

## مجلة العلوم القانونية والاجتماعية

Journal of legal and social studies

Issn: 2507-7333

Eissn: 2676-1742

الدفاع الشرعي في الفضاء الرقمي: دراسة تحليلية لأنظمة الحماية الرقمية ومشروعيتها

Self-Defense in Cyberspace : An Analytical Study of Digital Protection Systems  
and Their Legitimacy

د. عاصم عادل محمد العضيلة<sup>1\*</sup>، سارة مدين عبد الفتاح حسن<sup>2</sup>

<sup>1</sup> كلية الحقوق ، الجامعة الاردنية، (المملكة الأردنية الهاشمية)، [as.aladaileh@ju.edu.jo](mailto:as.aladaileh@ju.edu.jo)

<sup>2</sup> كلية الحقوق ، الجامعة الاردنية، (المملكة الأردنية الهاشمية)، [SAR3220686@ju.edu.jo](mailto:SAR3220686@ju.edu.jo)

تاريخ النشر: 2025/12/01

تاريخ القبول: 2025/10/01

تاريخ ارسال المقال: 2025/09/09

\*المؤلف المرسل

## الملخص:

تبحث هذه الدراسة في الدفاع الشرعي في الفضاء الرقمي باعتباره من القضايا المستحدثة التي تثير إشكاليات قانونية مهمة. وتأتي أهمية الموضوع من تصاعد خطورة الجرائم السيبرانية ؛ التي تتجاوز الحدود الجغرافية والسياسية، مما ينعكس سلباً على الأفراد والمؤسسات من خلال تهديد بياناتهم ومواردهم الرقمية وتعطيل أنشطتهم اليومية والاقتصادية. وتتناول الدراسة مدى إمكانية تطبيق أحكام الدفاع الشرعي التقليدي على الجرائم السيبرانية ، مع بيان الفروق بين الرد الفردي المباشر وأنظمة الحماية الرقمية. كما تناقش الضوابط اللازمة لمشروعية هذا الحق، مثل مبدأي الضرورة والتناسب، لتجنب تحول الدفاع إلى أفعال انتقامية غير مشروعة. وتخلص الدراسة إلى ضرورة وضع إطار تشريعي منظم للدفاع الشرعي في الفضاء السيبراني يضمن حماية الحقوق الرقمية للأفراد والمؤسسات ويعزز الأمن القانوني.

الكلمات المفتاحية: الدفاع الشرعي، الدفاع الشرعي الآلي ، الجريمة السيبرانية ، الفضاء الرقمي، أنظمة الحماية الآلية.

**Abstract :** This study explores lawful self-defense in cyberspace as an emerging legal issue that raises significant challenges. Its importance lies in the growing threat of cybercrimes that transcend geographical and political borders, directly affecting individuals and organizations by compromising their digital assets, threatening sensitive data, and disrupting their daily and economic activities. The study examines the applicability of traditional self-defense rules to cyberattacks and highlights the differences between individual direct responses and digital protection systems. It also discusses the legal constraints governing this right, particularly the principles of necessity and proportionality, to prevent unlawful retaliation. The research concludes by stressing the need for a clear legislative framework to regulate cyber self-defense, ensuring the protection of digital rights for individuals and organizations while strengthening legal security in cyberspace.

**Keywords :** Self-Defense , Automated Self-Defense , Cybercrime , Cyberspace , Automated Protection Systems .

## مقدمة:

في ظل التغيرات المتسارعة التي يشهدها العالم الرقمي، أصبحت الهجمات السيبرانية واحدة من أخطر التهديدات المعاصرة وأكثرها تدميرًا والتي تواجه الأفراد والمؤسسات على حد سواء (1)، إذ باتت تمثل شكلاً جديداً من أشكال العدوان، ولا تقل خطورة عن الأفعال المادية التقليدية، بل قد تتجاوزها في التأثير والضرر. فتعطيل أنظمة المعلومات، وسرقة البيانات البنكية، واختراق قواعد البيانات الخاصة بالمؤسسات، أضحت اعتداءات مباشرة تمس خصوصية الأفراد، كما تهدد استقرار المؤسسات ودوام خدماتها.

ولمواكبة هذا التطور، عمد المشرع الأردني إلى تحديث منظومته القانونية عبر استحداث قانون الجرائم الإلكترونية، الذي جاء استجابة لواقع رقمي جديد، يتم فيه تنفيذ الجرائم عن بُعد وبأدوات غير تقليدية تلحق أضراراً جسيمة بمستخدمي أنظمة تكنولوجيا المعلومات.

وقد اشتمل هذا القانون على تجريم أفعال لم تكن معروفة سابقاً، كالدخول غير المصرح به إلى الأنظمة وتعطيلها، ونشر البرامج الخبيثة، والابتزاز الإلكتروني، وغيرها من الجرائم مما يظهر وعي المشرع بخطورة هذا النوع من الأفعال وأهمية تجريمها.

وفي المقابل، فإن قانون العقوبات الأردني لا يزال ينظم في إطار قواعده العامة أسباب التبرير، ومنها الدفاع الشرعي والذي يعتبر من أهم الأدوات القانونية التي تُتيح للفرد أن يدفع خطراً غير محقق يهدد نفسه أو ماله ضمن شروط معينة دون أن يُعتبر فعله جريمة جزائية. (2).

وإنطلاقاً من هذا التباين بين النصوص التقليدية لقانون العقوبات وطبيعة الجرائم السيبرانية الحديثة، تبرز الحاجة إلى دراسة إمكانية تطبيق قواعد الدفاع الشرعي على الجرائم السيبرانية باعتبارها نمطاً جديداً من التعدي الذي قد يستوجب ردّاً فورياً ومناسباً، فالفضاء الرقمي رغم طبيعته غير المادية إلا أنه أضحى مجاًلاً واقعياً يتفاعل فيه الأفراد وتتقاطع فيه الحقوق والمصالح، تماماً كما الواقع المادي، إضافة إلى أنه يعتبر مسرّحاً لممارسة الأنشطة الجرمية ضد الأفراد والمؤسسات.

## إشكالية الدراسة :

تكمن إشكالية هذه الدراسة في الإجابة عن التساؤلات الآتية: هل يمكن تطبيق قواعد الدفاع الشرعي على الاعتداءات السيبرانية؟ وما الحدود التي يجب ان يُلتزم بها في ممارسة حق الدفاع في الفضاء الرقمي حتى لا يتحول الى فعل مجرّم؟ وما الضوابط التي يمكن إعمالها لتنظيم استعمال هذا الحق من قبل الأفراد والمؤسسات؟

## منهجية الدراسة :

استعملت هذه الدراسة المنهج التحليلي، وذلك من خلال تحليل مدى الكفاية التشريعية في تنظيم الجريمة الإلكترونية من جهة، وبيان إمكانية تطبيق أحكام الدفاع الشرعي على هذا النوع الجديد من العدوان من جهة أخرى، وصولاً إلى تقديم تصور قانوني متوازن يُراعي الحقوق والحريات، ويمنح الأفراد وسائل قانونية فعّالة للدفاع في بيئة رقمية باتت أكثر خطورة من أي وقت مضى.

## أهمية البحث :

تكمن أهمية هذا البحث في تناوله مسألة قانونية لم تحظ بعد بتنظيم واضح في التشريع الأردني، تتعلق بمدى امكانية اللجوء إلى الدفاع الشرعي في مواجهة الأعتداءات السيبرانية التي أصبحت تمس بشكل مباشر حقوقاً ومصالح محمية قانوناً.

ويسعى البحث إلى استكشاف مدى مرونة القواعد العامة في استيعاب هذا النوع من التعدي وطرح رؤية قانونية حديثة تُعيد رسم حدود الحماية في البيئة الرقمية، بما يعزز من قدرة الأفراد والمؤسسات على حماية أنفسهم في البيئة الرقمية ضمن إطار قانوني منظم.

## خطة البحث :

سيتم تقسيم هذا البحث إلى ثلاثة مطالب:

المطلب الأول: الطبيعة القانونية للدفاع الشرعي.

الفرع الأول: تعريف الدفاع الشرعي.

الفرع الثاني: الدفاع الشرعي في قانون العقوبات الأردني.

المطلب الثاني: مدى انطباق أحكام الدفاع الشرعي على الجريمة السيبرانية.

الفرع الأول: الجريمة السيبرانية وخصائصها.

الفرع الثاني: إمكانية تطبيق قواعد الدفاع الشرعي على الجريمة السيبرانية .

المطلب الثالث: ضوابط وحدود منح الأفراد والمؤسسات حق الدفاع الشرعي السيبراني.

الفرع الأول: تحديد الاعتراف المطلق بالدفاع الشرعي السيبراني.

الفرع الثاني: الضوابط المقترحة لتنظيم الدفاع الشرعي الآلي

## المطلب الأول : الطبيعة القانونية للدفاع الشرعي .

ستناول في هذا المطلب البحث في تعريف الدفاع الشرعي التقليدي كقاعدة عامة إضافة إلى الوقوف على تنظيم المشرع الأردني للدفاع الشرعي كأحد أسباب التبرير التي أخذ بها في قانون العقوبات .

### الفرع الأول: تعريف الدفاع الشرعي

يُعد الدفاع الشرعي ضرورة اجتماعية ملحة تمكن الأفراد من حماية أنفسهم وممتلكاتهم متى عجزوا عن إخبار السلطات كي تتدخل فوراً لحمايتهم، وقد ارتأت التشريعات الجزائية حماية هذا الحق وتقنينه واعتبرت الدفاع الشرعي أحد أسباب التبرير التي تُسقط صفة عدم المشروعية عن الفعل الجرمي وتحوله إلى فعل مباح قانوناً متى توافرت شروطه<sup>(3)</sup> .

ويقوم حق الدفاع الشرعي على فكرة الموازنة بين المصالح المتعارضة حيث يُفضل مصلحة المعتدي عليه على مصلحة المعتدي التي أهدرها بسلوكه الاجرامي<sup>(4)</sup>، فحين يهدد المعتدي حقاً محمياً، يفقد حمايته القانونية ويحق للمدافع أن يرد الأعتداء، ولكن في حدود الضرورة والتناسب<sup>(5)</sup> .

أما من حيث الطبيعة القانونية للدفاع الشرعي؛ فهو يُعد حقاً موضوعياً يُمنح لكل فرد دون اعتبار لصفته متى تعرض لخطر حالّ غير مشروع يهدد أحد الحقوق التي يحميها القانون<sup>(6)</sup>، كما يُعد من أسباب التبرير المطلقة إذ يمكن التمسك به في مواجهة جميع أنواع الجرائم دون أن يقتصر أثره على جرائم بعينها، فالعبرة هنا بفعل الاعتداء لا بالفاعل ولا بنوع الجريمة.

وقد اختلف الفقهاء في تعريفهم للدفاع الشرعي، ومن هذه التعاريف "استعمال القوة اللازمة لصد خطر حال غير مشروع يهدد بالإيذاء حقاً يحميه القانون"<sup>(7)</sup>، ومنها أيضاً "تمتع المدافع بحق ينطوي على طبيعة خاصة يؤهله في لحظة حصول خطر حالّ يهدد مصلحة يحميها القانون بدرء هذا الخطر عن نفسه أو ماله"<sup>(8)</sup>، أيضاً "استعمال القوة الضرورية لصد أي خطر أو اعتداء غير محقق يلحق الضرر بحق يُرتب له القانون حماية"<sup>(9)</sup>.

تُظهر هذه التعريفات أن جوهر الدفاع الشرعي يقوم على وجود خطر حقيقي وفوري، وأن يكون رد الفعل متناسباً معه من حيث الشدة والضرورة دون تجاوز، فهذا الحق ليس مطلقاً، بل هو مقيد بقيود تحفظ التوازن بين حماية الأفراد من جهة وعدم السماح بتحول الدفاع إلى وسيلة للانتقام من جهة أخرى.

### الفرع الثاني: الدفاع الشرعي في قانون العقوبات الأردني.

لقد تناول قانون العقوبات الأردني رقم ( 16 ) لسنة 1960 حق الدفاع الشرعي وقد بوب له تحت عنوان أسباب التبرير وذلك في المادة ( 60 ) والتي جاءت على النحو الآتي:

١. يعد ممارسة للحق: كل فعل قضت به ضرورة حالية لدفع تعرض غير محقق ولا مثار عن النفس، أو المال، أو نفس الغير، أو ماله.

٢. يستوي في الحماية الشخص الطبيعي والشخص المعنوي.

٣. إذا وقع تجاوز من المدافع بحسن نية بأن استعمل لدفع الاعتداء قوة تزيد على القدر اللازم دون أن يكون قاصداً إحداث أذى أشد مما يستلزمه الدفاع جاز للقاضي إعفاء الجاني من العقوبة أو تخفيفها."

وباستعراض أحكام المادة ( 60 ) أعلاه يتضح لنا أن المشرع الأردني اعتبر الدفاع الشرعي أحد أشكال ممارسة الحق، المعلق على توافر شروط دقيقة تضمنت في طياتها عدم استغلاله كذريعة للاعتداء، وقد جاءت الصياغة عامة تشمل الدفاع عن النفس والمال، وقد ساوى بين الأشخاص الطبيعيين والمعنويين، من حيث حق الحماية أيضاً، وهو ما يدل على اتساع نطاق الحماية القانونية لتشمل الكيانات القانونية المعترف بها<sup>(10)</sup>. ويمكننا من خلال ما سبق تناوله تحديد الشروط الموضوعية التي يجب توافرها في فعل الاعتداء الذي يتحقق به الدفاع الشرعي ويكون مبرراً، على النحو الآتي:

الشرط الأول: أن يكون هناك تعرض غير محقق

يقصد بالتعرض غير المحقق أن يكون الفعل الذي دفع المدافع إلى استعمال القوة فعلاً يُشكل جريمة وفقاً للقانون، وأن يكون التعرض موجهاً إلى مصلحة يحميها القانون، سواء أكانت المصلحة متعلقة بالنفس أم المال<sup>(11)</sup>.

ويجب أن يكون التعرض حقيقياً لا وهمياً، أي أنه يشكل خطراً جدياً لا مجرد خوف أو شك، ومع ذلك لا يشترط أن يكون التعرض قد بدأ فعلاً، بل يكفي أن يكون على وشك الوقوع والبدء فيه منتظر وفقاً السير العادي للأمر، أو أن يكون التعرض بدأ، ولكنه لم ينته بعد<sup>(12)</sup>.

الشرط الثاني: أن يكون الخطر حالاً

الخطر الحال هو الخطر القريب الذي يتوقع حدوثه مباشرة وفي أي لحظة أي أنه قد بدأ أو على وشك أن يبدأ، وفي هذه الحالة يبرر استعمال الدفاع الشرعي، وحيث أن هذا الشرط يستند في أساسه إلى أن المدافع يقوم بفعله لحماية حق يحميه القانون مع عدم إمكانية اللجوء للسلطات العامة لحماية هذا الحق<sup>(13)</sup>.

أما في حالة الخطر المستقبلي أو الخطر الذي وقع وانتهى لا يجوز التذرع بمواجهتهم بالدفاع الشرعي، وأي فعل يقوم به المدافع في هذه المراحل يعتبر إنتقاماً وإستيفاءً للحق بالذات الأمر الذي يعتبر جرماً معاقباً عليه قانوناً<sup>(14)</sup>.

الشرط الثالث: أن لا يكون التعرض مثاراً .

أي يشترط في التعرض أن يكون صادراً عن المعتدي نتيجة لإرادة خالصة منه، دون أن يكون المدافع قد تسبب في إثارته سواء بأفعال مباشرة أو بصورة غير مباشرة، فالمدافع الذي يخلق موقعاً خطيراً ثم يتذرع بأنه يدافع عن نفسه يفقد حقه بالحماية القانونية للدفاع الشرعي، أي يقصد به عدم إثبات المعتدى عليه (المدافع) أي فعل أو قول يجعل المعتدي يستعمل العنف تجاهه<sup>(15)</sup>.

ومع توسع دور المؤسسات والشركات في النشاط التجاري والاقتصادي، لم يعد الدفاع الشرعي يقتصر على حماية الأشخاص الطبيعيين وأموالهم المادية فقط، بل امتد ليشمل حماية الشخص المعنوي المادية وحماية حقوقه الرقمية أيضاً<sup>(16)</sup>، حيث أن أنظمة المعلومات والبنية التحتية الرقمية تعد جزءاً لا يتجزأ من كيان الشخص المعنوي القانوني إذ ترتبط بها مباشرة مصالحه المالية والتجارية وحقوقه المعنوية، ومع تزايد الاعتماد على البيئة الرقمية أصبحت تلك الأنظمة هدفاً محتملاً للاعتداءات الإلكترونية التي قد تعرض الشركة لأضرار جسيمة، وعليه فانه متى توافر خطر حال غير مشروع يستهدفها فإنه يمكن التمسك بحالة الدفاع الشرعي لحمايتها.

غير أنّ هذا الحق ليس مطلقاً، إذ لابد من توافر مجموعة من الشروط الخاصة بفعل الدفاع وإن أولها أن يكون فعل الدفاع لازماً وضرورياً بحيث يكون فعل الدفاع هو الوسيلة الوحيدة الكفيلة بدفع الخطر، فإذا كان بالإمكان تجنب الاعتداء بوسائل أقل ضرراً أو اللجوء إلى السلطات المختصة ولم يفعل المدافع، فإن الفعل يفقد صفته الدفاعية، فضلاً عن وجوب توجيه الرد إلى مصدر الاعتداء مباشرة<sup>(17)</sup>.

كما يشترط في فعل الدفاع أن يتناسب الفعل الدفاعي مع جسامته الخطر، بحيث يُقدّر التناسب وفق ظروف الواقع وما يعرض على المدافع من اعتداء من منظور الشخص المعتاد لا من منظور المدافع ذاته، فإذا كانت مصلحة المدافع مهددة جاز له رد الخطر، ولكن بالقدر اللازم فقط، دون أن يكون هنالك تجاوز مفرط يؤدي إلى تجريد الفعل من مشروعيته وتحوله إلى اعتداء جديد يستوجب المسؤولية<sup>(18)</sup>.

ومن جانب آخر يُعد تجاوز حدود الدفاع الشرعي من أهم المسائل التي توقف عندها المشرع، حيث أن الأصل أن الدفاع لا يُعتبر مشروعاً إلا إذا التزم المدافع بحدود الضرورة والتناسب، غير أن التجاوز قد يقع إما عمداً وإرادةً فيعدّ

في هذه الحالة مرتكبًا جريمة تستوجب العقاب، أو قد يقع بحسن نية بأن يعتقد المدافع أنه لا يزال في حدوده وأن الوسيلة التي أخذ بها استخدمت بالقدر المناسب لرد الإعتداء<sup>(19)</sup>، وهو ما أجاز فيه المشرع للقاضي أن يعفي المدافع من العقوبة أو يخففها<sup>(20)</sup>.

### المطلب الثاني: مدى انطباق أحكام الدفاع الشرعي التقليدي على الجريمة السيبرانية .

أدى التطور التكنولوجي إلى ظهور نوع جديد من الجرائم ألا وهي الجرائم السيبرانية التي باتت تشكل تهديدًا مباشرًا للأمن الفردي والمجتمعي والاقتصادي على حد سواء، وتمتاز هذه الجرائم بقدرتها على تجاوز الحدود الجغرافية وسرعتها في إحداث الأضرار وصعوبة تحديد مرتكبيها بدقة.

وفي ظل هذه التحديات، تطرح مسألة مدى امكانية تطبيق أحكام الدفاع الشرعي المنصوص عليها في قانون العقوبات الأردني على هذه الجرائم، فهل يمكن للضحية في الفضاء الرقمي أن يرد على الاعتداء بذات الحرية التي يتيحها له القانون في حالات الاعتداء التقليدي؟ أم أن طبيعة الفضاء الرقمي تستوجب ضوابط وإجراءات استثنائية؟

### الفرع الأول: الجريمة السيبرانية وخصائصها .

وفي هذا المقام سنتحدث عن الجريمة السيبرانية من حيث تعريفها بصورة عامة والخصائص المميزة لها عن غيرها من الجرائم .

#### أولاً: تعريف الجريمة السيبرانية .

وقبل الحديث عن الجريمة السيبرانية وتعريفها فإنه لا بد لنا أن نميز بين الجريمة السيبرانية والهجمات السيبرانية ، فإن الهجمات السيبرانية هي الاستخدام العدواني لتكنولوجيا المعلومات أو الاتصالات وذلك بهدف إلحاق الضرر بالمصالح الوطنية الأساسية للدولة والتي تتطلب القدرة على التجسس والإختراق والتخريب<sup>(21)</sup>.

وإن الاختلاف الجوهرى بينهما يكمن في أن الهجمات السيبرانية ترتكب من دول تهدف لإضعاف شبكات الحاسوب في دولة ، لتحقيق أهداف سياسية وإضافةً لذلك فإن نطاق هذه الهجمات يكون شاملاً ليشمل الأشخاص أو الممتلكات العائدة للدولة<sup>(22)</sup>.

في ظل تباين وجهات النظر حول هذه الجريمة، سواء من حيث المحل أو الأفعال الجرمية أو الحماية، وُجدت العديد من التعريفات الفقهية التي حاولت ضبط مفهوم الجرائم الالكترونية واستجماع محاورها، ومن هذه التعريفات ما يلي :

ما عرّفه الفقيه MERWE "أنها فعل غير مشروع يتورط في ارتكابه الحاسب الآلي أو الفعل الاجرامي الذي يستخدم في اقتراه الحاسب الآلي"<sup>(23)</sup>.

وعُرفت أيضًا بأنها "نشاط غير مشروع موجه لنسخ، أو تغيير، أو حذف، أو الوصول إلى المعلومات المخزنة داخل الحاسب أو التي تتعلق بالمعالجة الآلية للبيانات"<sup>(24)</sup> .

عرفت أيضًا بأنها " هي كل جريمة مقصودة ترتكب بواسطة تقنية أنظمة المعلومات وتُحدِث أو من شأنها أن تُحدِث ضررًا فيها"<sup>(25)</sup> .

من خلال إستعراض التعريفات الواردة للجريمة الالكترونية، يتضح أنها جميعها تلتقي عند كونها أفعالاً غير مشروعة تستخدم الحاسب الآلي أو تقنيات أنظمة المعلومات كأداة أو محل للإعتداء، وتستهدف بصورة مباشرة الوصول إلى البيانات أو التلاعب بها أو إلحاق الضرر بها أو بالأنظمة التي تحتويها.

وهذا يجعلها بطبيعتها تمثل إعتداء فعلياً على مجموعة من الحقوق والمصالح المحمية قانوناً، مثل الحق في سرية المعلومات، وسلامة البنية التحتية المعلوماتية، وحقوق الأفراد والمؤسسات في حماية بياناتهم من العبث أو الإتلاف أو الاستغلال غير المشروع، مما يعكس خطورتها البالغة على المستويات الفردية والمؤسسية والمجتمعية.

#### ثانياً: خصائص الجريمة السيبرانية .

تتميز الجريمة السيبرانية بمجموعة من الخصائص تجعلها مختلفة عن الجرائم التقليدية، وأهمها:

١. جرائم عابرة للحدود: فهي لا تلتزم بالحدود السياسية للدول ويمكن ارتكابها عن بعد بحيث يكون الجاني في دولة والمجني عليه في دولة أخرى<sup>(26)</sup> ، أو يمكن أن تقع الجريمة في وقت معين وتتحقق نتيجتها في وقت مختلف، هذه الطبيعة العالمية للإنترنت جعلته مسرحاً مفتوحاً للجرائم، ما يفرض تعاوناً دولياً لتبادل المعلومات وملاحقة الجناة<sup>(27)</sup> .

وإن خطورة هذا النوع من الجرائم يظهر جلياً نتيجة لوجود التباعد الجغرافي بين الجاني مرتكب الجريمة والمجني عليه فيها .

٢. يصعب اكتشافها وإثباتها: تعد الجرائم السيبرانية من أصعب الجرائم إثباتاً نظراً لوقوعها في بيئة رقمية واعتمادها وسائل تقنية متطورة وسريعة التنفيذ مما يسهل على الجاني محو الأدلة أو التلاعب بها مع غياب الدليل المادي التقليدي<sup>(28)</sup> .

كما أن التباعد الجغرافي واستخدام تقنيات الإخفاء والتشفير يصعب تتبع الفاعلين، ما يستلزم تعاوناً دولياً وخبراء متخصصين في التحقيق الرقمي.

٣. جرائم بالغة الخطورة: وذلك نظراً لما تسببه من خسائر مادية يصعب تقديرها وأضراراً تمس الأفراد والمؤسسات ، كما في حالات نشر الفيروسات المدمرة، فضلاً عن مساسها بالحياة الخاصة وتهديدها لأمن الدول القومي<sup>(29)</sup> .

ومن مظاهر هذه الخطورة أنها جرائم سهلة لا تتطلب مجهوداً أو مواجهة مباشرة بين الجاني والمجني عليه<sup>(30)</sup> ، حيث يكفي توافر التقنية المناسبة والوسيلة اللازمة لدى الفاعل لارتكابها وتزداد جاذبيتها للمجرمين مع انتشار نظم المعلومات وارتفاع الثقافة التقنية لدى الأفراد، مما يزيد سهولة تحقيق مكاسب مادية مرتفعة من خلالها<sup>(31)</sup> .

ومن خلال ما تقدم بيانه من التعريفات والخصائص الجوهرية للجرائم السيبرانية ( الالكترونية ) يتضح أن هذه الجرائم تحمل سمات استثنائية تميزها عن الجرائم التقليدية، ومن هذا المنطلق يصبح من الضروري عند دراسة تطبيق أحكام الدفاع الشرعي عليها مراعاة هذه الخصائص، فالاعتبار الدقيق لهذه السمات يتيح وضع إطار قانوني متوازن يحمي حقوق المجني عليه ويضمن ممارسة الدفاع الشرعي ضمن حدوده المشروعة، بما يمكن من التعامل بفاعلية مع التهديدات الرقمية ويهيئ الأرضية لدراسة تفصيلية في الفرع التالي حول انطباق احكام الدفاع الشرعي على الجريمة الالكترونية.

الفرع الثاني: انطباق أحكام الدفاع الشرعي على الجريمة السيبرانية

بعد أن بينا ماهية الدفاع الشرعي وشروطه، والطبيعة الخاصة للجرائم السيبرانية وخصائصها المميزة عن الجرائم التقليدية، يثور التساؤل حول الكيفية التي يمكن أن يمارس بها الدفاع الشرعي في البيئة الرقمية . فهل يُترك الأمر للرد الفردي المباشر الذي يقوم به الشخص المعتدى عليه عند مواجهة الهجوم الإلكتروني؟ أم يمكن الركون إلى الرد الآلي عبر أنظمة تقنية مبرمجة لمعالجة الاعتداء بصورة تلقائية؟ من هنا تبرز أهمية المقارنة بين النموذجين للكشف عن مدى انسجام كل منهما مع ضوابط الدفاع الشرعي وحدوده القانونية. أولاً: الدفاع الشرعي الفردي المباشر .

الدفاع الفردي المباشر في الفضاء الرقمي ويطلق عليه كذلك مسمى ( الدفاع النشط ، أو الدفاع السيبراني النشط ، أو الدفاع العكسي أو المضاد ، ) ويقصد به أن يقوم الفرد أو المؤسسة المتضررة بالرد بنفسها على الاعتداء الإلكتروني عبر إجراءات تقنية هجومية وبشكل يدوي (مثل: اختراق الجهاز المهاجم، تعطيله، أو سرقة بياناته وتخريبها كرد فعل على الاختراق) (32) .

غالبًا ما يُنظر إلى هذه الأفعال على أنها نوع من الردود التي تعد إمتدادًا لفكرة الدفاع الشرعي، لكن في بيئة رقمية، حيث يسعى الضحية إلى حماية نفسه بشكل فوري دون اللجوء إلى الجهات الرسمية، ورغم ما يبدو في هذا السلوك من منطق لتفادي الخطر أو رده إلا أن هناك العديد من الإشكاليات حول مدى مشروعيتها، خصوصًا أن هذه الأفعال غالبًا ما تُصنّف في ذاتها كجرائم رقمية مستقلة(33)، وفيما يلي بيان الحجج التي تُدلل على إنتفاء شرط المشروعية في هذه الأفعال:

١. غياب الشرعية الجزائية : إن الرد الفردي غالبًا ينطوي على أفعال مجرمة بذاتها (مثل الاختراق أو إتلاف البيانات) مما يجعله اعتداءً جديدًا لا يندرج ضمن إطار الدفاع الشرعي.

٢. الخطر لصعوبة التحديد الخاطئ للهدف: إن أساس هذا الخطر يستند إلى صعوبة تحديد مصدر الهجوم السيبراني بحيث يخطئ الفرد في تحديد مصدر الهجوم خاصة عند استخدام المهاجم لعناوين وهمية أو خوادم بسيطة مما يؤدي إلى توجيه الاعتداء نحو طرف بريء لا علاقة له بالهجوم الأصلي، وعليه فإنه يشكل إعتداءً على طرف لا علاقة له بالجريمة المدافع ضدها (34).

٣. غياب الرقابة القانونية: إن السماح للأفراد بالرد على الهجمات يمكن أن يؤدي إلى فوضى إلكترونية وتحويل الدفاع إلى إنتقام شخصي، وهو ما يتعارض مع فلسفة القانون التي تقصر سلطة العقاب والرد على الدولة فقط (35).

٤. فقدان شرط التناسب: كثير من الردود الفردية قد تتجاوز حجم الخطر الفعلي (مثل تعطيل أنظمة كاملة كرد فعل لمحاولة اختراق بسيطة) مما يفقد الرد صفة الدفاع المشروع، ويعتبر نشاطًا جرميًا جديد صادرًا عن المعتدى عليه(36).

٥. الجهل بأساليب الرد الإلكتروني: حيث يزداد خطر تجاوز الحدود القانونية للدفاع عندما يفتقر الأفراد إلى الخبرة الكافية في استخدام الأنظمة الإلكترونية مما يجعل ردودهم غير متناسبة وبالتالي تتحول إلى اعتداء بدلًا من دفاع مشروع.

يبرز جلياً أن الدفاع الفردي في الفضاء الرقمي - رغم اللجوء له لدفع الخطر أو الإعتداء بشكل فوري - يحمل في طياته أخطاراً جسيمة ويخضع لممارسات غير قانونية تجعله أقرب إلى الانتقام منه للدفاع المشروع ، كما أن هذا النمط من الردود قد يتحول إلى ذريعة لاستيفاء الحق بالذات ما يفتح الباب أمام العديد من التجاوزات والانتهاكات التي يجرمها القانون<sup>(37)</sup>.

ومن هنا تنبع الحاجة إلى البحث عن وسائل رد منظمة وآمنة تتوافق مع القانون، تسمح للمعتدى عليهم الاستجابة للهجمات الالكترونية دون الوقوع في التجاوز أو المخاطر المصاحبة للدفاع الفردي، ويشكل هذا التوجه مدخلاً لدراسة الأساليب الآلية للرد الالكتروني التي تقوم بحماية أنظمة المعلومات وقواعد البيانات بشكل فوري مُتَّبَعَةً بذلك ضوابط دقيقة تضمن التناسب في الرد وتقلل الأضرار المحتملة على الأطراف غير المعنية، بما يوازن بين الدفاع عن الحقوق من جهة؛ واحترام القانون وسيادة الدولة في ضبط الردود الالكترونية من جهة أخرى.

ثانياً: الدفاع باستخدام الوسائل الآلية (أنظمة الحماية الالكترونية) .  
عُرِفَ الدفاع الآلي أو ما يطلق عليه بالدفاع الإيجابي أو الدفاع الاوتوماتيكي بأنه مجموعة من التدابير الاحترازية أو الاحتياطية التي يلجأ إليها المالك للحفاظ على حقه ضد الأخطار المستقبلية<sup>(38)</sup>.

وقد أثار الدفاع الآلي خلافاً فقهيّاً لدى فقهاء القانون الجزائي وكانوا بين مؤيد ومعارض لهذه الفكرة فذهب الاتجاه المؤيد للدفاع الشرعي الآلي فيشترط فيه ما يشترط بالدفاع الشرعي التقليدي ، كما يشترط فيه أن يكون عمل الآلة وقت الخطر ، كما يشترط فيه أن يكون متناسباً مع حالة الخطر فإذا عملت الآلة قبل الخطر أو بعده أو كانت لا تتناسب مع مقدار الخطر فإن المدافع يكون مسؤولاً عن فعله الجرمي<sup>(39)</sup>.

ويبرر هذا الاتجاه استخدام الآلة لصد الخطر من خلال تفسير الخطر الحال تفسيراً موسعاً ، كما أنهم يقيمون تبريرهم استناداً لعدم إمكانية وضع حل مسبق لمشكلة التناسب الأمر الذي يتوقف على ظروف الدفاع و الخطر التي يجب على أساسها تحديد المقدار الواجب توافره في الدفاع والخطر .

أما الاتجاه المنكر لفكرة الدفاع الآلي فقد أكد أنه لا يعد وسيلة من وسائل الدفاع الشرعي فإنه تصرف غير مشروع وذلك لأن فعل الدفاع يجب أن يتزامن مع الخطر لحظة حلوله وبالتالي لا يجب أن يتحول الدفاع الشرعي لإجراء احتياطي أو احترازي لصد الخطر<sup>(40)</sup> .

إلا أن حق الدفاع الشرعي ينشأ وبصورة صحيحة في حال توقع الخطر من شخص معين أو غير معين مادام قد ثبت أن سلوك الدفاع كان متلائماً مع الخطر الحال أو وشيك الوقوع<sup>(41)</sup>.

وعلى هذا الأساس تُعتبر الوسائل الآلية أحد أهم أشكال الدفاع في المجال الإلكتروني، وهي أدوات أو برامج تُصمَّم لتعمل بشكل تلقائي عند وقوع اعتداء أو هجوم أو حتى عند مجرد محاولة التسلل، ومن أبرز هذه الوسائل: الجدران النارية (fire wall) التي تراقب حركة المرور وتسمح أو تمنع الوصول بناء على قواعد محددة، وأنظمة كشف ومنع التسلل (IDS/IPS) التي تعمل على التعرف على الأنشطة المشبوهة ووقفها فوراً، بالإضافة إلى برمجيات التشفير الذاتي التي تمنع المهاجم من الاستفادة من البيانات حتى لو تمكن من الوصول إليها<sup>(42)</sup>، كما أن بعض الأنظمة الأكثر تطوراً تتضمن آليات الاغلاق التلقائي للجهاز أو تعطيل الحسابات المشبوهة فور اكتشافها<sup>(42)</sup>.

تمثل أنظمة الحماية الإلكترونية من الناحية العملية والواقعية صورة متقدمة من وسائل الدفاع الشرعي فهي لا تنطلق من مبدأ الهجوم المضاد وإنما مع مبدأ الحماية والوقاية، وهي تشبه إلى حد كبير ما عرّفه الفقه التقليدي بمفهوم "الفخ" حيث يُنشئ صاحب الحق آلية تمنع المعتدي من إتمام اعتدائه دون أن يتجاوز ذلك إلى إلحاق ضرر زائد به، فلا يوجد ما يمنع أن يلجأ المدافع إلى وسائل آلية تعمل تلقائياً لحماية بياناته شريطة ألا تُفعل هذه الوسائل إلا عند تحقق الخطر فعلاً وأن يكون الأذى الناتج عنها متناسباً مع الخطر، أمّا إذا عملت الوسيلة الدفاعية دون وجود تهديد حقيقي أو ترتب عليها إيذاء غير متناسب مع الخطر فإنها تفقد صفة الدفاع الشرعي وتقوم بها المسؤولية الجزائية وفقاً للقواعد العامة.

وبناء على ما تقدم هناك العديد من الحجج التي تدعم مشروعية استخدام وسائل الحماية الإلكترونية في الدفاع الشرعي داخل الفضاء الرقمي:

١. الطبيعة الوقائية: تتميز الوسائل الآلية بأن وظيفتها الأساسية منع وقوع الضرر قبل حدوثه أو الحدّ من آثاره فهي لا تبشر اعتداءً جديداً وإنما تتعامل مع اعتداء قائم أو محتمل الوقوع، هذه الطبيعة الوقائية تجعلها أقرب إلى صورة التحصين والحماية وعدم اعتبارها صورة الإنتقام وهو ما ينسجم تماماً مع فلسفة الدفاع الشرعي التي تقوم على دفع الخطر وليس الإعتداء (43).

٢. تحقيق شرط التناسب: أحد أهم شروط الدفاع الشرعي هو أن يكون الرد متناسباً مع الخطر، وهنا تبرز ميزة الأنظمة الآلية إذ يمكن ضبطها تقنياً بحيث تستجيب لمستوى محدد من التهديد فإذا حاول المهاجم الدخول من منفذ غير مصرح به يمكن للنظام ببساطة أن يغلق هذا المنفذ أو يوقف البقاء المشبوه في النظام دون أن يلجأ إلى إجراءات أكثر خطورة كمسح بيانات الطرف الآخر أو إختراق جهازه، مما يجعل هذه الوسيلة أكثر دقة في تحقيق شرط التناسب (44).

٣. تفادي المخاطر الأخلاقية والقانونية: عندما يتدخل الفرد مباشرة في الرد على الهجمات الإلكترونية قد يدفعه الغضب أو الأرتباك إلى تجاوز حدود الدفاع والانتقال إلى الانتقام مثل محاولة إختراق جهاز المهاجم أو إتلاف بياناته وارتكاب جريمة مما يجعل فعله غير مشروع، في حين أن الأنظمة الآلية مبرمجة للعمل دون إنفعال أو نية إنتقامية مما يجعل فعلها أقرب إلى الفعل المحايد الذي يهدف فقط إلى حماية الحق المعتدى عليه دون تجاوز هذا الحد لتشكيل اعتداء أو جريمة يعاقب عليها القانون (45).

٤. تعتبر أنظمة منضبطة وملتزمة بالقيود: تقوم برمجة هذه الأنظمة (الوسائل) على صد الهجوم السيبراني الموجه للبيانات، ولكنها قد تفقد صفة الدفاع الشرعي إذا تجاوزت الحدود المشروعة إذا تم برمجتها بحيث تُتلف تلقائياً بيانات المهاجم حتى في حالة مجرد الاشتباه في هذه الحالة يُعد فعلها إعتداءً غير متناسب يترتب عليه مسؤولية قانونية.

بناء على ما تقدم فإننا نجد أنه يمكن القول بأن أنظمة الحماية الآلية الإلكترونية تُعدّ مثلاً على تطويع مفاهيم الدفاع الشرعي التقليدي لتناسب متطلبات العصر الرقمي، فهذه الوسائل لا تقوم على فكرة الرد أو الانتقام، وإنما على مبدأ الحماية الوقائية التي تمنع وقوع الاعتداء أو تحدّ من آثاره دون تجاوز إلى إيقاع ضرر غير مبرر بالمعتدي، وهذا

يجعلها أقرب إلى ما وصفه الفقه التقليدي بالفخ المشروع، حيث يُسمح لصاحب الحق بتهيئة وسائل دفاعية تلقائية تعمل فقط عند تحقق الخطر، بشرط أن تكون متناسبة مع حجم الاعتداء.

كما أن هذه الأنظمة تُسهم في تحقيق شرطَي الضرورة والتناسب اللذين يقوم عليهما الدفاع الشرعي، فهي قابلة للبرمجة بحيث لا تُلحق ضرراً يتجاوز المطلوب لحماية النظام، مثل إغلاق منفذ أو حجب الوصول دون إتلاف بيانات المهاجم أو التعدي على خصوصيته وبذلك تُجَنَّب الأفراد والمؤسسات أخطار الانزلاق إلى أفعال قد تُعتبر اعتداءً مضاداً غير مشروع.

إضافة إلى ذلك، فإن الاعتراف بمشروعية هذه الوسائل يعكس مرونة القواعد القانونية وقدرتها على مواكبة التطور التكنولوجي، حيث إن حماية الحقوق الرقمية في بيئة الهجمات السيبرانية المتصاعدة لا تقل أهمية عن حماية الحقوق المادية في الواقع التقليدي، وفي هذا السياق، يصبح الدفاع الآلي وسيلة متقدمة من وسائل الدفاع الشرعي، تحقق التوازن بين صون الحقوق الفردية من جهة؛ والحفاظ على الاستقرار القانوني ومنع الفوضى السيبرانية من جهة أخرى. ومن ثم، يمكن القول إن أنظمة الحماية الإلكترونية تُجسّد صورة حديثة من الدفاع الشرعي، تتماشى مع المبادئ العامة للقانون، وتستجيب في الوقت ذاته للتحديات العملية والأمنية التي تفرضها البيئة الرقمية، مما يفتح المجال أمام المشرع لتقنينها بوضوح باعتبارها إحدى الوسائل المشروعة لحماية الأصول الرقمية.

### المطلب الثالث : ضوابط وحدود منح الأفراد والمؤسسات حق الدفاع الشرعي.

تشكل الطبيعة العالمية للإنترنت تحدياً كبيراً في ملاحقة الجرائم السيبرانية، حيث تتجاوز هذه الجرائم الحدود الجغرافية التقليدية وتستلزم تعاوناً دولياً فعالاً بين الدول لتبادل المعلومات وملاحقة الجناة<sup>(46)</sup>، وقد سعت عدة دول إلى تعزيز إطارها القانوني والمؤسسي من خلال اتفاقيات دولية مثل: اتفاقية بودابست لمكافحة الجريمة الإلكترونية، التي وضعت آليات موحدة للتحقيق والتعاون القضائي.

وفي خِصَم هذه البيئة المعقدة، يبرز مفهوم الدفاع الشرعي الآلي كخيار وقائي يتيح للأفراد والمؤسسات حماية أنظمتهم الرقمية عبر وسائل تقنية آلية مثل الجدران النارية وأنظمة كشف الاختراق، بعيداً عن الردود الهجومية المباشرة التي قد تُعتبر في ذاتها جرائم<sup>(47)</sup>، ولكن الاعتراف بهذا الحق لا يمكن أن يكون مطلقاً، بل يجب أن يخضع لجملة من الضوابط القانونية تضمن تحقق شرط الخطر الحال، والتناسب في الرد، والرقابة المؤسسية، لتجنب تحوُّله إلى أداة للفوضى الإلكترونية أو العدوان الإلكتروني غير المشروع.

### الفرع الأول: تحدّيات الإقرار المطلق بالدفاع الشرعي الإلكتروني.

في ظل التطور التكنولوجي الذي يشهده العالم أصبحت الجرائم الإلكترونية تُمثل تهديداً خطيراً للأفراد والمؤسسات على حد سواء، ومع تزايد هذه التهديدات برزت فكرة "الدفاع الشرعي الآلي" كوسيلة لحماية الأنظمة والبيانات نظراً لأختلاف البيئة الرقمية عن الواقع المادي، ومع ذلك فإن الاعتراف المطلق بهذا الحق دون ضوابط قد يثير العديد من التحديات القانونية والأخلاقية، ومن أبرزها:

١. إمكانية خطأ الأنظمة البرمجيات في تحديد وجود الخطر: تعتمد الأنظمة الآلية على خوارزميات لمراقبة الشبكات والبيانات واكتشاف أي نشاط يُعد تهديدًا محتملاً<sup>(48)</sup>، ومع ذلك قد تُخطئ هذه الأنظمة أحياناً في التقييم؛ فقد تُعتبرُ عملية عادية جزءاً من الهجوم أو تفشل في رصد تهديد حقيقي، وإن هذه الأخطاء قد تؤدي إلى ردود فعل غير مناسبة، مثل تعطيل النظام أو حظر الخدمات الأساسية، مما قد يلحق الضرر بالأنظمة أو المستخدمين أنفسهم نتيجة للتوهم في الخطر .

٢. تجاوز حد التناسب: قد تقوم الأنظمة الآلية بالرد فوراً على الهجمات بشكل تتجاوز به حد الخطر الذي يهدد الأنظمة ، مثل تعطيل الخدمات أو مسح بيانات أكثر مما يستلزم تدخل الإنسان لإيقافها غالباً وقد يكون ذلك بعد فوات الأوان فلا يستطيع منعها قبل وقوع الضرر .

٣. برمجة الأنظمة الدفاعية على أفعال لا تتناسب مع الدفاع الشرعي: ففي بعض الحالات، قد تُبرمج الأنظمة الآلية على اتخاذ إجراءات هجومية بدلاً من الدفاعية، مثل الهجوم على أنظمة أخرى أو إتلاف بيانات مما يُعدّ تجاوزاً لحدود الدفاع الشرعي ، بحيث تعتمد هذه البرمجة على الهجوم العكسي المضاد بدلاً من صد الهجوم فقط .

٤. صعوبة تحديد هوية المعتدي: نتيجة لتطور البرمجيات والأنظمة لمراقبة الشبكات والبيانات ففي المقابل تتطور أنظمة التخفي بحيث يستخدم المهاجمون تقنيات لإخفاء هويتهم، مثل الشبكات الخاصة الافتراضية (VPN) أو الخوادم الوسيطة (Proxies) ما يجعل من الصعب تحديد الجاني بدقة، وبالتالي يزيد من احتمالية استهداف أطراف بريئة لا علاقة لها بالإعتداء<sup>(49)</sup>.

### الفرع الثاني: الضوابط المقترحة لتنظيم الدفاع الشرعي الآلي .

مع تزايد الاعتماد على الوسائل الرقمية في حياة الأفراد والمؤسسات، فقد أصبح من الضروري تطوير السياسة التشريعية للاعتراف بالدفاع الشرعي الآلي وذلك كضرورة لحماية الأنظمة والبيانات من الهجمات السيبرانية ، ومع ذلك فإن منح الأفراد والمؤسسات حق الرد التلقائي دون ضوابط قد يؤدي إلى تجاوزات كبيرة وغير محسوبة، مثل الإضرار بالأنظمة أو البيانات غير المستهدفة أو التصعيد غير المرغوب فيه، لذلك كان من الضروري وضع مجموعة من الضوابط القانونية والفنية التي تضمن ممارسة هذا الحق بشكل مسؤول وآمن، مع الحفاظ على مبدأ التناسب والتعاون مع الجهات الرسمية، ومن أهم هذه الضوابط التي يمكن اللجوء إليها لإقرار هذا الحق ما يلي:

١. إقتصار الحق في الدفاع على وسائل الدفاع الآلية: يجب أن يقتصر الدفاع الشرعي الإلكتروني على الوسائل التقنية ذات الطابع الوقائي، مثل الجدران النارية وأنظمة كشف ومنع الاختراق، دون اللجوء إلى الهجمات العكسية المضادة أو الردود الهجومية.

وإن هذا التوجه يهدف إلى تجنب المخاطر المرتبطة بالردود الهجومية، مثل الإضرار بالأنظمة غير المستهدفة أو تصعيد النزاعات الإلكترونية إلى مستويات غير مرغوب فيها أو رد الهجوم على جهات لا علاقة لها بالهجوم ، مما يعني عدم إمكانية الاعتراف بالدفاع العكسي المضاد وذلك على اعتبار انه يشكل جريمة أعتداء جديدة تتطلب المسألة الجزائية .

٢. الرقابة القانونية والمؤسسية: و تكون تلك الرقابة القانونية من خلال نصوص تشريعية واضحة تحدد الحالات المسموح بها والحدود التي يجب ألا تتجاوزها الوسائل الدفاعية، إضافة إلى تحديد شروط فعل الدفاع وطبيعة فعل الاعتداء الذي يميز الدفاع .

أما عن الرقابة المؤسسية فإنه يجب أن تكون هناك آليات رقابية تضمن التزام الأفراد والمؤسسات بالضوابط القانونية، وتمنع الاستخدام غير المشروع أو المفرط للوسائل الدفاعية، هذا يشمل إنشاء هيئات مستقلة لمراقبة الأنشطة الدفاعية وتوفير آليات للتظلم والمحاسبة في حال حدوث تجاوزات ، وهذا ما أقر به المشرع الأردني وبشكل جزئي عند إقرار قانون الأمن السيبراني رقم ( 16 ) لسنة 2019 والذي اعتبر مركز الأمن السيبراني هو الجهة المختصة بتلقي الشكاوى والإخبارات المتعلقة بالأمن السيبراني وحوادث الأمن السيبراني وله متابعتها واتخاذ الإجراء المناسب لمعالجتها ومنع حدوثها أو استمرارها وفق الصلاحيات الممنوحة له فقد نظم حماية البنى التحتية الحرجة الخاصة بمؤسسات الدولة وقطاعات الخدمات ومؤسسات القطاع الخاص دون أن ينظم تلك الحماية للأفراد<sup>(50)</sup>.

٣. إقرار المسؤولية عن التجاوز: في الدفاع الشرعي الآلي فإن تجاوز الضوابط والشروط القانونية لفعل الدفاع يترتب عليه قيام المسؤولية الجزائية والمدنية، تماماً كما في حالة الدفاع الشرعي التقليدي، وعليه يجب أن يكون هناك مساءلة قانونية للأفراد والمؤسسات التي تتجاوز الحدود المقررة له، مع فرض عقوبات مناسبة تتناسب مع جسامة المخالفة، وإن هذا يعزز من ثقافة الالتزام بالقانون ويمنع الفوضى أو التصرفات الفردية غير المسؤولة.

٤. التعاون مع السلطات المختصة: إن دور الأنظمة الآلية يقتصر على صدّ الهجوم الفوري، وعلى الصعيد الآخر يجب على الأفراد والمؤسسات الالتزام بإبلاغ الجهات الرسمية لمتابعة التحقيق والإجراءات القانونية<sup>(51)</sup>، وإن هذا التعاون يضمن تنسيق الجهود ويعزز من فعالية الإجراءات الأمنية والاستجابة السريعة للهجمات الإلكترونية.

#### الخلاصة :

يشكل الدفاع الشرعي في مواجهة الجريمة السيبرانية امتداداً لمبدأ قانوني تقليدي، إلا أنه يحتاج إلى مواءمة دقيقة مع طبيعة الفضاء الرقمي وخصائص الاعتداءات الحديثة، فالهجمات الإلكترونية تتميز بالسرعة والانتشار والقدرة على تجاوز الحدود المكانية والزمنية، مما يجعل الوسائل التقليدية للدفاع غير كافية بمفردها، وفي هذا الإطار يظهر الدفاع الشرعي الإلكتروني كأداة ضرورية لحماية الأفراد والمؤسسات، شريطة الالتزام بمبادئ الضرورة والتناسب، وتطبيق ضوابط دقيقة للوسائل الدفاعية الآلية، لتجنب الانزلاق إلى أعمال انتقامية أو غير قانونية.

من جهة أخرى، يظل الرد الفردي المباشر على الهجمات الإلكترونية خارج نطاق الدفاع الشرعي التقليدي، لما يترتب عليه من أخطار قانونية وأخلاقية وإمكانية تصعيد النزاع الإلكتروني ، وعليه فإن نجاح الدفاع الشرعي الرقمي يعتمد على وضع أطر قانونية واضحة وتوعية الأفراد والمؤسسات لضمان حماية الحقوق الرقمية بطريقة مشروعة وآمنة، دون التسبب بأضرار إضافية للغير أو مخالفة القانون.

في نهاية المطاف، يبرز الدفاع الشرعي الإلكتروني كخطوة أساسية نحو تأمين الفضاء الرقمي وحماية الحقوق الرقمية، مع التأكيد على أن فعاليته تتطلب التوازن بين الحماية القانونية والضوابط الأخلاقية، ومواكبة التشريعات الحديثة للتحديات الرقمية المتزايدة.

## أولاً : النتائج

١. إن الدفاع الشرعي التقليدي يمكن تطبيقه على الجريمة السيبرانية، لكن بشروط محددة تراعي طبيعة الاعتداء الرقمي والخصوصية التي تتمتع بها الجرائم الإلكترونية وذلك من خلال تمكين الأفراد من استخدام وسائل الدفاع الآلية لدفع الاعتداء عن بيئاتهم.
  ٢. إن الجرائم السيبرانية تتميز بسرعة تنفيذها وانتشار أثرها وقوة ضررها ، ما يستدعي وجود وسائل دفاع آلية تعمل على حماية البيانات في الفضاء الرقمي بشكل دائم.
  ٣. إن تحليل واقع الدفاع الشرعي قد أكد أن الرد الفردي المباشر على الهجمات الإلكترونية لا يُعتبر دفاعاً مشروعاً ويشكل تجاوزاً للحدود القانونية وجريمة مُجرمة بحد ذاتها.
  ٤. تبين أن التشريعات الأردنية المختصة في مجال الجرائم السيبرانية لا تلبي الاحتياجات القانونية، وخاصة فيما يتعلق بتنظيم الدفاع الشرعي، مما يجعل من الضروري وضع ضوابط قانونية واضحة لتنظيم هذا الحق بما يوازن بين حماية الحقوق ومنع الاعتداءات الإلكترونية، إلى جانب تطوير نصوص خاصة بالدفاع الشرعي الإلكتروني لتوفير حماية فعّالة للحقوق الرقمية.
- ثانياً: التوصيات .

١. نوصي المشرع الأردني بضرورة تبني فكرة الدفاع الشرعي في إطار تشريعي واضح يحدد شروط الدفاع الشرعي الإلكتروني والأدوات المسموح بها لممارسته في الفضاء الرقمي.
٢. ضرورة التدخل التشريعي لتحديد حدود الدفاع الآلي بحيث يقتصر على وسائل حماية مشروعة تمنع الضرر دون الإضرار بالغير، أي الاعتماد على فكرة الدفاع الشرعي الآلي دون الأخذ بفكرة الدفاع العكسي المضاد .
٣. اعتماد برامج منهجية لتعزيز الوعي القانوني حول الجرائم الإلكترونية وحقوق الدفاع الشرعي لدى الأفراد والمؤسسات.
٤. ضرورة إعداد برامج تدريبية للمؤسسات والأفراد لتدريبهم على استخدام وسائل الحماية الرقمية وفق معايير قانونية وأخلاقية.
٥. ضرورة الاستفادة من التجارب القانونية الدولية لتطبيق أفضل الممارسات في تنظيم الدفاع الشرعي في الفضاء الرقمي للأفراد والمؤسسات ، وخاصة ما تم الأخذ به في نطاق القانون الدولي لمواجهة الهجمات السيبرانية .

شكل كتابة المراجع:

المراجع العربية

1. حسن فياض، الهجمات السيبرانية من منظور القانون الدولي الإنساني، مجلة الدفاع الوطني اللبناني، ١١٤٤، ٢٠٢٠ .
2. د. محمود نجيب حسني ، شرح قانون العقوبات القسم العام ، ط4 ، دار النهضة العربية ، 1977.

3. طلال عبد حسين ، محمد عزت فاضل ، مشروعية الدفاع الآلي في القانون الجنائي ، مجلة الرافدين للحقوق ، جامعة الموصل ، مجلد 24 ، العدد 87 السنة 26 ، 2024 .
4. عماد حسين الفريجات، الجهود العربية والافريقية لمواجهة الجرائم الإلكترونية في الفترة ٢٠٢٣-٢٠١٠، مجلة ابن خلدون للدراسات والأبحاث، مج ٣، ع ٥٤ ، ٢٠٢٣ .
5. فاطمة الزباني، الجريمة الإلكترونية، مجلة منازعات الاعمال، ع ٩٢، المغرب، ٢٠٢٥ .
6. محمد حسن أحمد جاد، حق الدفاع الشرعي في مواجهة الهجمات السيبرانية في ضوء ميثاق الأمم المتحدة، مجلة الدراسات القانونية والأقتصادية، مج ١٠، ع ٤٤، ٢٠٢٤ .
7. محمد نعيم فرحات ، استخدام الأجهزة الآلية في الدفاع عن النفس والمال ، المجلة العربية للدراسات الأمنية ، جامعة نايف العربية للعلوم الأمنية ، مجلد 3 ، عدد 5 ، سبتمبر 1987 .
8. اسامة المناعسة، شرح قانون الجرائم الإلكترونية دراسة مقارنة، دار الثقافة، ط1، عمان ، 2025 .
9. باسل فريجات، الدفاع الشرعي في قانون العقوبات الأردني والمقارن، رسالة ماجستير، جامعة جرش، 2016 .
10. جمال محمد التلب، حق الدفاع الشرعي في الفقه الاسلامي والقانون: دراسة مقارنة، رسالة ماجستير، جامعة ام درمان الاسلامية، السودان ، 2015 .
11. د. أحمد بن علي الدباسي ، مبدأ التناسب في الدفاع الشرعي ضد الهجمات السيبرانية ، مجلة العلوم الشرعية ، جامعة القصيم ، مجلد 17 ، العدد 3 ، 2024 .
12. د. أنور مساعدا ، التناسب في الدفاع الشرعي : هل هو شرط إنشاء أو شرط استعمال ، المجلة القانونية والقضائية ، وزارة العدل ، مركز الدراسات القانونية والقضائية ، عدد 1 ، سنة 3 ، قطر 2009 .
13. د. علي جبار ، الدفاع الشرعي في التشريعات العربية ، المجلة الجنائية القومية ، المركز القومي للبحوث الاجتماعية والقانونية ، مجلد 53 ، عدد 3 ، 2010 .
14. د. فوزية عبد الستار ، بحث في الدفاع الشرعي ، مجلة الأمن والقانون ، أكاديمية شرطة دبي ، مجلد 2 ، عدد 1 ، 1994 .
15. د. يسر أنور علي ، الدفاع الشرعي : دراسة لمبدأ المشروعية ، المجلة الجنائية القومية ، المركز القومي للبحوث الإجتماعية ، مجلد 13 ، عدد 2 ، 1970 .
16. د.عبدالاله النوايسة، جرائم تكنولوجيا المعلومات، شرح الاحكام الموضوعية في قانون الجرائم الإلكترونية، دار وائل للنشر والتوزيع، ط1، عمان ، 2016 .
17. رزق أحمد سمودي ، حق الدفاع عن النفس نتيجة الهجمات الإلكترونية في ضوء القانون الدولي العام ، مجلة جامعة الشارقة للعلوم القانونية ، مجلد 15 ، عدد 2 ، ديسمبر 2018 .

18. سعيد السكوتي، حق الدفاع الشرعي: جوهره . حدوده . وخالات تجاوزه، مجلة الحقوق، محمد أوزيان ، ١٧٤، ٢٠١٤ .
19. عبد الرحمن المبيضين، الإطار القانوني للحقوق الرقمية: بين الحماية الدستورية والتنظيم الإداري، مجلة جامعة الزيتونة، مجلد 2 ، الاصدار 2 ، عمان، ٢٠٢٥ .
20. عبد الوهاب الطويل، الهجمات «السيبرانية»: حروب المستقبل مقال مجلة الاقتصاد الاسلامي، مج ٤٢، ٥٠١٤، ٢٠٢٢ .
21. غازي جرار، شرح قانون العقوبات القسم العام، ١٩٧٨ .
22. غسان عليان، الاثر القانوني المترتب على تجاوز حق الدفاع الشرعي، مجلة جامعة الاستقلال للأبحاث،  
جامعة الاستقلال - عمادة البحث العلمي والدراسات العليا ، مج ٩، ٢٤، ٢٠٢٤ .
23. كامل السعيد، شرح الاحكام العامة في قانون العقوبات دراسة مقارنة، المكتبة الوطنية ، عمان ١٩٩٨ ،
24. كمال بورحو، ماهية الجريمة الالكترونية وفق التشريعات العربية والاجتهادات الفقهية، مجلة الباحث للدراسات والابحاث القانونية والاقتصادية والعلوم الإنسانية والشرعية ،، ٧٨٤ ، 2025 .
25. ليلي خالد ، جريمة استيفاء الحق بالذات ، منشور على موقع موسوعة حماة الحق، 25 منشور بتاريخ ديسنبر 2020، <https://jordan-lawyer.com/>
26. محمد مسعودي، الدفاع الشرعي، رسالة ماجستير، المركز الجامعي، السودان، ٢٠١٥ .
27. محمود صالح محمد، الجريمة الالكترونية ومراحل تطورها، جامعة عدن . نيابة الدراسات العليا والبحث العلمي، ٥٢٤ ، ديسنبر 2024
28. نظام المجالي، شرح قانون العقوبات القسم العام، دار الثقافة ، ط ٨، عمان ، 2025

المراجع الأجنبية :

- 1- Alice M. Porch ( 2020 ) , Spoiling for a Fight: Hacking Back with the Active Cyber Defense Certainty Act, SOUTH DAKOTA LAW REVIEW, Vol .65, Iss . 3 .
- 2- Amjad A. Abdelkarim &Hebah H. Nasereddin. (2011), Intrusion Prevention System , INTERNATIONAL JOURNAL Of ACADEMIC RESEARCH Vol. 3. No.1. January, 2011, Part II .

- 3- Anthony Caldwell , Kevin Curran ,(2020 ) , A Critique of Active Defense or ‘Hack Back’, International Journal for Information Security Research (IJISR), Volume 10, Issue 1.
- 4- Dorothy E. Denning, (2007 ), The Ethics of Hacking Back: Cybersecurity and Active Network Defense, Carnegie Council for Ethics in International Affairs, p.2
- 5- Kesan, J. P., & Majuca, R. P. (2009). Hacking back: Optimal use of self-defense in cyberspace Chicago-Kent Law Review .
- 6-Nicholas Winstead , Hack-Back: Toward A Legal Framework For Cyber Self-Defense, June 26, 2020 ,American University .  
<https://www.american.edu/sis/centers/security-technology/hack-back-toward-a-legal-framework-for-cyber-self-defense.cfm>
- 7- Nobles, C. (2023). A Scoping Review of Hacking Back in Cybersecurity. Illinois Institute of Technology .
- 8- Schmitt, M. N., & Vihul, L. (2021). Autonomous cyber capabilities under international law .
- 9- Shackelford, S. J. (2018). When is cyber defense a crime? Evaluating active cyber defense measures under the Budapest Convention , Chicago Journal of International Law .

#### الهوامش:

- (1) عبد الوهاب الطويل، المحجمات «السيبرانية»: حروب المستقبل، مقال مجلة الاقتصاد الاسلامي، مج ٤٢، ع ٥٠١٤، ٢٠٢٢، ص 1 .
- (2) نظام المجالي، شرح قانون العقوبات اقسام العام، دار الثقافة، ط ٨، ص ٢٠٢
- (3) نظام المجالي، المرجع السابق، ص ١٧١
- (4) سعيد السكوتي، حق الدفاع الشرعي: جوهره - حدوده - وخالات تجاوزه، مجلة الحقوق، ع ١٧٤، ٢٠١٤، ص ٣٦٨
- (5) د. يسر أنور علي ، الدفاع الشرعي : دراسة لمبدأ المشروعية ، المجلة الجنائية القومية ، المركز القومي للبحوث الإجتماعية ، مجلد 13 ، عدد 2 ، 1970 ، ص 302.
- (6) باسل فريجات، الدفاع الشرعي في قانون العقوبات الأردني والمقارن، رسالة ماجستير، جامعة جرش، ص ٢٠
- (7) المرجع السابق، ص ٩
- (8) محمد مسعودي، الدفاع الشرعي، رسالة ماجستير، المركز الجامعي، السودان، ص ٤، ٢٠١٥
- (9) غسان عليان، الاثر القانوني المترتب على تجاوز حق الدفاع الشرعي، مجلة جامعة الاستقلال للأبحاث، مج ٩، ع ٢٤، ٢٠٢٤، ص ٣٣
- (10) انظر المادة ( 2/60 ) من قانون العقوبات والمتعلقة بجواز الدفاع الشرعي عن الشخص المعنوي .
- (11) نظام المجالي، مرجع سابق، ص ٢٠٧ .
- (12) كامل السعيد، شرح الاحكام العامة في قانون العقوبات دراسة مقارنة، ١٩٩٨، ص ١٤٤ .
- (13) د. فوزية عبد الستار ، بحث في الدفاع الشرعي ، مجلة الأمن والقانون ، أكاديمية شرطة دبي ، مجلد 2 ، عدد 1 ، 1994 ، ص 127 .
- (14) غازي جرار، شرح قانون العقوبات القسم العام، ١٩٧٨، ص ١٣٠
- (15) د. علي جبار ، الدفاع الشرعي في التشريعات العربية ، المجلة الجنائية القومية ، المركز القومي للبحوث الإجتماعية والقانونية ، مجلد 53 ، عدد 3 ، 2010 ، ص 141 .

- (16) تعرف الحقوق الرقمية بأنها "الحق في الافادة من كافة الخدمات التي تقدمها شبكة المعلومات وتأمين الوصول المستمر لها وضمان عدم حرمان المستفيدين منها بأي شكل" عبد الرحمن المبيضين، الإطار القانوني للحقوق الرقمية: بين الحماية الدستورية والتنظيم الاداري، مجلة جامعة الزيتونة، عمان، ٢٠٢٥، ص ٢٣
- (17) نظام المجالي، مرجع سابق، ٢٣٢
- (18) كامل السعيد، مرجع سابق، ص ١٦٩؛ د. أنور مساعدة، التناسب في الدفاع الشرعي : هل هو شرط إنشاء أو شرط استعمال، المجلة القانونية والقضائية، وزارة العدل، مركز الدراسات القانونية والقضائية، عدد 1، سنة 3، قطر 2009، 240.
- (19) جمال محمد التلب، حق الدفاع الشرعي في الفقه الاسلامي والقانون: دراسة مقارنة، رسالة ماجستير، جامعة ام درمان الاسلامية، السودان، ص ١١٦
- (20) انظر المادة ( 3/60 ) من قانون العقوبات .
- (21) د. أحمد بن علي الدباسي، مبدأ التناسب في الدفاع الشرعي ضد الهجمات السبرانية، مجلة العلوم الشرعية، جامعة القصيم، مجلد 17، العدد 3، ص 3329.
- (22) رزق أحمد سمودي، حق الدفاع عن النفس نتيجة الهجمات الإلكترونية في ضوء القانون الدولي العام، مجلة جامعة الشارقة للعلوم القانونية، مجلد 15، عدد 2، ديسمبر 2018، ص 356.
- (23) عبدالاله النوايسة، جرائم تكنولوجيا المعلومات، شرح الاحكام الموضوعية في قانون الجرائم الالكترونية، دار وائل للنشر والتوزيع، ط1، ص ٢٩.
- (24) المرجع السابق، ص ٤١.
- (25) اسامة المناعسة، شرح قانون الجرائم الالكترونية دراسة مقارنة، دار الثقافة، عمان، ط1، 2025، ص ٢١.
- (26) عبد الاله النوايسة، المرجع السابق، ص ٧٨.
- (27) كمال بورحو، ماهية الجريمة الالكترونية وفق التشريعات العربية والاجتهادات الفقهية، مجلة الباحث للدراسات والبحوث القانونية، ع ٧٨، ص ٢٤.
- (28) اسامة المناعسة، المرجع السابق، ص ٤٩.
- (29) كمال بورحو، المرجع السابق، ص ٢٧.
- (30) من خصائص الجرائم الالكترونية انها "جرائم ناعمة" لا تتطلب اي نوع من المجهودات العضلية مثل الجرائم التقليدية كجرائم القتل والايذاء والسرقه؛ أنظر محمود صالح محمد، الجريمة الالكترونية ومراحل تطورها، جامعة عدن. نيابة الدراسات العليا والبحث العلمي، ع ٥٢، ص ١٦٩.
- (31) فاطمة الزباني، الجريمة الالكترونية، مجلة منازعات الاعمال، ع ٩٢، المغرب، ٢٠٢٥، ص ١٨٠.
- ((32)) Dorothy E. Denning, (2007), The Ethics of Hacking Back: Cybersecurity and Active Network Defense, Carnegie Council for Ethics in International Affairs, p.2
- (( 33)) Nobles, C. (2023). A Scoping Review of Hacking Back in Cybersecurity. Illinois Institute of Technology ,p.18 .
- (34) Anthony Caldwell , Kevin Curran ,(2020) , A Critique of Active Defense or ‘Hack Back’, International Journal for Information Security Research (IJISR), Volume 10, Issue 1,p.960 .
- (35) انظر مادة (١٦) من قانون الأمن السيبراني رقم ١٦ لسنة ٢٠١٩

((36)) Nicholas Winstead , Hack-Back: Toward A Legal Framework For Cyber Self-Defense, June 26, 2020 ,American University .

<https://www.american.edu/sis/centers/security-technology/hack-back-toward-a-legal-framework-for-cyber-self-defense.cfm>

(37) يعرف استيفاء الحق بالذات بأنه: أن يأخذ الشخص حقه بنفسه أو أخذ الحق عنوة، دون اللجوء إلى السلطات القضائية المخولة باقتضاء الحقوق سواءً كانت مدنية أم جزائية . انظر ليلي خالد ، جريمة استيفاء الحق بالذات ، منشور على موقع موسوعة حماة الحق، 25 منشور بتاريخ ديسمبر 2020 ، <https://jordan-lawyer.com/> ، أنظر المادة (٢٣٣) قانون العقوبات رقم 16 لسنة 1960 .

(38) طلال عبد حسين ، محمد عزت فاضل ، مشروعية الدفاع الآلي في القانون الجنائي ، مجلة الراصد للحقوق ، جامعة الموصل ، مجلد 24 ، العدد 87 السنة 26 ، 2.24 ، ص 169 .

(39) د. محمد نجيب حسني ، شرح قانون العقوبات القسم العام ، ط4 ، دار النهضة العربية ، 1977 ، ص 213 .

(40) محمد نعيم فرحات ، استخدام الأجهزة الآلية في الدفاع عن النفس والمال ، المجلة العربية للدراسات الأمنية ، جامعة نايف العربية للعلوم الأمنية ، مجلد 3 ، عدد 5 ، سبتمبر 1987 ، ص 110 .

(41) د. محمد نعيم فرحات ، مرجع سابق ، ص 110 .

Intrusion Prevention ((42)) Amjad A. Abdelkarim &Hebah H. Nasereddin. (2011),  
INTERNATIONAL JOURNAL Of ACADEMIC RESEARCH Vol. 3. , System  
p. 432 . , No.1. January, 2011, Part II

(43) حسن فياض، الهجمات السيبرانية من منظور القانون الدولي الإنساني، مجلة الدفاع الوطني اللبناني، ع ١١٤، ٢٠٢٠

(44) محمد حسن أحمد جاد، حق الدفاع الشرعي في مواجهة الهجمات السيبرانية في ضوء ميثاق الأمم المتحدة، مجلة الدراسات القانونية والاقتصادية، مج ١٠، ع ٤٤، ص ١٦٣٤، ٢٠٢٤

((45)) Alice M. Porch ( 2020 ) , Spoiling for a Fight: Hacking Back with the Active Cyber Defense Certainty Act, SOUTH DAKOTA LAW REVIEW, Vol .65, Iss . 3, p.479 .

(46) عماد حسين الفريجات، الجهود العربية والافريقية لمواجهة الجرائم الإلكترونية في الفترة ٢٠٢٣.٢٠١٠، مجلة ابن خلدون للدراسات والأبحاث، مج ٣، ع ٥٤، ص ١٩٠، ٢٠٢٣

Shackelford, S. J. (2018). When is cyber defense a crime? Evaluating active cyber defense (47) measures under the Budapest Convention , Chicago Journal of International Law, p.19

Schmitt, M. N., & Vihul, L. (2021). Autonomous cyber capabilities under international (48) law, p.19

Kesan, J. P., & Majuca, R. P. (2009). Hacking back: Optimal use of self-defense in (49) cyberspace Chicago-Kent Law Review , p.12

(50) أنظر قانون الأمن السيبراني المادة (٨)، الفقرة (أ)، البند (١).

(51) أنظر قانون الأمن السيبراني، المادة (٨)، الفقرة (ب)، البند (٣).