الإطار القانوني والتشريعي للرقمنة والذكاء الاصطناعي

The Frame of legislative and judicial side to digitalization and Artificial Intelligence

د / عائشة عبد الحميد

أستاذة محاضرة قسم – ب–

كلية الحقوق – جامعة الشاذلي بن جديد الطارف – الجزائر.

malekcaroma23@gmail.com

المستخلص:

نتاجا لما فرضه الواقع المعاصر من انتشار هائل لنظم تكنولوجيا المعلومات التي تعتمد على البدائل الرقمية، مستغنية بذلك عن الكتابة على الورق. وتحت الضغط الكبير لتغلغل تقنية المعلومات في مختلف مناحي الحياة، بدأت على الصعيد القانوني تصاغ العديد من التساؤلات، ولا جدال على الإطلاق في أن أهم هذه الإختراعات في عصرنا الحديث جهاز الحاسوب أو الكمبيوتر، فمن إختراع هذه الآلة وتمازجها مع شبكات الاتصال، نتساءل عن كيفية حماية الحياة الخاصة في مواجهته، وكيفية حماية برامجه مدنيا وجنائيا.

الكلمات المفتاحية: المعلومات – النظام الرقمي – الجانب التشريعي والقضائي – القانون الجزائري.

Abstract :

As a result of the enormous proliferation of contemporary reality imposed by information technology systems that rely on digital alternatives, dispensing with writing on paper.

Under the great pressure of the penetration of information technology in various aspects of life, I began to formulate many questions at the legal level, and there is absolutely no argument that the most important of these inventions in our modern era is a computer or computer, so it is the invention of this machine and its mixing with communication networks, we ask how to protect Private life in the face of it, and how to protect its programs, both civilly and criminally.

Key words: information - digital system - legislative and judicial side - Algerian law.

مقدمة:

إن الاستخدام الواسع والمتزايد للتكنولوجيات الرقمية يسير بالموازاة مع الاعتماد المتزايد على هذه التكنولوجيات.

حيث شهد القرن الحادي والعشرون ثورة حقيقية في عالم تكنولوجيات المعلومات والاتصالات وانتشارا واسعا للإنترنت وتطبيقاتها في شتى المجالات الاقتصادية والاجتماعية والثقافية (التجارة، الخدمات الحكومية، التعليم، المعرفة، الترفيه، السياحة، الرعاية الصحية) وغيرها، وهذا ما يطلق عليه حاليا " الخدمات الإلكترونية"(**مجلة الجيش الجزائري، جانفي ٢٠١٦ على الموقع: www.mdn.dz**).

حيث أنه يمكن للتكنولوجيا أن تساعد في جعل عالما أكثر إنصافا وأكثر سلما وأكثر عدلا، ويمكن للإنجازات الرقمية أن تدعم كل هدف من أهداف التنمية المستدامة، من خلال إلمام الجميع بالقراءة والكتابة، ولكن التكنولوجيا يمكن أن تهدد أيضا الخصوصية وأن تؤدي إلى تقلص الأمن وتفاقم عدم المساواة (**www.um.org**).

وتعرف الرقمنة على أنها عملية نقل المادة من وعاء سمعي بصري أو ورقي، إلى آخر رقمي من خلال تقنيات تحويل المواد. (**مجلة الجيش الجزائرية، العدد ٦٥٧، أفريل ٢٠١٨ على الموقع:www.mdn.dz**).

وعليه يمكن إيجاد ارتباط وثيق بين الرقمنة التعليمية والتنمية المستدامة والقانون ؟.

ولكن كيف يمكن حماية معلوماتنا التعليمية القومية في ظل عدم إيجاد قانون ؟ أو على الأقل يوجد نظام تشريعي ولكنه قاصر وغير مكتمل؟.

لذا فإن هذه الدراسة يتم من خلالها تسليط الضوء على التجربة الجزائرية من خلال:

أولا– التعريف بالمصطلحات الدقيقة في مجال التعليم الرقمي والذكاء الاصطناعي.

ثانيا– الإطار التشريعي للاختراق الرقمي في الجزائر (المنظومة التشريعية).

ثالثا– سياسة جهاز الدفاع الوطني في تحقيق الأمن المعلوماتي .

وفيما يلي عرض لكل منهم.

أولا- التعريف بالمصطلحات الدقيقة في مجال التعليم الرقمي والذكاء الاصطناعي.

١)- ظهور الذكاء الاصطناعي:

ظهر الذكاء الاصطناعي خلال مؤتمر دولي جرى بأمريكا سنة ١٩٥٦ نشطه مختصون في مجالات علوم النفس، الرياضيات، الاقتصاديات والأعصاب، وبلغ ذروته في سنة ٢٠١٠ بفضل تسارع الإلكترونيات من خلال البيانات الرقمية.

التأطير القانوني والأخلاقي للذكاء الاصطناعي:

فيجب أن يستفيد الإنسان أو المجتمع من منافع الذكاء الاصطناعي وقد لا يكون منافسا لـــه أو ضحية لأحداث لا يعالجها القانون (**جريدة الشعب، ٢٧ نوفمبر ٢٠١٨**).

الذكاء الاصطناعي هو فرع من فروع العلم، يهتم بالحالات التي تستطيع حل ذلك النوع مـــن المسائل التي يلجأ الإنسان من حلها إلى ذكائه.

وهو مصطلح إزداد استخدامه مؤخرا في ظل النهضة التقنية التي يشاهدها العالم فـــي مجـــال تطوير الآلات رغم أن " الذكاء الاصطناعي " في القرن الواحد والعشرون أصبحت أبحـــاث الـــذكاء الاصطناعي على درجة عالية من التخصص، مما أسهم في انقسامه إلى مجالات فرعية مستقلة.

معظم هذه المجالات اتفقت في أن الآلة الذكية يجب أن يكـــون لهـــا القـــدرة علـــى الـــتحكم، الاستنتاج، ورد الفعل، على ظروف لم تبرمج عليها.

وفي كثير من الحالات يرتبط مصطلح " الذكاء الاصطناعي " بالآلات ككل، ولكـــن برنـــامج الحاسوب التي يتم تثبيتها على هذه الأجهزة، والتي تتسم بسلوك وخاصيات تقنيـــة تجعلهـــا تحـــاكي القدرات الذهنية البشرية، وأنماط عملها وهذا الأمر منطقي حيث أن الآلة أو الجهاز نفسه يشابه جـــسم الإنسان في الوقت الذي يقوم به العقل البشري بكافة الوظائف المتعلقة بالتفكير، إتخاذ القـــرار وحـــل المسائل.

(سليمان يعقوب الفرا، الذكاء الاصطناعي، على الموقع:

(http//www.03.ibm.com/innovation/us/waston/building.waston/index.html

الذكاء الاصطناعي : هو عبارة عن ٣ عمليات:

- **التعليم:** وتعني إكتساب المعلومات والقواعد التي تستخدم هذه المعلومات.
- **التحليل:** هو استخدام القواعد السابقة للوصول إلى استنتاجات تقريبية أو ثابتة .
- **التصحيح التلقائي أو الذاتي:(آل سعود، على الموقع :dr.alsaud.s@gmail.com).**

٢)- مصطلح التعليم الرقمي:

يقصد بالتعليم الرقمي (التعليم الإلكتروني) : شكل من أشكال التعليم عن بعد، ويمكن تعريفه على أنه:" طريقة للتعليم باستخدام آليات الاتصال الحديثة من حاسب وشبكاته ووسائطه المتعددة مـــن صوت وصورة، ورسومات وآليات بحث، ومكتبات إلكترونية، وكذلك بوابات الإنترنت ...

أو هو استخدام التقنية بجميع أنواعها، في إيصال المعلومة للمتعلم بأقصر وقت واقل جهد وأكبر فائدة ...، لأن المعرفة ليست فقط عملية نقل للمعلومات من المعلم إلى الطالب، بل هي أيضا عملية استقبال الطالب للمعلومة من الناحية الذهنية والنفسية. **(دياب، بروسيه، ٢٠١٩، ص ١٥٣)**.

فالتعليم الإلكتروني: هو مصطلح مرن، يستخدم لوصف وسيلة للتدريس من خلال التكنولوجيا، من خلال تسهيل عملية الاتصال بين الطلاب والمدرسين إلتكترونيا من خلال شبكة أو شبكات إلكترونية بحيث تصبح المدرسة أو الكلية مؤسسة شبكية، كما يعتبر أنه أسلوب حديث من اساليب التعليم توظف فيه آليات الاتصال الحديثة (**الزين**،http://jilrc.com).

التعليم الإلكتروني شكل من أشكال التعليم عن بعد، أو كما سمي ايضا بالتعليم اللاحضوري، حيث يعتمد على استخدام آليات الاتصال الحديثة كالحواسيب والشبكات والأنماط المتعددة (الصوت، الصورة، النص، الحركة)، عبر وسائط وهي (الحاسب، الإنترنت).

وتجدر الإشارة إلى أن التعليم الإلكتروني لا يلغي دور المعلم ولكنه يغير منه ويسانده، ويتيح مساعدته للمتعلم في أي وقت.

بالنسبة للتجربة الجزائرية في مجال التعليم الرقمي (في المدارس والجامعات) على حد سواء، لا زالت في بداياتها وتراوح مكانها ويرجع ذلك لغياب الوعي بفعالية هذا النوع من التعليم ومدى مساهمته في رفع المستوى التعليمي والتأهيلي للفرد. (**عزاف، د.س.ن، ص ٥٩-٨١**).

ويقوم التعليم الإلكتروني على استخدام الوسائل الإلكترونية المختلفة في عملية التعليم، وتتمثل هذه الوسائل الإلكترونية في: الكمبيوتر، الإنترنت، التلفزيون، الإذاعة، الفيديو، ومؤثرات الفيديو ...، الكتاب الإلكتروني. (**دياب، بروسيس، ٢٠١٩، ص ١٥٣**).

٣)- مصطلح السيادة الرقمية:

يعبر مصطلح السيادة الرقمية عن تطبيق مبادئ السيادة في مجال تكنولوجيا الإعلام والاتصال.

وتعتبر الجزائر ذو تعداد سكاني يقدر بأكثر من ٤٢ مليون نسمة، يحصي أكثر من ٢٢ مليون حساب على " فيسبوك "، ويتابع حوالي ٥٢،٣٤% الأخبار على الإنترنت، بالإضافة إلى الآلاف من المشتركين في الشبكة عبر الهاتف النقال.

وضمن ما يقارب عقدين من الزمن العالم في حالة سبات، حيث يقوم الكبار والصغار على حد سواء بالإبحار عبر العالم الإفتراضي، الذي يلغي الحدود الجغرافية، حيث اصبح من الصعب أن نتخيل عالم بدون هذه الوسيلة.

وفي ظل التطورات التكنولوجية الحاصلة أصبحنا أمام منحى خطير حول إدراك عواقب ذلك. (**مجلة الجيش، العدد ٦٨٠، مارس ٢٠٢٠ على الموقع الرسمي لوزارة الدفاع الجزائرية** www.mdn.dz).

حيث تحول الهاتف النقال منذ ظهوره أول مرة إلى ثورة تكنولوجية غير مسبوقة ومستمرة دون توقف، بحيث تعدى استخدامه من إجراء المكالمات الهواتفية إلى استخدامه كجهاز كمبيوتر وتلفزيون ومكتب ومكتبة ومفكرة شخصية وغيرها من التطبيقات والخدمات خاصة في ظل تقنية لجيل الثالث والجيل الرابع (**مجلة الجيش، عدد ٦٠٤، نوفمبر ٢٠١٣**).

ونظرا لدخول العقل الإلكتروني في كل مجالات الحياة العامة والخاصة، واليوم هناك من يرى أن المدرسة الرقمية أو الذكية تجربة ناجحة من العملية التعليمية تنتج أفراد يمتلكون القدرة في التعامل الإيجابي مع مختلف المواقف (**بوحميدة، ٢٠١٧، ص ٨٣**).

ويعود السبب أيضا إلى طبيعة الحاسوب وارتباطه الوثيق بحياة الإنسان اليومية ... وإلى الفوائد التي تعود على مستخدميه في كافة مجالات الحياة بصفة عامة، والتعليم بصفة خاصة (**ربيعي، ٢٠١٧، ص ٢١**).

وبفضل انتشار المجتمع المعلوماتي والبيانات الضخمة أمكن استثمار البيانات والعمليات " الرقمنة " في تغذية أنظمة الذكاء الاصطناعي.

حيث تستخدم الرقمنة التقنيات الرقمية لتغيير نماذج الأعمال والعمليات وتوفير فرص جديدة لتوليد الثروة وللتنمية المستدامة. كما يمكن النظر إلى الرقمنة بأنها أيضا تحويل العمليات إلى نسخ رقمية وإلغاء الحواجز بين البشر وتقنية المعلومات والاتصالات باستخدام تقنيات الذكاء الاصطناعي لتحقيق مردود اقتصادي واجتماعي بفاعلية وإنتاجية أعلى.

وتعتبر أخلاقيات العلوم وتكنولوجيا المعلومات والاتصالات وخاصة الذكاء الاصطناعي قضية حاسمة في السياسة التشريعية، فالذكاء الاصطناعي مثله مثل أي تكنولوجيا، فهي أيضا محل الكثير من الشكوك والمخاوف والمعارضة، ومثله مثل أي تكنولوجيا قد يكون سلبيا، فاستعمال الذكاء الاصطناعي في مختلف مجالات الحياة (النقل، الطاقة، التعليم، الصحة، الأمن، الدفاع، البحث العلمي، والقانون ... إلخ)، وما فرضته قواعد البيانات الأمنية وتصميم الفيروسات، وتدمير أنظمة التصويت الإلكتروني ...إلخ) ما هو إلا أمثلة يشهدها الواقع عن الاستعمال السلبي. (www.diae.events).

ثانيا- الإطار التشريعي للإختراق الرقمي في الجزائر (المنظومة التشريعية):

إن التجربة الجزائرية على غرار العديد من الدول، وخاصة في المجال الرقمي لا تزال في بداياتها، حيث يكتسي موضوع الرقمنة أهمية كبيرة، فهو ليس مجرد انتقال من نظام تقليدي روتيني

بطيء إلى نظام عصري حديث قائم على التكنولوجيا المتطورة، أو توفر أجهزة ومعدات حديثة، وبرامج مختلفة، ولكن ماذا عن سلبيات تلك وكيف تصدى المشرع الجزائري للاختراق المعلوماتي **(حلواجي، ٢٠١٧، ص ٩)**.

وطالما كنا أمام بدائل رقمية في كل مجالات الحياة تقريبا فإننا بذلك نجزم قطعا استغناءنا عن الكتابة على الورق (**الصالحين، ٢٠١٣، ص٥٣٥**)، وبالتالي فرضية رقمنة التعليم واستخدام الذكاء الاصطناعي ولكن ليس المشكل في الرقمنة وإنما في كيفية حماية المعطيات الرقمية ضد جنح التقليد واستعمال المقلد، والتزوير واستخدام المزور، وكذلك مختلف الجرائم المعلوماتية (**الأمر ٦٦-١٥٦ المتضمن قانون العقوبات الجزائري المعدل والمتمم**).

وبالموازاة مع منافعها وخدماتها الجمة، أضحت التكنولوجيا والإنترنت بصفة خاصة تستخدم لارتكاب الجرائم والإضرار بالأفراد والمؤسسات وممتلكاتهم، وبالتالي أصبح من واجب الدولة اتخاذ الإجراءات اللازمة لإحباط أي هجوم من شأنه تهديد سيادة الدولة ومؤسساتها وأمن مواطنيها.

لقد أبدت الجزائر التي تعتبر دولة رائدة إقليميا في مجال الأمن المعلوماتي استعدادها منذ سنوات لمكافحة الجرائم السيبريانية والمعلوماتية بشكل حازم، لذا عكفت على إعداد النصوص القانونية القادرة على إنشاء منظومة دفاعية وقائية يتم على أساسها مكافحة الأعمال الإجرامية المتعلقة بالإنترنت ومتابعة مرتكبيها قضائيا، كما تسمح بتقصي آثار المجرمين والجناة الذين يستغلون التكنولوجيا وتطبيقاتها لارتكاب أعمالا إجرامية وغير قانونية.

وقد واجه التشريع الجزائري الجرائم السيبريانية، وحاول المشرع الجزائري إصدار قوانين عامة وخاصة وهياكل وأجهزة للجرائم الالكترونية ومن بينها :

- كفل الدستور الجزائري الصادر في ٠٦ مارس ٢٠١٦ حماية الحقوق الأساسية والحريات الفردية وعلى أن تضمن الدولة عدم انتهاك حرمة الإنسان منها المواد ٣٨، ٤٤ من الدستور.
- وقد تم تكريس هذه المبادئ الدستورية في التطبيق بواسطة نصوص تشريعية أوردها قانون العقوبات وقانون الإجراءات الجزائية والتي تحظر كل مساس بهذه الحقوق.

أ- **قانون العقوبات :**

لقد تطرق المشرع الجزائري إلى تجريم الأفعال الماسة بأنظمة الحاسب الآلي حيث عدل قانون العقوبات بموجب القانون رقم ٠٤-١٥ المؤرخ في ١٠ نوفمبر ٢٠٠٤ المعدل والمتمم للأمر رقم ٦٦-١٥٦ المتضمن قانون العقوبات، تحت عنوان : "المساس بأنظمة المعالجة الآلية للمعطيات، ويتضمن هذا القسم ثمانية مواد من المادة ٣٩٤ مكرر إلى ٣٩٤ مكرر ٧.

ب- **قانون الإجراءات الجزائية :**

قام المشرع الجزائري بتمديد الاختصاص المحلي لوكيل الجمهورية في مجال الجرائم الالكترونية، طبقا للمادة ٣٧ فقرة ٠٢ من قانون الإجراءات الجزائية. (ق،إ،ج، الأمر ١٥-٠٢).

حيث يمتد الاختصاص المحلي إذا تعلق الأمر بجرائم المخدرات أو الجريمة المنظمة العابرة للحدود الوطنية أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات أو جرائم تبييض الأموال أو الإرهاب أو الجرائم المتعلقة بالتشريع الخاص بالصرف وجرائم الفساد والتهريب . (اوهايبية، ٢٠١٨، ص ٣٥٨).

كما تعد هذه الجرائم أيضا من الجرائم الموصوفة طبقا للتشريع الجنائي الجزائري.

كما نص على التفتيش في المادة ٤٥ فقرة ٧ من نفس القانون المعدل حيث اعتبر أن التفتيش المنصب على المنظومة المعلوماتية يختلف عن التفتيش المتعرف عليه من حيث القواعد الإجرائية العامة والشروط الشكلية والموضوعية، وبالتالي لا تطبق عليه المادة ٤٤ من قانون الإجراءات الجزائية إذا تعلق الأمر بالجرائم الإلكترونية ونص على توقيف النظر في جريمة المساس بأنظمة معالجة المعطيات طبقا للمادة ٥١ فقرة ٠٦ من القانون (قانون الإجراءات الجزائية).

كما نص أيضا قانون الإجراءات الجزائية بموجب المادة ٦٥ مكرر ٣ فقرة ٥ أنه في حالة الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات فإن وكيل الجمهورية المختص يقوم بوضع الترتيبات التقنية دون موافقة المعني، من أجل التقاط وتثبيت وبث وتسجيل الكلام المتفوه به بصفة خاصة أو سرية في أماكن خاصة أو عامة .

وفي عام ٢٠٠٦، أدخل المشرع تعديل آخر على قانون العقوبات بموجب القانون رقم ٠٦-٢٣ المؤرخ في ٢٠ ديسمبر ٢٠٠٤، من هذا التعديل القسم السابع مكرر والخاص بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، وقد تم تشديد العقوبة المقررة لهذه الأفعال.

وبعد التعديل الأخير لقانون العقوبات الجزائري بموجب القانون رقم ١٦-٠٢ المؤرخ في ١٩ يونيو ٢٠١٦ (ج، ر، ج، ج، عدد ٢٠١٦/٣٧)، ضمن القسم السابع مكرر من قانون العقوبات بموجب المواد من ٣٩٤ مكرر إلى المادة ٣٩٤ مكرر ٨.

وضمن نطاق الفصل الثالث الخاص بالجنايات والجنح ضد الأموال .

من بين هذه الجرائم : الغش أو الشروع فيه في كل أو جزء من المنظومة للمعالجة الآلية للمعطيات، حذف أو تغير للمعطيات المنظمة، إدخال أو تعديل في نظام المعطيات، تصميم أو بحث أو تجميع أو توفير أو نشر أو حيازة أو إفشاء أو نشر أو استعمال المعطيات، تكوين جمعية الأشرار.

ج- **صدور قانون رقم ٠٩-٠٤ :**

عمليا، سعت الجزائر إلى استدراك الفراغ القانوني من خلال تعزيز منظومتها التشريعية خاصة منذ ٢٠٠٩، بحيث سن المشرع الجزائري القانون رقم ٠٩-٠٤ المتعلق بالقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها بتاريخ ٠٥ أوت ٢٠٠٩. (القانون رقم ٠٩-٠٤) .

يحتوي هذا القانون على ١٩ مادة موزعة على ٠٦ فصول مستمدة من الاتفاقيات الدولية (اتفاقية بودابست حول الجرائم المعلوماتية لسنة ٢٠٠١).

كما جاء مطابقا للتشريعات الوطنية لاسيما تلك المتعلقة بمحاربة الفساد وتبييض الأموال وتمويل الإرهاب.

حيث نص القانون رقم ٠٩-٠٤ وبموجب الفصل الخامس منه على إنشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته.

و من مهام الهيئة الوطنية تفعيل التعاون القضائي والأمني الدولي وإدارة وتنسيق العمليات والوقاية ولمساعدة الجهات التقنية للجهات القضائية والأمنية مع إمكانية تكليفها بالقيام بخبرات قضائية في حالة الاعتداءات على المنظومة المعلوماتية على نحو يهدد مؤسسات الدولة أو الدفاع الوطني أو المصالح الإستراتيجية للاقتصاد الوطني.

و ذلك بالتعاون مع جهات قضائية أخرى منها المعهد الوطني للأدلة الجنائية وعلم الإجرام والمديرية العامة للأمن الوطني مكافحة الجريمة الإلكترونية ذات البعد الدولي من خلال انضمامها للمنظمة الدولية للشرطة الجنائية .INTERPOL.

علاوة على ذلك يجب التنويه بالجهود التي تقوم بها الجزائر منذ جانفي ٢٠١٥ من أجل تكييف إطارها التشريعي والتنظيمي من خلال تبني مجموعة من القوانين الهامة منها الخاصة بالتوقيع والمصادقة الالكترونية التي من شأنها تطوير الخدمات المقدمة عبر الإنترنت مثل الإدارة الالكترونية، التجارة الالكترونية وكذا البنوك الالكترونية، فضلا عن سعي الجزائر الحثيث إلى إرساء قاعدة قانونية لاستخدام التكنولوجيات الجديدة للإعلام والاتصال في تطوير قطاع العدالة.

ثالثا :سياسة جهاز الدفاع الوطني في تحقيق الأمن المعلوماتي :

لقد وضعت قيادة الدفاع الوطني الأمن السيبراني أحد أولوياتها، على غرار باقي دول العالم التي سارعت إلى مراجعة سياساتها الأمنية، وإدراجها لآليات وميكانيزمات جديدة تعني بهذه المسائل بالموازاة مع تطوير البنايات الأساسية المتعلقة بتكنولوجيات العالم الرقمي . ويفرض مطلب الأمن مضاعفة أنظمة الرقابة التي قد تشكل تهديدا ممكنا للحريات الفردية، ولهذا وجب مرافقة كل المقاربات

الأمنية في مجال الأمن الرقمي للأطر القانونية والتكنولوجية الملائمة، وتأخذ بعين الاعتبار دقة الهجمات الالكترونية وتعقيداتها والتي يزداد خطرها مع التطور التكنولوجي واستخداماتها اليومية.

و تجسيدا لذلك باشرت الدولة الجزائرية وفي مقدمتها مؤسسة الدفاع الوطني إلى إعداد برامج خاصة لمجابهة الجريمة الالكترونية والحد من انتشارها، وإنشاء أجهزة جديدة تنسجم في أدوارها وتجهيزاتها مع المتغيرات الحاصلة في هذا المجال، إذ أصبحت الحماية السيبرانية جزء مهما في أي منظومة للدفاع، وقد استطاع الجيش الشعبي الوطني المضي قدما ومسايرة التطورات التكنولوجية والإعلامية الحاصلة في العالم، ومن ثمة تأمين وحماية نطاقه المعلوماتي، وتأمين الفضاء المعلوماتي لكل الناشطين فيه. (دبارة سمر، المجلة الجزائرية للأمن الإنساني،ص ٢٦٢).

١- **الهياكل المنشأة لتقصي الجريمة السيبرانية :**

أ- **مركز الوقاية من جرائم الإعلام الآلي وجرائم المعلوماتية للدرك الوطني :**

أنشئ هذا المركز في ٢٠٠٨، يوجد مقره ببئر مراد رايس، أهدافه تأمين منظومة المعلومات لخدمة الأمن العمومي، وهو بمثابة مركز توثيق، ويقوم بتحليل المعطيات والبيانات للجرائم المعلوماتية المرتكبة، ومحاولة تحديد هوية أصحابها، مما يأمن الأنظمة المعلوماتية للمؤسسات والبنوك والبيوت والشركات ... الخ، ويعمل على التنسيق الأمني بين الأجهزة الأمنية الأخرى، والجدير بالذكر أن المركز استطاع معالجة أزيد من ١٠٠ جريمة الكترونية سنة ٢٠١٤، وما يفوق ٥٠٠ قضية رقمية خلال سنة ٢٠١٥، وهذا بفضل التركيبة البشرية المؤهلة التي اكتسبها الجهاز من التكوين المستمر والملتقيات الوطنية والدولية وتبادل الخبرات مع الدول الأخرى.

ب- **المعهد الوطني للأدلة الجنائية وعلم الإجرام :**

أنشأ المعهد الوطني للأدلة الجنائية وعلم الإجرام ببوشاوي التابع للقيادة العامة للدرك الوطني قسم الإعلام والاتصال الإلكتروني، أنشأ بموجب المرسوم الرئاسي رقم ٠٤-١٨٣ المؤرخ في ٢٦ يونيو ٢٠٠٤ وعدل نظامه الأساسي بموجب المرسوم الرئاسي رقم ٠٩-١١٨ المؤرخ في ١٤ أفريل ٢٠٠٤.

يتكون هذا الجهاز من "١١" إحدى عشر دائرة متخصصة في عدة مجالات متباينة، تضمن جميعها الخبرة والتكوين والتعليم، وتقديم جميع المساعدات التقنية، تقوم دائرة الإعلام الآلي والالكتروني المكلفة بمعالجة وتحليل وتقديم كل دليل رقمي يساعد العدالة مع تقديم المساعدة للمحققين، يتكون من عدة تجهيزات تتمثل في محطة ترميم وتصليح الأجهزة والحوامل المعطلة، الشبكات الإعلامية والتجهيزات البيانية، محطة محمولة وثابتة لإجراء خبرات الإعلام الآلي، ويحتوي سبع

قاعات، هي: كتب التوجيه، فصيلة الأنظمة المشحونة، فصيلة تحليل المعطيات، فصيلة الهواتف، اقتناء المعطيات، قاعة موزع وقاعات تخزين.

حيث يعد مؤسسة عمومية ذات طابع إداري تحت الوصاية المباشرة لوزير الدفاع الوطني مكلفة بالمهام التالية:

- إجراء الخبرات والفحوص العلمية في إطار التحريات الأولية والتحقيقات القضائية وهذا بغرض إقامة الأدلة التي تسمح بالتعرف على مرتكبي الجنايات والجنح.
- ضمان المساعدة العلمية أثناء القيام بالتحريات المعقدة باستخدام مناهج الشرطة العلمية.
- المشاركة في الدراسات والتحاليل المتعلقة بالوقاية والتقليل من كل أشكال الإجرام.
- تصميم وإنجاز بنوك المعطيات.
- المشاركة في تحديد سياسة جنائية مثلى لمكافحة الإجرام.
- المبادرة وإجراء بحوث متعلقة بالإجرام باللجوء إلى التكنولوجيات الدقيقة.
- العمل على ترقية البحوث التطبيقية وأساليب التحريات التي أثبتت فعاليتها في ميادين علمي الإجرام والأدلة الجنائية على الصعيدين الوطني والدولي.
- المشاركة في كل الملتقيات والمحاضرات والندوات على الصعيدين الوطني والدولي لتطوير مستوى مستخدمي المعهد.
- المساهمة في تنظيم دورات الإتقان والتكوين ما بعد التدرج في تخصيص العلوم الجنائية.

و لتأدية مهامه على أكمل وجه فإن المعهد الوطني للأدلة الجنائية وعلم الإجرام يحتوي علـــى العديد من الأقسام والمصالح المختصة من أهمها:

- **مصلحة البصمات:** يتم على مستوى هذه المصلحة مقارنة البصمات للتعرف على الجثث وتجدر الإشارة إلى أن الدرك الجزائري مجهز بأنظمة التعرف الآلي على البصمات THEAFIS (Automated Fingerprint Identification System.
- **مصلحة الوثائق:** في هذه المصلحة يتم التأكد من صحة الوثائق والإمضاءات والتحقق من النقود وكذلك التأكد من صحة الوثائق السرية .
- **مصلحة الإعلام الآلي:** على مستوى هذه المصلحة يتم رصد ومراقبة وتتبع عمليات الاختراق والقرصنة المعلوماتية وكذا اكتشاف المعلومات المسروقة وتفكيك البرامج المعلوماتية.

- **مصلحة البيئة:** تشرف هذه المصلحة على عمليات البحث في أسباب تلوث المياه والتربة وكذا الكشف عن المواد السامة المتواجدة في المحيط أو أماكن العمل. (بارة سمير، ٢٠١٧، ص ٤٣٦).

ج- **المصلحة المركزية لمكافحة الجريمة المعلوماتية التابعة لمديرية الأمن الوطني:**

استجابة لمطلب الأمن المعلوماتي ومحاربة التهديدات الأمنية الناجمة عن الجرائم الالكترونية قامت مصالح الأمن بإنشاء المصلحة المركزية للجريمة الالكترونية التي عملت على تكييف التشكيل الأمني لمديرية الشرطة القضائية، والتي كانت عبارة عن فصيلة شكلت النواة الأولى لتشكيل أمني خاص لمحاربة الجريمة الالكترونية على مستوى المديرية العامة للأمن الوطني والتي أنشئت سنة ٢٠١١، ليتم بعدها إنشاء المصلحة المركزية لمحاربة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال بقرار من المدير العام للأمن الوطني وأضيف للهيكل التنظيمي لمديرية الشرطة القضائية في جانفي ٢٠١٥.

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

تشكلت هذه الهيئة بمقتضى المرسوم الرئاسي رقم ١٥-٢٦١ وهي سلطة إدارية مستقلة لدى وزير العدل، تعمل تحت إشراف ومراقبة لجنة مديرية يترأسها وزير العدل وتضم أساسا أعضاء من الحكومة معنيين بالموضوع ومسؤولي مصالح الأمن وقاضيين من المحكمة العليا يعينهما المجلس الأعلى للقضاء.

و تضم الهيئة قضاة وضباط وأعوانا من الشرطة القضائية تابعين لمصالح الاستعلامات العسكرية والدرك الوطني والأمن الوطني وفقا لأحكام القانون الإجراءات الجزائية .

و كلفت الهيئة باقتراح عناصر الإستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها وتنشيط وتنسيق عمليات الوقاية منها، ومساعدة السلطات القضائية ومصالح الشرطة القضائية في مجال مكافحة هذه الجرائم، من خلال جمع المعلومات والتزويد بها ومن خلال الخبرات القضائية، وضمان المراقبة الوقائية للاتصالات الالكترونية، قصد الكشف عن الجرائم المتعلقة بالأعمال الإرهابية والتخريبية والمساس بأمن الدولة.

و هي سلطة إدارية تشكلت بمرسوم رئاسي رقم ١٥-٢٦١ تعمل تحت إشراف لجنة يديرها وزير العدل، تضم أعضاء من الحكومة ومسؤولي مصالح الأمن وقضاة وأعوان الشرطة القضائية تابعين للاستعلامات العسكرية والدرك الوطني والأمن الوطني . تعمل على الكشف عن الجرائم الإرهابية الالكترونية وجرائم المساس بأمن الدولة .(يوسف بوغرارة، مجلة الدراسات الإفريقية، ٢٠١٨، ص ١١٢).

٢- دور الجيش الوطني الشعبي في تحقيق الأمن المعلوماتي :

يقصد بالدفاع الالكتروني في الاستراتيجيات العسكرية : " مجموعة القدرات النظامية التي تمتلكها القوات المسلحة للحماية من تأثير الهجمات الالكترونية، والتخفيف من حدتها والتعافي منها بسرعة"، فقد اعتبرت الإستراتيجية النمساوية مصطلح الدفاع الالكتروني " جميع التدابير اللازمة للدفاع عن الفضاء الالكتروني بالوسائل المناسبة لتحقيق الأهداف العسكرية الإستراتيجية "، أما بخصوص الإستراتيجية العسكرية البلجيكية، اعتبرت الدفاع الالكتروني " تطبيق التدابير الوقائية الفعالة للحصول على مستوى مناسب من الأمن الالكتروني، وتقليل المخاطر الأمنية إلى مستوى مقبول، " وفيما يتعلق بالإستراتيجية العسكرية الفرنسية : " مجموعة الوسائل الفنية وغير الفنية التي تسمح للدولة بالدفاع عن نظم المعلومات الحرجة في الفضاء الالكتروني "، وفيما يتعلق بالإستراتيجية العسكرية الجزائرية، فقد اعتبرت الدفاع الالكتروني "مراقبة الأنظمة التي تحمي الدولة من كافة التهديدات، ومتابعة حالة تقدم نشاطات تجسيد السياسة الشاملة للدفاع السيبراني الرامية لضمان فعالية الحماية ضد التهديدات السيبرانية التي تستهدف أنظمة المعلومات ومنظومات الاتصال وكذا منظومة الأسلحة للجيش" (نوارة باشوش، جريدة الشروق، ٢٠١٩ ص ٠٣).

حيث أصبحت الحروب المستقبلية حروب الالكتروني، كما أبرزت مجلة الجيش في العدد ٦٧٦ لشهر نوفمبر ٢٠١٩ على أهمية المركز الوطني للإشارة للجيش الوطني الشعبي (مجلة الجيش، العدد ٦٧٦ لسنة ٢٠١٩).

أ- **الدفاع السيبراني في الجيش الوطني الشعبي :**

قررت القيادة العليا للجيش الوطني إحداث "مصلحة الدفاع السيبراني ومراقبة أمن الأنظمة " على مستوى دائرة الاستعمال والتحضير لأركان الجيش الوطني الشعبي، بهدف تأمين وحماية المنظومات والمنشآت الحيوية لقواتنا المسلحة ضد التهديدات السيبرانية .

وعيا منها بالتحديات التي بات يحملها هذا الواقع الجديد وقصد الإلمام بكافة التهديدات التي يشكلها الدفاع السيبراني على الأمن وحتى على سيادة الدول والحكومات . قامت قيادة الجيش الوطني الشعبي بوضع إستراتيجية دفاع سيبراني، تغطي كل الجوانب التي لها صلة بتحقيق نظام دفاع سيبراني متكامل وفعال بهدف تأمين وحماية المنظومات والمنشآت الحيوية للدولة الجزائرية، حيث تم في هذا الصدد وبتاريخ ٦ نوفمبر ٢٠١٥ إحداث على مستوى دائرة الاستعمال والتحضير لأركان الجيش الوطني الشعبي " مصلحة الدفاع السيبراني ومراقبة أمن الأنظمة "، تكلف أساسا بتخطيط وإدراج ومتابعة حالة تقدم نشاطات تجسيد السياسة الشاملة للدفاع السيبراني الرامية لتحقيق بفعالية الحماية ضد التهديدات السيبرانية التي تستهدف أنظمة المعلومات ومنظومات الاتصال وكذا منظومات الأسلحة للجيش الوطني الشعبي .

تتمحور إستراتيجية الدفاع السيبراني للجيش الوطني الشعبي حول سبعة محاور وهي :

- ✓ **جانب وظيفي وتنظيمي :** تكون أعمال الدفاع السيبراني ضمن الجيش الوطني الشعبي موجهة ومنفذة في إطار وظيفة و/ أو تنظيمية مكرسة لضمان تجانس وفعالية هذه الأعمال .
- ✓ **جانب قانوني :** تحيين وتعزيز باستمرار الإطار القانوني المتعلق باستعمال تكنولوجيات الإعلام والاتصال عموما وتأمين منظومات الإعلام خصوصا.
- ✓ **جانب الموارد البشرية :** تعد جاهزية مورد بشري تقني معتبر وذوي كفاءة عالية في مجال الدفاع السيبراني هدفا أساسيا لكي تضمن نجاح إدخال هذا المجال في النشاطات العملياتية والتسيير للجيش الوطني الشعبي.
- ✓ **جانب تقني :** تقوية وتكييف القدرات التقنية للحماية، الكشف والرد على الهجمات السيبرانية باستمرار، مع ضمان يقظة دائمة فيما يخص الطرق والوسائل المستعملة من طرف المهاجمين
- ✓ **جانب الوقاية والتحسيس :** الوقاية وتحسيس مستخدمي الجيش الوطني الشعبي من المخاطر والتهديدات التي تنجز عن استعمال تكنولوجيات الإعلام والاتصال في الإطار المهني أو الشخصي بطريقة مستمرة
- ✓ **جانب البحث والتطوير:** تعد درجة معتبرة من الاستقلالية التكنولوجية، باستعمال وسائل تقنية خاصة أو مشخصة من طرف هياكل البحث والتطوير للجيش الوطني الشعبي، لاسيما تلك المستعملة للحماية ضد التهديدات السيبرانية، عنصرا حاسما في إستراتيجية الدفاع السيبراني
- ✓ **جانب التعاون :** تعزيز التعاون في مجال الدفاع السيبراني مع جيوش الدول الشريكة من أجل السماح للجيش الوطني الشعبي من الاستفادة من الخبرات والوسائل التكنولوجية المتقدمة جدا

في سياق ذي صلة وتعزيزا لإستراتيجية الدفاع الوطني لمكافحة التهديدات السيبرانية، وقصد الإلمام بكافة المستجدات في هذا المجال، وبخاصة تلك التي تعالج موضوع الأمن السيبراني والدفاع كرهان للأمن والدفاع الوطنيين وحماية المنشآت الحساسة ضد الهجمات السيبرانية، تعكف مصلحة الدفاع السيبراني ومراقبة أمن الأنظمة لدائرة الاستعمال والتحضير لأركان الجيش الوطني الشعبي دوريا على تنظيم ملتقيات محاضرات وورش عمل تطبيقية، كان آخرها ملتقى بعنوان : " الدفاع السيبراني : مكون أساسي للأمن والدفاع الوطني " يومي ١٥ و١٦ ماي ٢٠١٧، والذي أكد من خلاله رئيس دائرة الاستعمال والتحضير لأركان الجيش الوطني الشعبي اللواء شريف زراد في كلمة افتتاحه، أن تنظيم مثل هذا الملتقى يأتي من أجل خلق فضاء نقاش بين مختلف الفاعلين في الفضاء السيبراني على المستوى الوطني، لفهم أفضل لرهانات الأمن والدفاع السيبرانين، ولتحسين وإثراء المعارف في

مجال الوقاية ومكافحة التهديدات السيبرانية وكذا تحديد أثرها على الأمن الوطني. (مجلة الجيش، العدد ٦٥١ لسنة ٢٠١٧).

مهام مصلحة الدفاع السيبراني ومراقبة أمن الأنظمة :

مصلحة الدفاع السيبراني ومراقبة أمن الأنظمة هي تركيبة ملحقة بدائرة التحضير والاستعمال لأركان الجيش الوطني الشعبي، فاستحداثها في نوفمبر ٢٠١٥، يندرج ضمن نهج إرساء السياسة الشاملة المسطرة من قبل القيادة العليا والهادفة إلى حماية مؤسستنا ضد المخاطر والتهديدات السيبرانية، وباعتبارها جهاز للتوجيه والخبرة من المستوى الاستراتيجي، تحرص هذه المصلحة أساسا على وضع وتطبيق السياسة العامة للدفاع السيبراني في الجيش الوطني الشعبي وأيضا إلى تقييم وتعزيز مستوى أمن الأنظمة المستغلة وكذا إلى تحيين وتطبيق الإطار التنظيمي المسير لمجال الدفاع السيبراني .

على الصعيد العملياتي : تتمثل مهام المصلحة التي تعد طرفا فاعلا في العمليات العسكرية في تعزيز قدراتنا في مجال الدفاع السيبراني، على نحو يسمح بتأمين أنظمة السلاح والإعلام والاتصال .

طبقا لتوجيهات القيادة العليا، وباعتبارها هيئة تابعة لوزارة الدفاع تساهم هذه المصلحة مع الهيئات الوطنية المعنية في إعداد ووضع السياسة الوطنية المتعلقة بالدفاع السيبراني، مع ضمان التنسيق مع مختلف الهيئات في مجال تأمين المنشآت الرقمية الحساسة.

ب- **الأمن والدفاع السيبراني للجيش الوطني الشعبي :**

تحت تأثير الفضاء الالكتروني أو ما أصبح يعرف بالقوة السيبرانية، دفعت العديد من الدول إلى تبني استراتيجيات في مجال دفاعها السيبراني وتدعيم مراكز قوتها بطريقة تشابه الاستراتيجيات الدفاعية التقليدية، خاصة في ظل توزع القوة السيبرانية بين عدد من الفاعلين من غير الدول وبروز التهديدات التي أصبحت تطال أمن واستقرار الدول موازاة مع تغيير منطق الحروب حاليا نحو الاتجاه اللاتماثلي.

شهد القرن الحالي ثورة منفردة في عالم تكنولوجيا الإعلام والاتصال، إلى الحد الذي أعدها بعض الخبراء والمختصين الميدان الخامس للنزاعات، بعد الأرض، البحر، الجو والفضاء، ويعود ذلك إلى درجة الانتشار والتطور السريعين لهذه التقنية، حيث يكاد لا يخلو مجال من مجالات الحياة إلا وارتكز عليها، وبالخصوص مع ارتباط معظم الخدمات وقواعد البيانات والبنى التحتية والأنظمة المالية والمصرفية بشبكة الإنترنت، وكذا اتجاه معظم الدول والحكومات لتبني نماذج الحكومات الذكية والتحول نحو الخدمات الالكترونية التي قلصت الجهد، الوقت والتكلفة، وساهمت بسرعتها ومرونتها في تلبية الاحتياجات، ولذا فإن الحفاظ على هذا البنى من أي هجمات الكترونية يدخل في صميم الأمن

القومي للدول، لأن تعرض أحد هذه الأنظمة لهجوم الكتروني يمكن أن يولد آلاف الضحايا في دقائق معدودة، فمثلا قد يؤدي اختراق نظام المواصلات كأنظمة ملاحة الطيران والسفن وسكك الحديد إلى تصادمها، وعليه فإن خلق نظام دفاع الكتروني فعال يعمل بمثابة حائط صد للهجمات الالكترونية يعد أمرا حيويا للأمن القومي للدول.

على الرغم من الايجابيات التي حملتها الإنترنت والتي جعلت من عصرنا الحالي عصر فضاء الكتروني بامتياز، وأضحت فيه (الإنترنت) الإطار العام الحاكم لتفاعلاته كافة، سواء كانت شخصية أو عامة، عسكرية أو سياسية، اقتصادية أو اجتماعية، إلا أنها جلبت معها العديد من التهديدات والمخاطر والأخص على الأمن القومي للدول، فإذا كان العدو في عهد الحرب الباردة معروفا وواضحا، ويمكن تعقبه والتنبؤ بسلوكه، فإن الأمر يختلف تماما في حالة العصر السيبراني، فالعدو ليس بالضرورة دولة، ولا يتقاسم بالضرورة جوارا جغرافيا، كما أن استهداف المناطق والخدمات الإستراتيجية قد يكلف أقل من الحرب التقليدية، وفي أحيان أخرى قد يكون أكثر تدميرا إذا كان الأمر يتعلق بالسيطرة على البنى التحتية والخدمات اللوجستية، سواء كانت مدنية أو عسكرية .

طبيعة وأشكال التهديدات السيبرانية :

هناك العديد من أنواع الهجمات السيبرانية، نذكر منها على سبيل المثال لا الحصر :

- ✓ **تخريب المواقع:** الهجمات التي تشوه صفحات على الإنترنت أو تدمرها أو تغير طبيعتها، وهذا النوع من الهجمات عادة ما يرد بسرعة ويكون ضرره محدودا.
- ✓ **الدعاية السلبية:** رسائل سياسية يمكن نشرها لأي شخص يستخدم الإنترنت.
- ✓ **جمع البيانات:** بمعنى أن المعلومات السرية غير المحفوظة بأمان يمكن اعتراضها والتقاطها، بل وتعديلها، مما يجعل التآمر في هذه الحالة ممكنا.
- ✓ **تعطيل المعدات العسكرية :** الأنشطة العسكرية التي تستعمل الحواسب والأقمار الاصطناعية للتنسيق هي في خطر من هذا النوع من الهجمات، حيث يمكن اعتراض الأوامر والاتصالات أو استبدالها، مما يعرض حياة الجنود للخطر.
- ✓ **مهاجمة البنى التحتية الحساسة :** شبكات الكهرباء والماء والوقود والاتصالات والمواصلات كلها معرضة لحروب الإنترنت، ويمثل هذا التدمير الاقتصادي الأشد وطأة في الحالات القصوى .

ويمكن لهذه الهجمات السيبرانية، أن تستعمل بالموازاة مع أعمال أخرى غير تقنية مثل الاستعلام والاستغلال والتخريب .

نتيجة لهذا التطور التكنولوجي أصبحت الدول في حاجة إلى استراتجيات جديدة لإدارة أمن الفضاء الالكتروني تنطلق من مبدأ رئيسي هو القابلية للاختراق خاصة أن الفضاء الالكتروني مجال عام لا يعترف بالحدود، وعليه فإن منطلق الأمن "السيبراني" لأي دولة يبدأ بتطوير سياسة وطنية لرفع الوعي حول قضايا الأمن "السيبراني" والحاجة لإجراءات وطنية وإلى التعاون الدولي، بل ويتعدى ذلك إلى تطوير مخطط وطني لتحفيز الأمن السيبراني بهدف تقليص مخاطر وأثار التهديدات السيبرانية وكذا المشاركة في الجهود الدولية والإقليمية لتحفيز الوقاية الوطنية والتحضير والاستجابة للتعافي من الحوادث السيبرانية، فعلى سبيل المثال سنت الولايات المتحدة الأمريكية على مدار السنوات الخمسة الماضية فقط ولوحدها ٣٤ قانونا و٥ أوامر تنفيذية لتحسين الأمن السيبراني.

ووفقا للمؤشر العالمي للأمن السيبراني GCI في نسخته الثانية الذي أصدرته وكالة الأمم المتحدة للاتصالات في ٥ يوليو ٢٠١٧، فإنه لا يزال هناك حاجة إلى بذل المزيد من الجهود في هذا المجال الحرج، خاصة أن الحكومات تعتبر المخاطر الرقمية ذات أولوية عالية، كما أصبح الأمن السيبراني مصدر قلق كبير للدفاع القومي، وأظهرت الدراسة وجود فجوات كبيرة في الأمن السيبراني بين الدول الأكثر قوة في العالم .

ويعتمد الأمن السيبراني بناء على توصيات الإتحاد الدولي للاتصالات على مزيج مركب من التحديات التقنية والسياسية، الاجتماعية والثقافية، وحصر المختصون صلاحياته في :

- تطوير إستراتيجية وطنية للأمن السيبراني وحماية البنية التحتية للمعلومات الحساسة .
- إنشاء تعاون وطني بين الحكومة ومجتمع صناعة الاتصالات والمعلومات.
- ردع الجريمة السيبرانية .
- خلق قدرات وطنية لإدارة حوادث الحواسب الآلية.
- تحفيز ثقافة وطنية للأمن السيبراني. (بوكبشة محمد، مجلة الجيش، ٢٠١٧).

خاتمة:

لم يستطع المشرع الجزائري الإحاطة الكلية بمفاهيم حديثة كالذكاء الاصطناعي، ونظام الرقمنة على الرغم من أنه قد تم تقنين نظام التجارة الإلكترونية سنة ٢٠١٨، وعصرنة قطاع العدالة، وغيرها إلا أن هذه التشريعات لا تواكب مطلقا التطور المتلاحق في تقنية الذكاء الاصطناعي، حيث لا تزال جميع البرامج في نظر القانون وبغض النظر عن درجة تطورها مجرد أدوات لتنفيذ أوامر مستخدميها.

١)- جاءت القوانين في هذا الصدد عاجزة عن حماية المستخدم من أخطاء الآلة واستيعاب النتائج.

٢)- ضرورة سن قانون خاص بالرقمنة وقانون خاص بالذكاء الاصطناعي شريطة أن يلعب هذا الأسلوب دورا في صياغة نصوصه بالاشتراك مع كافة القطاعات المعنية بتقنية الذكاء الاصطناعي.

٣)- يشهد عالم التكنولوجيا اليوم ثورة حقيقية بفضل التطور العلمي المتسارع، أمام قصور المنظومة القانونية والتشريعية الجزائرية.

٤)- لقد سن المشرع الجزائري قوانين متعلقة بالتجارة الإلكترونية بموجب القانون ١٨-٠٥ المؤرخ في ١٠ ماي ٢٠١٨، وكذا القانون رقم ١٥-٠٥ المتعلق بعصرنة قطاع العدالة ورقمنته، أما المجال التعليمي فلا يزال قاصرا.

قائمة المراجع:

١)- آل سعود، سارة.*التطبيقات التربوية للذكاء الغصطناعي في الدراسات الاجتماعية*، على الموقع: di.alsaud.s@gmail.com

٢)- الأمر رقم ٦٦-١٥٦ المؤرخ في ٠٨ يونيو ١٩٦٦، المتضمن قانون العقوبات الجزائري المعدل والمتمم.

٣)- الصالحين، محمد العتيبي.الجوانب القانونية لاستخدام المعلوماتية في المعاملات التجارية، *مجلة الحقوق*، العدد ٢، السنة ٣٧.

٤)- الفرا، سليمان يعقوب.*الذكاء الاصطناعي على الموقع*:

http//www.03.ibm.com/innovation/us/waston/building.waston/index.htm

٥)- بوحميدة، نصر الله . (٢٠١٧)، مجلة الحكمة للدراسات التربوية والنفسية، المجلد ٥، العدد ١١.

٦)- حلواجي، عبد الفتاح . (٢٠١٧)، *الرقمنة كمدخل لتحسين الخدمة العمومية في الجزائر، قطاعة العدالة نموذجا*، مذكرة ماستير، حقوق، جامعة الوادي، الجزائر.

٧)- دياب، زهية، (٢٠١٩). برويس وردة، معوقات التعليم الرقمي في المدرسة الجزائرية، *المجلة العربية للآداب والدراسات الإنسانية*، العدد ٧، فيفري .

٨)- ربيعي، فايزة، (٢٠١٧).إتجاهات أساتذة التعليم العالي نحو التعليم الإلكتروني، دراسة ميدانية بجامعة باتنة، *مجلة التواصل*، عدد ٥٠، شهر جوان.

٩)- عزاف، نصر الدين، التعليم الإلكتروني ومستقبل الإصلاحات بالجامعة الجزائرية، *مجلة Rust*، مج ١٩، ع ٢، على الموقع: gheraf.nacereddine@gmail.com

١٠)- لونيس، علي، اشعلال، ياسمينة .دور التعليم الرقمي في تحسين الأداء لدى المعلم والمتعلم (البيئة المهنية نموذجا)، *مجلة العلوم الإنسانية والاجتماعية*، (د.س.ن).

١١)- *مجلة الجيش*. العدد ٥٩٩، جوان ٢٠١٣، (www.mdn.dz).

١٢)- *مجلة الجيش*. العدد ٦٥٧، أبريل ٢٠١٨، على الموقع الرسمي لوزارة الدفاع الجزائرية (www.mdn.dz).

١٣-)*مجلة الجيش*. العدد ٦٨٠، مارس ٢٠٢٠، (www.mdn.dz).

13)- Abdouni Abdelhamid, informatique, intelligence et intelligence artificielle, Revue.Sciences Sociales et Humaines, N°4(1996).

http//www.03.ibm.com/innovation/us/waston/building.waston/index.html