
خدمات أكاديمية
كفاءات وطنية
معايير عالمية
دراسة
للاستشارات والدراسات والترجمة
UNIVERSITY
drasah1
www.drasah.com
00966555026526
00966560972772
info@drasah.com

خدماتنا

شركة دراسة
للاستشارات و الدراسات والترجمة

توفير المراجع العربية والأجنبية

التحليل الاحصائي وتفسير النتائج

الاستشارات الأكاديمية

جمع المادة العلمية

الترجمة المعتمدة

drasah1
info@drasah.com
00966555026526
00966560972772
drasah.com


دراسة
للاستشارات والدراسات والترجمة
تواصل معنا
00966555026526
00966560972772
متواجدون على مدار الســـاعة

الدكتورة عائشة عبد الحميد

دكتوراه علوم في القانون الدولي والعلاقات الدولية

أستاذة محاضرة

الإطـار القانوني والتشريعي للرقمنة والذكـاء الإصطناعي

Title of the intervention: The legal and legislative framework for digitization and artificial intelligence

ملخص :

نتاجا لما فرضه الو اقع المعاصر من إنتشار هائل لنظم تكنولوجيا المعلومات التي تعتمد على البدائل الرقمية، مستغنية بذلك عن الكتابة على الورق.

تحت 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 الإتصال، نتساءل عن كيفية حماية الحياة الخاصة في مواجهته، وكيفية حماية برامجه مدنيا وجنائيا.

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

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.

مقدمـــة:

إن الإستخدام الواسع والمتزايد للتكنولوجيات الرقمية يسير بالموازاة مع الإعتماد المتزايد على هذه التكنولوجيات.

حيث شهد القرن الحادي والعشرون ثورة حقيقية في عالم تكنولوجيات المعلومات والإتصالات وإنتشارا واسعا للأنترنت وتطبيقاتها في شتى المجالات الإقتصادية والإجتماعية والثقافية (التجارة، الخدمات الحكومية، التعليم، المعرفة، الترفيه، السياحة، الرعاية الصحية) وغيرها، وهذا ما يطلق عليه حاليا " الخدمات الإلكترونية"(مجلة الجيش الجزائري، جانفي 2016 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 أوورقي، إلى آخر رقمي من خلال تقنيات تحويل المواد. (مجلة الجيش الجزائرية، العدد 657، أفريل 2018 على الموقع:www.mdn.dz).

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

ولكن كيف يمكن لنا حماية معلوماتنا التعليمية القرمية في ظل عدم إيجاد قانون ؟ أو على الاقل يوجد نظام تشريعي ولكنه قاصروغير مكتمل؟.

لأن دراستنا هذه ستزيد من خلالها تسليط الضوء على التجربة الجزائرية ؟ أولا- التعريف بالمصطلحات الدقيقة في مجال التعليم الرقمي والذكاء الإصطناعي. ثانيا- الإطار التشريعي للإختراق الرقمي في الجزائر (المنظومة التشريعية). ثالثا- سياسة جهاز الدفاع الوطني في تحقيق الأمن المعلوماتي.

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

1)- ظهور الذكاء الإصطناعي:

ظهر الذكاء الإصطناعي خلال مؤتمر دولي جرى بأمريكا سنة 1956 نشطه مختصون في مجالات علوم النفس، الرياضيات، الاقتصاديات والأعصاب، وبلغ ذروته في سنة 2010 بفضل تسارع الإلكترونيات من خلال البيانات الرقمية.

التأطير القانوني والأخلاقي للذكاء الإصطناعي:

فيجب أن يستفيد الإنسان أو المجتمع من منافع الذكاء الإصطناعي وقد لا يكون منافسا له أو ضحية لأحداث لا يعالجها القانون (جريدة الشعب، 27 نوفمبر 2018).

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

وهو مصطلح إزداد استخدامه مؤخرا في ظل النهضة التقنية التي يشاهدها العالم في مجال تطوير الآلات رغم أن " الذكاء الإصطناعي " في القرن الواحد والعشرون أصبحت ابحاث الذكاء الإصطناعي على درجة عالية من التخصص، مما اسهم في إنقسامه إلى مجالات فرعية مستقلة.

معظم هذه المجالات اتفقت في أن الآلة الذكية يجب أن يكون لها القدرة على التحكم ، الإستنتاج، ورد الفعل، على ظروف لم تبرمج عليها.

وفي كثير من الحالات يرتبط مصطلح " الذكاء الإصطناعي " بالآلات ككل، ولكن برنامج الحاسوب التي يتم تثبيتها على هذه الأجهزة، والتي تتسم بسلوك وخاصيات تقنية تجعلها تحاكي القدرات الذهنية البشرية، و أنماط عملها وهذا الأمر منطقي حيث أن الآلة أو الجهاز نفسه

يشابه جسم الإنسان في الوقت الذي يقوم به العقل البشري بكافة الوظائف المتعلقة بالتفكير، إتخاذ القراروحل المسائل.

(سليمان يعقوب الفرا، الذكاء الإصطناعي، على الموقع:

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

الذكاء الإصطناعي : هو عبارة عن 3 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).

2)- مصطلح التعليم الرقمي:

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

أوهو استخدام التقنية بجميع أنواعها، في إيصال المعلومة للمتعلم بأقصروقت و اقل 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، 2019، ص 153).

فالتعليم الإلكتروني: هو مصطلح مرن، يستخدم لوصف وسيلة للتدريس من خلال التكنولوجيا، من خلال تسهيل عملية الإتصال 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 الإتصال الحديثة (الزين، http://jilrc.com).

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

وتجدر الإشارة إلى أن التعليم الإلكتروني لا يلغي دور المعلم ولكنه يعير 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 59-81).

أما تقنيات التعليم الإلكتروني فهي:

يقوم التعليم الإلكتروني على استخدام الوسائل الإلكترونية المختلفة في عملية التعليم، وتتمثل هذه الوصائل الإلكترونية في: الكمبيوتر، الأنترنت، التلفزيون، الإذاعة، الفيديو، ومؤثرات الفيديو...، الكتاب الإلكتورني. (دياب، بروسيس، 2019، ص 153).

3)- مصطلح السيادة الرقمية:

يعتبر مصطلح السيادة الرقمية عند تطبيق مبادئ السيادة في مجال تكنولوجيا الإعلام والإتصال.

الجزائر وبتعداد سكاني يقدر بأكثر من 42 مليون نسمة، يحصي أكثر من 22 .مليون حساب على " فايسبوك "، ويتابع حوالي 52,34% الأخبار على الأنترنت، بالإضافة إلى الآلاف من المشتركين في الشبكة عبر الهاتف النقال.

ضمن 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 خطيرحول إدراك عو اقب ذلك. (مجلة الجيش، العدد 680، مارس 2020 على الموقع الرسمي لوزارة الدفاع الجز ائرية www.mdn.dz).

حيث تحول الهاتف النقال منذ ظهوره أول مرة إلى ثورة تكنولوجية غير مسبوقة ومستمرة دون توقف، بحيث تعدى استخدامه من إجراء المكاملتاالهو اتفية إلى إستخدامه كجهاز كمبيوتر وتلفزيون وجريدى ومكتب، مكتبة ومفكرة شخصية وغيرها من التطبيقات والخدمات خاصة في ظل تقنية (الجيل الثالث والجيل الر ابع ... (مجلة الجيش، عدد 604، نوفمبر2013).

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 المو اقف (بوحميدة، 2017، ص 83).

ويعود السبب أيضا إلى إلى طبيعة الحاسوب وإرتباطه الوثيقة بحياة الإنسان اليومية ... وإلى الفو ائد التي تعود على مستخدميه في كافة المجالات الحياة بصفة عامة، والتعليم بصفة خاصة (ربيعي، 2017، ص 21).

وبفضل إنتشار المجتمع المعلوماتي والبيانات الضخمة أمكن استثمار البيانات والعمليات " المرقمنة " في تغذية أنظمة الذكاء الإصطناعي.

والرقمنة هي ايضا استخدام التقنيات الرقمية لتغيير نماذج الأعمال والعمليات وتوفير فرص جديدة لتوليد الثروة وللتنمية المستدامة.

ويمكن النظر إلى الرقمنة بأنها أيضا تحويل العمليات إلى نسخ رقمية وإلغاء الحواجز بين البشر وتقنية المعلومات والإتصالات باستخدام تقنيات الذكاء الإصطناعي لتحقيق مردود اقتصادي وإجتماعي بفاعلية و إنتاجية أعلى.

ويمكن تعريف الذكاء الإصطناعي بأنه قدرة الحاسب أو الربوتوت الذي يتحكم فيه حاسب على آداء المهام المقترنة عادة بالذكاء البشري، فهو يختلف عن الرقمنة. (أبو بكر سلطان، على الموقع:www.alarabiua.net).

في الوقت الذي أصبحت أخلاقيات العلوم وتكنولوجيا المعلومات والإتصالات وخاصة الذكاء الإصطناعي قضية حاسمة في السياسة التشريعية، فالذكاء الإصطناعي مثله مثل أي تكنولوجيا ، فهي أيضا محل الكثير من الشكوك والمخاوف والمعارضة، ومثله مثل أي تكنولوجيا قد يكون سلبيا، فاستعمال الذكاء الإصطناعي 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 ... إلا أمثلة يشهدها الو اقع عن الاستعمال السلبي. (www.diae.events).

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

إن التجربة الجز ائرية على غرار العديد من الدول، وخاصة في المجال الرقمي لا تزال في بداياتها، حيث يكتسي موضوع الرقمنة أهمية كبيرة، فهو ليس مجرد إنتقال من نظام تقليدي روتيني بطيء إلى نظام عصري حديث قائم على التكنلوجيا المتطورة، أو توفر أجهزة ومعدات حديثة، وبرامج مختلفة، ولكن ماذا عن سلبيات تلك وكيف تصدى المشرع الجز ائري للإختراق المعلوماتي (حلواجي، 2017، ص 9).

لأن هناك ر ابطين : المعلوماتية Informatiqueو الذكاء الإصطناعي Intelligence et intelligence artificielle(Abdouni, 1995, P5) .

وطالما كنا أمام بدائل رقمية في كل مجالات الحياة تقريبا فإننا بذلك نجزم قطعا استغناءنا عن الكتابة على الورق (الصالحين ، 2013، ص535)، وبالتالي فرضية رقمنة التعليم واستخدام الذكاء الإصطناعي ولكن ليس المشكل في الرقمنة و إنما في كيفية حماية المعطيات الرقمية ضد جنح التقليد واستعمال المقلد، والتزوير واستخدام المزور، وكذلك مختلف الجر ائم المعلوماتية (الأمر 66-156 المتضمن قانون العقوبات الجز ائري المعدل والمتمم).

بالموازاة مع منافعها و خدماتها الجمة ، أضحت التكنولوجيا و الانترنت بصفة خاصة تستخدم لارتكاب الجر ائم و الإضرار بالأفراد و المؤسسات و ممتلكاتهم ، و بالتالي أصبح من واجب الدولة اتخاذ الإجراءات اللازمة لإحباط أي هجوم من شأنه تهديد سيادة الدولة و مؤسساتها و أمن مواطنيها.

لقد أبدت الجزائر التي تعتبر دولة رائدة إقليميا في مجال الأمن المعلوماتي استعدادها منذ سنوات لمكافحة الجرائم السيبريانية و المعلوماتية بشكل حازم، لذا عكفت على إعداد النصوص القانونية القادرة على إنشاء منظومة دفاعية وقائية يتم على أساسها مكافحة الأعمال الإجرامية المتعلقة بالانترنت و متابعة مرتكبيها قضائيا، كما تسمح بثقفي آثار المجرمين و الجناة الذين يستغلون التكنولوجيا و تطبيقاتها لارتكاب أعمالا إجرامية و غير قانونية.

فكيف ساهمت النصوص المختلفة في مكافحة و محاربة الإجرام السبراني أو الإجرام المعلوماتي ؟

و بعبارة أخرى كيف واجه التشريع الجزائري الجرائم السيبريانية ؟

حاول المشرع الجزائري إصدار قوانين عامة و خاصة و هياكل و أجهزة للجرائم الالكترونية و من بينها :

- كفل الدستور الجزائري الصادر في 06 مارس 2016 حماية الحقوق الأساسية و الحريات الفردية و على أن تضمن الدولة عدم انتهاك حرمة الإنسان منها المواد 38، 44 من الدستور.

- و قد تم تكريس هذه المبادئ الدستورية في التطبيق بواسطة نصوص تشريعية أوردها قانون العقوبات و قانون الإجراءات الجزائية و التي 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 04-15 المؤرخ في 10 نوفمبر 2004 المعدل و المتمم للأمر رقم 66-156 المتضمن قانون العقوبات ، تحت عنوان : "المساس بأنظمة المعالجة الآلية للمعطيات، و يتضمن هذا القسم ثمانية مواد من المادة 394 مكرر إلى 394 مكرر 7.

ب- قانون الإجراءات الجزائية :

قام المشرع الجزائري بتمديد الاختصاص المحلي لوكيل الجمهورية في مجال الجرائم الالكترونية، طبقا للمادة 37 فقرة 02 من قانون الإجراءات الجزائية. (ق.إ.ج، الأمر 15-02).

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 الإرهـاب أو الجرائم المتعلقة بالتشريع الخاص بالصرف و جرائـم الفساد و التهريب . (عبد الله اوهايبية ، 2018، ص 358).

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

كما نص على التفتيش في المادة 45 فقرة 7 من نفس القانون المعدل حيث اعتبر أن التفتيش المنصب على المنظومة المعلوماتية يختلف عن التفتيش المتعرف عليه من حيث القواعد الإجرائية العامة و الشروط الشكلية و الموضوعية ، و بالتالي لا تطبق عليه المادة 44 من قانون الإجراءات الجزائية إذا تعلق الأمر بالجرائم الإلكترونية و نص على توقيف النظر في جريمة المساس بأنظمة معالجة المعطيات طبقا للمادة 51 فقرة 06 من القانون (قانون الإجراءات الجزائية).

كما نص أيضا قانون الإجراءات الجزائية بموجب المادة 65 مكرر3 فقرة 5 أنه في حالة الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات فإن وكيل الجمهورية المختص يقوم بوضع الترتيبات التقنية دون موافقة المعني، من أجل التقاط و تثبيت و بث و تسجيل الكلام المتفوه به بصفة خاصة أو سرية في أماكن خاصة أو عامة .

و في عام 2006، أدخل المشرع تعديل آخر على قانون العقوبات بموجب القانون رقـم 23-06 المؤرخ في 20 ديسمبـر 2004، من هذا التعديل القســم السابع مكــرر و الخاص بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، و قد تم تشديد العقوبة المقررة لهذه الأفعال.

و بعد التعديل الأخير لقانون العقوبات الجزائري بموجب القانون رقم 16-02 المؤرخ في 19 يونيو 2016 (ج، ر، ج ، ج ، عدد 2016/37) ، ضمن القسم السابع مكرر من قانون العقوبات بموجب المواد من 394 مكرر إلى المادة 394 مكرر8.

و ضمن نطاق الفصل الثالث الخاص بالجنايات و الجنح 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 09-04 :

عمليا ، سعت الجزائر إلى استدراك الفراغ القانوني من خلال تعزيز منظومتها التشريعية خاصة منذ 2009، بحيث سن المشرع الجزائري القانون رقم 09-04 المتعلق بالقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها بتاريخ 05 أوت 2009. (القانون رقم 09-04) .

يحتوي هذا القانون على 19 مادة موزعة على 06 فصول مستمدة من الاتفاقيات الدولية (اتفاقية بودابست حول الجرائم المعلوماتية لسنة 2001).

كما جاء مطابقا للتشريعات الوطنية لاسيما تلك المتعلقة بمحاربة الفساد و تبييض الأموال و تمويل الإرهاب.

حيث نص القانون رقم 09-04 و بموجب الفصل الخامس منه على إنشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحته.

و من مهام الهيئة الوطنية تفعيل التعاون القضائي و الأمني الدولي و إدارة و تنسيق العمليات و الوقاية و لمساعدة الجهات التقنية للجهات القضائية و الأمنية 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 و علم الإجرام و المديرية 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 2015 من أجل تكييف إطارها التشريعي و التنظيمي من خلال تبني مجموعة من القوانين الهامة منها الخاصة بالتوقيع و المصادقة الالكترونية التي من شأنها تطوير الخدمات المقدمة عبر الانترنت مثل الإدارة الالكترونية ، التجارة الالكترونية و كذا البنوك الالكترونية ، فضلا عن سعي الجزائر

الحثيث إلى إرساء قاعدة قانونية لاستخدام التكنولوجيات الجديدة للإعلام و الاتصال 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، و إدراجها لآليات و ميكانيزمات جديدة تعني بهذه المسائل بالموازاة مع تطوير البنايات الأساسية المتعلقة بتكنولوجيات العالم الرقمي . و يفرض مطلب الأمن مضاعفة أنظمة الرقابة التي قد تشكل تهديدا ممكنا للحريات الفردية ، و لهذا وجب مرافقة كل المقاربات الأمنية في مجال الأمن الرقمي للأطر القانونية و التكنولوجية الملائمة، و تأخذ بعين الاعتبار دقة الهجمات الالكترونية و تعقيداتها و التي يزداد خطرها مع التطور التكنولوجي و استخداماتها اليومية.

و تجسيدا لذلك باشرت الدولة الجزائرية و في مقدمتها مؤسسة الدفاع الوطني إلى إعداد برامج خاصة لمجابهة الجريمة الالكترونية و الحد من انتشارها ، و إنشاء أجهزة جديدة تنسجم في أدوارها و تجهيزاتها مع المتغيرات الحاصلة في هذا المجال ، إذ أصبحت الحماية السيبرانية جزء مهما في أي منظومة للدفاع ، و قد استطاع الجيش الشعبي الوطني المضي قدما و مسايرة التطورات التكنولوجية و الإعلامية الحاصلة في العالم ، ومن ثمة تأمين و حماية نطاقه المعلوماتي ، و تأمين الفضاء المعلوماتي لكل الناشطين فيه. (دبارة سمر ، المجلة الجزائرية للأمن الإنساني، ص 262).

1- الهياكل المنشأة لتقصي الجريمة السيبرانية:

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

أنشئ هذا المركز في 2008، يوجد مقره ببئر مراد رايس ، أهدافه تأمين منظومة المعلومات لخدمة الأمن العمومي ، و هو بمثابة مركز توثيق ، و يقوم بتحليل المعطيات و البيانات للجرائم المعلوماتية المرتكبة ، ومحاولة تحديد هوية أصحابها ، مما يأمن الأنظمة المعلوماتية للمؤسسات و البنوك و البيوت و الشركات ... الخ ، ويعمل على التنسيق الأمني بين الأجهزة الأمنية الأخرى، و الجدير بالذكر أن المركز استطاع معالجة أزيد من 100 جريمة الكترونية سنة 2014 ، و ما يفوق 500 قضية رقمية خلال سنة 2015 ، و هذا بفضل التركيبة

البشرية المؤهلة التي اكتسبها الجهاز من التكوين المستمر و الملتقيات الوطنية و الدولية و تبادل الخبرات مع الدول الأخرى.

ب- المعهد الوطني للأدلة الجنائية و علم الإجرام :

أنشأ المعهد الوطني للأدلة الجنائية و علم الإجرام ببوشاوي التابع للقيادة العامة للدرك الوطني قسم الإعلام و الاتصال الإلكتروني ، أنشأ بموجب المرسوم الرئاسي رقم 04-183 المؤرخ في 26 يونيو 2004 وعدل نظامه الأساسي بموجب المرسوم الرئاسي رقم 09-118 المؤرخ في 14 أفريل 2004.

يتكون هذا الجهاز من "11" إحدى عشر دائرة متخصصة في عدة مجالات متباينة، تضمن جميعها الخبرة و التكوين و التعليم ، و تقديم جميع المساعدات التقنية ، تقوم دائرة الإعلام الآلي و الالكتروني المكلفة بمعالجة و تحليل و تقديم كل دليل رقمي يساعد العدالـة مع تقديم المساعدة للمحققيـن ، يتكون من عدة تجهيـزات تتمثل في محطة ترميم و تصليح الأجهزة و الحوامل المعطلة ، الشبكات الإعلامية و التجهيزات البيانية ، محطة محمولة و ثابتة لإجراء خبرات الإعلام الآلي ، و يحتوي سبع قاعات ، هي: كتب التوجيه، فصيلة الأنظمة المشحونة ، فصيلة تحليل المعطيات ، فصيلة الهواتف ، اقتناء المعطيات ، قاعة موزع و قاعات تخزين.

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

- إجراء الخبرات و الفحوص العلمية في إطار التحريات الأولية و التحقيقات القضائية و هذا بغرض إقامة الأدلة التي تسمح بالتعرف على مرتكبي الجنايات و الجنح.
- ضمان المساعدة العلمية أثناء القيام بالتحريات المعقدة باستخدام مناهج الشرطة العلمية.
- المشاركة في الدراسات و التحاليل المتعلقة بالوقاية و التقليل من كل أشكال الإجرام.

- تصميم و إنجاز بنوك المعطيات.
- المشاركة في تحديد سياسة جنائية مثلى لمكافحة الإجرام.
- المبادرة و إجراء بحوث متعلقة بالإجرام باللجوء إلى التكنولوجيات الدقيقة.
- العمل على ترقية البحوث التطبيقية و أساليب التحريات التي أثبتت فعاليتها في ميادين علمي الإجرام و الأدلة الجنائية على الصعيدين الوطني و الدولي.
- المشاركـة في كل الملتقيات و المحاضرات و الندوات على الصعيدين الوطني و الدولي لتطوير مستوى مستخدمي المعهد.
- المساهمة في تنظيم دورات الإتقان و التكوين ما بعد التدرج في تخصيص العلوم الجنائية.

ولتأدية مهامه على أكمل وجه فإن المعهد الوطني للأدلة الجنائية و علم الإجرام يحتوي على العديد من الأقسام و المصالح المختصة من أهمها:

- مصلحة البصمات: يتم على مستوى هذه المصلحة مقارنة البصمات للتعرف على الجثث و تجدر الإشارة إلى أن الدرك الجزائري مجهز بأنظمة التعرف الآلي على البصمات (THEAFIS AutomatedFingerprint Identification System.
- مصلحة الوثائق: في هذه المصلحة يتم التأكد من صحة الوثائق و الإمضاءات و التحقق من النقود و كذلك التأكد من صحة الوثائق السرية .
- مصلحة الإعلام الآلي: على مستوى هذه المصلحة يتم رصد و مراقبة و تتبع عمليـات الاختراق و القرصنة المعلوماتية و كذا اكتشاف المعلومات المسروقة و تفكيك البرامج المعلوماتية.
- مصلحة البيئة: تشرف هذه المصلحة على عمليات البحث في أسباب تلوث المياه و التربة و كذا الكشف عن المواد السامة المتواجدة في المحيط أو أماكن العمل. (بارة سمير، 2017، ص 436).

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

استجابة لمطلب الأمن المعلوماتي و محاربة التهديدات الأمنية الناجمة عن الجرائم الالكترونية قامت مصالح الأمن بإنشاء المصلحة المركزية للجريمة الالكترونية التي عملت على تكييف التشكيل الأمني لمديرية الشرطة القضائية ، و التي كانت عبارة عن فصيلة شكلت النواة الأولى لتشكيل أمني خاص لمحاربة الجريمة الالكترونية على مستوى المديرية العامة للأمن الوطني و التي أنشئت سنة 2011 ، ليتم بعدها إنشاء المصلحة المركزية لمحاربة الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال بقرار من المدير العام للأمن الوطني و أضيف للهيكل التنظيمي لمديرية الشرطة القضائية في جانفي 2015.

د- الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها:

تشكلت هذه الهيئة بمقتضى المرسوم الرئاسي رقم 15-261 و هي سلطة إدارية مستقلة لدى وزير العدل ، تعمل تحت إشراف و مراقبة لجنة مديرية يترأسها وزير العدل و تضم أساسا أعضاء من الحكومة معنيين بالموضوع و مسؤولي مصالح الأمن و قاضيين من المحكمة العليا يعينهما المجلس الأعلى للقضاء.

و تضم الهيئة قضاة و ضباط و أعوانا من الشرطة القضائية تابعين لمصالح الاستعلامات العسكرية و الدرك الوطني و الأمن الوطني وفقا لأحكام القانون الإجراءات الجزائية .

و كلفت الهيئة باقتراح عناصر الإستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها و تنشيط و تنسيق عمليات الوقاية منها ، و مساعدة السلطات القضائية و مصالح الشرطة القضائية في مجال مكافحة هذه الجرائم ، من خلال جمع المعلومات و التزويد بها و من خلال الخبرات القضائية ، و ضمان المراقبة الوقائية للاتصالات الالكترونية ، قصد الكشف عن الجرائم المتعلقة بالأعمال الإرهابية و التخريبية و المساس بأمن الدولة.

وهي سلطة إدارية تشكلت بمرسوم رئاسي رقم 15-261 تعمل تحت إشراف لجنة يديرها وزير العدل ، تضم أعضاء من الحكومة و مسؤولي مصالح الأمن و قضاة و أعوان الشرطة القضائية تابعين للاستعلامات العسكرية و الدرك الوطني و الأمن الوطني . تعمل على الكشف عن الجرائم الإرهابية الالكترونية و جرائم المساس بأمن الدولة .(يوسف بوغرارة ، مجلة الدراسات الإفريقية ، 2018، ص 112).

2- 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 ، و التخفيف من حدتها و التعافي 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 ، و تقليل المخاطر الأمنية إلى مستوى مقبول ، " و فيما يتعلق بالإستراتيجية العسكرية الفرنسية : " مجموعة الوسائل الفنية و غير 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 ، و متابعة حالة تقدم نشاطات تجسيد السياسة الشاملة للدفاع السيبراني الرامية لضمان فعالية الحماية ضد التهديدات السيبرانية التي تستهدف أنظمة المعلومات و منظومات الاتصال وكذا منظومة الأسلحة للجيش" (نوارة باشوش ، جريدة الشروق ، 2019 ص 03).

حيث أصبحت الحروب المستقبلية حروب الالكتروني ، كما أبرزت مجلة الجيش في العدد 676 لشهر نوفمبر 2019 على أهمية المركز الوطني للإشارة للجيش الوطني الشعبي (مجلة الجيش، العدد 676 لسنة 2019).

أ- الدفاع السيبراني في الجيش الوطني الشعبي :

قررت القيادة العليا للجيش الوطني إحداث "مصلحة الدفاع السيبراني و مراقبة أمن الأنظمة " على مستوى دائرة الاستعمال و التحضير لأركان الجيش الوطني الشعبي، بهدف تأمين و حماية المنظومات و المنشآت الحيوية لقواتنا المسلحة ضد التهديدات السيبرانية .

وعيا منها بالتحديات التي بات يحملها هذا الواقع الجديد و قصد الإلمام بكافة التهديدات التي يشكلها الدفاع السيبراني على الأمن و حتى على سيادة الدول و الحكومات . قامت قيادة الجيش الوطني الشعبي بوضع إستراتيجية دفاع سيبراني ، تغطي كل الجوانب التي لها صلة بتحقيق نظام دفاع سيبراني متكامل و فعال بهدف تأمين و حماية المنظومات و المنشآت الحيوية للدولة الجزائرية ، حيث تم في هذا الصدد و بتاريخ 6 نوفمبر 2015 إحداث على مستوى دائرة الاستعمال و التحضير لأركان الجيش الوطني الشعبي " مصلحة الدفاع السيبراني و مراقبة أمن الأنظمة " ، تكلف أساسا بتخطيط و إدراج و متابعة حالة تقدم نشاطات تجسيد السياسة الشاملة للدفاع السيبراني الرامية لتحقيق بفعالية الحماية ضد التهديدات السيبرانية التي تستهدف أنظمة المعلومات و منظومات الاتصال و كذا منظومات الأسلحة للجيش الوطني الشعبي .

تتمحور إستراتيجيـة الدفـاع السيبراني للجيش الوطني الشعبي حول سبعة محاور و هي :

- ✓ جانب وظيفي و تنظيمي : تكون أعمال الدفاع السيبراني ضمن الجيش الوطني الشعبي موجهة و منفذة في إطار وظيفة و/ أو تنظيمية مكرسة لضمان تجانس و فعالية هذه الأعمال .
- ✓ جانب قانوني : تحيين و تعزيز باستمرار الإطار القانوني المتعلق باستعمال تكنولوجيات الإعلام و الاتصال عموما و تأمين منظومات الإعلام خصوصا.
- ✓ جانب الموارد البشرية : تعد جاهزية مورد بشري تقني معتبر و ذوي كفاءة عالية في مجال الدفاع السيبراني هدفا أساسيا لكي تضمن نجاح إدخال هذا المجال في النشاطات العملياتية و التسيير للجيش الوطني الشعبي.

- ✓ جانب تقني : تقوية و تكييف القدرات التقنية للحماية ، الكشف و الرد على الهجمات السيبرانية باستمرار، مع ضمان يقظة دائمة فيما يخص الطرق و الوسائل المستعملة من طرف المهاجمين
- ✓ جانب الوقاية و التحسيس : الوقاية و تحسيس مستخدمي الجيش الوطني الشعبي من المخاطر و التهديدات التي تنجز عن استعمال تكنولوجيات الإعلام و الاتصال في الإطار المهني أو الشخصي بطريقة مستمرة
- ✓ جانب البحث و التطوير: تعد درجة معتبرة من الاستقلالية التكنولوجية، باستعمال وسائل تقنية خاصة أو مشخصة من طرف هياكل البحث و التطوير 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 و الوسائل التكنولوجية المتقدمة جدا

في سياق ذي صلة و تعزيزا لإستراتيجية الدفاع الوطني لمكافحة التهديدات السيبرانية، و قصد الإلمام بكافة المستجدات في هذا المجال ، و بخاصة تلك التي تعالج موضوع الأمن السيبراني و الدفاع كرهان للأمن و الدفاع الوطنيين و حماية المنشآت الحساسة ضد الهجمات السيبرانية ، تعكف مصلحة الدفاع السيبراني و مراقبة أمن الأنظمة لدائرة الاستعمال و التحضير لأركان الجيش الوطني الشعبي دوريا على تنظيم ملتقيات محاضرات و ورش عمل تطبيقية ، كان آخرها ملتقى بعنوان : " الدفاع السيبراني : مكون أساسي للأمن و الدفاع الوطني " يومي 15 و 16 ماي 2017 ، و الذي أكد من خلاله رئيس دائرة الاستعمال و التحضير 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 و الدفاع السيبرانين، ولتحسين و إثراء المعارف في مجال الوقاية و مكافحة التهديدات السيبرانية و كذا تحديد أثرها على الأمن الوطني. (مجلة الجيش ، العدد 651 لسنة 2017).

مهام مصلحة الدفاع السيبراني و مراقبة أمن الأنظمة : مصلحة الدفاع السيبراني و مراقبة أمن الأنظمة هي تركيبة ملحقة بدائرة التحضير و الاستعمال لأركان الجيش الوطني الشعبي ، فاستحداثها في نوفمبر2015 ، يندرج ضمن نهج إرساء السياسة الشاملة المسطرة من قبل القيادة العليا و الهادفة إلى حمايـة مؤسستنا ضد المخاطـر و التهديدات السيبرانية ، و باعتبارها جهازللتوجيه و الخبرة من المستوى الاستراتيجي ، تحرص هذه المصلحة أساسا على وضع و تطبيق السياسة العامة للدفاع السيبراني في الجيش الوطني الشعبي و أيضا إلى تقييم و تعزيز مستوى أمن الأنظمة المستغلة و كذا إلى تحيين و تطبيق 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 و الإعلام و الاتصال .

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

ب- الأمن و الدفاع 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 و تدعيم مراكز قوتها بطريقة تشابه الاستراتيجيات الدفاعية التقليدية ، خاصة في ظل توزع القوة السيبرانية بين عدد من الفاعلين من غير الدول و بروز التهديدات التي أصبحت تطال أمن و استقرار الدول موازاة مع تغيير منطق الحروب حاليا نحو الاتجاه اللاتماثلي.

شهد القرن الحالي ثورة منفردة في عالم تكنولوجيا الإعلام و الاتصال ، إلى الحد الذي أعدها بعض الخبراء و المختصين الميدان الخامس للنزاعات ، بعد الأرض ، البحر ، الجو و الفضاء ، و يعود ذلك إلى درجة الانتشار و التطور السريعين لهذه التقنية ، حيث يكاد لا يخلو مجال من مجالات الحياة إلا و ارتكز عليها ، و بالخصوص مع ارتباط معظم الخدمات و قواعد

البيانات و البنى التحتية و الأنظمة المالية و المصرفية بشبكة الانترنت ، و كذا اتجاه معظم الدول و الحكومات لتبني نماذج الحكومات الذكية و التحول نحو الخدمات الالكترونية التي قلصت الجهد ، الوقت و التكلفة ، و ساهمت بسرعتها و مرونتها في تلبية الاحتياجات ، و لذا 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 و السفن و سكك الحديد إلى تصادمها ، و عليه فإن خلق نظام دفاع الكتروني فعال يعمل بمثابة حائط صد للهجمات الالكترونية يعد أمرا حيويا للأمن القومي للدول.

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

طبيعة و أشكال التهديدات السيبرانية :

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

- ✓ تخريب المواقع: الهجمات التي تشوه صفحات على الانترنت 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 الانترنت.
- ✓ جمع البيانات: بمعنى أن المعلومات السرية غير المحفوظة بأمان يمكن اعتراضها و التقاطها، بل و تعديلها، مما يجعل التآمر في هذه الحالة ممكنا.

- ✓ تعطيل المعدات العسكرية : الأنشطة العسكرية التي تستعمل الحواسب و الأقمار الاصطناعية للتنسيق هي في خطر من هذا النوع من الهجمات ، حيث يمكن اعتراض الأوامر و الاتصالات أو استبدالها ، مما يعرض حياة الجنود للخطر.
- ✓ مهاجمة البنى التحتية الحساسة : شبكات الكهرباء و الماء و الوقود و الاتصالات و المواصلات كلها معرضة لحروب الانترنت ، و يمثل هذا التدمير الاقتصادي الأشد وطأة في الحالات القصوى .

و يمكن لهذه الهجمات السيبرانية ، أن تستعمل بالموازاة مع أعمال أخرى غير تقنية مثل الاستعلام و الاستغلال و التخريب .

نتيجة لهذا التطور التكنولوجي أصبحت الدول في حاجة إلى استراتيجيات جديدة لإدارة أمن الفضاء الالكتروني تنطلق من مبدأ رئيسي هو القابلية للاختراق خاصة أن الفضاء الالكتروني مجال عام لا يعترف بالحدود، و عليه فإن منطلق الأمن "السيبراني" لأي دولة يبدأ بتطوير سياسة وطنية لرفع الوعي حول قضايا الأمن "السيبراني" و الحاجة لإجراءات وطنية و إلى التعاون الدولي ، بل و يتعدى ذلك إلى تطوير مخطط وطني لتحفيز الأمن السيبراني بهدف تقليص مخاطر و أثار التهديدات السيبرانية و كذا المشاركة في الجهود الدولية و الإقليمية لتحفيز الوقاية الوطنية و التحضير و الاستجابة للتعافي من الحوادث السيبرانية ، فعلى سبيل المثال سنت الولايات المتحدة الأمريكية على مدار السنوات الخمسة الماضية فقط و لوحدها 34 قانونا و 5 أوامر تنفيذية لتحسين الأمن السيبراني.

وفقا للمؤشر العالمي للأمن السيبرانيGCI في نسخته الثانية الذي أصدرته وكالة الأمم المتحدة للإتصالات في 5 جويلية 2017 ، 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 ، و أظهرت الدراسة وجود فجوات كبيرة في الأمن السيبراني بين الدول الأكثر قوة في العالم .

يعتمد الأمن السيبراني بناء على توصيات الإتحاد الدولي للاتصالات على مزيج مركب من التحديات التقنية و السياسية ، الاجتماعية و الثقافية ، و حصر المختصون صلاحياته في :

- تطوير استراتيجية وطنية للأمن السيبراني و حماية البنية التحتية للمعلومات الحساسة .
- إنشاء تعاون وطني بين الحكومة و مجتمع صناعة الاتصالات و المعلومات.
- ردع الجريمة السيبرانية .
- خلق قدرات وطنية لإدارة حوادث الحواسب الآلية.
- تحفيز ثقافة وطنية للأمن السيبراني. (بوكبشة محمد ، مجلة الجيش ، 2017).

خاتمـــة:

لم يستطع المشرع الجزائري الإحاطة الكلية بمفاهيم حديثة كالذكاء الإصطناعي، ونظام الرقمنة على الرغم من أنه قد تم تقنين نظام التجارة الإلكترونية سنة 2018، وعصرنة قطاع العدالة، وغيرها إلا أنهذه التشريعات لا تواكب مطلقا التطور المتلاحق في تقنية الذكاء الإصطناعي ، حيث لا تزال جميع البرامج في نظر القانون وبغض النظر عن درجة تطورها مجرد أدوات لتنفيذ أوامر مستخدميها.

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

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

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

4)- لقد سن المشرع الجزائري قوانين متعلقة بالتجارة الإلكترونية بموجب القانون 18-05 المؤرخ في 10 ماي 2018 ، وكذا القانون رقم 15-05 المتعلق بعصرنة قطاع العدالة ورقمنته، أما المجال التعليمي فلا يزال قاصرا.

قائمة المراجع:

1)- آل سعود سارة، التطبيقات التربوية للذكاء الإصطناعي في الدراسات الإجتماعية، على الموقع: di.alsaud.s@gmail.com

2)- الأمر رقم 66-156 المؤرخ في 08 يونيو 1966 ، المتضمن قانون العقوبات الجزائري المعدل والمتمم.

3)- الصالحين محمد العتيبي، الجوانب القانونية لإستخدام المعلوماتية في المعاملات التجارية، مجلة الحقوق، العدد 2، السنة 37.

4)- الفرا سليمان يعقوب، الذكاء الإصطناعي على الموقع:

5)- بوحميدة نصر الله ، (2017)، مجلة الحكمة للدراسات التربوية والنفسية، المجلد 5، العدد 11.

6)- حلواجي عبد الفتاح ، (2017)، الرقمنة كمدخل لتحسين الخدمة العمومية في الجزائر، قطاعة العدالة نموذجا، مذكرة ماستير، حقوق، جامعة الوادي، الجزائر.

7)- دياب زهية ، (2019)، برويس وردة، معوقات التعليم الرقمي في المدرسة الجزائرية، المجلة العربية للآداب والدراسات الإنسانية، العدد 7، فيفري .

8)- ربيعي فايزة، (2017)، إتجاهات أساتذة التعليم العالي نحو التعليم الإلكتروني، دراسة ميدانية بجامعة باتنة، مجلة التواصل، عدد 50، شهر جوان.

9)- عزاف نصر الدين، التعليم الإلكتروني ومستقبل الإصلاحات بالجامعة الجزائرية، مجلة Rust، مج 19، ع 2، على الموقع: gheraf.nacereddine@gmail.com

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

11)- مجلة الجيش، العدد 599، جوان 2013، (www.mdn.dz).

- مجلة الجيش، العدد 657، أفريل 2018، على الموقع الرسمي لوزارة الدفاع الجزائرية (www.mdn.dz).