أمن المعلومات في الجزائر: الإجراءات والتحديات.

Information security in Algeria: procedures and challenges.

سوهيلة بضياف

جامعة 20 أوت 1955 سكيكدة، الجزائر، souhilabediaf@yahoo.fr

آمنة حمراني

جامعة باتنة1، الجزائر، hamraniamina1905@gmail.com

تاريخ الارسال: 2019/09/21 **تاريخ القبول:** 2019/10/17 **تاريخ النشر:** 2020/01/01

ملخص:

تعرضت الجزائر مؤخرا إلى العديد من الهجمات الالكترونية التي استهدفت قطاعات حساسة، نتيجة لاعتمادها المتزايد على تكنولوجيا الاتصال في مختلف الإدارات والمؤسسات، مما يجعل أنظمة معلوماتها عرضة لمختلف التهديدات السيبيرية والجرائم الالكترونية وهو ما دفعها إلى الاهتمام أكثر بمجال أمن المعلومات. ونهدف من خلال دراستنا إلى تحليل مختلف الإجراءات التي اتخذتها الجزائر في هذا المجال لمعرفة واقع أمن المعلومات في الجزائر. وتوصلت الدراسة إلى أنه رغم المجهودات المبذولة في وضع نظام لأمن المعلومات ، إلا أن ذلك غير كاف مقارنة بالتحديات التي تفرضها بيئة تكنولوجيا الاتصال

الكلمات المفتاحية: *الأمن؛ المعلومة؛ أمن المعلومة؛ الجريمة الالكترونية.*

Abstract:

In Algeria, recently sensitive sectors have been a target to many cyber-attacks because of their increasing use of communication technologies in several administrations and companies. The information systems have been threatened and became vulnerable to various cyber threats, which prompted the authorities to pay more attention to the field of information security. This study aims to analyse the different procedures that Algeria has taken against cybercrimes and to find out the position of information security. The study concluded that despite of all the efforts to establish a strong information security system by the Algerian authorities, its not sufficient yet comparing to the challenges that are forced by technology

Keywords: *security; information; information security; cybercrime.*

* المؤلف المرسل: سوهيلة بضياف، souhilabediaf@yahoo.fr

مقدمة:

تعتبر المعلومات عصب الحياة في مختلف القطاعات لاسيما ونحن في عصر تكنولوجيا الاتصال ومجتمع المعلومات، فالمعلومة اليوم تعتبر سلعة استراتيجيه وخدمة ومصدرا للدخل الوطني وأساس المعرفة والاقتصاد والتجارة والسياسة ....الخ

إن البيئة المفتوحة التي تمنحها الانترنت لمستخدميها رغم ما لها من ايجابيات، إلا أنها جعلت المعلومة مهددة بأشكال مختلفة من التعدي والاختراق وهو ما وضع الأفراد والحكومات والمؤسسات والدول أمام نوع جديد من التحديات في مجال الأمن، لمواجهة التهديدات التي تستهدف الأشخاص والأمن الوطني بل تتعداه إلى الإقليمي والدولي، بظهور مجرمين ينشطون في الفضاء الالكتروني قادرين على الدخول إلى مواقع المؤسسات الرسمية والحكومات والتجسس عليها واختراقها أو إلحاق الضرر بها.

ونتيجة لانتشار الجرائم الالكترونية والتهديدات التي تنجم عن التزايد المستمر في استخدامات تكنولوجيا الاتصال في كل المجالات، لجأت العديد من الدول إلى الاهتمام بمجال أمن المعلومات الذي يكمن الهدف الأساسي منه في حماية الأنظمة المعلوماتية للأفراد والمؤسسات والحكومات من الهجمات والاختراقات، التي تقوم على الاستخدام غير المشروع لمواردها أو إحداث خلل في هياكلها ومحتوياتها، من خلال تهيئة بنيتها التحتية ضد أشكال الجرائم الالكترونية واستحداث قوانين لمعاقبة المجرمين والتوعية بمخاطر الجرائم الالكترونية.

وتعد الجزائر من بين الدول التي أولت في الآونة الأخيرة اهتماما بمجال الأمن المعلوماتي ومكافحة الجريمة الالكترونية، خاصة أنها تعرضت للعديد من الهجمات الالكترونية على مستوى قطاعات حساسة، بالإضافة إلى التحديات العالمية في مجال الأمن الوطني والإقليمي التي باتت تهدد الدول الضعيفة في تأمين معلوماتها وحمايتها وهو ما يدفعنا إلى طرح التساؤل الرئيسي التالي:

ما هو واقع الأمن المعلوماتي في الجزائر،وما مدى كفايته في مواجهة مختلف التهديدات والجرائم الالكترونية؟

وللإجابة على هذا التساؤل تتضمن خطتنا ما يلي:

- ✓ ماهية أمن لمعلومات
- ✓ أسس أمن المعلومات ومهدداته
- ✓ واقع أمن المعلومات في الجزائر

1. ماهية أمن المعلومات:

أ. مفهوم أمن المعلومات:

تعريف الأمن: إن مفهوم الأمن هو مفهوم واسع يتسع لعدة مجالات لها علاقة بالأنشطة الحياتية للإنسان فكل واحد يعرفه وفقا لاختصاصه وفي مفهومه الواسع هو "مجموع الجهود المبذولة والمشتركة من قبل الدولة وأفراد المجتمع من خلال مجموعة من النشاطات والفعاليات في شتى مجالات الحياة للحفاظ على حالة التوازن الاجتماعي في ذلك المجتمع" (المشاقبة 2012، ص. 52)

-**تعريف المعلومة**: هناك العديد من التعاريف للمعلومة؛ حيث عرفها كل باحث وفقا لاهتماماته فقد عرفت بشكل واسع وعام على أنها " الهيئة أو الحالة الخاصة للمادة أو الطاقة التي يمكن نقلها أو إبلاغها للغير" ، ولقد اهتمت مختلف التعاريف السابقة لتطور تكنولوجيا الاتصال بطريقة انتقال المعلومة ولم تهتم بمحتوى المعلومة التي تحملها الرسالة أو قيمتها المالية، أو مدى الاستفادة منها بقدر اهتمامهم بإمكانية نقلها أو تداولها بين مختلف الوسائل، فليس كل رسالة تنقل إلى الغير تمثل معلومة، تستوجب الحماية وإنما الحماية تشمل بعض المعلومات، التي لها ميزة أو قيمة معينة وليس كل المعلومات (ممدوح 2008، ص. 26).

وتعرف المعلومات أيضا بأنها مجموعة من الرموز و الحقائق أو المفاهيم أو التعليمات التي تصلح أن تكون محلا للتبادل أو الاتصال أو التفسير أو التأويل أو المعالجة، سواء بواسطة الأفراد أو الأنظمة الالكترونية، وهي تتميز بالمرونة بحيث يمكن تعبئتها و تجزئتها وجمعها و نقلها بوسائل وأشكال مختلفة. (ممدوح 2008، ص. 26)، ونلاحظ من خلال هذا التعريف أنه إهتم بالمعلومة في علاقتها بتكنولوجيا الاتصال؛ حيث أضاف مصطلح الأنظمة الالكترونية ومختلف العمليات التي قد تطرأ على المعلومة إلكترونيا.

ولقد أعطى المشرع الجزائري تعريفا للمعلومة وميزها عن مفهوم المعطيات من خلال القانون09- 04 وهو ما سنوضحه في المحور الثالث.

- **تعريف أمن المعلومات:** توجد هناك العديد من التوجهات في تعريف أمن المعلومات؛ حيث أن للمفهوم عدة توجهات ومتشعب من خلال تقاطع العديد من التخصصات في تعريفه، ذلك أن أمن المعلومة يشمل الجوانب التقنية والقانونية والتوجهات الأكاديمية.

فمن الناحية القانونية يعرف على "أنه مجموعة الإجراءات والقوانين، التي يتم فرضها بهدف تأمين حماية كل من المعلومات والوسائط والأجهزة المستخدمة في حفظ ومعالجة وتبادل المعلومات عبر الشبكة" (الطائي 2010، ص. 149)، فمن الناحية القانونية نجد الاهتمام بأمن المعلومات من الجانب التشريعي من خلال التركيز على الإجراءات القانونية والعقابية، لتأمين المعلومات من الاختراقات والإضرار بها، إلا أنها أهملت الجانب التقني الذي هو أساس أمن المعلومة وكيفية تهيئته لضمان حمايتها.

أما من الناحية التقنية فيعرف على أنه الإجراءات والتدابير الوقائية التي تستخدم سواء في المجال الفني أو الوقائي لصيانة المعلومات مثل الأجهزة، والبرمجيات والبيانات المتعلقة بالتطبيقات، وكذلك الأفراد العاملين في المجال، ويشير كذلك أمن المعلومات إلى الدخول إلى كل موارد المنشأة من قبل أطراف غير مخولة باستخدام النظام. (السالمي 2000، ص. 391)، ونلاحظ أن التعريف التقني يشير إلى الجانب المادي الذي يعتمد على التجهيزات والبرمجيات وكل ما يتعلق بها من مسببات، قد يكون السبب فيها مشكل في التقنية في حد ذاتها أو بسب إهمال أو خطأ بشري يؤثر على عمل التكنولوجيا ويلحق الضرر بالمعلومة ويجعلها عرضة للاختراق.

وتعرفه لجنة الأمن القومي الأمريكي أنه حماية المعلومات وعناصرها المهمة بما في ذلك الأنظمة والأجهزة التي تستخدم هذه المعلومات وتخزنها وترسلها.(Withman2005, p. 35)

ويعرف أيضا أنه المفاهيم والتقنيات والتدابير التقنية والإدارية التي تحمي المعلومات من الدخول إليها دون إذن وذلك إما عمدا أو خطأ عفوي يحدث سهوا أو حيازة هذه المعلومات أو إلحاق الضرر بها والتلاعب بها بالتعديل، أو التغيير، أو فقدها، أو سوء استخدامها (بن علي 2015، ص.35)

من خلال هذه التعاريف نستنتج بأن أمن المعلومات يشمل عدة جوانب هي:

- ✓ الأخطاء غير المتعمدة الناتجة عن تجهيز البيانات لإدخالها إلى الحاسب.

- ✓ الحوادث المتعلقة بتضييع المعلومات، أو تغييرها نتيجة لخلل أو عطب تقني في البرامج.
- ✓ الدخول غير المأذون للبيانات وسرقتها أو تغييرها جزئيا أو كليا وسوء استخدامها.
- ✓ الآثار الناجمة عن بعض الكوارث كالفيضانات والحرائق وحوادث الانفجار.

ب. أهمية أمن المعلومات:

هناك العديد من الأسباب التي تجعل لأمن المعلومات أهمية منها: (القحطاني 2015، ص. 65)

- ✓ انتشار تكنولوجيا الاتصال والحاجة إلى الارتباط الدائم بنظم الاتصالات وشبكة الانترنت، حيث توسع نطاق المعلومة ولم تعد محصورة في المجال المحلي.
- ✓ اعتماد مختلف المؤسسات والمنظمات على المعلومات في عملها، مما يجعلها عرضة للاختراقات والتجسس، أو حتى بعض المخاطر التقنية والطبيعية، التي قد تساهم في ضياعها أو إتلافها، مما يجعل وجود نظام أمن معلومات في أي مؤسسة ضرورة حتمية
- ✓ صعوبة تحديد الأخطار والتحكم بها ومتابعة المجرمين لذا فإن نظام أمن المعلومات قد يسهل عملية المراقبة، واتخاذ التدابير الاحترازية ضد الجريمة الالكترونية.
- ✓ التزايد المستمر في استخدام تطبيقات الانترنت وظهور المعاملات الالكترونية والتجارة الالكترونية مما يحتم التوجه نحو توفير بيئة الكترونية آمنة

2. أسس أمن المعلومات ومهدداتها:

أ. أسس أمن المعلومات:

لقد حدد الباحثون ثلاث عناصر أساسية ومهمة يجب توفرها، لضمان بيئة آمنة وتشكل هذه العناصر مثلثا أطلق عليه The CIA Triad وتعني التوافر، السلامة، السرية وهي جد ضرورية في كل أنظمة المعلومات لتحقيق الأمن المعلوماتي. (Stallings , Brown 2014, p. 145)

وتعني هذه العناصر مايلي: (الاتحاد الدولي للاتصالات 2006 .ص.ص 22-23)

-**التوافر:** وهو توفر المعلومة في كل وقت يحتاجها فيه المستخدم ولا تحجب عنه ولضمان التوافر يجب تحديد الأحجام المناسبة للنظم التحتية وأن تتوافر لها الأعداد الاحتياطية البديلة.

- **السلامة:** أي أن تكون المعلومة التي سنحميها معلومة صحيحة وغير مغلوطة، أي حمايتها من الوصول غير المشروع والتعديل والتغيير في محتواها، ويعد السبيل الوحيد لضمان سلامة البيانات هو حمايتها من السرقة وأساليب الاقتناص، عن طريق تحويل مسارها الأصلي والتي يمكن استخدامها لتعديل المعلومات المعترضة ويمكن توفير هذه الحماية بواسطة آليات مثل:

- ✓ المراقبة الصارمة على النفاذ
- ✓ تحفيز البيانات
- ✓ الحماية من الفيروسات والديدان وأحصنة طروادة

-**السرية:** وهي حماية المعلومات والحفاظ على سريتها وتدفقاتها وتضمن حماية الموارد من الإفشاء والإخفاء غير المرخص ولضمان سرية المعلومات يجب الاعتماد على التحفيز؛ حيث يساعد على حماية سرية المعلومات أثناء الإرسال أو التخزين، بتحويلها إلى شكل غير مفهوم لأي شخص لا يمتلك وسائل فك التحفيز

وهناك من الباحثين من أضاف عناصر أخرى يرى أنها مهمة مثل:

-**الهويـة أو الاسـتيقان**: إن الهـدف مـن الاسـتيقان هـو معرفـة هويـة أي مـورد وتحديـدها ومـن المفروض أن يحدد ذلك مسبقا وأي كيان معروف سواء برنامج أو شخص أو عتاد حاسوب، وهناك علامات تدل عليه مباشرة .

ب. مهددات أمن المعلومات:

تصنف المهددات التي تتعرض إليها المعلومات والأمن بصفة عامة إلى مايلي:

- **المهددات الطبيعية:** و هي الكوارث التي لا دخل للإنسان والأجهزة فيها، كالفيضانات والزلازل والحرائق والصواعق وموجات الغبار التي تمس بأنظمة المعلومات وقد تؤدي إلى انقطاع الخدمات الالكترونية نهائيا. (القحطاني 2015، ص. 72)

- **المهددات البشرية:** وهي التهديدات الناجمة عن العمال الذين يشتغلون في المؤسسات؛ حيث يتسببون في اختراق أمن المعلومة وقد تكون التهديدات البشرية داخلية من خلال اختراقها لخدمة مصالح معينة أو الإفشاء ببعض أسرار المعلومة ككلمات المرور مثلا وقد تكون الأخطاء البشرية عن قصد أو دون قصد، أما التهديدات الخارجية وهي تحدث من أفراد خارج المؤسسة وتشمل تهديدات البرمجيات، والأجهزة والمعلومات. (بن موسى2010، ص. 130)

- **المهددات التقنية والفنية :** تتعدد طرق وآليات انتهاك البنية التحتية لتكنولوجيا المعلومات، وهذه الأساليب تهدف إلى مهاجمة نظم وأمن المعلومات، لنيل أغراض معينة، و منهم من يلجأ إلى التخريب و التدمير ومنها مايلي:

- **الجرائم المعلوماتية وأشكالها**: تعتبر الجرائم المعلوماتية التي تستخدم التقنيات الالكترونية من الجرائم التي تتطلب إلماما خاصا بتقنيات وبرمجيات الحاسب الآلي ونظم المعلومات، و المقترف لهذا النوع من الجرائم يعد مخالفا لقواعد وأصول استخدام تلك النظم واستغلالها أو تزييفها أو تزويرها وذلك يكون منافيا لقواعد القانون.

- **الفيروسات:** تعتبر الفيروسات والبرامج الضارة من أهم أسباب ارتكاب الجرائم المعلوماتية أو الحاسوبية، وأكثرها انتشارا في الوقت الحاضر، و هي على عدة أنواع وفي تطور مستمر، تعد من أخطر مهددات الأمن المعلوماتي مثل فيروسات التشغيل: (boot sector virus)، فيروس الماكرو (macro virus)، - الفيروس المخفي، فيروسات العتاد، - الفيروسات المتحولة...الخ (شوابكة 2011، ص . 238)

- **البرمجيات الضارة:** و هي عبارة عن برامج تتسبب في أضرار تتراوح بين مجرد الإزعاج إلى غاية فقد البيانات، وصولا إلى سرقة الأموال وهذا الأسلوب يحتوي على عدة تقنيات منها: حصان طروادة (troyen Hors)، برامج الدودة Worm، القنبلة الموقوتة Bomb (القحطاني 2015، ص. 74)

3. واقع أمن المعلومات في الجزائر:

إن معرفة واقع أمن المعلومات في الجزائر يتطلب التركيز على مختلف الجوانب التي يشتملها أمن المعلومة، سواء جانب التشريعات أو البنى التحتية، أو اتفاقيات التعاون والدورات التدريبية، وهو ما نفصله في مجموعة من المحاور هي:

أ- أمن المعلومات في إطار التشريعات والقوانين الجزائرية:

تعتبر الجزائر من الدول التي تسعى إلى تكييف إطارها القانوني ومستحدثات تكنولوجيا الاتصال التي باتت تهدد أمن المعلومة؛ حيث سن المشرع الجزائري نصين قانونيين تعاقب على أساسهما الجريمة المعلوماتية وهما: قانون العقوبات والقانون المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، بالإضافة إلى قوانين وتعديلات أخرى تضمنت الاهتمام بأمن المعلومة.

- **قانون العقوبات:** المعدل بموجب القانون رقم 15/04 المؤرخ في 10 نوفمبر 2004 المتعلقة بالمساس بالشبكة المعلوماتية والذي تضم ثلاثة أصناف هي: (جنادي 2018، ص .17)
  - ✓ الجرائم المتعلقة بالمساس بالسرية ووحدة وأمن المعطيات في نظام ما
  - ✓ التزوير المعلوماتي والمساس بالمعطيات
  - ✓ الجرائم المتعلقة بالبحث والجمع والحيازة أو بث أو التجارة بالمعطيات

وقد استحدث المشرع الجزائري مجموعة من العقوبات لمرتكبي الجرائم الالكترونية من خلال مجموعة من المواد القانونية، فقد تضمنت المادة 394 مكرر مجموعة من العقوبات التي تتراوح بين الحبس من ثلاثة أشهر إلى سنة وبغرامة مالية من50.000 إلى 100.000دج كل من يدخل عن طريق الغش، في كل أو جزء من منظومة المعالجة الآلية للمعطيات أو يحاول ذلك، وتضاعف العقوبات في حالة حدوث حذف أو تغيير لمعطيات المنظومة، كما نصت المادة 394مكرر 1 على أن إدخال المعطيات في منظومة معلوماتية خلسة، وإزالة أو تعطيل معطيات في منظومة معلوماتية خلسة يؤدي إلى معاقبة مرتكبي هذه الجريمة، بالحبس من ستة أشهر إلى ثلاث سنوات وبغرامة مالية تصل إلى 50.000 1 كأقصى حد، أما المادة 394 مكرر2 فقد تضمنت عقوبات القيام عمدا وخلسة بتصميم أو بحث أو تجميع أو توفير أو نشر معطيات تمكن من ارتكاب جرائم المساس بأنظمة المعالجة الآلية للمعطيات، وتتراوح العقوبات فيها بين الحبس من شهرين إلى ثلاث سنوات وبغرامة مالية تصل إلى 5000.000دج، أما المادة 394 مكرر 3 فقد تناولت ارتكاب الجرائم سالفة الذكر إضرارا بالدفاع الوطني أو الهيئات أو المؤسسات الخاضعة للقانون العام. (الجريدة الرسمية 2004، ص. ص 11-12)

ورغم هذه العقوبات التي تضمنها قانون العقوبات إلا أنه يحتوي على بعض الفراغات القانونية، فمثلا ورغم أن المشرع الجزائري اهتم بالجرائم الماسة بأنظمة المعالجة الآلية، إلا أنه أغفل الجرائم الماسة بمنتجات أنظمة المعالجة الآلية، ولازالت جريمة التزوير جريمة تقليدية خاضعة للمواد من 214 إلى 229 عقوبات، دون أن يوسع مضمونها ليشمل كافة المحررات (بوربابة 2016/2015، ص.137)، ويعود هذا إلى التعامل مع الجريمة الالكترونية بنفس طريقة التعامل مع الجريمة التقليدية رغم أن الجريمة الالكترونية تفرض إدراج مواد أخرى تتضمن تفاصيل تخص حيثيات ارتكاب الجريمة الكترونيا، كما أن المجرم الالكتروني قد يستهدف منتجات أنظمة المعلومات في حد ذاتها، فلذلك يبقى هذا القانون ناقص ومن الضروري سن قانون خاص بالجريمة الالكترونية يشمل كل ما يتعلق بها .

- **القانون المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها:** (القانون09- 04 المؤرخ في 05 أوت2009 ويحتوي على 19 مادة موزعة على ستة فصول ومستمدا بنوده من الاتفاقيات الدولية خاصة منها اتفاقية بوداباست حول الجرائم المعلوماتية 2001.

تعرف الجرائم المتصلة بتكنولوجيا الإعلام والاتصال في هذا القانون في المادة (02) منه بأنها جرائم المساس بأنظمة المعالجة الآلية للمعطيات، المحددة بقانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية.

وقد جاء في المادة (3) تعريفات تقنية لبعض المفاهيم المتعلقة بتكنولوجيا الاتصال؛ حيث ميز بين المنظومة المعلوماتية والمعطيات المعلوماتية، فعرف **المنظومة المعلوماتية** على أنها أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة، يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين، أما **المعطيات المعلوماتية** فهي عملية عرض للوقائع أو المعلومات أو المفاهيم في شكل جاهز للمعالجة داخل أنظمة معلوماتية، بما في ذلك البرامج المناسبة التي تجعل منظومة معلوماتية تؤدي وظيفتها، كما أعطى تعريفا **لمقدمي الخدمات** على أنهم أي كيان عام أو خاص يقدم لمستعمليه خدماته وأي كيان آخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الاتصال المذكورة أو لمستعمليها، أما **المعطيات المتعلقة بحركة السير** وهي أي معطيات متعلقة بالاتصال عن طريق منظومة معلوماتية تنتجها هذه الأخيرة باعتبارها جزء في حلقة الاتصال والاتصالات الإلكترونية أو إرسال أو أي تراسل أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة الكترونية. (الجريدة الرسمية 2009، ص.5)

ونلاحظ من خلال هذه المفاهيم أن المشرع الجزائري اعتمد من خلال التعريفات السابقة للجرائم المعلوماتية على عدة معايير للدلالة على هذا النوع من الجرائم، وذلك باعتماده على معيار وسيلة الجريمة من جهة، ومعيار نظام الاتصالات الإلكترونية، ومن جهة أخرى على معيار موضوع الجريمة وهو المساس بأنظمة المعالجة الآلية للمعطيات، كما اعتمد على معيار آخر في تحديد نطاق الجريمة المعلوماتية باعتبارها جرائم الكترونية ترتكب في نظام معلوماتي أو نظام للاتصالات الالكترونية، كما أنه ميز بين مجموعة من المفاهيم المتعلقة بتكنولوجيا الاتصال لإزالة اللبس حولها، وتكييف كل مفهوم مع العقوبات التي تتناسب معه.

بالإضافة إلى ذلك وضع قواعد خاصة تجيز مراقبة الاتصالات الإلكترونية في المادة(04) في الحالات التالية: الوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب وجرائم أمن الدولة، معلومات حول اعتداء على منظومة معلوماتية تهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني لمقتضيات التحريات والتحقيقات القضائية في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة ولا يجوز القيام عمليات المراقبة في كل الحالات إلا بإذن مكتوب من السلطة القضائية المختصة، كما تناول القانون في الفصل الثالث القواعد الإجرائية لتفتيش المنظومات المعلوماتية، وفي الفصل الرابع التزامات مقدمي الخدمات، وفي الفصل الخامس أدرج إنشاء هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحته وتضمن الفصل السادس التعاون والمساعدات القضائية الدولية (الجريدة الرسمية 2009، ص.ص.6-8).

ولقد اهتم المشرع الجزائري في هذا الاطار باصدار قوانين ومراسيم أخرى لحماية أمن المعلومة منها:

- **قانون الإجراءات الجزائية**: المعدل بموجب القانون 04-14 المؤرخ في 10-2004 والذي جاء فيه بأن الجرائم الالكترونية، تتابع مثلها مثل الجريمة التقليدية، وتقوم على التفتيش، المعاينة، الاستجواب والضبط، التسرب، الشهادة، الخبرة ، كما استحدث القانون المحاكم الجزائية ذات الاختصاص الموسع التي أجازا لها تمديد اختصاصها للنظر في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات(المواد 37 ،40، 329)،

ومكن ضباط الشرطة القضائية من التدخل لمعاينة الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات إلى كامل الإقليم الوطني وفقا للمادة 16 التي تمدد الاختصاص الإقليمي للشرطة القضائية، و قد جاء بقواعد استثنائية في التفتيش كما ورد في المادة 47 كجواز التفتيش في المحلات السكنية وغير السكنية بناءا على إذن مسبق من وكيل الجمهورية المختص والتفتيش داخل المساكن دون حضور المشتبه فيه ودون شهود هذه القواعد الاستثنائية،كما مكن قانون الإجراءات الجزائية إمكانية استعمال أساليب خاصة في جرائم المساس بأنظمة المعالجة الآلية للمعطيات. (بن زروق، قصعة 2017، ص. 252)

-القانون 03-05 المتعلق بحقوق المؤلف والحقوق المجاورة: صدر في 19 يوليو 2003 نص على تجريم انتهاك حقوق المؤلف والحقوق المجاورة عن طريق التقليد بأي وسيلة كانت، بما فها منظومة المعالجة المعلوماتية (المادة 152)، وتعتبر حقوق المؤلف محمية في ضوء الدستور الجزائري فقد نص في المادة 54 منه على الحماية القانونية للحريات والملكيات؛ حيث جاء فيها أن حرية الإبداع الفكري والفني والعلمي للمواطن مضمونة في إطار القانون وحقوق التأليف محمية قانونيا، وقد سمح قانون **03-05** في المادة (03) منه بإدخال برامج الحاسب الآلي في إطار المصنفات المحمية بموجب حق المؤلف، ونصت المادة (41) منه على عدم الاستنساخ الخطي لأي مصنف سواء كان كتاب كامل أو موسيقي أو قاعدة بيانات رقمية وعدم استنساخ برامج الحاسب إلا في الحالات المنصوص عليها في المادة 52 من هذا الأمر. (بوفاس، طلحي 29\30 أفريل 2014)

-المرسوم التنفيذي رقم 98-256:المرسوم التنفيذي رقم (98-256 المؤرخ في 25 أوت 1998المعدل والمتمم للجزء التنظيمي من الأمر 75- 89 المؤرخ في 30 -12-1975: وتضمن تعريف خدمات الانترنت، شروط ممارسة مقدمي الخدمة ومستضيفي المواقع لنشاطهم، واجباتهم اتجاه السلطات العمومية، مسؤوليتهم عن محتوى الصفحات التي يطورونها أو يستضيفونها، واجباتهم تجاه زبائنهم (بن زروق، قصعة 2017، ص. 253)، بالإضافة إلى ذلك فقد جاء قانون البريد والاتصالات السلكية واللاسلكية لتنظيم التحويلات والمعاملات الالكترونية فقد نص في المادة (87) منه على سهولة إجراء التحويلات المالية الكترونيا واستعمال الحوالات العادية والالكترونية والمادة(127) التي تنص على عقوبة كل من يفتح أو يخرب بريد، بالإضافة إلى قانون التأمينات والذي نص على تنظيم الجريمة الالكترونية من خلال مؤسسات وهيئات الضمان الاجتماعي في عدة نصوص تتعلق بالبطاقة الالكترونية. (بوغرارة 2018، ص . 110).

وقد عكفت الجزائر منذ جانفي 2015 على تكييف إطارها التشريعي والقانوني والتنظيمي من خلال سن مجموعة من القوانين الهامة، منها الخاصة بالتوقيع والمصادقة الالكترونية، بالإضافة إلى تكييف قوانينها مع التشريعات الوطنية المتعلقة بمحاربة الفساد وتبييض الأموال وتمويل الإرهاب ومكافحة المخدرات (جنادي 2018، ص.45)، ولكن تبقى هذه الترسانة من القوانين غير كافية لانعدام قانون خاص بالجريمة الالكترونية يحيط بكل ما يتعلق بها لتحقيق الأمن المعلوماتي، خاصة أن التطور التكنولوجي يفرض علينا تعاملات الكترونية في بيئة مهددة بمختلف الجرائم، وهو ما يستوجب إصدار قانون خاص بالجريمة الالكترونية على غرار الدول الأولى في مصاف أمن المعلومات كاليابان مثلا.

وفي هذا الإطار فقد صنفت الجزائر في تصنيف موقع كومباريتش COMPARITECH سنة 2018 أنها من أول الدول نقصا في التشريعات، وسن القوانين المتعلقة بأمن المعلومات.(Moody 2019)

ب- الهيئات الوطنية لتقصي الجريمة وحماية أمن المعلومة

- **الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها:**

وهي سلطة إدارية تشكلت في الأول بمرسوم رئاسي رقم 15-261 تعمل تحت لجنة يشرف عليها ويديرها وزير العدل وتضم أعضاء من الحكومة ومسؤولي مصالح الأمن وقضاة وأعوان من الشرطة القضائية تابعين للاستعلامات العسكرية والدرك والأمن وتعمل على الكشف عن الجرائم الإرهابية الالكترونية وجرائم المساس بأمن الدولة (بارة 2017، ص. ص. 237-238)، وفي سنة 2019 صدر مرسوم رئاسي أخر رقم 19-172 مؤرخ في 3شوال عام 1440 الموافق ل 6 يونيو 2019؛ حيث ألحق الهيئة بوزارة الدفاع الوطني بدلا من وزارة العدل وهو ما نصت عليه المادة (02) وجاء فيها أن الهيئة هي مؤسسة عمومية ذات طابع إداري تتمتع بالشخصية المعنوية والاستقلالية المالية، توضع تحت سلطة وزارة الدفاع الوطني(الجريدة الرسمية 2019، ص.5)، والملاحظ أن وضع هذه الهيئة تحت سلطة وزارة الدفاع الوطني جاء عقب الحراك الذي عرفته الجزائر والذي عرف استخداما كبيرا لموقع شبكة الفايسبوك حيث حدثت العديد من الانتحالات للشخصيات، وتسريب للمعلومات ...الخ

وقد هدف المرسوم إلى توضيح تشكيلة الهيئة وتنظيمها وكيفية سيرها؛ حيث وحسب المادتين 04 و05 فإن الهيئة تنظم في مجلس توجيه ومديرية عامة، ويتشكل مجلس التوجيه من ممثلي كل من وزارة الدفاع، وزارة الداخلية وزارة العدل، وزارة المواصلات السلكية واللاسلكية، وتتولى المديرية العامة أمانة المجلس وتكلف الهيئة من خلال مجلس التوجيه بمهام تحددها المادة (06) من المرسوم وفقا لما يلي:

- ✓ تنفيذ الإستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاتصال والإعلام ومكافحتها.
- ✓ العمل على كل ما يتعلق بتطوير التعاون مع المؤسسات الوطنية المعنية بهذا النوع من الجرائم.
- ✓ التقييم الدوري لمهددات تكنولوجيا الإعلام والاتصال المتعلقة بالجرائم الالكترونية لتحديد مخططات المراقبة الواجب العمل بها وتحقيق الأهداف بدقة.
- ✓ اقتراح كل نشاط يتصل بالبحث في مجال الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال.
- ✓ الموافقة على برنامج الهيئة ودراسة التقرير السنوي لنشاطاتها. (الجريدة الرسمية 2019، ص.ص.5-6)

ج/ هياكل تقصي الجريمة

- **مركز الوقاية من جرائم الإعلام الآلي التابعة للدرك الوطني:**

أنشأ مركز الوقاية من جرائم الإعلام الآلي بعد صدور القانون المتعلق بمكافحة الإجرام المعلوماتي في سنة 2004 ومن أهم مهامه ما يلي:(جنادي2013، ص. 15)

- ✓ مساعدة وحدات الدرك الوطني الممارسة لمهام الشرطة القضائية في البحث على مرتكبي المخالفات المتعلقة بالمساس بأنظمة المعالجة الآلية للمعطيات.
- ✓ امتلاك أحدث الأنظمة والأجهزة والبرمجيات المتطورة في مجال الوقاية من الإجرام المعلوماتي ومكافحته
- ✓ التعاون والتنسيق مع المصالح الأمنية الوطنية وعدد من متعاملي الخدمات الهاتفية من أجل الاستجابة لطلبات مختلف وحدات الدرك الوطني المتعلقة بالتعرف على العناوين الالكترونية وأرقام المرسلين .
- ✓ التعاون مع مختلف السلطات القانونية والتشريعية في مجال طلبات التعاون مع الهيئات الدولية.

- ✓ يعتمد المركز على أنواع من اليقظة وهي اليقظة الأمنية، الاجتماعية، القانونية، لتكنولوجية،الاقتصادية.

جدول(1) يبين عدد القضايا المعالجة من طرف المركز من 2009 إلى السداسي الأول من سنة 2013

السنوات	2009	2010	2011	2012	2013
تحقيقات	18	18	22	28	24
معلومات إدارية ومصلحية	50	110	224	287	50
نشاط وقائي تحسيسي	14	18	23	34	30

- **المعهد الوطني للأدلة الجنائية وعلم الإجرام:** يتكون من 11 دائرة متخصصة في عدة مجالات متباينة، تضمن جميعها الخبرة والتكوين و التعليم وتقديم جميع المساعدات التقنية (بارة 2017، ص. 271)

- **المصلحة المركزية لمكافحة الجريمة المعلوماتية التابعة لمديرية الأمن الوطني:** ولقد أنشأت هذه المصلحة في سنة 2011 استجابة لمطلب الأمن السيبراني ومكافحة التحديات الأمنية الناجمة عن الجرائم الالكترونية وأضيفت رسميا للهيكل التنظيمي سنة 2015. (بوغرارة 2018، ص.111)

جدول (2) يبين عدد القضايا المعالجة من طرف مديرية الأمن الوطني

السنوات	القضايا	المتورطين
2007	**31**	**31**
2008	**6**	**10**
2009	**29**	**21**
2014	**245**	/
2015	**409**	**347**

(بوغرارة 2018، ص. 111)

ونلاحظ من خلال الجدول أن هناك ارتفاعا ملحوظا في عدد القضايا المتعلقة بالجرائم الالكترونية وتعمل هذه المصلحة على التوعية من خلال برمجة دروس توعوية في مختلف الأطوار المدرسية وكذا المشاركة في الملتقيات والندوات الوطنية للتوعية من خطورة الجرائم الالكتروني وقد عالجت مصالح الشرطة القضائية بالمديرية العامة للأمن الوطني 2130 قضية تتعلق بجرائم الكترونية، تم حل 1570 منها خلال سنة 2017 ، كما سجلت ذات المصالح 2704 ضحية للجرائم المتصلة بالإعلام الآلي(www.Radioalgerie.dz 2018)

- ا لهيئات الجزائية القضائية المتخصصة:

و هي هيئات تختص بالجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات وتتميز باختصاصها الإقليمي الموسع؛ حيث تنظر في القضايا المتعلقة بتكنولوجيا الإعلام والاتصال، التي ترتكب في الخارج وحتى القضايا التي يكون مرتكبوها من الخارج وتمس مؤسسات الدولة والدفاع الوطني وفقا للمادة 15 من قانون رقم 90/04 (عاقلي2017، ص. 133)

د- المعاهدات واتفاقيات التعاون:

تعتبر المعاهدات الوطنية بين مختلف المؤسسات واتفاقيات التعاون مع الدول في الحماية من جرائم الانترنت من أهم الأعمدة الأساسية في مكافحة الجرائم والاستفادة من الخبرات خاصة في الدول النامية، والجزائر من الدول التي تحاول أن تجد لها مكانا في هذا المجال خاصة إقليميا ومع الدول المجاورة، فقد كانت عضوا مشاركا في مساعي الاتحاد الإفريقي للتعاون في مكافحة الجريمة السيبرانية من خلال اتفاقية حول الأمن السيبراني وحماية البيانات الشخصية في جوان 2014 والتي تهدف إلى تزويد الدول المشاركة، بإطار قانوني يسمح بتنظيم نشاط مستخدمي الانترنت، إلا أن هذه الاتفاقية لم ترق إلى التطلعات واصطدمت باحتجاجات حول التدخل في السيادة الوطنية، (جنادي 2018، ص .42.)، واحتضنت الجزائر في نفس الإطار قمة افريقية في أفريل2018 بعنوان الأمن السيبراني في عصر التحول الرقمي الإفريقي؛ جمعت أصحاب القرار والشركات الناشطة في مجال تكنولوجيا الإعلام والاتصال، إلى جانب المصممين والمبتكرين، لدراسة طبيعة التحديات الواجب مواجهتها في إطار الجريمة الالكترونية (جنادي2018، ص.ص. 42-43)

كما حاولت عقد اتفاقيات في التبادل في مجال المعلومات من خلال تأكيد عضويتها الفعالة في المنظمة الدولية للشرطة الجنائية الانتربول والتي من شأنها أن تتيح مجالات للتبادل والتعاون الدولي في مجال المعلومات وتسهيل تسليم المجرمين ومباشرة الانابات القضائية الدولية ونشر أوامر القبض للمبحوث عنهم دوليا. (عاقلي2017، ص. 133)

وحسب التقرير العالمي للأمن المعلوماتي لسنة 2017 فقد كشف على مستوى متوسط في مجال التعاون، حيث تحصلت الجزائر على معدل درجة ايجابية في التعاون الدولي حول الأمن المعلوماتي، أما التعاون بين المؤسسات والتعاون الخاص والعام، فقد تحصلت على درجة متدنية وفي الاتفاقيات الثنائية تحصلت على معدل متوسط. (Sanou 2017, p. 31)

هـ البنية التحتية لأمن المعلومات في المؤسسات العامة والخاصة الجزائرية:

تعاني الجزائر من ضعف للأمن المعلوماتي في مؤسساتها الرسمية والعمومية، حيث تستضيف شركات أجنبية خاصة الفرنسية منها 70 % من مواقع تلك المؤسسات، مما يشكل خطرا كبيرا على تسريب المعلومات السرية، نظرا لتعامل الموظفين بايميلات لمواقع استضافة في دول أجنبية، لا تملك قاعدة بياناتها في الجزائر، إلى جانب خطورة استضافة مواقع مؤسسات إستراتيجية في الخارج، فأغلب المواقع الرسمية لمؤسسات عمومية تستضيفها مؤسسة فرنسية، فعندما يحدث عطب فيها تتوقف كل هذه المواقع عن العمل وهو ما حدث في سنة .2016 (خ 2018)

وقد كشفت دراسة بعنوان باروماتر 2018 حول الأمن السيبراني في المؤسسات الجزائرية مدى ضعف احترام مقاييس تأمين نظام المعلومات في المؤسسات الجزائرية نتيجة عدم اهتمامها بذلك؛ حيث أكدت الدراسة أن ثلث المؤسسات التي شملتها الدراسة تعرضت لاختراق أنظمة المعلومات خلال 12 شهرا عن طريق الفيروسات، في حين أن 15 % فقدت بياناتها جراء أخطاء بشرية، كما أن 47 % من المختصين في الإعلام الآلي عبروا على أن الأنظمة المعلوماتية في الجزائر غير مؤمنة ومحمية، كما عبروا أن 47 % من المؤسسات الجزائرية لا تخزن بياناتها في الوقت الحالي في شبكات معلوماتية جزائرية، و أكدت 27 % منها أنها تتعامل مع مؤسسات أجنبية في التزود بخدمة إيواء المواقع (جنادي، 2018، صفحة 44)، ولقد تعرض موقع بيانات وزارة البريد إلى

قرصنة سنة 2016 ، كما تكررت نفس العملية على مستوى اتصالات الجزائر، كما تعرضت وكالة الأنباء الجزائرية إلى قرصنة في نهاية مارس 2017 (خ. نسيمة 2018).

كما أن معظم المؤسسات سواء عامة أو خاصة تفتقر إلى فريق للاستجابة إلى طوارىء الكمبيوتر أو طوارىء الحوادث والأخطار، وحتى الفريق الجزائري الوحيد للاستجابة لطوارئ الكومبيوتر والمعروف ب CERT DZ الذي دوره مساعدة المجموعات الوطنية في تحسين أمن الاتصالات والأنظمة المعلوماتية، بهدف التقليل من أخطار الحوادث الأمنية، يبقى عمله في الواقع محتشما وقلما يعلن عن بعض الفيروسات أو الهجمات التي تهدد أمن الكومبيوتر

وحسب موقع كومباريتش COMPARITECH فإن الجزائر تتقدم أسوء الدول في الترتيب ،من حيث التعرض لفيروسات الموبايل والكومبيوتر قبل كل من تنزانيا واندونيسيا وأوزبكستان؛ حيث سجلت معدل نقاط مرتفع من حيث عدد الهجمات (Moody, 2019).

و- المؤسسات الجزائرية ومقاييس العالمية لأمن المعلومات:

قامت العديد من الشركات العالمية بتبني معيار موحد لتخطيط وتحديد السياسات الأمنية للمعلومات والشبكات، فقد استطاعت المنضمة الدولية للمقاييس ايزو ISO بتوفير المعيار العالمي لنظام أمن المعلومات ايزو 27001 والذي يعتبر من أحدث إصدارات المنظمة بعد تحديث النسخة الأولى التي كانت تسمى ISO 17799 .(ابراهيم، حمد، و بازرعة 17 فيفري 2012).

وتعد شهادة الايزو لأمن المعلومات، من الشهادات الأكثر ضمانا لحماية المعلومات في المؤسسات في العالم؛ حيث تكمن أهمية الشهادة في وضع معالم أمن المعلومات في المؤسسات، وبناء نظام متكامل يعتمد على عمليات مستمرة يؤدي تطبيقها إلى الحماية المرجوة والتطور المستمر بناء على مقاييس معتمدة للحفاظ على أمن المعلومات، وتعتبر مؤشرا بالتزام المؤسسات على جميع مستوياتها بحماية المعلومات وزيادة الثقة في المؤسسة، ويعتبر اهتمام الجزائر بهذه الشهادة ضعيفا رغم أنها مهمة جدا في استدامة المؤسسات، وحمايتها من الهجمات الالكترونية والتعدي عليها، فحتى سنة 2014 لا توجد أي مؤسسة جزائرية حاصلة على ايزو 27001، ماعدا بعض الفروع الجزائرية لمؤسسات أجنبية تعتمد هذا النظام مثل البنك العربي (بوفاس و طلحي، 29\30 أفريل 2014).

ووفقا للتقرير الدولي لأمن المعلومات الذي ضم دراسة على أمن المعلومات في 194 دولة في العالم حددت فيها مجموعة من المرتكزات لقياس أمن المعلومات منها التشريعات، التقنيات، التنظيمات، التجهيزات، والتعاون صنفت الجزائر من بين 77 دولة في خانة الدول الناضجة أو المتوسطة من حيث أمن المعلومات؛ حيث تحصلت على معدل عالمي يصنفها في المرتبة 67 عالميا وفي المرتبة التاسعة عربيا، ووفقا للتقرير فقد تحصلت على درجة متدنية من حيث الهياكل، وبرامج التربية والصناعات الوطنية والميكانيزمات لمواجهة الحوادث والطوارئ المتعلقة بأمن المعلومات (Sanou 2017, p. 54)

خاتمة:

إن الاهتمام بأمن المعلومات في الجزائر يبقى محتشما مقارنة بمستوى التهديدات، من جهة وتطور تكنولوجيا الاتصال وتزايد استخدامها من جهة أخرى؛ حيث من الضروري النظر إلى أمن المعلومات

كإستراتيجية شاملة يجب التخطيط لها في إطار منظومة الأمن القومي والتطور الاقتصادي؛ إذ يجب أن تخطط الجزائر لبرنامج شامل يضم مختلف القطاعات والهيئات سواء كانت عمومية أو خاصة وذلك من خلال ما يلي:

- ✓ التركيز على أمن المعلومات في مختلف القطاعات ليس فقط في مجال الدفاع الوطني، بل من الضروري الاهتمام بإرساء قواعد أمن المعلومات في كل المؤسسات العامة والخاصة.
- ✓ سن قانون قائم بذاته حول الجريمة الالكترونية مع التشديد على تنفيذه على أرض الواقع ولا يبقى حبرا على ورق.
- ✓ عقد اتفاقيات تعاون وشراكة دولية وإقليمية ووطنية وكذا بين المؤسسات لتبادل الخبرات
- ✓ عقد دورات تدريبية متعلقة بأمن المعلومات وتكوين مهندسين متخصصين في المجال يسهرون على خلايا أمن المعلومة في كل المؤسسات وخاصة الحساسة منها.
- ✓ تطوير الصناعات في مجال التكنولوجيات، وأمن المعلومة.
- ✓ وضع المؤسسات لاستراتيجيات أمن المعلومة وتوفير الهياكل لذلك.
- ✓ إرساء ميكانيزمات لمواجهة الحوادث والطوارئ في مجال المعلومات مثل حوادث الكومبيوتر من خلال تشكيل مراكز وفرق للاستجابة للطوارئ المتعلقة بأمن المعلومات على مستوى حكومي وطني وقطاعي وتكون ذات عمل جاد وتنفيذي.
- ✓ التوعية بمخاطر الجرائم الالكترونية من خلال الحملات الإعلامية وإدراج مواد توعوية في مجال أمن المعلومة في المناهج الدراسية.

قائمة المراجع:

1. ابراهيم،ح.م ، حمد، م.ح.إ، بازرعة، إ.ب. (17 فيفري 2012). دراسة تحليلية لأمن الشبكات والمعلومات. الملتقى السنوي الدولي للدراسات العليا والبحوث العلمية .الخرطوم.
2. الاتحاد الدولي للاتصالات .(2006) .دليل الأمن السيبراني للبلدان النامية .جنيف
3. بارة، س. (2017). الأمن السيبراني في الجزائر: السياسات والمؤسسات. المجلة الجزائرية للأمن الانساني ، المجلد 02 (02).
4. بوغرارة، ي. (2018). الأمن السبراني: الاستراتيجية الجزائرية للأمن والدفاع في الفضاء السيبيري. المركز الدديمقراطي العربي. مجلة الدراسات الافريقية وحوض النيل. المجلد(1). العدد (3)
5. بورابابة، ص. (2016/2015). قواعد الأمن المعلوماتي- دراسة مقارنة-. رسالة دكتوراه في العلوم القانونية. قسم الحقوق. جامعة سيدي بلعباس
6. بن علي، ع، ط.(2015). رؤية استراتيجية لتحقيق الأمن المعلوماتي في هيئة التحقيق والادعاء العام في المملكة العربية السعودية. السعودية: جامعة نايف العربية للعلوم الأمنية المملكة العربية السعودية
7. بن زروق .ج، قصعة.خ. (2017). تفعيل آليات الحماية القانونية للحد من انتشار الجريمة الالكترونية في العالم والجزائر. مجلة تاريخ العلوم (العدد 06)
8. بوفاس، أ، طلحي.ف .(2012). نظم الادارة حماية المعلومات في المؤسسة الجزائرية ISO 2700. ورقة مقدمة في المؤتمر الدولي الثاني للذكاء الاقتصادي حول اليقة الاستراتيجية ونظم المعلومات في المؤسسة الاقتصادية .عنابة : جامعة باجي مختار.
9. جنادي،إ. (جوان 2013). روبورتاج حول مركز الوقاية من جرائم الاعلام الآلي والجرائم المعلوماتية. ا الجزائر. مجلة الجيش. العدد (599).
10. جنادي، إ. (أكتوبر 2018). الأمن السيبراني- التحدي القادم للاتحاد الافريقي. الجزائر. مجلة الجيش. العدد(663)

11. الجريدة الرسمية. (6شوال عام 1440 الموافق ل 9 يونيو 2019). مرسوم رئاسي يحدد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها وتنظيمها وكيفيات سيرها. الجمهورية الجزائرية الديمقراطية الشعبية. العدد (37)
12. الجريدة الرسمية. (16 08, 2009). قانون 09-04 المؤرخ في 2009/08/05 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها. الجمهورية الجزائرية الديمقراطية الشعبية.العدد (47) .
13. الجريدة الرسمية. (2004/11/10). قانون رقم 04- 15 يعدل ويتمم الأمر رقم 66-156 المتضمن قانون العقوبات. الجمهورية الجزائرية الديمقراطية الشعبية، (العدد 47).
14. ممدوح، إ.خ .(2008) .أمن الجريمة الالكترونية .القاهرة :الدار الجامعية.
15. المشاقبة،ع. ب. (2012). الإعلام الأمني. عمان: دار أسامة للنشر والتوزيع.
16. السالمي، ع. (2000). تكنولوجيا المعلومات. عمان: دار المنهج.
17. شوابكة، م. أ .(2011). جرائم الحاسوب والانترنت-الجريمة المعلوماتية- (الإصدار 4). عمان: دار الثقافة.
18. الطائي ,م .ع .(2010) .التجارة الالكترونية المستقبل الواعد للأجيال القادمة .عمان :دار الثقافة للنشر والتوزيع.
19. عاقلي،ف. (2017). الجريمة الالكترونية في القانون الجزائري والقانون المقارن. المؤتمر الدولي الرابع الجرائم الالكترونية. لبنان.
20. عبد الله بن العزيز الموسى. مقدمة في الحاسب والانترنت.
21. القحطاني،ب. ذ. (2015). أمن المعلومات. الرياض: مكتبة الملك فهد الوطنية.
22. نسيمة، خ. (10 04/ 2018). الجرائم الالكترونية تهدد أمن الجزائريين. تاريخ الاسترداد 11 05, 2019، من أخبار اليوم:
http://Akhbarelyoum.dz/ar/index.php
23. Moody, R. (2019, 02 06). Which countries the worst and best cybersecurity. Retrieved 05 24, 2019, from
http://www.comparitech.com
24. Sanou, B. (July 2017). Global Cybersecurity Index CGI. Geneva: ITU.
25. Stallings, W. Brown, L. (2014). Computer Security Principles and Practice. London: Pearson.
26. Withman, M. a. (2005). Principles of Information Security. Thomson cours Techniologiy.
http://www.Radio algerie.com 17/04/2018