل القوانين التشريعية الخاصّة بتقنية المعلومات قياسًا على النصوص الخاصة بالأموال المادية، ولكن يجب زيادة الأسس الخاصة بها».

مؤدَّى ما سبق: أنه يمكن تحديد الضبط التشريعي للأمن «السَّيبرانيّ» في اتجاهين:

الأول: تنسيب العقوبة مع تأثير الجريمة؛ فتكون العقوبة خفيفةً، في حالة انتهاك الأمن «السَّيبرانيّ» بقصد التسلية والعبث، وتكون شديدة في حالات سرقة الأموال، أو سرقة المعلومات.

الثاني: توقيع عقوبة مُشدَّدة على أية حالة من حالات الانتهاك الأمني «السَّيبرانيّ»، بغض النظر عن تأثير الانتهاك. (47)

ويرى الفقه المقارن أن المعالجة التشريعية للأمن «السَّيبرانيّ» تكون بطريقتين: أولهما: قوانين التجسس.

والآخر: قوانين الاتصالات. (48)

غير أنه تجدر الإشارة إلى أن بعض التشريعات تعاني قصورًا تشريعيًا في الأمن «السَّيبرانيّ»، ويتمثل القصور التشريعي أحيانًا، بالنسبة للأمن «السَّيبرانيّ»، في حداثة الفعل المؤدِّي لانتهاك الأمن المعلوماتي، أو عدم الفهم المتكامل لعناصر الفعل الإجرامي، مثال ذلك: جريمة الدخول غير المصرَّح للنظام المعلوماتي؛ فالمتتبع لتلك الجريمة يجد أنها من الصعوبة بمكان كي تتم معالجتها تشريعيًا بشكل كامل بموجب النصوص العقابية التقليدية. (49)

ويتهدد الأمن «السَّيبرانيّ» للإدارة بصورة كبيرة؛ لاعتماد الإدارة في الوقت الحالي في إدارتها لمرافقها على نظام الحكومة «الإلكترونيّة»، وقد يصل الأمر لانتهاك أمن الدولة الوطني، كالاطلاع على معلومات تمس أمن الدولة، أو الوصول إلى أنظمة التحكم في محطات المفاعلات النووية. (50)

وإذا كانت أفكار الفقيه Ulrich المتقدمة، مما يتصل بأسس السياسة التشريعية في نطاق الحماية الجنائية للمعلومات، المفترض تأسيسها على حماية الحق في المعلومات، بمراعاة حرية انسيابها وتدفقها واستخدامها من جهة، والحماية الجنائية لمواجهة أنشطة الاعتداء على المعلومات من جهة أخرى، فإنها في الوقت ذاته تعطي انطباعًا واضحًا عن وجوب مغايرة الرؤى لآليات حماية المعطيات عن آليات حماية الأموال المادية، المنطلقة أساسًا من الاعتراف بطبيعتها الخاصة، ومراعاة ماهيّتها، وخصائصها، وخصائص الجرائم الواقعة عليها.

47 تفصيلا لذلك، انظر: مُتطلّبات نجاح وفعالية الاستراتيجية التشريعية الوطنية لحماية المعلومات:

- اعتماد استراتيجيات تدريبية أمنية، لإعداد القضاة، والمحامين، والضابطة العدلية، بشأن جرائم التقنية العالية: تحقيقها، وكشفها، وإثباتها.
- اعتماد استراتيجية وطنية لحماية الإبداع الوطني في حقل البرمجيات والمخترعات التقنية، وعدم الانشغال بحماية الأجنبي على حساب تشجيع الإبداع الوطني، الذي يكفل لنا إنتاج المعارف، لا استهلاكها.
- إعداد البنية الإدارية المناسبة لقيادة مؤسسات التقنية في عصر المعلومات.
- إشاعة الوعي بين الأفراد والمؤسسات لأهمية التعاون بخصوص كشف الاختراقات الأمنية، ومواجهتها، وعدم إخفائها، وإشاعة الثقة بقدرة الأجهزة الأمنية على كشف هذه الأنماط الجرمية المستحدثة.
- اعتماد الدراسة البحثية المقارنة، بخصوص حاجة التشريعات الوطنية الموضوعية والإجرائية للإحاطة بالأنماط المستجدة من الجرائم في ميدان التقنية العالية.

48 (48) Safer -Abraham D., National security and leaks, the Government's Authority to Discipline itself. International studies in Human Rights volume 16, p. 69.

- تفصيلا لذلك انظر للمزيد: عرب: 2001 ، مرجع سابق ص (280) وما بعدها .
- محتوى الاستراتيجية التشريعية الوطنية لحماية المعلومات:
- الاعتراف بالحق في المعلومات، انسيابها وتدفقها وتداولها.
- تحديد مفهوم معلومات الكمبيوتر / المعطيات / البرامج / البيانات لجهة تحديد نطاق الحماية ومحله.
- اعتماد معايير قياسية ورقابية بشأن الخدمات التقنية / « الإنترنت» / مقاهي « الإنترنت» / البريد « الإلكتروني» / التجارة «الإلكترونيّة» / البنوك « الإلكترونيّة»...إلخ.
- تحديد معايير الموثوقية والسرية والاستمرارية اللازمة لمعالجة وتداول البيانات، وتحديدًا في طور نقلها.
- تحديد أنماط السلوك الإجرامي في ميدان التقنية العالية ويشكل رئيس جرائم الاتصالات وشبكات المعلومات، مع اعتماد الحد الأدنى المقرر في التشريعات المقارنة، من صور جرائم التقنية العالية، واعتماد تدابير ردعية واحترازية تتناسب معها، كل ذلك بما يتلاءم مع الواقع الوطني، ومرتكزات النظام القانوني، والموائمة مع السائد من نظريات القانون العامة ومستويات تفريد العقاب للجرائم المنصوص عليها في القسم الخاص، وبخاصة جرائم الأموال والجرائم الاقتصادية.
- اتخاذ التدابير التشريعية، في ميدان البيانات والإثبات والأدلة والقواعد الإجرائية المتناسبة مع طبيعة هذه الجرائم، بما لا يُخِلّ بالحقوق الدستورية، وقواعد المشروعية الإجرائية، والحق في الخصوصية.

49 أ. د. النوايسة،عبد الإله محمد: جريمة الدخول غير المشروع في تشريعات الجرائم «الإلكترونيّة» العربية «دراسة مقارنة» – المجلة القانونية والقضائية الصادرة من مركز الدراسات القانونية والقضائية وزارة العدل – دولة قطر – العدد الأول – (السنة العاشرة) يونيو 2016 ص(10، 11).

50 (50) bridge -Brain. D: introduction to computer law, London 2000, fourth edition p. 307.

ومن أحد أهم أدوات الضبط التشريعي: تشديد العقوبات إذا تعلق انتهاك الأمن «السَّيبرانيّ» بالأمن الداخلي أو الخارجي للدولة، أو اقتصادها الوطني، أو أية بيانات حكومية سرية، (51)ومن ذلك بالطبع – فيما يخص جرائم المحتوى – إذا ارتبط الانتهاك «السَّيبرانيّ» بالعمل الإرهابي.

وتجدر الإشارة في مجال الضبط التشريعي – خاصة فيما يتعلق بقوانين الحاسوب– إلى أنها تتفرع إلى العديد من التعريفات، وذلك كالتالي:

1) تشريعات حماية برامج الحاسوب: وهي تعكس الاتجاهات العالمية في إدراج الملكية الفكرية ضمن تنظيمات التجارة الدولية، تبعًا للاقتصاد الرقمي، والاقتصاد المؤّسسي على المعرفة.

2) تشريعات الأصول الإجرائية الجزائية: وهي في الواقع تطوير لقواعد الإثبات في الإجراءات، لكنها تتصل بالحقوق الجديدة المعترف بها في الميدان التقني المعلوماتي.

3) تشريعات المحتوى الضار: وهي تهدف في المقام الأول إلى الحماية من محتوى المعلومات الضارة.

4) تشريعات معايير الأمن «السَّيبرانيّ»: وهي تهدف إلى تبادل البيانات والتشفير، ويستهدف البعض دراستها ضمن محتوى التجارة «الإلكترونيّة». (52)

مؤدَّى ما سبق: أن العديد من الدول تلجأ – في سبيل حماية أمنها «السَّيبرانيّ»– إلى تطبيق قوانين موضوعية، وأخرى إجرائية، على العكس من دول أخرى تعتمد على قوانين غير فعّالة. (53)

51 () كمثال: نص المشرع القطري في قانون (14)، لسنة (2014)، الخاص بمكافحة الجرائم «الإلكترونيّة»، في المادة (2)، على أن «يُعاقَب بالحبس مدة لا تجاوز ثلاث سنوات، وبالغرامة التي لا تزيد على خمسمائة ألف ريال، كل من تمكّن عن طريق الشبكة المعلوماتيّة، أو بإحدى وسائل تقنية المعلومات، بغير وجه حق، من الدخول إلى موقع إلكتروني، أو نظام معلوماتي لأحد أجهزة الدولة، أو مؤسساتها، أو هيئاتها، أو الجهات، أو الشركات التابعة لها.
وتتضاعف العقوبة المنصوص عليها في الفقرة السابقة، إذا ترتب على الدخول الحصول على بيانات أو معلومات إلكترونية، أو الحصول على بيانات أو معلومات تمس الأمن الداخلي أو الخارجي للدولة، أو اقتصادها الوطني، أو أية بيانات حكومية سرية بطبيعتها، أو بمقتضى تعليمات صادرة بذلك، أو إلغاء تلك البيانات والمعلومات «الإلكترونيّة»، أو إتلافها أو تدميرها أو نشرها، أو إلحاق الضرر بالمستفيدين أو المستخدمين، أو الحصول على أموال أو خدمات أو مزايا غير مستحَقَّة».
ونص المشرع الإماراتي في المادة (22) من القانون الاتحادي الإماراتي، رقم (2) لسنة (2006)، بشأن مكافحة جرائم تقنية المعلومات، على أن يعاقب بالسجن كل من دخل، بغير وجه حق، موقعًا، أو نظامًا، مباشرة، أو عن طريق الشبكة المعلوماتية، أو إحدى وسائل تقنية المعلومات، بقصد الحصول على بيانات، أو معلومات حكومية سرية، إما بطبيعتها أو بمقتضى تعليمات صادرة بذلك... ويسري حكم هذه المادة على البيانات، والمعلومات الخاصة بالمنشآت المالية، والتجارية، والاقتصادية».
52 () في السياق ذاته، هناك العديد من تشريعات الأمن «السَّيبرانيّ» على مستوى العالم، نذكر منها على سبيل المثال: في الولايات المتحدة الأمريكية، قانون خصوصية الاتصالات «الإلكترونيّة» لعام (1986)، وقانون خصوصية الاتصالات لعام (1997)، وقانون خصوصية المعطيات لعام (1997). أما في ألمانيا، فنجد قانون حماية المعطيات، ومشروع قانون حماية البيانات عام (2000)، المتوافق مع القانون الأوروبي لعام (1995)، وفي فرنسا: قانون المعالجة الآلية للمعطيات، المعدل في عام (2000)، وفي النرويج: قانون تسجيل البيانات الشخصية لعام (2000)، وفي بلجيكا: قانون حماية الحياة الخاصة فيما يتعلق بالتعامل مع المعطيات الشخصية المعدل عام (2000)، وقانون حماية البيانات الشخصية والوثائق «الإلكترونيّة» لعام 2000، وفي بريطانيا: قانون حماية المعطيات لعام (1984)، وقانون حماية البيانات لعام (1998)، المُعدِّل لقانون (1984)، وقانون حرية المعلومات لعام (2000)، وفي اليابان: قانون حماية المعلومات، في الشخصية رقم (95)، الصادر في (16/12/1998)، وفي التشيك: قانون حماية البيانات الشخصية في نظم المعلومات لعام (1992)، وقانون حماية البيانات لعام (2000)، وفي هنجاريا: قانون حماية البيانات الشخصية ونشر البيانات للمصالح العامة لعام (1992)، وفي رومانيا: قانون حماية البيانات لعام (1992)، وفي كوريا الجنوبية: قانون حرية المعلومات لعام (1996)، وفي روسيا: قانون حماية المعلومات لعام (1995)، وفي إيطاليا: قانون حماية البيانات لعام (1996)، وفي ليتوانيا قانون الحماية القانونية للبيانات الشخصية لعام (1996)، وفي الصين: نظم حماية وإدارة الشبكات= =لعام(1997)، وفي تايلاند قانون حماية البيانات في القطاع العام لعام (1998)، وفي الهند: مشروع قانون حماية البيانات، الموصَى بإصداره من الفريق الوطني لتقنية المعلومات وتطوير البرمجيات، وفي جنوب أفريقيا: قانون الوصول إلى المعلومات لعام (2000)، وفي تركيا: مشروع قانون حماية البيانات الشخصية لعام (2000).
53 (53) Weisbord -David, cyber – conflict, cyber – crime, and cyber Espionage, Minnesota Journal of International Law's 2013 symposium, p. 3
For more: (1) Susan W. Brenner, cybercrime: - criminal threats for cyberspace (2010)
(2) Jonna than clough, principles of cybercrime (2010).
(3) Richard Clarke, threats to u.s. National security: proposed partnership initiatives towards preventing cyber terrorist Attacks, 12 Depaul Bus, L. J. (1999 – 2000).

الفرع الثاني
المواجهة التشريعية الأمريكية والفرنسية للتهديدات «السَّيبرانيّة»

بالنظر إلى التجربة الأمريكية في تعزيز الأمن «السَّيبرانيّ» نجدها تنقسم إلى شقين؛ أولهما: المعايير الفنية ((Technical standards، و الآخر: التشريعات والرقابة (Legislation and Monitoring) ونتناولهما كالتالي:-(54)

أولًا: المعايير الفنية:

تم إنشاء المعهد القومي للمعايير القياسية والتكنولوجيا، بوصفه باكورة أوليّة، في عام (1901)، وهو يتتبع وزارة التجارة الأمريكية، علاوة على وحدة المعلومات التابعة لمعمل تكنولوجيا المعلومات، حيث تضع سياسات ومعايير تبادل المعلومات، (55) ومن أهم اللجان: لجنة الحاسب الآلي والاتصالات، التابعة للمجلس القومي للبحوث، وترجع أهمية تلك اللجنة إلى أنها تشفر المعلومات والبيانات "cryptography". (56)

ثانيًا: التشريعات والرقابة:

لن تكتمل منظومة الأمن «السَّيبرانيّ» إلا بوجود إطار تشريعي؛ كي تُطبَّق معايير الأمن القومي المعلوماتي، لذا صدرت في الولايات المتحدة الأمريكية قوانين تعزز ذلك المفهوم، كقانون حرية المعلومات، في عام (1966)، ولئن كان غرض ذلك القانون هو تعزيز الحق في المعرفة وتداول المعلومات، فإنّ التعديلات اللاحقة على ذلك القانون كانت تهدف إلى تعزيز السرية والأمن المعلوماتي، والدليل صدور التعديل الذي يسمى مجموعة المعلومات «الإلكترونيّة» (Electronic freedom of Information Act، (EFIA))؛ لتعزيز الأمن «السَّيبرانيّ»، حيث يطالب جميع جهات الإدارة (بأتمتة الملفات)، أي جعل الملفات الورقية في صورة إلكترونية، وإعداد غرف خاصة لإطلاع المواطنين عليها.

ويأتي القانون الفيدرالي لأمن المعلومات، الصادر في عام (2002)، ليكون أهم التشريعات التي تعزز الأمن «السَّيبرانيّ» لجهة الإدارة في الولايات المتحدة الأمريكية، من خلال إلزام المؤسسات والهيئات بالإجراءات القياسية التي أصدرها المعهد القومي للمعايير القياسية والتكنولوجيا. (57)

وبالنظر إلى القانون الفيدرالي لإدارة أمن المعلومات، نجد أنه يشكل حجر الزاوية للأمن «السَّيبرانيّ» الأمريكي من الناحية القانونية؛ إذ يوفر إطارًا عامًا لتأمين نظم تكنولوجيا

54 () أنظر المري، راشد محمد: رسالة دكتوراه بعنوان «الجرائم «الإلكترونيّة» في ظل الفكر الجنائي المعاصر، رسالة مقدمة لكلية الحقوق جامعة القاهرة 2013 ص(182).
55 ()تفصيلا لذلك: يقوم ذلك المعهد بإصدار القواعد، والمعايير الفنية لتصنيف نظم المعلومات، على أنها نظم قومية، من وجهة نظر أمن المعلومات (مرجع سابق ص182).
56 () مرجع سابق ص (182)، في إشارة إلى المرجع:
Kasperson (W. K. Henrik) computer crimes & other crimes Against Information Technology in U. S. A., R. I. D. P. 2001, P. 273.
57 () لمزيد من الإيضاح أنظر :المري، 2013، مرجع سابق، ص(183)، وتتلخص المعايير المذكورة في: تعريف نظام المعلومات، وتحديد نوع المعلومات، من خلال تقسيمها في مجموعات محددة، وعمل توثيق كامل للنُظم، وعمل قياس للمخاطر التي قد يتعرض لها النظام.

المعلومات والمحتوى «السَّيبرانيّ» الرقمي في جميع الوكالات الفيدرالية الأمريكية، وكل الوكالات والمؤسسات الواردة في هذا القانون يتعين عليها تنفيذ الاحتياجات والمتطلبات التي يفرضها القانون، ويتعين عليها تقديم تقارير سنوية إلى مكتب الإدارة، والميزانية، والكونجرس، عن مدى فعالية وقدرة هذه الوكالات على تنفيذ برامج أمن المعلومات، وحماية ما لديها من معلومات. (58)

ويوفر القانون إطارًا لتأكيد فعالية السيطرة الإدارية على مصادر المعلومات، بما فيها حماية المعلومات الفيدرالية، ونظم المعلومات، مع تحديد الاختصاصات المتعلِّقة بكل رئيس وكالة فيدرالية(59).

ويهدف ذلك القانون إلى ثلاثة أهداف، هي:-

أولًا: السِّرية: بالاحتفاظ بالقيود المرخّص بها للوصول إلى المعلومات وكشفها، بما في ذلك الوسائل الخاصة بحماية الخصوصية الشخصية، والمعلومات المملوكة لجهة ما.

ثانيًا: السلامة: بمنع دخول معلومات غير صحيحة، أو إتلاف المعلومات.

ثالثًا: التوفُّر (الإتاحة): بضمان الوصول الفوري والموثوق به للمعلومات، واستخدامها.

علاوة على ما سبق، يمكن أن تقوم النُّظُم القانونية الأوروبية بتغليب الأمن «السَّيبرانيّ»، في حالة تهديد الأمن العام، كالذي جاء في المادة الثالثة، من القانون الفرنسي الصادر في (10 يوليو 1991)، حيث نصَّت على الأسباب القانونية التي يمكن الاستناد إليها لإجراء المراقبة، أو التنصُّت الإداري، وجاء فيها (يجوز الإذن، أو التصريح بالتنصُّت، الذي يكون موضوعه أو محله البحث عن المعلومات التي تهم الأمن القومي، أو المحافظة على المصالح الاقتصاديّة والعلمية للمجتمع الفرنسي، أو منع الإرهاب والمجموعات الإجرامية المنظمة، وكذلك منع تكوين أو إعادة تكوين المجموعات، التي تم حلها وفقًا لقانون (10، يناير 1963). (60)

58 () غطاس، بدون سنة نشر، مرجع سابق، ص (234). تفصيلًا لذلك: تم التصديق على هذا القانون، بوصفه جزءًا من قانون الأمن الداخلي، الذي تم إقراره عام (2002)، وقانون الحكومة «الإلكترونيّة»، ويطلب القانون من كُلّ الوكالات والمؤسسات الحكومية، تأمين معلوماتها، ونظم المعلومات لديها التي تدعم عملياتها وأصولها، بما فيها تلك التي تُقدَّم أو تدار بواسطة وكالات أخرى متعاقدة ومقاولين، أو أي مصدر آخر».

59 () «على كل رئيس وكالة فيدرالية»: 1) تقييم المخاطر واتجاهات الضرر الذي قد يحدث من عمليات الوصول، والاستخدام، والإفصاح، والتوزيع، والتعديل، والتدمير غير المرخّص به للمعلومات، أو لنظم المعلومات.

2) تحديد مستويات أمن المعلومات المناسبة لحماية كل المعلومات ونظم المعلومات بوكالته.

3) تنفيذ السياسات والإجراءات التي تقلل المخاطر لأدنى حد ممكن

4) القيام باختبارات دورية وتقييم لأدوات أمن المعلومات.

60 () د. أحمد،نشوى رأفت إبراهيم، حماية الحقوق والحريات الشخصية في مواجهة التقنية الحديثة «البيانات الشخصية، المراسلات والمحادثات الشخصية، الحق في الصورة» رسالة دكتوراه مُقدَّمة لكلية الحقوق، جامعة المنصورة، 2012. ص(277).

في السياق ذاته: اشترطت المادة الرابعة من القانون، أن يتم الإذن بالمراقبة بإذن مكتوب ومُسبَّب، يصدر من رئيس الوزراء أو من يقوم بتفويضه تفويضًا خاصًّا، وذلك بناءً على اقتراح مكتوب ومُسبَّب من وزير الدفاع، ووزير الداخليّة، والوزير المكلف بأعمال الجمارك». ومن الجدير بالذكر: أن شروط وضوابط المراقبة الإدارية تراقبها اللجنة القومية للرقابة. تفصيلًا لذلك، انظر بالتفصيل: ص(278) من مرجع سابق، فيما يخص اللجنة القومية للرقابة، وتشكيلها، وآليات عملها.

علاوة على ما سبق، يمكن التَّخلّي عن فكرة الخصوصية المعلوماتية إذا تعلق الأمر بالنظام العام للدولة، ومن ذلك: ما نص عليه قانون الأمن ومكافحة الإرهاب والجريمة (2001)، في المملكة المتحدة (الفصل 24)، حيث نصت المادة (17)، من الجزء الثالث منه، على نطاق سُلطات الكشف عن المعلومات؛ حيث تُحدِّد الفقرة الأولى بنودًا معينة لتلك السلطة، وأحالت للجدول رقم (4) المرفق بالقانون، ونصت الفِقْرة الثانية من المادة ذاتها على أن تلك البنود، الواردة في ذلك القسم، تُطبَّق للكشف عن المعلومات، بواسطة أو لمصلحة السلطة العامة؛ إذا كانت أغراض الكشف عن تلك المعلومات مصرَّحًا بها، بموجب البنود التالية:-

أ) لأغراض أيِّ تحقيق جنائي، سواء يجرى بالفعل، أو سيتم لاحقًا، وسواء بالمملكة المتحدة أو بأي مكان.

ب) لأغراض أيِّ إجراءات جنائية، سواء تتم بالفعل، أو ستبدأ لاحقًا، وسواء بالمملكة المتحدة أو بأي مكان آخر.

بالإضافة إلى ما سبق، صدرت العديد من قوانين الخصوصية الأمريكية على مستوى القطاعات (sectoral privacy laws)، ومن ذلك تبنى قسم الصحة والخدمات الإنسانية(The department of Health Human Services)، في العام (2001)، قواعد مصرحًا بها من الكونجرس، لا تجيز الإفصاح عن المعلومات الشخصية الصحيّة، ما لم يكن ذلك في إطار من القانون.(61)

وبالنظر إلى الحماية الواجبة للبيانات الشخصية الحسَّاسة عند تعزيز الأمن «السَّيبرانيّ»، فقد تضمَّن دليل حماية البيانات الأوروبي، لعام (1995)، حمايةً فاعلةً ضد استخدام تلك البيانات، كالبيانات المتعلقة بالصحة والأمور المالية، لذا ظهر التوجُّه الأوروبي نحو إيجاد جهة رقابة تعمل على تنفيذ القانون، فيما يُعرَف في بعض الدول باسم (المفوَّض) وفي دول أخرى (المراقِب)، وفي دول ثالثة (مسجِّل البيانات)، ويفرِض دليل حماية البيانات على الدول الأعضاء التزامات، فيما يخُص التَّأكُّد من الطابع الأمني للبيانات الشخصية التي ترتبط بالمواطنين الأوروبيين؛ كي تحظى بالمستوى نفسه من الحماية، إذا تم نقلها إلى خارج الحدود، ويَحظُر نقل البيانات إلى الدّول التي لا توفِّر قوانينها حمايةً للخصوصية. (62)

61 () While, facially restrictive, in reality, those rules permit broad disclosure of personal health information to the government in response to a warrant, court order, subpoena, discovery request administrative request, investigate demand or even a law enforcement official's "request".
For more:- see standards for privacy of Individually Identifiable Health Information, 65 fed. Feg. 82, 462 (2000) (codified at 45 C.F. R. pt. 160, 164. 502, 164. 506).

62 () الجنبيهي،منير محمد،و الجنبيهي،ممدوح محمد، أمن المعلومات « الإلكترونيّة»، دار الفكر الجامعي 2006، ص(84).

وبالنظر إلى التجربة الفرنسية في تعزيز الأمن «السَّيبرانيّ»، فإن فرنسا تُعدّ من أوائل الدول التي تدرجت التشريعات فيها، وبخاصة فيما يتعلق بمبدأ استغلال فضاء الدولة في بث المعلومات. (63)

وتتمثّل الإجراءات كذلك في رقابة جهة الإدارة مسبقًا على الرقابة في بث المعلومات، وتختلف تلك الرقابة بحسب النظام القانوني؛ ففي القانون الإنجليزي تكون الرقابة على بث المعلومات وفقًا للقواعد العامة، دون حاجة إلى الرجوع لجهة الإدارة بصفة عامة، وبالتالي تكون تلك الرقابة وفقًا للقواعد العامة دون الحاجة إلى وجود جهة إدارية مستقلّة، بينما تسلك العديد من التشريعات أسلوبًا مغايرًا في الرقابة، وبالتالي تكون الرقابة بين مجالس ولجان وجهات مختصة؛ فقد عرفت ألمانيا سلطة رقابة المفوِّض «وهو يعيَّن خصيصًا لنُظُم المعلومات، ويراقب عمليات بنوك المعلومات الشخصية. (64)

وبالنظر إلى الأسلوب الفرنسي في الرقابة، نجد أن الدولة أقامت نظامًا نموذجيًّا للرقابة على معالجة المعلومات وبثها، في القانون رقم (78–17) الصادر في (يناير 1978)، بشأن معالجة المعلومات والحريات(65)،وإلى جانب ذلك هناك لجنة أخرى للرقابة على بث المعلومات، باستخدام أجهزة الحاسب الآلي، وهي اللجنة الوطنية للاتصالات والحريات (C.N.C.L)، وقد خولها المشرع سلطة الرقابة بوسائل متنوعة على موضوع ومضمون البرامج التي يبثها الحاسب الآلي، وأساليب البث، وعمليات الإرسال المرخَّص بها قانونًا. (66)

المطلب الثاني

استراتيجية أمن المعلومات وأمن «الإنترنت» داخل المنشأة

الفرع الأول

استراتيجية أمن المعلومات داخل المنشأة

إن استراتيجية أمن المعلومات، أو سياسة أمن المعلومات، هي مجموعة القواعد التي يطبّقُها الأشخاص لدى التعامل مع التقنية، ومع المعلومات داخل المنشأة، وتتصل بشؤون الدخول إلى المعلومات، والعمل على نُظُمها وإدارتها، فالمعنيون بإعداد سياسة أمن المعلومات يتوزعون إلى مراتب وجهات عديدة داخل المنشأة، لكن بوجه عام تشمل: مسؤولي أمن الموقع،

63 () د. رشدي،محمد السعيد: «الإنترنت» والجوانب القانونية لنظم المعلومات، مؤسسة دار الكتب للطباعة والنشر والتوزيع، 1997، ص(56).
في السياق ذاته تعرَّض الرأي السابق إلى أن المشرع الفرنسي تبنى في البداية مبدأ حرية الاتصالات، في قانون (29 يوليو 1982)، ثم أصدر قانون (17 يناير 1989)، بشأن حرية الاتصال، وبعدها صدرت تشريعات لاحقة، خاصة (عام 1990)، بشأن تنظيم المرفق العام للبريد والاتصالات عن بعد، ثم مرسوم (4 فبراير 1992)، بشأن تحديد معدات الاستقبال المعتمَدة ومواصفاتها، وكل ذلك كشف بوضوح عن نية المشرع الفرنسي تحرير نظام البث عبر فضاء الدولة.

64 () مرجع سابق، ص(64، 65).

65 () مرجع سابق، ص(67).
تفصيلًا لذلك: من مهام اللجنة: الرقابة على تنفيذ معالجة المعلومات، وحماية النظام العام، واحترام حرّيّات الآخرين، وإنشاء نُظُم للمعلومات، وتلقي الإخطارات بذلك، والتحقق من احترام نظم المعلومات لأحكام القانون.

66 () راجع في موقف التشريع الفرنسي واتجاهات القضاء، فيما يتعلق بحماية المعلومات الشخصية، المجلة الدولية للقانون المقارن، 1987، ص(62) وما بعدها، مشار إليه في مرجع سابق ص66 وما بعدها.
والجدير بالذكر أن تلك اللجنة مستقلة في عملها ولا تخضع للسلطة الرئاسية أو الوصائية للجهاز الإداري في الدولة بل تخضع لرقابة القضاء فقط.

ومديري الشبكات، وموظفي وحدة الكمبيوتر، ومديري الوحدات المختلفة في المنشأة موحدة الأعمال، والتسويق، والبحث، وغيرها، وتشمل أيضًا: فريق الاستجابة للحوادث والأعطال، وممثلي مجموعات المستخدمين، ومستويات الإدارة العليا، إلى جانب الإدارة القانونية. وتضم استراتيجية المعلومات أيضًا: استراتيجية الاشتراكات التي تحدِّد سياسة المنشأة بشأن اشتراكات الغير في شبكتها أو نظمها، وكذلك استراتيجيات التعامل مع المخاطر، وإجراءات الإبلاغ عنها والتعامل معها، والجهات المسؤولة عن التعامل مع هذه المخاطر.(67)

وفي اعتقادنا أنه لكي توصف استراتيجية أمن المعلومات بأنها استراتيجية ناجحة، يتعين أن تُعمَّم بشكل شامل على كافة قطاعات الإدارة، وأن تكون مقبولةً واقعيًّا من المنوط بهم تنفيذها، إلى جانب توفر الأدلة التوجيهية والإرشادية؛ لضمان إدامة التنفيذ، وعدم التقاعس فيه. والتنفيذ هنا هو الاستخدام الفعلي لأدوات الحماية التقنية من جهة، والتطبيق الفعلي لقواعد العمل والتعامل مع البيانات ونظمها من جهة أخرى، ولا تحقِّق الاستراتيجية نجاحًا إن كان ثمة غموض فيها؛ لهذا لابد أن تكون واضحة دقيقة في محتواها، ومفهومة لدى كافة المعنيين.

أما من حيث المحتوى: فإن استراتيجية أمن المعلومات تمتد إلى العديد من المناحي المتصلة بنظم المعلومات، وإدارتها، والتعامل معها، إضافة إلى المسائل المتعلقة بالمعلومات ذاتها، وتعامل الغير مع معلومات المنشأة، من هنا تشكل الاستراتيجية سياسة واضحة بشأن اقتناء وشراء الأجهزة التقنية وأدواتها، والبرمجيات، والحلول المتصلة بالعمل، والحلول المتعلقة بإدارة النظام". (68)

وأما فيما يتعلق بالدخول إلى الشبكات والمعلومات، فلابد من استراتيجية دخول واضحة، تحدد حقوق وامتيازات كل شخص في المنشأة، للوصول إلى ملفات أو مواقع معينة في النظام، إضافة إلى سياسة بشأن التعامل مع الاتصالات الخارجية، والمعطيات: أجهزة، ووسائل الاتصال المستخدمة، وإضافة البرامج الجديدة، واستراتيجيات المراسلة مع الآخرين، لذا تشكِّل استراتيجية الخصوصية المعلوماتية، مراتب المعلومات، وقيمتها، ووصفها من حيث السرية، كما تبين الاستثناءات التي تعتمدها الاستراتيجية على حق الخصوصية لموظفي المنشأة، مع

67 ()عرب، 2001،مرجع سابق، ص (281) وما بعدها.
تفصيلا لذلك : تهدف استراتيجية أمن المعلومات إلى: تعريف المستخدمين والإداريين بالتزاماتهم، وواجباتهم المطلوبة لحماية نظم الحاسوب والشبكات، وكذلك حماية المعلومات بكافة أشكالها، وفي مراحل إدخالها، ومعالجتها، وخزنها، ونقلها، وإعادة استرجاعها، وتحديد الآليّات التي يتم من خلالها تحقيق وتنفيذ الواجبات، على كل من له علاقة بالمعلومات ونظمها، وتحديد المسؤوليّات عند حصول الخطر، وبيان الإجراءات المتَّبعة لتجاوز التهديدات والمخاطر والتعامل معها، والجهات المنوط بها القيام بها بذلك.
علاوة على ما تقدم، فإن الأسس التي تُبنى عليها استراتيجية أمن المعلومات، القائمة على الاحتياجات المتباينة لكل منشأة، تقوم على السرية (Con-fidentiality) من ناحية أولى، بمعنى: التأكد من أن المعلومات لا تُكشَف، ولا يُطّلع عليها من قبل أشخاص غير مخوَّلين بذلك، و التكاملية وسلامة المحتوى (Integrity) من ناحية ثانية، أي: التأكد من أن محتوى المعلومات صحيح، لم يتم تعديله أو العبث به، وبشكل خاص لن يتم تدمير المحتوى أو تغيره أو عن طريق تدخل غير مشروع، واستمرارية توفر المعلومات أو الخدمة (Availability) من ناحية ثالثة، أي: التأكد من أن مستخدم المعلومات لن يتعرض إلى إنكار استخدامه لها أو دخوله إليها.
68 () مرجع سابق، ص (281) وما بعدها.

مبررات هذه الاستثناءات، كرقابة البريد «الإلكترونيّ» مثلًا، أو رقابة الدخول إلى المنشأة، أو رقابة الوصول إلى ملفات المستخدمين بالمنشأة. (69) وفي ذلك: قضت محكمة الاستئناف الفرنسية، بإدانتها لمدير الشبكة بعد قيامه بإخبار رؤسائه بمضمون ما اطلع عليه (70)

الفرع الثاني

استراتيجية أمن «الإنترنت» داخل المنشأة

تنصب استراتيجية أمن «الإنترنت» على مواضع ثلاثة: أمن الشبكة، وأمن التطبيقات، وأمن النظام. وكل منها ينطوي على قواعد ومتطلبات تختلف عن الأخرى،ويتعين أن تكون أنظمة الأمن – في هذه المواضع الثلاثة – متكاملةً بعضها مع بعض؛ حتى تحقَّق الوقاية المطلوبة ؛ لأنها – بالعموم – تنطوي أيضًا على اتصال، وارتباط بمستويات الأمن العامة؛ كالحماية المادية، والحماية الشخصية، والحماية الإدارية، والحماية الإعلانية.

وفيما تقدم، أشرنا إلى العناصر المتصلة بأمن النظم، والبرمجيات، والمعطيات، وبقي أن نشير في هذا المقام إلى أمن الشبكات:

إن ما يُحمى من خلال أمن الشبكة هو: عملية الاتصال والتبادل بين أحد حواسيب الشبكة (النظام النهائي) – سواء أكان نظام الزبون، أو نظام المستضيف (الخادم) – وبين كمبيوتر آخر ضمن الشبكة، فإذا ارتبط النظام النهائي بـ«الإنترنت» مباشرة، دون وجود وسائل أمن ما بين هذا النظام والشبكة، فإن أية حزمة بيانات مرسلة قد يلحق بها ما يلي:

أ. قد يتم تغيرها خلال عملية النقل.

ب. قد لا تظهر من حيث مصدرها من الجهة التي قدمت منها.

ج. قد تكون جزء من هجوم يستهدف النظام.

69 () مرجع سابق، ص (281) وما بعدها.

- في السياق ذاته باتت مراقبة رسائل البريد «الإلكترونيّ» للعمال، من قبل شركاتهم، أمرًا شائعًا و مألوفًا في الولايات المتحدة الامريكية، حتى إن ثلث الشركات الكبرى في أمريكا و بريطانيا، تعين موظّفين يعملون خصوصًا على قراءة و تحليل رسائل البريد «الإلكترونيّ» للموظفين؛ خوفا من تسرُّب المعلومات العامة التي تخص الشركة، أو نقل فيروسات للنظام «الإلكترونيّ» للشركة، أو انعقاد مسؤوليتها القانونية نتيجة رسائل البريد «الإلكترونيّ» للموظفين.
- و يلاحظ أن للرئيس الاداري في العمل الحق في المتابعة، فله أن يتابع سير العمل اليومي، وله في سبيل ذلك مراقبة و تسجيل البيانات الموجودة على حاسبات الموظفين. ومن الجدير بالذكر: أنه بصدور قانون مكافحة الإرهاب، الصادر في اكتوبر (2001)، زادت سلطات جهاز الاستخبارات الامريكي في مراقبة الأفراد، سواء في أماكن عملهم أو في حياتهم الخاصة
- لقد سنَّ المشرِّع الانجليزي في (24 اكتوبر2000) قانونًا يُجوِّز لأرباب العمل استعراض اتصالات عمّالهم، التي تتم عبر الهواتف، سواء كانت ثابتة أو محمولة، و كذلك التي تتم عبر الشبكة، ولم يشترط علم العمال ورضاءهم، و لكن اشترط ان تكون الغاية من الاعتراض تحقيق أغراض مشروعة، و نص على هذه الأغراض، ومنها: منع، أو كشف الجرائم، والتحقق والكشف عن الاستعمال غير المسموح به للأدوات المهنية، و التأكد من حسن سير ادارة النظام « السَّيبرانيّ». و من الجدير بالذكر بأن النقابات العمالية وجهت نداءً بإلغاء هذا القانون؛ استنادًا إلى مخالفته نص المادة الثامنة من الاتفاقية الأوروبية لحقوق الانسان، و ذلك على إثر فصل هواتف محمولة لأربعين عاملا لديها، بعد نشر صور لهم مخلة بالآداب عبر البريد «الإلكترونيّ»، مما أعطى لأرباب العمل سندًا شرعيًا، لفحص وحدة الاقراص الصلبة للأجهزة الخاصة بهم، دون علمهم، ودون إذن منهم.

70 () مشار لذلك لدى د. العوضي،عبد الهادي فوزي -الجوانب القانونية للبريد « الإلكترونيّ» –دار النهضة العربية –بدون سنة النشر ص 158

- وتجدر الاشارة أن مدير الشبكة يلتزم بالمحافظة على سر المهنة أي أن له الحق في الاطلاع على مضمون البريد « الإلكترونيّ» وكل المعلومات الشخصية للمستخدمين كضمان حسن سير الشبكة واتخاذ الاجراءات الفنية والأمنية اللازمة،ألا أنه يلتزم بعدم نشر ما اطلع عليه بحكم طبيعة عمله كمدير الشبكة أو نشرها أو إذاعة مضمونها حتى لرؤسائه في العمل ويحظر عليه ضبط وسائل البريد « الإلكترونيّ» أو اعتراضها أو رفض سيرتها وإلا وقع تحت طائلة المساءلة القانونية وفقا للقوانين الخاصة بحمايةَ الخصوصية كالمادة 432/9 من قانون العقوبات الفرنسي.

د. قد لا تصل إلى العنوان المرسلة إليه.
ه. قد يتم قراءتها والاطلاع عليها وإفشاءها من الغير.

ويهدف أمن الشبكات – من جهة أخرى – إلى حماية الشبكة نفسها، وإظهار الثقة لدى مستخدم النظام النهائي، بتوفر وسائل الحماية في تعامله مع الشبكة، وكذلك إظهار الشبكة ذاتها على أنها تحتوي وسائل أمن، لا تتطلب معها أن يكون حاسوب المستخدم محتويًا على وسائل خاصة، وتتضمن وسائل أمن الشبكة ما يلي:

1- التعريف والسلامة، من خلال تزويد نظام المُستقبِل بالثقة في حماية حزم المعلومات، والتأكُّد من أن المعلومات التي وصلت لم يتم تعديلها.

2-السرية: بحماية محتوى حزم المعلومات من الإفشاء، إلا للجهات المرسلة إليها.

التحكم بالدخول: بتقييد الاتصالات، بحصرها ما بين النظام المرسِل والنظام المستقبل.

3- وترتبط استراتيجية أمن «الإنترنت» داخل المُنشأة بمناطق أمن المعلومات، من خلال أمن الاتصالات من ناحية أولى، ويراد بذلك: حماية المعلومات خلال عملية تبادل البيانات من نظام إلى آخر، وأمن الكمبيوتر من ناحية ثانية، ويراد بذلك: حماية المعلومات داخل النظام، بكافة أنواعها وأنماطها، كحماية نظام التشغيل، وحماية برامج التطبيقات، وحماية برامج إدارة البيانات، وحماية قواعد البيانات بأنواعها المختلفة. (71)

ولا يتحقق ذلك إلا من خلال أنماط ومستويات أمن المعلومات كالتالي:

1- الحماية المادِّية: وتشمل كافّة الوسائل التي تمنع الوصول إلى نظم المعلومات وقواعدها، كالأقفال، والحواجز، والغرف المحصنة، وغيرها من وسائل الحماية المادية، التي تمنع الوصول إلى الأجهزة الحساسة.

2- الحماية الشخصية: وهي تتعلق بالموظفين العاملين على النظام التقني المعني، من حيث توفير وسائل التعريف الخاصة بكل منهم، وتحقيق التدريب والتأهيل للمتعاملين بوسائل الأمن، إلى جانب الوعي بمسائل الأمن ومخاطر الاعتداء على المعلومات.

3- الحماية الإدارية: ويراد بها سيطرة جهة الإدارة على إدارة نظم المعلومات وقواعدها، مثل التحكم بالبرمجيات الخارجية أو الأجنبية عن المنشأة، ومسائل التحقيق باختلالات الأمن، ومسائل الإشراف، والمتابعة لأنشطة الرقابة، إضافة إلى القيام بأنشطة الرقابة ضمن المستويات العليا، ومن ضمنها مسائل التحكم بالاشتراكات الخارجية.

71 ()عرب 2001: مرجع سابق ص (281) وما بعدها .
في السياق ذاته، انظر للمزيد د. هلال، ناجي محمد سليم: الجرائم المستحدثة – تحليل سوسيولوجي – الهيئة المصرية العامة للكتاب – 2015.

4- الحماية الإعلامية – المعرفية: كالسيطرة على إعادة إنتاج المعلومات، وعلى عملية إتلاف مصادر المعلومات الحساسة عند اتخاذ القرار بعدم استخدامها.

وهناك خمسة أنواع أساسية لخدمات الأمن، تستهدف حماية خمسة عناصر رئيسية في ميدان المعلومات، وهي:

1- **خدمات (وسائل) حماية التعريف (Identification and authentication):**

هذه الخدمات تهدف إلى التثبت من الهُوِيّة، وتحديدًا عندما يقوم شخص ما بالتعريف عن نفسه؛ فإن هذه الخدمات تهدف إلى التثبت من أنه هو الشخص نفسه، ولهذا فإن التعريف يعد الوسائل التي تحمي من أنشطة التخفي والتنكر، ومن هنا فإن هناك نوعين من خدمات، التعريف الأول: تعريف الشخصية، وأشهر وسائلها: كلمات السر،والآخر: التعريف بأصل المعلومات، كالتثبت من أصل الرسالة.

2- **خدمات (وسائل) السيطرة على الدخول (Access Control):**

وهذه الخدمات تستخدم للحماية ضد الدخول غير المشروع إلى مصادر الأنظمة والاتصالات والمعلومات، ويشمل مفهوم الدخول غير المصرح به، ولهذا فإن خدمات التحكم بالدخول تعد الوسائل الأولية لتحقيق التخويل والتثبت منه.

3- خدمات (وسائل) السرية (Data and message Confidentiality):

هذه الخدمات تحمي المعلومات من الإفشاء للجهات غير المصرح لها بالحصول عليها، والسرية تعني بشكل عام إخفاء المعلومات، من خلال تشفيرها – على سبيل المثال – أو من خلال وسائل أخرى، كمنع التعرف على حجمها، أو مقدارها، أو الجهة المرسِلة إليها.

4- خدمات (وسائل) حماية التكاملية وسلامة المحتوى (Data and Message integrity):
هذه الخدمات تهدف إلى حماية مخاطر تغيير البيانات، خلال عمليات إدخالها، أو معالجتها، أو نقلها، وعملية التغيير تعني بمفهوم الأمن هنا: الإلغاء أو التحوير، أو إعادة تسجيل جزء منها، أو غير ذلك، وتهدف هذه الوسائل – أيضًا – إلى الحماية من أنشطة تدمير المعطيات بشكل كامل، أو إلغاءها دون تخويل.

5- خدمات (وسائل) منع الإنكار (Non – repudiation): وهذه الخدمات تهدف إلى منع الجهة التي قامت بالتصرف، من إنكار حصول نقل البيانات، أو النشاط من قبلها.

النتائج

1- إمكانية ملاءمة المفاهيم التقليدية للضبط الإداري للوسائل الحديثة في مجال الأمن «السَّيبرانيّ» كتأمين الشبكات، و تأمين بيانات الحكومة الإليكترونية

2 - أهمية الأمن «السَّيبرانيّ»، لاسيما في ظل تنامي التهديدات الأمنية «الإلكترونيّة»، على مستوى الدول، والمؤسسات العامة، والحكومية، والخاصة، سواء من جهة ارتفاع عدد الهجمات أو الأضرار الناجمة عنها، وأهمية التأمين «السَّيبرانيّ» في المناسبات الرياضية، التي تتسم بزخم في الأعداد، من خلال التعرض إلى الوسائل الحديثة للضبط الإداري .

3- تعدد صور التهديدات «السَّيبرانيّة» في المناسبات الرياضية، مما يستدعي مواجهة تلك التهديدات كلها أو جلها، من خلال المواجهة الإدارية للتهديدات «السَّيبرانيّة» من ناحية، والمواجهة التشريعية للتهديدات «السَّيبرانيّة»، و استراتيجية أمن المعلومات من ناحية أخرى.

4- التعرض إلى الوسائل الحديثة للضبط الإداري؛ حيث هناك العديد من الوسائل الحديثة إلى مواجهة شاملة لتلك التهديدات، ومنها: تأمين الشبكات على نحو يمنع من اختراقها، وثانيًا: تأمين بيانات الحكومة «الإلكترونية» فنيًا، من خلال وسائل الحماية الفنية لبيانات الحكومة «الإلكترونية»، كمثال الجدار الناري أو حوائط المنع (Fire Walls) ،ومكافحة الفيروس المعلوماتي.

التوصيات:

1- إدراج مادة ضمن المفردات العلمية لكلٍّ من كلية القانون والشرطة؛ لضمان فهم سلامة البنية المعلوماتية الوطنية من التهديدات «السَّيبرانيّة»، والإشراف على صياغة الكوادر المعلوماتية الوطنية، وإدخال مادة علوم التشفير ضمن المواد الأساسية في أقسام علوم الحاسبات، وهندسة الحاسبات، وإدخال مادة فيروسات الحاسوب في محاور بحوث الدراسات العليا، و هذا ما فعلته دولة قطر ، من خلال إنشاء برنامج بكالوريوس الأمن السبراني وأمن الشبكات بكلية المجتمع الذي يهدف إلى تزويد الطلاب بالمعرفة والمهارات الأساسية في مجال الأمن التقني والشبكات لتمكينهم لاحقاً من تلبية الاحتياجات الوطنية في مجال الأمن المعلوماتي والشبكات.

2- نقترح أن تعمل السلطات الادارية علي تحديث الآليات المعتادة لرصد وحيازة البيانات والمعلومات، ووضع إدارات، أو وحدات إدارية خاصة بنظم المعلومات وأمنها، بكل هيكل تنظيمي للوزارات والإدارات الحكوميةوغيرها.

3- أصبحت التطورات التكنولوجية، خاصة تكنولوجيا المعلومات، وتوسُّع مجالات استخدامها ومستخدميها تُشكِّل عاملًا أساسيًّا مباشرًا، مؤثرًا بشكل كبير في تطور وظهور الجرائم المستحدثة وعابرة الدول، وهو ما قد يمكن نعته بالفراغ القانوني، لذا لابد من سد ذلك الفراغ التشريعي، عن طريق الضبط التشريعي، وتأهيل رجال الضبط الإداري لمواجهة التهديدات «السَّيبرانيّة».

4- نقترح الاستعانة في سد الفراغ التشريعي، الناتج عن تطور وظهور الجرائم المستحدثة وعابرة الدول، بالتجارب التشريعية المقارنة لبعض الدول في الضبط التشريعي، وتأهيل رجال الضبط الإداري لمواجهة التهديدات «السَّيبرانيّة»، كالولايات المتحدة الأمريكية.

5- تعتمد جهة الإدارة عامَّةً على الضبط الإداري في مواجهة التهديدات «السَّيبرانيّة»، لذا لابد أن تحدث جهة الإدارة وسائلها؛ لتواجه الجرائم المستحدَثة التي نشأت بعد التطور التكنولوجي الهائل، من خلال تهيئة أدوات البيئة المعلوماتية الآمنة، وأولها الإدارة «الإلكترونيّة»، والحكومة «الإلكترونيّة».

6- نقترح أن تعمل الجهات الإدارية على وضع سياسة أمنية معلوماتية عامة للمواطن العادي، وسياسة أمنية معلوماتية أكثر خصوصية للموظف العام؛ لكون الأمن «السَّيبرانيّ» الحكومي الأكثر تطلُّبًا، والأكثر حساسية.

قائمة المراجع

أولًا: باللغة العربية:

1: المؤلفات العامة والمتخصصة :

1- قاموس مختار الصحاح، الطبعة الثالثة.

2- قاموس لسان العرب، الجزء التاسع، القاهرة، الدار المصرية للتأليف والترجمة.

3- البروفيسور/أورين كير، نطاق الجريمة الافتراضية، الأكاديمية الدولية للتجارة «الإلكترونيّة»، مؤسسة آدم للنشر والتوزيع (مالطا)، 2008.

4- ياسين، السيد، شبكة الحضارة المعرفية من المجتمع الواقعي إلى العالم الافتراضي ، الهيئة المصرية العامة للكتاب، 2009.

5- غطاس، جمال محمد: أمن المعلومات والأمن القومي، مكتبة نهضة مصر، دون سنة نشر،

6- د. الصغير، جميل عبد الباقي، أدلة الإثبات الجنائي والتكنولوجيا الحديثة، دار النهضة العربية، القاهرة، 2001.

7- د. بهنام، رمسيس، علم النفس القضائي، الإسكندرية، منشأة المعارف، سنة النشر غير مذكورة.

8- المري،راشد محمد، رسالة دكتوراه بعنوان: «الجرائم «الإلكترونيّة»في ظل الفكر الجنائي المعاصر، رسالة مقدمة لكلية الحقوق، جامعة القاهرة، 2013.

9- بوقرة،سامية: المخاطر المعلوماتية لنظم المعلومات وآليات مواجهتها، مجلة صوت الجامعة (2015)، تصدر عن الجامعة الإسلامية في لبنان.

10- د.الشرقاوي: سعاد، القانون الإداري، القاهرة، دار النهضة العربية،(1983)

11- د.الطماوى، سليمان محمد، الوجيز في القانون الإداري «دراسة مقارنة»، القاهرة، دار الفكر العربي، (1979).

12- د.الزغبي، محمد على فارس: الحماية القانونية لقواعد البيانات وفقا لقانون حق المؤلف-دراسة مقارنة ما بين النظام اللاتيني والنظام الأنجلوأمريكى

13- د. فوزي، صلاح الدين، الإدارة العامة بين علم متغير ومتطلبات التحديث - دار النهضة العربية 1998

14- د. الجرف :طعيمة: القانون الإداري والمبادئ العامة في تنظيم ونشاط السلطات الإدارية، القاهرة، دار النهضة العربية، 1978.

15- د.عطية، طارق إبراهيم الدسوقي: «الأمن المعلوماتي» (النظام القانوني لحماية المعلومات) دار الجامعة الجديدة 2009

16- د.أبو الخير: عادل، الضبط الإداري وحدوده – الهيئة المصرية العامة للكتاب – 1995.

17- د.عبادة :عبادة أحمد :- التدمير المتعمد لأنظمة المعلومات الإليكترونية – بحث منشور لدى مركز البحوث والدراسات، الإدارة العامة لشرطة دبى – مارس 1999.

18- م. د. حجازي: عبد الفتاح بيومي، مكافحة جرائم الكمبيوتر و«الإنترنت» في القانون العربي النموذجي «دراسة متعمقة في القانون المعلوماتي» - دار الكتب القانونية – 2007.

– نحو صياغة نظرية عامة فى علم الجريمة والمجرم المعلوماتي – دار النهضة العربية – الطبعة الأولى – 2009.

19- د. خليل: عزة محمود أحمد: مشكلات المسئولية المدنية فى مواجهة فيروس الحاسب – دراسة مقارنة فى القانون المدنى والشريعة الإسلامية – دار النهضة العربية – القاهرة – 1994.

20- د. القهوجي: على عبد القادر: الحماية الجنائية لبرامج الحاسب الآلي – دار الجامعة الجديدة – الإسكندرية – 1997.

21- د. الديربي: عبد العال والاستاذ اسماعيل: محمد صادق: الجرائم «الإلكترونيّة»دراسة قانونية قضائية مقارنة –الطبعة الأولى–المركز القومي للإصدارات القانونية القاهرة 2012

22- العقيد الحقوقي: عبد الله جعفر كوفلي: مراقبة الاتصالات في التنظيم الدولي والداخلي: المركز القومي للإصدارات القانونية الطبعة الأولى 2017.

23- أ. د. النوايسة،عبد الإله محمد: جريمة الدخول غير المشروع في تشريعات الجرائم «الإلكترونيّة» العربية «دراسة مقارنة» – المجلة القانونية والقضائية الصادرة من مركز الدراسات القانونية والقضائية وزارة العدل – دولة قطر – العدد الأول – (السنة العاشرة) يونيو 2016.

24- د. حب الله،عماد يوسف: ورشة عمل حول «بناء القدرات في مجال الحماية القانونية على «الإنترنت» 5-4 شباط 2009 - الهيئة المنظمة للاتصالات في لبنان - أمن الفضاء «السَّيبرانيّ» .

25- د .أبو صديق: فوزى، إشكالية المعلوماتية بين حق الخصوصية وإفشاء الأسرار المهنية، مؤتمر الأعمال المصرفية الإلكترونية، كلية الشريعة والقانون، الإمارات.

26- عبد الهادي: فوزي، الجوانب القانونية للبريد «الإلكترونيّ»، دار النهضة العربية، بدون سنة النشر

27- د. منصور، محمد حسين - المسؤولية «الإلكترونيّة»، دار الجامعة الجديدة للنشر، الإسكندرية، 2007.

28- د. البشرى: محمد الأمين: «التحقيق فى جرائم الحاسب الآلي»، بحث مقدم إلى مؤتمر القانون والكمبيوتر و«الإنترنت». مقدم إلى كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، الفترة من (3-1 مايو 2000م).

29- د .جعفر: محمد أنس قاسم، الوسيط فى القانون العام «أسس وأصول القانون الإداري»، دار النشر غير مذكورة، سنة النشر غير مذكورة.

30- د .الألفي: محمد محمد صالح: الجرائم المضرة بأمن الدولة عبر « الإنترنت»، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة.

31- د. الشريف: محمود سعد الدين،النظرية العامة للضبط الإداري، مقالة منشورة بمجلة مجلس الدولة، السنة الحادية عشرة، 1962.

32- د. خشبة: محمد سعيد، نظم المعلومات - المفاهيم والتكنولوجيا، بدون ناشر، 1990.

33- د. البنا: محمود عاطف، الوسيط فى القانون الإداري، القاهرة، دار الفكر العربي، 1984.

34- الرزو: مظفر حسن: الأمن المعلوماتي، معالجة قانونية أولية، مجلة الأمن والقانون، أكاديمية شركة دبى، السنة (12)، العدد (1)، 2006.

35- د. هلال :ناجى محمد سليم:- الجرائم المستحدثة - تحليل سوسيولوجى - الهيئة المصرية العامة للكتاب، 2015.

36- د. قوره: نائلة عادل محمد فريد، جرائم الحاسب الآلي الاقتصادية: دراسة نظرية وتطبيقية، منشورات الحلبى الحقوقية.

37- د. قشقوش: هدى، جرائم الحاسب الآلي فى التشريع المقارن – دار النهضة العربية – القاهرة – 1992.

38- د.رستم :هشام محمد فريد، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة، أسيوط، 1992.

39- عرب،يونس: قانون الكمبيوتر-موسوعة القانون وتقنية المعلومات، اتحاد المصارف العربية، 2001.

2- **المواقع «الإلكترونيّة»:**

https//:political-encyclopedia.org/dictionary/الأمن%20«السَّيبرانيّ»/

الموسوعة السياسية،موقع على شبكة « الإنترنت» -آخر تحديث 2020/4/17

ثانيًا: باللغة الإنجليزية:

Abraham D .Safaer ,National security and leaks ,the Government's Autority to Discipline itself .International studies in Human Rights volume16

- Brain bridge .D :introduction to computer law ,London ,2000 fourth edition
- Bruce P. smith, Hacking, Poaching, and counterattacking: Digital counterstrikes and the contours of self-Help, I J.L Econ, & Pol'Y 171, 173 (2005),
- Cezar PETA: cyber security – current topic of National security Public security studies, volume II, Issue 3)7) / 2013
- David weissbrodt, cyber – conflict, cyber – crime, and cyber Espionage, Minnesota Journal of Internatinal Law's 2013 symposium,
- Jona than clough, principles of cyber crime (2010).
- Nathan Alexander sales: Regulating cyper security – Northwestern university law Review 2013 vol., 107, No 4
- Richard Clarke, threats to u.s. National security: proposed partnership initiatives towards preventing cyber terrorist Attacks, 12 Depaul Bus, L. J. (1999 – 2000).
- Scott J. Shackelford, JD, PhiD, scott Russell, JD & Andreas juehn, Defining cybersecurity Due Diligence under International law: lessons from the private sector. 15.Electronic copy available at: http://ssrn.com/abstract =2594323
- Sieber Urlich, computer crimes and other crimes related to information technology. I.R.P.. 1994. Vol. 62
- Susan W. Brenner, cyber crime:- criminal threats for cyberspace (2010)
- Standards for privacy of Individually Identifiable Health Information, 65 fed. Feg. 82, 462 (2000) (codified at 45 C.F. R. pt. 160, 164. 502, 164. 506).
- Task force on national security in the information Age, Markle found creating AA Trasted Network for Homeland security (2003
- The Cantigny principles on technology terrorism, and privacy, National security law Report, feb. 2005, "The Cantigny" conference on counter terrorism technology and privacy organized by the standing committee on law and Nation security of the American Bar Association".
- The Emergence of cyber security law, prepared for the Indiana university Maurer school of law by Hanover Research, February, 2015