آليات تعزيز حق الإنسان في الأمن المعلوماتي

سهيلة هادي
طالبة دكتوراه، كلية الحقوق و العلوم السياسية،
جامعة محمد خيضر-بسكرة.

مقدمة:

تساهم تطورات تقنية المعلومات الحديثة و المتسارعة إحداث تغيرات في كافة المجالات، حيث أصبحت أهم علامات العصر الحالي التي لا يمكن الاستغناء عنها؛ لتأثيرها الواضح في تسهيل متطلبات الحياة العصرية من خلال التقليل من عاملي التكلفة، و الوقت في تسيير شؤون الحياة على مستوى عدة مجالات، لكن بالمقابل انتشار أنظمة المعلومات جعلها أكثر عرضة للقيام بالأنشطة غير القانونية، لذلك أصبحت هذه التقنية سلاحاً ذا حدين تحرص كل من المؤسسات، الدول، والمنظمات الدولية على توفير سبل الحماية له.

إن أهمية هذه الورقة البحثية تكمن في شيوع استخدام تكنولوجيا المعلومات وتكنولوجيا الحواسيب والانترنت في إدارة معظم الأنشطة الحياتية، ولضخامة الخسائر التي تسببها الجرائم الالكترونية أو أي عملية ناجحة تحت مسمى الحروب الالكترونية ،لاسيما في ظل التحولات الاقتصادية الراهنة؛ حيث أصبحت الدول تعتمد على الاقتصاد الرقمي و التجارة الالكترونية، بالإضافة إلى انتشار العالم الافتراضي الذي يعتبر مكانا لتفاعل الأفراد و الجماعات، ومنه أصبح الأمن المعلوماتي ضرورة قصوى خصوصا مع تعدد منافذ مهاجمة المعلومات الشخصية للأفراد و بيانات المؤسسات والدول، هذا ما جعل من الدول على غرار الجزائر، المنظمات الإقليمية و الدولية تسعى إلى المبادرة بمجموعة من الضمانات القانونية والآليات المؤسساتية واتخاذ إجراءات لتعزيز الأمن المعلوماتي الذي يعتبر من قضايا حقوق الإنسان المستحدثة.

انطلاقا مما تقدم سيتم طرح الإشكالية التالية:

كيف توفر الآليات الدولية و الوطنية ضمان الأمن المعلوماتي في ظل تنامي استخدام تقنية المعلومات؟

وللإجابة على هذه الإشكالية سيتم تقسيم الورقة البحثية إلى:

المبحث الأول: الاطار المفاهيمي للأمن المعلوماتي.

المطلب الأول: مفهوم الأمن المعلوماتي.

المطلب الثاني: مهددات أمن المعلومات.

المطلب الثالث: مكونات أمن المعلومات.

المبحث الثاني: الآليات الدولية و الوطنية لضمان الأمن المعلوماتي.

المطلب الأول: الآليات القانونية.

المطلب الثاني: الآليات المؤسساتية.

المطلب الثالث: الآليات الإجرائية.

المبحث الأول: الاطار المفاهيمي للأمن المعلوماتي.

المطلب الأول: مفهوم الأمن المعلوماتي (information security).

تكمن القيمة الحقيقية للمعلومات في دقة، صحة و مصداقية البيانات التي تحتويها، لذلك لابد من تحديد الأخطار المختلفة التي تهدد هذه المعلومات و ضمان أمنها لحمايتها من الأخطار المهددة لها.

إن أمن المعلومات يندرج ضمن إطار الأمن غير التقليدي، هذا الأخير ظهر نتيجة تفاعل الصراعات الداخلية و العوامل الخارجية ليترتب عن ذلك آثار تتميز بالتعقيد و التشابك، فهو يُعبر عن مجموعة مصادر التهديد التي تمتد من الإنسان الفرد إلى الوجود الإنساني، فهو يشمل المشاكل الاقتصادية، البيئية، الصحية، والاجتماعية متعددة المصادر التي تؤثر على حماية الحق المتساوي في الوجود و في الحياة الكريمة لمختلف الأفراد و الجماعات البشرية(1)، و نظرا لاعتبار الحق في سرية المعلومات وإتاحتها من حقوق الإنسان الحديثة ظهر الاهتمام بأمن المعلومات لاسيما في ظل التطور الذي تعرفه تقنيات المعلومات، و كثرة المعلومات وتشعبها الأمر الذي يُحتم المحافظة عليها وحمايتها.

يُقصد بأمن المعلومات؛ ذلك الأمن الذي يشمل العديد من المحاور من أهمها: الأخطاء العفوية أثناء إدخال البيانات إلى الحواسيب، فقدان المعلومات بسبب تعطل الحواسيب و حدوث خلل للبرامج ، سرقة المعلومات وفقدانها بسبب حدوث الكوارث الطبيعية(2)، ما يعني أن مصادر تهديد المعلومة قد تكون مقصودة أو غير مقصودة ، كما قد تكون بشرية (يتسبب بها الإنسان بطريقة مباشرة أو غير مباشرة) أو طبيعية نتيجة تأثير الكوارث الطبيعية.

1- محمد جمال مظلوم، **الأمن غير التقليدي**. الرياض: مركز الدراسات و البحوث، 2012، ص ص 76- 80.

2- دلال صادق، حميد ناصر الفتال، **أمن المعلومات**. عمان: دار اليازوري العلمية للنشر و التوزيع، 2008، ص 12.

وهناك من عرّف الأمن المعلوماتي استناداً للطبيعة الهادفة له، حيث « يهدف الأمن المعلوماتي (ثالوث الأمن المعلوماتي) إلى :

* **السرية:** من خلال التأكد من أنه لا أحد يرى المعلومات الخاصة بك.

* **النزاهة:** التأكد من أنه لم يتم تغيير المعلومات.

* **الوفرة:** التأكد من أن المعلومات متاحة للاستخدام عند الحاجة» (3).

بالتالي فالأمن المعلوماتي يهدف إلى تحقيق ثلاثة أبعاد أساسية هي : سرية، نزاهة ووفرة المعلومة بتوفير مجموعة من الضمانات القانونية، و الآليات المؤسساتية والإجرائية للحد من الجرائم الالكترونية.

هذا و تجدر الإشارة إلى أن المقصود من الدراسة ليس فقط السعي نحو تحقيق الأمن المعلوماتي المتعلق بالمنظمات الإدارية، بل أوسع من ذلك لأن؛ المعلومة في حد ذاتها لا ترتبط بالتنظيمات الإدارية فحسب بل ترتبط أيضا بالمنظمات السياسية، الاقتصادية، العسكرية والثقافية، إضافة إلى هذا ضمان الأمن المعلوماتي للأفراد والدولة، فالمعلومة محور ارتكاز الأنشطة اليومية للأفراد، وهي وسيلة وهدف للمنظمات الحكومية وغير الحكومية، الوطنية و الدولية، فعصر اليوم هو عصر المعلومات بامتياز؛ من يمتلك المعلومة يمتلك القوة، و لتوضيح مفهوم أمن المعلومات أكثر ينبغي توضيح بعض المصطلحات ذات الصلة منها:

تقنية المعلومات (information technology): «فهي تشمل الأجهزة و ما يتعلق بها من شبكات ونظم تشغيل البرامج، و من أهم الأجهزة الحاسب الآلي؛ و هو عبارة عن جهاز الكتروني يعمل طبقا لتعليمات محددة سلفا و يمكن استقبال البيانات و تخزينها و القيام بمعالجتها بدون الإنسان ثم استخراج النتائج المطلوبة»(4)، فتقنية المعلومات

3- Report Robert H. Williams. « introduction to information security consepts», [N.P], August 2007. p 3.

4- منصور بن سعيد القحطاني، « مهددات الأمن المعلوماتي و سبل مواجهتها «، **رسالة ماجيستير** ، (جامعة نايف العربية للعلوم الأمنية، كلية الدراسات العليا، قسم العلوم الإدارية، الرياض، 2008)، ص 17.

تدل على مجموع الأجهزة والشبكات التي يتم من خلالها تهديد الأمن المعلوماتي و تعزيز الأمن المعلوماتي، أي أنها أداة للهجوم و الحماية الالكترونية.

الجريمة الالكترونية (cybercrime) : « هي المخالفات التي تُرتكب ضد الأفراد أو المجموعات من الأفراد بقصد إيذاء سمعة الضحية أو الأذى المادي أو العقلي للضحية بطريقة مباشرة أو غير مباشرة باستخدام تقنيات الاتصالات مثل: الانترنت عبر غرف الدردشة، البريد الالكتروني و الموبايل»(5)، فهي نشاط غير قانوني يهدف إلى سرقة الهوية الشخصية، الهندسة الاجتماعية(6*)، الاختراق الأمني، كسر حماية البرامج و سرقة تفاصيل بطاقة الائتمان عبر الانترنت الأمر الذي ينجر عنه كسر لسرية، نزاهة ووفرة المعلومة.

الحرب الالكترونية (Electronic Warfare): يعتبر تعريف (ريتشارد كلارك)(Richard Clarke) مستشار البيت الأبيض من أبسط التعريفات و أشملها لهذا المصطلح حيث عرف الحرب الإلكترونية على أنها: «الإجراءات المتخذة من قبل الدولة لاختراق أجهزة الكمبيوتر والشبكات التابعة لدولة أخرى لغرض تحقيق أضرار بالغة أو تعطيلها»(7)، فالحرب الالكترونية حرب افتراضية تجري معاركها في الوسائط

5- ذياب موسى البداينة، « الجرائم الالكترونية: المفهوم و الأسباب» ورقة بحث مقدمة في **ملتقى** « الجرائم المستحدثة في ظل المتغيرات و التحولات الإقليمية و الدولية»، كلية العلوم الاستراتجية، عمان، 2 - 4 سبتمبر 2014. ص 3.

6-الهندسة الاجتماعة (Social Engineering): هي استخدام المهاجم حيلا نفسية لخداع مستخدمي الحاسوب للوصول إلى معلوماتهم؛ قد يتخذ الأسلوب الحسي (التجول في مكان العمل، الهاتف، سرقة المعلومات الموجودة في النفايات، إنشاء مواقع لتنزيل البرامج المجانية شرط إدخال اسم المستخدم و كلمة المرور و من ثم سرقتها)، و الأسلوب النفسي بإيهام الضحية أنه شخص موثوق به.

خالد بن سليمان الخثبر، مهندس محمد بن عبد الله القحطاني، **أمن المعلومات.** الرياض: مركز التميز لأمن المعلومات، جامعة الملك سعود، 2009، ص ص 34-31. متحصل عليه من :
http://download-internet-pdf-ebooks.com/2602-free-book

بتاريخ: 01-02-2017

7- Nathalie Caplan, « Cyber War: the Challenge to National Security», **Global Security Studies review**, Vol4 ., no.1 Winter 2013,p 94.

الالكترونية، تعتمد على تقنية المعلومات و البرامج وشبكات الانترنت مستهدفةً الدول المنظمات و الأفراد، و العديد من المجالات العسكرية الاقتصادية و الثقافية عن طريق الهجوم الإلكتروني.

يُلاحظ من خلال تعريفي الجريمة الالكترونية والحرب الالكترونية أنهما مصطلحان مترابطان كثيرا؛ فالفعل الناجم عن الحرب الالكترونية هو جريمة الكترونية، وكلاهما يعتبران انتهاك لحق الإنسان في الأمن المعلوماتي.

انطلاقا مما سبق نصل إلى المعادلة المتمثلة في أنه؛ من مصادرتهديد الأمن المعلوماتي الحروب الإلكترونية التي تعتمد على تقنية المعلومات لتحقيق أهدافها التي تُوجه نحو المعلومات والبيانات الأمر الذي يترتب عنه الجريمة الإلكترونية.

إن أهمية الأمن المعلوماتي تكمن في أهمية المعلومة في حد ذاتها باعتبارها كهدف و وسيلة لممارسة أنشطة وتحقيق أهداف الأفراد، المنظمات و الدول، وكذلك لتنامي تأثير التهديدات المعلوماتية على العديد من القطاعات منها(8) :

* قطاع الاتصالات و الأعمال الحكومية: و يشمل جميع شبكات الاتصال في الدولة شبكات الانترنت، مجالات البث التلفزيوني مراكز استقبال الموجات السلكية واللاسلكية، فأهمية هذا القطاع تجعل من اختراقه تهديدا للأمن القومي نظرا لما قد يتأثر به من سرقة وتعطيل واستخدام غير شرعي للمعلومات.

* قطاع الأعمال العسكرية و الحربية: نظرا لتنامي التهديدات الأمنية أصبح هذا القطاع يطلق نيرانا إلكترونية نتيجة اعتماده على الرقمنة، وفي حال اطلاع الخصم على بياناته الرقمية ما يعني هزيمته في أول ضربة عسكرية.

8-وليد غسان سعيد جلعود، « دور الحرب الالكترونية في الصراع العربي الإسرائيلي «، رسالة ماجيستير، (جامعة النجاح الوطنية، نابلس، 2013)، ص ص 96-90. متحصل عليه من :
https://scholar.najah.edu/sites/defaultfiles/%D9%88%D9%84%D9%8A%D8%AF%20%D8%AC%D9%84%D8%B9%D9%88%D8%AF.pdf
بتاريخ: 28-01-2017.

قطاع الإعلام: تأثير الحرب على هذا القطاع هو تأثير معنوي مما جعل منه بيئة مناسبة لحسم الحرب الالكترونية، لأنه في ظل الثورة المعلوماتية أصبح هناك الإعلام الالكتروني و الجمهور الذكي وأدوات التواصل التكنولوجية الحديثة.

القطاع الاقتصادي و قطاع الطاقة: نتيجة التحولات الاقتصادية و الالكترونية أصبحت تعتمد الاقتصاديات المتقدمة على الاقتصاد الرقمي القائم على وسائل التواصل الرقمي، البورصات وصكوك الانتساب الرقمي والإنتاج الرقمي و التجارة الالكترونية، و نظرا لارتباط الإدارات المسؤولة عن الطاقة في أي بلد بشبكات الانترنت التي تقوم عليها أنظمة الأمن و توزيع الطاقة مما جعل ضرب هذا القطاع يعود بانعكاسات سلبية على الاقتصاد.

انطلاقا مما تقدم يمكن القول أن الأمن المعلوماتي هو مجموعة الإجراءات التي تهدف إلى حماية معلومات الأفراد، المنظمات، و الدول؛ بالتصدي للتهديدات المعلوماتية التي تُؤثر على العديد من القطاعات والمجالات بهدف تحقيق سرية، نزاهة و وفرة المعلومة.

المطلب الثاني: مهددات أمن المعلومات.

تبرز الحاجة إلى الأمن المعلوماتي كحاجة جدّ ملحة، فهناك الكثير من الدراسات الاستطلاعية حول القضايا المتعلقة بحالات الهجوم الالكتروني و من أشهر المؤسسات التي تقوم بإعداد هذه الدراسات مؤسسة (CERT)، حيث سجلت عام 2003 حوالي 138000 حالة قرصنة، و في سنة 2004م تمّت دراسة أكثر من 500 شركة حيث بلغ مجموع الخسائر المالية الناجمة عن الهجمات الالكترونية لهذه الشركات حوالي 666 مليون دولار رغم أن هذه الشركات وظّفت تقنيات متعددة و حديثة للحماية كتقنية الجدران النارية بنسبة 98 %(9)، ما يعني أنه رغم استخدام التقنيات الالكترونية للحماية فهي غير كافية لضمان حمايتها و هذا راجع إلى:

9- خضر مصباح إسماعيل الطيطي، **أساسيات أمن المعلومات و الحاسوب**. عمان: دار حامد للنشر و التوزيع، 2010، ص 33.

* تعدد مصادر تهديد الأمن المعلوماتي الداخلية و الخارجية؛ فجميع الفواعل أفرادٌ، منظمات أو دولا هدفهم الاستحواذ على المعلومة و هذا الذي تنجر عنه الجرائم الالكترونية.

* التطور المتزايد لتكنولوجيا المعلومات و الاتصالات و تقنية المعلومات.

* وجود عقل بشري يهدف إلى امتلاك المعلومة لممارسة أنشطته، سعيا للبحث عن القوة، لاستغلالها في أعمال غير شرعية، إرضاءً لفضوله، أو بدافع الانتقام و الابتزاز.

تنبع مصادر تهديد الأمن المعلوماتي من طرف مصادر داخلية (داخل المنظمة، الدولة) و خارجية (خارج المنظمة، الدولة) يمكن توضيحها كالآتي:

الفرع الأول: مصادر تهديد الأمن المعلوماتي الداخلية.

تتمثل في مختلف مصادر التهديد التي تنتمي للجهة المستهدفة بالقيام بأعمال تضر حماية أنظمة المعلومات التي تستخدمها تلك الجهة، فمثلا؛ في تقرير صدر عن وزارة الدفاع الأمريكية عام 2000م ذكرت فيه أن 87 % من الهجمات المكتشفة التي استهدفت أنظمة المعلومات هي من طرف أشخاص من الوزارة نفسها، و بحسب تقديرات معهد أمن الحاسبات (CSI) فإن تكاليف الهجوم الالكتروني من الداخل هو 2.7 مليون دولار للهجوم الواحد مقابل 57 ألف دولار للهجوم من الخارج(10)، ما يعني أن مصادر التهديد الداخلية لا تقل خطورة عن مصادر التهديد الخارجية؛ لكون الذين يقومون باستهداف الأمن المعلوماتي للمنظمة على دراية بنظامها المعلوماتي وتفاصيل تسيير المنظمة، أما عن أسباب الهجوم الداخلي فقد تكون لعدة عوامل من بينها(11):

* اختلاس الصكوك، الأسهم، السندات، الأوراق المالية، و بيع المعلومات للأطراف المنافسة.

* إرضاء فضول فكري أو لتحدي إثبات أن المنظمات لا تملك نظاما معلوماتيا آمنا.

* وقوع صدام مع المنظمة أو التعرض لنقد شديد و غير موضوعي .

10- خالد بن سليمان الخثبر، مهندس محمد بن عبد الله القحطاني، **مرجع سابق**، ص ص 29-26.
11- دلال صادق، حميد ناصر الفتال، **مرجع سابق**، ص 16.

و لمواجهة تهديدات أمن المعلومات الداخلي ينبغي السعي نحو تحفيز العاملين في المنظمة ماديا ومعنويا و العمل على سيادة روح الفريق داخل المنظمة و إرساء جو يسوده التعاون و الاحترام، لتجنب خطر تهديد الأمن المعلوماتي الداخلي.

الفرع الثاني: مصادر تهديد الأمن المعلوماتي الخارجية.

هي مجموعة التهديدات الصادرة من خارج الجهة المستهدَفة، تكمن خطورتها في صعوبة و عدم معرفة مصدر الهجوم الالكتروني و مدى اختراقه لنظم المعلومات وحدود خبرته في التخريب، حيث تقوم هذه المصادر بحذف البرامج أو سرقتها أو تعطيل الأجهزة و إصابتها بالفيروسات أو قطع كابلات هذه الأجهزة، أو حتى إتلافها بالحرق أو استعمال المياه، إضافة إلى حذف أو نسخ المعلومات(12).

و رغم ما تُشكله مصادر تهديد الأمن المعلوماتي الداخلي من خطورة تعتبر مصادر تهديد الأمن المعلوماتي الخارجي خطرا للمنظمات و الأمن القومي للدولة؛ فقد أفرزت العديد من المخاطر من بينها الإرهاب الإلكتروني(Cyber terrorism)؛ هذا الأخير الذي يحظى باهتمام الدول والمنظمات الدولية للتصدي للهجمات التي تعتمد على أساليب جديدة و متطورة، حيث بدأت التنظيمات الإرهابية اِتباع آليات خطيرة لتحقيق أهدافها التي لم يقتصر نشاطها على المجال المادي بل انتقل إلى الفضاء الالكتروني الذي أصبح عاملا مساعداً للعمل الإرهابي؛ بتوفير المعلومات و الحصول على التمويل والتبرعات وعملية التجنيد وممارسة الأعمال التخريبية لشبكات الحاسوب و الانترنت ونشر الأفكار المتطرفة (حرب الأفكار)، إضافة إلى التنسيق بين الجماعات الإرهابية لتحقيق الأهداف المبتغاة في أسرع وقت و بدقة عالية، و هو الأمر الذي ساهم بشكل كبير في اختراق بيانات الأفراد ذات الطابع الشخصي و المنظمات بحجة مكافحة الإرهاب بصفة عامة والإرهاب الإلكتروني بصفة خاصة. هذا و من بين أشكال تهديد أمن المعلومات على سبيل المثال لا الحصر(13):

12- منصور بن سعيد القحطاني، **مرجع سابق**، ص 42.

13- خضر مصباح إسماعيل الطيطي، **مرجع سابق**، ص ص 32-30.

* التطفل : ويتم باعتاراض المعلومات بين الأطراف بطريقة غير شرعية من خلال؛ التنصت على الاتصالات أو تصفح ملف ما أو النظام المعلوماتي.

* التعديل: و هي عملية تستهدف تغيير أو تعديل للمعلومات بعد اطلاع المتطفل؛ بقراءة محتوى الرسالة من الطرف الأول إلى الطرف الثاني، مع احتمال قيام المتطفل بالرد دون إشعار الطرفين بوجود طرف وسيط.

* انتحال شخصية: و هو نوع من الخداع بإيهام الضحية على التصديق بأن الكائن المزور الذي يتعامل و يتواصل معه هو الكائن الحقيقي، و ذلك بهدف معرفة مثلا: رقم بطاقة الدفع المالي الالكتروني وكلمة المرور لسرقة الأموال أو قراءة ملف ما.

* إنكار الإرسال و استلام رسالة أو ملف ما؛ كأن يقوم زبون بإرسال رسالة إلى تاجر يؤكد فيها موافقته على دفع مبلغ مالي كبير لمنتج ما، و بناءً على ذلك يقوم التاجر بشحن هذا المنتج إلى الزبون و بعد ذلك يُنكر الزبون طلب هذا المنتج.

مما سبق يتضح أن مصادر و مخاطر تهديد أمن المعلومات عديدة و هذا راجع إلى:

* ميزة عصر المعلومات؛ فالمعلومة تساهم في تحقيق ميزات اقتصادية، سياسية و أمنية و حتى ثقافية.

* تعدد أسباب و وسائل تهديد الأمن المعلوماتي.

المطلب الثالث: مكونات أمن المعلومات.

لتحقيق الأمن المعلوماتي بشكل فعال لا بد أن تكون نظم المعلومات مبنية على ثلاثة مكونات أساسية بحيث يتوجب على كل منظمة و دولة أن توفرها بوضع القوانين الضامنة لها، و الآليات المؤسساتية و الإجرائية لتعزيز هذه المكونات و التي تتمثل في:

الفرع الأول: سرية المعلومات (Confidentiality).

«هي عملية ضمان حفظ المعلومات المخزنة أوالمنقولة عبر الشبكة وعدم الاطلاع عليها أو استخدامها لأية أغراض دون إذن» (14).

14-منصور بن سعيد القحطاني، **مرجع سابق**، ص 21.

تتنامى أهمية سرية المعلومات لتزايد التنافس الشديد بين مختلف أنواع الشركات، و نظرا لكون هذه الأخيرة تعتمد في جميع تعاملاتها على الحاسوب و شبكة الانترنت فهي بحاجة إلى حماية معلوماتها من مخاطر تهديدات القراصنة الذين يسعون إلى التخريب و الوصول إلى الملفات السرية للأفراد ، المنظمات و الدول.

الفرع الثاني: سلامة المعلومات (Integrity).

تعني ضمان عدم التغيير في المعلومات المخزنة أو المنقولة، و لها بُعدان؛ سلامة البيانات و المعلومات المرسلة، و سلامة المصدر أي مصدر إرسال البيانات والمعلومات، هذا و تجدر الإشارة إلى أن عملية الحفاظ على سلامة المعلومات أصعب بكثير من الحفاظ على سريتها؛ فضمان سرية المعلومات يتم بالحفاظ على سريتها، أما الحفاظ على سلامة المعلومات فتشمل ضمان السرية وعدم التغيير في البيانات(15).

و نظرا لانتشار محادثات الدردشة عبر العديد من مواقع التواصل الاجتماعي، و الاتصالات الالكترونية من خلال البريد الالكتروني، و العمل على تطبيق الحكومة الالكترونية فقد أصبح الاتصال عبر الوسائط الالكترونية واسع الانتشار و بالمقابل عرضة للتنصت و لاختراق الاتصالات الالكترونية وسرقة المعلومات، التطفل و انتحال الشخصية و غيرها من أشكال تهديد أمن المعلومات.

الفرع الثالث: وفرة المعلومات(Availability). وهي تعني ضمان بقاء المعلومات وعدم حذفها أوتدميرها؛ كأن تكون مواقع صفحات الانترنت متاحة للاستخدام 24/24 ساعة وسبعة أيام في الأسبوع، بحمايتها من أي هجوم قرصنة للموقع الالكتروني و خرق للإجراءات الأمنية الالكترونية، وتجدر الإشارة إلى أنه حتى كبرى الشركات تتعرض أيضا لعمليات القرصنة مثل شركة (ياهو) (yahoo) و شركة (هوتمايل) (hotmail) فقد تم تعطيلهما لمدة 24 ساعة (16)، في هذا الصدد يعتبر من التحدي الكبير ـ للدولة والمنظمات الإدارية ـ حماية قواعد البيانات والمعلومات الخاصة بكل دولة ومواطنيها من سجلات أحوال مدنية وجنائية، الإحصائيات السكانية و غيرها، عقود الملكيات

15-خضر مصباح إسماعيل الطيطي، **مرجع سابق** ، ص ص 26، 28.

16-**المرجع نفسه**، ص ص 28، 29.

و المعلومات البنكية، والقدرة على حمايتها من الاختراق وتدميرها أو التلاعب بها أو استغلالها، لذلك تعتبر الجريمة الالكترونية أهم تحدٍ للحكومة والإدارة الالكترونية.

إن هذه المكونات عبارة عن هرم قاعدته سرية المعلومات، ووسطه يتمثل في سلامة المعلومات لتكون وفرة المعلومات في قمة الهرم؛ أي أنه لا يمكن ضمان أمن المعلومات في ظل غياب أحد مكوناته، فسرية المعلومات تعزز من سلامتها، لتأمين الدعم لوفرة المعلومات.

المبحث الثاني: الآليات الدولية و الوطنية لضمان الأمن المعلوماتي.

المطلب الأول: الآليات القانونية.

تتعدد ضمانات تعزيز الأمن المعلوماتي على المستوى الدولي، الإقليمي و الوطني؛ و هذا راجع للتهديدات المعلوماتية التي لم تستثن أية دولة، لذلك تُبذل الجهود سواء من طرف المنظمات الدولية، الإقليمية و الدولة في إطار سيادتها على إقليمها للتصدي للتهديدات التي تعتبر تعدياً على خصوصية الإنسان و انتهاك لحقه في سرية معلوماته، لكن السؤال الذي يطرح نفسه هو : هل تعتبر الآليات القانونية المتخذة على المستوى الدولي، الإقليمي و الوطني كفيلة لتعزيز الأمن المعلوماتي؟

الفرع الأول: على المستوى الدولي.

من بين الجهود الدولية التي تم اعتمادها من أجل دعم المنظومة القانونية لدرء مخاطر الجرائم الالكترونية على سبيل المثال لا الحصر:

أولا: منظمة الأمم المتحدة) (United Nations. لقد تبنت منظمة الأمم المتحدة دليلا يتعلق باستخدام الحاسبات في تدفق البيانات الشخصية سنة 1989م، وفي سنة 1990 م تبنت الهيئة العامة دليل تنظيم استخدام المعالجة الآلية للبيانات الشخصية، و هي مبادئ غير ملزمة للدول الأعضاء لضمان التدابير التشريعية للتصدي للجريمة الالكترونية(17) و هو الذي يُقوض من فعالية هذا الدليل لأن محتواه كان مجرد توصيات للدول لتعزيز أمنها المعلوماتي.

17- منير محمد الجنبيهى، ممدوح محمد الجنبيهى، **أمن المعلومات الالكترونية.** الإسكندرية: دار الفكر الجامعي، 2006، ص 73.

و لقد عقدت منظمة الأمم المتحدة مؤتمرها الثاني عشر بالبرازيل سنة 2010م؛ و دعت من خلاله لجنة منع الجريمة و العدالة الجنائية إلى اجتماع خبراء حكومي دولي لدراسة الجريمة المعلوماتية و اتخاذ تدابير مواجهتها، و في مؤتمرها الثالث عشر بقطر سنة 2015م؛ صدر عن الجمعية العامة القرار 67 /184 المتعلق بإنشاء حلقات لتعزيز تدابير الجرائم المعلوماتية، و من بين قرارات الجمعية العامة للأمم المتحدة المتعلقة بالأمن المعلوماتي القرار رقم 57 /239 المؤرخ في 31 /01 /2003 والقرار 58 /199 المؤرخ في 30 /01 /2004 المتعلق بإنشاء ثقافة عالمية للأمن المعلوماتي و دعوة الدول الأعضاء للتعاون على تعزيزها، إضافة إلى قرار لجنة مكافحة المخدرات 48 /5 حول تعزيز التعاون الدولي لمنع ارتكاب الجرائم المتعلقة بالمخدرات باستخدام الانترنت، إضافة إلى القرار رقم 55 /63 المتعلق بمكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية؛ فقد أكدت فيه على ضرورة أن تعمل الدول على تدريب العاملين في مجال القوانين وتزويدهم بما يحتاجون لمكافحة إساءة استعمال التكنولوجيا(18)، تبدو جهود الأمم المتحدة جلية لتسليط الضوء على هذا النوع من الجرائم الحديثة من خلال المؤتمرات التي تنظمها والقرارات الصادرة عنها التي تهدف أساسا إلى تعزيز دعم التعاون الدولي للتصدي للجرائم المعلوماتية و تنمية الوعي العالمي بالأمن المعلوماتي من أجل تعزيز ثقافة الأمن المعلوماتي على المستوى الداخلي للدول.

ثانيا: الاتحاد الدولي للاتصالات(The International Telecommunication Union) . يسعى إلى تنظيم الاتصالات الدولية من خلال المعاهدات و الأنظمة الملزمة و المعايير غير الملزمة، فاللوائح تمنع التدخل في خدمات الاتصالات للدول الأخرى و لكنها ترخص السيطرة على الاتصالات لدواعي أمنية(19)، فرغم الجهود التي يبذلها الاتحاد الدولي للاتصالات إلا أن بعض الأنظمة غير الملزمة تعتبر عائقا أمام فعالية دور الاتحاد

18- فاروق خلف، « الآليات القانونية لمكافحة الجريمة المعلوماتية « ورقة بحث مقدمة في **الملتقى الوطني** « الجريمة المعلوماتية بين الوقاية و المكافحة» ، جامعة محمد خيضر، بسكرة، 2015. ص 5.

19-Report Catherine A. Theohary ,John W. Rollins. « Cyberwarfare and Cyberterrorism: In Brief », [N.P], Congressional Research Service , March 27, 2015. p ٨.

في تعزيز الأمن المعلوماتي، هذا فضلا عن التذرع بالدواعي الأمنية واستغلال التحديات الأمنية للتنصت على الدول شعوباً وحكومات للتجسس عليها، فحتى قادة الدول الكبرى تعرضوا للتنصت على مكالماتهم الهاتفية مثل: الرئيس الأمريكي (باراك أوباما) (Barack Obama) والمستشارة الألمانية (أنجيلا ميركل) (Angela Merkel).

ثالثا: حلف شمال الأطلسي الناتو) (North Atlantic Treaty Organisation.
تم اتخاذ التدابير المضادة للهجوم الالكتروني من خلال تعزيز سياسة الدفاع الالكتروني؛ فقد اعتمد الحلف سنة 2008م سياسة رسمية تجاه الفضاء الالكتروني أهم ما تقوم عليه هو تقديم المساعدة عند الطلب، والتعاون القائم على الثقة دون تغاضي النظر عن حساسية المعلومة، هذا و قد تم إضافة إلى سياسة الناتو التهديدات الالكترونية كمصدر محتمل للدفاع المشترك وفقا للمادة 05 من ميثاق الناتو(20)، هذا الذي يعكس تنامي التهديدات الأمنية الالكترونية من جهة، و التخوف الدولي وعجز الدولة منفردةً مواجهة الحروب الالكترونية و الجرائم المعلوماتية من جهة أخرى لذا تبرز ضرورة التعاون الدولي في هذا المجال.

انطلاقا مما تقدم يُلاحظ بروز الاهتمام من طرف المنظمات الدولية لتعزيز الأمن المعلوماتي و هو الأمر الذي يعكس خطر التهديدات المعلوماتية على الأمن القومي و تداعياتها على حق الإنسان في أمنه معلوماتيا، لكن ينقص هذه الجهود الدولية طابع الإلزامية لكي تتجسد هذه الجهود على أرض الواقع، وهذا راجع إلى:

أ - التفاوت الموجود بين الدول المتقدمة و الدول النامية و الدول المتخلفة: فهناك دول متطورة تقنيا تكنولوجيا و معلوماتيا عكس دول أخرى.

ب - المنافسة و تضارب المصالح بين الدول: فالدول اليوم تشهد نوع جديد من الحروب التي تتمثل في الحروب الالكترونية؛ لذلك ليس من مصلحة بعض الدول تعزيز المنظومة القانونية المتعلقة بالأمن المعلوماتي؛ كونها هي من تشن الهجومات الالكترونية على الدول التي تتعارض مع مصالحها.

20-مجلة الناتو، « التهديدات الجديدة: الأبعاد الالكترونية «. متحصل عليه من : http://www.nato.int/docu/AR/Threads-Cyber/september-٢٠١١/review-ind.ex-htm

بتاريخ: 06-02-2017.

الفرع الثاني: على المستوى الإقليمي.

فقد تمّ إبرام اتفاقية مجلس أوروبا (Council of Europe) بشأن الجريمة الالكترونية والمعروفة أيضا (باتفاقية بودابست) سنة 2001 م، وهي أول معاهدة دولية لملاءمة القوانين في مختلف الدول فيما يخص النشاط الإجرامي في عالم الانترنت، بحيث تُلزم الدول الموقعة على اتخاذ القوانين الجنائية ضد أنواع محددة من الأنشطة في الفضاء الالكتروني، وما يميز هذه الاتفاقية ـ وإن كانت بالأساس إقليمية ـ هو إمكانية مصادقة الدول غير الأوروبية عليها مثلما قامت به الولايات المتحدة الأمريكية(21)، فهي تعتبر من أهم الاتفاقيات الداعمة للأمن المعلوماتي، وتستمد أهميتها من الطابع الإلزامي لها من خلال توحيد القوانين المتعلقة بالجرائم الالكترونية بين الدول الموقعة عليها.

حيث تنص الفقرة الأولى من المادة 24 من اتفاقية بودابست على أنه: «تنطبق على تبادل المجرمين بين الأطراف بالنسبة للجرائم الجنائية المعرفة وفقا للمواد 11-2 من الاتفاقية (22*) الحالية شريطة أن يكون معاقباً عليها في قانون الطرفين بعقوبة سالبة للحرية لا تقل عن سنة أو بعقوبة أشد»، وتنص المادة 25 من نفس الاتفاقية على أنه: « يجب على كل الأطراف أن توفر لبعضها بعضاً مساعدة قضائية متبادلة إلى أقصى مدى ممكن لأغراض التحقيقات أو الإجراءات بالنسبة للجرائم الجنائية المرتبطة بنظم وبيانات معلوماتية أو بغرض جمع الأدلة الالكترونية المرتبطة بنظم وبيانات معلوماتية أو بغرض جمع الأدلة الالكترونية للجريمة الجنائية»(23)، فاتفاقية بودابست لم تهمل المساعدة القضائية بين الدول الموقعة على الاتفاقية، هذا الذي يعتبر عاملا مساعداً لتعزيز الأمن المعلوماتي خصوصا وأنها اتفاقية تتسم بإلزامية التضمين في الأنظمة القانونية الداخلية للدول الموقعة عليها، فمثلا الفقرة الأولى من المادة 24 من الاتفاقية

21- Report Catherine A. Theohary ,John W. Rollins, **Op.cit** . p 7.

- تتعلق المواد 2- 11 من اتفاقية بودابست بالولوج و الاعتراض غير القانوني، الاعتداء على سلامة البيانات، إساءة استخدام أجهزة الحاسوب، التزوير و الغش المعلوماتي، و الجرائم المتعلقة بالمواد الإباحية للأطفال و الاعتداءات على الملكية الفكرية . هلالى عبد الله أحمد، **اتفاقية بودابست لمكافحة جرائم المعلوماتية.** القاهرة: دار النهضة العربية، 2007، ص ص 8، 9.

23- المرجع نفسه، ص ص 308، 325.

حدّدت تسليم المجرمين كنوع من التعاون لمكافحة الجرائم المعلوماتية، إضافةً إلى ضبطها لنوع الجرائم المتعلقة بالتعاون القضائي بين الدول الموقعة على الاتفاقية.

الفرع الثالث: على المستوى الوطني (على ضوء التشريع الجزائري).

لتكييف المنظومة القانونية مع المتغيرات الراهنة لم يُغفل المشرّع الجزائري أهمية تعزيز الأمن المعلوماتي بتعديل قانون العقوبات، و سن بعض التشريعات الأخرى، ويتمثل أهمها في:

أولا: قانون رقم 04 - 15 المتعلق بقانون العقوبات. إذْ أن المشرع في المادة 394 مكرر نصّ على أنه: «يعاقب بالحبس من ثلاثة (3) أشهر إلى سنة (1) و بغرامة مالية من 50.000 إلى 100.000 كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة للمعطيات أو يحاول ذلك»(24)، ما يعني أن المشرع أكد على تعزيز مكونات الأمن المعلوماتي سابقة الذكر (سرية، سلامة و إتاحة المعلومة) و هذا الذي يتجلى من خلال معاقبة حتى من يحاول تهديد الأمن المعلوماتي، أو بمعنى آخر فالعقوبة تقع حتى في حالة نجاح الاختراق للمنظومة المعلوماتية دون حذف أو تعديل للمعلومات والبيانات لأن هذا الفعل يُعد بمثابة اطلاع غير شرعي على المنظومة المعلوماتية.

هذا و يؤكد المشرع في المادة 394 مكرر 3 بأن العقوبة تتضاعف إذا تم استهداف منظومة الدفاع الوطني و المؤسسات الخاضعة للقانون العام، و في المادة 394 مكرر 6 تطرق إلى غلق المواقع التي تكون محلا لجريمة من الجرائم المعاقب عليها في حالة المساس بالأنظمة الآلية لمعالجة المعطيات(25). إنّ حرص المشرع على مضاعفة العقوبة في حالة استهداف أي مؤسسة خاضعة للقانون العام بصفة عامة والدفاع الوطني بصفة خاصة معلوماتياً يرجع لحساسية معلومات هذه المؤسسات و تأثيرها على استقرار الدولة على كافة المستويات.

24- الجمهورية الجزائرية الديمقراطية الشعبية، « قانون رقم 04 - 15 المتضمن قانون العقوبات»، **الجريدة الرسمية**. العدد 71، الصادرة بتاريخ: 10 /11/ 2004، ص 11.

25-المرجع نفسه، ص 12.

ثانيا: قانون رقم 09 - 04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال و مكافحتها. لقد تطرق للحالات التي تسمح بمراقبة الاتصالات الالكترونية للوقاية من الجرائم التي تمس أمن الدولة كالإرهاب أو الاقتصاد الوطني أو لصعوبة الوصول إلى الحقيقة في التحقيقات القضائية، و في إطار تنفيذ طلب المساعدة القضائية الدولية، هذا و قد وضّح إجراءات تفتيش و حجز المعطيات المعلوماتية في الفصل الثالث من القانون(26) ، فالقانون رقم 04-09 يُعتبر من القوانين التي فصلت كثيرا في كيفية التصدي للجرائم الالكترونية من خلال؛ توضيح حالات مراقبة الاتصالات الالكترونية، و القواعد الإجرائية لتفتيش المنظومات المعلوماتية، و في التزام مقدمي الخدمات تقديم المساعدة للسلطات إذا اقتضت الضرورة ذلك.

أما في الفصل الخامس فقد تعلق باستحداث الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال و مكافحتها التي تعمل على التنسيق فيما يخص عمليات الوقاية من الجرائم المتعلقة بتكنولوجيا الإعلام والاتصال و مكافحتها، و مساعدة السلطات القضائية ومصالح الشرطة القضائية في هذا الخصوص، و كذلك تبادل المعلومات مع الدول الأخرى للتعرف على مرتكبي الجرائم المرتبطة بتكنولوجيا الإعلام و الاتصال، و في هذا الصدد لقد خص المشرع الفصل السادس من هذا القانون للتعاون والمساعدة القضائية الدولية مع التأكيد في المادة 18 على أنه تقابل بالرفض طلبات المساعدة التي تمس السيادة الوطنية و الأمن العام(27).

إن الفصل الخامس من القانون رقم 04-09 يعتبر من أهم فصول هذا القانون؛ كونه استحدث هيئة وطنية تساهم في تعزيز الأمن المعلوماتي هذا من جهة، و من جهة أخرى يعكس تفطن المشرع الجزائري في المادة 18 لإمكانية استغلال المساعدة القضائية الدولية للتدخل في الشؤون الداخلية للدول.

26-الجمهورية الجزائرية الديمقراطية الشعبية، " قانون رقم 09 - 04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها"، **الجريدة الرسمية**. العدد 47، الصادرة بتاريخ: 16 /08/ 2009، ص ص 6، 7.

27- المرجع نفسه، ص 8.

ثالثا: قانون رقم 03-15 المتعلق بعصرنة العدالة. إذ أكد المشرع في الفصل الخامس في المادة 17 على أنه: « يعاقب بالحبس من سنة (1) إلى خمس (5) سنوات و بغرامة تتراوح بين 100000 دج إلى 500000 دج كل شخص يستعمل بطريقة غير قانونية العناصر الشخصية المتصلة بإنشاء توقيع الكتروني يتعلق بتوقيع شخص آخر»(28)، نظرا لسماح المشرع إمكانية إرسال الوثائق والإجراءات القضائية الكترونيا إذا استلزم الأمر ذلك، و سعي الجزائر نحو الإدارة الالكترونية لتلبية حاجات المواطنين في أسرع وقت، هذا ما دفع المشرع الجزائري لعدم إهمال عقوبة الاستعمال غير القانوني للتوقيع الالكتروني.

بناءً على ما تقدم يمكن القول أن المشرع الجزائري اهتم بمكافحة الجرائم المعلوماتية بتقديم الضمانات اللازمة لذلك في بعض النصوص القانونية، لكن الجزم بأن هذه الأخيرة كفيلة لدرء مخاطر الجرائم الالكترونية أمر من الصعب تحقيقه؛ إذ لا بد أن تتفاعل الآليات القانونية مع الآليات المؤسساتية والإجرائية لتعزيز حق الإنسان في الأمن المعلوماتي.

المطلب الثاني: الآليات المؤسساتية.

لتعزيز آليات حق الإنسان في الأمن المعلوماتي لا بد من تأسيس مجموعة من الهيئات الداعمة لتطبيق النصوص التشريعية المتعلقة بحماية الأمن المعلوماتي لا يقتصر نشاطها على المستوى الوطني بل يتعداه إلى المستوى الدولي في إطار التعاون الدولي و التنسيق في هذا المجال، ويمكن إبراز أهم هذه المؤسسات في:

الفرع الأول: الآليات المؤسساتية الدولية لتعزيز الأمن المعلوماتي.

فقد سارعت المنظمات الدولية لاسيما تلك المتعلقة بمكافحة الجريمة المنظمة و الإرهاب إلى استحداث هيئات فرعية تختص بمكافحة والوقاية من الجرائم الالكترونية، و في هذا الصدد توجد منظمة الشرطة الجنائية الدولية (الانتربول) INTERPOL))؛على

28-الجمهورية الجزائرية الديمقراطية الشعبية، " قانون رقم 03-15 يتعلق بعصرنة العدالة"، **الجريدة الرسمية**. العدد 06، الصادرة بتاريخ: 10 /02/ 2015، ص6.

اعتبار أن معظم الجرائم الالكترونية ذات طابع عبروطني، لذلك يعتبر الانتربول شريك المنظمات الدولية و الإقليمية و الدول لتنفيذ القوانين و التعاون في التحقيقات لهذا النوع من الجرائم، بحيث له دور في الدعم العملياتي والتحقيق، الطب الشرعي الرقمي، الابتكار و القيام بالأبحاث الاستباقية للجرائم الالكترونية، استخدام أحدث تقنيات التدريب و تطوير أدوات جديدة للشرطة، لذلك استحدث الانتربول المجمع العالمي للابتكار (IGCI) في سنغافورة عام 2014 للكشف و الوقاية من الجرائم الالكترونية من خلال دوره الأساسي في القيام بالأبحاث ودعم الخبرة العالمية بخصوص تنفيذ القوانين المتعلقة بمكافحة الجريمة المعلوماتية (29).

نظرا لكون الدولة بمفردها لا تستطيع القضاء على الجرائم الالكترونية فالحاجة ملحة كي يكون هناك تعاون دولي يتفق مع طبيعة هذا النوع من الجرائم التي تتميز مكافحتها بسرعة إجراءات التحقيق والتنسيق الجيد بين أجهزة الشرطة للعديد من الدول.

الفرع الثاني: الآليات المؤسساتية الإقليمية لتعزيز الأمن المعلوماتي.

من أهمها؛ وكالة تطبيق القانون الأوروبية المتخصصة في مكافحة الجريمة و الإرهاب في دول الاتحاد الأوروبي (أوروبول) (Europol): حيث أعلنت في 01/09/2014 عن إنشاء قوة خاصة لمحاربة الجرائم المعلوماتية في دول الاتحاد الأوروبي و خارجه لتنضم دول أخرى إليها مثل: كندا، استراليا و الولايات المتحدة الأمريكية، وظيفتها التنسيق مع التحقيقات الدولية لمواجهة التهديدات الالكترونية التي تستهدف خاصة القطاع المالي ومكافحة المواقع الالكترونية التي تبيع الممنوعات(30) ، و إن كانت صعوبة الإثبات بالأدلة الالكترونية ـ لتلك الجرائم ـ أهم تحدٍ يواجه مهام هذه الأجهزة .

29-International Criminal Police Organization, «Cybercrime », from :

https://www.interpol.int/ar/Crime-areas/Cybercrime/Cybercrime on: 09-02-2017.

30- فاروق خلف، مرجع سابق، ص 6.

الفرع الثالث: الآليات المؤسساتية الوطنية لتعزيز الأمن المعلوماتي.

إن تنامي تهديد الأمن القومي ـ لجميع الدول من طرف الحروب الالكترونية و ما خلفته من الجرائم الالكترونية ـ جعل من الدول ـ على غرار الجزائر ـ حريصة على أمنها المعلوماتي بإنشاء هيئات هدفها الرئيسي ضمان أمنها المعلوماتي والوقاية من مختلف الجرائم الالكترونية.

فعلى سبيل المثال تعتبر الولايات المتحدة الأمريكية من الدول الحريصة على أمنها المعلوماتي؛ فقد أنشأت على إثر ذلك المعهد القومي للتكنولوجيا و المعايير الذي يتولى مهمة تشفير المعلومات و البيانات المتداولة الكترونيا و حفظها من الاندثار، إضافةً إلى إنشاء الوكالة الفيدرالية المسؤولة عن أمن المعلومات و التي لها ارتباطات مع وكالة المخابرات الأمريكية، وكالة الأمن القومي و وزارة الدفاع الوطني بغرض الحصول على المعلومات المتعلقة بالأمن القومي(31)، هذا الحرص يعكس التخوف الأمريكي نتيجة توجهات سياساتها الداخلية و الخارجية على مختلف الأصعدة السياسية، العسكرية، الاقتصادية، الاجتماعية والثقافية، و ما يُدعم أكثر نشاط هذه الهيئات هو التطور الذي تعرفه تقنية المعلومات في الولايات المتحدة.

و الجزائر كغيرها من الدول سعت هي الأخرى لدعم الأمن المعلوماتي مؤسساتيا، حيث يوجد:

أولا: على المستوى المركزي؛ يوجد المعهد الوطني للأدلة الجنائية و علم الإجرام الذي تم إنشاؤه بمرسوم رئاسي رقم 183-04 المؤرخ في 26 جوان 2004 و المُكلف بالقيام بالخبرات التطبيقية المدعومة بالتكنولوجيا المناسبة بطلب من القضاة لتحديد هويات مرتكبي الجنايات و الجنح خدمةً للعدالة، والمشاركة بأبحاث للتقليل من جميع أشكال الإجرام(32)، كما يوجد مركز الوقاية من جرائم الإعلام الآلي و الجرائم المعلوماتية

31-وليد غسان سعيد جلعود، **مرجع سابق**، ص ص 64، 65 .

32- الدرك الوطني، « المعهد الوطني للأدلة الجنائية و علم الإجرام». متحصل عليه من :

undefined#ar=L?php.index/cgn_site/dz.mdn.www//:http

بتاريخ: 09-02-2017.

للدرك الوطني، والمصلحة المركزية لمكافحة الجريمة المعلوماتية التابعة لمديرية الأمن الوطني.

دون إغفال أهمية و دور الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال و مكافحتها التي تم تحديد تشكيلتها و تنظيمها و سيرها من خلال المرسوم الرئاسي 261-15 المؤرخ في 08 أكتوبر 2015؛ حيث تمارس مهامها تحت رقابة السلطة القضائية وفق المادة 4 من المرسوم، و تُناط لها عدة مهام من بينها: مساعدة السلطات القضائية ومصالح الشرطة القضائية في مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، ضمان المراقبة الوقائية للاتصالات الالكترونية تحت سلطة القاضي المختص قصد كشف الأعمال التي تمس أمن الدولة، وتكوين محققين في التحريات التقنية و التعاون مع المؤسسات الوطنية المعنية بالجرائم المتصلة بتكنولوجيات الإعلام و الاتصال(33)، إن خصوصية هذه الهيئة تستمدها من ممارسة مهامها تحت إشراف السلطة القضائية ما يضفي عليها فعالية أكثر خصوصا أثناء مراقبة الاتصالات الالكترونية لأن هذه الأخيرة تكون تحت سلطة القاضي.

ثانيا: على المستوى المحلي؛ للوقاية من الجريمة الالكترونية ومكافحتها على المستوى المحلي استحدثت المديرية العامة للأمن الوطني مخابر للشرطة العلمية سنة 2007 بالجزائر العاصمة، وهران وقسنطينة، مهمتها تتبع الأدلة الرقمية باستخدام الأجهزة الالكترونية لإجراء التحقيقات ومساعدة العدالة في تقرير الأحكام القضائية(34*)، بالإضافة إلى مخابر الشرطة العلمية تم إنشاء خلايا مكافحة الجرائم الالكترونية سنة 2010 كان عددها في البداية 23 خلية ليتم تعميمها على مستوى جميع مصالح أمن ولايات الوطن؛ حيث تضم عناصر يتم انتقاؤها على أساس الشهادة الجامعية والمؤهلات التي يحملونها والخبرة في الشرطة القضائية، وتدعيمهم بدورات

33-الجمهورية الجزائرية الديمقراطية الشعبية، " المرسوم الرئاسي رقم 261-15 يحدد تشكيلة و تنظيم و كيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال "، **الجريدة الرسمية**. العدد 53، الصادرة بتاريخ: 08 /10/ 2015، ص ص 16، 17.

34-(*) انظر الملحق رقم (01).

تكوينية متخصصة بعد ذلك تنصيبهم لتولي مهمة التصدي للجريمة الالكترونية(35)، لكن يجب أن تكون الدورات التكوينية بصفة دورية لتحيين الجانب العلمي و العملي لعناصر خلايا مكافحة الجرائم الالكترونية لتميز الوسائل المستخدمة في هذه الجرائم بالسرعة في التطور.

على ضوء ما تقدم يتبن جلياً أن المنظومة المؤسساتية الأمنية المعلوماتية في الجزائر تتميز بكونها منظومة متشابكة؛ فالجريمة و الحروب الالكترونية تُحتّم وجود ذلك الترابط و التنسيق لضمان فعالية محاربتها و الوقاية منها.

المطلب الثالث: الآليات الإجرائية.

يكشف الواقع حجم المخاطر والخسائر التي تترتب عن الحروب و الجرائم الالكترونية، الأمر الذي يفرض على الأفراد، المنظمات المختلفة، و الدول الإسراع في تبني مجموعة من الإجراءات للمواجهة والوقاية من آثارها، وعلى العموم تنقسم هذه الإجراءات إلى:

الفرع الأول: الآليات التقنية. هي عديدة، من أهمها (36) :

* توفير مصدر احتياطي للطاقة الكهربائية: لضمان استمرار عمل مراكز الحاسب الآلي ينبغي التزويد المستمر لمراكز الحاسب الآلي بمصدر آخر للطاقة الكهربائية؛ ويستخدم لذلك مزود الكهرباء المستمر (UPS) .

* استخدام وسائل التحقق من شخصية المستخدم:عن طريق تعريف المستخدم بنفسه للنظام المعلوماتي من خلال إدخال الرقم السري الخاص به إلى النظام، أو إدخال بطاقة ممغنطة مخصص لها مكان في الحاسب الآلي، و جهاز الكشف عن بصمة الأصبع وكف اليد، ملامح الوجه و العينين.

35- عبد الرحمان حملاوي، « دور المديرية العامة للأمن الوطني في مكافحة الجرائم الالكترونية» ورقة بحث مقدمة في **الملتقى الوطني** « الجريمة المعلوماتية بين الوقاية و المكافحة» ، جامعة محمد خيضر، بسكرة، 2015. ص ص 8، 9.

36-منصور بن سعيد القحطاني، **مرجع سابق**، ص ص 48- 59.

* توظيف جدران الحماية: وهي عبارة عن أجهزة وبرامج تعمل على تصفية البيانات بين الشبكة الداخلية والشبكة الخارجية لحماية الأنظمة المعلوماتية الداخلية المتعلقة بالمنظمات والأفراد عبر التحقق من صلاحية المستخدم، التشفير، وبرامج الحماية من الفيروسات.

* برامج مكافحة الفيروسات: تعتبر من أهم وسائل حماية أجهزة الحاسب الآلي بالبحث عن الفيروسات المعروفة وغير المعروفة التي تهدد أجهزة الحاسب الآلي والبرامج لاكتشافها قبل حدوث الأضرار، ومن ثم القضاء عليها.

نظرا لتزايد الاعتماد على البريد الالكتروني تزيد معه فرصة اختراق أمنه و سرية معلوماته، وعن البرامج التي توفر الحماية للبريد الالكتروني برنامج يوجد برنامج ((PGP Pretty Good Privacy))؛ حيث يعمل على توفير خدمات الخصوصية، التحقق، تخزين الملفات باستخدام أفضل خوارزميات التشفير، و من جانب آخر يمتاز بعدم سيطرة أية شركة حكومية عليه و إمكانية استخدامه من قبل الشركات والأفراد معا لضمان الاتصال مع الآخر بطريقة آمنة(37).

يتضح أن هناك العديد من الآليات التقنية لمواجهة مهددات المعلومات، إلا أنه رغم ذلك تواجه تحدي الجهل أو اللامبالاة، أو قلة وعي الأفراد أو المنظمات بضرورة توفيرها لحماية أنظمتها المعلوماتية.

الفرع الثاني: الآليات التكوينية.

تحرص المديرية العامة للأمن الوطني في الجزائر على التكوين الجيد للعنصر البشري؛ فقد سطرت برنامجاً تكوينياً للإطارات و الرتباء و الأعوان، فمنذ سنة 2003 م إلى غاية 2010 م كانت هناك 6 دورات تكوينية بالداخل بمشاركة خبراء أجانب ليتم تكوين 128 ضابطا، و 4 دورات بخارج الجزائر استفاد منها 9 ضباط، و دورة واحدة وطنية بمشاركة كفاءات وطنية لتكوين 39 ضابطا(38)، في حين برز تشجيع للأفراد

37-خضر مصباح إسماعيل الطيطي، **مرجع سابق** ، ص ص 379، 380.

38- عبد الرحمان حملاوي، **مرجع سابق**، ص 7.

الذين يمتلكون مهارات و مواهب في العمل الالكتروني فعلى سبيل المثال؛ تعقد أجهزة الاستخبارات البريطانية مسابقة سنوية لتعيين أبرز كاسري الأرقام السرية، هذا وتحرص الولايات المتحدة الأمريكية على تعيين أبرز القراصنة في مسابقة (ديفكون defcon) (39)، لأنه من متطلبات الحماية الالكترونية وجود عنصر بشري كفء له القدرة العالية على المناورة ، يتميز بالذكاء و سرعة البديهة.

الفرع الثالث: الآليات البحثية/التوعوية.

حيث تُبرمج المديرية العامة للأمن الوطني من أجل توعية المواطن بمخاطر الجرائم الالكترونية أيام دراسة لمختلف الأطوار الدراسية، كما شاركت في العديد من الملتقيات أو الندوات و المؤتمرات ذات الصلة بالأمن المعلوماتي، والجريمة الالكترونية(40)، فالتوعية جزء من الحماية، لذلك لا بد من توعية المواطن لماهية هذه الجرائم، الحروب الالكترونية و أسلحتها و كل ما يترتب عليها من مخاطر، و عليه يتوجب أن تتضافر جهود العديد من المؤسسات للقيام بالدور التوعوي و البحثي منها: الأسرة، المدرسة، الجامعة، منظمات المجتمع المدني و وسائل الإعلام.

بناءً على ما سبق تجدر الإشارة إلى أن فعالية الآلية الإجرائية محدودة ما لم يتم تدعيم الموارد البشرية و المادية بالإرادة الحقة من طرف القيادة على المستوى المركزي أو المحلي، الوطني أو الدولي لتأمين الدعم المستمر و الكافي لتعزيز الأمن المعلوماتي.

39-عبد الكريم صالح المحسن، " الاختراقات الالكترونية ...قوة سياسية تتناسب مع الحروب الجديدة". متحصل عليه من: http://all4syria.info/Archive/237537
بتاريخ: 10-02-2017.

40- عبد الرحمان حملاوي، **مرجع سابق**، ص 9.

الملحق رقم (01): القضايا المعالجة من طرف المديرية العامة للأمن الوطني المتعلقة بالجوانب الالكترونية

السنوات	عدد القضايا المعالجة	عدد الأشخاص الموقوفين
2007	31	31
2008	06	10
2009	29	21
2014	245	/
2015	409	347

المصدر: عبد الرحمان حملاوي، مرجع سابق، ص 10.

الخاتمة:

على ضوء ما تقدم تم التوصل إلى مجموعة من النتائج نوجزها في النقاط التالية:

- يهدف تعزيز حق الإنسان في الأمن المعلوماتي إلى تحقيق ثالوث الأمن المعلوماتي بتوفير؛ سرية، سلامة و وفرة المعلومة، لحماية هذه الأخيرة من مصادر التهديد المعلوماتي الداخلية والخارجية التي ينجر عنها الجرائم الالكترونية باستهدافها العديد من القطاعات والشرائح من خلال اختراق تقنية المعلومات بهدف التطفل، تعديل أو حذف المعلومات.
- فرَضَ تنامي خطر التهديدات الالكترونية سعي المنظمات الدولية و الإقليمية تقديم مجموعة من الضمانات القانونية للمواجهة والوقاية من الجرائم المتعلقة بتقنية المعلومات، إلا أن نقص إلزامية التطبيق خاصة على مستوى المنظمات الدولية يُشكل أهم عائق لهذه الضمانات، في حين أن المشرع الجزائري و رغم

تأخره عن سن القوانين المتعلقة بمكافحة الجرائم الالكترونية، إلا أنه حاول استدراك ذلك في القانون رقم 15-04 المتعلق بالعقوبات، و بعض القوانين الأخرى من أهمها القانون رقم 04-09 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال؛ التي تجلى فيها تأكيد المشرع ضمان الأمن المعلوماتي من خلال تشديده على العقوبات المتعلقة بهذا النوع من الجرائم.

- تحرص المنظمات الدولية على ضرورة تأكيد التعاون الدولي لدرء مخاطر التهديدات المعلوماتية لما تتطلبه هذه الأخيرة من توحيد الجهود و التنسيق الجيد بين الدول، لذلك تم استحداث وحدات فرعية على مستوى بعض المنظمات الدولية من بينها المجمع العالمي للابتكار التابع لمنظمة الشرطة الجنائية الدولية (الانتربول)، و القوة الخاصة لمحاربة الجرائم المعلوماتية في دول الاتحاد الأوروبي و خارجه.
- إن تنامي خطر التهديد المعلوماتي جعل من الجزائر تعمل على استحداث هيئات على المستوى المركزي و المحلي لمحاربة الجرائم الالكترونية تتميز بكونها متشابكة، يرتبط دورها أساساً بالقيام بالأبحاث و مساعدة السلطات القضائية لتحقيق العدالة.
- توجد العديد من الآليات الإجرائية لتعزيز الحق في الأمن المعلوماتي منها الآليات التقنية، التكوينية، البحثية و التوعوية ، لكن فعالية هذه الآليات مرهونة بعاملين رئيسيين هما: وجود مورد بشري كفء يمتلك مجموعة من المؤهلات الذهنية التي تؤهله لضمان حماية المعلومة، و وجود تقنية المعلومات المتطورة المدعمة بالبرامج الضامنة لحماية الأنظمة المعلوماتية من أي اختراق.

بالتالي على اعتبار أن عصر اليوم عصر المعلومات بامتياز، لا بد من تعزيز الحق في الأمن المعلوماتي من خلال:

- قيام مؤسسات التنشئة الاجتماعية كالأسرة، المدرسة، الجامعة، منظمات المجتمع المدني، الأحزاب السياسية، و وسائل الإعلام بمختلف أنواعها بالدور التوعوي حول المخاطر المترتبة عن تهديد ثالوث الحق في الأمن المعلوماتي المتمثلة في سرية، سلامة و وفرة المعلومة، في ظل الحرص على توعية المواطنين بصفة دورية و بطريقة سهلة حول الآليات المختلفة للمواجهة و الوقاية من الجرائم الالكترونية.
- توفير الدعم المادي اللازم لبرامج الحماية المعلوماتية لتعزيز حماية الأنظمة المعلوماتية من أي هجوم الكتروني يُقوض حق الإنسان في أمنه معلوماتياً.
- وجوب تكوين الموارد البشرية للمنظمات بمختلف أنواعها دورياً لتعزيز حق الإنسان في الأمن المعلوماتي.

قائمة المراجع:

أولا: باللغة العربية.

أ - الوثائق الرسمية:

1 - الجمهورية الجزائرية الديمقراطية الشعبية، « قانون رقم 04 - 15 المتضمن قانون العقوبات»، الجريدة الرسمية. العدد 71، الصادرة بتاريخ: 10 /11/ 2004.

2 - الجمهورية الجزائرية الديمقراطية الشعبية، « قانون رقم 09 - 04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها»، الجريدة الرسمية. العدد 47، الصادرة بتاريخ: 16 /08/ 2009.

3 - الجمهورية الجزائرية الديمقراطية الشعبية، « قانون رقم 15 - 03 يتعلق بعصرنة العدالة»، الجريدة الرسمية. العدد 06، الصادرة بتاريخ: 10 /02/ 2015.

4 -الجمهورية الجزائرية الديمقراطية الشعبية، « المرسوم الرئاسي رقم 15 - 261 يحدد تشكيلة و تنظيم و كيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة

بتكنولوجيات الإعلام و الاتصال «، الجريدة الرسمية. العدد 53، الصادرة بتاريخ: 08 /10/ 2015.

ب - الكتب:

5 - أحمد ، هلالى عبد الله . اتفاقية بودابست لمكافحة جرائم المعلوماتية. القاهرة: دار النهضة العربية، 2007.

6 - الجنبيهى، منير محمد. الجنبيهى، ممدوح محمد. أمن المعلومات الالكترونية. الإسكندرية: دار الفكر الجامعي، 2006.

7 - صادق، دلال . الفتال، حميد ناصر. أمن المعلومات. عمان: دار اليازوري العلمية للنشر و التوزيع، 2008.

8 - الطيطي، خضر مصباح إسماعيل. أساسيات أمن المعلومات و الحاسوب. عمان: دار حامد للنشر و التوزيع، 2010.

9 -مظلوم، محمد جمال. الأمن غير التقليدي. الرياض: مركز الدراسات و البحوث، 2012.

ج- الدراسة غير المنشورة:

10 - القحطاني، منصور بن سعيد. « مهددات الأمن المعلوماتي و سبل مواجهتها «، رسالة ماجيستير ، (جامعة نايف العربية للعلوم الأمنية، كلية الدراسات العليا، قسم العلوم الإدارية، الرياض، 2008).

د- الملتقيات العلمية:

11 - البداينة، ذياب موسى. « الجرائم الالكترونية: المفهوم و الأسباب» ورقة بحث مقدمة في ملتقى « الجرائم المستحدثة في ظل المتغيرات و التحولات الإقليمية و الدولية»، كلية العلوم الاستراتجية، عمان، 4-2 سبتمبر 2014.

12 - حملاوي، عبد الرحمان. « دور المديرية العامة للأمن الوطني في مكافحة الجرائم الالكترونية» ورقة بحث مقدمة في الملتقى الوطني « الجريمة المعلوماتية بين الوقاية و المكافحة» ، جامعة محمد خيضر، بسكرة، 2015.

13 - خلف، فاروق. « الآليات القانونية لمكافحة الجريمة المعلوماتية « ورقة بحث مقدمة في الملتقى الوطني « الجريمة المعلوماتية بين الوقاية و المكافحة» ، جامعة محمد خيضر، بسكرة، 2015.

ثانيا: باللغة الأجنبية.

A - Articles :

14 -Caplan, Nathalie. « Cyber War: the Challenge to National Security», Global Security Studies review, Vol. 4, no.1 Winter 2013.

B - REPORTS:

15 - Report Theohary,Catherine A. Rollins, John W. « Cyberwarfare and Cyberterrorism: In Brief »,[N.P], Congressional Research Service , March 27, 2015.

16 - Report Williams, Robert H. « introduction to information security consepts», [N.P], August 2007.

c - ELECTRONIC RESOURSE:

17 - International Criminal Police Organization, «Cybercrime », from :

https://www.interpol.int/ar/Crime-areas/Cybercrime/Cybercrime on: 09-02-2017.