جامعـــة النجاح الوطنية

كلية الدراسات العليـــا

الحماية الجنائية للمستهلك في السوق الالكتروني

إعداد

مأمون طاهر محمد سمارة

إشراف

الـــدكتور عبد اللطيف ربايعة

قدمت هذه الرسالة استكمالا لمتطلبات الحصول على درجة الماجستير فـــي القـــانون الجنائي بكلية الدراسات العليا في جامعة النجاح الوطنية، نابلس، فلسطين.

2025

الحماية الجنائية للمستهلك في السوق الالكتروني

إِعداد

مأمون طاهر محمد سمارة

نوقشت هذه الرسالة بتاريخ 2025/12/14م، وأجيزت:

د. عبد اللطيف رباعية	
المشرف الرئيسي	**التوقيع**
د. محمد شتية	
الممتحن الخارجي	**التوقيع**
د. نور عدس	
الممتحن الداخلي	**التوقيع**

الإهداء

إلى مَن هما سبب وجودي، وبوصلة طريقي في هذه الحياة.. إلى سندي ومنبع العطاء والرضا.. **والدي**

العزيز ووالدتي الغالية (أطال الله في عمرهما).

إلى عائلتي وإخوتي وأخواتي.. الذين شاركوني عناء المسير، وكانوا لي خير رفيق وسند في دروب

العلم.

إلى كل من آمن بي، وشجعني بكلمة طيبة أو دعوة صادقة في ظهر الغيب.

إلى أرواح الشهداء الأبرار،

وإلى وطني الغالي فلسطين.. أرض الصمود ومنارة الحق.

إلى سدنة العدالة، وحماة الحقوق، وإلى كل طالب علم يسعى بجهده لخدمة الإنسانية وإرساء قواعد

القانون.

أهدي هذا الجهد المتواضع.

الشكر

الحمد لله الذي بنعمته تتم الصالحات، وبفضله وتوفيقه أُنجز هذا العمل، والصلاة والسلام على خير معلمٍ للبشرية محمد وعلى آله وصحبه أجمعين.. وبعد،،

فإن من باب الوفاء لأهل الفضل، أتقدم بخالص شكري وعظيم امتناني إلى جامعة النجاح الوطنية، هذا الصرح العلمي الشامخ، وإلى كلية الدراسات العليا وكافة أساتذة كلية القانون الذين نهلنا من علمهم الوافر.

ويطيب لي أن أخص بالشكر والتقدير أستاذي الفاضل الدكتور عبد اللطيف ربايعة، الذي شرفني بقبول الإشراف على هذه الدراسة، فكان نعم الموجّه والمحرّض على الإبداع، وأشكره على سعة صدره، ونصائحه العلمية القيمة، ودقته التي كانت مناراً لي في رحلة إعداد هذا البحث.

كما أتقدم بجزيل الشكر وعميق العرفان إلى السادة أعضاء لجنة المناقشة الموقرين:

الدكتور محمد شتية (الممتحن الخارجي) والدكتورة نور عدس (الممتحن الداخلي)

الذين تفضلوا بقبول مناقشة هذه الرسالة، وإثرائها بملاحظاتهم العلمية القيمة التي لا شك ستكون إضافة نوعية لهذا الجهد المتواضع.

كما لا يفوتني أن أتقدم بالشكر والامتنان إلى كل المؤسسات والجهات التي يسرت لي سبل الحصول على المعلومات، وإلى كل من قدم لي يد العون والمساعدة، أو كلمة تشجيعٍ صادقة طوال فترة الدراسة.

وختاماً، أسأل الله العلي القدير أن يكون هذا العمل خالصاً لوجهه الكريم، ولبنةً نافعةً في صرح المعرفة القانونية.

الباحث/ مأمون طاهر محمد سمارة

الإقرار

أنا الموقع أدناه مقدم الرسالة التي تحمل عنوان:

الحماية الجنائية للمستهلك في السوق الإلكتروني

أقر بأن ما اشتملت عليه هذه الرسالة هي نتاج جهدي الخاص، باستثناء ما تمت الإشارة اليه حيثما ورد، وأن هذه الرسالة ككل أو أي جزء منها لم يقدم من قبل لنيل أية درجة أو لقب علمي أو بحثي لدى أية مؤسسة تعليمية أو بحثية أخرى.

اسم الطالب: **مأمون طاهر محمد سمارة**

التوقيع: ***مأمون سمارة***

التاريخ: **2025/12/14م**

فهرس المحتويات

الحماية الجنائية للمستهلك في السوق الالكتروني

إعداد

مأمون طاهر محمد سمارة

إشراف

عبد اللطيف ربايعة

الملخص

تناولت هذه الدراسة موضوع "الحماية الجنائية للمستهلك في السوق الإلكتروني" في ظل التحول الرقمي المتسارع وما فرضه من أنماط مستحدثة من المعاملات الإلكترونية. وقد كشفت الدراسة عن اختلال واضح في مراكز القوة بين أطراف العلاقة التعاقدية، مما جعل المستهلك الإلكتروني الطرف الأضعف والأكثر عرضة للاعتداءات الرقمية.

ولتحقيق أهداف الدراسة، اعتمد الباحث المنهج الوصفي التحليلي؛ من خلال رصد وتحليل الإطار التشريعي الفلسطيني الناظم لحماية المستهلك الإلكتروني في شقيه الموضوعي والإجرائي، مع التركيزعلى تقييم مدى كفاية قواعد التجريم والعقاب، وآليات الملاحقة الجنائية، وقواعد الإثبات في مواجهة الجرائم الإلكترونيةالمستحدثة.

وخلصت الدراسة إلى نتيجة جوهرية مفادها أن التشريعات الفلسطينية النافذة –وعلى الرغم مما تتضمنه من نصوص تُجرّم الأفعال الضارة بالمستهلك– إلا أنها تعاني من التشتت وغياب التخصص التشريعي، ولا تواكب الطبيعة الخاصة للسوق الإلكتروني والدليل الرقمي؛ الأمر الذي يحدُّ من فاعلية الردع الجنائي ويُضعف حماية المستهلك الإلكتروني، لا سيما في مرحلتي الملاحقة والإثبات.

وتوصي الدراسة بضرورة سنِّ تشريع فلسطيني موحّد وشامل لحماية المستهلك الإلكتروني، يتضمن تنظيماً متكاملاً للجوانب الموضوعية والإجرائية، ويقرُّ تعريفاً صريحاً للمستهلك الإلكتروني، ويحدد صور الجرائم الرقمية الواقعة عليه، وينظم آليات الملاحقة الجنائية والإثبات الرقمي؛ بما يكفل تعزيز الثقة في السوق الإلكتروني الفلسطيني.

الكلمات المفتاحية: الحماية الجنائية، المستهلك الإلكتروني، الأدلة الرقمية، السوق الإلكترونية، التجزئة التشريعية، القانون الموضوعي والإجرائي.

المقدمة

أفرز التحول الرقمي المتسارع في العالم المعاصر أنماطًا جديدة من المعاملات التجارية، تمثلت في توسّع السوق الإلكتروني واعتماد الأفراد بشكل متزايد على الوسائل الرقمية في إبرام العقود والحصول على السلع والخدمات. وذلك لا يتم إلا عبر شبكة الإنترنت (ابراهيم، 2008، صفحة 38) وقد أسهم هذا التطور في تسهيل التعاملات وتسريعها، إلا أنه في المقابل أوجد مخاطر قانونية مستحدثة، جعلت المستهلك الإلكتروني أكثر عرضة للاعتداءات، نظرًا لطبيعة البيئة الرقمية وما تتسم به من تعقيد تقني، وغياب الاتصال المباشر، وتفاوت واضح في مراكز القوة بين أطراف العلاقة التعاقدية.

وفي هذا السياق، يبرز المستهلك الإلكتروني بوصفه الطرف الأضعف في السوق الرقمي، إذ يواجه صورًا متعددة من الجرائم الإلكترونية، فضلًا عن صعوبة ملاحقة مرتكبي هذه الجرائم وإثباتها. الأمر الذي يفرض على المشرّع إقرار حماية جنائية فعّالة، لا تقتصر على تجريم الأفعال الضارة بالمستهلك، وإنما تمتد إلى تنظيم آليات الملاحقة والإثبات بما يضمن صون حقوقه وتحقيق العدالة الجنائية.

وعلى الصعيد الفلسطيني، تتوزع الحماية الجنائية للمستهلك الإلكتروني بين عدة تشريعات، من بينها قانون حماية المستهلك رقم (21) لسنة 2005، وقرار بقانون الجرائم الإلكترونية رقم (10) لسنة 2018، وقانون العقوبات، وقانون المواصفات والمقاييس، وغيرها من القوانين ذات الصلة. ورغم ما توفره هذه التشريعات من أساس قانوني للحماية، إلا أنها جاءت متفرقة وغير موحّدة، ولم تُصغَ في معظمها لمعالجة خصوصية السوق الإلكتروني وما يفرضه من تحديات موضوعية وإجرائية، الأمر الذي يثير تساؤلات حول مدى كفايتها وفعاليتها في حماية المستهلك الإلكتروني.

وانطلاقًا من ذلك، تهدف هذه الدراسة إلى بحث الحماية الجنائية للمستهلك في السوق الإلكتروني، من خلال دراسة الجوانب الموضوعية المتمثلة في التجريم والعقاب، والجوانب الإجرائية المتعلقة بالملاحقة الجنائية والإثبات، في ضوء التشريعات الفلسطينية النافذة. كما تسعى الدراسة إلى بيان أوجه القصور في

الإطار القانوني القائم، وخصوصية الجرائم الرقمية التي تستهدف المستهلك، وصولًا إلى استخلاص نتائج علمية وتقديم توصيات عملية تسهم في تطوير منظومة الحماية الجنائية، بما يحقق التوازن بين فعالية الردع الجنائي، وحماية الحقوق والحريات، وتعزيز الثقة في السوق الإلكتروني.

أهمية الدراسة

تكمن أهمية هذه الدراسة في البعد الذي تُحظى به على المستويين العملي والعلمي، إذ تستمد هذه الدراسة أهميتها من تزايد الاعتماد على المعاملات التجارية الإلكترونية وما أفرزه ذلك من مخاطر قانونية مستحدثة تهدد حقوق المستهلك الإلكتروني، وذلك في ظل التطور التكنولوجي المتسارع وتعدد صور الجرائم الإلكترونية غير التقليدية. فمن الناحية النظرية، تهدف الدراسة إلى بيان مدى مواءمة وكفاية النصوص التشريعية الفلسطينية النافذة في توفير الحماية الجنائية للمستهلك الإلكتروني، والكشف عن أوجه القصور التشريعي في هذا المجال. أما من الناحية العملية، فتبرز أهمية الدراسة في إبراز دور التشريع الجزائي في تجريم الأفعال الماسة بالمستهلك الإلكتروني وفرض العقوبات الرادعة بحق المخالفين، بما يحقق الردع العام ويعزز الأمن القانوني والثقة في البيئة الرقمية. كما تسهم في تعزيز الأمن القانوني وبناء الثقة في البيئة الرقمية، وتحفيز المشرع الفلسطيني على تطوير الإطار التشريعي بما يواكب خصوصية السوق الإلكتروني ويحمي المستهلك من الاعتداءات الرقمية.

اشكالية الدراسة

تتمثل إشكالية هذه الدراسة في مدى كفاية وفعالية الحماية الجنائية، بشقيها الموضوعي والإجرائي، التي توفرها التشريعات للمستهلك في السوق الإلكتروني، ومدى قدرتها على مواكبة التحديات القانونية والتقنية المستجدة في البيئة الرقمية.

لذلك فإن التساؤل الرئيسي للدراسة: ما مدى كفاية وفعالية الحماية الجنائية التي تقرّها التشريعات الفلسطينية للمستهلك في السوق الإلكتروني، في ضوء التحديات القانونية والتقنية التي تفرضها الجرائم الرقمية؟

وينبثق عن هذا التساؤل مجموعة من الأسئلة الفرعية المتتابعة:

- ما هو الإطار المفاهيمي والتنظيمي للحماية الجنائية للمستهلك في البيئة الإلكترونية؟
- ما أبرز الجرائم الإلكترونية التي قد يتعرض لها المستهلك، وما عناصرها وأركانها القانونية؟
- ما طبيعة العقوبات الجنائية التي يقرّها القانون الفلسطيني لردع الجرائم الواقعة على المستهلك في السوق الرقمي؟
- كيف تُنظم الإجراءات الجنائية المتعلقة بضبط الجرائم الإلكترونية، وملاحقة مرتكبيها، ومحاكمتهم؟
- ما مدى خصوصية قواعد الإثبات في الجرائم التي تستهدف المستهلك الإلكتروني، وما التحديات العملية المتعلقة بالدليل الرقمي؟
- ما هو النظام الذي اتبعه المشرّع الفلسطيني في الاعتداد بالأدلة الرقمية، وكيفية تكيفه مع خصوصية الإثبات في الجرائم الإلكترونية؟
- هل تلبّي التشريعات الفلسطينية النافذة متطلبات الحماية الجنائية الفعالة للمستهلك من الناحيتين الموضوعية والإجرائية في السوق الإلكتروني، أم أنّ ثمة حاجة لتطوير تشريعي وإجرائي؟

أهداف الدراسة

لكل عمل هدف، ولا بد من اتباع الأساليب العلمية لتحقيق الأهداف المرجوة، وهذه الدراسة تسعى إلى تحقيق عدد من الأهداف المتمثلة في التالي:

- إثراء المعرفة القانونية في مجال الحماية الجنائية للمستهلك الإلكتروني، وبيان خصوصيتها في ظل تطور المعاملات الإلكترونية.
- إيضاح التنظيم القانوني الناظم لحماية المستهلك الإلكتروني في التشريعات ذات الصلة، ولا سيما قوانين حماية المستهلك والمعاملات الإلكترونية والجرائم الإلكترونية.
- تقييم مدى كفاية النصوص التشريعية الجزائية المقررة لحماية المستهلك في السوق الإلكتروني، من خلال تحليل نصوص التجريم والعقاب.

- رصد أوجه القصور والثغرات القانونية في التشريعات النافذة، وقياس مدى مواءمتها لطبيعة الجرائم الإلكترونية التي تستهدف المستهلك.
- بناء إطار مفاهيمي واضح وشامل للحماية الجنائية للمستهلك الإلكتروني، عبر تعريف المصطلحات الأساسية وبيان خصائصها المميزة عن الحماية التقليدية.
- تقديم توصيات وحلول عملية قابلة للتطبيق لتعزيز الحماية الجنائية للمستهلك الإلكتروني، بما يشمل تطوير الآليات الإجرائية والفنية لكشف الجرائم الإلكترونية وجمع الأدلة الرقمية، مع ضمان احترام الحقوق الدستورية والقانونية لجميع الأطراف.

المنهج المستخدم في الدراسة

اعتمد الباحث في هذه الدراسة على المنهج الوصفي التحليلي، بغية الإلمام بكافة الجوانب المتعلقة بموضوع هذه الدراسة المتمثل في الحماية الجنائية للمستهلك الإلكتروني، وذلك من خلال الاستناد على النصوص التشريعية ذات الصلة الصادرة عن المشرع الفلسطيني ومع الاستعانة بالأحكام القضائية والإحصائيات الصادرة عند الضرورة، وأيضاً الاستناد على الدراسات الفقهية والابحاث العلمية وصولاً إلى الأهداف التي ترمي إليها هذه الدراسة.

خطة الدراسة

تتطلب دراسة هذا الموضوع بيان الحماية الجنائية الموضوعية للمستهلك الالكتروني ومن ثم توضيح الحماية الجنائية الاجرائية للمستهلك في السوق الالكتروني، لذا رأينا تقسيم هذه الدراسة على النحو التالي:

الفصل الاول: الحماية الجنائية الموضوعية للمستهلك الالكتروني

- المبحث الأول :التنظيم القانوني والمفاهيمي للحماية الجنائية للمستهلك في السوق الإلكتروني
- المطلب الأول :التأصيل القانوني لمفهوم المستهلك الإلكتروني

- المطلب الثاني :التنظيم القانوني للحماية الجنائية للمستهلك في السوق الإلكتروني
- المبحث الثاني : التجريم والعقاب في الجرائم الماسة بالمستهلك الإلكتروني
- المطلب الأول: صور الجرائم الماسة بالمستهلك الإلكتروني وأركانها
- المطلب الثاني :العقوبات المنصوص عليها في القوانين لحماية المستهلك الإلكتروني
- الفصل الثاني: الحماية الجنائية الاجرائية للمستهلك في السوق الالكتروني.
- المبحث الأول : خصوصية الملاحقة الإجرائية
- المطلب الأول : خصوصية إجراءات البحث والتحري
- المطلب الثاني : خصوصية اجراءات التحقيق
- المبحث الثاني :خصوصية الإثبات الجنائي في حماية المستهلك الإلكتروني
- المطلب الأول: مركز المستهلك الإلكتروني في الإثبات الجنائي
- المطلب الثاني :خصوصية الاثبات الجنائي في الجرائم الواقعة على المستهلك الالكتروني

الفصل الأول
الحماية الجنائية الموضوعية للمستهلك الإلكتروني

يُعد هذا الفصل حجر الأساس لفهم الإطار القانوني للحماية الجنائية الموضوعية للمستهلك الإلكتروني، إذ يتناول تحليل القواعد القانونية التي تُحدّد الأفعال المجرّمة في مجال المعاملات الإلكترونية، والعقوبات المقرّرة لها من منظور المشرّع، بما يحقق الردع العام والخاص، ويسهم في الوقاية من الجرائم قبل وقوعها. وتكتسب هذه الحماية أهمية متزايدة في ظل التحوّل الرقمي المتسارع الذي شهدته فلسطين والعالم، وما ترتّب عليه من توسّع في أنماط الاستهلاك الإلكتروني، قابله ازدياد في المخاطر والاعتداءات التي تهدد حقوق المستهلك في البيئة الرقمية. وتُعدّ الحماية الجنائية للمستهلك في البيئة الإلكترونية جزءًا من الحماية الجنائية الاقتصادية، التي تهدف إلى صيانة الثقة في التعاملات الحديثة وضبط السلوك الإجرامي المتصل بها. (فهمي، 2008، صفحة 322)

ويركّز هذا الفصل على بيان مدى قدرة التشريعات الفلسطينية على توفير حماية جنائية فعّالة للمستهلك الإلكتروني داخل السوق الرقمي، من خلال تحليل الأسس القانونية التي اعتمدها المشرّع في تنظيم هذه الحماية، ومدى كفايتها في تحقيق التوازن بين أطراف العلاقة الاستهلاكية الإلكترونية.

وانطلاقًا من ذلك، قُسِّم هذا الفصل على النحو الآتي:

- المبحث الأول: التنظيم القانوني والمفاهيمي للحماية الجنائية للمستهلك في السوق الإلكتروني.
- المبحث الثاني: التجريم والعقاب في الجرائم الماسة بالمستهلك الإلكتروني.

المبحث الأول

التنظيم القانوني والمفاهيمي للحماية الجنائيةللمستهلك في السوق الإلكتروني

يهدف هذا المبحث إلى التطرق للحماية الجنائية المقرّرة للمستهلك في السوق الإلكتروني، من خلال الوقوف على موقف المشرّع الفلسطيني والنصوص القانونية ذات الصلة، مع الاستئناس بالاتجاهات المقارنة عند الضرورة. ويُقصد بالحماية الجنائية، في هذا السياق، مجموعة من القواعد القانونية التي تُحدّد الأفعال المجرّمة وتُنظّم آليات إنفاذها، بما يكفل حماية إرادة المستهلك وبياناته وخصوصيته في البيئة الرقمية. وهو ما أكّد عليه عدد من الفقهاء في إطار تأصيل الحماية الجنائية الإلكترونية، باعتبارها ضرورة تفرضها تطورات العصر الرقمي وخصوصية المعاملات الإلكترونية(الزغبي، 2016، صفحة 45)،

وانطلاقًا من ذلك، قُسِّم هذا المبحث على النحو الآتي:

- المطلب الأول: التأصيل القانوني لمفهوم المستهلك الإلكتروني.
- المطلب الثاني: التنظيم القانوني للحماية الجنائية للمستهلك في السوق الإلكتروني.

المطلب الأول

التأصيل القانوني لمفهوم المستهلك الإلكتروني

يهدف هذا المطلب إلى تأصيل المفاهيم القانونية الأساسية التي تحكم علاقة المستهلك بالسوق الإلكتروني، وذلك من خلال بيان مفهوم المستهلك الإلكتروني، وتحديد مضمون حماية المستهلك، وتعريف السوق الإلكتروني بوصفه بيئةً تعاقدية رقمية ذات خصوصية قانونية. وتتبع أهمية هذا التأصيل القانوني من كونه يشكّل الأساس الذي تُبنى عليه قواعد الحماية القانونية، ولا سيما الحماية الجنائية، إذ لا يمكن تحديد نطاق التجريم أو آليات الردع دون وضوح المركز القانوني للمستهلك وحدود السوق التي يتحرك ضمنها (قرار بقانون رقم 15 لسنة 2017؛ قانون حماية المستهلك رقم 21 لسنة 2005؛(حجازي، شرح قانون العقوبات: القسم العام، 2007، الصفحات 45–48).وبناءً على ما سبق، سيتم تقسيم هذا المطلب إلى ثلاثة فروع متتالية، وذلك على النحو الآتي:

الفرع الأول

الإطار القانوني لمفهوم المستهلك في عقد الاستهلاك الإلكتروني

يُعد عقد الاستهلاك الإلكتروني الإطار القانوني الذي تتجسد من خلاله علاقة المستهلك بالسوق الرقمي، ويُشكّل تحديد مفهوم هذا العقد ومركز المستهلك فيه مدخلًا أساسيًا لفهم نطاق الحماية الجنائية المقرّرة له. وقد اختلف الفقه القانوني في تعريف العقد الإلكتروني؛ فذهب بعض الفقهاء إلى تعريفه بأنه اتفاق يتلاقى فيه الإيجاب والقبول عبر وسائل التبادل الإلكترونية، بينما عرّفه اتجاه آخر بأنه العقد الذي يتم فيه تلاقي الإيجاب والقبول عبر شبكة اتصالات دولية باستخدام التبادل الإلكتروني للبيانات بقصد إنشاء التزامات تعاقدية.

ويُستفاد من هذه التعريفات أن المعيار الجوهري في العقد الإلكتروني لا يكمن في طبيعته القانونية، وإنما في الوسيلة التي يتم بها انعقاده(حجازي، شرح قانون العقوبات: القسم العام، 2007، الصفحات 33–36).

ويتميّز العقد الإلكتروني عن العقد التقليديبغياب مجلس العقد المادي، حيث يتم التعبير عن الإرادة عن بُعد بواسطة وسائط إلكترونية دون التقاء فعلي بين أطراف العلاقة التعاقدية، الأمر الذي يجعل الوسيلة الإلكترونية العنصر الفارق والأساسي بين النوعين، وينعكس على قواعد الإثبات والتنفيذ وتحديد المسؤولية، لا سيما في ظل البيئة الرقمية التي تتسم بالسرعة والتعقيد وصعوبة التحقق، ويتميز عن العقد المبرم عبر الهاتف والذي يكون شفاهةً بين أطرافه لعدم حضور المتعاقدين في مجلس العقد بسبب البعد المكاني (الأودن، 2005، صفحة 28).

واذا كانت وسائل التعبير عن الإرادة كما نشأت القول والفعل والإشارة والكتابة والسكوت، فإن الثورة المعلوماتية جعلت الإنسان يعيش بالأذهان أكثر من اتصاله بالأبدان، وأصبح يعيش معلوماتياً بعد أن كان يعيش مطعوماتياً(عطار، 2009، صفحة 98).

وعلى الصعيد التشريعي، عرّف القرار بقانون رقم (15) لسنة 2017 بشأن المعاملات الإلكترونية الفلسطيني العقد الإلكتروني بأنه: «اتفاق يتم بين شخصين أو أكثر بوسائل أو وسائط إلكترونية». كما تناول التوجيه الأوروبي EU/83/2011 المتعلق بحماية المستهلك في العقود المبرمة عن بُعد العقد الإلكتروني بوصفه أحد صور هذه العقود، حيث عرّفته المادة (2) منه بأنه العقد المتعلق بالسلع أو الخدمات المبرم بين مورد ومستهلك دون التواجد المادي والمتزامن للطرفين، باستخدام وسيلة أو أكثر من وسائل الاتصال عن بُعد حتى لحظة إتمام التعاقد (قرار بقانون رقم 15 لسنة 2017، المادة 1).

مما رتب على هذا التنوع في صور العقود الإلكترونية اختلاف الفقه والتشريع بشأن إيراد تعريفاً لعقد الاستهلاك الإلكتروني، إلا أنه يمكن استخلاص إطار عام لانعقاده يتمثل في توافق إرادتي المستهلك والمهني باستخدام وسيلة إلكترونية بقصد إحداث أثر قانوني.

وبناءً عليه، يمكن تعريف عقد الاستهلاك الإلكتروني بأنه: العقد الذي يُبرم بين مستهلك من جهة، ومهني أو مزوّد من جهة أخرى، يتعهد بموجبه المهني بتوريد سلعة أو تقديم خدمة لإشباع حاجة استهلاكية

مقابل ثمن، عبر إحدى الوسائل الإلكترونية (حوى، 2012، صفحة 19)، في حين عرفه آخرون بأنه العقد الذي يتلاقى فيه الإيجاب بالقبول عبر شبكة اتصالات دولية باستخدام التبادل الإلكتروني للبيانات بقصد إنشاء التزامات تعاقدية(العجمي، 2011، صفحة 24).

ويُبرز هذا التعريف الطبيعة غير المتكافئة لعقد الاستهلاك الإلكتروني، إذ يقوم بين طرفين متفاوتين في المركز القانوني والاقتصادي والتقني؛ مستهلك يُعد الطرف الضعيف يسعى لإشباع حاجاته الشخصية أو العائلية، ومهني يتمتع بتفوّق معلوماتي وتقني واقتصادي، وهو ما يبرّر تدخل المشرّع بقواعد خاصة لحماية المستهلك(السنهوري، 1963، صفحة 437).

وانطلاقًا من ذلك، تبرز أهمية تحديد مفهوم المستهلك الإلكتروني ذاته. فقد عرّف قانون حماية المستهلك الفلسطيني رقم (21) لسنة 2005 المستهلك بأنه: «كل من يشتري سلعة أو يستفيد من خدمة لإشباع حاجاته الشخصية أو العائلية»، ويكتسي هذا التعريف أهمية في تحديد نطاق الحماية القانونية (وفقًا لقانون حماية المستهلك الفلسطيني رقم (21) لسنة 2005 (المادة 1))، وعرّف نفس ذاك القانون السلعة على أنها:" كل منتج صناعي أو زراعي أو نصف مصنع وأية مادة أخرى تعتبرها الوزارة سلعة لغايات تطبيق أحكام هذا القانون .

ويذهب الاتجاه الضيق في الفقه إلى قصر وصف المستهلك على من يتعاقد لإشباع حاجاته الشخصية أو العائلية دون أي هدف مهني أو تجاري، ويُستبعد من نطاقه من يشتري بقصد إعادة البيع أو تحقيق الربح. ووفق هذا الاتجاه يُعرّف المستهلك الإلكتروني بأنه من يستخدم الإنترنت لأغراض استهلاكية غير تجارية(منصور، 2007، صفحة 44)، وبعد النظر في تعريف المستهلك الذي قد عرفه المشرع الفلسطيني نجده قد أخذ باتجاه المفهوم الضيق .

في المقابل، يتبنى الاتجاه الواسع مفهومًا أشمل للمستهلك، فيعتبره كل من يستخدم سلعة أو خدمة ولو في إطار نشاط مهني، متى كان التعاقد خارج نطاق تخصصه الفني، غير أن هذا الاتجاه يُؤخذ عليه مساواته بين المستهلك والمزوّد في بعض الحالات(سلامة، 2009، الصفحات 18–20).

ويرى الباحث ضرورة تبنّي مفهوم مركّب ومتوازن للمستهلك الإلكتروني، يجمع بين الاتجاهين، بحيث يُعد مستهلكًا كل من يتعاقد لإشباع حاجاته الشخصية أو العائلية، وكذلك حاجاته المهنية غير المتخصصة، متى لم يكن الهدف تحقيق ربح أو ممارسة نشاط تجاري(عبدالرحمن، 2018، الصفحات 67–69).

وخلاصة القول، إن تحديد مفهوم المستهلك في عقد الاستهلاك الإلكتروني يُعد الأساس الذي تُبنى عليه الحماية الجنائية، ويبرز الحاجة إلى تطوير الإطار التشريعي الفلسطيني بما يواكب خصوصية البيئة الرقمية (حوى، 2012، صفحة 19).

ومن هنا، يرى الباحث ضرورة أن يُعيد المشرّع الفلسطيني النظر في موقفه، بحيث يعتمد تعريفًا متوازنًا للمستهلك يجمع بين المفهومين الضيّق والواسع، بدلاً من الاقتصار على أحدهما. فالمستهلك، في هذا السياق، هو كل من يشتري سلعة أو خدمة لإشباع حاجاته الشخصية أو العائلية أو حتى المهنية غير الربحية. كما يوصي الباحث بأن يُبنى تعريف المستهلك في عقود الاستهلاك الإلكتروني على أساس معيار اختلال التوازن المعلوماتي والتقني بين أطراف العلاقة التعاقدية، لا على الصفة المهنية المجردة للمتعاقد. فكل من يبرم عقدًا عبر الوسائط الإلكترونية خارج نطاق خبرته الفنية، ودون قصد تحقيق الربح، يظل الطرف الأضعف الذي يستحق الحماية القانونية المقرّرة للمستهلك. ويُعد هذا التوجّه أكثر انسجامًا مع الأهداف الحمائية للتشريع، ومع خصوصية البيئة الرقمية، ويؤكد الحاجة إلى إطار تشريعي فلسطيني أدق وأكثر شمولًا لعقود الاستهلاك الإلكتروني.

الفرع الثاني

مفهوم حماية المستهلك

يحتاج المستهلك إلى الحماية على الصعيدين الوطني والدولي، وإن هذه الحماية تنبع من أن المستهلك هو الطرف الضعيف في العملية التعاقدية، لأن رغبة التجار ومقدمي السلع في الربح السريع دفعتهم لاتباع وسائل وطرق غير مشروعة، ومن هنا ظهرت حاجة ملحة لتوفير الحماية للمستهلك الإلكتروني (الزغول، 2023، صفحة 15).

وترتيباً على ما تقدم، فإن حماية المستهلك تُشكل بحد ذاتها منظومة متكاملة من القواعد القانونية والتشريعات والإجراءات التنظيمية التي تهدف إلى ضمان حقوق المستهلك عند حصوله على المنتجات أو السلع أو الخدمات بطريقة آمنة وسليمة، بما يتوافق مع المواصفات المتفق عليها بين المستهلك والمزوّد. وتهدف هذه الحماية أيضًا إلى تحقيق الشفافية والصدق في التعامل التجاري بين الطرفين، وتقليل المخاطر التي قد يتعرض لها المستهلك، سواء في السوق التقليدي أو السوق الإلكتروني، مثل الغش، أو الاحتيال، أو الإذعان في العقود .

ومن هنا فإن الباحث يرى لضمان حماية المستهلك لابد من وضع قواعد إجرائية وواجبات تنظيمية لتكفل سلامة وجودة المنتجات والخدمات المتداولة في الأسواق، ومن ثم تعزيز ثقة المستهلك وتنمية شعوره بالأمان القانوني، لا سيما في البيئة الرقمية حيث تتزايد المخاطر التقنية.

وفي فلسطين، عرّفت جمعية حماية المستهلك الفلسطيني حماية المستهلك بأنها عملية مستمرة تهدف إلى توعية المستهلك بحقوقه، وتقديم الدعم والاستشارات القانونية له، مع العمل على توفير بيئة تسوق آمنة ومحمية بالقانون. كما أكدت الجمعية على دور المستهلك في دعم المنتجات الوطنية لتعزيز الاقتصاد المحلي (جمعية حماية المستهلك الفلسطيني، 2026).

وقد أظهرت الدراسات الحديثة، مثل دراسة حماية المستهلك في التسويق الإلكتروني، أن حماية المستهلك تمثل إطارًا قانونيًا يهدف إلى تأمين حقوقه وضمان سلامة التعاملات التجارية عبر الإنترنت، مع مقارنة التنظيم القانوني الفلسطيني بالتشريعات المقارنة لمواجهة المخاطر المتجددة في البيئة الرقمية (المناصرة، 2023، صفحة 24).

وتشمل حقوق المستهلك الأساسية، وفق التشريعات المحلية والدولية، الحق في الأمان، والحصول على معلومات دقيقة وشفافة، والاختيار الحر دون تضليل أو غبن، والحق في التعويض عن الأضرار التي قد تلحق به نتيجة أي انتهاك لحقوقه الاستهلاكية. وتزداد أهمية هذه الحقوق في مجال الاستهلاك الإلكتروني، نظرًا لخصوصية المعاملات الرقمية ومخاطرها التقنية (وزارة الاقتصاد الفلسطينية الوطني، 2021).

وبالرغم من تعدد التشريعات الفلسطينية ذات الصلة بحماية المستهلك، مثل قانون حماية المستهلك رقم 21 لسنة 2005، وقانون المواصفات والمقاييس، وقانون الجرائم الإلكترونية، إلا أن هذا التنوع قد يؤدي أحيانًا إلى تشتيت الحماية وإرباك التطبيق القضائي والرقابي. ومن الأجدر توحيد الأحكام في تشريع جامع يتضمن بابًا خاصًا بالمستهلك الإلكتروني، بدل الاكتفاء بالقياس على قواعد حماية المستهلك التقليدي .

نستخلص مما سبق أن مختلف التعريفات تتفق على أن حماية المستهلك تشكل منظومة من القواعد القانونية والإجراءات الهادفة إلى صون حقوق المستهلك وحمايته من المخاطر التي قد يتعرض لها في علاقاته التعاقدية، وهو توجه محمود يعكس إدراك المشرّع لأهمية حماية الطرف الضعيف في العلاقة الاستهلاكية.

غير ان التركيز التشريعي ينصرف في الغالب إلى حماية المستهلك من أفعال المزوّد أو التاجر، في حين يلاحظ قصورٌ نسبي في معالجة المخاطر الناشئة عن تدخل أطراف ثالثة في البيئة الرقمية، كحالات

الاختراق والاحتيال الإلكتروني وسرقة البيانات، وهي مخاطر لا تقل جسامة عن المخاطر التقليدية، وقد تؤدي إلى زعزعة ثقة المستهلك بالتجارة الإلكترونية وتنعكس سلبًا على الاقتصاد الوطني.

ومع التطور التكنولوجي المتسارع واتساع نطاق المعاملات الإلكترونية، يرى الباحث أن هناك حاجة ملحة إلى تطوير قانون حماية المستهلك وسن مواد خاصة من شأنها تُعزز حماية المستهلك الإلكتروني من المخاطر المستمرة والمتجددة في الفضاء الرقمي، مما ينتج عنه ثقة المستهلك في التجارة الإلكترونية.

الفرع الثالث

مفهوم السوق الإلكتروني

يُقصد بالسوق الإلكتروني الفضاء الافتراضي غير المادي الذي يُتاح فيه عرض وبيع وتقديم السلع والخدمات باستخدام شبكة الإنترنت كوسيلة أساسية للتواصل والتعاقد بين مختلف الأطراف، مثل المستهلكين والتجار والمؤسسات، عبر منصات إلكترونية ومواقع وتطبيقات رقمية، دون الحاجة لوجود مادي مباشر لطرفي العلاقة التعاقدية. ويُعد هذا السوق امتدادًا للتجارة التقليدية إلى بيئة رقمية تتيح تنفيذ المعاملات التجارية بكفاءة وسرعة، وتفتح آفاقًا واسعة للتبادل التجاري المحلي والدولي بسهولة أكبر(الحميدي، 2019، صفحة 85).

وتتميز البيئة الرقمية للسوق الإلكتروني بأنها واسعة ومتعددة المخاطر في الوقت نفسه، حيث يصعب حصر المخاطر أو ضبطها من خلال القواعد التقليدية وحدها نظرًا لوجود مواقع وهمية ومنصات غير مرخّصة قد تهدف إلى الاحتيال أو سرقة البيانات أو النصب على المستهلكين. وهذا الواقع يتطلب تكامل الأطر القانونية والتنظيمية لحماية الحقوق وتوفير بيئة تجارية آمنة وموثوقة(الحياة، 2026).

وقد أشارت الدراسات المحلية إلى أن التجارة الإلكترونية في فلسطين تشهد نموًا ملحوظًا في السنوات الأخيرة، مع توسّع استخدام الإنترنت وزيادة الاعتماد على الشراء الإلكتروني، ما يجعل السوق

الإلكتروني ضرورة اقتصادية واجتماعية مع تحديات قانونية تحتاج تنظيماً واضحًا يعطي حماية للمستهلكين في هذه البيئة الرقمية (رؤيا الثاقبة، 2026).

وقد عرّف بعض الباحثين السوق الإلكتروني بأنه منصة تجارية افتراضية تتيح إبرام التعاملات الرقمية عن بُعد بين المستهلك والتاجر، سواء كان هذا الأخير محليًا أو من خارج الحدود، مع التأكيد على أهمية تطوير القواعد القانونية التي تحكم هذه البيئة الرقمية لضمان حماية حقوق المستهلكين، مثل حق المعاينة قبل الشراء، وحق العدول، واسترداد الثمن، والتعويض عن الأضرار في حال عدم مطابقة السلعة أو الخدمة للمواصفات المتفق عليها (الجهاز المركزي للإحصاء الفلسطيني و وزارة الاتصالات وتكنولوجيا المعلومات، 2021).

وبناءً على ذلك، يمكن القول إن السوق الإلكتروني يمثل تطورًا جوهريًا في طبيعة التجارة الحديثة لما يوفره من خصائص إيجابية مثل سهولة الوصول إلى المنتجات وتنوع الخيارات مع القدرة على مقارنة السلع وتخفيض التكاليف، إلا أنه يقابله سلبيات ومخاطر قانونية وتقنية حقيقية تلزم تطوير التشريعات القائمة ووضع إطار قانوني متكامل يوفر حماية فعّالة للمستهلك في المعاملات الإلكترونية، ويضمن تحقيق نسبة وتناسب بين تشجيع التجارة الإلكترونية وحماية المستهلك في البيئة الإلكترونية.

ويرى الباحث، في ضوء ما تقدم، أن السوق الإلكتروني يُعد منصة افتراضية غير مادية تمثل تحولًا جوهريًا في طبيعة التجارة الحديثة، لما يترتب عليه تنوع في السلع والخدمات، وسهولة الوصول إليها، وإمكانية المقارنة بين الخيارات المختلفة، بما يسهم في تعزيز الكفاءة الاقتصادية وتوسيع نطاق التبادل التجاري.

غير أن هذه المزايا تقابلها مخاطر قانونية وتقنية حقيقية، في مقدمتها غياب المعاينة المادية المباشرة، وصعوبة التحقق من جودة السلع، وارتفاع مخاطر الغش والاحتيال والقرصنة وسرقة البيانات، الأمر الذي قد يُفضي إلى الإضرار بالمستهلك وتقويض ثقته بالتجارة الإلكترونية.

وانطلاقًا من ذلك، يؤكد الباحث ضرورة تطوير إطار قانوني متكامل يراعي خصوصية السوق الإلكتروني، ويوفر حماية فعّالة للمستهلك، بما يحقق التوازن بين تشجيع التجارة الإلكترونية وضمان حقوق المستهلك في البيئة الرقمية.

المطلب الثاني

التنظيم القانوني للحماية الجنائية للمستهلك في السوق الإلكتروني

يُقصد بالتنظيم القانوني للحماية الجنائية الموضوعية للمستهلك الإلكتروني مجموعة القواعد القانونية والتشريعات الجنائية التي تهدف إلى حماية المستهلك من الأفعال غير المشروعة التي قد يتعرض لها أثناء إبرام وتنفيذ المعاملات التجارية الإلكترونية، ولا سيما الجرائم التي تمس أمن التعاملات الرقمية، مثل الغش والاحتيال الإلكتروني والاعتداء على البيانات والمعلومات الشخصية. وتستند هذه الحماية إلى تجريم الأفعال التي تُلحق ضررًا بالمستهلك وفرض الجزاءات الجنائية الرادعة بحق مرتكبيها، بما يضمن تحقيق الردع العام والخاص وحماية الطرف الضعيف في العلاقة الاستهلاكية (سرور، 1989، ص.46)،وبناءً على ماسبق، سيتم تقسيم هذا المطلب إلى فرعين متتاليين على النحو الآتي:

الفرع الأول

الأساس التشريعي للحماية الجنائية للمستهلك الإلكتروني.

أولًا/ قانون حماية المستهلك الفلسطيني:

يشكّل قانون حماية المستهلك رقم (21) لسنة 2005 الإطار التشريعي الأساسي لحماية المستهلك في فلسطين، إذ أقرّ مجموعة من الحقوق الجوهرية التي يتمتع بها المستهلك، من أبرزها الحق في الحصول على سلع وخدمات مطابقة للمواصفات المتفق عليها، والحق في الاختيار الحر، والحصول على معلومات صحيحة وواضحة، إضافة إلى الحق في التعويض عن الأضرار الناتجة عن أي إخلال بحقوقه الاستهلاكية. كما تضمّن القانون نصوصًا جزائية تُجرّم الأفعال التي تنتهك هذه الحقوق وتفرض عقوبات

على مرتكبيها، بما يعكس توجه المشرّع نحو إقرار حماية جنائية للمستهلك، وإن كان ذلك في إطار عام لا يراعي خصوصية البيئة الإلكترونية بشكل مباشر.

إلى جانب ذلك فإن المشرع الفلسطيني قد أوجب على المهني أو المزود او المروج تلك السلع والخدمات بعدم تضمين إعلانه التجاري أية معلومات أو بيانات من شأنها تضلل أو تخدع المستهلك، وبدوره لم يقف على هذا الحد بل رتب على الإخلال بما تقدم عقوبة السجن لمدة ثلاث سنوات أو بغرامة تُقدر بثلاث دينار أردني أو ما يعادلها بالعملة المتداولة قانوناً أو بكلتا العقوبتان وذلك بحسب نص المادة الثامنة والعشرين من قانون حماية المستهلك.

ثانيًا/ قانون الجرائم الإلكترونية ودوره في حماية المستهلك:

يُعد القرار بقانون رقم (10) لسنة 2018 بشأن الجرائم الإلكترونية من أهم التشريعات التي تسهم في حماية المستهلك الإلكتروني بصورة غير مباشرة، من خلال تجريم الأفعال التي تُرتكب عبر الوسائل الإلكترونية، كجرائم الاحتيال الإلكتروني، وانتهاك الخصوصية، وسرقة البيانات. وقد عرّف القانون البيانات الإلكترونية بأنها كل ما يمكن تخزينه أو معالجته أو إنشاؤه أو نقله باستخدام تكنولوجيا المعلومات، وقرّر عقوبات جزائية بحق من يعتدي عليها، الأمر الذي يوفّر مظلة جنائية تحمي المستهلك من المخاطر الرقمية التي قد يتعرض لها أثناء تعامله في السوق الإلكتروني.

ثالثًا /دور قانون المواصفات والمقاييس في ضمان سلامة المنتجات:

أسهم قانون المواصفات والمقاييس الفلسطيني رقم (6) لسنة 2000 في تعزيز حماية المستهلك من خلال وضع معايير وضوابط فنية تُلزم المزوّدين والتجّار بالالتزام بمواصفات محددة للسلع والخدمات المتداولة في السوق الفلسطيني. وتكمن أهمية هذا القانون في كونه يوفّر حماية وقائية للمستهلك، من خلال ضمان سلامة المنتجات والحد من المخاطر الصحية والمالية والاقتصادية، وهو ما ينعكس أيضًا على المعاملات الإلكترونية، رغم أن نصوصه لم تُصغَ خصيصًا لمعالجة خصوصية السوق الإلكتروني .

رابعًا/ موقف الفقه والدراسات القانونية:

أشارت العديد من الدراسات القانونية إلى وجود قصور تشريعي في تنظيم حماية المستهلك الإلكتروني في فلسطين، إذ أكدت بعض الدراسات، مثل دراسة الطبيعة الخاصة لحماية المستهلك الإلكتروني ضمن قواعد القانون الدولي الخاص، أن غياب ضوابط واضحة لتحديد القانون الواجب التطبيق على العقود الإلكترونية غالبًا ما يؤدي إلى تطبيق قانون المزوّد، وهو ما ينتقص من الحماية التي يفترض أن يتمتع بها المستهلك بوصفه الطرف الأضعف في العلاقة التعاقدية. كما خلصت دراسات أخرى، كدراسة الحماية المدنية للمستهلك في عملية التسوق الإلكتروني في القانون الفلسطيني، إلى ضرورة استحداث نصوص قانونية خاصة تنظم عملية التسوق الإلكتروني وتراعي خصوصية هذا النوع من المعاملات. لاسيما وأن موضوع التعاقد على الإنترنت والحماية المدنية للمستهلك في العقد الإلكتروني أصبحت تمثل جانباً هاماً من اهتمام الحكومات في سعيها لتنظيم تعاملات شعبها .

خامسًا / تقييم الإطار التشريعي القائم:

يتضح من استعراض التشريعات الفلسطينية ذات الصلة بحماية المستهلك أن المشرّع الفلسطيني أولى هذا المجال اهتمامًا ملحوظًا، إلا أن هذا الاهتمام اتّسم بالتجزئة والتشعيب، حيث تتوزع الحماية بين عدة قوانين، مثل قانون حماية المستهلك، وقانون المواصفات والمقاييس، وقانون الجرائم الإلكترونية، وقانون المعاملات الإلكترونية، وقانون العقوبات. ويؤدي هذا التعدد إلى صعوبة التكييف القانوني للأفعال الجرمية، وإرهاق الجهات القضائية والرقابية، فضلًا عن اتساع مجال التفسير والقياس، بما قد ينعكس سلبًا على فعالية الحماية الجنائية للمستهلك الإلكتروني (سرور، 1989، صفحة 47).

وبناءً على ذلك فإن الباحث يرى أن التشريعات الفلسطينية الحالية تمثل خطوة إيجابية نحو إقرار حماية جنائية للمستهلك، إلا أنها تعاني من قصور واضح في مواكبة خصوصية السوق الإلكتروني، سواء من حيث غياب تعريف صريح للمستهلك الإلكتروني، أو من حيث عدم تنظيم المسائل الجوهرية للعقد الإلكتروني، كحق المعاينة، والعدول، والاستبدال، وحماية البيانات الشخصية. كما أن تشتيت الأحكام بين

عدة تشريعات يُضعف من فعالية الحماية ويستدعي تدخلًا تشريعيًا موحدًا، من خلال سن قانون جامع يتضمن تنظيمًا خاصًا وشاملًا لحماية المستهلك الإلكتروني، بما يحقق التوازن بين تشجيع التجارة الإلكترونية وضمان حماية فعّالة للمستهلك في البيئة الرقمية.

الفرع الثاني

التطبيقات الجنائية لحماية المستهلك الإلكتروني في القوانين النافذة

يُقصد بالتطبيقات الجنائية لحماية المستهلك الإلكتروني مجموعة النصوص الجزائية الواردة في القوانين النافذة، التي تُجرِّم الأفعال الضارة بحق المستهلك، وتُقرِّر لها عقوبات جنائية، سواء وردت هذه النصوص في قوانين عامة أو في تشريعات خاصة، وذلك بهدف تحقيق الردع وحماية الثقة في المعاملات الإلكترونية.

أولًا / تطبيقات قانون العقوبات في حماية المستهلك الإلكتروني

رغم أن قانون العقوبات رقم (16) لسنة 1960 لم يُنظَّم خصيصًا لمواجهة الجرائم الإلكترونية، إلا أن نصوصه العامة ما زالت تُطبَّق على العديد من الأفعال التي تمسّ المستهلك الإلكتروني، وذلك عن طريق التكييف القانوني التقليدي. فقد جرّم المشرّع أفعال الغش في البضاعة من حيث النوع أو الكمية أو الجودة، وقرّر لها عقوبات سالبة للحرية أو مالية، وهي نصوص يمكن تطبيقها على حالات الغش التي تقع عبر المنصات الإلكترونية عند عرض منتجات مخالفة للمواصفات المعلن عنها.

كما تناول قانون العقوبات جريمة الاحتيال القائمة على استعمال طرق احتيالية أو بيانات كاذبة بقصد الاستيلاء على مال الغير، وهي صورة تنطبق على الإعلانات الإلكترونية المضللة والمواقع الوهمية التي تستهدف المستهلكين. كذلك يمكن تكييف بعض صور الاعتداء على بيانات المستهلك ضمن جريمة خيانة الأمانة متى توافرت أركانها القانونية (قانون العقوبات، 1960، الصفحات 417–422).

ثانيًا / التطبيقات الجنائية في قانون حماية المستهلك

شكّل قانون حماية المستهلك رقم (21) لسنة 2005 أداة جزائية مباشرة لحماية المستهلك، من خلال تجريم عدد من الأفعال التي تمسّ سلامته وحقوقه الأساسية، مثل بيع سلع فاسدة أو منتهية الصلاحية، أو تقديم بيانات غير صحيحة عن طبيعة السلع والخدمات. وتُعد هذه الجرائم قابلة للتطبيق على البيئة الإلكترونية متى تم تسويق هذه السلع أو الخدمات عبر الإنترنت، ولو لم ينص القانون صراحة على المستهلك الإلكتروني.

وقد قرّر المشرّع عقوبات جزائية تهدف إلى ردع المزوّدين المخالفين وضمان حماية المستهلك، إلا أن هذه النصوص بقيت مرتبطة بمنطق السوق التقليدي، ولم تتناول خصوصيات المعاملات الإلكترونية كالإعلانات الرقمية أو منصات التجارة الإلكترونية بشكل تفصيلي (قانون حماية المستهلك الفلسطيني، 2005، الصفحات 4–21).

ثالثًا/ الدور الجزائي لقانون المواصفات والمقاييس

يُسهم قانون المواصفات والمقاييس الفلسطيني رقم (6) لسنة 2000 في حماية المستهلك من خلال إقرار جزاءات جنائية بحق كل من يخالف المواصفات المعتمدة للسلع والمنتجات. وتكمن أهمية هذا القانون في كونه يُشكّل خط دفاع وقائي يحول دون تداول منتجات غير مطابقة للمواصفات، سواء في السوق التقليدي أو الإلكتروني.

غير أن تطبيق هذا القانون في مجال التجارة الإلكترونية يواجه صعوبات عملية تتعلق بآليات الرقابة وضبط المخالفات، لا سيما عندما يتم تسويق السلع عبر منصات خارج الإقليم الفلسطيني (قانون المواصفات والمقاييس الفلسطيني رقم 6 لسنة 2000، المواد 23–27).

رابعًا /التطبيقات الجنائية في قرار الجرائم الإلكترونية

يُعد القرار بقانون رقم (10) لسنة 2018 بشأن الجرائم الإلكترونية الإطار التشريعي الأوضح في مجال حماية المستهلك الإلكتروني، إذ تناول بشكل مباشر جرائم الاحتيال الإلكتروني، وإنشاء المواقع الوهمية،

وانتحال الهوية، والدخول غير المشروع إلى البيانات والمعلومات الشخصية. وقد قرّر المشرّع عقوبات جزائية تهدف إلى حماية مستخدمي الوسائل الإلكترونية، وفي مقدمتهم المستهلك الإلكتروني، من المخاطر الرقمية المتزايدة.

ويمتاز هذا القرار بأنه انتقل بالحماية من منطق القياس على الجرائم التقليدية إلى منطق التجريم المباشر للأفعال الإلكترونية، إلا أن نطاقه بقي عامًا ولم يُخصِّص أحكامًا تفصيلية تتعلق بحقوق المستهلك الإلكتروني بوصفه طرفًا ضعيفًا في العلاقة التعاقدية (القرار بقانون رقم 10 لسنة 2018، المواد 9، 11، 14).

خامسًا / التقييم العام للتطبيقات الجنائية القائمة

يتضح من استعراض القوانين النافذة أن الحماية الجنائية للمستهلك الإلكتروني في فلسطين ما زالت تعتمد على مزيج من النصوص العامة والخاصة، دون وجود تنظيم جنائي متكامل ومخصص لهذا النوع من الاستهلاك. كما أن العقوبات المقررة في بعض النصوص لا تواكب جسامة الأضرار الناجمة عن الجرائم الإلكترونية، ولا تحقق الردع الكافي في ظل التطور التقني المتسارع(سرور، 1989، صفحة 48).

ومن هنا فإن الباحث يرى أن التطبيقات الجنائية الحالية، رغم أهميتها، لا توفر حماية كافية للمستهلك الإلكتروني، لكونها جاءت متناثرة بين عدة قوانين، وتعتمد في كثير من الأحيان على القياس والتكييف التقليدي. ويؤكد الباحث الحاجة إلى سن تشريع خاص يتناول الجرائم التي تستهدف المستهلك الإلكتروني بصورة مباشرة، مع إعادة النظر في العقوبات المقررة بما يحقق الردع العام والخاص، ويعزز الثقة في السوق الإلكتروني الفلسطيني.

المبحث الثاني

التجريم والعقاب في الجرائم الماسة بالمستهلك الإلكتروني

يقصد بشرعية العقوبة خضوع التجريم والعقاب لنص قانوني يقرّره المشرّع، إذ يقوم مبدأ الشرعية الجنائية على قصر سلطة التجريم والعقاب على السلطة التشريعية، مع حصر دور القاضي في تطبيق العقوبة المقررة قانوناً دون إنشاء أو توسّع(المنشاوي، 2015، صفحة 37).ويُعد هذا المبدأ من المبادئ القانونية الراسخة ذات القيمة الدستورية، لِما يمثّله من ضمانة أساسية لحقوق الأفراد وحرياتهم، ومفاده أنه لا جريمة ولا عقوبة إلا بنص قانوني.

وفي إطار حماية المستهلك في البيئة الإلكترونية، تسعى التشريعات الحديثة إلى إقرار حماية جزائية فعّالة من خلال تجريم الأفعال التي قد يتعرض لها المستهلك الإلكتروني وفرض عقوبات تحقق الردع العام والخاص. ويُجسّد التشريع الفلسطيني هذا التوجّه باعتماده مبدأ شرعية الجرائم والعقوبات في نصوصه الدستورية والقانونية، الأمر الذي يقتضي تحديد صور الجرائم الواقعة على المستهلك الإلكتروني وبيان أركانها والعقوبات المقررة لها، خاصةً في ظل الطبيعة المتخصصة والمتجددة للجرائم الإلكترونية.

ولكل ما سبق سوف نقوم بتقسيم هذا المبحث إلى مطلبين على النحو التالي:

- المطلب الأول : صور الجرائم الماسة بالمستهلك الإلكتروني وأركانها.
- المطلب الثاني: العقوبات المنصوص عليها في القوانين لحماية المستهلك الالكتروني.

المطلب الأول

صور الجرائم الماسة بالمستهلك الإلكتروني وأركانها

تشتمل الجرائم الماسة بالمستهلك الإلكتروني على سلوكيات وأفعال إجرامية تعتمد على الوسائل الإلكترونية بشتى طرقها وباختلاف انواعها والتي تمس أموال أو حقوق المستهلك الالكتروني، وتقع في إطار الجرائم الإلكترونية أو الجرائم العامة المرتكبة عبر الإنترنت. ويميزها أنها ترتكب على المستهلك كطرف ضعيف في التعاقد الإلكتروني. ولذلك سوف يتم في الفرع الاول من هذا المطلب استعراض

صور رئيسية لهذه الجرائم على سبيل المثال لا الحصر ومن ثم في الفرع الثاني بيان وتوضيح الأركان القانونية التي تقوم عليها.

الفرع الأول

صور الجرائم الماسة بالمستهلك الإلكتروني

تشير بيانات الجهاز المركزي للإحصاء الفلسطيني ووزارة الاتصالات وتكنولوجيا المعلومات إلى أن ما يقارب 89% من الأفراد في فلسطين (10 سنوات فأكثر) استخدموا شبكة الإنترنت، كما بلغت نسبة الأسر التي لديها خدمة إنترنت في المنزل حوالي 92%، بينما بلغت نسبة امتلاك الهواتف الذكية حوالي 73%،مما يعكس انتشار واسع للتفاعل الرقمي بين السكان، وهو ما يهيّئ بيئة خصبة لوقوع الجرائم الإلكترونية التي تمس بيانات الأفراد والمستهلكين عبر هذا الفضاء الرقمي(الحياة، 2026)، لذلك أصدر المشرّع الفلسطيني القرار بقانون رقم (10) لسنة 2018م بشأن الجرائم الإلكترونية، والذي يُعد الإطار القانوني الأساسي لمكافحة الجرائم المرتكبة باستخدام الوسائل الإلكترونية، بما في ذلك الجرائم التي تمس حقوق المستهلك الإلكتروني في البيئة الرقمية. وقد تضمّن هذا القرار عدة صور إجرامية تُشكّل اعتداءً مباشرًا على مصالح المستهلك، ولا سيما تلك المرتبطة بالمعاملات التجارية الإلكترونية.

أولًا: الدخول غير المشروع إلى الأنظمة الإلكترونية

يعاقب القرار بقانون على الدخول غير المصرح به إلى أنظمة الحاسوب أو الشبكات الإلكترونية، لما يشكله هذا الفعل من خطر على بيانات المستهلك الإلكترونية، ولا سيما البيانات المتعلقة بالحسابات الشخصية أو وسائل الدفع الإلكتروني، الأمر الذي قد يؤدي إلى استغلالها بصورة غير مشروعة والإضرار بالمستهلك.

تطبيق عملي (ظاهرة معاصرة في فلسطين):

تشهد فلسطين تصاعدًا في عمليات الاحتيال المالي الرقمي والاحتيال على المحافظ الإلكترونية والحسابات البنكية الرقمية، حيث يستغل المحتالون ضعف الوعي الرقمي والبيانات الشخصية للوصول إلى حسابات الضحايا، ما يُعد شكلًا من أشكال الدخول غير المصرح به إلى الأنظمة أو استغلال الثقة للوصول إلى معلومات حسّاسة، ومن ثمّ الاستيلاء على المال. فقد سجّلت تقارير رسمية ارتفاعًا في حالات الاحتيال الإلكتروني المصرفي، مع تسجيل خسائر إجمالية بملايين الدولارات في النصف الأول من عام 2025م (شبكة القدس الإخبارية، 2026).

دلالة على الواقع الفلسطيني: تشير هذه الظاهرة إلى حقيقة أن بيانات الحسابات أو أنظمة المحافظ الإلكترونية يمكن الوصول إليها أو استغلالها بشكل غير مشروع عبر حيل خداعية تقنيًا واجتماعيًا، حتى لو لم يرتبط ذلك بحالة واحدة محددة منشورة قضائيًا(الجزيرة نت، 2026).

ثانيًا: الاحتيال الإلكتروني

يُعد الاحتيال الإلكتروني من أبرز الجرائم الماسة بالمستهلك الإلكتروني، إذ يتحقق من خلال استخدام الوسائل التقنية لخداع المستهلك والحصول على أمواله بطرق غير مشروعة، كإنشاء مواقع إلكترونية وهمية، أو انتحال صفة مورد أو تاجر، أو نشر إعلانات كاذبة ومضللة بقصد استدراج المستهلك وإيقاعه في الغلط.

شهدت المنطقة حالات نصب واسعة عبر منصات تداول واستثمار وهمية تعتمد الواجهة الرقمية لإيهام الضحايا بتحقيق أرباح، ثم تتوقّف فجأة عن دفع الأموال أو تنفيذ التزاماتها وتعطّل حسابات المستخدمين. من أبرز الأمثلة في العام 2025 كانت ظاهرة منصة «البروفيسور»/«PCEX» الاحتيالية التي استدرجت آلاف الأشخاص لاستثمار أموالهم عبر منصة تداول إلكترونية وهمية، ثم انقطعت المنصة عن دفع العوائد أو الأصل، مما دفع العديد من الضحايا إلى تقديم بلاغات للجهات المختصة في محاولة

لاستعادة أموالهم، فعشرات الضحايا في فلسطين وخارجها واجهوا إخلالًا واضحًا بتنفيذ الالتزامات الرقمية من مزوّدي خدمات الاستثمار الإلكتروني الوهمي، وهي حالة تبرز الإخلال الاحتيالي بالالتزامات التعاقدية(الأيام، 2026).

ومن التطبيقات القضائية التي جاءت بهذا الصدد حيث وجدت في القضاء المصري أنه قد وضح أن :" لاحتيال القائم على تقديم بيانات كاذبة للمستهلك بقصد الاستيلاء على ماله يتحقق ولو تم عبر وسيلة غير تقليدية متى انصرف قصد الجاني إلى الخداع." (محكمة النقض، 2004) (محكمة النقض الفلسطينية، طعن جزائي رقم (2018/644) (جلسة 7 أبريل)، 2019)، وقضت محكمة التمييز الأردنية" إن علم البائع بأنه لا يستطيع تحويل المطعم باسم المشتري، واخفائه له في مجلس العقد يعتبر تغيراً بالمشاريع بأمر جوهري، بحيث لو علم المشتري بهذا الأمر لما تقدم على شراء المطعم"

ثالثًا: انتهاك الخصوصية والاعتداء على البيانات الشخصية

تتحقق جريمة انتهاك بيانات المستهلك وخصوصيته من خلال الدخول غير المشروع إلى بياناته الشخصية أو المالية،أو الحصول عليها أو استخدامها أو نشرها دون رضاه الصريح، سواء تم ذلك قبل إتمام المعاملة الإلكترونية أو بعدها، وهو ما يُشكّل اعتداءً مباشرًا على حق المستهلك في الخصوصية والأمان الرقمي

ويُواجه التحقيق في هذا النوع من الجرائم تحديات تقنية وقانونية معقّدة، تتطلب خبرة متخصصة في مجال الأدلة الرقمية وأمن المعلومات الجنائي، ولا سيما في ما يتعلق بتحديد طريقة حدوث الاختراق، ونطاق البيانات المتضررة، ومصدر الاعتداء، بما يضمن سلامة الدليل الرقمي وصلاحيته للإثبات أمام الجهات القضائية المختصة(فايق، 2026).

مثال تطبيقي على ذلك: في مطلع عام 2025، باشرت الجهات الأمنية المختصة التحقيق مع متهم قام بانتحال صفة موظف خدمة العملاء، زاعمًا تحديث بيانات بطاقات الدفع الإلكتروني للمواطنين بهدف

"تحديث معلوماتهم البنكية". وقد أسفر ذلك عن استيلاء المتهم على بيانات بطاقات الدفع الخاصة بالضحايا واستخدامها في عمليات شراء إلكترونية غير مشروعة، فضلًا عن تحويل أموال الضحايا عبر منصات دفع غير مصرح بها، مما يعكس كيف يمكن لجرائم التلاعب ببيانات الدفع أن تؤثر مباشرة على المستهلك الذي وضع ثقته في النظام الإلكتروني (اليوم السابع، 2025).

رابعًا: الإخلال الاحتيالي بتنفيذ الالتزامات التعاقدية الإلكترونية

تتمثل هذه الجريمة في امتناع المورد أو المهني عن تنفيذ التزاماته الناشئة عن العقد الإلكتروني بسوء نية، كعدم تسليم السلعة المتفق عليها، أو تسليم سلعة مغايرة للمواصفات المعروضة إلكترونيًا، أو الامتناع عن رد المبالغ المدفوعة، وهو ما يُعد اعتداءً على إرادة المستهلك ويُفرغ العقد الإلكتروني من مضمونه.

وفيما يتعلق بقانون حماية المستهلك رقم (21) لسنة 2005، فقد تناول بدوره عددًا من صور الجرائم التي تمس المستهلك، والتي تمتد آثارها إلى البيئة الإلكترونية، ومن أبرزها:

أولًا: الخداع في المنتجات أو الخدمات

ويتحقق ذلك من خلال تقديم أو عرض معلومات غير صحيحة أو مضللة بشأن طبيعة المنتج أو جودته أو مكوناته أو خصائصه الجوهرية، بما يؤثر في قرار المستهلك ويدفعه إلى التعاقد بناءً على بيانات غير واقعية.

تطبيق عملي (احتيال إلكتروني واسع يشمل خداعًا عن طريق المعلومات المضللة)

تعكس عمليات الاحتيال على المحافظ الرقمية والبنوك الرقمية في غزة وأجزاء أخرى من فلسطين، مثل عمليات النصب التي تُدار عبر اتصالات أو رسائل تنتحل صفة ممثلي الخدمة وتطلب رموزًا سرية ثم تُفرغ الحسابات الإلكترونية بالكامل، مثالًا حيًا على خداع المستهلك عبر معلومات مضللة تُقدَّم له في سياق الخدمة الرقمية. في هذه الحوادث، يُغرَّر بالمستهلك ليُدلي بمعلوماته الشخصية بناءً على ادعاءات كاذبة عن الخدمة، ما يعكس خداعًا في الخدمة أو المنتج الرقمي، ومن الحالات التطبيقية: رصيد مواطن

في غزة ضاع بالكامل بعد مكالمة احتيالية ادّعى فيها المتصل أنه من مقدّم الخدمة، واستطاع الحصول على رموز التحقق للوصول إلى محفظته وسحب المال(الجزيرة نت، 2026) .

وقد أكدت التطبيقات القضائية الفلسطينية هذا التوجه، إذ قضت محكمة النقض الفلسطينية في حكمها الصادر في الطعن الجزائي رقم 2018/644 بتاريخ 2019/4/7، بأن عرض أو بيع سلع فاسدة أو غير مطابقة للمواصفات المعتمدة يُعد جريمة قائمة بذاتها متى ثبت توافر أركانها القانونية، ولا يجوز التوسع في تفسير النصوص بما يؤدي إلى إهدار الحماية التي قصدها المشرّع للمستهلك. وبيّنت المحكمة أن جوهر الحماية الجنائية يتمثل في صون حق المستهلك في سلامة السلعة وصحة البيانات المقدمة بشأنها، وأن أي إخلال بذلك يشكل اعتداءً يستوجب المساءلة الجزائية، تطبيقًا لأحكام المادتين (8) و(27) من قانون حماية المستهلك رقم (21) لسنة 2005(محكمة النقض الفلسطينية، طعن جزائي رقم (2018/644) (جلسة 7 أبريل)، 2019).

ثانيًا: التضليل في الكمية أو المقاس أو الوزن

وتقع هذه الجريمة عندما يتم الإعلان عن كميات أو مقاسات غير مطابقة للحقيقة، كعرض عبوات تحتوي على كميات أقل مما هو مُعلن عنه في الوصف الإلكتروني، وهو ما يُلحق ضررًا مباشرًا بالمستهلك.

تطبيق عملي قريب (امتداد للجرائم التقليدية إلى الرقمي):

لا توجد حالة منشورة رسميًا في فلسطين تُظهر ضبطًا قضائيًا مذكرًا نقص الكمية أو المقاس غير المطابق في عرض إلكتروني، لكن الواقعة شائعة في المعاملات الرقمية، وتُوثّق وفق تقارير إعلامية عن شكاوى المستهلكين من اختلاف ما استلموه عن ما عُرض لهم عبر مواقع التجارة الإلكترونية (مثلاً: منتجات لا تطابق المواصفات أو الحجم الموضح في الإعلان الإلكتروني) — وهو ما يحاكي جرائم التضليل التقليدي عندما تمتد إلى الفضاء الرقمي. تقارير مراقبة المستهلكين توثق ارتفاع الشكاوى في هذا

السياق، ولا سيما فيما يتعلق بالمنتجات المستوردة والمباعة عبر الإنترنت في فلسطين(وكالة سند للأنباء، 2026).

إضافةً إلى الحماية الجزائية العامة التي كفلها قانون العقوبات للمستهلك، أفرد المشرّع الفلسطيني حمايةً جزائيةً خاصة ضمن قوانين تكميلية، وفي مقدمتها قانون حماية المستهلك، تأكيدًا لخصوصية المصالح التي يرمي إلى حمايتها وخطورة الأفعال التي تمس سلامة المستهلك وصحته وأمنه الاقتصادي. فقد نصّت المادة (27) من قانون حماية المستهلك (قانون حماية المستهلك رقم 21، 2005)، على تجريم عرض أو بيع السلع التموينية الفاسدة أو التالفة أو التلاعب بتاريخ صلاحيتها، وقرّرت لذلك عقوبات مشددة تتمثل بالحبس لمدة تزيد على عشر سنوات أو بالغرامة التي لا تتجاوز عشرة آلاف دينار أردني أو ما يعادلها بالعملة القانونية، أو بكلتا العقوبتين، كما وسّعت نطاق التجريم ليشمل عرض أو بيع أي منتج مخالف للتعليمات الفنية الإلزامية.

وبذات الاتجاه، جاءت المادة (31) من قانون المواصفات والمقاييس الفلسطيني (قانون المواصفات والمقاييس رقم 6، 2000)، لتقرر المسؤولية الجزائية بحق كل من يصنّع أو يطرح أدوات أو منتجات غير مطابقة بقصد بيعها أو بقصد الغش، أو يتلاعب بالأوزان أو الأحجام أو الكميات، أو يرتكب أي فعل من شأنه خداع أو غش المستهلك، حيث فرض المشرّع عقوبة الحبس لمدة لا تقل عن شهر ولا تزيد على سنة، أو الغرامة التي لا تقل عن ألف دينار، أو كلتا العقوبتين.

يُلاحظ الباحث من خلال هذه النصوص أن المشرّع الفلسطيني قد اتجه إلى تشديد الحماية الجزائية للمستهلك عبر تجريم صور متعددة من الأفعال التي تمس جوهر الثقة في التعاملات التجارية، سواء تعلقت بسلامة المنتجات أو بصحة البيانات والمواصفات المعلنة عنها. كما يُستدل من شدة العقوبات المقررة، لا سيما في قانون حماية المستهلك، على إدراك المشرّع لخطورة هذه الجرائم وآثارها الممتدة

إلى الصحة العامة والأمن الاقتصادي، الأمر الذي يبرر إخراجها من نطاق القواعد العامة إلى إطار تشريعي خاص.

ويرى الباحث أن هذه النصوص، وإن صيغت في الأصل لمواجهة الأفعال التقليدية، إلا أنها تتسم بالمرونة الكافية التي تسمح بانطباقها على صور الغش والبيع غير المشروع التي تتم عبر الوسائط الإلكترونية، متى تحقق عنصر العرض أو البيع أو الإعلان للمستهلك، مما يكرّس امتداد الحماية الجزائية إلى مجال الاستهلاك الإلكتروني، ويؤكد الحاجة إلى قراءة النصوص بروحها لا بحرفيتها لمواكبة تطور أساليب الاعتداء على المستهلك.

ثالثًا: الكذب بشأن مصدر أو بلد منشأ المنتج

وهو الإعلان التجاري المضلل أو الكاذب الذي يقوم على بيانات غير صحيحة تتعلق بخصائص السلعة أو مصدرها أو نتائج استخدامها، مما يؤدي إلى إحداث خطأ في إرادة المستهلك، ويستلزم معاقبة من يقوم به وفقاً لمتبنيات حماية المستهلك(شعوة، 2016).

ويتحقق ذلك من خلال إيهام المستهلك بأن المنتج ذو منشأ معين لما يحمله من سمعة أو جودة، في حين أن حقيقته تخالف ذلك، كعرض منتجات مقلدة على أنها أصلية أو ذات منشأ أجنبي معيّن، قررت محكمة النقض المصرية بشرط الغش والتدليس على ما عرفته المادة 125 من القانون المدني المصري وعلى ما جرى به قضاء المحكمة أن يكون ما استعمل في خداع المتعاقد حياة وان تكون هذه الحيلة غير مشروعة قانوناً

وبذلك يتضح أن الجرائم الماسة بالمستهلك الإلكتروني تتوزع بين جرائم إلكترونية ذات طابع تقني، وجرائم استهلاكية تقليدية امتدت إلى الفضاء الرقمي، الأمر الذي يستوجب تفسير النصوص القانونية القائمة تفسيرًا يحقق الحماية الفعلية للمستهلك الإلكتروني، إلى حين استحداث تنظيم تشريعي أكثر تخصيصًا وشمولًا.

الفرع الثاني

أركان الجرائم الماسة بالمستهلك الإلكتروني

تقوم الجرائم الماسة بالمستهلك الإلكتروني، كغيرها من الجرائم، على توافر مجموعة من الأركان القانونية التي لا تقوم الجريمة إلا باكتمالها، وهي: الركن الشرعي، والركن المادي، والركن المعنوي.

أولًا: الركن الشرعي (القانوني)

يتمثل الركن الشرعي في وجود نص قانوني يجرّم الفعل ويقرر له عقوبة، تطبيقًا لمبدأ شرعية الجرائم والعقوبات، الذي يُعد من المبادئ الدستورية المستقرة، ومؤداه أنه لا جريمة ولا عقوبة إلا بنص قانوني سابق على الفعل. وفي هذا الإطار، تستند الجرائم التي تمس المستهلك الإلكتروني في فلسطين إلى قرار بقانون رقم (10) لسنة 2018 بشأن الجرائم الإلكترونية، إضافة إلى قانون حماية المستهلك رقم (21) لسنة 2005، حيث جرّمت هذه النصوص أفعالًا متعددة تمس حقوق المستهلك سواء ارتُكبت بوسائل تقليدية أو عبر الوسائط الإلكترونية(سرور، 1989، الصفحات 87–89).

وفي هذا السياق، فإن الباحث يرى أن قانون العقوبات الفلسطيني(قانون العقوبات الفلسطيني، 1936)، يتضمن عددًا كبيرًا من النصوص التي تشكّل الأساس الشرعي لتجريم أفعال تمس حقوق المستهلك، سواء تعلّقت بالغش، أو الاحتيال، أو الخداع في المعاملات، وهي نصوص وُضعت ابتداءً لتنظيم العلاقات التقليدية، إلا أن نطاق تطبيقها يمتد ليشمل الأفعال المرتكبة عبر الوسائط الإلكترونية متى توافرت عناصر الجريمة.

وإلى جانب قانون العقوبات، فإنه يرى أن القوانين التكميلية أسهمت في تدعيم الركن الشرعي للحماية الجنائية في البيئة الرقمية، حيث تضمّن قانون الاتصالات السلكية واللاسلكية الفلسطيني لسنة من(قانون الاتصالات رقم (3)، 1996)، تجريم عدد من أنماط السلوك غير المشروع المرتبطة باستخدام وسائل

الاتصال، كإساءة استعمال شبكات الاتصال أو توظيفها في أغراض غير مشروعة، وهي أفعال يتسع نطاقها ليشمل النشر والتواصل الإلكتروني في صورته الحديثة.

كما يُعد قانون المطبوعات والنشر(قانون شأن المطبوعات رقم (9)، 1995 ب والنشر)، أحد الأطر التشريعية المكمّلة التي تؤسس للركن الشرعي في الجرائم المرتبطة بالمحتوى المنشور، إذ يضع قيودًا قانونية على ما يُنشر أو يُبث عبر وسائل الإعلام، وهو ما يمكن تطبيقه – في حدود معينة – على المحتوى الرقمي والإعلانات الإلكترونية التي قد تنطوي على تضليل أو خداع للمستهلك.

ويُستفاد من ذلك أن الركن الشرعي للمسؤولية الجنائية في مجال حماية المستهلك الإلكتروني في فلسطين لا يستند إلى تشريع واحد جامع، وإنما يقوم على منظومة تشريعية متفرقة، تضم قانون العقوبات والقوانين التكميلية ذات الصلة، الأمر الذي يحقق حماية جزائية جزئية، لكنه في الوقت ذاته يكشف عن حاجة ملحّة إلى تدخل تشريعي موحّد يُنظّم التجريم في البيئة الرقمية بصورة أكثر وضوحًا ودقة.

ثانيًا: الركن المادي

يتمثل الركن المادي في السلوك الإجرامي الملموس الذي يأتيه الجاني باستخدام الوسائل الإلكترونية، كالدخول غير المشروع إلى الأنظمة أو الشبكات، أو إنشاء مواقع وهمية، أو نشر إعلانات مضللة، أو استغلال المنصات الرقمية لبيع سلع غير مطابقة للمواصفات أو منتهية الصلاحية. ويتميز هذا الركن في الجرائم الماسة بالمستهلك الإلكتروني بكونه يتحقق في بيئة رقمية غير مادية، وهو ما يميزه عن الجرائم التقليدية التي تقع في مكان مادي محدد، ويُثير صعوبات خاصة في مسألة الإثبات

يُلاحظ الباحث أن المشرّع الفلسطيني قد ربط تحقق الركن المادي في الجرائم ذات الطابع التعبيري بأمرين متلازمين؛ أولهما صدور سلوك تعبيري غير مشروع يحرّمه القانون، وثانيهما إعلان هذا السلوك أو نشره على نحو يضفي عليه صفة العلانية. ولا يكفي في هذا المقام مجرد توافر الفعل المجرّم في

ذاته، وإنما يُشترط أن يتخذ هذا الفعل مظهرًا خارجيًا يسمح باطلاع الغير عليه، بما يحقق الخطر أو الضرر الذي استهدف المشرّع منعه.

وبالرجوع إلى نصوص قانون العقوبات (قانون العقوبات الفلسطيني، 1936)،يُلاحظ أن المشرّع لم يعتمد قالبًا تشريعيًا واحدًا لصياغة هذا الركن، وإنما استخدم عبارات متعددة تؤدي الغرض ذاته، كما هو الحال في المادة (125) من قانون العقوبات رقم (74) لسنة 1936، والمادة (152) من قانون العقوبات رقم (16) لسنة 1960، حيث وردت صيغ من قبيل: «كل من طبع أو نشر»، و*«كل من نشر»*. ويُفهم من تنوع هذه العبارات أن العبرة ليست بوسيلة النشر ذاتها، وإنما بتحقق العلانية ووصول السلوك التعبيري إلى الغير.

ومن ثمّ، فإن استخدام المشرّع لمصطلحات الطبع والكتابة والنشر لا يُفهم منه حصر التجريم في الوسائل التقليدية، بل ينطوي على مرونة تشريعية تسمح بامتداد نطاق التجريم إلى صور النشر الإلكتروني، باعتباره أحد الأشكال الحديثة لإعلان السلوك التعبيري وإتاحته للجمهور. وعليه، فإن تحقق الركن المادي في الجرائم المرتكبة عبر الوسائط الرقمية ينسجم مع الفلسفة العامة للنصوص العقابية، متى ثبت أن الفعل قد اتخذ صورة العلانية، ولو كان ذلك عبر منصة إلكترونية أو وسيلة رقمية.

ثالثًا: الركن المعنوي

يتحقق الركن المعنوي بتوافر القصد الجنائي لدى الجاني، أي علمه بعدم مشروعية الفعل واتجاه إرادته إلى ارتكابه، وغالبًا ما يكون القصد في الجرائم الماسة بالمستهلك الإلكتروني قصدًا جنائيًا عامًا، وقد يتخذ في بعض الصور قصدًا خاصًا، كنية الاحتيال أو التضليل أو الاستغلال المتعمد لضعف المستهلك في البيئة الرقمية، خاصة في حالات الإعلانات الكاذبة أو سرقة البيانات(حسني، الصفحات 302-305).

وقد أشارت المحكمة إلى عدم تحقيق ركن الجريمة (القصد الجنائي/ الركن المعنوي)، إذ انتفى القصد الجنائي المتطلب لقيام الجريمة(محكمة النقض الفلسطينية، طعن رقم (2025/38) (جلسة 3 مارس)، 2025).

وعليه وفقاً للقواعد العامة للمسؤولية الجنائية، لا يكفي قيام ماديات جريمة النشر كنشر الكتروني لمقال يتضمن محتوى غير مشروع، لقيام تلك المسؤولية، بل يجب إثبات قيام علاقة بين تلك الماديات وشخص معين، تربطه بتلك الماديات علاقة نفسية خالصة، اي إرادة القيام بتلك الماديات إرادة حرة واعية يسبقها العلم فلا إرادة بلا علم، وهو ما يستقيم مع المبدأ الدستوري شخصية المسؤولية الجنائية الذي تبناه المشرع الفلسطيني، بحيث لا يكون مسؤولاً عن الجريمة الا من كان فاعلاً للجريمة أو مشتركاً فيها، فلا مسؤولية لشخص عن سلوك غيره

ووفقاً لما سبق فإن الباحث يلاحظ أن الجرائم الماسة بالمستهلك الإلكتروني تشترك مع الجرائم التقليدية في بنيانها القانوني من حيث الأركان، إلا أنها تختلف من حيث وسيلة ارتكابها وطبيعتها الرقمية، الأمر الذي يجعل النصوص العامة غير كافية أحيانًا لمواجهتها. ويرى الباحث أن خصوصية هذه الجرائم تقتضي تدخلًا تشريعيًا خاصًا ينظم صورها وأركانها وعقوباتها في إطار قانوني موحّد يحقق حماية جنائية فعّالة للمستهلك الإلكتروني.

المطلب الثاني

العقوبات المنصوص عليها في القوانين لحماية المستهلك الإلكتروني

تهدف العقوبات إلى تحقيق الردع العام والخاص، وإعادة تأهيل الجاني، وحماية النظام العام والمصلحة المجتمعية، وذلك من خلال فرض جزاء قانوني على السلوك الإجرامي يحد من تكراره ويؤكد سيادة القانون(حجازي، شرح قانون العقوبات، 2007، صفحة 45)، وتشتمل التشريعات الفلسطينية على مجموعة من العقوبات المقررة على الجرائم المختلفة التي يمكن أن يتعرض لها المستهلك الالكتروني

سواء كانت واردة في قانون حماية المستهلك أو في قانون الجرائم الإلكترونية أو في قانون العقوبات او غيرها من القوانين.

لذا سوف نتناول في هذا المطلب في الفرع الاول عرض لأهم العقوبات للجرائم التي يتعرض لها المستهلك الالكتروني وفي الفرع الثاني الاستعانة ببعض التشريعات العربية للمقارنة .

الفرع الاول

العقوبات المنصوص عليها في القوانين

مع ازدياد الاعتماد على التجارة الالكترونية في مختلف المجالات كان لا بد من مواكبة كل التحديات التي من الممكن ان يتعرض لها المستهلك الالكتروني بصفته الطرف الاضعف و الذي يعنى المشرع في حمايته حماية كاملة من كافة المخاطر التي من الممكن ان يتعرض لها حيث ان قانون حماية المستهلك يعتبر الاساس التشريعي الذي يرتكز عليه المشرع في حماية المستهلك مع تعديلاته بموجب قرار بقانون رقم 27 لسنه 2018 وقانون المواصفات والمقاييس وقانون الجرائم الالكترونية وقانون العقوبات وغيره من القوانين وسوف نتحدث عن بعض الجرائم والعقوبات التي نصت عليها مختلف القوانين ومن ثم التعليق عليها .

ان قانون حماية المستهلك قد شدد على الجرائم المتعلقة بالسلع الغذائية الفاسدة او المغشوشة فقد نصت المادة 27 من قانون حماية المستهلك المعدل على ان كل من يبيع او يتداول او يخزن سلع غذائية فاسدة او مغشوشة او منتهية الصلاحية يعاقب بالسجن ما بين ثلاث سنوات و 10 سنوات وبغرامة لا تقل عن خمسة الالف دينار اردني ولا تزيد عن خمسة عشر الف دينار اردني وعند النظر الى هذا النص نجد بان المشرع قد وضع عقوبة صارمة على مرتكب هذه الجرائم وعند النظر الى قانون المواصفات والمقاييس رقم 16 لسنة 2000 فان اقصى عقوبة قد نص عليها القرار بقانون هي الحبس لمدة لا تزيد عن سنة وبغرامة لا تزيد عن 10000 دينار اردني لجريمة بيع او صنع ادوات قياس غير قانونية او

التلاعب بالأوزان و المقاييس او عدم مطابقة المواصفات والمقاييس وعند النظر الى قرار بقانون رقم 10 لسنة 2018 بشان الجرائم الالكترونية فإننا نجد بان اقصى عقوبة هي السجن لمدة لا تقل عن ثلاث سنوات ولا تزيد عن 15 سنة في حالات التشديد مثل ارتكابها من قبل عصابة او ضد انظمة الدولة.

اما فيما يتعلق بجرائم الاحتيال فان المادة 417 من قانون العقوبات الاردنيرقم (16) لسنة 1960 تنص على أنه " كل من حمل الغير على تسليمه مالاً منقولاً أو غير منقول أو أسناداً تتضمن تعهداً أو إبراء فاستولى عليها احتيالاً: باستعمال طرق احتيالية من شأنها إيهام المجني عليه بوجود مشروع كاذب أو حادث أو أمر لا حقيقة له أو إحداث الأمل عند المجني عليه بحصول ربح وهمي أو بتسديد المبلغ الذي أخذ بطريق الاحتيال أو الإيهام بوجود سند دين غير صحيح أو سند مخالصة مزور أو بالتصرف في مال منقول أو غير منقول وهو يعلم أن ليس له صفة للتصرف به، أو باتخاذ اسم كاذب أو صفة غير صحيحة، عوقب بالحبس من ثلاثة أشهر إلى ثلاث سنوات وبالغرامة من خمسة دنانير إلى خمسين ديناراً ."

تشتبه جريمة الاحتيال الالكتروني جريمة الاحتيال العادية، فكلاهما يقومان على وسائل الغش والخداع، وكلاهما من جرائم الاموال هدف الجاني فيها الاستيلاء على أموال غيره لتملكه. لهذا فكثير من الدول لم تشرع نصوصاً قانونية تجرم وتعاقب مرتكبي جريمة الاحتيال الالكتروني لان القضاء الجزائي في هذه الدول وسع من تفسيره للنصوص القانونية الخاصة بجريمة الاحتيال العادية وجعلها تمتد لتشمل هذه الجريمة، وهذا ما اخذت به كافة الدول الانجلوسكسونية كبريطانيا واستراليا وكندا كما ظهرت اتفاقات على المستوى الاقليمي لمواجهة جرائم الانترنت مثل الاتفاقية الاوروبية حول الجريمة الافتراضية، والقانون العربي الاسترشادي لجرائم المعلومات على المستوى العربي(الفيل، 2011، صفحة 2).

ومع ذلك تختلف جريمة الاحتيال الالكتروني عن جريمة الاحتيال العادية كون أن الأولى تتم من خلال وسيلة الكترونية باستخدام شبكة الانترنت، في حين أن الثانية تكون وسيلة الخداع فيها بأي طريقة من

شأنها إيهام الغير وخداعة، فجريمة الاحتيال العادية أعم وأوسع من جريمة الاحتيال الالكتروني. ثم أن محل جريمة الاحتيال العادية هو المال المنقول بينما محل جريمة الاحتيال الالكتروني يشمل المنافع والخدمات والسلع والمنتجات عبر الانترنت.

وتقع جريمة الاحتيال العادية مباشرة بين الجاني والمجني عليه بينما في جريمة الاحتيال الالكتروني تقع الجريمة بين اشخاص متواجدين في مناطق متباعدة وفي دول مختلفة قاسمهم المشترك استخدامهم لرسائل البريد الالكتروني عبر شبكة الانترنت (الفيل، 2011، صفحة 2).

على ضوء ما تقدم وعلى الرغم من وجود فوارق بين جريمة الاحتيال التقليدية وفق مفهومها الوارد في قانون العقوبات وبين الجريمة الإلكترونية إلا أن هذه الفوارق تنحصر في الأسلوب الإجرامي فقط، فبدلا من أن كانت تتم الجريمة بطريقة تقليدية أصبحت اليوم في ظل التطور التكنولوجي تأخذ أسلوبا أخر إلا أن ذلك لا يمنع تطبيق نص المادة 417 من قانون العقوبات للتصدي لجرائم الاحتيال التي تتم من خلال شبكات الانترنت بالوسائل الالكترونية.

وفي الحديث عن الجرائم كان لابد من التطرق الى جرائم السرقة فقد عرفت المادة 399 من قانون العقوبات رقم 16 لسنة 1960 جريمة السرقة بأنها (هي أخذ مال الغير المنقول دون رضاه، وتعني عبارة (أخذ المال) إزالة تصرف المالك فيه برفعه من مكانه ونقله وإذا كان متصلاً بغير منقول فبفصله عنه فصلاً تاماً ونقله، وتشمل لفظة (مال) القوى المحرزة.

والآن وفي الفضاء الالكتروني فإن عملية السرقة الالكترونية كالاستيلاء على ماكينات الصرف الآلي والبنوك،وفيها يتم نسخ البيانات الإلكترونية لبطاقة الصراف الآلي ومن ثم استخدامها لصرف أموال من حساب الضحية أو إنشاء صفحة انترنت مماثلة جدا لموقع أحد البنوك الكبرى أو المؤسسات المالية الضخمة لتطلب من العميل إدخال بياناته أو تحديث معلوماته بقصد الحصول على بياناته المصرفية وسرقته، وبذلك أصبحت البنوك والمصارف هي هدف لمحترفي الأجهزة الالكترونية الذين يتلاعبون في

كشوف حسابات العملاء ونقل الأرصدة من حساب لآخر، وقد تكون بصورة ثانية كإضافة بضعة أرقام أو أصفار إلى رقم ما في هذا الحساب(مديرية تكنولوجيا المعلومات، 2015).

والسؤال الذي يطرح في هذا الجانب، فيما لو عرضت قضية سرقة عبر الوسائل الالكترونية فما هو التكييف القانوني السليم لهذه القضية؟.

ابتداءً نستطيع أن نقول ووفق المادة 399 من قانون العقوباتالمطبق في الضفة الغربية أن عمليات السرقة التي تتم عبر شبكة الانترنت تدخل في مفهوم جريمة السرقة وفق المفهوم المتقدم لها.

للأسف لا تسعفنا نصوص قانون العقوبات رقم 16 لسنة 1960 م على تكييف نوع هذه التهمة، ذلك أن نصوص قانون العقوبات صنفت أنواع السرقة التي تتم بالطرق العادية ووصفتها وشددت عقوبة بعضها ما بين جنح بسيطة كتلك التي تتم بالأخذ والنشل حسب نص المادة 407 من القانون المذكور، وجنح مشددة كتلك التي نصت عليها المادة 406، وجنايات بسيطة كتلك التي تتم بالكسر والخلع حسب نص المادة 404، وجنايات مشددة كتلك التي تتم بالسطو وفق المواد 401، 402، 403) (قانون العقوبات، 1960).

لهذا نجد أن كافة الدعاوى المنظورة أمام المحاكم الفلسطينية حول السرقات التي تتم من حسابات الأشخاص عبر الانترنت يتم تكييفها تارة بتهمة السرقة خلافا للمادة 407 على اعتبار أن مفهوم الأخذ ينطبق على السرقة الالكترونية وهنا نجد أن عقوبة هذه الجريمة هي الأخف من بين جرائم السرقات، وأحيانا يتم تكييفها على جريمة الاحتيال على اعتبار أن ما حصل هو خداع أوقع المجني عليه على تسليم أمواله.

واما فيما يتعلق بجرائم التزوير فقد عرفت المادة 260 من قانون العقوبات رقم 16 لسنة 1960 التزوير بأنه تحريف مفتعل للحقيقة في الوقائع والبيانات التي يراد اثباتها بصك أو مخطوط يحتج بهما نجم أو يمكن أن ينجم عنه ضرر مادي أو معنوي أو اجتماعي.

باعتقادنا بأن التوقيع الالكتروني والبصمة الالكترونية إذا ما كان واقعا على صك أو مخطوط رسمي فإننا نكون أمام جريمة تزوير في أوراق رسمية حسب مفهوم المادة 265 من قانون العقوبات المذكور، وإذا كان واقعا على أوراق خاصة فإنه يكون تزوير في أوراق خاصة وفق المادة 271 من ذات القانون، وكذلك الأمر فإن تزوير البريد الالكتروني وبطاقات الدفع الالكتروني فإنها تدخل هي الأخرى في التزوير في الأوراق الخاصة لعدم صبغتها في الأوراق الرسمية وبالتالي – وفي ظل هذا القصور التشريع – تكون عقوبتها جنحوية بسيطة رغم خطورتها.

اللائحة التنفيذية لقانون حماية المستهلك

تُفصّل هذه اللائحة الإجراءات والآليات اللازمة لتنفيذ أحكام قانون حماية المستهلك، بما في ذلك:

- آليات الرقابة والتفتيش: تحديد الجهات المسؤولة عن مراقبة الأسواق وضبط المخالفات.
- إجراءات تقديم الشكاوى: توضيح كيفية تقديم المستهلكين لشكاواهم والجهات المختصة بالنظر فيها.

عند النظر الى هذه القوانين نجد بان جميعها تقريبا عدا قانون الجرائم الالكتروني(قانون الجرائم الإلكترونية الأردني رقم (17)، 2023)، قد تحدثوا عن المستهلك التقليدي ولم يتم ذكر المستهلك الالكتروني فيهم وهذا يجعلنا اما معضلة القياس في كل جريمة تحدث مع المستهلك الالكتروني ويجعلنا امام مقارنة الجرائم التي يتعرض لها المستهلك الالكتروني والجرائم التي يتعرض لها المستهلك التقليدي ومحاولة ايجاد تكييف قانوني مطابق له الامر الذي يجعل القاضي او دوائر تنفيذ القانون او الرقابة في مهمة صعبة في كل مرة وذلك للحاجة الى ايجاد تكييف قانوني واضح وقريب .

وعند النظر الى العقوبات المفروضة والغرامات المفروضة على مرتكبي جرائم ضد المستهلك نجد بان حتى العقوبات بحاجة الى تعديلات ايضا كون ان هناك بعض الجرائم بحاجة الى تشديد العقوبات بها او رفع الغرامات بها لتحقيق الغاية من التشريع وهو الردع العام والخاص .

ويرى الباحث في ان التحديات والصعوبات التي يواجهها القضاء والجهات المنفذة للقانون هي صعبه للغاية من حيث ايجاد التكييف القانوني السليم والصحيح من جهة ومن حيث تشعب القوانين والنصوص القانونية من جهة اخرى لذا انا ارى بان على المشرع اولا تعديل قانون حمايه المستهلك ووضع كافه الجرائم في قانون واحد لتسهيل تطبيق القانون اولا وثانيا وضع باب خاص في قانون حماية المستهلك يعنى فقط في جرائم حماية المستهلك الالكتروني الذي يعتبر مهم للغاية وهو يعاني من قصور كبيرة في هذا الامر .

الفرع الثاني

مقارنة بالتشريعات الأخرى

عند مقارنة التشريع الفلسطيني بالتشريعات العربية الأخرى، نلاحظ ما يلي:

يتميز القانون الاردني بالصرامة في حجم العقوبات المفروضة على جرائم الاحتيال الالكتروني مثلا حيث انه يعاقب على جرائم الاحتيال التي تمس المال و المستهلك الالكتروني بان كل من كل من استولى عبر وسيلة احتيالية أو انتحال صفة على مال منقول أو وثيقة مالية بغير حق بالسجن المؤقت لمدة لا تقل عن سنة وبغرامة مالية ما بين 5000 دينار اردني – 25000 دينار اردني (قانون الجرائم الإلكترونية الأردني رقم (17)، 2023).

كما تحدث ذات القانون عن عقوبة الاعتداء على بيانات الدفع الالكتروني، اذ انه يعاقب بالسجن من سنة الى ثلاث سنوات وبغرامة مالية ما بين 2500 دينار اردني و 10000 دينار اردني كل من يصل بغير وجه حق الى بيانات او بطاقات بنكية او خدمات دفع الكتروني واستخدامها في النصب على الغير .

وبالمثل،يقضي القرار بقانون الفلسطيني رقم (10) لسنة 2018 بمعاقبة من استولى عبر الشبكة الإلكترونية على مال أو توقيع إلكتروني بوسائل احتيالية بالسجن لمدة لا تقل عن سنة واحدة أو بغرامة مالية تتراوح ما بين 1000 دينار اردني – 3000 دينار اردني وعلى الرغم ورغم تشابه النص الفلسطيني بالأردني في وصف الجريمة، إلا أن العقوبات التي نص عليها المشرع الفلسطيني – أقل حدة من نظيرها في التشريع الأردني . ومن الجدير بالذكر أن القانون الفلسطيني يضاعف العقوبة إذا ارتكبت الجريمة على نظم أو مواقع تتعلق بخدمات الدفع والتحويلات المالية.

أما القانون المصري رقم (175) لسنة 2018 فيعرِّف جريمة الاحتيال المصرفي الإلكتروني بمواد عدة، أبرزها المادة (23)، التي تعاقب كل من يستخدم الشبكة المعلوماتية للوصول إلى بيانات بطاقات بنكية أو أدوات دفع إلكتروني بدون وجه حق بالسجن مدة لا تزيد عن ثلاثة اشهر وغرامة مالية 30000 جنيه – 50000 جنيه وترتفع العقوبة إلى ستة اشهر وغرامة مالية 50000 جنيه – 100000 جنية الى قام باستعمالها لغايات الحصول على اموال الغير وفي حال اكتمل الفعل حتى الحصول على مال الغير فان العقوبة من الممكن ان تصل إلى سنة سجن وغرامة مالية 100000 جنيه –200000 جنيه، ويبيّن ذلك شمولية النص المصري في معاقبة مختلف مراحل الاحتيال الإلكتروني على الأموال، من الحصول على بيانات الدفع إلى استغلالها في اختلاس أموال الغير.

وعند المقارنة فإن العقوبات تختلف تفاوتاً ملحوظاً بين التشريعات. فالعقوبات الأردنية العامة (سجن سنة على الأقل وغرامة تبدأ من 5000 دينار) تفوق من حيث المبلغ والغرامة أقرانها المصرية والفلسطينية، حيث تتراوح الغرامات المصرية في المادة (23) بين (30000–200000) جنيه مصري في حين لا تتجاوز الغرامات الفلسطينية (ألف–3000 دينار أردني).

أما شمولية النصوص فقد برزت في القانون الإماراتي بانتقاء واسع للجرائم التي ترتكب على المستهلك الالكتروني، حيث لم يقتصر على الجرائم الماليـــة فقط بل أدرج الابتزاز والشائعات والكذب والإعلانات

الخاطئة في الملاحقة الجنائية،أما القانون المصري فقد وسع دائرة المعاقَب عليهم لتشمل منتجات تقنية المعلومات بالكامل، فجرّمه تدنيس سرية البيانات أو الاعتداء على الشبكات الحكومية وحرمة النظم المعلوماتية .والقانون الأردني معاصر نسبياً، لكنه يركز على الجرائم التقليدية مثل الاحتيال والاستيلاء والتلاعب المالي عبر التقنية والقانون الفلسطيني يغطي بعض من الجرائم المعلوماتية .

ولابد من الإشارة إلى أن المحاولات التشريعية في الدول العربية جارية على قدم وساق وهناك اهتمام ملحوظ بهذا النوع من التشريعات، ونذكر منها مشروع قانون التجارة المصري، وكذلك مشروع القانون البحريني، وجميعها قيد الإصدار، وقد صدر فعلاً في تونس القانون رقم (83)في 2000/8/9م المتعلق بالتجارة الإلكترونية، وكذلك قانون المعاملات الإلكترونية الأردني رقم (85) لسنة 2001م، وكذلك القانون رقم (2) لسنة 2002م بشأن المعاملات والتجارة الإلكترونية في إمارة دبي (العتيبي، 2013).

الفصل الثاني

الحماية الجنائية الإجرائية للمستهلك في السوق الإلكتروني

تُعد شبكة الإنترنت فضاءً واسعًا للإعلان والترويج الإلكتروني عن السلع والخدمات، إذ تجاوزت في تأثيرها ونطاقها وسائل الإعلان التقليدية، لما توفره من سرعة في الانتشار واتساع في دائرة المتلقين. ويُعرَّف الإعلان بأنه كل وسيلة تهدف إلى الترويج لسلعة أو خدمة بقصد تسويقها والتأثير في إرادة المستهلك، بما يجعل الإعلان الإلكتروني أحد أكثر الأدوات تأثيرًا في السلوك التعاقدي للمستهلك داخل السوق الإلكتروني، نظرًا لما يحمله من بعد معنوي وتوجيهي مباشر (ابراهيم، 2008، صفحة 81).

وقد أفرز هذا الواقع حاجة ملحّة إلى إرساء حماية جنائية إجرائية فعّالة، قادرة على مواجهة خصوصية الجرائم الإلكترونية وما تتسم به من تعقيدات تقنية، وصعوبات في التتبع، وإشكاليات في التكييف القانوني، فضلًا عن القصور النسبي في النصوص الإجرائية التقليدية عن استيعاب هذه الجرائم المستحدثة.

ويُعد تدخل المشرّع في المجال الإجرائي ضرورة حتمية لتحقيق التوازن بين فعالية الملاحقة الجزائية من جهة، وضمان الحقوق والحريات الدستورية للمستهلك من جهة أخرى .

وانطلاقًا من ذلك، يتناول هذا الفصل إلى ملحقين رئيسين :

- المبحث الأول : خصوصية الملاحقة الجنائية الإجرائية في جرائم السوق الإلكتروني.
- المبحث الثاني: خصوصية الإثبات الجنائي في الجرائم الإلكترونية.

المبحث الأول
خصوصية الملاحقة الإجرائية

أفرز التطور التكنولوجي المتسارع واتساع نطاق السوق الإلكتروني في فلسطين واقعًا قانونيًا مستحدثًا، فرض تحديات جوهرية على منظومة العدالة الجنائية، ولا سيما في جانب الملاحقة الإجرائية للجرائم الواقعة على المستهلك الإلكتروني(حجازي، شرح قانون العقوبات: القسم العام، 2007، الصفحات 45–50).

وتكمن الملاحقة في طبيعة إجراءات البحث والتحري التي يجب أن تراعي الخصوصية الرقمية للأدلة الإلكترونية، كما تمتد هذه الخصوصية إلى مرحلة التحقيق الابتدائي وما يصدر عنها من قرارات إجرائية. وفي هذا الإطار، ذهب جانب من الفقه إلى أن الجرائم الإلكترونية قد استعصى إدراجها ضمن الأوصاف الجنائية التقليدية، وذلك بسبب قصور وهشاشة أنظمة الملاحقة الإجرائية المعمول بها عن استيعاب هذه الظاهرة الإجرامية المستحدثة، سواء على مستوى الملاحقة الجنائية في إطار القوانين الوطنية أم على صعيد الملاحقة الجنائية الدولية، مما يستدعي إعادة النظر في الآليات الإجرائية القائمة وتطويرها بما ينسجم مع الطبيعة التقنية لهذه الجرائم.(الزنداني، 2020، صفحة 8).

وانطلاقًا مما سبق، تبرز الحاجة إلى دراسة خصوصية الملاحقة الإجرائية في الجرائم التي تمس المستهلك الإلكتروني، بما يضمن تحقيق العدالة الجنائية وعدم إفلات الجناة من العقاب، دون الإخلال بضمانات المحاكمة العادلة. وعلى هذا الأساس، سيتم تناول هذا المبحث من خلال مطلبين رئيسيين: يتناول المطلب الأول خصوصية إجراءات البحث والتحري، في حين يُخصص المطلب الثاني لبيان خصوصية إجراءات التحقيق في الجرائم الواقعة على المستهلك الإلكتروني.

المطلب الأول
خصوصية إجراءات البحث والتحري

إن ظاهرة جرائم الانترنت هي ظاهرة إجرامية مستجدة نسبياً تقرع في جنباتها أجراس الخطر، لتنبيه مجتمعات العصر الراهن حجم المخاطر وهول الخسائر (مدين، 2020)، فتتميز الجرائم الإلكترونية، ولا سيما الجرائم الواقعة على المستهلك الإلكتروني، بخصوصية إجرائية تفرضها طبيعتها التقنية وبيئتها الرقمية، إذ تُرتكب غالبًا في فضاء افتراضي يتسم بالسرعة والتعقيد وصعوبة تتبع الجناة وتحديد هوياتهم.

وانطلاقًا من ذلك، سيتم تناول هذا المطلب من خلال ثلاث فروع متتالية؛ يُعنى الفرع الأول بخصوصية إجراءات البحث في الجرائم الإلكترونية، بينما يتناول الفرع الثاني خصوصية إجراءات التحري، وذلك في إطار السوق الإلكتروني الفلسطيني، ثم أخيراً الفرق بين إجراءات البحث عن إجراءات التحري.

الفرع الاول

خصوصية اجراءات البحث

تعد إجراءات البحث من الخطوات الأولى والحاسمة في مسار الملاحقة الجنائية للجرائم الإلكترونية التي يتعرض لها المستهلك الالكتروني، حيث تشكل نقطة الانطلاق ونطقه الاساس لكشف تفاصيل الجريمة وجمع الأدلة الأولية اذ ان إجراءات البحث في السوق الإلكتروني تتميز بخصوصيات مختلفة وفريدة عن تلك المتبعة في الجرائم المتعلقة في السوق الفلسطيني التقليدي والتي تنبع من طبيعة السوق الالكتروني الذي لا يتسم بحدود جغرافية محدده وثابتة ولا يتسم بصفات واضحة او محليه او مكانيه او زمانية اذ ان كل شيء يتميز في كونه مختلف وغير متوقع ومرن للغاية وصعب تحديده بدقه إضافة إلى تعقيد الأدلة الالكترونية وصعوبة الوصول إليها مقارنة بالأدلة المتعلقة بالجرائم المستهلك التقليدية لذلك فإن تنظيم هذه الإجراءات بشكل دقيق ومتوازن يتطلب مراعاة الخصوصية القانونية والاجرائية والشخصية لضمان سلامة الأدلة وعدم انتهاك حقوق الأفراد او سلامه خصوصياتهم .

و في القانون الفلسطيني، تُنظم إجراءات البحث وفقًا لقانون الإجراءات الجزائية رقم (3) لسنة 2001م، الذي يحدد الإطار القانوني لضمان شرعية هذه الإجراءات، مع ضرورة حصول الجهات المختصة على اذن قضائي مسبق في حالات البحث التي تمس خصوصية الافراد او الشركات او أي جهة كانت .

و تتميز إجراءات البحث في الجرائم الإلكترونية بوجوب وجود اليات وتقنيات خاصة لتحقيق الغاية منها وانجاز المطلوب منها باستخدام أدوات وبرمجيات متقدمة ومتطورة لجمع البيانات الرقمية والالكترونية وتحليلها ودراستها إضافة إلى ضرورة التواصل مع الجهات الفنية المسئولة لضمان التحديث المستمر في هذه التقنيات، مثل التشفير أو التخزين والتحقيق الخصوصية والسرية و إن هذه الخصوصية الالكترونية تضفي على إجراءات البحث مفهوم مختلف تماما عن ما هو متعارف عليه في الجريمة التقليدية والذي بالضرورة يتطلب من الأجهزة الأمنية والقضائية والتنفيذية والمؤسسات تطوير مهاراتها وقدراتها باستمرار لمواكبة هذا الكم الهائل من التطورات الالكترونية و الرقمية.

وتُعد إجراءات البحث مرحلة أساسية ومهمة تسبق التحقيق الجنائي وتبني وتوضح الاسس السليمة للوصول الى حل الجرائم الالكترونية وتهدف إلى جمع المعلومات الأولية حول وقوع الجريمة وتحديد معالمها وهوية المشتبه بهم تحليل كل البيانات والبحث عن الادلة الجنائية ودراسة وتفصيل كل شيء من الممكن ان يوضح هذه الجريمة فقد نظّم المشرّع الفلسطيني هذه المرحلة ضمن قانون الإجراءات الجزائية رقم (3) لسنة 2001، واضعًا ضوابط واضحة وصريحه لحدود صلاحيات مأموري الضبط القضائي و الاليات المتبعة لتحري الجريمة وجمع الاستدلالات و الادلة والخيوط .

اذ تنص المادة (21) من القانون على أن: "يقوم مأمورو الضبط القضائي، كلٌ في دائرة اختصاصه، بالبحث والتحري عن الجرائم، وجمع المعلومات والأدلة التي تؤدي إلى الكشف عنها وعن مرتكبيها." وهو نص صريح يبين أن مرحلة البحث تدخل ضمن الصلاحيات المخولة لمأموري الضبط القضائي قبل مباشرة التحقيق الابتدائي من قبل النيابة العامة .

تُبيّن المادة (22) من قانون الإجراءات الجزائية رقم (3) لسنة 2001 أن عمل مأموري الضبط القضائي لا يقتصر على الجرائم المشهودة أو الظاهرة، وإنما يمتد ليشمل جمع المعلومات الأولية والتحري استنادًا إلى الشكاوى المقدمة من الأفراد أو تلك التي يتم الكشف عنها تلقائيًا. وتبرز أهمية هذا الدور في الجرائم الإلكترونية الواقعة على المستهلك الإلكتروني، حيث يعتمد كشف الجريمة في الغالب على مؤشرات رقمية غير محسوسة، مثل عناوين بروتوكول الإنترنت (IP)، وتتبع التحركات الإلكترونية المشبوهة، ورصد الحوالات المالية غير الاعتيادية، واكتشاف المواقع الوهمية أو الروابط الضارة ووقائع الاختراق، الأمر الذي يستلزم تعاونًا تقنيًا عالي الكفاءة مع جهات متخصصة في الأمن السيبراني لضمان فعالية التحري وسلامة الدليل.

وفي هذا السياق، يواجه التحقيق في الجرائم الإلكترونية تحديًا عمليًا يتمثل في محدودية الخبرة التقنية لدى عدد من مأموري الضبط القضائي وبعض القائمين على التحقيق، نتيجة ضعف الثقافة الرقمية وأمن المعلومات، وهو ما قد يؤثر سلبًا على كفاءة إجراءات التحري وجمع الأدلة الإلكترونية وحجيتها أمام القضاء. وقد أشار الفقه إلى ضرورة إشراك مختصين في أمن المعلومات الجنائي ضمن فرق التحقيق والمحاكمة، ومواكبة المستجدات التقنية الحديثة، بما يضمن حسن إثبات الجرائم الإلكترونية دون المساس بالضمانات القانونية أو انتهاك خصوصية الأفراد(الرشيد، 2022، صفحة 64).

ويؤكد الفقه القانوني أن مرحلة البحث تُعد من أدق مراحل الدعوى الجزائية وأكثرها حساسية، لما يترتب عليها من آثار مباشرة على سلامة الإجراءات اللاحقة ومشروعية الأدلة المستمدة منها، إذ إن أي تجاوز أو إخلال بالضوابط القانونية في هذه المرحلة قد يؤدي إلى بطلان الدليل أو استبعاده أمام جهات التحقيق أو القضاء(شمالة،، 2010، صفحة 115).

من جهة أخرى، فإن الدستور الفلسطيني (القانون الأساسي المعدل لسنة 2003) ينص في المادة (10) على أن: "حقوق الإنسان وحرياته الأساسية ملزمة وواجبة الاحترام"، مما يعني أن كل إجراء بحث يجب

أن يوازن بين متطلبات الأمن العام وحقوق الأفراد دون أي اعتداء على خصوصيه الافراد وسرية بياناتهم وحياتهم الشخصية او الالكترونية وهو ما يظهر بشكل خاص في قضايا المستهلك الإلكتروني، حيث قد تمس إجراءات البحث خصوصية البيانات ومراسلات الأفراد ومعلوماتهم وبياناتهم الالكترونية و / او الشخصية وهو المحظور بنص الدستور.

تشير إحدى الدراسات المتخصصة في الجرائم الإلكترونية في فلسطين إلى أن القصور في الإطار القانوني الناظم لإجراءات البحث والتحري الإلكتروني ما زال يُشكّل فجوة تشريعية واضحة، لا سيما في ما يتعلق بآليات جمع البيانات من مزودي خدمات الاتصالات والإنترنت، الأمر الذي يستدعي وجود تنظيم قانوني خاص للجريمة الإلكترونية يتكامل مع قانون الإجراءات الجزائية بما يضمن فعالية الملاحقة الإجرائية وسلامتها(جرادات، 2021، الصفحات 89-91).

ان الإطار القانوني لإجراءات البحث في فلسطين مستند إلى قانون الإجراءات الجزائية رقم (3) لسنة 2001، لكنه بحاجة إلى تحديث تشريعي كبير يتلاءم مع خصوصيات جرائم المستهلك الإلكتروني بما يضمن حماية حقوق المستهلك الالكتروني وضمان عدم التعدي على بياناته الشخصي او معلوماته الخاصة او حياته الشخصية من جهة ومن جهة اخرى ضمان تحقيق العدالة القانونية ووجود اليات قانونية الكترونية ومتطورة ومستحدثه مع فريق قانوني من مأموري الضبط ذو خبرة واسعة لضمان تحقيق اقصى درجات الحماية القانونية للمستهلك وضمان عدم التعدي عليه بذات الوقت.

و تتسم الجريمة الالكترونية بخصوصية فريدة وخاصة تقنيه كانت او قانونية تجعلها مختلفة اختلاف كلي عن الجرائم التقليدية المرتكبة ضد المستهلك الالكتروني وذلك ليس في طريقه او وسائل ارتكابها بل في طبيعتها الخاصة المتعلقة في الادلة الكاشفة لها والبيئة الالكترونية المعقدة التي تتم فيها ارتكابها فان هذه الجرائم الالكترونية غالبًا ما تُرتكب عبر الإنترنت باستخدام أجهزة إلكترونية مثل الهواتف والحواسيب وأجهزة خاصة ومواقع تواصل ومنصات عالمية او محلية وهمية كانت ام حقيقة ما يجعل الوصول إلى

مرتكبيها واكتشاف ادلة ارتكابها صعب ويتطلب خبرة كبيرة واليات الكترونية معقدة ومتطورة وتقنيات متقدمة والتي لا يمكن تحققها بالإجراءات التقليدية المتبعة وقد أدى ذلك إلى ضرورة تطوير أدوات وإجراءات البحث مع ضمان التزامها بالقانون وخصوصية بيانات الافراد او معلوماتهم الشخصية ولا سيما الحق في الخصوصية الرقمية (جرادات، 2021، الصفحات 89-91)

رغم صدور قرار بقانون رقم (10) لسنة 2018 بشأن الجرائم الإلكترونية، إلا أن المشرّع الفلسطيني لم يضع إطارًا إجرائيًا خاصًا ينظم إجراءات البحث والتحري في الجرائم الإلكترونية الواقعة على المستهلك الإلكتروني، وإنما اقتصر هذا القرار على تجريم عدد من الأفعال المرتكبة باستخدام الوسائل الإلكترونية دون التطرق إلى تنظيم آليات الملاحقة الإجرائية الخاصة بها. وبناءً عليه، تظل القواعد العامة المنصوص عليها في قانون الإجراءات الجزائية رقم (3) لسنة 2001 هي الإطار القانوني الحاكم لإجراءات البحث والتحري في هذا النوع من الجرائم.

وفي هذا السياق، تنص المادة (21) من قانون الإجراءات الجزائية على أن مأموري الضبط القضائي مكلفون بالبحث والتحري عن الجرائم، كلٌّ في دائرة اختصاصه، وجمع الاستدلالات والمعلومات التي تؤدي إلى كشفها وكشف مرتكبيها، وهو ما يُشكّل الأساس القانوني الذي تستند إليه الجهات المختصة، بما فيها وحدات الجرائم الإلكترونية، في مباشرة إجراءات البحث والتحري، حتى في الجرائم المرتكبة في البيئة الرقمية.

لكن هذا الأساس العام لا يكفي وحده لملاحقة مرتكبي الجريمة الإلكترونية التي تتم عبر بيئة الكترونية رقمية تتطلب تقنيات مختلفة عن التقنيات المتبعة في الجرائم التقليدية فعلا سبيل المثال لا الحصر تتبع عناوين IP و تحليل بيانات الدخول واسترجاع المحذوف من الأجهزة وهي إجراءات معقدة تمس معلومات شخصية خاصة وبيانات شخصية حساسة محمية قانوناً وبموجب الدستور فعلى سبيل المثال لا الحصر فان حالة اختراق بريد إلكتروني أو حساب مصرفي او الكتروني يوجب على الجهات القضائية

المكلفة بالبحث أن تتعامل مع بيانات حساسة وشخصيه تتعلق بمراسلات خاصة وبيانات محمية وأحيانًا بيانات مصرفية مالية مما يُلزمها بالتقيد التام بقواعد التفتيش الإلكتروني التي تشترط إذنًا قضائيًا مسبقًا اذ ان المادة (39) من قانون الإجراءات الجزائية تنص على أنه "لا يجوز تفتيش أي شخص أو مسكن أو ضبط أي شيء إلا في الأحوال التي يبينها القانون وبموجب أمر صادر عن الجهة المختصة". هذه المادة تنطبق كذلك على الأجهزة الإلكترونية، بحسب التفسير القضائي الموسع لمفهوم "المكان". اذ ان المكان ليس شرطا ان يكون منزل او شيء مادي ملموس فان البيانات الموجودة في الاجهزة والمعلومات الخاصة في المراسلات تعتبر من قبيل المكان بالمفهوم الواسع له .

وان الخصوصية البحث لا تقتصر في الجرائم الإلكترونية على محل التفتيش فحسب (كدواني و شريهان، 2023، صفحة 147)، وإنما تمتد إلى كيفية جمع الأدلة الرقمية وحفظها وتحليلها وتكييفها القانوني، بما يتطلب مراعاة المبادئ الدستورية المتعلقة بحماية الحقوق والحريات الأساسية، وعلى رأسها الحق في الخصوصية. ويُجمع الفقه على أن تفتيش الأجهزة الإلكترونية أو البيانات الشخصية يجب أن يتم في نطاق الجريمة محل البحث وبحدودها، دون التوسع في المساس بالبيانات الخاصة غير المرتبطة بالفعل الجرمي، وهو ما يفرض على القائمين على إجراءات البحث امتلاك كفاءة قانونية وفنية عالية تضمن تحقيق التوازن بين متطلبات الملاحقة الجنائية واحترام الحقوق الدستورية للأفراد(شمالة،، 2010، صفحة 115).

وتبرز الإشكالية الأكبر في غياب النصوص التشريعية من المشرع الفلسطيني التي تتسم بالوضوح وتعنى بالتنظيم المتعلق في قواعد التفتيش في الجرائم الالكترونية فحتى يومنا هذا لا يوجد أي قانون خاص بالجرائم الالكترونية المرتكبة ضد المستهلك الالكتروني وإنما يتم الاستناد إلى أحكام عامة واللجوء الى التكييف في كثير من الحالات مما يجعل بعض الإجراءات عرضة للبطلان او عدم الصلاحية القانونية خاصة إذا طُعِن فيها بعدم التناسب أو انتهاك الخصوصية وقد أكد الباحث رائد الدويك في بحثه بعنوان حماية الخصوصية الرقمية في فلسطين أن معظم مذكرات التفتيش الإلكتروني التي تصدر حاليًا لا

تستوفي الشروط التي تضمن حماية البيانات الشخصية للمتهم أو المشتبه به ما يُضعف من حجية الدليل الرقمي أمام المحاكم (الدويك، 2022، صفحة 27).

من ناحية أخرى، فإن الجهات القانونية الفلسطينية تواجه تحديًا كبيرًا في الحصول على البيانات الرقمية من الشركات العالمية المزودة للخدمات مثل فيسبوك وغوغل وواتساب بسبب عدم وجود اتفاقيات رسمية ملزمة معها مما يُعرقل بشكل كبير سير البحث ويؤدي إلى ضياع الأدلة في كثير من الاحيان او صعوبة العثور على الادلة او عدم مشروعية الحصول عليها وفي ذلك اشار تقرير رسمي صادر عن الأمانة العامة لمجلس الوزراء الفلسطيني عام 2023 أن التعاون الدولي في هذا المجال لا يزال محدودًا ويعتمد غالبًا على المبادرات الفردية أو الوساطات عبر منظمات دولية (الأمانة العامة لمجلس الوزراء، 2023، صفحة 13).

ويرى الباحث أن إجراءات البحث في الجرائم الإلكترونية تُعد من أكثر المراحل الإجرائية تعقيدًا وحساسية، نظرًا لطبيعة الدليل الرقمي التي تجعل سلامته القانونية عرضة للبطلان عند أي خلل إجرائي ولو كان يسيرًا، الأمر الذي يفرض اعتماد تقنيات متقدمة وآليات مستحدثة تتلاءم مع التطور المتسارع في النظم الإلكترونية، إلى جانب ضرورة تمتع جهات الضبط القضائي بدرجة عالية من الخبرة والكفاءة الفنية. غير أن الواقع التشريعي الفلسطيني يكشف عن قصور واضح في تنظيم إجراءات البحث والتحري في الجرائم الإلكترونية، ولا سيما تلك التي تمس المستهلك الإلكتروني، إذ ما زالت هذه الإجراءات تخضع للقواعد العامة في قانون الإجراءات الجزائية ولبعض النصوص المتفرقة في قانون الجرائم الإلكترونية، دون وجود تنظيم إجرائي خاص يراعي خصوصية هذا النوع من الجرائم في جميع مراحلها، بدءًا من جمع الاستدلالات وصولًا إلى التحقيق. ويؤدي هذا القصور إلى إرهاق الجهات القضائية والنيابية في التكييف القانوني والقياس بين النصوص، بما يعرّض الأدلة الرقمية لخطر البطلان نتيجة أي خطأ في الإجراء أو الوصف القانوني. وعلى خلاف ذلك، اتجهت العديد من التشريعات المقارنة إلى إقرار أطر قانونية متخصصة تنظم بدقة إجراءات البحث والتحقيق في الجرائم الإلكترونية،

وهو ما يفتقر إليه التشريع الفلسطيني حتى الآن. وبناءً عليه، يؤكد الباحث على ضرورة تبني إصلاح تشريعي شامل يقوم على استحداث تنظيم إجرائي متكامل ضمن قانون الإجراءات الجزائية أو قانون حماية المستهلك، يُعنى بإجراءات التفتيش والتحقيق وجمع الأدلة الإلكترونية، ويوفر ضمانات واضحة لحماية الخصوصية الرقمية، ويمنح الجهات المختصة صلاحيات محددة ضمن ضوابط قانونية دقيقة، بما يحقق التوازن بين فعالية الملاحقة الجنائية وصون حقوق الأفراد، إلى أن يتحقق ذلك يبقى الاجتهاد القضائي هو الأداة الرئيسية لضبط هذا التوازن في ظل القواعد العامة القائمة.

الفرع الثاني

خصوصية اجراءات التحري

لأعمال التحري وجمع الأدلة اهميه كبيره نتيجة لما تتمتع به السلطة القائمة بإجراءات التحري من نشاط وفعالية اكبر مما تتمتع به سلطات التحقيق الامر الذي يفضي الى امكانيه القائمين بإجراءات التحري من الحصول على معلومات تتعلق بشان الجريمة التي تتصف بالغموض او الخفاء (الحسيناوي، 2018، صفحة 68).

لا تقتصر خصوصية الإجراءات الجنائية في الجرائم الواقعة على المستهلك في السوق الالكتروني على مرحلة البحث فقط بل ان البحث هو من المراحل الابتدائية في كشف هذا النوع من الجرائم ولان البحث هو المرحلة الاولى فان المرحلة الثانية تعتمد على التحري التي تُعدّ من أخطر مراحل ما قبل التحقيق لما تتضمنه من تدخل مباشر او غير مباشر في الخصوصية المتعلقة في الافراد والمحمية بموجب القانون فالتحري هنا هو عمل أمني وقانوني يقوم به المتحري مستخدماً إلى جانب حواسه الخمس الإقامات الإلكترونية الرقمية من الحاسبات والشبكات (الزنداني، إجراءات الاستدلال والتحقيق الابتدائي في الجرائم الإلكترونية وأثرها على حجية أدلة الإثبات [أطروحة دكتوراه]، 2020، صفحة 83)، وذلك في الجرائم الواقعة على المستهلك الإلكتروني يتطلب متابعة الأنشطة الافتراضية او الحركات المالية او المواقع الالكترونية وجمع معلومات حساسة تتعلق بالمراسلات بين الافراد او المستهلكين مع المزودين او التجار

و ايضا الحسابات البنكية او تفاصيل عقد الشراء الالكتروني وكل ذلك ضمن بيئة لا تترك أثرًا ماديًا تقليديًا كالموجود في التعاملات الاستهلاكية او التجارية التقليدية بين المستهلك التقليدي والتاجر ومن هذا المنطلق برزت أهمية تنظيم هذه المرحلة بقواعد قانونية دقيقة توازن بين تحقيق الغاية من الملاحقة الجنائية للجريمة وحماية الخصوصية الالكترونية والشخصية للمستهلك الالكتروني (الزنداني، إجراءات الاستدلال والتحقيق الابتدائي في الجرائم الإلكترونية وأثرها على حجية أدلة الإثبات [أطروحة دكتوراه]، 2020، صفحة 83).

وبالعودة الى قانون الإجراءات الجزائية الفلسطيني، نجد أن الضابطة القضائية مهمتها التحري عن الجرائم بعد وقوعها والبحث عن مرتكبها، حيث يتولى رجال الضابطة القضائية مهمة جمع الاستدلالات عن طريق التحري عن الجرائم ومرتكبيها وإثبات كافة الإجراءات التي يقومون بها (الوليد، 2024، الصفحات 265–270)، فقد نصت المادة 22 منه على أن من مهام مأموري الضبط القضائي "التحري عن الجرائم وجمع ما يلزم من معلومات بشأنها"، ما يشمل كافة الأفعال الاستباقية التي يقوم بها مأموري الضبط القضائي بناءً على ورود شكوى او بلاغ أو او حالة التلبس وبالعودة الى الجرائم الواقعة على المستهلك الالكتروني في السوق الالكتروني فان التحري أكثر حساسية واكثر تعقيدا لأنه يعتمد على تحليل بيانات شخصية ومعلومات الكترونية حساسة قد تمتد الى خصوصيات الافراد وتفاعلاتهم عبر الإنترنت مما يجعل أي خطأ إجرائي سببًا في الطعن بالبطلان لاحقًا او بصحة هذا الدليل كحجة صحيحة امام القضاء كما أن طبيعة الجريمة المتصفة بأنها الكترونية توجب أن تتم معظم إجراءات التحري عبر أدوات تقنية و برامج الكترونية مثل برامج تحليل الشبكات و أدوات استعادة البيانات وتطبيقات تتبع المواقع الإلكترونية و الحركات المالية والحركات المشبوهة في المواقع الوهمية او المواقع التي توجد عليها ملاحظات من قبل الدولة وهنا يبرز الفرق الجوهري بين الجريمة التقليدية الواقعة على المستهلك التقليدي وبين الجريمة الواقعة على المستهلك الالكتروني ففي الجريمة التقليدية يتم التحري ميدانيا في مسرح الجريمة مع وجود دلائل ملموسة ماديا مسرح جريمة فعلي بينما في الجريمة الالكترونية يتم التحري فيها

عن بعد وأحيانًا دون علم المشتبه فيه وهذا الامر يفرض رقابة قضائية مضاعفة على منفذيه القانون حتى لا تُستغل إجراءات التحري في انتهاك حقوق الأفراد او بياناتهم الشخصية او انتهاك خصوصياتهم أو الوصول لمعلومات لا علاقة لها بالجريمة. وقد اكد هذا الامر د. محد ابو زينة في كتابه بعنوان التحري الالكتروني وحدود الملاحقة الجزائية حيث اكد على ان التحري الرقمي يحتاج إلى ضوابط قانونية تفصيلية تتضمن حدود الزمان والمكان والنطاق الفني حتى لا يتحول إلى وسيلة للمراقبة الشاملة او وسيلة لاختراق خصوصية وحياة الافراد (أبو زينة، 2022، صفحة 77).

يعد الحصول على اذن قضائي مسبق هو شرط اساسي في صحة الدليل وحجيته اما القضاء ويكون هذا الاذن موضح به تفاصيل التحري وحدود الصلاحية لمأموري الضبط القضائي كمراقبة البريد الالكتروني مثلا او الرسائل الخاصة او مواقع التواصل الاجتماعي وفي حال تم التحري دون إذن قانوني صحيح ومستوفي الشروط القانونية فإن كل ما يتم جمعه يُعتبر باطلًا حتى وان كان صحيح وحتى وان كان دليل قاطع ويؤكد المبدأ هذا في اجتهادات محكمة النقض الفلسطينية، التي اعتبرت أن "أي جمع لمعلومات تمس الحياة الخاصة دون أمر قضائي يُعدّ باطلًا حتى وإن كشفت عن جريمة"(محكمة النقض الفلسطينية، طعن جزائي رقم (2018/644) (جلسة 7 أبريل)، 2019).

و من جهة أخرى، فإن المستهلك الإلكتروني غالبًا ما يكون الطرف الأضعف في المعاملات الالكترونية خاصة وانه في كثير من الاحيان يتعامل مع طرف لا يعرف هويته الحقيقة ومدى مصداقيته ويكون معرض دائما للوقوع في حالات النصب او الاحتيال او الخداع او الغبن ولهذا فإن التحري في هذه القضايا يتطلب من مأموري الضبط تتبع معاملات إلكترونية عبر منصات الكترونية تكون داخل و / او خارج فلسطين مما يجعل هذه المهمة صعبه للغاية خصوصًا في غياب اتفاقيات التعاون الدولية التي تمنحهم الاذن في تتبع و التحري عن الدلائل عبر المنصات الالكترونية في خارج فلسطين وقد أشار تقرير الأمانة العامة لمجلس الوزراء في 2023 إلى أن ضعف البنية القانونية في هذا المجال يؤدي إلى

فقدان العديد من الأدلة الالكترونية خلال مرحلة التحري أو إلى عدم قبولها لاحقًا في المحكمة لأي سبب من الممكن ان يعرضها للبطلان(الأمانة العامة لمجلس الوزراء، 2023، صفحة 17).

وفي البحث في خصوصية إجراءات التحري يتبيّن أن هذه المرحلة في الجرائم الإلكترونية ليست مجرّد جمع معلومات أولية تساعد المحقق في الوصول الى الدليل القاطع بل هي في الحقيقة الاساس والركيزة الاساسية التي تم بها البناء في كافه مراحل كشف هذه الجريمة وتحقيق العدالة اذ ان خطا واحد فيها ولو كان بسيط من الممكن ان يؤدي الى فقدان الحقوق وسقوط الدليل فالتحري في الجرائم الواقعة على المستهلك الالكتروني لا تقتصر فقط على معرفة هوية الفاعل فحسب بل هي امتداد لمجموعة كبيرة ومعقدة من الاجراءات من تحليل العقود الالكترونية والإعلانات الخادعة المضللة والمواقع الوهمية وتتبع لحركات الاموال والمصارف والحوالات المالية داخلية كانت ام خارجية و كل هذه الإجراءات تحتاج إلى أدوات متخصصة وخبرة كبيرة قد لا يمتلكها مأموري الضبط القضائي التقليديين في الجرائم التقليدية مما يجعل الدول امام مهمة صعبة في تدريب مأموري ضبط قضائي ذات كفاءة عالية في التحري الالكتروني وعلى دراية واسعة وشامله لحدود صلاحياتهم القانونية مما يضمن تحقيق العدالة وبذات الوقت عدم انتهاك خصوصية الافراد (الزنداني، 2020، صفحة 75).

وفي النصوص القانونية الفلسطينية لا يوجد نصوص قانونية واضحة وصريحة تنظم عملية التحري في الجرائم الالكترونية مما يفتح المجال امام جهات تنفيذ القانون للاجتهاد والقياس والربط والتوسع الامر الذي قد يؤدي في بعض الاحيان الى انتهاكات جسيمة تمس خصوصيات الافراد ويؤكد الباحث القانوني محمد جرادات أن هذا الغموض القانوني هو أحد الأسباب الرئيسية التي تجعل الأدلة الرقمية غير مقبولة أحيانًا أمام المحاكم لأن طرق جمعها تفتقر للغطاء التشريعي الواضح خصوصًا عندما يتم التحري عبر وسائل التواصل الاجتماعي أو الرسائل المشفّرة (جرادات، 2021، ص.92)

وتكمن خطورة التحري في الجرائم الالكترونية في أنه يمكن أن يتحوّل بطريقة ما إلى مراقبة جماعية إن لم يكن مقيدًا قانونيًا ومحددا للصلاحيات القانونية اذ انه من الممكن ان يتوسع التحري عن الدليل ويصل الامر الى الوصول الى بيانات شخصية وانتهاك لخصوصية مجموعة من الاشخاص ليس فقط المشتبه به الرئيسي حيث ان القانون الاوروبي لحماية البيانات (GDPR تُلزم الجهات الأمنية بتحديد غرض التحري بدقة والاقتصار على أقل قدر ممكن من البيانات وهي معايير ما زال القانون الفلسطيني بحاجة إلى تطويرها ودراستها وتحليلها لتطبيقها بأفضل طريقة وبأكثر طريقة تحمي الحقوق من جهة وتحقق العدالة من جهة اخرى وفي هذا السياق، تُظهر دراسة نُشرت في جامعة بيرزيت أن السلطة التقديرية الواسعة التي تُمنح أحيانًا لمأموري الضبط تؤدي إلى تجاوزات غير مقصودة و ربما مقصودة في احيان اخرى خصوصًا في غياب رقابة قضائية فورية ومتابعة دقيقة ودورية لكل تفاصيل عملية التحري (مركز إبراهيم أبو لغد للدراسات، 2022، ص. 44).

على أرض الواقع يواجه مأموري الضبط القضائي والنيابة العامة تحديات كبيرة في التحري على الجرائم الواقعة على المستهلك الالكتروني تتعلق بإثبات الركن المادي للجريمة والخوف من ضياع الدليل وسهوله التلف او الحذف او التعديل خصوصًا في حالات الإعلانات التجارية الكاذبة أو منصات البيع الوهمية فان تتبعها خصوصا اذا كانت خارج حدود فلسطين امر بالغ في الصعوبة والخطورة فالبائع قد يستخدم أسماء مزيفة أو يعمل من خارج فلسطين مما يجعل الوصول إليه أمرًا معقدًا ووجوب وجود اتفاقيات دولية تعاونية في هذا الخصوص لذلك فإن التحري هنا يشمل استخدام أدوات التحقيق المفتوح (OSINT) مثل تحليل الروابط الإلكترونية التحقق من مصدر الصور تتبع الرسائل التسويقية وغيرها من الأساليب غير التقليدية التي يجب أن تعتمد على دليل رقمي قابل للتوثيق والتقديم أمام المحكمة(المناصرة، 2023)

لذلك قضت محكمة النقض المصرية بأنه:" لا تثريب على مأموري الضبط القضائي فيما يقومون به من التحري عن الجرائم بقصد اكتشافها ولو اتخذوا في سبيل ذلك التخفي وانتحال الصفات حتى يأنس الجاني

لهم، ويأمن جانبهم وليتمكنوا من أداء واجبهم ما دام أن إرادة الجانب تبقى حرة غير معدومة(الوليد، 2024، صفحة 271).

أما عن الإجراءات الشكلية في التحري، فهي تشمل – حسب ما أوضحه جانب من الفقه، إصدار محاضر واضحة، تحديد زمان ومكان التحري بدقة، وتوثيق كل خطوة تتم بوسائل فنية تحفظ سلامة الدليل. إذ إن أي تلاعب أو قصور في المحاضر قد يؤدي إلى فقدان الدليل الرقمي لحجيته القضائية (شمالة،، 2010، صفحة 118).

ويرى الباحث في ان مرحلة التحري هي المرحلة التي تبنى عليها ملامح الجريمة الالكترونية لذا فان هذه المرحلة مهمة وحساسة للغاية وتطلب بذات الوقد فريق قضائي ذو خبرة وكفاءة عالية في معرفة حدود الصلاحيات المنوط بهم حمايتها وبذات الوقت الوصول الى خيوط الجريمة وحلها تباعا وفي فلسطين نجد بان هذا الامر يكاد يكون غير موجود نظرا لضعف الامكانيات وضعف النصوص القانونية التي تجعل من جهات تنفيذ القانون أمام خيارات متعددة مثل القياس والاجتهاد والتكييف القانوني الامر الذي من الممكن ان يعرضهم الى فقدان حجية الدليل امام القضاء بسبب انتهاك خصوصيات البيانات الخاصة بالمستهلكين او المشتبه بهم او لأي سبب كان لذا انا ارى بانه يجب تجهيز فريق عمل متكامل وتدريبه على مثل هذه الامور وعدم الاكتفاء بوجود جهاز او فرع في جهاز يعنى بالجرائم الالكترونية والمعروف للجميع بان مأموريه الضبط القضائي في فرع الجرائم الالكترونية هم بذاتهم مأموري الضبط القضائي في الجرائم التقليدية ويجب على المشرع تعديل وإضافة باب خاص في قانون الاجراءات لتوضيح حدود واليات التحري التي يجب اتباعها في الجرائم الواقعة على المستهلك الالكتروني .

الفرع الثالث

الفرق بين إجراءات البحث وإجراءات التحري

لفرق الجوهري بين إجراءات البحث وإجراءات التحري

من خلال تحليل الفرعين، يتبيّن أن إجراءات البحث وإجراءات التحري وإن كانتا تندرجان ضمن أعمال مأموري الضبط القضائي، إلا أن لكل منهما طبيعة قانونية ووظيفية مختلفة، خاصة في الجرائم الإلكترونية الواقعة على المستهلك الإلكتروني.

من حيث المرحلة الإجرائية

- إجراءات البحث

تمثل المرحلة الأولية السابقة على التحري، وتهدف إلى اكتشاف وقوع الجريمة من الأساس، وجمع معلومات أولية عامة حولها، دون تركيز مباشر على شخص معين كمشتبه به.

- إجراءات التحري

تأتي لاحقًا لإجراءات البحث، وتُباشر عندما تتوافر مؤشرات جدية على وقوع الجريمة، وتهدف إلى تضييق دائرة الاشتباه وتتبع الفاعل أو المساهمين في الجريمة.

من حيث الهدف

- البحث:

غايته الأساسية كشف معالم الجريمة، وتحديد طبيعتها، وبيان ما إذا كانت هناك جريمة أصلًا، وذلك من خلال رصد المؤشرات الرقمية العامة، مثل بلاغات المستهلكين، أو وجود مواقع وهمية، أو شكاوى أولية.

- التحري

يهدف إلى تعميق المعلومات التي تم التوصل إليها في مرحلة البحث، وتتبع الأنشطة الإلكترونية والمالية المرتبطة بالفعل الجرمي، وصولًا إلى بناء تصور شبه متكامل عن الجريمة ومرتكبها.

من حيث درجة المساس بالخصوصية

- إجراءات البحث

تكون أقل مساسًا بالخصوصية، وغالبًا ما تقتصر على جمع بيانات عامة أو أولية، ولا تتطلب بالضرورة الدخول في تفاصيل دقيقة تتعلق بالحياة الخاصة أو البيانات الحساسة، إلا في نطاق ضيق ومحدد.

- إجراءات التحري

تُعد أكثر خطورة وحساسية، لأنها قد تنطوي على تتبع الحسابات الإلكترونية، أو الحركات المالية، أو المراسلات الخاصة، وهو ما يجعلها أكثر ارتباطًا بضرورة الحصول على إذن قضائي وضبط نطاقها بدقة.

من حيث الوسائل المستخدمة

- البحث

يعتمد أساسًا على وسائل الرصد الأولي وجمع البلاغات، وتحليل المؤشرات الرقمية العامة، والتواصل مع الجهات الفنية للحصول على معلومات أولية دون تعمق تقني شديد.

- التحري

يعتمد على أدوات تقنية متقدمة، مثل تحليل الشبكات، تتبع عناوين IP، استرجاع البيانات، تحليل المعاملات المالية الإلكترونية، واستخدام أدوات التحقيق الرقمي (OSINT)، وهو ما يتطلب خبرة تقنية عالية.

من حيث الأثر على سلامة الدليل

- إجراءات البحث

تمهّد الطريق لجمع الأدلة، لكنها لا تُنشئ بالضرورة دليلًا حاسمًا، وإنما تُسهم في توجيه مسار التحقيق لاحقًا.

- إجراءات التحري

يُبنى عليها الدليل الجنائي الرقمي بصورة مباشرة، وأي خطأ فيها قد يؤدي إلى بطلان الدليل أو استبعاده أمام القضاء.

يتضح مما سبق أن إجراءات البحث تختلف عن إجراءات التحري من حيث المرحلة والغاية ودرجة المساس بالخصوصية وطبيعة الوسائل المستخدمة، إذ تمثل إجراءات البحث مرحلة تمهيدية أولية تهدف إلى كشف الجريمة ورصد مؤشراتها العامة، في حين تُعد إجراءات التحري مرحلة أكثر تعمقًا وخطورة، تنصب على تتبع الفاعل وجمع الأدلة الرقمية الحساسة. وتبرز هذه الفروق بشكل أوضح في الجرائم الإلكترونية الواقعة على المستهلك الإلكتروني، نظرًا لطبيعة البيئة الرقمية وتعقيد الدليل الإلكتروني، وهو ما يفرض إخضاع كل مرحلة لضوابط قانونية خاصة تضمن فعالية الملاحقة الجنائية دون المساس بالحقوق الدستورية للأفراد.

المطلب الثاني

خصوصية إجراءات التحقيق

في ظل تصاعد النشاط الاقتصادي الرقمي في فلسطين وازدياد اعتماد المستهلك على المنصات الإلكترونية، برزت ضرورة إقرار حماية جنائية خاصة للمستهلك الإلكتروني (كميل، 2023، صفحة 69). وتفرض طبيعة هذه الجرائم، من حيث أساليب ارتكابها والأدوات المستخدمة فيها، خصوصية إجرائية مغايرة لتلك المعتمدة في الجرائم التقليدية، لا سيما في مرحلة التحقيق. وتُعدّ إجراءات التحقيق

حجر الأساس في سلامة الدعوى الجزائية، لما تنطوي عليه من تعامل مع الأدلة الرقمية والبيانات الشخصية والحسابات الإلكترونية والمعاملات المالية. الأمر الذي يستلزم مواءمة أساليب التحقيق مع مفاهيم الخصوصية الرقمية وأمن المعلومات، مع ضمان حقوق جميع الأطراف. ومن هذا المنطلق، لكل ذلك سنقوم بتقسيم ذلك المطلب على النحو التالي :

الفرع الأول

خصوصية التحقيق في الجرائم الإلكترونية

مع تزايد الاعتماد على التجارة الإلكترونية في فلسطين وتطورها بشكل كبير جدا برزت تحديات جديدة تتعلق بحماية المستهلك من الجرائم الإلكترونية الواقعة عليهأو التي من الممكن ان تقع عليه مستقبلا فعلى سبيل المثال لا الحصر جرائم الاحتيال وسرقة البيانات وانتهاك الخصوصية و التضليل والغبن وتقديم معلومات ومواصفات كاذبة وغيره من الجرائم و هذه الجرائم تتطلب آليات تحقيق متخصصة ومختلفة عن تلك المستخدمة والمتبعة في الجرائم التقليدية(حسني، شرح قانون العقوبات: القسم العام، 2022، صفحة 27) التي يتعرض لها المستهلك في السوق التقليدي نظرًا لطبيعتها الالكترونية وتعقيداتها التقنية والغموض المرفق لها في بعض الاحيان.

لذلك عُرف التحقيق في الجرائم الإلكترونية على أنه :"عملية جمع المعلومات والأدلة الرقمية المرتبطة بجريمة ارتُكبت باستخدام الوسائل التقنية أو داخل البيئة الرقمية، كشبكات الإنترنت أو الأنظمة المعلوماتية، بهدف الكشف عن الجناة وتحديد مسؤولياتهم القانونية، مع الالتزام بالضمانات القانونية الخاصة بسرية البيانات وخصوصية الأفراد " (عبدالرحمن ع.، 2019، صفحة 225)

و يُعد قانون الإجراءات الجزائية رقم (3) لسنة 2001 الإطار العام والمرجعية العامة لتنظيم إجراءات التحقيق المتبعة في الجرائم التي ترتكب في فلسطين إلا أن هذا القانون يعاني من قصور واضح وغموض كبير إذ أنه لا يتضمن نصوصًا صريحة تتعلق بالتحقيق في الجرائم الإلكترونية مما يفتح

المجال للاجتهادات والتفسيرات المختلفة والتكييف العائد إلى مختلف القوانين مثل قانون الاجراءات وقانون الجرائم الالكترونية وقانون العقوبات وغيره وقد أشار في ذلك بعض الباحثين إلى أن "القوانين الجزائية القائمة تفتقر إلى إجراءات البحث والتحري وجمع الأدلة وتفتيشها وضبطها"(أبوالرب، 2018).

ان ابرز ما تتسم به الادلة الالكترونية الرقمية هو الهشاشة وسرعة التلاشي وإمكانية الحذف و/أو التعديل مما يستدعي بالضرورة إجراءات تحري سريعة ودقيقة من جهات ذات كفاءة وخبرة عالية في ذلك فالمعلومات المخزنة على الأجهزة الإلكترونية يمكن تعديلها أو حذفها بسهولة الامر الذي يفرض على الجهات المختصة استخدام أدوات وتقنيات متقدمة ومتطورة مع فرق تحقيق ذات خبرة وكفائه عالية لضمان جمع الأدلة بطريقة قانونية وفعالة وذات حجية صحيحة وقانونية امام القضاء وفي هذا السياق جانب من الباحثين على "ضرورة تعديل قانون الإجراءات الجزائية ليشمل قواعد للتحقيق في الجرائم الإلكترونية، والتفتيش في أجهزة الكمبيوتر وأجهزة الاتصال الذكية بما يضمن فعالية ضبط وتحريز الأدلة الرقمية"(عبدالباقي، 2018، صفحة 284).

حفاظاً على أدلة الجريمة وعدم ضياعها، فلم يحدد التشريعات الإجراءات الجزائية لمختلف الدول فترة زمنية محددة يتوجب خلالها الانتهاء من إجراءات التحقيق، ولعل السبب في ذلك اختلاف كل قضية عن الأخرى في ظروفها وعناصرها وكيفية التحقيق فيها(عزيز، 2014، صفحة 117).

مثال تطبيقي محلي: في قطاع غزة، وفي سياق الحرب والأزمات الاقتصادية، تم رصد حالات سرقة للحسابات البنكية للمواطنين عبر استهداف شريحة الهاتف المرتبطة بالحساب البنكي، حيث يقوم المهاجمون بإيقاف الشريحة الأصلية المرتبطة بحساب الضحية ثم الحصول على شريحة جديدة باسم الضحية، ما يمنحهم القدرة على تفعيل رمز الدخول إلى التطبيق البنكي وسحب الأموال دون رضى صاحب الحساب، مما يؤدي إلى خسارة فورية للمستهلك وثقته في المنظومات الإلكترونية(قناة المواطن، 2026) .

تقوم النيابة العامة وهي الجهة المخولة بالتحقيق في الجرائم الالكترونية بمساعدة ضابطة قضائية متخصصة في هذا النوع من الجرائم وهذا يختلف من حيث الاسلوب و الطريقة والكيفية عن الجرائم التقليدية التي تختص بها النيابة العامة بمساعدة مأموري الضبط القضائي ذات الاختصاص العام فالتحقيق في الجرائم الإلكترونية وكيفية ضبط الأدلة الرقمية وجمعها من الموضوعات المستجدة في فلسطين وغيرها من دول العالم(عبدالباقي، 2018، صفحة 285).

يلعب تشفير البيانات دوراً حاسماً في تأمين بيانات المستهلكين (الحق و وعبد العال، 2025، صفحة 201)، إلا أن استخدام الشبكات الخاصة الافتراضية، والتخزين السحابي من أبرز التحديات التي تواجه المحققين في جمع الأدلة الرقمية، إذ تفرض هذه الوسائل واقعًا تقنيًا معقّدًا يتطلب كفاءة عالية في استخدام أدوات التحليل الجنائي الرقمي، بما يضمن سلامة الدليل من جهة، وعدم التعدي على الخصوصية أو البيانات غير المرتبطة بالجريمة من جهة أخرى. فإن إجراءات الحصول على الأدلة الجنائية الرقمية يجب أن تكون ضمن الإطار العام الذي حدده الدستور وإلا فإن الدليل المستمد بطريق مخالف للأحكام الواردة في الدستور يكون باطلاً بطلاناً مطلقاً لتعلقه بالنظام العام (مدين، 2020، صفحة 152).

ونظرًا للطبيعة العابرة للحدود للجرائم الإلكترونية، تبرز أهمية التعاون الدولي كأداة أساسية في إجراءات التحقيق (الرشيد، مرجع سابق، ص65)، وهو ما أكده القرار بقانون رقم (10) لسنة 2018 بشأن الجرائم الإلكترونية، من خلال إقراره مبدأ التعاون مع الجهات النظيرة في الدول الأخرى ضمن الأطر القانونية والاتفاقيات المصادق عليها.

وتثير إجراءات التحقيق في الجرائم الإلكترونية إشكاليات جدية تتعلق بحماية الخصوصية الرقمية، خاصة في ظل غياب تشريع فلسطيني متكامل لحماية البيانات الشخصية، الأمر الذي يفتح المجال لاحتمالات التعدي على الحقوق الرقمية للمستهلك، وهو ما أشار إليه عدد من التقارير الحقوقية التي أكدت أن

القصور التشريعي في هذا المجال يُضعف الضمانات القانونية في مرحلتي التحري والتحقيق (عبدالباقي، 2018، صفحة 286).

وفي هذا السياق، يبرز الدور المحوري لمزودي خدمات الإنترنت والاتصالات في دعم التحقيق الجنائي الإلكتروني، إذ خوّل القرار بقانون رقم (10) لسنة 2018 النيابة العامة صلاحية طلب البيانات والمعلومات الإلكترونية اللازمة لمصلحة التحقيق، ضمن ضوابط قانونية توازن بين متطلبات العدالة الجنائية وحماية الخصوصية الرقمية .

حيث يرى بعض الفقه في أنحاء العالم عقود التجارة الإلكترونية بأنها " مجموع المبادلات المرقة المرتبطة بالأنشطة التجارية بين المشروعات أو بين المشروعات والأفراد أو بين المشروعات والإدارة ويتميز بإلغاء المسافات الجغرافية واختصار الوقت(خليفة، 2020، صفحة 15)نظرًا للتطور السريع في مجال التكنولوجي والاعتماد الكبير من شتى فئات المجتمع سواء المستهلك او التاجر او المؤسسات الحكومية والغير حكومية على الانترنت وعلى هذا الفضاء والعالم الكبير فإنه اصبح امر حتمي تدريب المحققين على احدث تقنيات التحقيق واحدث الادوات المستخدمة في التحقيق والمتبعة عالميا لإنجاز التحقيق بطريقه قانونية وشرعية ومن ثم الوصول إلى تحقيق ناجح وفعّال بالجرائم الإلكترونية، يتطلب اهتمامًا بالتشريع والأنظمة والإجراءات الإلكترونية وحماية الخصوصية، إلى جانب تدريب القضاة وأعضاء النيابة ومأموري الضبط (عبدالباقي، 2018، صفحة 286).

أيضاً ابرز ما يميز الجرائم الواقعة على المستهلك الالكتروني في السوق الالكتروني هو انها تتداخل الجرائم ضد المستهلك الالكتروني مع مجالات تقنية وقانونية دقيقة متعددة مما يفرض على التحقيق أن يتم بدقة عالية وبحساسية عالية للحفاظ على التوازن بين مصلحة العدالة في كشف هذا النوع من الجرائم وحماية حقوق الأفراد المقدسة في القانون من أي اختراق للخصوصية او للبيانات الشخصية فعلى سبيل المثال لا الحصر تحليل المعاملات المالية الالكترونية أو تتبع سلوك المستهلك على المنصات يتطلب

حفاظ وقيود صارمة لخصوصيته وهو أمر نص عليه القانون الأساسي الفلسطيني في المادة (32) التي تحظر انتهاك الخصوصية دون إذن قضائي صريح ومحدد و مسبب مما يقيّد سلطات جهات التحقيق ويمنع التوسع غير المشروع في ملاحقة الأفراد.

إن الأدلة الالكترونية كالبريد الإلكتروني وسجلات تحديد المواقع تخضع لمتطلبات قانونية خاصة حتى تعد صالحة أمام المحكمة وكي تكسب حجيتها امام القضاء وقد أكدت المحكمة العليا الفلسطينية في أحد قراراتها المتعلقة بقضية نصب إلكتروني أن "الإجراءات التي يتم فيها جمع المعلومات الرقمية يجب أن تُثبت قانونيًا لضمان حجيتها، هذا يؤكد أن خصوصية التحقيق لا تقتصر وتتمحور حول طريقة الجمع الادلة بل تمتد إلى تأمين الغطاء القانوني والشرعي لاستخدام المعلومة ذاتها لاحقًا لكسب شرعيتها امام القضاء.

ومن الإشكاليات الاساسية في خصوصية التحقيق في هذا النوع من الجرائم هو أن الجهة التي تحقق في الجريمة قد تضطر في بعض الاحيان للوصول إلى بيانات اشخاص يعتبروا غير متورطين بشكل مباشر في هذه الجريمة او ربما لا علاقة لهم في هذه الجريمة انما كل ما في الامر انهم تعاملوا مع المشتبه به دون أي شبهه تدور حولهم مثل معلومات من حسابات مشبوهة تم تحويل الأموال منها أو إليها او تحركات مالية عبر الحسابات او ورود اكثر من حركه مالية او تجاوز الحد الاعلى للحركات المالية الشرعية وقد أشار الى ذلك بعض الباحثين إلى أن "نطاق التحقيق الإلكتروني الواسع قد يؤدي لانتهاك مبدأ التناسب إذا لم تحدد أوامر التفتيش والضبط بدقة في الجرائم الاقتصادية" (جرادات، 2021، صفحة 94).

يبرز أيضًا في التحقيق الجنائي الإلكتروني مبدأ "حماية البيانات في ظل الرقابة التقنية"، وهو مفهوم قانوني مستحدث نسبيًا في الفقه الفلسطيني حيث أشار د. نعيم أبو فروة إلى أن "التحقيق الرقمي يتطلب

الموازنة بين حماية البيانات الشخصية وتوسيع صلاحيات الضبط القضائي، وهو ما يجب أن يُضبط بنصوص قانونية واضحة" .

ولا بد من الإشارة إلى أثر غياب قانون خصوصية الكترونية فلسطيني مستقل على خصوصية إجراءات التحقيق. لأنه حتى يومنا هذا لا يوجد قانون تفصيلي ينظم حماية البيانات الشخصية والخصوصية في فلسطين مما يجعل المستهلك عرضة لتجاوزات او انتهاكات أثناء مرحله سير التحقيق و هذا ما أكدته دراسة مؤسسة "مسلك" التي أشارت إلى أن "الفراغ التشريعي يهدد بتعطيل الحق في الخصوصية في كافة مراحل الملاحقة، خاصة عند التحقيق مع الضحايا"

اما في الحالات التي تحتاج الى تحقيق دولي بسبب تعدد الاطراف الخارجية او وجود اطراف اجنبية مثل مواقع البيع الأجنبية أو أنظمة دفع عالمية او تجارة عالمية فان تنفيذ التحقيق بطريقه قانونية يصبح أكثر تعقيدًا ويتطلب تدخلًا عبر النيابة العامة أو وزارة الاتصالات من خلال طلبات قانونية قد يتم قبولها وقد ترفض في احيان كثيره وقد أورد الباحث خليل عصفور أن "التعاون القضائي الدولي في الجرائم الرقمية لا يزال ضعيفًا ومجزأً بسبب غياب الاتفاقيات الثنائية (عصفور، 2021، صفحة 78).

مع التأكيد على ان الجهات المنفذة للتحقيق يجب أن تتلقى تدريبات مستمرة لأن الجريمة الالكترونية متطورة بطبيعتها ومتجددة دائما وقد بيّنت دراسة أجرتها النيابة العامة الفلسطينية أن "70% من ضباط الشرطة لا يملكون أدوات تقنية كافية لاكتشاف عمليات النصب الإلكتروني"، مما يهدد مصداقية التحقيق من أساسه

كما أن التحقيق في الجرائم الالكترونية الواقعة على المستهلك لا يهدف فقط إلى تحديد هوية الجاني بل يمتد إلى تعويض الضحية التي وقعت عليها هذه الجريمة التعويض المادي ايضا. وهذا يتطلب توثيقًا دقيقًا لمسار الأدلة الالكترونية بحيث يتمكن القضاء من إلزام الجهة المسؤولة عن الضرر سواء كانت شخصًا طبيعيًا أو اعتباريًا بإعادة الحق الى اصحابه والتعويض عن الضرر الحاصل (فايق، 2026).

و ايضا يلعب عنصر السرعة دورًا محوريًا في التحقيق بالجرائم الواقعة على المستهلك، خاصة عند التعامل مع الجرائم الإلكترونية العابرة للحدود، حيث تتغير طبيعة البيانات أو تختفي كليًا خلال وقت قصير او يتم التلاعب بها بطريقة يصعب اكتشافها او يتم حذفها وفي هذا السياق .

وتكمن خصوصية هذا النوع من التحقيق أيضًا في ارتباطه بأدوات تقنية لا تخضع دومًا للرقابة المباشرة للسلطات الفلسطينية مثل الحسابات على المنصات الدولية او المواقع الاجنبية حتى وان كانت وهمية.

إجراءات التحقيق يجب أن تحترم كذلك مبدأ التناسب، والتوازن بين مصلحة التحقيق في اظهار الحقيقة وبين مصلحة الافراد في الحفاظ على خصوصيتهم وعدم انتهاكها وهو مبدأ دستورييقضي بعدم تجاوز الإجراء المطلوب للغرض القانوني منه فعلى سبيل المثال لا الحصر لا يجوز تفتيش جميع أجهزة المستهلك لمجرد ورود شكوى عامة.

من الجوانب المهمة أيضًا ضرورة إبلاغ المستهلك بحقوقه أثناء التحقيق، خاصة إن كان ضحية، لأن كثيرًا من المستهلكين لا يدركون ما يُسمح به قانونًا أثناء جمع بياناتهم الشخصية. وقد أوردت دراسة أجرتها الهيئة المستقلة لحقوق الإنسان أن "أكثر من 60% من المستهلكين الذين خضعوا لتحقيق في قضايا نصب إلكتروني لم يبلغوا بحقهم في الاعتراض أو الاستئناف على الإجراءات (تقرير اجرائي) (الهيئة المستقلة لحقوق الإنسان، د.ت).

ويرى الباحث ان خصوصية التحقيق في الجرائم الواقعة على المستهلك في السوق الالكتروني لا تقتصر فقط على اظهار الدليل واظهار الحقائق بل هي تمتد الى اعمق واعقد من ذلك بكثير فهي مرحلة حساسة للغاية ويعتمد على صحتها حجية الدليل من بطلانه اذ انها متصلة اتصال وثيق في ان أي خطا بسيط يمكن ان يؤدي الى انتهاء خصوصية الافراد او سلامة بياناتهم الشخصية او امتدادها الى اطراف لا شان لهم في الدعوى فهذه المرحلة متعلقة بقيم قانونية وثوابت دستورية لا يمكن التهاون فيها اذ ان في هذه المرحلة يجب ان يكون هناك توازن ما بين تحقيق العدالة من جانب ومن جانب اخر الحفاظ على

خصوصية الافراد وعدم انتهاكها الامر الذي يتطلب بالضرورة اعداد كوادر قانونية من مأموري الضبط القضائي وأعضاء النيابة العامة بطريقه ذات كفاءة عالية وتدريبهم باستمرار لضمان نجاحه هذه المرحلة وأيضا توفير المعدات والأجهزة اللازمة لضمان تحقيق افضل النتائج.

وعلى الصعيد الدولي قد تم توضيح ان هناك قصور كبيرة في التعاون الدولي في هذا الخصوص الامر الذي من الممكن ان يؤدي في بعض الاحيان الى ضياع الحقوق و/أو الادلة والى تعديل او حذف الادلة التي تدين الجاني اذ ان على الدولة اولا تجهيز تشريع قانوني واضح الملامح والنصوص الاجرائية المتعلقة في سلامة التحقيق وخصوصيته وايضا اعداد الكوادر القانونية ذات كفاءة عالية ممثلة بمأموري الضبط القضائي وأعضاء النيابة العامة وأيضا اعداد الاتفاقيات التعاون الدولية المتعلقة في هذا الخصوص.

الفرع الثاني

انعكاس إجراءات التحقيق على حماية المستهلك في التعاقد الإلكتروني

ان ابرز ما يميز إجراءات التحقيق في الجرائم الواقعة على المستهلك الإلكتروني هو ضرورة المحافظة على الخصوصية العاليةالتي تتمتع بها بسبب طبيعة الأدلة الالكترونية الحساسة ومدى اهميتها ما يستوجب وجود ضمانات قانونية واضحة وفعاله تحمي حقوق المستهلك من التعرض الى أي اختراق لخصوصية او أي مساس في امن معلوماته وبياناته الخاصة فالإجراءات التي تتعلق بجمع البيانات الالكترونية والتحقق من الأدلة تتطلب احترام القوانين التي تنظم خصوصية المعلومات وحماية البيانات الشخصية لان الكشف عن هذه البيانات او المساس بها بدون ضوابط صارمة وفعالة سوف يؤدي إلى انتهاك الحقوق الأساسية للمستهلك المحمية بموجب الدستور وتشير التشريعات الفلسطينية إلى ضرورة تقييد عمليات التحقيق بأوامر قضائية مسبقة تضمن عدم تجاوز السلطات لصلاحياتها وتكون هذه الاوامر القضائية مسببة ومحددة ومذكور بها كل التفاصيل المتعلقة في التحقيق وحدود الصلاحيات المتمتعين بها

مما يوفر حماية قانونية للمستهلك ضد التعديات غير المشروعة وضمان عدم انتهاك خصوصياته وعدم المساس بها (المادة 22 من قانون الإجراءات الجزائية الفلسطيني رقم 3 لسنة 2001).

و يُعتبر ضمان حماية الخصوصية الشخصية من أبرز الضمانات التي يجب مراعاتها خلال مرحلة التحقيقات اذ ان القانون الاساسي قد نص على ضرورة احترام الحريات والحقوق الأساسية للمواطنين (المادة العاشرة من القانون الاساسي المعدل)، مما يلزم الجهات المختصة بتطبيق قواعد دقيقة أثناء القيام بمرحلة التحقيق لا سيما عند معالجة بيانات إلكترونية حساسة أو معلومات شخصية او بيانات خاصة وقد أكد الفقه القانوني على أن تجاوز هذه الحدود يُعد إخلالاً قانونيًا يُعرض الأدلة التي تم الحصول عليها للبطلان، وهو ما يؤثر سلبًا على سير العدالة وبالتالي يكون سبب في تعرض الدليل للسقوط في وزنه القانوني وضياع الحقوق حتى وان كان الدليل صحيح (شمالة،، 2010، الصفحات 120-125).

ان التحقيق في الجرائم الالكترونية يتمتع في خصوصية خاصة اذ انه يتطلب استخدام أدوات تقنية الكترونية متطورة ومتخصصة لجمع وتحليل البيانات الالكترونية بطريقة تحفظ حقوق جميع الاطراف في التحقيق فالأدلة الالكترونية مثل سجلات الدخول للمواقع والروابط الإلكترونية ورسائل البريد الإلكتروني والمعاملات المالية الإلكترونية والحركات والحوالات المالية تحتاج إلى معالجة خاصه لضمان عدم التلاعب بها ولضمان عدم التعدي على حقوق المستهلك في ضمان عدم التعرض الى بياناته الشخصية وأوضحت دراسة بحثية منشورة في مجلة جامعة النجاح أن تطبيق الضمانات القانونية أثناء التحقيقات الرقمية يساهم في زيادة ثقة المستهلكين بالسوق الإلكتروني ويعزز من فعالية الملاحقة الجنائية(حمودة، 2020، صفحة 115).

ومن ناحية اخرى تعتبر قواعد اصدار أوامر التفتيش المتعلقة في الجرائم الالكترونية والضبط القضائي من أهم الضمانات القانونية التي تحفظ حقوق المستهلك أثناء مرحلة التحقيق فقد نص قانون الإجراءات الجزائية الفلسطيني على ضرورة الحصول على إذن قضائي قبل أي اجراء متعلق في التفتيش أو مراقبة

إلكترونية مثل المواقع والحركات المالية وغيرها مع تحديد واضح لنطاق ومدة التفتيش واسبابه وصلاحياته وحدوده ويُظهر ذلك جليا وواضحا في حرص المحاكم على رفض الأدلة التي تُجمع دون احترام هذه الشروط او التي يتم الحصول عليها وبها أي عيب من عيوب السقوط و البطلان كما يكون ذلك ركز قوه للمحامين لسقوط حجية الدليل امام القضاء مما يعكس أهمية الضمانات القانونية في الحفاظ على حقوق المستهلكين ومصداقية النظام القضائي(محكمة استئناف رام الله، 2018).

ان الامتثال للمعايير الدولية في مجال حماية البيانات خلال مرحلة التحقيق في الجرائم الإلكترونية يعزز من حماية المستهلك ويجعل النظام القانوني متوافقًا مع الاتفاقيات الدولية ذات العلاقة في هذا الامر ويعزز ثقة المستهلك في الدولة وفي تشريعاتها وفي اجهزتها ومؤسساتها المختلفة فقد أكدت وثيقة مبادئ حماية البيانات الصادرة عن الاتحاد الأوروبي على ضرورة وجود توازن بين تحقيق الأمن ومراعاة خصوصية الأفراد لتحقيق العدالة من جهة والحفاظ على خصوصية المستهلك وبياناته من جهة اخرى وهذا ما يستدعي تبني فلسطين لممارسات مشابهة تضمن للمتهم والمستهلك حقه في عدم التعدي على خصوصيته او سلامة بياناته المالية او الشخصية خلال مرحله التحقيق (الاتحاد الأوروبي، 2018).

واضافة الى كل ما سبق كان لا بد من توفر اليات رقابية فعاله شاملة وواضحة وذلك للرقابة على اجراءات التحقيق بكافه مراحلها والتأكد من عدم استعمال الحق لمن لا سلطة له او عدم التعسف في استعمال الحقوق او الصلاحيات الممنوحة موجب القانون ولكي لا يكون ذلك سبب من اسباب بطلان الدليل حتى وان كان دليل قطعي لان هذا الحق من الحقوق الاساسية للمستهلك وللمشتبه به ايضا فقد نص القانون الفلسطيني على وجود جهات رقابية مستقلة لمتابعة عمليات التحقيق وضمان احترام حقوق الأفراد، وهو ما يحد من التجاوزات المحتملة ويحفظ نزاهة التحقيق (الهيئة المستقلة لحقوق الإنسان، 2023، صفحة 23).

اضافه الى ان الحفاظ وعدم التعدي على هذه الضمانات اثناء التحقيق يساهم بشكل فعلي في تقليل المخاطر المتعلقة في تجاوز او التعسف او الاختراق في الخصوصيات او الصلاحيات ويظهر ذلك بشكل واضح في القضايا الإلكترونية التي يصعب فيها أحياناً تأكيد صحة الأدلة الالكترونية ويشير الفقه القانوني إلى أن التحقيق في الجرائم الإلكترونية يجب أن يُجرى وفق قواعد واضحة تضمن صحة الأدلة ومراعاة حقوق الدفاع وحقوق جميع الاطراف وهو ما يؤكد ضرورة التوازن بين تحقيق الأمن من جهة وحماية حقوق الفرد من جهة اخرى (درويش، 2022، صفحة 65).

ان مبدأ التناسب في استخدام سلطات التحقيق او السلطات الممنوحة من قبل القانون مبدأ مهم وحساس للغاية حيث يجب أن تكون التدخلات والتحقيق و الكشف عن أي شيء في خصوصية المستهلك محدودة بقدر الضرورة فقط وبقدر ما نحتاجه من معلومات وبإذن خطي واضح من السلطات المختصة فالتحقيق لا يجوز أن يتجاوز ما يلزم لكشف الحقيقة وضبط الجريمة خاصة عندما نتحدث عن الوصول إلى البيانات الشخصية للمستهلك أو تتبع سلوكياته على الإنترنت او الحسابات المالية الخاصة به وتؤكد المواثيق الدولية اهمية ذلك مثل ميثاق الأمم المتحدة لحقوق الإنسان اذ وضح أهمية احترام التناسب والضرورة في أي إجراء يؤثر على حرية وخصوصية الأفراد وهو ما يجب أن ينعكس على التشريعات الفلسطينية ذات الصلة بكل مرحلة من مراحل كشف الحقيقة من لحظة وقوع الجريمة وحتى الحكم البات.

ومن ناحية اخرى التأكد من صحة الدليل الالكتروني وتوثيقه جزء لا يتجزأ من الضمانات المتعلقة في التحقيق اذ ان غياب التأكد من صحة الدليل قد يؤدي إلى قبول أدلة مغلوطة أو معدلة او غير صحيحة مما يؤثر على صحة هذا الدليل وصحة قبوله في التحقيق وقد أوضح خبراء القانون الإلكتروني أن التوثيق الدقيق لجميع الخطوات من التحفظ على الأجهزة الرقمية إلى استخراج البيانات وتحليلها، ضروري لضمان سلامة الأدلة أمام القضاء.

وبالحديث عن الضمانات القانونية كان لا بد من الحديث عن حق الدفاع للمستهلك المتهم أو المرتبط بالقضية أثناء مرحلة التحقيق في الجرائم الالكترونية اذ انه يحق للمستهلك الحصول على محامٍ يطلع على إجراءات التحقيق ويُشارك في كافة مراحل جمع الأدلة مما يضمن عدم تعرضه لأي تجاوزات أو انتهاكات قد تضر بموقفه القانوني حالا او مستقبلا ويفرض قانون الإجراءات الجزائية الفلسطيني على جهات التحقيق إعلام المتهم بحقوقه قبل البدء في التحقيق وهو ما يُعزز مبدأ العدالة ويمنع التعسف في الصلاحيات او السلطات .

المبحث الثاني

خصوصية الإثبات الجنائي في حماية المستهلك الإلكتروني

يروم الإثبات الجنائي الوصول إلى الحقيقة، وهذه العملية الأخيرة لن تتأتى إلا من خلال العملية الإصلاحية المتمثلة في البحث عن الدليل الجنائي وتقديمه إلى القضاء (الجيلاوي، 2018، صفحة 11)، لذلك فإنه يُعدّ في الجرائم الواقعة على المستهلك الإلكتروني إثباتًا ذا طبيعة رقمية خاصة، يتسم بحساسية عالية لخصوصية البيانات، وبصعوبات تقنية وقانونية في جمع الأدلة ونسبتها إلى الفاعل في بيئة عابرة للحدود. وتفرض هذه الخصوصية ضرورة تكييف قواعد الإثبات الجنائي بما يضمن مشروعية الدليل الرقمي وسلامته الفنية وحجيته القانونية، مع مراعاة متطلبات الإذن القضائي وسلسلة الحيازة ومعايير الاقتناع القضائي. كما تبرز تحديات عملية تتعلق بعبء الإثبات والتعاون مع مزوّدي الخدمة خارج الولاية القضائية. ويستدعي ذلك اعتماد آليات إجرائية متخصصة توازن بين فعالية حماية المستهلك الإلكتروني وصون حقوقه وخصوصيته أثناء سير الدعوى الجنائية.

وانطلاقًا من ذلك سنقوم بتقسيم ذلك المبحث على نحو مطالبين متتالين وذلك بالشكل التالي :

- المطلب الأول: مركز المستهلك الإلكتروني في الإثبات الجنائي
- المطلب الثاني : خصوصية الاثبات في الجرائم الواقعة على المستهلك الالكتروني

المطلب الأول

مركز المستهلك الإلكتروني في الإثبات الجنائي

يُعرَّف الإثبات بأنه: الدليل أو البرهان أو البينة أو الحجة، وهو مأخوذ من الفعل "ثَبَت" أي "جلس متمكنًا" (الجيلاوي، مرجع سابق، ص١٥)، ويقصد به في المجال القانوني إقامة الدليل أمام الجهات المختصة على وقوع الجريمة ونسبتها إلى مرتكبها. ويُعدّ الإثبات في المسائل الجنائية من أهم مراحل الإجراءات الجزائية، لما له من أثر مباشر على تقرير المسؤولية الجنائية أو نفيها.

يُثير الإثبات الجنائي في الجرائم الواقعة على المستهلك الإلكتروني إشكاليات خاصة، بالنظر إلى الطابع الرقمي للأدلة، وتعقيد وسائل ارتكاب الجريمة، وعدم تكافؤ القدرات التقنية والمعرفية بين المستهلك والجاني. فالمستهلك الإلكتروني غالبًا ما يفتقر إلى الوسائل الفنية التي تمكّنه من حفظ الدليل الرقمي أو توثيقه أو إثبات نسبته إلى الفاعل، الأمر الذي ينعكس مباشرة على مركزه في مرحلة الإثبات أمام جهات التحقيق والمحاكمة.

وانطلاقًا من ذلك، يُقسَّم هذا المطلب إلى فرعين متتالين:

- يُخصَّص الفرع الأول لبحث مركز المستهلك الإلكتروني في الإثبات الجنائي بوصفه طرفًا متأثرًا بخصوصية الدليل الرقمي.
- بينما الفرع الثاني سَيُخصص لبحث مدى ملائمة الاجراءات التقليدية لطبيعة الجريمة الالكترونية.

الفرع الأول

الطبيعة الخاصة للمستهلك الإلكتروني كطرفٍ ضعيفٍ في المحاكمة

إن انفراد الطرف القوي الموجب بوضع شروط العقد، فإن قبول الطرف الآخر يكون تسليماً منه للشروط التي انفرد بوضعها (خلف، 2024، صفحة 128)،لذلك ينعقد وصف "الطرف الضعيف" للمستهلك الإلكتروني في نطاق المحاكمة الجنائية لا لقصورٍ شخصيٍّ فيه، وإنما نتيجة لاختلالٍ موضوعيّ في موازين الخصومة، يتمثّل في عدم تكافؤ القدرات التقنية والمعرفية بينه وبين الجاني الرقمي أو المهني المزوّد، فضلًا عن تعرّضه لمخاطر مضاعفة تتصل بإمكانية كشف بياناته الشخصية والمالية أثناء إجراءات الإثبات، وارتفاع كلفة الدليل الفني وتعقيده. ويترتّب على هذه الخصوصية أن تُدار إجراءات المحاكمة إدارةً مرِنة تراعي هذا الاختلال، بما يحقق التوازن بين حقوق الدفاع من جهة، وحقوق الضحية في الخصوصية والإنصاف وعدم إعادة الإيذاء الإجرائي من جهة أخرى.

تنطلق المعالجة من التشريع الفلسطيني الذي يضمن كرامة الإنسان وحرمة حياته الخاصة وحقه في محاكمة عادلة، ويمنح المحكمة سلطة إدارة الجلسة ومنع الأسئلة المجحفة والاستعانة بالخبراء، ويُقر حقوق المستهلك الموضوعية (السلامة، المعلومة، الاختيار، التعويض) التي تُحدّد المصلحة المحمية محلّ الإثبات.ويترجم ذلك في ستة محاور عملية:

سدّ فجوة المعرفة التقنية: تتّسم الأدلة الرقمية—كسجلات الدخول، وعناوين الـIP، وبيانات الميتاداتا، وبصمات الأجهزة—بطابع فني معقّد لا يتوافر للمستهلك الإلكتروني إدراكه أو مناقشته بذات الكفاءة التي يمتلكها الجاني أو الجهات الفنية. ويُعدّ هذا القصور المعرفي أحد مظاهر ضعف المستهلك كطرف في المحاكمة، الأمر الذي يبرّر تدخل المحكمة لتعيين خبير فني محايد يشرح طبيعة الدليل ومنهجيته واحتمالات الخطأ، مع تمكين الضحية من توجيه الأسئلة الفنية عبر المحكمة، ضمانًا لتكافؤ السلاح الإجرائي (المادة (99) من قانون الإجراءات الجزائية رقم (3) لسنة 2001).

تكييف العلنية مع الخصوصية: على الرغم من أن علانية الجلسات تمثّل مبدأً إجرائيًا عامًا، إلا أن تطبيقه الحرفي في قضايا الانتهاك الرقمي قد يُفضي إلى انتهاك جديد لخصوصية المستهلك الإلكتروني، من خلال كشف بياناته المالية أو مراسلاته الخاصة أثناء الإثبات. ويُعدّ هذا الخطر لصيقًا بطبيعة المستهلك الإلكتروني، باعتباره طرفًا هشّ الخصوصية في البيئة الرقمية، مما يبرّر تمكين المحكمة من تقرير سرّية جزئية للجلسات أو تنقيح المحاضر والمستندات، بحيث تُحجب البيانات غير اللازمة للإثبات دون الإخلال بحقوق الدفاع أو بمبدأ المواجهة (المادة (11) من القانون الأساسي الفلسطيني المعدّل لسنة 2003).

تمكين الحضور والمشاركة – ضعف إجرائي ناتج عن الطبيعة الرقمية، ونظرًا لما يتّسم به المستهلك الإلكتروني من ضعفٍ إجرائي ناجم عن البعد الجغرافي والطابع التقني للجريمة، فإن تمكينه من الحضور والمشاركة يُعدّ امتدادًا لحمايته كطرف ضعيف في الخصومة. ولهذا تُيسّر المحكمة الحضور عن بُعد عند اللزوم، وتقبل المذكرات الرقمية وفق ضوابط سلامة الدليل، وتُتيح له الادعاء بالحق المدني وطلب تدابير

تحفظية تهدف إلى وقف الضرر المستمر، كتعطيل الحسابات الوهمية أو إلزام المنصات بحفظ البيانات أو تسليمها (المادة العاشرة من قانون الإجراءات الجزائية، والمواد (58/56) منه).

منع إعادة الإيذاء الإجرائي – مرتبط مباشرة بخصوصية المستهلك ويُعدّ منع إعادة الإيذاء الإجرائي أحد أهم مظاهر حماية المستهلك الإلكتروني كطرف ضعيف؛ إذ إن التوسّع غير المنضبط في تفتيش أجهزته أو مناقشة مراسلاته قد يُحوّل المحاكمة ذاتها إلى انتهاك جديد لخصوصيته الرقمية. لذلك تضبط المحكمة نطاق الأسئلة وحدود الاطلاع على الملفات الرقمية وفق مبدأي الضرورة والتناسب، بحيث لا يُستباح من بيانات المستهلك إلا ما له صلة مباشرة بموضوع الإثبات (المادة (11) من القانون الأساسي الفلسطيني (حرمة الخصوصية). والمادة (51) من قانون الإجراءات الجزائية).

عبء المناقشة الفنية للدليل – ضعف معرفي تقني للمستهلكوبسبب الفجوة التقنية بين المستهلك الإلكتروني وبقية أطراف الخصومة، فإن عبء مناقشة الدليل الرقمي لا يمكن أن يُترك للمستهلك وحده. ومع بقاء عبء الإثبات على عاتق النيابة العامة، تُكثّف المحكمة دورها الاستجوابي في المسائل الفنية، وتُعيد فتح باب المرافعة متى ثارت شكوك حول مشروعية الدليل أو سلامة سلسلة حيازته، ضماناً لمحاكمة عادلة لا يُقصى فيها الطرف الأضعف تقنيًا (المادة 99 والمادة 273 من قانون الإجراءات الجزائية الفلسطيني).

معالجة عقبات العبور الحدودي – طبيعة الجريمة لا قدرة المستهلكويزداد ضعف المستهلك الإلكتروني وضوحًا في الجرائم العابرة للحدود، حيث تكون الأدلة بحوزة مزوّدي خدمة أجانب خارج الولاية القضائية الوطنية. وفي هذا السياق، تُثبت المحكمة في محاضرها مساعي التعاون الدولي ومخاطبة الجهات الأجنبية، وتُمهل آجالًا واقعية، وتستجيب لطلبات الحفظ الفوري للبيانات، منعًا لضياع الأدلة الرقمية المتطايرة وتحميل المستهلك عبئًا لا طاقة له به (المواد 134/131 من قانون الإجراءات الجزائية الفلسطيني).

ويتبيّن مما تقدّم أن هذه الأدوات الإجرائية لا تُطرح بوصفها ضمانات عامة، وإنما باعتبارها استجابة مباشرة للطبيعة الخاصة للمستهلك الإلكتروني كطرف ضعيف في الإثبات الجنائي، وهو ضعف ذو مصدر تقني وإجرائي، يستوجب تكييف تطبيق القواعد العامة دون المساس بضمانات المحاكمة العادلة.

ومن هنا، فلا يُقصد بوصف المستهلك الإلكتروني "طرفًا ضعيفًا" توصيفًا اجتماعيًا أو افتراضيًا، وإنما توصيفًا قانونيًا إجرائيًا يترتب عليه آثار محددة في إدارة الخصومة الجنائية. فالمستهلك في هذا السياق هو مجنيّ عليه يتمتع بحقوق إجرائية خاصة بحكم طبيعة المصلحة المحمية (البيانات، الخصوصية، الثقة التعاقدية)، وبحكم اختلال التوازن التقني مع الجاني، الأمر الذي يوجب تكييف قواعد الإثبات بما يضمن فعالية الحماية الجنائية دون المساس بضمانات المحاكمة العادلة (المادة 9 من القانون الأساسي المعدل، والمواد ٣ــ٥ من قانون حماية المستهلك رقم 21 لسنة2005).

فجوة المعرفة التقنية

تتجلى الطبيعة القانونية الخاصة للمستهلك الإلكتروني في عجزه عن مناقشة الدليل الرقمي مناقشة واعية بسبب تعقيده الفني، وهو ما يُنشئ ضعفًا إجرائيًا حقيقيًا في مرحلة الإثبات، يستدعي تدخل المحكمة لسدّ هذه الفجوة عبر الخبرة الفنية المحايدة (المادتين 99و214 من قانون الإجراءات الجزائية الفلسطيني).

تكييف العلنية مع الخصوصية

إن خصوصية المستهلك الإلكتروني لا تنبع من شخصه، بل من طبيعة محل الاعتداء ذاته، المتمثل في البيانات والمراسلات والمعاملات الرقمية، الأمر الذي يجعل تطبيق علانية الجلسات دون تقييد مصدر خطر على المصلحة المحمية، ويبرر قانونًا اعتماد السرّية الجزئية أو تنقيح المستندات (المادة 11 من القانون الأساسي المعدل، والمادة 165 من قانون الإجراءات الجزائية الفلسطيني).

الكلفة والطابع العابر للحدود

يُعد تشتّت مصادر الدليل الرقمي خارج الإقليم الفلسطيني عنصرًا من عناصر الضعف الإجرائي للمستهلك، إذ يتحمل عبئًا غير متكافئ في تتبع الأدلة ومخاطبة مزودي الخدمة الأجانب، ما يقتضي دورًا إيجابيًا للمحكمة في إدارة الإثبات (المادة 15 من قانون الإجراءات الجزائية) .

إعادة الإيذاء الإجرائي

يُعد الاستجواب غير المنضبط أو التوسع في تفتيش الحياة الرقمية للمستهلك صورة من صور الإيذاء الإجرائي، وهو ما يتعارض مع وظيفته القانونية كمجنيّ عليه، ويخالف مبدأ الضرورة والتناسب في الإثبات (المادة 13 من القانون الأساسي المعدل).

عدم تماثل القوى

يتعزز ضعف المستهلك الإلكتروني قانونًا عندما يواجه مهنيين أو شركات ذات قدرات تقنية وقانونية عالية، وهو ما ينعكس على مركزه في الإثبات، ويبرر تدخل المحكمة لضبط توازن الخصومة (المادتين 2 و6 من قانون حماية المستهلك الفلسطيني).

الأدوات الإجرائية

تكييف العلنية – الخبرة – الحضور عن بُعد – تنقيح الأحكام تشكّل هذه الأدوات تطبيقًا عمليًا للطبيعة القانونية الخاصة للمستهلك، وليست امتيازات استثنائية (قانون الإجراءات الجزائية، المواد (165، 99، 214). والقانون الأساسي الفلسطيني، المواد (11، 30).

اللمحة المقارنة

تؤكد التشريعات المقارنة أن توصيف الضحية الرقمية بوصفها طرفًا ذا مركز إجرائي خاص أصبح اتجاهًا تشريعيًا مستقرًا (قانون رقم (08–09) ، 2009).

وعليه، فإن الحديث عن الطبيعة الخاصة للمستهلك الإلكتروني لا يخرج عن الإطار القانوني، بل يُعدّ مدخلًا لازمًا لفهم كيفية تكييف قواعد الإثبات الجنائي بما يحقق الحماية الفعالة للمصلحة محل الاعتداء دون الإخلال بضمانات المحاكمة العادلة.

تطبيقات عملية أمام المحكمة الجزائية الفلسطينية

الاستماع المسبق للخبير قبل مناقشة الدليل الرقمي

قبل الشروع في مناقشة سجلات الدخول، وبيانات الميتاداتا، والبصمات الرقمية، يتعيّن على المحكمة الاستماع إلى الخبير الفني لبيان مصدر الدليل، وآلية استخراجه، والأدوات المعتمدة في النسخ الجنائي، ومدى سلامة سلسلة الحيازة، مع تبسيط المصطلحات الفنية بلغة مفهومة للمستهلك المجني عليه، تمكينًا له من ممارسة حقه في المناقشة الواعية وعدم اختزال دوره في مجرد متلقٍّ للإجراءات(المادة 99و 214 من قانون الإجراءات الجزائية رقم ٣ لسنة 2001).

حجب البيانات الحساسة أثناء تداول الدليل

عند احتواء ملف الدعوى على صور بطاقات مصرفية، أو محادثات خاصة، أو بيانات تعريفية للمستهلك، يجوز للمحكمة الأمر بحجبٍ جزئي للنسخ المتداولة بين الخصوم، مع حفظ الأصل غير المنقّح في حرزٍ قضائي، تحقيقًا للتوازن بين مقتضيات الإثبات وحماية الخصوصية الرقمية للمجني عليه (المادة 11 من القانون الأساسي المعدل، والمادة 165 من قانون الإجراءات الجزائية الفلسطيني).

إدارة القضايا العابرة للحدود دون تحميل المستهلك عبئها

في القضايا التي تتطلب مخاطبة مزوّدي خدمة خارج فلسطين، تُثبت المحكمة في محاضرها صعوبات التعاون القضائي وخطوات الإنابة، وتمنح المستهلك أجلًا واقعيًا لتلقّي ردود الجهات الأجنبية، منعًا لتحميله تبعات بطء التعاون الدولي أو قصوره، باعتباره عنصرًا خارجًا عن إرادته (قانون الإجراءات الجزائية المادة 17 والمادة 59 وما بعدها منه).

ضبط إدارة الجلسة ومنع التنقيب غير المشروع في الحياة الرقمية

تلتزم المحكمة بضبط نطاق الأسئلة الموجّهة للمستهلك وحدود الاطلاع على ملفاته الرقمية، بما يمنع طرح أسئلة لا صلة لها بموضوع الإثبات أو تتجاوز مبدأ الضرورة والتناسب، تفاديًا لتحويل المحاكمة إلى اعتداء جديد على حياته الرقمية (القانون الأساسي الفلسطيني، المادة (13)،وقانون الإجراءات الجزائية، المواد (51، 52)).

ويرى الباحث أن توصيف المستهلك الإلكتروني بوصفه "طرفًا ضعيفًا" لا يُنشئ امتيازًا إجرائيًا استثنائيًا، وإنما يُحتّم تدخّلًا تشريعيًا منظّمًا داخل قانون الإجراءات الجزائية، من خلال:

- استحداث فصل خاص بالعلنية والخصوصية الرقمية في القضايا الإلكترونية.
- اعتماد نماذج رسمية لتنقيح المحاضر والأحكام التي تتضمن بيانات المستهلك.
- إلزامية الخبرة الفنية المحايدة متى كان الدليل الرقمي جوهريًا.
- وضع قواعد عملية لسلسلة حيازة الأدلة الرقمية.

قضائيًا، يُوصى بإعداد دليل عمل قضائي لقضايا المستهلك الإلكتروني يتضمن قوالب أوامر حجب البيانات، وآليات الاستماع عن بُعد، وأسئلة معيارية للخبراء.

مؤسسيًا، يُقترح إنشاء وحدة معونة قانونية–فنية لضحايا الجرائم الرقمية ضمن وزارة العدل أو النيابة العامة، بما يُعيد التوازن الإجرائي داخل قاعة المحكمة دون المساس بحقوق الدفاع أو بعبء الإثبات.

الفرع الثاني

مدى ملاءمة الإجراءات التقليدية لطبيعة الجريمة الإلكترونية

يثير تطبيق الإجراءات الجزائية التقليدية على الجرائم الواقعة على المستهلك الإلكتروني أسئلة جوهرية حول الكفاية والملاءمة؛ ذلك أن الدليل في البيئة الرقمية سريع الزوال، وعابر للحدود، ومعقّد فنيًا، بينما

صيغت أغلب القواعد الإجرائية لتتعامل مع أشياء مادية وشهود مباشرين ومسرح جريمة محدّد. وتالياً، يلزم تفحّص أين تكفي القواعد القائمة بذاتها، وأين تحتاج إلى تكييف أو استكمال تشريعي وإجرائي.

أولًا: الولاية والاختصاص في فضاء عابر للحدود

تقوم القواعد التقليدية على مبدأ الإقليمية وتحديد مكان وقوع الجريمة أو محلّ إقامة المتهم أو مكان الضرر. غير أن معاملات المستهلك الإلكتروني تتم عبر منصّاتٍ تخزّن بياناتها خارج فلسطين، وقد تتوزّع عناصر الفعل بين جهاز الضحية وخوادم أجنبية ووسيط دفع دولي. هنا يُصبح إثبات الاختصاص الزمني والمكاني متعذرًا أحيانًا بالمعايير التقليدية وحدها، فتبرز الحاجة إلى مسارات إنابة قضائية سريعة وتفعيل أدوات التعاون الدولي وحفظ البيانات الفوري كي لا تفلت الأدلة. يظلّ المبدأ العام للاختصاص صالحًا، لكن وسائله الإجرائية تحتاج إلى مسارات معاصرة لحفظ الأدلة العابرة للحدود واستجلابها (قانون الإجراءات الجزائية الفلسطيني رقم (3) لسنة 2001، المواد (9–13) .

ثانيًا: أوامر التفتيش والضبط بين الخصوصية وسرعة التلف

يفترض التفتيش التقليدي مكانًا ماديًا محدّدًا ومتسترا للأشياء المضبوطة. أما في الجريمة الإلكترونية، فالمقصود "بيانات" في حساباتٍ سحابية أو أجهزة متصلة، وبعضها متطاير (قصيرة العمر). ومع أن قانون الإجراءات الجزائية يتيح أوامر تفتيش وضبط عامة، فإن فعالية هذه الأوامر تتطلب تحديدًا دقيقًا للنطاق والزمان والغاية في الوسيط الرقمي، مع مراعاة مبدأ الضرورة والتناسب حمايةً لخصوصية الضحية. ولأن فوات ساعاتٍ معدودات قد يعني ضياع السجلات، تُصبح الأوامر "العاجلة" لحفظ البيانات ثم طلبات الإنتاج التسليم اللاحقة أكثر ملاءمة من انتظار المسار التقليدي البطيء (القانون الأساسي الفلسطيني المعدل، 2003)

ثالثًا: سلامة الدليل الرقمي وسلسلة الحيازة

القواعد التقليدية تفترض أشياءً تُحفظ في حرز ماديّ. أما النسخ الرقمية فتتطلّب تصويرًا جنائيًا مع توثيق القيم التجزيئية قبل النسخ وبعده، وتسجيل هوية وأداة الخبير،ومسار انتقال الوسيط الأصلي والمنسوخ. من دون هذه الطبقات، يتعذّر على المحكمة التي تعتمد الاقتناع القضائي أن تستبعد فرضيّات العبث أو التعديل. وهنا تُسدّ الفجوة بالاستئناس بالمعايير الفنية الدولية (ISO IEC27037 وما يتصل بها) التي تحوّل الإجراءات إلى مسارٍ قابل للتكرار والتحقق.

إنّ مفهوم الحيازة التقليدي يُترجَم رقميًا إلى سجلٍّ محكم الخطوات لا يقلّ صرامةً عن الحرز المادي(قانون الإجراءات الجزائية الفلسطيني، المادة 99و المادة 214).

رابعًا: الشهادة والخبـــرة—من "المشاهدة المباشرة" إلى التفسير الفني

يقوم الإثبات التقليدي على شهادة الشهود المباشرة وإفاداتهم حول الوقائع المرئية أو المسموعة. في الجرائم الرقمية، يتحوّل "الشاهد المركزي" إلى سجلات إلكترونية تحتاج تفسيرًا: من أين جاءت؟ بأي أداة استُخرجت؟ ما هامش الخطأ؟ هل يمكن انتحال الهوية أو استخدام جهازٍ واحد من أكثر من شخص؟ لذا يصبح تعيين خبيرٍ محايد وسماعُه جزءًا جوهريًا من الملاءمة الإجرائية، وهو ما يسمح به قانون الإجراءات أصلاً، لكنّ القضايا الرقمية تجعل الخبرة لازمة لا اختيارية كلما كان الدليل إلكترونيًا جوهريًا (قانون الإجراءات الجزائية، المواد (96–103) و (99) و(214)منه).

خامسًا: العلنية وحماية البيانات توازن دقيق

مبدأ العلنية حجر زاوية في المحاكمة العادلة، لكنه قد يفضي—في قضايا المستهلك الإلكتروني—إلى نشر أرقام بطاقاتٍ أو محادثاتٍ خاصة أو بيانات هوية. الإجراء التقليدي (جلسة علنية وحكم منشور) يلزمه تنقيحٌ للمرفقات والحكم، وسرّية جزئية لبعض الجلسات عند الحاجة، مع حفظ النسخ غير المنقّحة في حرزٍ قضائي يضمن حقوق الدفاع. هذه الملاءمة لا تنقص من شفافية القضاء، بل تمنع تحويل المحاكمة

إلى مسرح لإعادة الإيذاء(القانون الأساسي المعدل، المادة 11 منه، وقانون الإجراءات الجزائية، المادتان 165و 172 منه).

سادسًا: عبء الإثبات ومعيار الاقتناع القضائي

لا تغيّر الجريمة الإلكترونية من القاعدة: عبء الإثبات على النيابة، والشك يُفسَّر لصالح المتهم. لكن طبيعة الدليل الرقمي تفرض على المحكمة دورًا استجوابيًا فنيًا أوسع: سؤال الخبير عن المنهج والأداة والقيود، وطلب الإيضاحات حول احتمالات الانتحال وتقنيات الإخفاء (Tor،VPN)، وربط القرائن المتفرّقة في لوحةٍ واحدة تقود إلى الاقتناع أو تترك شكًا معقولًا. إذن، المعيار هو نفسه، لكن أدوات الوصول إليه تختلف (قانون الإجراءات الجزائية الفلسطيني، المادتان 206 و 214 منه).

سابعًا: الإجراءات عن بُعد وتمكين الطرف الضعيف

تسمح الممارسات الحديثة بعقد جلساتٍ عبر الاتصال المرئي، وتلقّي مذكرات وملفات رقمية وفق ضوابط تقنية. وهذه الملاءمة تُخفّف كلفة التقاضي على المستهلك الضحية، وتُيسّر حضور الخبراء عبر الحدود، مع صون حق المواجهة. وهي أدوات تنظيمية في متناول المحكمة ضمن سلطتها في إدارة الجلسة، وتزداد أهميتها في القضايا الرقمية (القانون الأساسي المعدل، المادة 30 منه).

تقدير عام للملاءمة

الخلاصة أنّ المبادئ الإجرائية التقليدية (شرعية الإجراءات، علانية، مواجهة، حياد المحكمة، عبء الإثبات) ما زالت صالحة. غير أن وسائل التنفيذ تحتاج تكييفًا تشريعيًا وإجرائيًا: أوامر حفظ بيانات عاجلة، نماذج تفتيش رقمية محدّدة، بروتوكولات سلسلة الحيازة، إلزامية الخبرة عند تقديم دليلٍ إلكتروني جوهري، وتنقيح الأحكام المنشورة. وتُظهر التجربة الدولية—وخاصةً اتفاقية بودابست (2001) ومعايير ISO—أن التكييف ممكن دون المساس بالضمانات، بل يعزّزها في بيئةٍ يتفوّق فيها الجاني تقنيًا على الضحية.

ويرى الباحث أنّ الإطار العام الفلسطيني بحاجةٍ إلى ملاحق إجرائية رقمية تُلحَق بقانون الإجراءات الجزائية تتضمن: (1) أوامر نموذجية لحفظ البيانات وإنتاجها، (2) تعريفًا دقيقًا للتفتيش الإلكتروني وحدوده الزمانية والمكانية، (3) اعتمادًا مرجعيًا لسلسلة الحيازة الرقمية وفق ISO IEC 27037،(4) قاعدة تُلزم بتعيين خبيرٍ محايد متى كان الدليل إلكترونيًا حاسمًا، (5) بروتوكولًا قضائيًا للتنقيح ونشر الأحكام. هذه الإضافات لا تغيّر جوهر العدالة الجنائية، لكنها تجعل الإجراءات التقليدية ملائمة لطبيعة الجريمة الإلكترونية وتحمي المستهلك بصفته الطرف الأضعف في الخصومة.

المطلب الثاني

خصوصية الاثبات الجنائي في الجرائم الواقعة على المستهلك الالكتروني

تُعد الجرائم الواقعة على المستهلك الإلكتروني من الجرائم المستحدثة التي أفرزت إشكاليات خاصة في مجال الإثبات الجنائي، نظرًا لاعتمادها على الوسائط والتقنيات الرقمية. وقد أفرز ذلك خصوصية في طبيعة الدليل الإلكتروني وحجيته، فضلًا عن الصعوبات التي تعترض عبء الإثبات في هذا النوع من الجرائم.

وعليه، سنقوم بتقسيم هذا المطلب إلى ثلاثة فروع متتالية وذلك على النحو التالي :

الفرع الاول

خصوصية الاثبات

وتبدأ الخصوصيّة من تعريف الدليل نفسه: فالدليل الرقمي ليس ورقةً ثابتة بل «حالة» متغيّرة محفوظة داخل منظومات تشغيل وأجهزة وخدمات متداخلة. لذا لا تكفي صور الشاشة أو نسخ المحادثات ما لم تُسندها إجراءات فنيّة وقانونيّة تُثبت سلامة الطريق الذي سلكه الدليل منذ لحظة ضبطه وحتى عرضه على المحكمة، بما في ذلك توثيق لحظة الاكتشاف، وكيفية الاستخراج، ومن تعامل معه، وأين حُفِظ، وكيف أمكن التحقّق من عدم تعرّضه للعبث. وهنا يتعيّن ترجمة مفهوم الحرز التقليدي إلى سلسلة حيازة

رقمية دقيقة تُظهِر كل انتقال ومعالجة، وتربط كل خطوة ببيّنة زمنية واضحة، وتُخضع الوصول إلى الدليل لقيودٍ مُحكمة توازن بين مصلحة الإثبات وصيانة الخصوصية.

وتظهر الخصوصيّة أيضًا في شرط المشروعيّة عند جمع الدليل؛ فالتفتيش الرقمي—سواء وقع على جهازٍ مادي أو على حسابٍ في خدمةٍ عن بُعد—يمسّ مباشرةً حرمة الحياة الخاصة. وعليه، يجب أن يكون أمرُ التفتيش محدّدًا بالدقّة اللازمة في موضوعه ونطاقه وزمانه وغايته، وأن يُراعى فيه معيار الضرورة والتناسب، وأن تُبيَّن حدود ما يجوز الاطلاع عليه وما يجب حجبه، مع إمكان قصر الاطلاع على ما يتّصل بموضوع الدعوى فقط. كما أن علنيّة الجلسات—وهي أصلٌ عام—قد تفضي في هذا الباب إلى إعادة إيذاء الضحية، فيستقيم تقييدها جزئيًا عبر تدابير منها: التنقيح المسبق للمستندات، وقصر الاطلاع على ذوي الصفة، وحجب الهوّيات الحسّاسة في النسخ المتداولة علنًا، والاكتفاء بإيداع نسخةٍ غير منقّحة في حرزٍ قضائي تُتاح لحقوق الدفاع (القانون الأساسي المعدل، المادة 32 منه).

وتتّسع الفوارق حين ننتقل إلى الإسناد إلى الفاعل؛ فاشتراك أفراد الأسرة في جهازٍ واحد، أو استخدام وسائل إخفاء الهوية، أو تعرّض الحسابات للاختراق، كلّها عوامل تُضعف قدرة المحكمة على ربط الفعل بشخصٍ بعينه بقرينةٍ واحدةٍ منفردة. ومن ثمّ يلزم بناء لوحة قرائن متساندة: توافق سجلات الدخول مع حركات الدفع، تطابق الطوابع الزمنية المتولّدة عن المنصّة مع إعدادات الجهاز المضبوط، انتظام نمط الاستخدام قبل الواقعة وبعدها، ظهور سلوكٍ يُفهم منه قصد الإخفاء أو المحو، وتوافق بيانات موقع الشبكة مع المكان المفترض. هذه الطريقة التركيبية تُحافظ على قرينة البراءة من جهة، وتتيح تكوين قناعة قضائيّة متماسكة من جهة أخرى من دون الارتهان لعنصرٍ واحدٍ قابلٍ للجدل.

ومن خصوصيّات هذا الباب كذلك الهشاشة الزمنيّة: فالسجلات الرقمية في منصّات كثيرة تُمحى تلقائيًا بعد مددٍ قصيرة، وقد تُغلق الحسابات أو تُجمّد، وقد تُستبدل ملفات التشغيل وتضيع معها البيانات الوصفية. لهذا تصبح الأوامر العاجلة لحفظ البيانات أداةً جوهرية تسبق إجراءات الإنابة أو تبادل

المساعدة مع الخارج، ويغدو التأخير ساعاتٍ قليلة كافيًا لفقدان مادّةٍ حاسمة في الإثبات. كما تفرض هذه الهشاشة اعتماد إجراءات إسعاف رقمي تُقدّم الحسّاس والعرضة للزوال على غيره، وتؤطّر أولويّات الضبط والاستخراج والحفظ وفق ترتيبٍ واضح.

وتُثير طبيعة الدليل الرقمي أسئلةً خاصةً حول قاعدة الدليل الأفضل: فالأصل في العالم الورقي هو الوثيقة ذاتها، أما في العالم الرقمي فالأصل هو الملفّ بما يلازمه من بيانات وصفية تكشف تاريخ إنشائه وتعديله وخصائص مصدره. وعليه، تُفضَّل إحالة المحكمة إلى الأصل أو إلى نسخةٍ جنائية منه جرى استخراجها بوسيلةٍ تحفظ خواصَّه، على أن تُوثَّق القيم الرقمية التي تُظهر عدم تغيّره بين مرحلةٍ وأخرى. وتبقى الصور والنسخ المطبوعة مكمّلةً لا بديلة، إلا إذا قام عذرٌ موضوعي على تعذّر الوصول إلى الأصل.

وتتجلّى الخصوصيّة أخيرًا في التوازن بين الإثبات والستر: فالمستهلك المتضرّر طرفٌ ضعيف بطبيعته أمام المزوّدين والمنصّات، وقد يُحجم عن التبليغ خوفًا من التشهير أو من انتشار بياناته الحسّاسة. لذا يجب أن يصاحب جمع الأدلة نظامُ حمايةٍ إجرائي يُطمئنه: تمكينه من المشاركة عن بُعد، وحصر الأسئلة في نطاق الضرورة، وتحديد دوائر الاطلاع، والأخذ بالتنقيح الآمن، وإتاحة مسارٍ مدني موازٍ لوقف الضرر الجاري عبر إزالة المحتوى المضلّل أو إغلاق الحسابات الوهمية ريثما تُستكمَل محرّكات الدعوى الجزائيّة(القانون الأساسي المعدل، 2003، المواد 9، 10، 19، 32) و(قانون الإجراءات الجزائية رقم 3، 2001، المواد 164–166) و(التوجيه الأوروبي UE/29/2012، 2012).

وخلاصة القول: إن خصوصيّة الإثبات في قضايا المستهلك الإلكتروني لا تعني الخروج على الأصول، بل تكييف الأصول ذاتها مع مادّةٍ إثباتيّةٍ مختلفة في طبيعتها: تُجمع بسرعة وتضيع بسرعة، وتُنتجها منظوماتٌ خارج الحدود، وتلتصق بأسرارٍ شخصيّة. ومن هنا وجوب ترسيخ أدواتٍ عمليّة—في مقدّمها الأوامر العاجلة لحفظ البيانات، وسلسلة الحيازة الرقمية المحكمة، وتنقيح المستندات والأحكام—كي نحفظ

حجّية الدليل ونصون في الوقت نفسه كرامة الضحية وحقوق الدفاع، مع التزام البدء دائمًا بما قرّره المشرّع الفلسطيني ثم الاستفادة ممّا راكمته الخبرات المقارنة من معايير وإجراءات.

الفرع الثاني

حجّية الدليل الإلكتروني في الإثبات الجنائي

تقوم حجّية الدليل الإلكتروني على ثلاثة أركان مترابطة: المشروعية في التحصيل، والسلامة الفنيّة في الجمع والحفظ والمعالجة، والقدرة على الإسناد إلى شخصٍ بعينه (قانون الإجراءات الجزائية، 2001، المادة 206) و(المادة 30 من القانون الأساسي المعدل).

أوّلًا: الأساس الفلسطيني للاعتداد بالسجلات والوسائط الإلكترونية

أرسى المشرّع الفلسطيني قاعدة الاعتداد بالرسائل والسجلات الإلكترونية من خلال القرار بقانون بشأن المعاملات الإلكترونية الذي قرّر المساواة الوظيفية بين السجل الإلكتروني والمحرّر الورقي متى أمكن التحقّق من صحة وكمال البيانات وإمكانية حفظها واسترجاعها وموثوقية وسيلة الإنشاء، كما عرّف القرار بقانون بشأن الجرائم الإلكترونية البيانات والمعلومات الإلكترونية ومنح النيابة العامة صلاحية إصدار أوامر حفظٍ وتجميدٍ عاجلة للبيانات ضمانًا لعدم ضياعها؛ وتكمّل ذلك قواعد قانون الإجراءات الجزائية التي تفوّض المحكمة تقدير الدليل والاستعانة بالخبرة وتحديد ما يلزم لحفظ وعرض الوسائط، ولو دون باب تفصيلي خاص بالأدلّة الرقمية(قرار بقانون رقم 15 بشأن المعاملات الإلكترونية، 2017، المواد 6–8).

ثانيًا: المشروعيّة وحماية الخصوصيّة

لا يُعتدّ بدليل جُمع عبر إجراء يمسّ الحقوق الأساسية؛ لذا يتعيّن أمرٌ قضائي محدّد النطاق والزمان والغاية لتفتيش الأجهزة أو الحسابات أو طلب السجلات من مزوّد الخدمة، مع مراعاة شرط الضرورة والتناسب، وإلا تعرّض الدليل للبطلان أو لاهتزاز قيمته. وتتعاظم حساسيّة هذا الشرط حين تكون

الضحية مستهلكًا، إذ قد يفضي كشف الرسائل الخاصة أو بيانات الدفع إلى إعادة إيذاء غير مقبول. ومن ثمّ يلزم ضبط علنيّة الجلسات عبر تمكين المحكمة من تنقيح المرفقات والأحكام المنشورة، بحجب ما لا لزوم له من أرقامٍ وبياناتٍ شخصية، مع حفظ نسخةٍ غير منقّحة في حرز قضائي يضمن حقوق الدفاع .

ثالثًا: السلامة الفنيّة وسلسلة الحيازة

لا تكتسب لقطات الشاشة أو نسخ المحادثات المجهولة حجّةً بذاتها ما لم تُثبت سلامة الطريق الفني التي وصلت اليه. والمقصود بالسلامة أن يُنجَز النسخ الجنائي الكامل للوسيط الأصلي، وأن تُثبَت قيم التجزئة قبل النسخ وبعده بوصفها بصمةً رقمية تكشف أي تغيير، وأن يُدوَّن في المحضر اسم الأداة المستخدمة وإصدارها وهوية من باشر العمل وتوقيته ومكان إيداع الأصل ونسخه. ومن دون هذه الطبقات يستحيل طرد فرضيات العبث أو الاستبدال. وتوفّر المواصفات الدولية التي أصدرتها المنظمة الدولية للتوحيد القياسي إطارًا إجرائيًا موضوعيًا لخطوات التعريف والجمع والاكتساب والحفظ، مع مواصفات متمّمة لضمان العملية والتحليل والتحقيق الحاسوبي. ويقابل الحرز المادي في عالم الورق سلسلة حيازة رقمية دقيقة تُظهر كل انتقالٍ ومعالجة للدليل منذ لحظة ضبطه (قانون الإجراءات الجزائية رقم 3 لسنة 2001، المادة 27 منه).

رابعًا: الإسناد إلى الفاعل

تتعقّد نسبة الفعل إلى فاعله في الفضاء الرقمي بسبب مشاركة الأجهزة داخل الأسرة، ووسائل إخفاء الهوية عبر الشبكة كالشبكات الخاصة الافتراضية، واحتمالات الاختراق أو السيطرة على الحسابات. لذا يميل القضاء إلى بناء لوحة قرائن متساندة تجمع بين سجلات الدخول والاستخدام، وتطابق الطوابع الزمنية مع نشاطاتٍ موازية، وبصمة الجهاز أو المتصفح، ومسارات الدفع الإلكتروني، ورسائل التأكيد والاسترجاع، وبيانات الموقع الشبكي بحسب المناطق الزمنية وبروتوكولات ضبط الوقت، وسلوك ما بعد الواقعة كالمحو والتعطيل والإخفاء. ومع بقاء عبء الإثبات على النيابة العامة، قد تكفي مجموعة القرائن

المتماسكة لبناء قناعةٍ قضائية، فيما يُفسَّر الشك المعقول لصالح المتهم متى وُجد احتمالٌ واقعي للانتحال أو العبث (قانون الإجراءات الجزائية رقم 3 لسنة 2001، المادة 206 منه).

خامسًا: التواقيع والتصديقات الإلكترونية

أقرّ القرار بقانون بشأن المعاملات الإلكترونية الاعتراف بالتوقيع الإلكتروني متى أمكن تعيين هوية الموقّع، وإثبات سيطرته على وسيلة التوقيع، وكشف أي تعديلٍ لاحق على البيانات. وتقوى الحجّية حين يستند التوقيع إلى خدمة تصديق مرخّصة تستوفي معايير الاعتماد والرقابة. وفي التجربة الأوروبية، رتّبت اللائحة الخاصة بالتعرّف الإلكتروني وخدمات الثقة درجاتٍ للتوقيع بحسب قوّة التحقّق، وهو ما يصلح للاستئناس الفني أمام القضاء الوطني دون إخلالٍ بأولويّة القانون الفلسطيني.

سادسًا: أدلة المنصّات ومزوّدي الخدمة

غالبًا ما يحمل ملف الدعوى مادتين تقنيّتين: ما قدّمه المستهلك من لقطاتٍ ومراسلات وكشوفٍ مصرفية، وما تستخرجه المنصّة من سجلات الإنشاء والتعديل والوصول والعناوين الشبكيّة. وتختلف القيمة الإثباتيّة لكل منهما: فالأولى استدلالية إن انفردت، بينما تتعزّز حجّية الثانية إذا قُدّمت عبر مساراتٍ رسمية بموجب أوامر حفظٍ وإنتاجٍ بموثقة بتوثيقٍ من المزوّد. وتتحقّق المحكمة من اتساقٍ زمني وتقني بين الملفّين: توافق وقت الرسالة مع المنطقة الزمنية للخادم، وتشابه بصمة الملف المرسل مع ما لدى المزوّد، وتلازم سجلّات الدخول مع حركة الدفع (قرار بقانون رقم 10 بشأن الجرائم الإلكترونية، 2018، المادة 39).

ويرى الباحث ضرورة تقنينٍ تفصيلي داخل قانون الإجراءات الجزائية لتعريف "الأصل الرقمي" ونسخته" على وجهٍ لا لبس فيه، وإلزام محاضر الضبط بذكر الأدوات والقيم التجزيئية بوصفها بصماتٍ رقمية، ووضع نموذج وطني لسلسلة الحيازة مستلهَم من أفضل الممارسات الدولية، وجعل الخبرة

المحايدة لازمة متى كان الدليل الإلكتروني جوهريًا. كما أوصي بإرساء قاعدة التنقيح الإلزامي عند نشر الأحكام في قضايا المستهلك، مع إيداع نسخة حرزيّة غير منقّحة لصون حقوق الدفاع.

الفرع الثالث

عبء الإثبات وصعوباته في الجرائم الإلكترونية

يبقى عبء الإثبات الجنائي على عاتق النيابة العامة وفق معيار القناعة القضائية مع صون قرينة البراءة. غير أنّ الطبيعة الرقمية للدليل تُنشئ عوائق عملية تستدعي تنظيمًا رشيدًا للمسؤوليات دون المساس بجوهر العبء (قانون الإجراءات الجزائية، 2001، المواد 205، 206).

أوّلًا: تجزّؤ الدليل والعبور الحدودي

تتوزّع الأدلة بين أجهزة الضحية، وحساباته المخزّنة في بيئاتٍ سحابية، وخوادم منصّاتٍ أجنبية، ووسطاء دفعٍ دوليين. وتخضع كل جهةٍ لسياسات احتفاظٍ وحذفٍ آلي تختلف مددُها؛ ما يعني أنّ ساعاتٍ قليلة قد تكفي لفقدان سجلاتٍ حاسمة. وعلى سلطات الضبط والادّعاء المبادرة العاجلة بإصدار أوامر حفظ البيانات قبل مسارات الإنابة الكاملة، وتوثيق كل مخاطبةٍ مع المزوّدين حفاظًا على أثرٍ إجرائي يُظهر بذل العناية الواجبة ولا يُحمّل الضحية تبعة فوات المدد الفنيّة. وتعرض اتفاقية بودابست لمجلس أوروبا نماذج عملية لأوامر الحفظ والإنتاج والتفتيش الإلكتروني تصلح للاستئناس التنظيمي (قرار بقانون رقم 10، 2018، المواد 38، 39).

ثانيًا: هشاشة الدليل ومتطلّبات السرعة

تُعدّ أدلة المستهلك الإلكتروني متطايرة: رسائل تُحرَّر ثم تُسحَب، إعلانات تُحذف، حسابات تُغلق، سجلات دخول تُستبدل دوريًا. ويقتضي ذلك اعتماد بروتوكول إسعافٍ رقمي يُقدّم حفظ الأدلة الأشدّ عرضةً للزوال وفق ترتيب قابلية الفقد، مع استخلاص نسخٍ جنائية فورية للأجهزة والحسابات حين يتاح

ذلك، وتحرير محاضر ضبطٍ دقيقة تُدرج الطوابع الزمنية والمناطق الزمنية وإعدادات الأجهزة وإصدارات التطبيقات ومسارات التخزين (قانون الإجراءات الجزائية، 2001، المواد 30،31،32 منه).

ثالثًا: ترجمة الدليل التقني إلى قناعة قضائية

لا تكفي التقارير الفنيّة وحدها لإقناع المحكمة؛ إذ يتعيّن اختبار المنهج: ما أداة الجمع؟ وهل ثُبّتت السلامة عبر قيم التجزئة؟ وما هامش الخطأ؟ وما بدائل التفسير المعقولة؟ وهل يُحتمل الانتحال أو الدخول غير المصرّح؟ وهل السجلّ صادرٌ عن طرفٍ ثالثٍ موثوق أم عن مصدرٍ يمكن التلاعب به؟ وتتساند أسئلة المحكمة للخبير مع مرافعات الدفاع لبناء القناعة. وعلى النيابة تقديم عرضٍ مترابط يُظهر تساند القرائن القادمة من منصّاتٍ متعددة زمنيًا وتقنيًا، ويقابل ذلك على الدفاع بيان احتمالاتٍ واقعية تُقوّض هذا الاتساق كدعوى الاختراق أو مشاركة الجهاز أو اضطراب ضبط الوقت أو وجود ثغرات في المنصّة (قانون الإجراءات الجزائية، 2001، المواد 205–207).

رابعًا: أعباء ثانوية على ذوي الاختصاص

مع بقاء العبء الأصلي على النيابة، قد ينهض عبءٌ ثانوي على مزوّدٍ مرخّص بحفظ حدٍّ أدنى من السجلات لمددٍ معقولة وتقديم شهادات صحّةٍ بشأنها، أو على المتهم في مسائل فنيةٍ خالصة لإثارة احتمالٍ معقول (كإثبات إصابة الجهاز ببرمجيةٍ خبيثة وقت الواقعة). وليس ذلك نقلًا للعبء، وإنّما تنظيمٌ لمساره في بيئةٍ تقنية معقّدة، مع بقاء الشكّ المعقول لصالح المتهم (قرار بقانون رقم 10، 2018، المواد 38–40).

خامسًا: تمكين المستهلك الضحية

إن المستهلك هو الضحية لأنه معرض لمؤثرات كبيرة، ولذلك فهو الضحية الأولى في ظل الخداع اليومي لشراء ما ليس هو بحاجة إليه (الأخرس، 2024، صفحة 112).

تُثقل كلفة الإثبات على الضحية: ترجمة مراسلات، أتعاب خبرة، نسخٌ جنائي للأجهزة. ويُوازَن ذلك بوسائل المشاركة عن بُعد، والسماح بإيداع مذكّراتٍ وملفّات رقمية عبر قنواتٍ آمنة، وتمكين الادّعاء المدني بطلب تدابير تحفظية لإزالة المحتوى المضلّل، وإغلاق الحسابات الوهمية، وإلزام المنصّات بتسليم البيانات الضرورية، بحيث يتوقّف الضرر الجاري وتتيسّر الحجّة. كما ينبغي تحديد نطاق الأسئلة وإطلاع الخصوم على حدود الاطلاع منعًا لتحويل إجراءات الإثبات إلى انتهاكٍ جديد للحياة الرقمية (قانون الإجراءات الجزائية، 2001، المواد 60–62؛ القانون الأساسي المعدل، 2003، المواد 9، 10، 32؛ قانون حماية المستهلك، 2005، المواد 3، 4، 9).

سادسًا: التشفير والتراسل المأمون

قد يحول التشفير الطرفي دون الاطلاع على المحتوى، لكن ذلك لا يُعدم القرائن؛ إذ تبقى البيانات الوصفية للطوابع الزمنية والعلاقات الاتصالية، وسجلات استعادة الحساب، وتغييرات الأجهزة الموثّقة لدى المنصّة، ومسارات الدفع، قرائنَ ذات وزن إذا تكاملت مع غيرها. وعليه، لا ينبغي حصر الإثبات في "نص الرسالة"، بل يُبنى على البنية المحيطة التي قد تُقيم لوحة قرائنٍ كافية أو تُنشئ شكًّا معقولًا (قانون الإجراءات الجزائية، 2001، المادة 205؛ القرار بقانون رقم 10، 2018).

سابعًا: قاعدة الدليل الأفضل في البيئة الرقمية

في عالم الورق تُفضّل النسخة الأصلية. أمّا رقميًا فالأصل هو الملفّ الثنائي ببياناته الوصفية، لا اللقطة المصوّرة القابلة للتعديل. وعليه يتعيّن تقديم الأصل أو نسخةٍ جنائية منه مع بصمته الرقمية، وتظلّ اللقطات مكمّلة لا بديلة، ما لم يتعذّر تحصيل الأصل لأسبابٍ موضوعيةٍ موثّقة كإغلاق المنصّة أو انقضاء مدّة الاحتفاظ (القرار بقانون رقم 15، 2017، المواد 6–9؛ قانون الإجراءات الجزائية، 2001، المادة 205).

ويرى الباحث أنّ معالجة صعوبات عبء الإثبات تمرّ عبر ترتيبات مؤسسية وتشريعية متكاملة: إنشاء وحدة إنفاذٍ رقمي متخصّصة تصدر أوامر حفظٍ قياسية وتدير سلسلة الحيازة، وإلزام المزوّدين المرخّصين محليًا بمعايير احتفاظٍ دنيا وبواجهات استجابةٍ قضائية محدّدة الآجال، ووضع دليلٍ مرجعي للقضاة بأسئلةٍ فنية معيارية لاختبار التقارير، والنصّ على لزوم الخبرة المحايدة عند تقديم دليلٍ إلكتروني جوهري، واستحداث آليةٍ قضائيةٍ سريعة للأوامر العابرة للحدود بالتنسيق مع الجهات المختصّة. وبهذا يُصان معيار القناعة القضائية وتُحترم قرينة البراءة وتُحفظ حقوق الضحية في آنٍ معًا.

خاتمة المطلب

موقف المشرّع الفلسطيني من نظام الإثبات فيالجرائم الواقعة على المستهلك الإلكتروني

يتّضح من استقراء نصوص قانون الإجراءات الجزائية الفلسطيني، وما استقرّ عليه القضاء، أنّ المشرّع الفلسطيني لم يعتمد نظامًا إثباتيًا خاصًا أو مستقلًا للجرائم الإلكترونية أو لجرائم المستهلك الإلكتروني على وجه التحديد، وإنما أخضعها – من حيث المبدأ – للنظام العام للإثبات الجنائي القائم على حرية القاضي الجنائي في تكوين قناعته، في إطار الشرعية الإجرائية وضمانات المحاكمة العادلة.

فالأصل أن المشرّع الفلسطيني تبنّى نظام الاقتناع القضائي الحر، الذي لا يقيّد المحكمة بدليلٍ معيّن أو ترتيبٍ جامد للأدلة، ويُجيز لها استخلاص الحقيقة من أي دليل تطمئن إليه، متى كان قد جُمع بطريقٍ مشروع وخضع للمناقشة العلنية. ويشمل ذلك – بحكم العموم – الأدلة الرقمية، ولو لم يُفرد لها تنظيمًا إجرائيًا خاصًا.

غير أنّ تطبيق هذا النظام العام على الجرائم الواقعة على المستهلك الإلكتروني يكشف عن قصور تشريعي وظيفي، لا في المبادئ، بل في الوسائل؛ إذ إن قواعد الإثبات صِيغت ابتداءً للتعامل مع أدلة مادية تقليدية، في حين أن الدليل الرقمي يتميّز بالهشاشة الزمنية، والطابع الفني المعقّد، وارتباطه الوثيق بالخصوصية، وكونه غالبًا عابرًا للحدود.

وعليه، يمكن القول إن المشرّع الفلسطيني انتهج نظامًا عامًا مرنًا في الإثبات يسمح – من حيث الإطار النظري – باستيعاب الدليل الرقمي، لكنه ترك مسألة تكييف هذا الدليل وإجراءاته العملية لاجتهاد القضاء والخبرة الفنية، دون أن يضع قواعد تفصيلية لسلسلة الحيازة الرقمية، أو لأوامر حفظ البيانات العاجلة، أو لتنقيح الأدلة والأحكام حمايةً لخصوصية الضحية.

وبذلك، فإن خصوصيّة الإثبات في الجرائم الواقعة على المستهلك الإلكتروني لا تستند إلى نظام قانوني خاص أقرّه المشرّع صراحةً، وإنما تنشأ من: تطبيق النظام العام للإثبات الجنائي على مادة إثباتية ذات طبيعة رقمية مختلفة؛ وتوسّع الدور التفسيري للقاضي الجنائي في تقدير حجّية الدليل الرقمي ومناقشة الخبرة الفنية؛ ومن ثم الاستعانة بالمعايير الفنية المقارنة لسدّ الفراغ الإجرائي، دون أن ترقى هذه المعايير إلى مرتبة النص الملزم.

وخلاصة الأمر، أن المشرّع الفلسطيني اتبع نظام الإثبات الجنائي الحر القائم على الاقتناع القضائي، مع إخضاع الجرائم الرقمية – بما فيها الجرائم الواقعة على المستهلك الإلكتروني – للقواعد العامة، الأمر الذي يفرض اليوم ضرورة تطوير هذا النظام عبر ملاحق إجرائية رقمية أو تدخل تشريعي صريح، لا لتغيير فلسفة الإثبات، بل لجعلها أكثر ملاءمة لطبيعة الدليل الرقمي وحمايةً للطرف الأضعف في الخصومة.

الخاتمة

خلصت هذه الدراسة إلى أن التحول الرقمي أفرز تحديات قانونية جديدة كشفت عن قصور التشريعات الفلسطينية الحالية في توفير حماية جنائية متكاملة للمستهلك الإلكتروني بوصفه الطرف الأضعف في العلاقة التعاقدية. كما تبيّن أن تشتت القواعد الموضوعية والإجرائية، وغياب تنظيم خاص بالإثبات والأدلة الرقمية، يحدّ من فاعلية المواجهة الجنائية للجرائم الإلكترونية. وعليه، تبرز الحاجة إلى إطار تشريعي وإجرائي موحّد يواكب خصوصية السوق الإلكتروني ويوازن بين حماية المستهلك وتشجيع التجارة الرقمية.

وانطلاقًا من هذه الخلاصات، تنتقل الدراسة إلى عرض مجموعة من النتائج التي تم التوصل إليها، متبوعة بجملة من التوصيات المقترحة لتعزيز الحماية الجنائية للمستهلك الإلكتروني في السوق الفلسطيني.

أولاً : النتائج

الإطار المفاهيمي للحماية يقوم على تحديد المستهلك الإلكتروني كطرف ضعيف، والإطار التنظيمي يشمل التشريعات والإجراءات والإشراف على العقود الإلكترونية لضمان حقوقه، مع وضع الجرائم الإلكترونية ضمن دائرة التدابير الجزائية لحمايته.

يتعرض المستهلك الإلكتروني لجرائم ماسة بحمايته تشمل: الدخول غير المشروع إلى الأنظمة الإلكترونية، والاحتيال الإلكتروني، وانتهاك الخصوصية والاعتداء على البيانات الشخصية، والإخلال بالالتزامات التعاقدية الإلكترونية والخداع في المنتجات والخدمات.

الجرائم الماسة بالمستهلك الإلكتروني تشترك مع الجرائم التقليدية في الأركان القانونية، لكنها تختلف من حيث وسيلة ارتكابها وطبيعتها الرقمية. لذلك، تحتاج هذه الجرائم إلى تدخل تشريعي خاص ينظم صورها وأركانها وعقوباتها لضمان حماية جنائية فعّالة للمستهلك في البيئة الرقمية.

رغم أهمية العقوبات الجنائية الحالية في حماية المستهلك الإلكتروني، إلا أنها تبقى متناثرة بين نصوص عدة وتستند أحياناً إلى القياس التقليدي على الجرائم المادية، مما يقلل من فعالية الردع في البيئة الرقمية المتطورة. وتُطبق هذه العقوبات على كل من يرتكب أفعالًا ضارة بحق المستهلك الإلكتروني، سواء كان مزوّدًا أو تاجرًا أو أي طرف آخر يستغل الوسائل الإلكترونية للاحتيال، الغش، الانتحال، أو التلاعب بالبيانات والمعلومات الشخصية للمستهلك.

إن الإجراءات الجنائية المتعلقة بضبط الجرائم الإلكترونية وملاحقة مرتكبيها في فلسطين تعتمد على منظومة متدرجة بين البحث والتحري والتحقيق، مع مراعاة الخصوصية الرقمية للأدلة وحماية الحقوق الفردية. فإجراءات البحث تمثل المرحلة الأولية، وتهدف إلى كشف وقوع الجريمة وجمع المعلومات العامة، بينما تركز إجراءات التحري على تتبع المشتبه بهم وجمع الأدلة الرقمية الحساسة باستخدام أدوات تقنية متقدمة.

أن التنظيم القضائي الفلسطيني الحالي يوفر إطارًا قانونيًا عامًا لضبط الجرائم الإلكترونية الواقعة على المستهلك، لكنه يحتاج إلى تطوير آليات إجرائية وتقنية محددة تتناسب مع خصوصية البيئة الرقمية وطبيعة الأدلة الإلكترونية، بما يضمن فاعلية الملاحقة الجنائية، وحماية المستهلك، وصون حقوق المتهم في الوقت ذاته.

أن خصوصية الإثبات الرقمي ليست مجرد قاعدة عامة، بل استجابة عملية للطبيعة الخاصة للمستهلك الإلكتروني كطرف ضعيف، وتستلزم تطوير آليات التحقيق والملاحقة القضائية لضمان سلامة الأدلة الرقمية وحجيتها أمام القضاء، بما يحقق حماية فعّالة للمستهلك الإلكتروني في بيئته الرقمية.

تتسم قواعد الإثبات في الجرائم التي تستهدف المستهلك الإلكتروني بخصوصية عالية، نتيجة اختلال التوازن بين قدرات المستهلك التقنية والمعرفية وقدرات الجاني الرقمي أو المهني، إضافة إلى هشاشة

الأدلة الرقمية وتعقيدها وكلفتها العالية. ويترتب على هذه الخصوصية ضرورة تكييف إجراءات الإثبات بما يحقق التوازن بين حماية حقوق المستهلك وضمانات المحاكمة العادلة.

المشرّع الفلسطيني اتبع نظام الإثبات الجنائي الحر مع تطبيقه على الجرائم الرقمية، مما يستدعي اليوم تطوير أدوات إجرائية رقمية أو تدخل تشريعي صريح لجعل النظام أكثر توافقًا مع طبيعة الأدلة الرقمية، وضمان حماية المستهلك كطرف ضعيف في الخصومة.

إن التشريعات الفلسطينية النافذة لحماية المستهلك الإلكتروني، مثل قانون حماية المستهلك رقم (21) لسنة 2005، وقانون الجرائم الإلكترونية رقم (10) لسنة 2018، وقانون المواصفات والمقاييس رقم (6) لسنة 2000، تقدّم أساسًا لحماية المستهلك، سواء من الناحية الموضوعية أو الجزائية. فهي تجرّم الأفعال الضارة بالمستهلك، وتفرض عقوبات على المخالفين، وتضع معايير لضمان سلامة المنتجات والخدمات، بما يعكس اهتمام المشرّع بحماية الطرف الأضعف في العلاقة التعاقدية.

ثانياً: التوصيات :

سن تشريع موحد ومتكامل للمستهلك الإلكتروني: يوصى بإصدار قانون فلسطيني شامل ينظم حماية المستهلك في السوق الرقمي، يجمع بين الحقوق الموضوعية والإجراءات الجزائية، ويحدد بوضوح المستهلك الإلكتروني، وحقوقه، وواجبات المزودين، وضوابط العقود الإلكترونية، بما يحقق حماية متكاملة للطرف الأضعف في العلاقة التعاقدية.

تطوير التجريم الجزائي للجرائم الرقمية: ينبغي تعديل النصوص الجنائية لتغطية جميع صور الجرائم الإلكترونية الواقعة على المستهلك، مثل الاحتيال، والخداع، وانتهاك الخصوصية، والتلاعب بالبيانات، وتحديد أركانها القانونية وعقوباتها بما يتناسب مع خطورة الأضرار الرقمية، لضمان فعالية الردع العام والخاص.

تعزيز آليات الضبط والملاحقة التقنية: يجب تجهيز الأجهزة القضائية والأمنية بالأدوات والبرمجيات المتقدمة للتحري الرقمي، وتحليل الأدلة الإلكترونية، مع تدريب الكوادر الفنية لضمان سرعة وفعالية الملاحقة الجنائية، مع الالتزام بضمانات حماية البيانات والحقوق الفردية.

تكييف إجراءات الإثبات مع خصوصية الأدلة الرقمية: ينبغي تطوير آليات متخصصة لإثبات الجرائم الرقمية، تشمل سلسلة الحيازة الرقمية، وطرق التحفظ على البيانات، وضمان سلامة الأدلة وحجيتها أمام القضاء، مع مراعاة حقوق المستهلك في الخصوصية ومنع إعادة الإيذاء الإجرائي.

تعزيز دور الخبراء الفنيين في المحاكم: يوصى بالاستعانة بخبراء مستقلين لتفسير الأدلة الرقمية أمام المحكمة، وتمكين المستهلك من المشاركة الفاعلة في مناقشة هذه الأدلة، لضمان تكافؤ القدرات بين الأطراف وتطبيق المحاكمة العادلة.

ضبط العقوبات لتواكب البيئة الرقمية: ينبغي مراجعة العقوبات الجنائية الحالية لتكون صارمة وملائمة للأضرار الرقمية، مع تحديد مسؤولية المزودين، والتجار، وأي طرف يستغل الوسائل الإلكترونية لارتكاب جرائم بحق المستهلك، لضمان فعالية الردع.

تعزيز التعاون القضائي الدولي: في الجرائم العابرة للحدود، يجب تطوير آليات فعالة للتعاون مع الجهات الأجنبية لاستصدار البيانات الرقمية، وحفظ الأدلة، ومتابعة مرتكبي الجرائم، بما يحافظ على حقوق المستهلك ويضمن عدم ضياع الأدلة الرقمية.

دمج التشريعات والإجراءات لتسهيل التطبيق: يوصى بتقليص التشتت التشريعي بين عدة قوانين، ودمج الحماية الموضوعية والإجرائية في إطار واحد يسهل على القضاء والجهات الرقابية التكييف القانوني، ويضمن حماية المستهلك الإلكتروني بفعالية ومرونة.

يوصى بدعم وتوفير كوادر وطنية متخصصة في أمن المعلومات والتحقيق الرقمي، بما يعزز قدرة الجهات المختصة على كشف الجرائم الإلكترونية التي تستهدف المستهلك الإلكتروني وحماية بياناته وحقوقه في البيئة الرقمية.

كما يُوصى بوضع تنظيم قانوني واضح يُلزم مزوّدي خدمات الإنترنت بحفظ ملفات المراجعة والسجلات الرقمية وفق ضوابط دقيقة توازن بين متطلبات الملاحقة الجنائية وضمان خصوصية المستهلك وعدم التعسف في استخدام بياناته. وفي هذا الإطار، يُشجَّع على تعزيز البحث العلمي والدراسات القانونية والتقنية المتخصصة في الجرائم الإلكترونية الواقعة على المستهلك الإلكتروني، بما يسهم في تطوير التشريعات الوطنية ومواءمتها مع المخاطر الرقمية المتجددة، ويحقق حماية فعّالة ومستدامة للطرف الأضعف في السوق الإلكتروني.

المراجع العلمية

ابراهيم، خالد ممدوح. (2008). إبرام العقد عبر الوسائل الإلكترونية. *دار الفكر العربي*، صفحة 38.

أبو زينة،محمد. (2022). التحري الإلكتروني وحدود الملاحقة الجزائية. *مجلة العلوم القانونية جامعة النجاح الوطنية*.

أبو شمالة ، فايز. (2010). شرح قانون الإجراءات الجزائية الفلسطيني. *المكتبة القانونية*.

أبوالرب، نبيل محمود. (2018). مفهوم الجرائم المعلوماتية وتحدياتها التشريعية في فلسطين. *جامعة النجاح الوطنية*.

الاتحاد الأوروبي. (2018). اللائحة العامة لحماية البيانات.

الأخرس، إبراهيم. (2024). الدعم وحماية المستهلك في ظل العولمة (ط. 2). *مكتبة مدبولي*.

الأمانة العامة لمجلس الوزراء. (2023). تقرير حول جهود مكافحة الجريمة الإلكترونية.

الأودن، سمير عبد السميع. (2005). العقد الإلكتروني. *منشأة المعارف*، صفحة 28.

الأيام. (15 1، 2026). *https://www.alayam.com/alayam/first/1092467/News.html*.

جرادات، محمد. (2021). إشكاليات الملاحقة الإجرائية للجرائم الإلكترونية في فلسطين. *مجلة جامعة الأزهر، 23(1)*، الصفحات 89-91.

الجزيرة نت. (2026). *https://www.aljazeera.net*.

جمعية حماية المستهلك الفلسطيني. (2026). http://www.palconsumers.org.

الجهاز المركزي للإحصاء الفلسطيني، و وزارة الاتصالات وتكنولوجيا المعلومات. (2021). *تقرير واقع التجارة الإلكترونية في فلسطين*.

الجيلاوي،أحمد رعد. (2018). التسجيل الصوتي وحجيته في الإثبات الجنائي (ط. 1). *المركز العربي*.

حجازي، عبد الفتاح بيومي. (2007). شرح قانون العقوبات: القسم العام. *دار الفكر الجامعي*، الصفحات 45-48.

حسني،محمود نجيب. (2022). شرح قانون العقوبات: القسم العام. *دار النهضة العربية*، صفحة 27.

الحسيناوي، محمد حسن. (2018). ضمانات حقوق الإنسان في مرحلة التحري وجمع الأدلة: دراسة مقارنة. *المركز العربي للدراسات*.

حمودة، سارة. (2020). المسؤولية المدنية عن الجرائم الإلكترونية [رسالة ماجستير غير منشورة]. *جامعة النجاح الوطنية*.

الحميدي، يوسف محمد. (2019). القانون التجاري الإلكتروني: نظرية عامة في عقود التجارة الإلكترونية. *(ط. 1). دار الفكر الجامعي*، صفحة 85.

حوى، فاتن حسين. (2012). الوجيز في قانون حماية المستهلك. *منشورات الحلبي الحقوقية*.

الحياة. (2 1، 2026). *التجارة الإلكترونية في فلسطين: نمو وتحديات قانونية واقتصادية*. تم الاسترداد من https://www.alhaya.ps.

خالد عبد الحق، و دعاء وعبد العال. (2025). أساسيات التشفير. دار اليازوري.

خلف، حلا محمود. (2024). الحماية القانونية للمذعن في عقود الإذعان. *دار اليازوري*.

خليفة، حمد أحمد. (2020). الإثبات والالتزامات في العقود الإلكترونية (ط. 1). *دار الفكر الجامعي*.

درويش، رامي. (2022). حدود مشروعية التفتيش الرقمي. *مجلة القانون الجنائي المعاصر*، الصفحات 259-302.

الدويك، رائد. (2022). حماية الخصوصية الرقمية في فلسطين [ورقة مقدّمة إلى مؤتمر الجرائم الإلكترونية]. *رام الله، فلسطين*.

الرشيد، عادل عبد العزيز. (2022). *قرائن الجريمة الإلكترونية وأثرها في الإثبات*. دار الدكتور للنشر.

رؤيا الثاقبة. (2026). *التجارة الإلكترونية في فلسطين: النمو والفرص والتحديات*. تم الاسترداد من https://www.roya-thaqba.com.

الزغبي، محمد عبد الكريم. (2016). الحماية الجنائية للمستهلك في التجارة الإلكترونية. *دار الثقافة للنشر والتوزيع*، صفحة 45.

الزغول،أسيل نايف. (2023). الحماية القانونية للمستهلك في العقود الإلكترونية وفقاً لأحكام التشريع الأردني. *[رسالة ماجستير غير منشورة]. جامعة فيلادلفيا*، صفحة 15.

الزنداني،إبراهيم محمد. (2020). إجراءات الاستدلال والتحقيق الابتدائي في الجرائم الإلكترونية وأثرها على حجية أدلة الإثبات [أطروحة دكتوراه]. *جامعة فطاني*.

سرور،أحمد فتحي. (1989). الوسيط في قانون العقوبات. *القسم العام. دار النهضة العربية.*، صفحة 47.

سلامة،أحمد عبد الكريم. (2009). لحماية القانونية للمستهلك. *دار النهضة العربية*، الصفحات 18-20.

السنهوري،عبد الرزاق. (1963). الوسيط في شرح القانون المدني: نظرية العقد (الجزء 1). *دار إحياء التراث العربي*، صفحة 437.

شبكة القدس الإخبارية. (15 1، 2026). *https://qudsn.com*.

شعوة، هلال. (2016). *حماية المستهلك من جريمة الإعلان التجاري المضلل أو الكاذب*. تم الاسترداد من مركز البصيرة للبحوث، (23).

شيرين كدواني، و توفيق شريهان. (2023). الإعلام الرقمي: تشريعات وأخلاقيات النشر (ط. 2). *العربي للنشر والتوزيع*.

عبدالباقي، مصطفى. (2018). التحقيق في الجريمة الإلكترونية وإثباتها في فلسطين: دراسة مقارنة. دراسات: علوم الشريعة والقانون. *الجامعة الأردنية*.

عبدالرحمن، محمد. (2018). حماية المستهلك في البيئة الرقمية. *دار الثقافة للنشر والتوزيع*.

العتيبي، محمد ذعار. (2013). النظام القانوني للعقد الإلكتروني. *دراسة مقارنة [رسالة ماجستير غير منشورة]*.

العجمي، فلاح فهد. (2011). الحماية المدنية للمستهلك في العقد الإلكتروني. *[رسالة ماجستير غير منشورة]. جامعة الشرق الأوسط.*، صفحة 24.

عزيز، سردار علي. (2014). ضمانات المتهم أثناء الاستجواب (ط. 1). *المركز القومي للإصدارات القانونية*.

عصفور، خليل. (2021). التحقيق في الجرائم عبر الحدود. . *المجلة الفلسطينية للعلوم القانونية*، الصفحات 11-50.

عمرو عبدالرحمن. (2019). الجرائم الإلكترونية: دراسة قانونية مقارنة. *دار الفكر الجامعي*.

فايق، مينا. (2026). التحقيق في الجرائم المرتكبة ضد المستهلكين عبر الإنترنت. *[مقال منشور]*.

فهمي، عبد الفتاح مراد. (2008). الجرائم الإلكترونية: دراسة مقارنة. . *دار الكتب القانونية*، صفحة 322.

الفيل، علي عدنان. (2011). الجرائم الإلكترونية. ستار تايمز – شؤون قانونية. *http://www.startimes.com*.

قانون الاتصالات رقم (3). (1996). بشأن الاتصالات السلكية واللاسلكية.

القانون الأساسي الفلسطيني المعدل. (2003). الوقائع الفلسطينية.

قانون الجرائم الإلكترونية الأردني رقم (17). (2023). قانون الجرائم الإلكترونية. *الجريدة الرسمية الأردنية*.

قانون العقوبات الفلسطيني. (1936). رقم (74) لسنة 1936. *(المطبق في قطاع غزة)*.

قانون العقوبات. (1960). رقم (16). *المطبق في الضفة الغربي*، الصفحات 417-422.

قانون حماية المستهلك الفلسطيني. (2005). رقم (21). *الوقائع الفلسطينية*، الصفحات 4-21.

قانون رقم (08-09) . (2009). المتعلق بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي. *الجريدة الرسمية المغربية*.

قانون شأن المطبوعات رقم (9). (1995 ب والنشر). الوقائع الفلسطينية .

قناة المواطن. (2026). سرقة حسابات بنكية في قطاع غزة: كيف تتم وما الوسائل المستخدمة؟ *https://www.almwatin.com*.

كميل، طارق. (2023). حماية المستهلك في التعاقد عبر شبكة الإنترنت. *مجلة الجامعة العربية الأمريكية للبحوث*.

محكمة استئناف رام الله. (27 12، 2018). حكم في القضية رقم (45) . *منشورات المقتفي، جامعة بيرزيت*.

محكمة النقض الفلسطينية. (2019). طعن جزائي رقم (2018/644) (جلسة 7 أبريل). *منشور على موقع مقام، جامعة النجاح الوطنية*.

محكمة النقض الفلسطينية. (2025). طعن رقم (2025/38) (جلسة 3 مارس). *منشورات موقع مقام، جامعة النجاح الوطنية*.

المختار عطار. (2009). دراسة في العقد الإلكتروني. *[بحث منشور]*.

مديرية تكنولوجيا المعلومات. (2015). أنواع الجريمة الإلكترونية وأهدافها. *https://search.emarefa.net*.

مدين، محمود. (2020). فن التحقيق والإصابات في الجرائم الإلكترونية. *المصرية للنشر والتوزيع*.

المناصرة، آية فيصل. (2023). حماية المستهلك في التسويق الإلكتروني. *دراسة مقارنة [رسالة ماجستير غير منشورة]. جامعة النجاح الوطنية*، صفحة 24.

المنشاوي، محمد أحمد. (2015). مبادئ علم العقاب. *دار القانون والاقتصاد*، صفحة 37.

منصور، محمد حسين. (2007). المسؤولية المدنية في مجال التجارة الإلكترونية. *دار النهضة العربية*.

الهيئة المستقلة لحقوق الإنسان. (2023). تقرير الممارسات الإجرائية. صفحة 23.

وزارة الاقتصاد الفلسطينية الوطني. (2021). تقرير حماية المستهلك.

وكالة سند للأنباء. (2026). *https://snd.ps/pos*.

الوليد، ساهر إبراهيم. (2024). شرح قانون الإجراءات الجزائية الفلسطيني (الجزء 1، ط. 1). *دار النهضة العربية*.

اليوم السابع. (2025). *بزعم تحديث البيانات: تفاصيل التحقيق مع متهم بالاستيلاء على بيانات عملاء البنوك*. تم الاسترداد من https://www.youm7.com/story/2025/5/28/7003426.

.

An-Najah National University

Faculty of Graduate Studies

CRIMINAL PROTECTION OF THE CONSUMER IN THE ELECTRONIC MARKET

By

MamounTaher Mohammed Samara

Supervisor

Dr. Abdul Latif Rabaya

This Thesis is submitted in partial fulfillment of the requirements for the degree of Master's in Criminal Law, Faculty of Graduate Studies, An-Najah National University, Nablus - Palestine.

2025

CRIMINAL PROTECTION OF THE CONSUMER IN THE ELECTRONIC MARKET

By
MamounTaher Mohammed Samara
Supervisor
Dr. Abdul Latif Rabaya

Abstract

This thesis examines the challenges of criminal protection for consumers within the electronic market amid rapid digital transformation. It investigates emerging patterns of electronic transactions, revealing a pronounced power imbalance between parties in contractual relationships. The study emphasizes that electronic consumers constitute the weaker party, rendering them particularly vulnerable to digital threats.

To accomplish the objectives of this study, the researcher employed a descriptive-analytical methodology. This approach entailed a comprehensive examination and analysis of the Palestinian legislative framework regulating electronic consumer protection, considering both substantive and procedural dimensions. The study specifically addresses the sufficiency of provisions related to criminalization and penalties, mechanisms for criminal prosecution, and evidentiary rules in effectively addressing contemporary electronic crimes.

The study concluded that, although existing Palestinian legislation contains provisions criminalizing harmful acts against consumers, it is characterized by fragmentation and a lack of legislative specificity. Moreover, the legislation does not adequately address the evolving nature of the electronic market and digital evidence. These limitations undermine the effectiveness of criminal deterrence and weaken the protection afforded to electronic consumers, especially during the prosecution and evidentiary phases.

The study advocates for the establishment of a unified and comprehensive Palestinian law on electronic consumer protection. This legislation should encompass integrated regulations addressing both substantive and procedural matters, offer a precise definition of the term "electronic consumer," and delineate the various types of digital offenses, their constituent elements, and corresponding penalties. Furthermore, it should govern the mechanisms for criminal prosecution and the handling of digital evidence to strengthen trust in the Palestinian electronic market.

Keywords: criminal protection, electronic consumer, digital evidence, electronic market, legislative fragmentation, substantive and procedural law.