ISSN: 2352-9806 مجلة الحقوق والعلوم السياسية جامعة خنشلة EISSN: 2588-2309
المجلد 09/العدد 02/السنة 2022/ص ص 622-641

شرعية النص التجريمي في عدم خضوع الفعل لسبب إباحة الإلكتروني

The legality of the offence in the fact that the act is not subject to the cause of electronic permissibility

موفق نورالدين*
جامعة محمد لمين دباغين سطيف2
Nouri199191@gmail.com

تاريخ الإيداع:2022/05/12	تاريخ المراجعة:2022/09/21	تاريخ القبول:2022/09/22

ملخص:

تحكم قواعد القانون الجنائي مبدأ الشرعية في وجود نص تجريمي وعدم خضوعه لسبب من أسباب الإباحة، وفي ظل التطورات الحاصلة على الجريمة الالكترونية أصبح هناك أسباب إباحة الكترونية لا زالت تخضع للقواعد العامة، تتمحور هذا الدراسة في إبراز القواعد العامة لأسباب الإباحة وفق المادة 39 من قانون العقوبات وإسقاطها على البيئة الافتراضية.

الكلمات المفتاحية: أسباب الاباحة؛ جريمة الكترونية؛ جريمة سيبرانية؛ ردع سيبراني.

Abstract:

The rules of the Criminal Code govern the principle of legality in the existence of a criminal provision and its non-submission for a reason of permissibility, and in the light of the advances in cybercrime, there are reasons for cybercrime, still subject to general rules This study focuses on highlighting the general rules for permissibility reasons According to article 39 of the Penal Code and its drop on the virtual world.

Keywords : Reasons for permissive ;cybercrime ;electronic crime ;cybercrime deterrence.

* المُؤلِف المُراسِل.

مقدمة:

قد تبدو بعض الأفعال ظاهريا أنها فعل مجرم يستوجب العقاب، لكن لغلبة المصلحة العامة في الفعل من الناحية الإيجابية وأثره الحسن في المجتمع كان سببا كافيا لجعله مباح، وهذا ما يسمى بأسباب الإباحة، وقد يكون هذا الأمر مقبولا في البيئة التقليدية لكن ما يستوجب البحث كينونة الفعل في البيئة الافتراضية فهل يمكن اسقاط القواعد العامة التقليدية على أفعال تدخل في خانة الإباحة الكترونية، فتأخذ نظرية الاباحة نفس قواعد مبدأ الشرعية كونها جزء من قيامها سواء كانت في بيئة تقليدية أو الكترونية سيبرانية.

وأسباب الاباحة تنفي الجريمة ابتداء، كما تشمل اثارها على المسؤولية الجنائية للفاعل والشريك، أين تشمل الإباحة وعدم العقاب على كل من قام بالفعل سواء بصفته فاعلا أصليا أو شريك، كون أن أسباب الاباحة أسباب موضوعية تنصب على الفعل فتنفي عنه الجرم، ولا تنصب على الفاعل كموانع المسؤولية والعقاب.

كذلك تمتاز أسباب الإباحة بخروجها عن مسلمات قانون العقوبات الذي يعتبر أساس مبدأ الشرعية، فيجوز للقاضي اللجوء إلى أحكام الشريعة الإسلامية والعرف الذي له دور في تفسير النص التشريعي و تأثيره[1] على التجريم وقواعد العدالة كما هو معمول به في القانون المدني وفق أحكام المادة الأولى فقرة 1 و2، كونها تعيد الأمر إلى أصله " الأصل في الأفعال الاباحة"، أخرجها المشرع من قاعدة "التشريع المصدر الوحيد" كونها لا تدعو للتجريم والعقاب بل هي أسباب موضوعية تؤدي إلى البراءة، ولهذا سمح المشرع فيها اللجوء إلى القياس والتفسير الواسع واللجوء إلى أحكام الشريعة والعرف.

من خلال ما سبق نستشف أهمية هذه الأسباب في مسألة التجريم والعقاب وإخراج الفعل من دائرة التجريم إلى دائرة الاباحة لانتفاء علة التجريم وانتفاء الضرر.

وما يزيد من أهمية الموضوع أنه مع التطور التكنولوجي الحاصل وتوسع مجال استعمال وسائل الاعلام والاتصال الحديثة وارتباطها الالكتروني بالشبكات التي تربط الافراد ببعضها، ظهرت بيئة إلكترونية يمكن أن تكون مجالا خصبا للجريمة، فيعاقب أصحابها على الفعل الذين قاموا به الكترونيا، وبالتبعية تظهر أفعال لها صورة الجريمة لكن فيها مصلحة عامة،

تهدف هذا الدراسة إلى إبراز مسألة أسباب الاباحة في الفضاء الالكتروني، وتوافره في هذه البيئة و أي نص يحكم قواعده سواء الشق المتعلق بأمر و إذن القانون أو حالة الدفاع الشرعي كسبب من أسباب الاباحة.

ومن هنا يثار التساؤل في إشكالية بحثنا حول مدى توافر أسباب الاباحة في البيئة الالكترونية واتساقها مع نص المادة 39 من قانون العقوبات المكرس على البيئة التقليدية؟ ولتوضيح الإشكالية نطرح وتساؤلات فرعية منها:

- هل يسري ما أمر القانون وإذن به القانون وفق نص المادة 39 على البيئة الالكترونية؟
- هل تحكم حالة الدفاع الشرعي الالكتروني نفس الشروط المذكورة في المادة 39؟

وعلى هذا الأساس للإجابة على الإشكاليات المطروحة سنقسم بحثنا إلى مبحثين

[1] حسن إيهاب محمد، دور العرف في التجريم، المجلة المصرية للدراسات القانونية والاقتصادية، مصر، العدد 10، جانفي 2018، ص 541.

أولا: إسقاط نص المادة 39 من قانون العقوبات على ما أمروإذن به القانون على البيئة الالكترونية

ثانيا: إسقاط نص المادة 39 وشروطها على حالة الدفاع الشرعي الالكتروني

معتمدين في ذلك على المنهج الوصفي في وصف الأفعال والأوامر والمنهج التحليلي في تحليل النصوص القانونية ورؤية المشرع والفقه.

1- إسقاط نص المادة 39 من قانون العقوبات على ما أمروإذن به القانون على البيئة الالكترونية.

نصت المادة 39 من قانون العقوبات على أنه " لا جريمة إذا كان الفعل قد أمر به القانون أو اذن به القانون.....". يستخلص من هذا النص أن المشرع حدد الخانات التي يكون فيها الفعل مباحا دون تحديد أفعال على سيبل الحصر، ولو حصرها لفُقدت الحكمة من النص كون الاباحة تجيز التوسع فيها وليس حصرها كما في قواعد التجريم والعقاب، ولهذا اعطانا المشرع الخانات التي تزيل عن الفعل الصفة الاجرامية، إذا كان الأمر بإتيانه بأمر من القانون أو بإذن من القانون.

وشمول النص يجعلنا نرى إمكانية أن يكون هذا الأمر وهذا الإذن في البيئة التقليدية كما قد يكون في البيئة الالكترونية، وعليه سنقوم بالتطرق إلى ما أمر به القانون أولا، ثم ما أذن به القانون، بإسقاط هذا النص التقليدي على البيئة الالكترونية للوقوف صلاحية النص فيما يخص أسباب الاباحة الالكترونية.

1.1- الإباحة الالكترونية وفق ما أمربه القانون.

أمر القانون هنا ليس محصورا في نصوص قانون العقوبات بل تتعداه إلى قوانين أخرى، وهذا ما يميز الظرف المعفى عن الظرف المبيح، فالظرف المعفي، القانون الجنائي هو الذي يقرره، بينما الظرف المبيح يرجع الاعتداد به والترخيص فيه بالجريمة إلى إرادة قانون غير جنائي أقرها القانون الجنائي وجعل منها إرادته هو الآخر[1]

ولا يطرح اشكال في أسباب الاباحة التقليدية فيما يخص أمر القانون، فقد يأمر القانون الطبيب بتبليغ السلطات المختصة في حالة وقوفه على مرض معدي لدى أحد الأشخاص ولا يكون بهذا قد قام بجريمة افشاء الاسرار وفق احكام المادة 301 من قانون العقوبات، كون أن القانون من أمره بالإفشاء ومن غير المقبول أن يأمرك القانون بإتيان فعل ثم يعاقبك عليه[2].

لكن الاشكال يقوم حول إمكانية قيام أمر القانون في البيئة الالكترونية وبيئة الانترنت، أين يأمر القانون بالقيام بأفعال مجرمة الكترونيا لكن أمر القانون يجعل القائم بها فعله مباحا.

وقد يكون الأمر في القانون بحد ذاته كما قد يكون الأمر صادر عن سلطة أو هيئة خولها القانون إعطاء هذا الأمر، وعلى هذا الأساس سنتطرق الى الأمر الذي مصدره القانون، ثم نعرج عن الأمر الصادر عن سلطة سلمية.

1.1.1- الإباحة الالكترونية الناتجة عن أمر القانون في ذاته.

بالرجوع للدستور وقانون العقوبات نجد أن حرمة الحياة الخاصة للأفراد مصانة بما فيها سرية مراسلاتهم واتصالاتهم، سواء كانت هذه الاتصالات والمراسلات عن طريق تقليدي أو متطور بواسطة الهاتف وشبكات التواصل

[1] رمسيس بهنام، نظرية التجريم في القانون الجنائي، معيار سلطة العقاب تشريعا وتطبيقا، دار الجامعة الجديدة، مصر، دون سنة، ص 91

[2] عبد الله سليمان، شرح قانون العقوبات القسم العام، الجزء الأول، دار الهدى للطباعة والنشر، عين مليلة، الجزائر، دون سنة، ص 99

الاجتماعي والايميلات، ويعتبر اعتراضها ومراقبتها، وتفتيش وحجز تلك المراسلات والاتصالات والتقاطها جريمة يعاقب عليها القانون[1].

إلا أنه وفقا لأحكام القانون 09-04[2]، أمر القانون مقدمي خدمات الانترنت بتقديم يد المساعدة للسلطات المكلفة بالتحريات القضائية وفقا للمادة 11 و12 منه، فتنص المادة 11 على سبيل المثال " .... يلتزم مقدمو الخدمات بحفظ:

- المعطيات التي تسمح بالتعرف على مستعملي الخدمة،
- المعطيات المتعلقة بالتجهيزات الطرفية المستعملة للاتصال،
- الخصائص التقنية وكذا تاريخ ووقت ومدة كل اتصال،
- المعطيات التي تسمح بالتعرف على المرسل إليه أو المرسل إليهم الاتصال وكذا عناوين المواقع المطلع عليها...."

فيتضح من النص أن هناك اعتراض لخصوصية الحياة الخاصة للأفراد يعاقب عليها قانون العقوبات حسب عدة مواد منها المادة 303 مكرر، لكن النص اباح الفعل لمقدمي خدمة الانترنت بموجب أمر القانون، بل عاقب على عدم الالتزام، بما ورد في نص المادة 11 من ق 09-04، بعقوبة الحبس من 6 أشهر إلى 5 سنوات وبغرامة من 50.000 دج إلى 500.000 دج واعتبرها جريمة عرقلة السير الحسن للتحريات القضائية.

كما أن التقاط صور للأشخاص سواء عن طريق الصورة الثابتة أو الفيديو ممنوع ومعاقب عليه، كما أن الدخول إلى أي نظام خاص بالدولة أو منظومة معلوماتية معاقب عليه بموجب المواد 394 مكرر، إلا أن القانون أباح هذا الفعل كذلك لبعض الهيئات وفق المرسوم الرئاسي رقم 15-228 المؤرخ في 22 أوت 2015[3]، في المادة 11 منه التي تنص على أنه " يتولى أمن الولاية تسيير النظام المحلي للمراقبة بواسطة الفيديو الموضوع على مستوى الولاية.

وتطلع على هذا النظام، بقوة القانون، المصالح الإقليمية لقيادة الدرك الوطني ومديرية الأمن الداخلي ....".

يتضح من النص أن القانون أمر سلطات الدرك بالاطلاع على النظام ومراقبة الأشخاص من اجل مكافحة الجريمة فأباح لهم الفعل عن طريق هذه المادة من المرسوم.

لكن الجدير بالمناقشة هنا وفق مبدأ الشرعية أن النص الذي يجرم أو يعاقب أو يضيق من الحريات يجب أن يكون تشريعا صادرا عن البرلمان، والملاحظ أن الاباحة في المراقبة والتقاط الصور عبر الفيديو للأشخاص كانت بأمر مرسوم رئاسي وليس بأمر القانون بمفهومه الضيق – التشريع-، الشيء الذي يوحي أن المشرع انتهج في أسباب الاباحة الأخذ بالمفهوم الواسع للقانون سواء كان تشريعا أو مراسيم صادرة عن السلطة التنفيذية طالما أن الغرض منها الاباحة وليس التجريم، ومنه لا مساس بمبدأ الشرعية في هذه المسألة.

---

[1] تدخل هذه الاباحة في نطاق الاباحة الطارئة التي اجازها القانون كونها بدون النص تكون فعلا مجرما، للمزيد في مسألة الاباحة الاصلية والطارئة راجع الصديق أبو الحسن محمد، حق الدفاع الشرعي الخاص، دراسة مقارنة بالقانون الوضعي، دار التوفيق النموذجية، الطبعة الأولى، مصر، 1992، ص – ص 12، 15.

[2] قانون رقم 09-04 مؤرخ في 5 أوت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية، عدد 47، 2009

[3] مرسوم رئاسي رقم 15-228 المؤرخ في 22 أوت 2015، يحدد القواعد العامة المتعلقة بتنظيم النظام الوطني للمراقبة بواسطة الفيديو وسيره، الجريدة الرسمية، عدد 45، 2015.

2.1.1- الإباحة الالكترونية الناتجة عن أمر السلطة.

وقد تكون هذه السلطة هي السلطة السلمية للعون كما قد تكون سلطة غير خاضع لها العون كما هو الحال بأمر السلطة القضائية.

و قد جاءت أحكام المادة 119 من القانون 18-04 بهذا النوع من الأوامر في البيئة الالكترونية، التي بواسطتها تصبح الأفعال مباحة حيث تنص على أنه " يلتزم متعاملو الاتصالات الالكترونية باتخاذ التدابير التي من شأنها أن تضمن سرية المكالمات والمعلومات التي يحوزونها مشتركيهم، و ألا يسمحوا بوضع أي ترتيبات بغرض اعتراض الاتصالات أو مراقبة المكالمات الهاتفية و الوصلات و المحادثات و المبادلات الالكترونية دون إذن مسبق من السلطة القضائية وفقا للتشريع المعمول به، و يجب عليهم أن يطلعوا أعوانهم على الالتزامات التي يخضعون لها و على العقوبات التي يتعرضون لها في حال عدم احترامهم لهذه الأحكام."

كما نصت المادة 41 من القانون 18-07، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي[1]، على أنه " لا يجوز لأي شخص يعمل تحت سلطة المسؤول عن المعالجة أو سلطة المعالج من الباطن الذي يلج إلى معطيات ذات طابع شخصي، أن يعالج هذه المعطيات دون تعليمات المسؤول عن المعالجة، باستثناء حالة تنفيذ التزام قانوني".

والجدير بالملاحظة هنا ان الاستثناء الوحيد للخروج على أمر سلطة المسؤول هو تنفيذ التزام أمر به القانون ففي هذه الحالة يسمو أمر القانون على أمر السلطة، فيعتبر تنفيذ الالتزام القانوني أولى.

ونفس الشيء نستشفه في المواد 22 و23 من القانون رقم 20-05، المتعلق بالوقاية من التمييز وخطاب الكراهية ومكافحتهما[2]، التي تنص على انه " يمكن الجهات القضائية المختصة وبمناسبة التحقيق في إحدى الجرائم المنصوص عليها في هذا القانون، أن **تأمر** مقدمي الخدمات أو أي شخص أخر بتسليمها أي معلومات أو معطيات تكون مخزنة باستعمال وسائل تكنولوجيات الإعلام والاتصال، تحت طائلة العقوبات المنصوص عليها قانونا."

هنا يتضح أن القانون قد يتطلب في بعض الأحيان شكلية معينة في أمر السلطة المختصة كأن يكون كتابة كما هو الحال في المادة 109 من قانون الإجراءات الجزائية التي توجب أن يكون كتابة، وإذا لم تحترم هذه الشكلية يجوز للمرؤوس عدم تنفيذ الأمر لأنه جاء مخالف لأحكام القانون[3]، وكذا المرسوم رقم 83-373 المعدل والمتمم، المتعلق بسلطات الوالي وأوامره للضبطية القضائية في مجال الأمن و الحفاظ على النظام العام[4]، في مادته 16 التي تنص " يخول الوالي في حالة وقوع حدث خطير أن يسعى إلى تدخل وحدات الأمن الوطني المتخصصة، بعد إعلام مكتب التنسيق الموسع إلى النائب العام.

ويتم تدخل هذه الوحدات بناء على تعليمات مكتوبة ويعلم وزير الداخلية بذلك فورا..."

[1] قانون رقم 18-07 مؤرخ في 10 جوان 2018، يتعلق بحماية المعطيات ذات الطابع الشخصي، الجريدة الرسمية، عدد 34، 2018.

[2] قانون رقم 20-05 مؤرخ في 28 أفريل 2020، يتعلق بالوقاية من التمييز وخطاب الكراهية ومكافحتهما، الجريدة الرسمية، عدد 25، 2020.

[3] عبد الله سليمان، مرجع سابق، ص 123

[4] مرسوم رقم 83-373 مؤرخ في 28 ماي 1983، يحدد سلطات الوالي في ميدان الأمن والمحافظة على النظام العام، الجريدة الرسمية، عدد 22، 1983.

وهو ما نستنتجه في المواد 22 و23 السابقة أنه حتى في أمر السلطة الخاص بالتحقيقات الالكترونية يجب أن يكون الأمر كتابيا لمقدم الخدمات، فالشكلية التي تطلبها القانون تكون أولى بالاحترام من أمر السلطة، وإذا طبقها المرؤوس رغم عدم احترامها للقانون تطاله المسؤولية عن فعله.

2.1- الإباحة الالكترونية وفق ما أذن به القانون.

وهو السماح قانونا بإتيان فعل معين ليصبح مباحا وفي غياب هذا السماح القانوني نكون أمام جريمة، لكن ليس هناك إجبار على إتيان المسموح تحت طائلة العقوبات.

وهذا هو الفرق بين ما أمر به القانون وما أذن به القانون، فالأمر وجب تنفيذه تحت طائلة العقوبات القانونية كون رفض تنفيذه يعتبر جريمة يعاقب عليها، أما إذن القانون فهو رخصة تجيز للشخص أن يقوم بالفعل أو تركه على سبيل الاختيار منه وليس على سبيل الإجبار.

وقد يكون الإذن صادر من القانون، وقد يكون القانون خول سلطة تقديرية لأحد الأشخاص بأن يقوم هو بالإذن لمن هم تحت إمرته، وهذا ما سيتم التطرق إليه كما يلي:

1.2.1- الإباحة الالكترونية الناتجة عن إذن القانون في ذاته

وهي الرخصة التي يمنحها القانون لشخص دون غيره للقيام بفعل معين، كما هو الحال في المادة 70 من القانون 18-04 المحدد للقواعد العامة المتعلقة بالبريد والاتصالات الالكترونية[1]، بقولها " **يرخص** لبريد الجزائر فقط، وبقوة القانون، إقامة صناديق الرسائل في الطريق العمومي لجمع البريد.".

لكن الملاحظ هنا أن المشرع أذن لبريد الجزائر بجمع الرسائل التقليدية دون الرسائل في الفضاء الرقمي ولخطورة هذا الفعل ومساسه بالحريات حصره المشرع في اختصاصات الضبطية القضائية أو السلطات القضائية.

كما نجد أن المشرع جعل من معالجة المعطيات الشخصية للأفراد ممنوعة تحت طائلة التجريم إلا بموافقة صريحة من الشخص المعني، إلا أنه أعطى رخصة في حالات للمسؤول عن المعالجة الالكترونية، بمعالجة تلك المعطيات دون موافقة صاحب الشأن وهذا ما جاءت به المادة 07 من القانون 18-07، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، " ... غير أن موافقة الشخص المعني لا تكون واجبة، إذا كانت المعالجة ضرورية:

- لاحترام التزام قانوني يخضع له الشخص المعني أو المسؤول عن المعالجة
- لحماية الشخص المعني
- لتنفيذ عقد يكون الشخص المعني طرفا فيه أو لتنفيذ إجراءات سابقة للعقد اتخذت بناء على طلبه
- للحفاظ على المصالح الحيوية للشخص المعني، إذا كان من الناحية البدنية أو القانونية غير قادر على التعبير عن رضاه
- لتنفيذ مهمة تدخل ضمن مهام الصالح العام أو ضمن ممارسة مهام السلطة العمومية التي يتولاها المسؤول عن المعالجة أو الغير الذي يتم اطلاعه على المعطيات

[1] قانون رقم 18-04 مؤرخ في 10 ماي 2018، يحدد القواعد العامة المتعلقة بالبريد والاتصالات الالكترونية، الجريد الرسمية، عدد 27، 2018.

- لتحقيق مصلحة مشروعة من قبل المسؤول عن المعالجة أو المرسل إليه مع مراعاة مصلحة الشخص المعني و/ أو حقوقه وحرياته الاساسية"

كما اذن القانون بالمراقبة الالكترونية، التي فيها مساس بالحريات في بعض الحالات وهو ما جاءت به المادة 04 من القانون 09-04 تحت عنوان " الحالات التي تسمح باللجوء إلى المراقبة الالكترونية"، فعلى هذا الأساس رخص القانون وأعطى إذن للقيام بالمراقبة الالكترونية إذا كان الغرض منها:

- الوقاية من الأفعال الإرهابية والجرائم التي تمس بأمن الدولة
- حالة احتمال اعتداء على منظومة معلوماتية تهدد النظام العام والأمن السيبراني الجزائري.
- لمقتضيات التحريات والتحقيقات القضائية، ولا يكون هذا مرخصا إلا إذا كان المبرر للقيام بالمراقبة الالكترونية قائم على مسببات صعوبة الوصول إلى نتيجة في التحقيق دون اللجوء إلى هذا النوع من المراقبة
- في إطار التعاون القضائي الدولي المتبادل وفقا لمبدأ المعاملة المثل.

و رغم أن القانون ربط القيام بالمراقبة الالكترونية بإذن مكتوب من السلطة القضائية، إلا أن هذه الرخصة لا تجعل من الإذن هنا يدخل في خانة في اذن السلطة التقديرية للموظف بل تبقى في خانة الاذن الصادر من القانون في ذاته كون أن القانون حصر الحالات التي يسمح فيها باللجوء بالمراقبة القانونية على سبيل الحصر و لم يعط للسلطة القضائية سلطة تقديرية مفتوحة في اختيار الحالات، و هذا ما يجسد أن القانون كرس الاذن المكتوب الصادر عن السلطة القضائية ليكون ضمانة قضائية و قانونية لعدم المساس بالحريات إلا في حدود ما سطره القانون، و لتبسط رقابتها على العمل الرقابي الالكتروني.

وكحوصلة يمكن القول إن القانون خول لبعض الهيئات ورخص لها إتيان بعض الأفعال تعتبر دون تلك الرخصة القانونية مجرمة، في حالات حددها على سبيل الحصر حتى لا يكون هناك مساس بالحقوق والحريات الأساسية إلا وفقا لما سطره القانون من جهة، ومن جهة تكون الرخصة خدمة للمصلحة العامة.

لكن ما يثير التساؤل هل إذن القانون يكون محصورا دائما في هيئة أو سلطة لموظف أم يمكن في بعض الحالات أن تكون الرخصة للأفراد على هيئة واشخاص طبيعية ومعنوية؟

فكما أجابتنا المادة 61 من قانون الإجراءات الجزائية عن الاذن الخاص بالأشخاص في البيئة التقليدية، أجابتنا المادة 16 من قانون 04-08 المتعلق بممارسة الأنشطة التجارية[1]، على البيئة الالكترونية بأنه " يجوز لكل شخص يهمه الأمر، وعلى نفقته الحصول من المركز الوطني للسجل التجاري على كل معلومة تتعلق بشخص طبيعي أو اعتباري مسجل في السجل التجاري"، خاصة وأن التسجيل في السجل التجاري كل معطياته أصبحت رقمية.

ومن هنا يتبين أن الإذن غير محصور على السلطات او الهيئات فقط، ويمكن للفرد الاطلاع على معلومات سرية خاصة، مثل السجل التجاري، سواء في صيغته الورقية أو في البوابة الالكترونية التي استحدثها القانون والتي بواسطتها يمكن الاطلاع على المعلومات الخاصة بالتجار الكترونيا دون أن يعتبر هذا جريمة الاطلاع على معلومات خاصة وسرية.

[1] قانون رقم 04-08، يتعلق بشروط ممارسة الأنشطة التجارية، معدل ومتمم بالقانون 18-08، المؤرخ في 10 جوان 2018، الجريدة الرسمية، عدد 35، 2018.

2.2.1- الإباحة الالكترونية الناتجة عن إذن من السلطة:

إن التفتيش مجرم قانونا دون إذن القانون سواء في البيئة التقليدية، لكن يلاحظ أن المشرع الجزائري جعل مسألة التفتيش في البيئة الالكترونية خاضع لأحكام أخرى، بما أنه جعله على سبيل الجواز، مما يدخله في دائرة الإذن القانوني وليس الأمر، فحسب المادة 05 من القانون 09-04 " يجوز للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية في إطار قانون الإجراءات الجزائية وفي الحالات المنصوص عليها في المادة 4 أعلاه الدخول بغرض التفتيش، ولو عن بعد إلى:

أ- منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها.

ب- منظومة تخزين معلوماتية "

وهنا يتضح أمرين الأول أن القانون أذن بالتفتيش لضباط الشرطة القضائية و السلطات القضائية بناء على السلطة التقديرية لها و اختيار ما تراه مناسب و تقرر مثلا أن يكون التفتيش في عين المكان أو عن بعد خدمة لحسن سير العدالة و ليس لأغراض شخصية تحت طائلة العقوبة، أما الأمر الثاني هو أن إذن القانون شمل كل من السلطات القضائية وضباط الشرطة القضائية و منه لا يحتاج ضباط الشرطة إلى إذن من وكيل الجمهورية للقيام بالتفتيش المنصوص عليه في هذا النص، كون أن المادة 45 من قانون الإجراءات الجزائية استثنت الجرائم الكترونية من تطبيق القواعد العامة عليها.

وتجدر الإشارة كذلك أنه طالما احالتنا هذه المادة على القواعد العامة للإجراءات الجزائية في التفتيش، وبما أننا في جريمة معالجة آلية للمعطيات فإنه يجوز التفتيش في أي ساعة من ليل أو نهار وفي أي مكان سكني أو غيره بإذن من وكيل الجمهورية المختص حسب المادة 46 من قانون الإجراءات الجزائية.

كما نجد أن المادة 26 و27 من قانون 20-05 جاءت بأحكام الإذن الصادر من السلطة، فقد نصت المادة 26 على أنه " مع مراعاة أحكام قانون الإجراءات الجزائية، يمكن وكيل الجمهورية أو قاضي التحقيق بعد إخطار وكيل الجمهورية، أن **يأذن** تحت رقابته، لضباط الشرطة القضائية، بالتسرب الالكتروني إلى منظومة معلوماتية أو نظام للاتصالات الالكترونية أو أكثر، قصد مراقبة الأشخاص المشتبه في ارتكابهم لأي جريمة من الجرائم المنصوص عليها في هذا القانون وذلك بإيهامهم أنه فاعل معهم أو شريك ..."

والاذن عكس الأمر لا يحمي صاحبه إذا كان الأمر مجرما قانونا وهذا ما اشارت اليه المادة 26، فحتى وأن ضابط الشرطة تحصل على إذن للتسرب الالكتروني فهذا الأمر لا يخوله أن يتعداه إلى أفعال مجرمة أخرى كتحريض المشتبه فيهم بارتكاب جريمة من أجل حصوله على الدليل فهنا يعاقب على جريمة التحريض، أو كان قصد الضابط لا يرمي إلى مراقبة الأشخاص بل للتجسس أو أغراض شخصية.

فهنا هذا التعدي يرتب آثار قانونية على عمل الضابط أين تعتبر إجراءات التسرب الإلكتروني التي قام بها باطلة، وهي ضمانة قانونية من ضمانات الحقوق والحريات كي لا يستند الدليل إلى إجراءات مشوبة باللاشرعية وأن الحصول عليها فيه شبهة الطرق الملتوية

أما المادة 27 فقد نصت على التحديد الجغرافي بوسائل الكترونية ماسة بذلك الحق الدستوري في حرية تنقل الافراد دون رقابة عليهم بقولها " يمكن وكيل الجمهورية أو قاضي التحقيق بعد إخطار وكيل الجمهورية، أن يأذن تحت رقابته، لضباط الشرطة القضائية، متى توفرت دواع ترجح ارتكاب جريمة من الجرائم المنصوص عليها في هذا القانون، بتحديد الموقع الجغرافي للشخص المشتبه فيه أو المتهم أو وسيلة ارتكاب الجريمة أو أي شيء آخر له صلة بالجريمة و ذلك باستعمال أي وسيلة من وسائل تكنولوجيات الاعلام و الاتصال، أو بوضع ترتيبات تقنية معدة خصيصا لهذا الغرض"

وهنا يتضح جليا من عبارة " متى توافرت دواع " السلطة التقديرية للقاضي ولوكيل الجمهورية بإصدار الإذن وفق سلطته التقديرية بمجرد توفر دواع حتى لو لم تكن مؤكدة، ويتسع الاذن ليشمل الأشخاص المشتبه فيهم وحتى المركبات المستعملة أو تتبع هواتفهم النقالة عن طريق GPS، أو حواسيبهم عن طريق بروتوكول IPأو بروتوكول MAC.

ونفس الشيء جاءت به أحكام المادة 15 من قانون 20-15 المتعلق بالوقاية من جرائم اختطاف الأشخاص ومكافحتها[1]

3.1- الإباحة الالكترونية الناتجة عن ممارسة أحد الحقوق المقررة

وهو ما يدخل في نطاقه حق التأديب وحق ممارسة الأعمال الطبية وحق ممارسة الرياضة، والحق المقرر هنا وفق القانون بمفهوم عبارة القانون كل القواعد القانونية بما فيها العرف والشريعة الإسلامية والقياس وليس قانون العقوبات فقط، وقد اجمع الفقه التقليدي على أسباب الاباحة في التأديب والاعمال الطبية وممارسة الرياضة، لكن ما نريد تسليط الضوء عليه هل يمكن تصور هذا في مجال أسباب الاباحة الالكترونية؟

وعلى هذا سيتم اسقاط ما هو معمول به في الاباحة التقليدية على الاباحة الالكترونية للخروج بنتيجة عما إذا كان يمكن العمل بالحقوق المقررة في إذن القانون على الاباحة الالكترونية أم لا.

1.3.1 حق التأديب

يتفق الفقه أن حق التأديب المقرر للأب لتأديب أولاده أو ضرب الزوج لزوجه ضربا غير مبرح، يدخل ضمن أسباب الاباحة، رغم أن القانون الجزائري لم يجب على هذه المسألة بل جعل من ضرب الزوج لزوجه جريمة وفقا لنص المادة 266 مكرر من قانون العقوبات، ونفس الشيء بالنسبة إلى ضرب الأطفال فهو معاقب عليه بموجب القانون[2].

إلا أن التأديب لا يكون بالضرب فقط فقد يكون بأساليب أخرى، ويجب أن يكون الغرض من الضرب والمراقبة هو التأديب وهذا ما قرر الفقه أنه يدخل في أسباب الاباحة التقليدية.

أما في البيئة الالكترونية فيمكن أن نستشف أن مراقبة الزوجة والأبناء بغرض التأديب والتربية وارد وفق ما نستشفه من المادة 06 من القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، التي استثنت من مجال تطبيق هذا القانون المعالجة من طرف شخص طبيعي لغايات لا تتجاوز الاستعمال الشخصي أو العائلي، وبشرط عدم احالتها للغير أو نشرها.

[1] قانون رقم 20-15 مؤرخ في 30 ديسمبر 2020، يتعلق بالوقاية من جرائم اختطاف الأشخاص وحمايتها، الجريدة الرسمية، عدد 81، 2020

[2] القانون رقم 15-12 المؤرخ في 15 جويلية 2015، المتعلق بحماية الطفل

فمن خلال هذا نستنتج أن الأب الذي يقوم بمعالجة ومراقبة المعطيات الشخصية الخاصة بأبنائه، التي يتداولونها في البيئة الالكترونية والانترنت، لا يكون فعله جريمة بل يدخل ضمن نطاق أسباب الاباحة الالكترونية طالما أن الغاية منها هو التأديب، وما يعزز هذا هو قيام مصالح اتصالات الجزائر بإنتاج تطبيق الكتروني يمكّن الأولياء من تأديب أطفالهم. البرنامج الذي أُطلق عليه اسم "**في أمان**"، لمراقبة استخدام الأطفال والمراهقين للإنترنت، جاء استجابة لحاجة عبّر عنها الكثير من الأولياء، الذين باتوا يخشون تأثير هذه الوسيلة الاتصالية على أبنائهم، لاسيما في ظل الأوضاع التي تعيشها المنطقة. فهذه الخدمة الجديدة، تهدف إلى "الحماية" وليس الرقابة بمفهومها الضيق[1].

2.3.1 حق مباشرة الاعمال الطبية:

يعترف القانون بالطب ويخرج الجروح التي تكون بصدده من دائرة التجريم لما فيها من مصلحة، وهذا الاعتراف يشمل حتى الوسائل المستعملة في العلاج.

ونرى أن شرط الاختصاص في مهنة الطب عن طريق شهادة معترف بها من جامعة، وموافقة المريض لخضوعه للعلاج للتنصل الطبيب من مسؤوليته[2] وغاية العلاج، تشترك في الاباحة سواء كانت تقليدية أو الالكترونية إلا ان الاختلاف يمكن في الوسيلة المستعملة.

فقد يكون وفق التطورات التكنولوجية الحاصلة أن يستعمل الطبيب وسائل متطورة عن بعد، فيجري عملية جراحية بالطريقة الالكترونية عن بعد عن طريق تطبيق " زووم" مثلا والتحكم الالي عن بعد في الأجهزة، فهذه الوسائل الالكترونية لا تخرج الفعل من دائرة الاباحة الى التجريم بل تبقى في إطار الاباحة الالكترونية للوسيلة طالما الغرض هو التطبيب.

3.1.1 ممارسة الألعاب الرياضية:

ليس هناك خلاف أن القانون يأذن بممارسة الرياضة حتى وإن كانت قتالية وفيها ضرر بالسلامة الجسدية في حدود قوانين اللعبة وإلا خرج عن نطاق الإباحة.

ونجد أن الأمر نفسه في الاباحة الالكترونية رغم اختلاف الساحة الواقعية والافتراضية، فنجد أن المشرع يبيح الألعاب الالكترونية حتى لو كانت فيها عنف افتراضي يمكن أن يؤثر على الجانب النفسي للأفراد، إلا أنه إذا تجاوزت الحدود وقوانين اللعبة فتخرج من نطاق الاباحة إلى نطاق التجريم، كمن يلعب لعبة الكترونية مع أشخاص يحرضونه فيها بالانتحار مثلا أو السرقة وغيرها كما هو الحال في لعبة " الحوت الأزرق".

ويبقى الاشكال هنا في قيام المسؤولية الجنائية على صاحب اللعبة في حال كان وضع بند في تعليمات وقوانين اللعبة ينفي عنه المسؤولية الجنائية، ناهيك عن صعوبة الوصول اليه.

---

[1] جزايرس : اتصالات الجزائر تطلق "في أمان "لمراقبة استخدام الأطفال للإنترنت(djazairess.com) اطلع عليه يوم 29 أفريل 2022، الساعة 15:12

[2] قد تسقط المسؤولية الجنائية للطبيب، لكن لا تسقط المسؤولية المدنية عنه إذا لم يخطر المريض عن خطورة العملية حتى ولو وقع على وثيقة اجراء العملية وكانت تتضمن عبارة " يتحمل المريض النتائج السلبية للعملية " وهذا ما ذهبت اليه المحكمة العليا في قرارها للملف رقم 1193813 المؤرخ في 21 جوان 2018، مجلة المحكمة العليا، العدد الثاني، 2018، ص 44

ونخلص في نهاية الدراسة أن أمر القانون وإذن القانون كأسباب إباحة المذكور في نص المادة 39 ليس محصورا على أسباب الاباحة التقليدية، بل يمكن إعمال النص التقليدي " نص المادة 39 من قانون العقوبات" على أسباب الاباحة الالكترونية دون إي إشكالات.

ولعل الاشكال يقوم في الشق المتعلق بالدفاع الشرعي المنصوص عليه في المادة 39 من ق ع، فهل يمكن أن نطبق نفس الاحكام والشروط المطلوبة في الدفاع الشرعي التي تحكم البيئة الواقعية، على البيئة الافتراضية والقول إن هناك دفاع شرعي الكتروني كون أنه يصعب تطبيق كل الشروط على الدفاع الشرعي الالكتروني، هذا ما سيتم التطرق اليه في المحور الثاني.

2- إسقاط نص المادة 39 وشروطها على حالة الدفاع الشرعي الالكتروني.

نصت المادة 39 من قانون العقوبات حالة الدفاع الشرعي وبين نطاقها أنها تنصب على جرائم النفس والمال ونفس الغير ومال الغير دون حصر، كما لم يحصر الدفاع الشرعي في الجرائم العمدية فقط دون الجرائم غير العمدية[1].

وقد أجمع الفقه الجنائي أنه لقيام حالة الدفاع الشرعي يجب توافر شروط تنصب على فعل الاعتداء وشروط تنصب على فعل رد الاعتداء، التي تكون في ساحة الاعتداء وتبرر الضرورة الحالة لرد الاعتداء والخطر الحال.

ولا نقوم بدراسة شروط حالة الدفاع الشرعي في هذه الدراسة بل سيتم دراسة مدى توافر حالة الدفاع الشرعي في البيئة الالكترونية، على ضوء الشروط المطلوبة في الدفاع الشرعي التقليدي.

بما أن خصوصية الجريمة الالكترونية هي جريمة عابرة للحدود الوطنية فإن دفاعها الشرعي إذا ثبت سيكون دفاعا فيه تعدي للحدود، ويكون دفاع على المستوى الدولي سواء كان فيه مساس بالمصالح الأساسية للدول أو الافراد.

وعلى هذا الأساس سيتم التطرق إلى الدفاع الشرعي الالكتروني على ضوء الشروط الموضوعية التقليدية أولا، ثم يتم التطرق إلى حالة الدفاع الشرعي الالكتروني الدولي.

1.2- الدفاع الشرعي الالكتروني وفق الشروط الموضوعية التقليدية.

للوصول إلى معرفة توفر حالة الدفاع الشرعي الالكتروني استوجب اخضاعها للشروط التي يتطلبها القانون وفق النص التقليدي " المادة 39 من ق ع " لقيام حالة الدفاع المشروع وعلى هذا الأساس سيتم اسقاط هذه الشروط على الدفاعي الشرعي الالكتروني كما يلي:

1.1.2- الشروط الواجبة في فعل الاعتداء:

1.1.1.2 أن يكون الاعتداء والخطر حالا: وهو ما عبرت عنه المادة 39 فقرة 2 بالضرورة الحالة[2]، ويستوي في ذلك أن يكون الخطر ناجم عن فرد أو مجموعة من الأفراد.

---

[1] كمال بلارو، أحكام الدفاع الشرعي في التشريع الجزائري، مجلة العلوم الإنسانية، قسنطينة، الجزائر، العدد 49، مجلد ب، جوان 2018، ص 10.

[2] لا يقصد بالضرورة الحالة المذكورة في النص حالة الضرورة التي تعتبر مانع من موانع المسؤولية و ليس سبب من أسباب الاباحة، والذي يختلف عن حالة الدفاع الشرعي، ففي حالة الدفاع الشرعي استوجب الوقوف على أن يكون الخطر ناجم عن لفعل غير مشروع، لكن حالة الضرورة لا تشترط هذا لقيامها فناك فرق بين الدفاع الشرعي و حالة الضرورة راجع في هذا: ناصر بن محمد الجوفان، الدفاع الشرعي، دراسة مقارنة، مجلة العدل، العدد 58، السنة الخامسة عشرة، ربيع الثاني 1434 هـ ، ص 13

والمشرع الجزائري وسع من نطاق الدفاع الشرعي، في أن يكون الخطر حالا بل اعتمد كذلك على الخطر المستمر، الذي يأخذ وقتا في التحضير والتخطيط واعتد بالدفاع الشرعي فيه فقد جاءت المادة 22 من الأمر رقم 95- 24 المتعلق بحماية الأملاك العمومية وأمن الأشخاص فيها[1]، بقولها " يستفيد المستخدمون المكلفون بأمن المؤسسة، حال تعرضها للعدوان، من قرينة الدفاع الشرعي عن كل الأفعال التي يقومون بها العدوان.

ويمكنهم في هذه الحالة أن يسلموا الأشخاص المعتدين أو المشتبه فيهم لارتكابهم جرائم أو تعد أو التحضير لها أو تنفيذها أو تقديم أي مساعدة مهما كان شكلها داخل المحيط الأمني للمؤسسة فورا إلى مصالح الأمن المختصة إقليميا".

فيفهم من هذا النص أن الخطر يكون حالا كقاعدة عامة وقد يكون حلول الخطر بالتحضير له ففي هذه الحالة أعطاه المشرع حكم الخطر الحال لما فيه من تهديد للممتلكات وأمن الأشخاص.

وحسن فعل المشرع الجزائري في هذا خاصة في الجرائم الإرهابية، التي غيرت من السياسة الجنائية والمفاهيم التقليدية التي تحكم قواعد الدفاع الشرعي.

وبالرجوع للنص نجدها استعمل عبارة " مهما كان شكلها" بما يوحي عدم حصر الخطر و رد الاعتداء عليه، فهذه العمومية تسمح أن تدخل في نطاقها الخطر الإلكتروني الذي يهدد المؤسسات و أمنها المعلوماتي، و يجوز رد الاعتداء بالتصدي له و كسر التحضير له بنفس الطريق، مما يوحي أنه يمكن العمل بالدفاع الشرعي الالكتروني في هذه الحالة و اعتبار الخطر الالكتروني وارد.

وتجدر الإشارة أن الخطر قد يكون من فعل إيجابي أو سلبي، وإن كان نادرا لكن يمكن تصوره في الدفاع الالكتروني وارغام الممتنع عن القيام بالفعل، فقد أعطت المادة 15 من القانون 20-15 للسلطات القضائية الحق في ارغام مقدمي الخدمات الذين يمتنعون عن القيام بعمل بإتيانه، ويعتبر هذا صورة من صورة الدفاع الشرعي الناتج عن فعل سلبي.

2.1.1.2 أن يكون الخطر غير مشروع: وهنا يخرج من نطاق تطبيق حالة الدفاع الشرعي أن يكون الخطر مشروعا بما أمر به أو أذن به القانون أو كان من الحقوق المقررة وهنا كذلك يمكن تصور الدفاع الشرعي الالكتروني فمن يقوم بمراقبة أطفاله الكترونيا يكون فعله مشروعا لا يستوجب دفاعا مشروعا كما سبق ذكره.

3.1.1.2 أن يهدد الخطر النفس والمال: وتهديد النفس يشمل جميع الجرائم المنصوص عليها في قانون العقوبات التي فيها مساس بالسلامة الجسدية أو النفسية للأقراد دون حصر، كذلك الجرائم المنصبة على الأموال غير محصورة في جرائم معينة[2].

وقد يسهل الأمر في الدفاع الشرعي الالكتروني على الجرائم التي تمس النفس لكن يصعب الأمر في الجرائم التي تمس المال كون أن مسرح الجريمة يختلف ومنه تختلف النظرة من البيئة التقليدية عن البيئة الالكترونية.

ففي جريمة السرقة مثلا الاعتداء وسلب الأموال بنيه تملكها يخول الدفاع الشرعي كون أن المعتدي سلب المعتدى عليه من ماله، أما في البيئة الالكترونية فمفهوم المال يثير اشكالا فسرقة مصنف أدبي أو كتب الكترونيا لا يجعل المال في

[1] أمر رقم 95-24 مؤرخ في 25 سبتمبر 1995، يتعلق بحماية الأملاك العمومية وأمن الأشخاص فيها، الجريدة الرسمية، عدد 55، 1995

[2] اعتد المشرع كذلك بالدفاع المشروع على ممتلكات المؤسسات العمومية والخاصة، وعرف الأملاك العمومية بأنها " يقصد بالأملاك العمومية في مفهوم هذا الأمر، المنشآت الأساسية والتركيبات والمنشآت الكبرى والوسائل، والممتلكات العمومية المنقولة والعقارية التي تستغل في الأنشطة الإدارية والاقتصادية والاجتماعية والثقافية و التربوية و الرياضية و الدينية" أمر 95-24.

حوزة المعتدي كلية بل يبقى في حوزة المعتدى عليه ماله، أي أن المعتدي يسرق نسخة وتبقى نسخة أخرى لدى المعتدى عليه، مما يجعل الفعل ليس سرقة بل جريمة تقليد، مما يصعب القول بحالة الدفاع الشرعي في هذه الحالة بل القول بجريمة التقليد بمفهومها للجنائي أصلا.

لهذا ذهبت المحكمة العليا في قرارها رقم 368024 المؤرخ في 2007/11/28، بأن القاضي المدني هو المختص نوعيا لتعويض الضرر الناجم عن جريمة تقليد مصنف أدبي أو فني[1].

2.2- الشروط الواجبة في رد الاعتداء

إذا توافرت الشروط السابقة في فعل الاعتداء ووجد المعتدى عليه نفسه أمام خطر قائم له الحق في رد الاعتداء.

وهنا نلاحظ أن رد الاعتداء في الدفاع الشرعي التقليدي مبني على استعمال القوة اللازمة لصد العدوان، في الحدود المناسبة لرد الخطر دون تجاوزه ليصبح انتقاما، ما يبين أن شروط رد العدوان هي اللزوم والتناسب.

لكن رد الاعتداء في البيئة الالكترونية ليس مبني على القوة البدنية، بل على القوة الفكرية والذهنية والتي قد تتجاوز قوة المعتدي، ومنه نحاول معرفة مدى استعمال اللزوم والتناسب في رد الاعتداء الالكتروني

1.2.2 اللزوم: والذي يعني أن فعل رد الاعتداء والدفاع يكون لازما وليس أمام المعتدى عليه من وسيلة أخرى لرد الاعتداء وإتيان فعل مجرم، فمن هم شخص لضربه بعصا وكان في مقدوره نزع العصا له، لا يجوز رد الاعتداء بالضرب.

وهذا ما يجعل اللزوم في الاعتداء الالكتروني الحال قد يكون في حال تعرض شخص لقذف أو سب عن طريق وسائل التواصل الاجتماعي فيكون رد الاعتداء بحظر الشخص مثلا " BLOQUE" أو " SIGNALE" لصفحة الشخص، فيعتبر هذا من قبيل رد الاعتداء الالكتروني، ولا يوجب سبه وقذفه فهذا ليس من قبيل اللزوم في رد الاعتداء، كما قد يكون رد الاعتداء بالمنع في حالة التعدي على نظام، كما نصت عليه المادة 05 من المرسوم التنفيذي رقم 18-63، حيث تمنع من استخدام النظام المعلوماتي لإدارة الجمارك بصفة مؤقتة في حال وجود تعدي على النظام او ارتكاب جرائم في هذا الشأن[2]

مع الاخذ في الاعتبار دائما أنه إذا كان أمام المعتدى عليه في البيئة الالكترونية متسع من الوقت لتبليغ السلطات، تسقط حالة اللزوم، فمن يهدد شخص عبر الانترنت بالقتل أو التشهير، لا يجوز له قتله والاحتجاج بحالة الدفاع الشرعي.

2.2.2 التناسب: وهو شرط نصت عليه المادة 39 الفقرة 2، وهو أن يلجأ المدافع إلى فعل يكفيه درء الخطر الحال به وحسب دون مبالغة والا خرج عن نطاق الدفاع الشرعي، فكما سبق و أشرنا في المثال السابق من يتعرض لسب و قذف في صفحة في الانترنت يكون رده متناسب مع رد الاعتداء بحظر الصفحة مثلا، و ليس القيام باختراق حاسوب الشخص و صفحته و اتلاف حاسوبه، فهنا نكون امام انتقام و تجاوز لحدود التناسب.

[1] قرار ملف رقم 368024 مؤرخ في 28 نوفمبر 2007، مجلة المحكمة العليا، العدد الأول، 2009، ص 349

[2] مرسوم تنفيذي رقم 18-63 مؤرخ في 13 فيفري 2018، يتعلق باستخدام المتعاملين للنظام المعلوماتي لإدارة الجمارك، الجريدة الرسمية، عدد 10، 2018.

كما يمكن أن يكون رد الاعتداء بالطريقة المناسبة وباللزوم القانوني بطلب من الجهات القضائية المختصة إجراءات تحفظية استعجالية لوضع حد لهذا التعدي أو للحصول على تعويض حسب ما جاءت به أحكام المادة 52 من القانون 07-18.

3.2.2 حالة الدفاع الشرعي الجماعي " المنظم":

غالبا ما نتحدث عن الدفاع الشرعي بحاله المنفرد، أين يكون معتدي ضد معتدى عليه أو عدة معتدين على معتدى عليه واحد، وقد يكون المنظمين إلى المعتدى عليه أناس لا يعرفهم فيأخذون حكم الدفاع الشرعي، لكن هل يمكن تصور أن تتشكل مجموعات منظمة قانونا لرد الاعتداءات وتستفيد من حالة الدفاع الشرعي؟ خاصة بظهور جرائم الإرهاب وجرائم العصابات.

وهذا ما استحدثه المشرع الجزائري سنة 1997 بظهور الإرهاب واستفحاله عن طريق المرسوم التنفيذي رقم 97-04 الذي يحدد شروط ممارسة عمل الدفاع المشروع في إطار منظم[1]، فأعطى من خلال المادة 04 منه أمكانية تأسيس مجموعات للدفاع المشروع في إطار الدفاع المشروع المنظم، التي تكون من السكان والمواطنين على سبيل التطوع وليس بأجر، ويحصلون على رخصة من الوالي لإنشاء مجموعة للدفاع المشروع.

وبذلك يخضع الدفاع الشرعي الفردي لأحكام المواد 39 و40 من قانون العقوبات فقط، بينما يخضع الدفاع الشرعي الجماعي بالإضافة للقواعد العامة لأحكام هذا المرسوم.

ويكون عمل هذه المجموعة في إطار الدفاع الشرعي الاستباقي الذي يستهدف الوقاية والتدابير الأمنية، كما قد يكون في حالة الخطر الحال استعمال الرد والتصدي بالقوة واستعمال السلاح وفقا لأحكام المادة 09 من المرسوم.

وهذا ما نحث المشرع الجزائر تقنينه في القانون الخاص بجرائم عصابات الاحياء التي نص عليها القانون 20-03 بإدراج نص يجيز العمل بنظام الدفاع الشرعي المنظم في عصابات الاحياء برخصة من الوالي.

كما يجوز العمل بهذا النظام في مجال الدفاع الشرعي الالكتروني خاصة لرد عدوان الذباب الالكتروني وجرائم الجوسسة والحرب السيبرانية على المستوى الدولي.

2.3- حالة الدفاع الشرعي الالكتروني الدولي.

قد يتوسع مفهوم الدفاع الشرعي الذي يمس بأمن الدولة والنظام العام لها، فلا تستند حينها إلى شرط الخطر الحال، وتعتبر أن كل تهديد لأمنها ونظامها يعتبر خطرا حالا و لو حكما، و هذا ما يبرر فكرة الدفاع الشرعي الاستباقي الذي تعتمده الدول سواء على المستوى الداخلي أو الخارجي في حالة نشوب حرب، و ما يهمنا في هذا البحث هو تسليط الضوء على الدفاع الشرعي الاستباقي الالكتروني على المستويين، سواء كان يهدد كيان الدولة و مؤسساتها داخليا أو الحرب الجديدة التي اطلق عليها تسمية الحرب السيبرانية مبرزين موقف المشرع الجزائري من هذا.

1.2.3- الدفاع الشرعي الوقائي والاستباقي

[1] مرسوم تنفيذي رقم 97-04 مؤرخ في 04 جانفي 1997، يحدد شروط ممارسة عمل الدفاع المشروع في إطار منظم، الجريدة الرسمية، عدد 01، 1997.

قد يجد الدفاع الشرعي الوقائي او الاستباقي أصله في الشريعة الإسلامية الغراء أين اباحت الدفاع عن الستر، فكل دولة لها اسرارها وسترها الذي لو اطلعت عليه اشخاص أو دول جاز للدولة الدفاع عن نفسها[1]، ويجوز حتى الدفاع الشرعي ضد السفراء وأعضاء البعثة الدبلوماسية الموجودة في البلد، كون أن الحصانة الدبلوماسية تخضع لقوانين ومعاهدات بين الدول ومن قام باعتداء أي كان يمس الدولة يكون قد نقض تلك العهود مما يعطي الدولة حق الدفاع الشرعي[2].

ويتخذ الدفاع الشرعي الاستباقي في المجال الالكتروني عدة صور منها المراقبة الاستباقية والآنية الالكترونية للاتصالات وللمواقع و للبيئة الالكترونية بصفة عامة، ففيما يخص الدفاع الشرعي الاستباقي المبني على المراقبة القبلية كرسه المشرع في المرسوم الرئاسي رقم 15-228[3]، الذي جاء في مادته 2 " النظام الوطني للمراقبة بواسطة الفيديو الذي يخضع إلى أحكام هذا المرسوم، أداة تقنية للاطلاع و **الاستباق** بهدف المساهمة فيما يأتي:

- مكافحة الإرهاب
- الوقاية من الأعمال الإجرامية
- حماية الأشخاص والممتلكات
- الحفاظ على النظام العام ...."

من خلال هذا النص يتضح جليا أن المشرع خرج عن الشروط العامة التي تحكمها المواد 39 و40 من قانون العقوبات الخاصة بالدفاع الشرعي، حيث وسع في مفهوم الخطر الحال وجعله مفترض، ليتسنى له الدفاع الاستباقي قبل وقوع الجرائم والا يفقد الدفاع الشرع الاستباقي معناه.

وهذا ما شرعت فيه الجزائر فعليا سنة 2004، وحسن فعل المشرع الجزائري كون أن هذا النوع من الجرائم في منحنى تصاعدي رهيب حيث بدأ ب 16 قضية سنة 2008، إلى 102 سنة 2013، إلى 1652 سنة 2019.[4]

كذلك نجد أن المشرع خول السلطات من مراقبة الشبكة الالكترونية بموجب القانون 09- 04، بموجب المادة 04 منه كإجراء استباقي للوقاية من جرائم الإرهاب وأمن الدولة، أو في حالة توفر معلومات عن **احتمال اعتداء** على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني.

وتجدر الإشارة هنا أن المشرع الجزائري في هذا النص خرج عن الراجح لدى الفقه الجنائي في كون أن الخطر يجب أن يكون حال ووشيك الوقوع وليس خطر احتمالي أو مستقبلي[5]، مما يبين وجه الاختلاف بين الدفاع الشرعي التقليدي

---

[1] الصديق أبو الحسن محمد، مرجع سابق، ص 112

[2] مسفر رزق الله محمد الزحامي، الدفاع الشرعي الخاص، دفع الصائل، رسالة ماجستير في مكافحة الجريمة، تخصص التشريع الجنائي الإسلامي، جامعة أم القرى، السعودية، السنة الجامعية 1996-1997، ص 115

[3] مرسوم رئاسي رقم 15-228 مؤرخ في 22 أوت 2015، يحدد القواعد العامة المتعلقة بتنظيم النظام الوطني للمراقبة بواسطة الفيديو و سيره، الجريدة الرسمية، عدد 45، 2015.

[4] جويدة بوعرابة، ترجمة معيوف محمد، رجال الدرك الوطني في مواجهة الجريمة السيبرانية، تحد جديد، مجلة الجيش، الجزائر، العدد 685، أوت 2020، ص،ص 20- 21.

[5] عبد الله سليمان، مرجع سابق ، ص 134.

والدفاع الشرعي الالكتروني الذي يقوم أساسا على الدفاع الشرعي الاستباقي وكذا تقييم الخطر الموجب لرد الاعتداء دوريا واعتباره حال في كل الأوقات.

ومن أجل إضفاء طابع الشرعية على العمل في هذا المجال أوكلت مهامه إلى الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها، التي خولها القانون عدة مهام منها ما يتعلق بمسألة الدفاع الشرعي الوقائي الاستباقي:

- ضمان المراقبة الوقائية للاتصالات الالكترونية قصد الكشف عن الجرائم المتعلقة بالأعمال الإرهابية والتخريبية والمساس بأمن الدولة.
- القيام دوريا عن طريق مجلسها بتقييم حالة التهديد في مجال الجرائم المتصلة بتكنولوجيا الإعلام والاتصال للتمن من تحديد مضامين العمليات الواجب القيام بها والأهداف المنشودة بدقة[1]

وهنا يطرح اشكال الحرية الخاصة للأفراد المصونة دستوريا، حيث أنه لا يجوز التنصت أو التجسس ومراقبة الاتصالات الالكترونية للأفراد، وهذا ما جعل بعض الدول تلجأ إلى استعمال تطبيقات لا تقوم باختراق خصوصية الافراد كبريطانيا.

أما المشرع الجزائري فقد جعل المساس في أضيق حدوده وفق ما نصت عليه المادة 03 من القانون 09-04،

هذا وقد أقدمت السلطات الجزائرية على حجب مواقع "توالى"، و"الطريق نيوز"، و"أنترليني"، و"مغرب ايمرجنت"، و"راديو أم"، و"قصبة تريبون"، و"شهاب برس"، و"ألترا صوت"، و"كل شيء عن الجزائر[2]."

ولم تعلن السلطات الجزائرية عن أي قرار أو خلفيات توضح أسباب حجب موقعَي "توالى" و"طريق نيوز" وغيرهما، واللافت أن هذه القرارات جاءت بعد أسبوع فقط من إصدار البرلمان الأوروبي لائحة تدين تعامل السلطات الجزائرية مع الصحافة وقضايا حرية التعبير، والتضييق على الصحف ووسائل الإعلام. وطالبت مؤسسات الاتحاد الأوروبي التنفيذية إلزام السلطات الجزائرية بمضمون اتفاق الشراكة الموقع عام 2002، والذي يتضمن إشارة إلى ضرورة التزام الجزائر بقواعد حرية التعبير[3].

وتجدر الاشارة أن إجراء حجب المواقع يجد مظلته القانونية في عدة نصوص خاصة، نذكر على سبيل المثال الأمر 21-09[4]، الذي ينص صراحة في مادته 23 – 2 بالتدخل الفوري وبأمر من السلطات القضائية، تحت طائلة العقوبات، من أجل سحب أو تخزين المحتويات التي يتيحون الاطلاع عليها أو جعل الدخول إليه غير ممكن عندما تشكل جريمة من الجرائم المنصوص عليها في هذا الأمر، أو بوضع ترتيبات تقنية تسمح بسحب أو تخزين هذه المحتويات أو لجعل الدخول إليها غير ممكن.

---

[1] مرسوم رئاسي رقم 21-439مؤرخ في 07 نوفمبر 2021، يتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية، عدد 86، 2021.

[2] السلطات الجزائرية تحجب 7 مواقع إخبارية: تضييق جديد(alaraby.co.uk) اطلع عليه يوم 07 ماي 2022 ، سا 19:12

[3] لكن الاشكال انه يمكن الدخول للمواقع المحجوبة بكل بساطة عند استخدام برنامج شبكة خاصة افتراضية (VPN) التي تقوم بتغيير الآيبي IP، فبدلا من أن تتصل على موقع هكر من الجزائر سوف تتصل من الموزمبيق مثلا. و الطريقة سهلة للغاية، حيث تقوم بالإتصال بسيرفر في الموزمبيق و بدلا من تصفح موقع هكر بالآيبي الخاص بك و الذي هو من الجزائر و فرضا أن الموقع محظور سوف يقوم برنامج vpn بفتح الموقع بالخادم الموجود في الموزمبيق،

[4] أمر رقم 21-09 مؤرخ في 08 جوان 2021، يتعلق بحماية المعلومات والوثائق الإدارية، الجريدة الرسمية، عدد 45، 2021.

وهذا ما يعاقب عليه قانون خطاب الكراهية في حال نشر أي معلومات تؤدي إلى الاضرار بالوحدة الوطنية، لهذا أصبح من المستساغ اللجوء إلى الدفاع الشرعي الاستباقي الذي يهدد المساس بالوحدة الوطنية.

ومن هنا نخلص أن الدفاع الشرعي يمكن أن تستعمله الدولة استباقيا على فرضية الخطر المهدد لكيانها ومساس أمنها سواء كان هذا المساس من طرف الأفراد عن طريق استخدامهم لمواقع التواصل الاجتماعي فتكون الحرب داخلية، أو من طرف الدول عن طريق رد الهجومات والحروب التي تشن ضد معلومات الدول و تعطيل حتى مصالحها و مطاراتها و هذا اطلق عليه الحرب في الفضاء السيبراني.

2.2.3-الدفاع الشرعي في ظل الحروب السيبرانية

ولتسمية هذه الفكرة، جمع جيبسون كلمة "السبرنطيقا Cybernetics "التي تعني علم التحكم الآلي، مع كلمة "الفضاءSpace "، وسك منهما مصطلح "الفضاء السيبراني Cyberspace "الذي أصبح حقيقة مع انتشار شبكة الانترنت على نطاق العالم. فالفضاء السيبرانيCyberspace مصطلح حديث، ظهر نتيجة لثورة تكنولوجيا المعلومات .ويشمل جميع الحواسيب والمعلومات التي بداخلها والأنظمة والبرامج والشبكات المفتوحة لإستعمال الجمهور العام أو تلك الشبكات التي صممت لاستعمال فئة محددة من المستعملين ومنفصلة عن شبكة الانترنت العامة، فـ "الفضاء السيبراني" هو العالم المادي والمفاهيمي الذي توجد فيه جميع هذه الأنظمة[1]

وبظهور هذا النوع من الحروب حتى بدأ استعماله منذ الثمانينيات، ففي ديسمبر من العام 2009 صرحت الحكومة الكورية الجنوبية عن تعرضها لهجوم نفذه قراصنة بهدف سرقة خطط دفاعية سرية تتضمن معلومات عن شكل التحرك الكوري الجنوبي والأمريكي في حالة حصول حرب في شبه الجزيرة الكورية .

وفي 2010، أعلنت ألمانيا أنها واجهت عمليات تجسس شديدة التعقيد لكل من الصين وروسيا كانت تستهدف القطاعات والبنى التحتية الحساسة في البلاد ومن بينها شبكة الكهرباء التي تغذي الدولة[2]، وما يزيد من خطورتها سهولة الحصول على الاسلحة السيبرانية وغموض هوية الطرف القائم بهذه العملية.

و تجدر الاشارة هنا أن الفقه فرق بين مفهومي " الهجوم السيبراني" و " الحرب السيبرانية" ، فيعني الأول إلى استخدام الخصوم لشيفرات و أكواد كمبيوتر بغرض التدخل في وظيفة و نظام الكمبيوتر أو الشبكة، سواء كانت انظمة حاسوبية خاصة بمؤسسات الدولة " مؤسسات اقتصادية، مطارات، موانئ، و غيرها" أو أنظمة الاجهزة الدفاعية و الاستخباراتية، عن طريق تعطيل تلك الشبكات و الانظمة، و افشال محاولة الاتصال بها أو تدميرها بالكامل، أما مصطلح " الحرب السيبرانية" فيشير حسبهم إلى الإجراءات التي تتخذها الدولة لاختراق أجهزة كمبيوتر أو شبكات خاصة بدولة أخرى بغرض التسبب في تلفها أو تعطيلها[3].

كذلك هناك من يطلق على مصطلح الدفاع السيبراني " الردع السيبراني"

[1] علاء فرحات، الفضاء السيبراني، تشكيل ساحة المعركة في القرن الحادي والعشرين، مجله العلوم القانونية و السياسية، المجلد10، العدد 03، ديسمبر 2019، ص 90.

[2] فيصل محمد عبد الغفار، الحروب الإلكترونية، الجنادرية للنشر والتوزيع، 2015، ص ص 11 –13

[3] حسين قوادرة، الردع السيبراني بين النظرية والتطبيق، المجلة الجزائرية للأمن والتنمية، المجلد 9، العدد 16، جانفي 2020، ص 521

وأمام هذه الخطورة جعل المجتمع الدولي نظام العمليات العسكرية في الفضاء السيبراني تستهدف عدة أهداف من بينها العملية الدفاعية التي يكون هدفها حماية المعالجة الالية للمعطيات الالكترونية على مستوى الشبكات العنكبوتية والخاصة بالدولة والوقوف دون الحاق اضرار بالدولة وشعبها وممتلكاتها[1].

و هذا ما دفع الدول الى تبني استراتيجيات ردعية دفاعية على نطاقها السيبراني قصد تحقيق ما اضحى يسمى " الأمن السيبراني"، و الجزائر أحد هذه الدول التي استهدفتها العديد من الهجمات السيبرانية، الشيء الذي ادى أيلائها أهمية قصوى للأمن السيبراني على جميع المستويات، بداية بوضع مرسوم سنة 2020 ينشئ مجلس و وكالة للأمن السيبراني [2]، هذه المنظومة الوطنية أعطى لها المشرع من خلال مجلسها و وكالاتها صلاحيات واسع في مجال التحقيق الالكتروني و الأمن و الدفاع عن الهجمات السيبرانية باعتماد استراتيجية ترتبط بنظام يقظة شامل هدفه التصدي للتهديدات الجديدة و انعكاساتها على استقرار الدولة.

ولتعزيز هذا المسار استحدث المشرع الجزائري في أوت 2021 قطب جزائي وطني لمكافحة الجرائم المتصلة بتكنولوجيات الاعلام والاتصال، يختص بالفصل في الجنح الخاصة بالجريمة الالكترونية والمتصلة بها سواء كانت ضد الأفراد أو الدولة أو الدفاع الوطني[3]، وهو ما يعكس الاهتمام الذي توليه الجزائر لمكافحة الجريمة السيبرانية ومواكبتها من الجانب التشريعي والقضائي.

كما أنه تم في نوفمبر 2015 استحداث مصلحة على مستوى دائرة الاستعمال والتحضير بأجهزة الجيش الوطني الشعبي " مصلحة الدفاع السيبراني ومراقبة أمن الأنظمة" مهمتها تأمين وحماية المنظومات والمنشآت الحيوية في البلاد، ضد التهديدات والارهاب الالكتروني.

أين تتمحور استراتيجية الدفاع الشرعي السيبراني للجيش الوطني حول تعزيز وتحيين الإطار القانوني المتعلق باستعمال تكنولوجيات الاعلام والاتصال وتأمين منظومات الإعلام، كما تتضمن تكوين للمورد البشري في هذا الشأن[4].

من خلال ما سبق يتضح أن المشرع الجزائري والدولة الجزائرية، تشعران بحجم خطورة هذه الحروب الجديدة، فهي تسعى دائما إلى تكريس قواعد قانونية وفق سياسة جنائية مواكبة للعصر غير متقيدة بالقواعد التقليدية، وهو خيار سليم طالما أن الجريمة تطورت واساليبها تغيرت فمن غير المنطقي أن تبقى الدول تحت وطأة القواعد التقليدية التي لا تحقق حماية المصلحة الجديرة بالحماية والتي تعتبر غاية قانون العقوبات.

لكن من وجهة نظرنا نرى أن المشرع باحترام القواعد القانونية وتحيينها التي لا تتعارض مع المصلحة العامة للدولة والافراد ومبدأ الشرعية أن يعيد النظر المادة 39 من قانون العقوبات أين يشير صراحة إلى الخطر المستقبلي والخطر الافتراضي الالكتروني.

---

[1] جون باسيت، حرب الفضاء الالكتروني: التسلح وأساليب الدفاع الجديدة، الحروب المستقبلية في القرن الـ 21، الطبعة 1، مركز الإمارات للدراسات والبحوث الاستراتيجية، 2014، ص 57.

[2] مرسوم رئاسي رقم 20-05 مؤرخ في 20 جانفي 2020، يتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية، الجريدة الرسمية، عدد 04، 2020.

[3] أمر رقم 21-11 مؤرخ في 25 أوت 2021، يتمم الأمر 66-155 المؤرخ في 08 جوان 1966، المتعلق بقانون الإجراءات الجزائية، الجريدة الرسمية، عدد 65، 2021.

[4] إ، جنادي، م، بوكبشة، أ، قيدوم، إ، غازي، حروب الجيل الجديد، تحطيم الأمم بأقل تكلفة، مجلة الجيش، الجزائر، العدد 701، ديسمبر 2021، ص 39.

الخاتمة:

تسعى كل التشريعات دائما بوضع سياسة جنائية تخدم التوازن المطلوب لحماية المصلحة العامة من جهة، دون هضم المصلحة الخاصة حقها من جهة خاصة، وبما أنه في بعض الاحيان تتقابل مصلحتان يحميهما القانون في نفس الوقت، يخلق هذا الاشكال وجوب ايجاد حل قانوني بغض النظر عن البيئة التي ولدت فيه.

فهنا يكرس القانون الجنائي قاعدة المصلحة الاجدر بالحماية، فيضحي بالمصلحة الاقل جدارة أمامها.

ومن هذا ودون الخروج عن مبدأ الشرعية جاءت فكرة اسباب الاباحة خدمة لفكرة المصلحة الجديرة بالحماية سواء كانت عامة أو خاصة، تقليدية أو الكترونية، وحاصل هذا العمل نجمله في النتائج التالية:

- أن الاباحة المقصودة في نص المادة 39 هي الاباحة الطارئة التي تأتي بعد تجريم فعل وتشوبه الشبهة وفيه مصلحة وليس الاباحة الاصلية لأن الأصل لا يحتاج إلى نص يبيحه.
- أن نص المادة 39 من قانون العقوبات يمكن إسقاطه على ما أذن به القانون وما أمر به القانون لعموم النص وعدم حصر الاوامر والأذن في البيئة التقليدية.
- أنه يمكن تصور أسباب اباحة في الفضاء الافتراضي، فكما هناك جريمة الكترونية هناك اسباب اباحة الكترونية
- أن التفتيش الالكتروني تحكمه قواعد تختلف عن قواعد التفتيش التقليدية.
- أنه يمكن تصور أن يكون هناك حالة دفاع شرعي حتى في البيئة الالكترونية سواء للأفراد أو الدولة.
- أن نص المادة 39 المعمول به في مجال اسباب الاباحة الالكترونية قاصر في مسألة شروط الدفاع الشرعي كون أن الدفاع الشرعي الالكتروني لا يحكمه شرط الخطر الحال دائما، ولا يمكن تقدير التناسب فيه تقديرا نافيا للجهالة.
- أن الدفاع الشرعي بالنسبة للدول توسعت دائرته بظهور الحروب السيبرانية التي تستهدف المعلومة.

وبناء على ما سبق نتوصل الى بعض الاقتراحات والتوصيات يمكن أن يحينها المشرع منها:

- تعديل المادة 3 من قانون العقوبات والنص على إقليم الجمهورية " بر وبحر وجو **ونطاق الكتروني**" حتى فهو الاقليم الذي يشمل الجريمة والاباحة على حد سواء.
- تحيين نص المادة 39 من قانون العقوبات والاشارة إلى الخطر المفترض في مسألة الدفاع الشرعي الالكتروني.
- تحديد شرط اللزوم والتناسب في الاباحة الالكترونية في نص المادة 39.
- اعتماد الدفاع الشرعي المنظم حتى في المجال الالكتروني بموجب نص قانوني ليكون مجابه للذباب الالكتروني.
- تبيان حدود الدفاع الشرعي والاباحة الالكترونية في مسألة الاختراق سواء اختراق حسابات الافراد أو مواقع الدول خاصة، ومنه تحديد استثناءات الدفاع وقت السلم.

قائمة المراجع:

1-الكتب:

(1) جون باسيت، حرب الفضاء الالكتروني: التسلح وأساليب الدفاع الجديدة، الحروب المستقبلية في القرن الـ 21، الطبعة 1، مركز الإمارات للدراسات والبحوث الاستراتيجية، 2014.

(2) رمسيس بهنام، نظرية التجريم في القانون الجنائي، معيار سلطة العقاب تشريعا وتطبيقا، دار الجامعة الجديدة، مصر، دون سنة.

(3) عبد الله سليمان، شرح قانون العقوبات القسم العام، الجزء الأول، دار الهدى للطباعة والنشر، عين مليلة، الجزائر، دون سنة.

(4) فيصل محمد عبد الغفار، الحروب الإلكترونية، الجنادرية للنشر والتوزيع، 2015

2-المجلات:

(1) جنادي، م، بوكبشة، أ، قيدوم، إ، غازي، حروب الجيل الجديد، تحطيم الأمم بأقل تكلفة، مجلة الجيش، الجزائر، العدد 701، ديسمبر 2021.

(2) جويدة بوعرابة، ترجمة معيوف محمد، رجال الدرك الوطني في مواجهة الجريمة السيبرانية، تحد جديد، مجلة الجيش، الجزائر، العدد 685، أوت 2020

(3) حسن إيهاب محمد، دور العرف في التجريم، المجلة المصرية للدراسات القانونية والاقتصادية، مصر، العدد 10، جانفي 2018.

(4) حسين قوادرة، الردع السيبراني بين النظرية والتطبيق، المجلة الجزائرية للأمن والتنمية، المجلد 9، العدد 16، جانفي 2020،

(5) علاء فرحات، الفضاء السيبراني، تشكيل ساحة المعركة في القرن الحادي والعشرين، مجله العلوم القانونية والسياسية، المجلد10، العدد 03، ديسمبر 2019.

(6) كمال بلارو، أحكام الدفاع الشرعي في التشريع الجزائري، مجلة العلوم الإنسانية، قسنطينة، الجزائر، العدد 49، مجلد ب، جوان 2018.

(7) ناصر بن محمد الجوفان، الدفاع الشرعي، دراسة مقارنة، مجلة العدل، العدد 58، السنة الخامسة عشرة، ربيع الثاني 1434 هـ

3-الرسائل الجامعية:

(1) مسفر رزق الله محمد الزحامي، الدفاع الشرعي الخاص، دفع الصائل، رسالة ماجستير في مكافحة الجريمة، تخصص التشريع الجنائي الإسلامي، جامعة أم القرى، السعودية، السنة الجامعية 1996-1997،

4-المو اقع الالكترونية:

(1) السلطات الجزائرية تحجب 7 مواقع إخبارية: تضييق جديد(alaraby.co.uk) اطلع عليه يوم 07 ماي 2022، سا 19:12.

(2) جزايرس : اتصالات الجزائر تطلق "في أمان "لمراقبة استخدام الأطفال للإنترنت(djazairess.com) اطلع عليه يوم 29 أفريل 2022، الساعة 15:12

5-قرارات المحكمة العليا:

(1) قرار ملف رقم 1193813 المؤرخ في 21 جوان 2018، مجلة المحكمة العليا، العدد الثاني، 2018،

(2) قرار ملف رقم 368024 مؤرخ في 28 نوفمبر 2007، مجلة المحكمة العليا، العدد الأول، 2009.