



وزارة التعليم العالي والبحث العلمي
جامعة عمار ثليجي الأغواط
كلية الحقوق والعلوم السياسية
قسم الحقوق



دراسة تحليلية لجرائم العنف ضد الأشخاص المتصلة بالمعلوماتية

مذكرة لنيل شهادة الماستر في الحقوق
تخصص قانون جنائي والعلوم الجنائية

إشراف الأستاذ

د/

من إعداد الطالب

جلول دحو

السنة الجامعية 2025 - 2026

فمحمداً

الإهداء

إلى مَنْ أضاء لي دروب العلم بصبرهما ودعائهما، ولم ييخلا يوماً بتضحية من أجل أن أصل إلى ما وصلت إليه... إلى **والديّ الكريمين**، أطال الله في عمرهما وأمدّهما بالصحة والعافية.

إلى إخوتي وأخواتي، سندي وعوني في محطات الحياة كافة.

إلى كل أستاذ كريم مدّ لي يد العون والمعرفة طيلة مساري الدراسي، فكان نبراساً أهتدي بعلمه.

إلى كل صديق وزميل رافقني في هذه المسيرة، وشدّ من أزري في لحظات التعب والإحباط.

إلى كل من يؤمن بأن العدالة يجب أن تلاحق الجريمة أينما وُجدت، ولو كانت خلف شاشة أو حساب مجهول.

أهدي هذا العمل المتواضع.

جلول دحو

شكر وتقدير

الحمد لله رب العالمين الذي وفقني بفضلِهِ وكرمه لإتمام هذا العمل المتواضع، وأسأله سبحانه أن يجعله خالصاً لوجهه الكريم، نافعاً لكل من يطّلع عليه.

كما يطيب لي أن أتقدم بجزيل الشكر والامتنان والتقدير إلى الأستاذ المشرف على هذه المذكرة، على ما أولانيه من وقت ثمين وتوجيهات سديدة وملاحظات قيّمة، كان لها بالغ الأثر في إخراج هذا العمل بالصورة التي هو عليها، فله (لها) مني كل التقدير والاحترام. كما أتقدم بالشكر إلى أعضاء لجنة المناقشة الموقرين، على تفضلهم بقبول مناقشة هذا العمل وإثرائه بملاحظاتهم القيمة.

ولا يفوتني أن أشكر كل أساتذتي الأفاضل الذين تعاقبوا على تكويني العلمي طيلة مساري الجامعي، وكل من ساهم من قريب أو بعيد، بمعلومة أو نصيحة أو تشجيع، في إنجاز هذا البحث.

كما أتوجه بالشكر إلى إدارة وموظفي المكتبات التي أتاحت لي الاطلاع على مختلف المراجع والمصادر التي استعنت بها في إعداد هذه الدراسة.

وأخيراً، شكر خاص لعائلي الكريمة على دعمها المتواصل وصبرها الكبير طيلة فترة إعداد هذا البحث.

ملخص الدراسة

تتناول هذه الدراسة موضوع "دراسة تحليلية لجرائم العنف ضد الأشخاص المتصلة بالمعلوماتية"، باعتباره أحد أبرز الإشكاليات القانونية المستحدثة التي أفرزتها الثورة التكنولوجية الراهنة، حيث لم تعد وسائل التواصل الاجتماعي والأجهزة الذكية مجرد أدوات للتواصل والتقدم، بل تحولت إلى أدوات جديدة لارتكاب صور مستحدثة من الإجرام تستهدف الإنسان في سلامته الجسدية والنفسية والمعنوية، كالتهديد والابتزاز الإلكتروني، والتشهير والتحرش والمطاردة الإلكترونية.

وقد انطلقت هذه الدراسة من إشكالية رئيسية مفادها: إلى أي مدى استطاع المشرع، من خلال النصوص القانونية القائمة، الموضوعية منها والإجرائية، مواجهة هذا النمط من الإجرام وتوفير الحماية اللازمة لضحاياه؟ وللإجابة عن هذه الإشكالية، اعتمدت الدراسة المنهج الوصفي التحليلي والمنهج المقارن، وقُسمت إلى فصلين: تناول الفصل الأول الإطار المفاهيمي والقانوني لهذه الجرائم، من خلال تحديد ماهيتها وخصائصها وصورها المتعددة، ثم تحليل أساسها القانوني وأركانها الموضوعية. في حين تناول الفصل الثاني الإطار الإجرائي والوقائي لمواجهتها، من خلال دراسة خصوصية التحقيق والإثبات في هذا النمط من الجرائم، والجهات المختصة بالتحقيق والملاحقة، وصولاً إلى آليات حماية الضحايا وسبل الوقاية من هذه الظاهرة. وخلصت الدراسة إلى أن هذا النمط الإجرامي يتميز بخصائص فنية وتقنية (كاللامادية، والطابع العابر للحدود، وسهولة الإخفاء) تجعله يفلت أحياناً من قبضة النصوص القانونية التقليدية، وأن المشرع، رغم تدخله الملموس على المستويين الوطني والدولي، لا يزال مطالباً بمزيد من الجهد التشريعي والمؤسساتي لمواكبة هذا التطور المتسارع، وتعزيز آليات حماية الضحايا ومرافقتهم نفسياً واجتماعياً، وتفعيل التعاون الدولي بما يتناسب مع الطابع العابر للحدود لهذه الجريمة.

الكلمات المفتاحية: الجريمة المعلوماتية؛ العنف الرقمي؛ التهديد الإلكتروني؛ الابتزاز الإلكتروني؛ التشهير الإلكتروني؛ المطاردة الإلكترونية؛ الدليل الرقمي؛ حماية الضحايا.

Abstract

This study addresses "An Analytical Study of Cybercrimes of Violence Against Persons," considered one of the most prominent emerging legal issues resulting from the current technological revolution. Social media platforms and smart devices are no longer mere tools for communication and progress; they have become new instruments for committing novel forms of crime that target individuals' physical, psychological, and moral integrity, such as cyber threats, online extortion (sextortion), cyber defamation, harassment, and cyberstalking. This research is guided by a central problem: to what extent has the legislator, through existing substantive and procedural legal texts, succeeded in confronting this type of crime and providing adequate protection for its victims? To answer this question, the study adopts a descriptive–analytical approach combined with a comparative method, and is divided into two chapters. The first chapter examines the conceptual and legal framework of these crimes by defining their nature, characteristics, and various forms, then analyzing their legal basis and the constituent elements of the offense. The second chapter addresses the procedural and preventive framework for confronting these crimes, examining the specificity of investigation and evidence–gathering in this type of offense, the competent authorities for investigation and prosecution, and finally the mechanisms for victim protection and prevention strategies. The study concludes that this criminal pattern is characterized by technical features (such as immateriality, its cross–border nature, and ease of concealment) that often allow it to escape the grip of traditional legal texts. Despite tangible legislative intervention at both the national and international levels, legislators remain called upon to make further legislative and institutional efforts to keep pace with this rapid development, strengthen victim–protection mechanisms and psychosocial support, and activate international cooperation commensurate with the transnational nature of this crime.

Keywords: Cybercrime; Digital Violence; Cyber Threats; Sextortion; Cyber Defamation; Cyberstalking; Digital Evidence; Victim Protection.

الصفحة	العنوان
-	الإهداء
-	شكر وتقدير
-	ملخص الدراسة (بالعربية)
أ	المقدمة
8	الفصل الأول: الإطار المفاهيمي والقانوني لجرائم العنف ضد الأشخاص المتصلة بالمعلوماتية
9	المبحث الأول: ماهية جرائم العنف ضد الأشخاص المتصلة بالمعلوماتية
9	المطلب الأول: تعريف هذه الجرائم وخصائصها
9	الفرع الأول: تعريف الجريمة المعلوماتية العنيفة ضد الأشخاص
12	الفرع الثاني: خصائص وسمات هذه الجرائم
17	المطلب الثاني: صور وأنواع جرائم العنف ضد الأشخاص المتصلة بالمعلوماتية
17	الفرع الأول: جرائم التهديد والابتزاز الإلكتروني
19	الفرع الثاني: جرائم التشهير والتحرش والمطاردة الإلكترونية
23	المبحث الثاني: الأساس القانوني والتكييف الجزائي لهذه الجرائم
23	المطلب الأول: الأساس القانوني لتجريم العنف المعلوماتي ضد الأشخاص
23	الفرع الأول: النصوص القانونية الوطنية
25	الفرع الثاني: الاتفاقيات والمواثيق الدولية
26	المطلب الثاني: التكييف القانوني وأركان الجريمة
26	الفرع الأول: الركن المادي
29	الفرع الثاني: الركن المعنوي
31	خلاصة الفصل الأول

33	الفصل الثاني: الإطار الإجرائي والوقائي لمواجهة جرائم العنف ضد الأشخاص المتصلة بالمعلوماتية
34	المبحث الأول: الإجراءات الجزائية الخاصة بمكافحة هذه الجرائم
34	المطلب الأول: خصوصية التحقيق والإثبات في الجرائم المعلوماتية
34	الفرع الأول: أساليب جمع الأدلة الرقمية
38	الفرع الثاني: صعوبات الإثبات وحجية الدليل الرقمي
41	المطلب الثاني: الجهات المختصة بالتحقيق والملاحقة
41	الفرع الأول: الأجهزة الوطنية المتخصصة
43	الفرع الثاني: آليات التعاون القضائي والدولي
46	المبحث الثاني: الحماية القانونية للضحايا وسبل الوقاية
46	المطلب الأول: آليات حماية ضحايا العنف المعلوماتي
46	الفرع الأول: الحماية القانونية والقضائية
48	الفرع الثاني: الحماية النفسية والاجتماعية
50	المطلب الثاني: سبل الوقاية ومكافحة هذه الجرائم
50	الفرع الأول: الوقاية التقنية والتوعوية
52	الفرع الثاني: تطوير التشريعات ومقترحات الإصلاح
54	خلاصة الفصل الثاني
56	الخاتمة
57	نتائج الدراسة
58	التوصيات
61	قائمة المصادر والمراجع

مقدمة

يشهد العالم في العصر الراهن ثورة تكنولوجية غير مسبوقة في مجال المعلوماتية والاتصالات، أحدثت تحولاً جذرياً في مختلف مناحي الحياة الاجتماعية والاقتصادية والثقافية والسياسية، حتى أصبحت شبكة الإنترنت ووسائل التواصل الاجتماعي والأجهزة الذكية جزءاً لا يتجزأ من الحياة اليومية للأفراد والمجتمعات. فقد ألغت هذه الثورة الرقمية الحدود الجغرافية والزمنية، وقربت المسافات بين الشعوب، ويسّرت سبل التواصل والتبادل المعرفي والتجاري، بما جعل العالم أشبه بقرية صغيرة تتفاعل عناصرها في الزمن الحقيقي.

غير أن هذا التطور التقني الهائل، على الرغم مما حققه من إيجابيات جمّة، لم يكن خالياً من الآثار السلبية والمخاطر الجسيمة، إذ سرعان ما تحوّلت هذه الوسائل التقنية من أدوات للتواصل والتقدم إلى أدوات جديدة لارتكاب الجريمة، فظهر إلى الوجود نمط إجرامي مستحدث يُعرف بـ"الجريمة المعلوماتية" أو "الجريمة الإلكترونية"، والتي تُعد من أخطر صور الإجرام المعاصر نظراً لخصوصيتها التقنية، وصعوبة اكتشافها وإثباتها، وسهولة ارتكابها عبر الحدود دون حاجة إلى تواجد مادي للجاني في مكان الجريمة.

ومن بين أخطر الصور التي اتخذتها الجريمة المعلوماتية، تلك التي تمس بسلامة الأشخاص الجسدية والنفسية والمعنوية، إذ لم يعد العنف مقتصرًا على صورته التقليدية المرتبطة بالاعتداء المادي المباشر، بل امتد ليأخذ أبعاداً جديدة عبر الفضاء الرقمي، فظهرت جرائم التهديد الإلكتروني، والابتزاز الجنسي والمالي عبر الشبكة، والتحرش والمطاردة الإلكترونية (Cyberstalking)، والتشهير والقذف والسب عبر مواقع التواصل الاجتماعي، والتحرّيش على الانتحار أو الإيذاء الذاتي، وغيرها من الصور التي تستهدف الإنسان في كرامته وحرمة الشخصية وسلامته النفسية، وقد تمتد آثارها لتصل إلى المساس بحياته أو سلامته الجسدية ذاتها.

وتتميز هذه الجرائم بخطورة استثنائية تفوق في كثير من الأحيان خطورة الجرائم التقليدية المماثلة، ويعود ذلك إلى عدة عوامل، أهمها: سرعة انتشار الفعل الإجرامي وأثره عبر الشبكة العنكبوتية إلى عدد هائل من الأشخاص في زمن وجيز، وإمكانية إخفاء هوية الجاني أو انتحاله

لهوية مزيفة، مما يصعب عملية تتبعه وملاحقته قضائياً، فضلاً عن الطابع العابر للحدود لهذه الجرائم الذي يثير إشكالات معقدة تتعلق بالاختصاص القضائي والتعاون الدولي في مجال التحقيق والملاحقة. يضاف إلى ذلك الأثر النفسي البالغ الذي تخلفه هذه الجرائم لدى الضحايا، والذي قد يفوق أحياناً الأثر الناجم عن الاعتداء المادي المباشر، لما يترتب عليها من شعور بالمهانة والخوف والقلق الدائم، خاصة أن الفعل الإجرامي يبقى موثقاً ومتداولاً عبر الشبكة، مما يُطيل من أمد المعاناة النفسية للضحية ويصعب عملية التعافي منها.

ولم تكن الفئات الهشة في المجتمع، كالنساء والأطفال والمراهقين، بمنأى عن استهداف هذا النمط من الإجرام، بل باتت الأكثر عرضة له، إذ تشير العديد من الدراسات والإحصائيات الحديثة إلى تنامي ظاهرة التمرر الإلكتروني والابتزاز الجنسي الموجه للقاصرين، وجرائم العنف الرقمي القائم على النوع الاجتماعي، مما يستدعي تدخلاً تشريعياً وقضائياً حازماً وفعالاً لحماية هذه الفئات من مخاطر الفضاء الرقمي المتنامية.

وإدراكاً من المشرّع لخطورة هذا النمط الإجرامي المستحدث، فقد بادرت العديد من التشريعات الوطنية، على غرار التشريعات المقارنة، إلى سن نصوص قانونية خاصة تجرم هذه الأفعال وتحدد لها عقوبات رادعة، إلى جانب المصادقة على العديد من الاتفاقيات والمواثيق الدولية والإقليمية المتعلقة بمكافحة الجريمة الإلكترونية، وعلى رأسها اتفاقية بودابست لمكافحة الجريمة الإلكترونية باعتبارها أول اتفاقية دولية شاملة في هذا المجال. غير أن هذا التدخل التشريعي، على أهميته، لا يزال يواجه صعوبات جمة تتعلق بمواكبة التطور المتسارع للتقنية، وسد الثغرات القانونية التي يستغلها الجناة، وتذليل العقبات الإجرائية المرتبطة بجمع الأدلة الرقمية وإثباتها أمام القضاء.

أهمية الموضوع

تكمن أهمية هذا الموضوع في عدة جوانب، يمكن إجمالها في البعدين النظري والعملية:

فمن الناحية النظرية، تبرز أهمية الدراسة في كونها تتناول موضوعاً حديث النشأة والتكوين، لا يزال الفقه القانوني بصدد بلورة مفاهيمه وتأسيس أحكامه، مما يستدعي تحليلاً معمقاً لطبيعة هذه الجرائم وخصائصها المميزة، وتحديد موقعها ضمن التصنيفات القانونية التقليدية للجرائم الماسة بالأشخاص، والوقوف على مدى ملاءمة النصوص القانونية القائمة لمواجهة هذا النمط الإجرامي المستحدث.

أما من الناحية العملية، فتتجلى أهمية الموضوع في التزايد المضطرد لأعداد الجرائم المعلوماتية الماسة بسلامة الأشخاص، وما يخلفه ذلك من آثار وخيمة على الأفراد والمجتمع ككل، الأمر الذي يستوجب الوقوف على مدى فعالية الآليات القانونية والإجرائية المعتمدة حالياً لمواجهة هذه الجرائم، سواء من حيث التجريم والعقاب، أو من حيث آليات الإثبات والتحقيق، أو من حيث سبل حماية الضحايا ورعايتهم، بغية تقديم رؤية تحليلية نقدية قد تسهم في تطوير الإطار القانوني والمؤسساتي المعني بمكافحة هذه الظاهرة.

أسباب اختيار الموضوع

تعود دوافع اختيار هذا الموضوع إلى مجموعة من الأسباب الذاتية والموضوعية، يمكن إيجازها فيما يلي:

فمن الأسباب الذاتية، الميل الشخصي والاهتمام الأكاديمي بمواضيع القانون الجنائي المعلوماتي باعتباره من أكثر فروع القانون تطوراً وحدثاً، والرغبة في التعمق في دراسة إشكالياته المعقدة التي تتقاطع فيها المعارف القانونية مع المعارف التقنية.

أما من الأسباب الموضوعية، فتتمثل في التنامي الملحوظ لهذا النمط من الجرائم في السنوات الأخيرة، وما رافقه من قصور تشريعي وقضائي في التعامل معه بالشكل الأمثل، إضافة إلى قلة الدراسات الأكاديمية المتخصصة التي تناولت هذا الموضوع بالتحليل والتفصيل، خاصة فيما يتعلق بالجانب الإجرائي وحماية الضحايا، مما يجعل من هذه الدراسة إضافة علمية قد تسد جزءاً من هذا الفراغ البحثي.

إشكالية الدراسة

انطلاقاً مما سبق، تتبلور إشكالية هذه الدراسة في التساؤل الرئيسي التالي:

إلى أي مدى استطاع المشرع من خلال النصوص القانونية القائمة، الموضوعية منها والإجرائية، مواجهة جرائم العنف ضد الأشخاص المتصلة بالمعلوماتية، وتوفير الحماية اللازمة لضحايا هذا النمط الإجرامي المستحدث؟

ويتفرع عن هذا التساؤل الرئيسي مجموعة من التساؤلات الفرعية، أهمها:

- ما المقصود بجرائم العنف ضد الأشخاص المتصلة بالمعلوماتية، وما هي أبرز صورها وخصائصها المميزة لها عن الجرائم التقليدية؟
- ما هو الأساس القانوني الذي استند إليه المشرع في تجريم هذه الأفعال، وما مدى كفاية هذا التجريم لمواجهة التطور المتسارع لهذه الظاهرة؟
- ما هي خصوصية الإجراءات الجزائية المتبعة في التحقيق في هذه الجرائم وإثباتها، وما هي أبرز الصعوبات التي تواجه الجهات المختصة في هذا الشأن؟
- ما هي آليات الحماية القانونية المقررة لضحايا هذه الجرائم، وما مدى فعاليتها في جبر الضرر الواقع عليهم ووقايتهم من التعرض لها مستقبلاً؟

فرضيات الدراسة

للإجابة عن الإشكالية المطروحة، يمكن صياغة الفرضيات التالية كإجابات مؤقتة تسعى الدراسة إلى التحقق من صحتها أو نفيها:

- الفرضية الأولى: تتسم جرائم العنف ضد الأشخاص المتصلة بالمعلوماتية بخصائص مميزة تجعلها تختلف جوهرياً عن الجرائم التقليدية، سواء من حيث وسيلة ارتكابها أو نطاق آثارها أو صعوبة إثباتها.

- الفرضية الثانية: يعاني الإطار القانوني الحالي من قصور نسبي في مواكبة التطور المتسارع لهذا النمط الإجرامي، مما يستدعي تدخلاً تشريعياً لسد الثغرات القائمة.
- الفرضية الثالثة: تواجه الإجراءات الجزائية التقليدية صعوبات عملية جمة عند تطبيقها على الجرائم المعلوماتية، خاصة فيما يتعلق بجمع الأدلة الرقمية والحفاظ على حجيتها أمام القضاء.
- الفرضية الرابعة: لا تزال آليات حماية ضحايا هذه الجرائم غير كافية، وتحتاج إلى تعزيز من الناحيتين القانونية والمؤسسية.

المنهج المتبع

اقتضت طبيعة هذا الموضوع الاعتماد على مجموعة من المناهج العلمية المتكاملة، يأتي في مقدمتها المنهج الوصفي التحليلي، الذي تم الاعتماد عليه في وصف وتحليل النصوص القانونية المنظمة لجرائم العنف ضد الأشخاص المتصلة بالمعلوماتية، سواء على المستوى الوطني أو المقارن. كما تم الاستعانة بالمنهج المقارن من خلال عقد مقارنات بين التشريع الوطني والتشريعات المقارنة والاتفاقيات الدولية ذات الصلة، بغية الوقوف على أوجه التشابه والاختلاف واستخلاص الحلول الأنسب. وأخيراً، تم توظيف المنهج النقدي في تقييم مدى كفاية النصوص القانونية القائمة ومدى فعاليتها في مواجهة هذا النمط الإجرامي، وصولاً إلى تقديم مقترحات وتوصيات قد تسهم في تطوير الإطار القانوني المنظم لهذا الموضوع.

الدراسات السابقة

تناولت بعض الدراسات الأكاديمية جوانب من الجريمة المعلوماتية بصفة عامة، إلا أن الدراسات المتخصصة التي تناولت بالتحديد جرائم العنف ضد الأشخاص المتصلة بالمعلوماتية تبقى قليلة نسبياً، وغالباً ما اقتصر على معالجة صورة واحدة من صور هذا النمط الإجرامي، كالتحرش الإلكتروني أو الابتزاز دون التطرق إلى باقي الصور بشكل شامل ومتكامل. وتسعى

هذه الدراسة إلى تجاوز هذا القصور من خلال تقديم معالجة تحليلية شاملة تجمع بين الجانب الموضوعي والإجرائي لهذا النمط من الجرائم.

الصعوبات التي واجهت الدراسة

اعترضت إعداد هذه الدراسة جملة من الصعوبات، أبرزها قلة المراجع الفقهية المتخصصة التي تناولت الموضوع بالتحديد والتفصيل، نظراً لحدثة الظاهرة محل الدراسة، إضافة إلى التطور المستمر والمتسارع للتقنيات المستخدمة في ارتكاب هذه الجرائم، مما يجعل من الصعب الإحاطة بكل صورها المستحدثة، فضلاً عن ندرة الأحكام والاجتهادات القضائية المنشورة والمتعلقة بهذا الموضوع، مما حدّ من إمكانية الاستناد إلى تطبيقات قضائية كافية لتدعيم التحليل النظري.

خطة الدراسة

للإجابة عن الإشكالية المطروحة واختبار الفرضيات الموضوعية، ارتأينا تقسيم هذه الدراسة إلى فصلين، نتناول في الفصل الأول الإطار المفاهيمي والقانوني لجرائم العنف ضد الأشخاص المتصلة بالمعلوماتية، من خلال بحثين، يتناول أولهما ماهية هذه الجرائم بتعريفها وبيان خصائصها وصورها، ويتناول ثانيهما الأساس القانوني لتجريمها والتكليف الجزائي لها من حيث أركانها. أما الفصل الثاني، فنخصصه لدراسة الإطار الإجرائي والوقائي لمواجهة هذه الجرائم، من خلال بحثين أيضاً، يتناول أولهما خصوصية الإجراءات الجزائية المتبعة في التحقيق والإثبات، ويتناول ثانيهما آليات الحماية القانونية للضحايا وسبل الوقاية من هذا النمط الإجرامي.

الفصل الأول

يُعد تحديد الإطار المفاهيمي والقانوني لأي ظاهرة إجرامية مستحدثة خطوة تأسيسية لا غنى عنها قبل الخوض في تحليل جوانبها الإجرائية والوقائية، ذلك أن ضبط المفهوم وتحديد الأركان يُعدّان الأساس الذي تُبنى عليه سائر الأحكام القانونية اللاحقة، فلا يمكن الحديث عن حماية جنائية فعالة لضحايا جريمة ما دون تحديد دقيق لماهيتها وأركانها وصورها أولاً. كما أن غياب الدقة المفاهيمية في هذا المجال قد يُفضي إلى تضارب في التكييف القانوني أمام القضاء، وإلى تفاوت في المعاملة بين حالات متشابهة موضوعياً، وهو ما يُهدد مبدأ المساواة أمام القانون ومبدأ الشرعية الجزائية في آنٍ واحد. ولهذا الغرض، نتناول في هذا الفصل، من خلال مبحثين، ماهية جرائم العنف ضد الأشخاص المتصلة بالمعلوماتية في مبحث أول، ثم الأساس القانوني والتكييف الجزائي لهذه الجرائم في مبحث ثانٍ.

المبحث الأول: ماهية جرائم العنف ضد الأشخاص المتصلة بالمعلوماتية

يقتضي البحث في ماهية هذه الجرائم الوقوف أولاً على تعريفها وبيان خصائصها التي تميزها عن الجرائم التقليدية (مطلب أول)، قبل الانتقال إلى استعراض أبرز صورها وأنواعها التي أفرزها الواقع العملي والتطور التقني المتسارع (مطلب ثان).

المطلب الأول: تعريف هذه الجرائم وخصائصها

الفرع الأول: تعريف الجريمة المعلوماتية العنيفة ضد الأشخاص

أولاً- في تعريف الجريمة المعلوماتية بصفة عامة وإشكالية ضبط مصطلحها:

لم يتفق الفقه القانوني، سواء على المستوى الوطني أو المقارن، على تعريف جامع مانع للجريمة المعلوماتية، نظراً لحداثة الظاهرة وتعدد صورها وتشعب جوانبها التقنية، الأمر الذي انعكس على تعدد التعريفات الفقهية وتباينها بحسب الزاوية التي ينظر منها كل فقيه إلى الظاهرة، فمنهم من ركّز على الوسيلة المستخدمة، ومنهم من ركّز على محل الجريمة، ومنهم من جمع بين الاثنين¹. ويُضاف إلى ذلك أن تعدد التسميات المستخدمة للدلالة على هذا النمط الإجرامي (كالجريمة المعلوماتية، والجريمة الإلكترونية، والجريمة السيبرانية، وجريمة الحاسوب) قد زاد من حدة هذا التشتت المفاهيمي، رغم أن هذه المصطلحات تُستخدم في الغالب بصفة تبادلية دون تمييز دقيق بينها من الناحية الاصطلاحية².

فقد عرّف جانب من الفقه الجريمة المعلوماتية بأنها "كل سلوك غير مشروع يرتكب باستخدام الحاسب الآلي أو أي وسيلة معلوماتية أخرى، يترتب عليه ضرر يلحق بالمجني عليه"³، وهو تعريف واسع يجعل من الحاسوب أو الوسيلة التقنية مجرد أداة لارتكاب جرائم قد تكون تقليدية في طبيعتها القانونية. في حين ذهب اتجاه آخر إلى تعريفها بأنها "كل فعل

¹ عبد الفتاح بيومي حجازي، النظام القانوني لحماية التجارة الإلكترونية، دار الفكر الجامعي، الإسكندرية،

² دراسة اصطلاحية مقارنة حول تعدد تسميات الجريمة المعلوماتية (معلوماتية/إلكترونية/سيبرانية).

³ محمد أمين الرومي، جرائم الحاسوب وحقوق المؤلف والمصنفات الفنية، دار الفكر الجامعي، الإسكندرية،

إجرامي تُستخدم فيه تقنية المعلومات كأداة رئيسية لارتكابه أو كمحل له⁴، فيدخل بذلك ضمن مفهوم الجريمة المعلوماتية كلاً من الجرائم التي تكون فيها التقنية وسيلة (كالنصب الإلكتروني)، والجرائم التي تكون فيها التقنية ذاتها محلاً للاعتداء (كجرائم الدخول غير المشروع إلى الأنظمة المعلوماتية).

وذهب فريق ثالث من الفقه إلى تعريفها من زاوية أكثر تقنية، فعرفها بأنها "كل نشاط غير مشروع منظم قوامه المعالجة الآلية للبيانات ونقل المعلومات"⁵، وهو تعريف يُبرز الطابع الفني والتقني لهذه الجريمة أكثر من إبرازه للجانب القانوني الجزائي، مما جعله محل انتقاد من بعض الفقه باعتباره تعريفاً وظيفياً أقرب إلى علوم الحاسوب منه إلى العلوم القانونية⁶. وقد حاول اتجاه رابع التوفيق بين هذه المقاربات المتعددة، فعرف الجريمة المعلوماتية بأنها "كل فعل أو امتناع يشكل اعتداءً على مصلحة يحميها القانون، يتم ارتكابه أو تسهيله باستخدام تقنية المعلومات والاتصال، بصرف النظر عن كون هذه التقنية وسيلة أو محلاً للاعتداء"⁷، وهو تعريف جامع يبدو أكثر شمولاً وأقرب إلى الضبط القانوني الدقيق.

ثانياً- تعريف جرائم العنف ضد الأشخاص المتصلة بالمعلوماتية تحديداً:

انطلاقاً من هذه التعريفات العامة للجريمة المعلوماتية، ووصولاً إلى الصنف الخاص محل الدراسة، يمكن تعريف جرائم العنف ضد الأشخاص المتصلة بالمعلوماتية بأنها: "تلك الأفعال غير المشروعة التي تُرتكب باستخدام الوسائل التقنية والمعلوماتية، كشبكة الإنترنت ووسائل التواصل الاجتماعي والهاتف الذكي والبريد الإلكتروني والتطبيقات الرقمية، وتستهدف بصفة مباشرة أو غير مباشرة المساس بسلامة الشخص الطبيعي الجسدية أو النفسية أو

⁴ هدى حامد قشقوش، جرائم الحاسب الآلي في التشريع المقارن، دار النهضة العربية، القاهرة،

⁵ عمر محمد أبو بكر بخيت، الجرائم المعلوماتية عبر الإنترنت، دار الجامعة الجديدة، الإسكندرية،

⁶ ملاحظة نقدية فقهية على التعريفات ذات الطابع التقني البحت للجريمة المعلوماتية.

⁷ تعريف توفيقى مستخلص من مقارنة الاتجاهات الفقهية المتعددة سالفة الذكر.

المعنوية أو حرته، سواء عن طريق التهديد أو الترهيب أو الابتزاز أو التحرش أو التشهير أو المطاردة أو غير ذلك من الصور، بما يلحق به ضرراً مادياً أو معنوياً⁸.

ويلاحظ من هذا التعريف أن جرائم العنف ضد الأشخاص المتصلة بالمعلوماتية تشترك مع الجريمة المعلوماتية بصفة عامة في عنصر الوسيلة، أي استخدام التقنية والمعلوماتية في ارتكاب الفعل، لكنها تتفرد عنها بعنصر المحل والهدف، إذ ينصب الاعتداء فيها بصفة مباشرة على الشخص الطبيعي ذاته، في سلامته الجسدية أو النفسية أو المعنوية أو حرته، لا على ذمته المالية كما في جرائم الاحتيال والنصب المعلوماتي، ولا على النظام المعلوماتي ذاته كما في جرائم الدخول والتخريب المعلوماتي⁹.

ثالثاً - علاقة هذا المفهوم بمصطلح "العنف الرقمي" وموقعه من التصنيفات الجرمية التقليدية:

وتجدر الإشارة إلى أن هذا النمط من الجرائم بات يُعرف في الأدبيات الحديثة، خاصة الصادرة عن المنظمات الدولية، بمصطلح "العنف الرقمي" (Digital Violence) أو "العنف القائم على النوع الاجتماعي عبر الإنترنت" (Online Gender-Based Violence) "حين يستهدف النساء بصفة خاصة، وهو مصطلح أوسع من الناحية الاجتماعية، لكنه يتقاطع إلى حد بعيد مع المفهوم القانوني الذي تسعى هذه الدراسة إلى تحديده وضبط أركانه، إذ إن ما يهمنا هنا هو البعد القانوني الجزائي لهذا العنف، أي الأفعال التي يُمكن أن تُشكل جريمة يعاقب عليها القانون، وليس مجرد السلوكيات المسيئة التي لا ترقى إلى مرتبة الجريمة¹⁰.

وعلى صعيد آخر، يثير هذا المفهوم إشكالية تصنيفية تتعلق بموقعه من التقسيم التقليدي للجرائم الواقعة على الأشخاص إلى جرائم واقعة على الحياة والسلامة الجسدية، وجرائم واقعة على الشرف والاعتبار، وجرائم واقعة على الحرية، إذ يُلاحظ أن جرائم العنف الرقمي تتداخل

⁸ تعريف مقترح من إعداد الباحث، بالاستناد إلى التعريفات الفقهية المشار إليها في الهوامش (1) إلى (7) أعلاه.

⁹ جميل عبد الباقي الصغير، *الجرائم الناشئة عن استخدام الحاسب الآلي*، دار النهضة العربية، القاهرة، [ص. ...].

¹⁰ يُنظر تقارير المنظمات الدولية المتخصصة (منظمة الصحة العالمية، هيئة الأمم المتحدة للمرأة) بشأن مفهوم Online Gender-Based Violence، وموقعها من مفهوم الجريمة المعلوماتية بالمعنى القانوني الدقيق.

مع هذه التصنيفات الثلاثة في آنٍ واحد، فقد تُشكل مساساً بالسلامة النفسية (وهي امتداد حديث لمفهوم السلامة الجسدية)، وقد تُشكل مساساً بالشرف والاعتبار (كالتشهير والقذف)، وقد تُشكل مساساً بالحرية (كالمطاردة والتحرش)، مما يجعلها فئة "عابرة للتصنيفات" تستعصي على الحصر ضمن باب واحد من أبواب قانون العقوبات التقليدي¹¹.

رابعاً- التمييز بين جرائم العنف الرقمي والجرائم المعلوماتية المالية والتقنية البحتة:

ولتحديد المفهوم بدقة أكبر، يقتضي الأمر التمييز بوضوح بين جرائم العنف ضد الأشخاص المتصلة بالمعلوماتية من جهة، وبين صنفين آخرين من الجرائم المعلوماتية قد يختلط الأمر بينهما أحياناً: فمن جهة أولى، تختلف هذه الجرائم عن الجرائم المعلوماتية المالية (كالاحتيال والنصب الإلكتروني وسرقة بيانات البطاقات المصرفية)، والتي وإن كانت تستهدف شخصاً طبيعياً أيضاً، إلا أن محل الاعتداء فيها هو الذمة المالية للضحية لا سلامته الشخصية¹². ومن جهة ثانية، تختلف عن الجرائم المعلوماتية التقنية البحتة (كالدخول غير المشروع إلى الأنظمة المعلوماتية، والفيروسات المعلوماتية، وهجمات الحرمان من الخدمة)، والتي ينصب الاعتداء فيها في المقام الأول على النظام المعلوماتي أو البنية التحتية التقنية ذاتها، وإن كان قد ينجم عنها أحياناً ضرر غير مباشر بالأشخاص¹³.

ونخلص مما سبق إلى أن التعريف المختار لهذه الدراسة يقوم على ثلاثة عناصر جوهرية: عنصر الوسيلة (استخدام التقنية المعلوماتية)، وعنصر المحل (استهداف الشخص الطبيعي في ذاته)، وعنصر النتيجة (إحداث ضرر جسدي أو نفسي أو معنوي)، وهي عناصر سنعود إليها بالتفصيل عند دراسة أركان هذه الجريمة في المبحث الثاني من هذا الفصل.

الفرع الثاني: خصائص وسمات هذه الجرائم

¹¹ دراسة تصنيفية نقدية حول موقع جرائم العنف الرقمي من التقسيم التقليدي للجرائم الواقعة على الأشخاص.

¹² عبد الفتاح بيومي حجازي، مرجع سابق، [ص. ...]، بشأن التمييز بين الجرائم المالية والجرائم الماسة بالأشخاص.

¹³ هدى حامد قشقوش، مرجع سابق، [ص. ...]،

تتميز جرائم العنف ضد الأشخاص المتصلة بالمعلوماتية بجملة من الخصائص التي تميزها عن الجرائم التقليدية المماثلة (كجريمة التهديد أو القذف أو التحرش في صورتها التقليدية)، ويكتسي تحديد هذه الخصائص أهمية بالغة، ذلك أنها هي التي تُفسر الصعوبات العملية التي تواجه عملية التكييف القانوني والتحقيق والإثبات لاحقاً، كما تُشكل الأساس الذي ينبغي أن تُبنى عليه أي مقارنة تشريعية أو إجرائية خاصة بهذا النمط من الإجرام. ويمكن إجمال أهم هذه الخصائص فيما يلي:

أولاً- خاصية اللامادية والافتراضية: إذ لا يستلزم ارتكاب هذه الجرائم تواجداً مادياً للجاني في مسرح الجريمة بالمفهوم التقليدي، بل يمكن ارتكابها عن بُعد باستخدام وسائل تقنية بحتة، دون أي تلامس مادي أو مواجهة مباشرة بين الجاني والضحية، مما يضفي عليها طابعاً افتراضياً يصعب من عملية إثباتها وتتبع مرتكبها، ويجعل مسرح الجريمة بمفهومه التقليدي (المكان المادي) عديم الجدوى أحياناً، ليحل محله "مسرح جريمة رقمي" يتمثل في الأجهزة والشبكات والخوادم¹⁴. وتترتب على هذه الخاصية نتيجة مهمة تتمثل في أن الجاني قد لا يشعر بذات الحاجز النفسي أو الأخلاقي الذي يشعر به مرتكب الجريمة التقليدية عند مواجهته المباشرة لضحيته، مما قد يُفسر جزئياً ارتفاع منسوب العنف والقسوة في الخطاب الرقمي مقارنة بالتفاعل المباشر وجهاً لوجه، وهي ظاهرة يُطلق عليها الباحثون في علم النفس الاجتماعي "أثر عدم الكبح عبر الإنترنت"¹⁵ (Online Disinhibition Effect) "

ثانياً- خاصية العابرة للحدود (الطابع عبر الوطني): حيث لا تراعي هذه الجرائم الحدود الجغرافية للدول، فقد يكون الجاني في دولة والضحية في دولة أخرى، وقد يُستضاف المحتوى غير المشروع على خوادم موجودة في دولة ثالثة، بل قد تنتزع عناصر الجريمة الواحدة على عدة دول في آنٍ واحد، مما يثير إشكاليات معقدة تتعلق بتحديد الاختصاص القضائي والقانون

¹⁴ جميل عبد الباقي الصغير، مرجع سابق، [ص. ...].

¹⁵ دراسات في علم النفس الاجتماعي حول ظاهرة "أثر عدم الكبح عبر الإنترنت". (Online Disinhibition Effect) "

واجب التطبيق، ويستوجب تفعيل آليات التعاون القضائي الدولي التي سنفصل فيها في الفصل الثاني من هذه الدراسة¹⁶.

ثالثاً- خاصية سهولة الإخفاء وصعوبة الإثبات: إذ يستطيع الجاني إخفاء هويته الحقيقية عبر استخدام أسماء مستعارة أو حسابات وهمية أو تقنيات إخفاء عنوان بروتوكول الإنترنت (VPN) أو تقنية "تور" (TOR) "أو غيرها من وسائل التخفي التقني، مما يصعب من عملية كشف هويته الحقيقية وملاحقته قضائياً، ويجعل من "مجهولية الجاني" سمة غالبية في هذا النمط من الإجرام¹⁷.

رابعاً- خاصية السرعة والانتشار الواسع (اللاتناسبية بين الفعل والضرر): إذ ينتقل الفعل الإجرامي وآثاره عبر الشبكة إلى عدد هائل من الأشخاص في وقت قياسي قد لا يتجاوز بضع دقائق أو ثوانٍ، وذلك بفضل خاصية "المشاركة" و"إعادة النشر" في وسائل التواصل الاجتماعي، مما يضاعف من حجم الضرر الواقع على الضحية مقارنة بالجرائم التقليدية المماثلة، ويجعل ثمة عدم تناسب صارخ بين بساطة الفعل الإجرامي (كضغط زر واحدة) وجسامة الضرر الناتج عنه¹⁸.

خامساً- خاصية استمرارية الأثر النفسي وتجده: فخلافاً للاعتداء المادي المباشر الذي قد ينتهي أثره بانتهاء الفعل ذاته، فإن المحتوى الرقمي المسيء (كصورة أو فيديو أو منشور) يبقى متداولاً ومتاحاً للاطلاع عليه لفترة طويلة، بل قد يُعاد نشره وتداوله من جديد بعد سنوات، مما يُطيل من أمد المعاناة النفسية للضحية ويصعب عملية التعافي منها، ويجعلها عرضة "للإيذاء متكرر (Re-victimization)" كلما أُعيد تداول المحتوى¹⁹.

¹⁶ نفس المرجع (جميل عبد الباقي الصغير)، [ص. ...].

¹⁷ عبد الله سليمان سليمان، أثر الأنظمة المعلوماتية في قواعد الإثبات الجنائي، دار النهضة العربية، القاهرة، [ص. ...].

¹⁸ دراسات ميدانية حول سرعة انتشار المحتوى الرقمي على منصات التواصل الاجتماعي، يُنظر تقارير الاتحاد الدولي للاتصالات (ITU) ذات الصلة.

¹⁹ يُنظر أدبيات علم النفس الجنائي حول أثر التشهير والتتمر الإلكتروني على الصحة النفسية للضحايا وظاهرة الإيذاء المتكرر.

سادساً- **خاصية تعدد الجناة واحتمال التواطؤ الجماعي**: إذ لا تقتصر هذه الجرائم في الغالب على جانب واحد، بل قد يُشارك فيها عدد كبير من الأشخاص عبر إعادة النشر أو التعليق المسيء أو المشاركة في حملة تشهير جماعية، وهو ما يُعرف بظاهرة "الغوغائية الرقمية" (Cyber Mob)، مما يثير إشكاليات خاصة في تحديد المسؤولية الجزائية لكل مساهم في الفعل الإجرامي، وفي التمييز بين الفاعل الأصلي والشريك والمساهم العرضي²⁰.

سابعاً- **خاصية الحاجة إلى خبرة تقنية متخصصة في الإثبات**: إذ لا يمكن التعامل مع هذا النمط من الجرائم بالوسائل التقليدية للتحقيق والإثبات، بل يستلزم الأمر خبرة تقنية متخصصة في مجال الأدلة الرقمية (Digital Forensics)، سواء لدى أجهزة الشرطة القضائية أو لدى الخبراء المساعدين للقضاء، وهو ما سنفصل فيه لاحقاً في الفصل الثاني من هذه الدراسة²¹.

ثامناً- **خاصية استهداف فئات معينة بصفة غالبية**: إذ تُظهر الدراسات الإحصائية والميدانية أن هذا النمط من الجرائم لا يستهدف كافة فئات المجتمع بالتساوي، بل يتركز بصفة أكبر على فئات بعينها، كالنساء (خاصة في صور التحرش والابتزاز الجنسي)، والقاصرين (في صور التنمر والاستدراج الجنسي)، والشخصيات العامة والناشطين والصحفيين (في صور التهديد والتشهير الجماعي)، مما يستدعي مقاربات تشريعية وحمائية خاصة تراعي هذه الخصوصية الفئوية²².

تاسعاً- **خاصية التطور التقني المستمر لأساليب الارتكاب**: إذ تتسم هذه الجرائم بالتجدد المستمر في أساليب ووسائل ارتكابها تبعاً لتطور التقنية ذاتها، فما كان يستلزم في السابق مهارة تقنية متقدمة (كاختراق الحسابات) بات اليوم في متناول عامة المستخدمين بفضل توفر أدوات جاهزة الاستخدام، كما أن ظهور تقنيات مستحدثة كالذكاء الاصطناعي التوليدي قد

²⁰ نفس المرجع، بشأن ظاهرة الغوغائية الرقمية. (Cyber Mob)

²¹ هدى حامد قشقوش، مرجع سابق، [ص. ...].

²² تقارير إحصائية دولية حول الفئات الأكثر استهدافاً بجرائم العنف الرقمي (نساء، قاصرون، صحفيون).

أضاف صوراً جديدة كلياً لم تكن متصورة من قبل (كتريف الصور ومقاطع الفيديو)، مما يجعل هذا النمط من الإجرام في تطور دائم يستعصي على الإحاطة الشاملة والنهائية²³.

المطلب الثاني: صور وأنواع جرائم العنف ضد الأشخاص المتصلة بالمعلوماتية

يتسع نطاق جرائم العنف ضد الأشخاص المتصلة بالمعلوماتية ليشمل صوراً متعددة ومتجددة، تبعاً لتطور الوسائل التقنية المستخدمة في ارتكابها، ويمكن تصنيف أبرز هذه الصور، دون حصر، إلى صنفين رئيسيين: جرائم التهديد والابتزاز الإلكتروني من جهة، وجرائم التشهير والتحرش والمطاردة الإلكترونية من جهة أخرى.

الفرع الأول: جرائم التهديد والابتزاز الإلكتروني

أولاً- جريمة التهديد الإلكتروني:

يُقصد بالتهديد الإلكتروني ذلك الفعل الذي يعمد من خلاله الجاني إلى إيصال رسالة تحمل وعيداً بإلحاق ضرر بالمجني عليه أو بأحد أقاربه، سواء تعلق هذا الضرر بالنفس أو المال أو العرض، وذلك باستخدام إحدى الوسائل المعلوماتية كالبريد الإلكتروني أو تطبيقات التواصل الاجتماعي أو الرسائل النصية أو تطبيقات المراسلة الفورية²⁴. ويشترط لقيام هذه الجريمة أن يكون التهديد جدياً من شأنه إحداث حالة من الخوف والرعب لدى شخص عادي في مثل ظروف المجني عليه، دون اشتراط تحقق الضرر المهدد به فعلاً، إذ تُعد جريمة التهديد في الغالب من الجرائم الشكلية التي تكتمل أركانها بمجرد وصول الرسالة التهديدية إلى علم المجني عليه²⁵.

وتتميز صورة التهديد الإلكتروني عن التهديد التقليدي بعدة أوجه: فمن جهة، تُتيح الوسيلة الإلكترونية للجاني إخفاء هويته بسهولة أكبر بكثير من التهديد الشفهي أو الكتابي التقليدي؛

²³ دراسات حول أثر تقنيات الذكاء الاصطناعي التوليدي على تطور أساليب ارتكاب جرائم العنف الرقمي.

²⁴ قياساً على النصوص العامة المتعلقة بجريمة التهديد في قانون العقوبات، مقارنة بصورتها الإلكترونية المستحدثة.

²⁵ اجتهاد فقهي مستقر بشأن شرط الجدية وطبيعة جريمة التهديد كجريمة شكلية؛ محمود نجيب حسني، شرح قانون العقوبات - القسم الخاص، دار النهضة العربية، القاهرة، [ص. ...].

ومن جهة أخرى، تُتيح هذه الوسيلة إمكانية تكرار الفعل وتوجيهه لعدد كبير من الأشخاص في آنٍ واحد، كما هو الحال في حملات التهديد الجماعي التي تستهدف صحفيين أو ناشطين أو شخصيات عامة عبر وسائل التواصل الاجتماعي؛ كما أن التهديد الإلكتروني قد يتخذ صوراً متعددة من حيث المحتوى، فقد يكون تهديداً صريحاً مباشراً، وقد يكون تهديداً ضمنياً يُستشف من سياق الرسائل أو من إرفاق صور أو رموز ذات دلالة تهديدية معينة²⁶.

ثانياً- جريمة الابتزاز الإلكتروني:

يُعد الابتزاز الإلكتروني من أخطر صور جرائم العنف ضد الأشخاص المتصلة بالمعلوماتية وأكثرها انتشاراً في الآونة الأخيرة، ويتحقق حين يستولي الجاني، بأي وسيلة كانت (كالاختراق أو الخداع أو الاستدراج)، على صور أو مقاطع فيديو أو محادثات أو معلومات شخصية حساسة تخص الضحية، ثم يُهددها بنشرها أو إفشائها للعموم أو لدائرة معارفها ما لم تستجب لمطالبه، سواء كانت هذه المطالب مالية أو جنسية أو غير ذلك من المطالب غير المشروعة²⁷.

ويأخذ الابتزاز الإلكتروني في الغالب صورتين رئيسيتين: **الصورة الأولى**، الابتزاز الجنسي (Sextortion)، الذي يستهدف بصفة خاصة النساء والقاصرين، ويقوم فيه الجاني باستدراج الضحية عبر انتحال هوية مزيفة أو التظاهر بعلاقة عاطفية، للحصول منها على صور أو مقاطع ذات طابع حميمي، ثم تهديدها بنشرها، وقد تتطور هذه الجريمة أحياناً إلى ما يُعرف بـ"سلسلة الابتزاز المستمر"، حيث لا يكتفي الجاني بمطلب واحد، بل يستمر في تصعيد مطالبه كلما استجابت الضحية له، مستغلاً حالة الضعف والخوف التي تعيشها²⁸.

والصورة الثانية، الابتزاز المالي، الذي يهدف إلى الحصول على مبالغ مالية أو منافع مادية مقابل عدم الإفصاح عن معلومات أو محتوى مسيء يخص الضحية، وقد يمتد ليشمل ابتزاز

²⁶ تقارير منظمات حرية الصحافة (كمراسلون بلا حدود) بشأن حملات التهديد الإلكتروني الجماعي الموجهة للصحفيين والناشطين.

²⁷ عبد الله سليمان سليمان، مرجع سابق، [ص. ...].

²⁸ تقارير المركز الوطني الأمريكي للأطفال المفقودين والمستغلين (NCMEC) حول ظاهرة Sextortion وسلسلة الابتزاز المستمر.

الشركات والمؤسسات بالتهديد بنشر بيانات سرية أو تعطيل أنظمتها المعلوماتية) وهو ما يُعرف بابتزاز الفدية الرقمية أو ²⁹ (Ransomware).

ومن الصور المستحدثة التي أفرزتها التطورات التقنية الأخيرة في مجال هذه الجريمة، ما يُعرف بـ"الابتزاز بالمحتوى المفيبرك" باستخدام تقنيات الذكاء الاصطناعي (Deepfake)، حيث يعتمد الجاني إلى تركيب وجه الضحية على مقاطع أو صور ذات طابع مخل، دون الحاجة إلى الحصول على أي محتوى حقيقي منها أصلاً، وهي صورة تكشف عن مدى خطورة التطور التقني وضرورة مواكبة النصوص القانونية لهذا التطور، إذ إن كثيراً من التشريعات القائمة لا تزال تشترط لقيام جريمة الابتزاز الجنسي إثبات أن المحتوى المهدد بنشره حقيقي وليس مفيبركاً، مما يخلق ثغرة قانونية خطيرة يستغلها الجناة في هذه الصورة المستحدثة³⁰.

كما تجدر الإشارة إلى صورة أخرى مستحدثة، وهي "الابتزاز بالوكالة" أو "الابتزاز الثانوي"، حيث لا يكتفي الجاني بابتزاز الضحية المباشرة، بل يمتد إلى تهديد أفراد أسرته أو معارفها بنشر المحتوى إن لم يتدخلوا لإقناع الضحية بالاستجابة لمطالبه، وهو ما يُضاعف من الضغط النفسي الممارس ويُوسع من دائرة المتضررين من الجريمة الواحدة³¹.

الفرع الثاني: جرائم التشهير والتحرش والمطاردة الإلكترونية

أولاً- جريمة التشهير والقذف الإلكتروني:

يتحقق التشهير الإلكتروني بنشر أقوال أو صور أو معلومات، صحيحة كانت أو كاذبة، من شأنها المساس بشرف واعتبار المجني عليه عبر الوسائل المعلوماتية، بقصد الإساءة إلى سمعته أمام الرأي العام أو دائرة معارفه³². ويرتبط بهذه الجريمة ما يُعرف بـ"القذف الإلكتروني"،

²⁹ عمر محمد أبو بكر بخيت، مرجع سابق، [ص. ...].

³⁰ تقارير حديثة حول استغلال تقنيات الذكاء الاصطناعي التوليدي (Deepfake) في الابتزاز، يُنظر تقارير اليوروبول (Europol) ذات الصلة.

³¹ دراسات ميدانية حول ظاهرة الابتزاز بالوكالة أو الابتزاز الثانوي عبر تهديد أفراد أسرة الضحية.

³² قياساً على أحكام جريمة القذف والسب التقليدية الواردة في قانون العقوبات، محمود نجيب حسني، مرجع سابق، [ص. ...].

والذي يتميز عن التشهير بضرورة أن يتضمن إسناد وقائع محددة كاذبة للمجني عليه من شأنها لو صحت أن تعرضه للعقاب أو الاحتقار، وذلك باستخدام إحدى الوسائل المعلوماتية³³.

وتزداد خطورة التشهير الإلكتروني بالنظر إلى خاصية الانتشار السريع والواسع سائلة الذكر، إذ قد يتحول منشور واحد إلى "حملة تشهير" جماعية في غضون ساعات، تتضافر فيها جهود عدد كبير من مستخدمي الشبكة، دون أن يكون لهم بالضرورة أي معرفة مسبقة بحقيقة الوقائع المنسوبة إلى الضحية، وهو ما يُعرف بظاهرة "المحاكمة الرقمية" أو "محاكم الرأي العام الافتراضية" التي قد تُلحق بالضحية ضرراً بالغاً حتى لو ثبتت براءته لاحقاً أمام القضاء، إذ إن "تبرئة" الضحية أمام القضاء نادراً ما تحظى بذات الانتشار والصدى الذي حظي به الاتهام الأولي³⁴. وتثير هذه الظاهرة كذلك إشكالية التوازن بين حرية التعبير المكفولة دستورياً وحقوق الأفراد في حماية سمعتهم وشرفهم، وهو توازن دقيق يستلزم من المشرع والقضاء على حد سواء معايير واضحة للتمييز بين النقد المشروع الذي يدخل في إطار حرية الرأي، والتشهير غير المشروع الذي يستهدف الإساءة المتعمدة³⁵.

ثانياً- جريمة التحرش الإلكتروني:

يشمل التحرش الإلكتروني كل سلوك ذي طابع جنسي أو مسيء يُمارس عبر الوسائل التقنية، كإرسال رسائل أو صور أو مقاطع ذات مضمون جنسي غير مرغوب فيه، أو التعليقات المسيئة المتكررة ذات الطابع الجنسي، أو المضايقات المستمرة عبر الرسائل الخاصة، والتي من شأنها المساس بكرامة المجني عليه وسلامته النفسية³⁶. وتستهدف هذه الجريمة بصفة خاصة النساء والفتيات، حيث تُشير العديد من الدراسات الميدانية إلى ارتفاع نسبة تعرضهن لهذا النمط من الاعتداء مقارنة بالرجال، وإلى أن هذا التحرش غالباً ما يمتد من الفضاء الرقمي

³³ نفس المرجع، [ص. ...].

³⁴ دراسات إعلامية وقانونية حول ظاهرة "محاكم الرأي العام الافتراضية". (Trial by Social Media) "

³⁵ دراسات حول التوازن بين حرية التعبير وحقوق حماية السمعة في الفضاء الرقمي.

³⁶ أنظر تعريفات التحرش الإلكتروني في الأدبيات الفقهية المقارنة؛ جميل عبد الباقي الصغير، مرجع سابق، [ص. ...].

إلى التأثير سلباً على مشاركتهن الفعلية في هذا الفضاء، بل قد يدفع بعضهن إلى الانسحاب الكلي منه تقادياً لهذا النمط من الإيذاء³⁷.

ثالثاً- جريمة المطاردة الإلكترونية: (Cyberstalking)

يتصل بالتحرش الإلكتروني ما يُعرف بالمطاردة الإلكترونية، والتي تتمثل في نمط سلوكي متكرر ومستمر يقوم على مراقبة الضحية ومتابعة تحركاتها وأنشطتها عبر الوسائل المعلوماتية بشكل غير مرغوب فيه، كمتابعة حساباتها على مواقع التواصل الاجتماعي بصفة لصيقة، أو محاولة التواصل معها بشكل متكرر رغم رفضها، أو تتبع موقعها الجغرافي عبر تطبيقات التتبع، مما يُشعرها بالخوف والقلق الدائمين، وقد يتطور الأمر أحياناً إلى مطاردة مادية فعلية في الواقع، مما يجعل من المطاردة الإلكترونية في كثير من الأحيان "مقدمة" أو "منذراً" لجرائم أشد خطورة قد تصل إلى العنف الجسدي المباشر³⁸.

رابعاً- صور مستحدثة أخرى:

وتمتد هذه الجرائم لتشمل أيضاً صوراً أخرى تستحق الإشارة، أهمها:

• **التنمر الإلكتروني: (Cyberbullying)** الذي يستهدف بصفة خاصة الأطفال والمراهقين عبر الإهانة والسخرية المتكررة داخل الفضاءات الرقمية، خاصة في الألعاب الإلكترونية الجماعية ومنصات التواصل الخاصة بالفئات العمرية الصغيرة، ويتميز عن التنمر التقليدي بأنه لا يتوقف عند حدود المدرسة أو المحيط المباشر، بل يلاحق الضحية إلى داخل بيتها عبر هاتفها الذكي، مما يحرمها من أي ملاذ آمن للهروب منه³⁹.

• **التحريض على الانتحار أو إيذاء النفس:** الذي يستغل فيه الجاني حالة الضعف

النفسى للضحية للدفع بها نحو إلحاق الأذى بنفسها، وقد ظهرت في هذا السياق ما

³⁷ تقارير هيئة الأمم المتحدة للمرأة (UN Women) بشأن تعرض النساء والفتيات للتحرش الرقمي وأثره على مشاركتهن الرقمية.

³⁸ مفهوم Cyberstalking كما تناولته الأدبيات الأنجلوسكسونية المتخصصة في الجريمة الرقمية.

³⁹ تقارير اليونيسف (UNICEF) ومنظمات حماية الطفولة بشأن ظاهرة التنمر الإلكتروني.

يُعرف بـ"تحديات الانتحار الرقمية" التي راح ضحيتها عدد من المراهقين حول العالم، والتي تقوم على استدراج القاصرين تدريجياً عبر سلسلة من التحديات المتصاعدة الخطورة تحت إشراف "مُحرّض" مجهول الهوية⁴⁰.

• **انتحال الشخصية الرقمية:** الذي يقوم فيه الجاني بإنشاء حساب مزيف باسم الضحية أو اختراق حسابها الحقيقي، بهدف الإساءة إلى سمعتها أو خداع الغير باسمها أو ابتزازها، وقد يمتد ليشمل انتحال الشخصية لأغراض الاحتيال المالي على أطراف ثالثة باسم الضحية، مما يلحق بها ضرراً مضاعفاً يجمع بين المساس بسمعتها والمساس المحتمل بذمتها المالية غير المباشرة⁴¹.

• نشر المحتوى الحميمي دون رضا (Non-Consensual Intimate Imagery):

(Imagery) وهي صورة قد تنفصل أحياناً عن الابتزاز، حين يقوم الجاني بنشر محتوى حميمي كان قد حصل عليه برضا الضحية في سياق علاقة سابقة (كعلاقة زوجية أو عاطفية منتهية)، دون أن يكون هناك بالضرورة مطلب مسبق أو ابتزاز، بل بدافع الانتقام أو الإساءة المجردة، وهي صورة تُعرف أحياناً بـ"إباحية الانتقام" (Revenge Porn)، وتستلزم معالجة تشريعية خاصة نظراً لاختلاف عناصرها عن جريمة الابتزاز التقليدية⁴².

• الإفصاح الخبيث عن المعلومات الشخصية: (Doxing) ويتمثل في قيام

الجاني بنشر معلومات شخصية حساسة عن الضحية (كعنوان سكنها أو مكان عملها أو أرقام هواتفها) دون رضاها، بهدف تعريضها لمضايقات أو تهديدات من أطراف

⁴⁰ نفس المصدر، وتقارير منظمة الصحة العالمية بشأن العلاقة بين التمر الرقمي ومحاولات الانتحار لدى المراهقين وظاهرة تحديات الانتحار الرقمية.

⁴¹ هدى حامد قشقوش، مرجع سابق، [ص. ...]، بشأن انتحال الشخصية الرقمية.

⁴² دراسات مقارنة حول ظاهرة "إباحية الانتقام" (Revenge Porn) وتمييزها عن جريمة الابتزاز.

أخرى، وهي صورة تجمع بين المساس بالحياة الخاصة والتحريض غير المباشر على إيذاء الضحية من قبل الغير⁴³.

المبحث الثاني: الأساس القانوني والتكليف الجزائي لهذه الجرائم

بعد الوقوف على ماهية جرائم العنف ضد الأشخاص المتصلة بالمعلوماتية وصورها، يقتضي الأمر الانتقال إلى بيان الأساس القانوني الذي استند إليه المشرع، وطنياً ودولياً، في تجريم هذه الأفعال (مطلب أول)، ثم تحليل التكليف القانوني لها وبيان أركانها (مطلب ثان).

المطلب الأول: الأساس القانوني لتجريم العنف المعلوماتي ضد الأشخاص

الفرع الأول: النصوص القانونية الوطنية

أولاً- منهج المشرع في مواجهة هذا النمط من الإجرام:

بادر المشرع، إدراكاً منه لخطورة هذا النمط الإجرامي المستحدث، إلى سنّ نصوص قانونية خاصة تتضمن تجريم الأفعال المتصلة بالمعلوماتية والماسة بسلامة الأشخاص، إلى جانب استعانتة ببعض النصوص التقليدية القائمة في قانون العقوبات وتطويعها لتشمل هذه الصور المستحدثة من الإجرام، عبر تقنية الإحالة أو التفسير الموسّع لبعض العناصر المكونة للجريمة (كوسيلة الارتكاب)⁴⁴. ويمكن رد هذا المنهج التشريعي إلى مقاربتين رئيسيتين اعتمدتهما التشريعات المقارنة: **المقاربة الأولى**، وتقوم على الاكتفاء بتعديل النصوص التقليدية القائمة في قانون العقوبات بإضافة الوسيلة الإلكترونية كوسيلة من وسائل ارتكاب الجريمة التقليدية (كإضافة عبارة "أو بأية وسيلة إلكترونية" إلى نص جريمة التهديد أو القذف)؛ **والمقاربة الثانية**، وتقوم على استحداث نصوص خاصة ومستقلة تماماً عن قانون العقوبات، ضمن

⁴³ دراسات حول ظاهرة الإفصاح الخبيث عن المعلومات الشخصية. (Doxing)

⁴⁴ قياساً على تقنية "الإحالة" التشريعية المعتمدة في العديد من التشريعات المقارنة عند تعديل نصوص قانون العقوبات لتشمل الوسائل الإلكترونية.

قانون خاص بمكافحة الجرائم المعلوماتية، تُفرد لكل صورة من صور العنف الرقمي نصاً خاصاً بها بأركان وعقوبات مستقلة⁴⁵.

ثانياً- النصوص الخاصة بتقنيات الإعلام والاتصال:

فمن جهة أولى، تناولت القوانين الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها جملة من الأحكام الموضوعية والإجرائية المتعلقة بمكافحة هذا النمط من الجريمة، سواء من حيث تجريم بعض الأفعال بصفة مستقلة (كالاعتداء على الأنظمة المعلوماتية)، أو من حيث تشديد العقوبة إذا ما ارتكبت الجريمة التقليدية بوسيلة معلوماتية، مع إحالة صريحة في بعض الأحيان إلى النصوص العامة الواردة في قانون العقوبات فيما يخص التهديد والقذف والسب والتحرش⁴⁶.

ثالثاً- النصوص التقليدية لقانون العقوبات وحدود كفايتها:

ومن جهة ثانية، لا تزال النصوص التقليدية لقانون العقوبات، المتعلقة بجرائم التهديد والقذف والسب وهتك العرض، تُشكل الأساس القانوني الذي يستند إليه القضاء في التعامل مع كثير من صور العنف الرقمي، عبر تفسير عبارة "أي وسيلة من وسائل النشر" أو ما شابهها تفسيراً موسعاً يشمل الوسائل الإلكترونية الحديثة⁴⁷. غير أن الاعتماد على هذا التفسير الموسع يظل حلاً مؤقتاً وغير مُرضٍ من الناحية النظرية، إذ يُخالف من حيث المبدأ قاعدة التفسير الضيق للنصوص الجزائية التي تقضي بعدم جواز القياس أو التوسع في تفسير النص الجزائي لغير مصلحة المتهم، وهو ما يجعل هذا الحل عرضة للنقد من زاوية مبدأ الشرعية الجزائية⁴⁸.

⁴⁵ دراسة مقارنة بين مقاربتي التعديل التشريعي والاستحداث المستقل في التشريعات محل المقارنة.

⁴⁶ أنظر القوانين الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها (وفق التشريع الوطني المعتمد في الدراسة).

⁴⁷ اجتهاد قضائي مستقر بشأن التفسير الموسع لعبارة "وسائل النشر" لتشمل الوسائل الإلكترونية الحديثة.

⁴⁸ ملاحظة نقدية حول تعارض التفسير الموسع مع مبدأ التفسير الضيق للنص الجزائي.

رابعاً - ملاحظات نقدية على واقع التشنت التشريعي:

غير أن هذا التدخل التشريعي، وإن كان يُشكل خطوة إيجابية لا يستهان بها، إلا أنه لا يزال يتسم بشيء من التشنت وعدم الانسجام، إذ توزعت النصوص ذات الصلة بين قانون العقوبات والقوانين الخاصة، دون وجود تقنين موحد وشامل لجرائم العنف الرقمي بالتحديد، الأمر الذي قد يُفضي أحياناً إلى تنازع النصوص أو إلى وجود ثغرات تشريعية تستغلها بعض الصور المستحدثة من الإجرام التي لم يتنبأ لها المشرع وقت وضع النص، كما هو الحال بالنسبة لجرائم الابتزاز بالمحتوى المفبرك بتقنية الذكاء الاصطناعي سألقة الذكر⁴⁹. ويستدعي ذلك تدخلاً تشريعياً لتجميع هذه النصوص وتحيينها بشكل دوري يواكب التطور المتسارع للتقنية.

خامساً - الاستئناس بالتجارب المقارنة:

وفي هذا السياق، تجدر الإشارة إلى أن بعض التشريعات المقارنة، كالتشريع الفرنسي والتشريع المصري والتشريع الإماراتي، قد اتجهت نحو استحداث نصوص خاصة ومستقلة لجرائم بعينها كالمطاردة الإلكترونية والابتزاز الجنسي، بدلاً من الاكتفاء بتطويع النصوص التقليدية، وهو توجه تشريعي جدير بالدراسة والاستئناس به عند التفكير في تطوير الترسانة القانونية الوطنية، خاصة فيما يتعلق بتحديد ظروف مشددة عند استهداف القاصرين أو عند استخدام تقنيات الذكاء الاصطناعي في ارتكاب الجريمة⁵⁰.

الفرع الثاني: الاتفاقيات والمواثيق الدولية

نظراً للطابع العابر للحدود الذي يميز جرائم العنف ضد الأشخاص المتصلة بالمعلوماتية، فإن مواجهتها الفعالة تستلزم بالضرورة إطاراً دولياً متكاملًا للتعاون والتنسيق بين الدول، وهو ما تجسد في عدد من الاتفاقيات والمواثيق الدولية والإقليمية.

⁴⁹ ملاحظة نقدية مستخلصة من التحليل المقارن للنصوص القائمة في مواجهة الصور المستحدثة للجريمة.

⁵⁰ دراسة مقارنة لموقف التشريعات الفرنسية والمصرية والإماراتية من جرائم المطاردة والابتزاز الجنسي الإلكتروني.

أولاً- اتفاقية بودابست لمكافحة الجريمة الإلكترونية:

تُعد اتفاقية بودابست، الصادرة عن مجلس أوروبا سنة 2001، أول اتفاقية دولية شاملة تتناول مكافحة الجريمة المعلوماتية بمفهومها الواسع، وقد تضمنت أحكاماً تتعلق بتجريم بعض الأفعال الماسة بالأشخاص عبر الوسائل المعلوماتية، إلى جانب أحكام إجرائية مهمة تتعلق بالتنقيش والضبط والاحتفاظ السريع بالبيانات المخزنة، وأحكام خاصة بالتعاون الدولي في جمع الأدلة الرقمية وتسليم المجرمين⁵¹. وقد انضمت إليها دول عديدة من خارج القارة الأوروبية، مما يعكس مكانتها كمرجعية دولية معيارية في هذا المجال، وإن كانت لا تخلو من انتقادات تتعلق بعدم مواكبتها الكافية لبعض الصور المستحدثة من الجرائم الماسة بالأشخاص كالتهرش والمطاردة الإلكترونية بشكل مفصل، باعتبارها اتفاقية وُضعت في مرحلة مبكرة من تطور الجريمة المعلوماتية لم تكن فيها هذه الصور قد بلغت ذروة انتشارها الحالية⁵².

ثانياً- مشروع الاتفاقية الأممية الشاملة:

وعلى المستوى الأممي، تجدر الإشارة إلى الجهود التي بذلتها الأمم المتحدة في السنوات الأخيرة، والتي توجت باعتماد الجمعية العامة للأمم المتحدة لاتفاقية دولية شاملة لمكافحة استخدام تكنولوجيا المعلومات والاتصالات في الأغراض الإجرامية، والتي تهدف إلى توفير إطار قانوني عالمي أكثر شمولية من اتفاقية بودابست، يضم عدداً أكبر من الدول الأعضاء، مع تخصيص أحكام تتعلق بحماية الفئات الهشة كالأطفال والنساء من الاستغلال والعنف الرقمي⁵³.

⁵¹ نص اتفاقية بودابست لمكافحة الجريمة الإلكترونية، مجلس أوروبا، 2001، المواد ذات الصلة.

⁵² تعليقات فقهية نقدية على اتفاقية بودابست بشأن مدى شمولها لصور العنف الرقمي المستحدثة.

⁵³ قرار الجمعية العامة للأمم المتحدة بشأن اعتماد الاتفاقية الدولية الشاملة لمكافحة استخدام تكنولوجيا المعلومات والاتصالات في الأغراض الإجرامية.

ثالثاً - الاتفاقيات الإقليمية:

إلى جانب ما سبق، برزت جهود إقليمية موازية، أهمها الاتفاقية العربية لمكافحة جرائم تقنية المعلومات الصادرة عن جامعة الدول العربية، والتي تضمنت هي الأخرى تجريم بعض صور الاعتداء على الأشخاص عبر الوسائل المعلوماتية، وحثت الدول الأعضاء على تطوير تشريعاتها الوطنية بما ينسجم مع أحكامها⁵⁴، فضلاً عن الاتفاقية الأفريقية بشأن الأمن السيبراني وحماية البيانات الشخصية (المعروفة باتفاقية مالابو)، والتي تناولت جوانب مشابهة على المستوى القاري الأفريقي، وإن كانت لا تزال تعاني من محدودية عدد الدول المصادقة عليها مقارنة بعدد الدول الموقعة، مما يحد من فعاليتها العملية حتى الآن⁵⁵.

رابعاً - القيمة المضافة لهذا الإطار الدولي:

وتكتسي هذه الاتفاقيات، على تفاوت درجة إلزاميتها وشمولها، أهمية بالغة كونها تُشكل إطاراً مرجعياً للتشريعات الوطنية، وتُسهّم في تقريب المفاهيم وتوحيد المصطلحات القانونية، وتُيسّر سبل التعاون القضائي الدولي، بما يُعزز من فعالية مواجهة الطابع العابر للحدود الذي يميز هذا النمط من الإجرام، على النحو الذي سنفصّل فيه عند دراسة الجوانب الإجرائية في الفصل الثاني من هذه الدراسة.

المطلب الثاني: التكيف القانوني وأركان الجريمة

الفرع الأول: الركن المادي

يتحقق الركن المادي في جرائم العنف ضد الأشخاص المتصلة بالمعلوماتية، شأنها في ذلك شأن سائر الجرائم، بتوافر ثلاثة عناصر أساسية: السلوك الإجرامي، والنتيجة الإجرامية، وعلاقة السببية الرابطة بينهما⁵⁶.

⁵⁴ نص الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، جامعة الدول العربية، المواد ذات الصلة.

⁵⁵ نص الاتفاقية الأفريقية بشأن الأمن السيبراني وحماية البيانات الشخصية (اتفاقية مالابو)، الاتحاد الأفريقي.

⁵⁶ محمود نجيب حسني، شرح قانون العقوبات - القسم العام، دار النهضة العربية، القاهرة، [ص. ...] (نظرية أركان الجريمة).

أولاً- السلوك الإجرامي:

يتمثل السلوك الإجرامي في الفعل المرتكب عبر الوسيلة المعلوماتية، سواء تمثل في إرسال رسالة تهديد، أو نشر محتوى مسيء، أو إرسال صور أو مقاطع بقصد الابتزاز، أو أي فعل آخر من الأفعال سالفة الذكر⁵⁷. ويشترط في هذا السلوك أن يتم بواسطة إحدى الوسائل المعلوماتية أو التقنية (كشبكة الإنترنت أو الهاتف الذكي أو أي جهاز إلكتروني آخر)، وهو ما يميز هذه الجريمة عن نظيرتها التقليدية التي قد تتحقق بأي وسيلة أخرى كالشفافة أو الكتابة اليدوية. ويثير هذا الشرط إشكالية تتعلق بمدى اعتبار الوسيلة عنصراً في التكيف القانوني ذاته أم مجرد ظرف مشدد للعقوبة، وهي مسألة تتباين الحلول التشريعية بشأنها⁵⁸.

ويلاحظ أن السلوك الإجرامي في هذا النمط من الجرائم قد يتخذ صورة الفعل الإيجابي في الغالب الأعم (كإرسال أو نشر أو تهديد)، لكنه قد يتخذ استثناءً صورة الامتناع، كما في حالة عدم الاستجابة لأمر قضائي بإزالة محتوى مسيء صادر ضد ناشره الأصلي أو ضد من يحوز صلاحية إزالته⁵⁹.

ثانياً- النتيجة الإجرامية:

تتمثل النتيجة الإجرامية في الضرر الذي يلحق بالمجني عليه، سواء كان ضرراً نفسياً كحالة الخوف والقلق والاضطراب، أو ضرراً معنوياً كالمساس بالشرف والاعتبار، أو ضرراً مادياً في حال الابتزاز المالي⁶⁰. ويلاحظ أن بعض صور هذه الجرائم تُعد من الجرائم الشكلية (أو جرائم الخطر) التي تكتمل أركانها بمجرد إتيان السلوك الإجرامي دون اشتراط تحقق نتيجة معينة بالمعنى المادي الدقيق، كجريمة التهديد التي تقوم بمجرد إيصال الرسالة التهديدية بصرف النظر عن مدى تحقق الخوف الفعلي لدى المجني عليه، في حين تُعد صور أخرى

⁵⁷ نفس المرجع، [ص. ...]، بشأن السلوك الإجرامي في الجرائم المستحدثة.

⁵⁸ دراسة مقارنة حول موقع "الوسيلة المعلوماتية" من التكيف القانوني: عنصر تأسيسي أم ظرف مشدد.

⁵⁹ دراسة حول صورة الامتناع في السلوك الإجرامي المتعلق بجرائم العنف الرقمي.

⁶⁰ محمود نجيب حسني، مرجع سابق، [ص. ...]، بشأن النتيجة الإجرامية.

من الجرائم المادية التي تستلزم تحقق ضرر فعلي، كجريمة الابتزاز التي تستلزم تحقق الرضوخ الفعلي أو الشروع فيه⁶¹.

ثالثاً - علاقة السببية:

يُشترط أخيراً توافر علاقة سببية مباشرة بين السلوك الإجرامي والنتيجة المتحققة، بحيث تكون هذه الأخيرة أثراً مباشراً لذلك السلوك، وتثور في هذا الصدد إشكاليات عملية تتعلق بتعدد الأسباب المتداخلة، خاصة في حالات التشهير الجماعي التي يُساهم فيها عدد كبير من الأشخاص عبر إعادة النشر، إذ يصعب أحياناً عزل الأثر الذي أحدثه كل مساهم على حدة⁶².

رابعاً - إشكالية تحديد مكان ارتكاب الجريمة:

وتثير هذه الجرائم، بالنظر إلى طابعها اللامادي والعابر للحدود سالف الذكر، إشكالية خاصة تتعلق بتحديد مكان ارتكاب الجريمة، والذي يُعتد به لتحديد الاختصاص القضائي، إذ قد يتوزع مكان الفعل (مكان تواجد الجاني)، ومكان النتيجة (مكان تواجد الضحية)، ومكان تخزين البيانات (مكان الخادم) على عدة دول مختلفة، مما يستدعي إعمال نظرية "معيّار مكان تحقق أي عنصر من عناصر الجريمة" التي تبنتها أغلب التشريعات المقارنة لتوسيع نطاق اختصاصها القضائي في مواجهة هذا النمط من الإجرام العابر للحدود⁶³.

خامساً - إشكالية الجريمة المستمرة والجريمة الوقتية:

ومما يزيد من تعقيد الركن المادي في هذا النمط من الجرائم، التساؤل حول طبيعتها الزمنية، فهل تُعد جريمة وقتية تنتهي بمجرد النشر الأول للمحتوى المسيء، أم جريمة مستمرة تتجدد آثارها بتجدد إتاحة المحتوى للاطلاع عليه؟ وتترتب على هذا التساؤل نتائج عملية بالغة الأهمية، تتعلق بتاريخ سريان التقادم، وبتحديد الاختصاص القضائي، وقد ذهب اتجاه فقهي

⁶¹ التمييز الفقهي التقليدي بين الجرائم الشكلية (جرائم الخطر) والجرائم المادية (جرائم الضرر)؛ نفس المرجع، [ص. ...].

⁶² عبد الله سليمان سليمان، مرجع سابق، [ص. ...]، بشأن إشكالية تعدد الأسباب في جرائم التشهير الجماعي.

⁶³ جميل عبد الباقي الصغير، مرجع سابق، [ص. ...]، بشأن معايير تحديد الاختصاص القضائي في الجرائم عبر الوطنية.

راجع إلى اعتبار هذه الجرائم في حكم الجرائم المستمرة ما دام المحتوى المسيء متاحاً للاطلاع عليه على الشبكة، إذ إن الضرر يتجدد كل مرة يطلع فيها شخص جديد على هذا المحتوى⁶⁴.

الفرع الثاني: الركن المعنوي

تُعد جرائم العنف ضد الأشخاص المتصلة بالمعلوماتية، في غالب صورها، من الجرائم العمدية التي تستلزم توافر القصد الجنائي لدى الجاني، والذي يتخذ صورة القصد العام المتمثل في علم الجاني بعناصر الجريمة كافة، واتجاه إرادته إلى ارتكاب السلوك الإجرامي وتحقيق نتيجته، فلا مجال لتصور هذه الجرائم في صورتها غير العمدية، إذ إن الخطأ غير العمدي لا يكفي لقيامها⁶⁵.

أولاً- القصد العام:

يستلزم القصد العام في هذه الجرائم علم الجاني بأن الفعل الذي يقوم به (كإرسال رسالة تهديد أو نشر محتوى مسيء) من شأنه إحداث ضرر بالمجني عليه، واتجاه إرادته الحرة والواعية إلى إتيان هذا الفعل رغم علمه بذلك⁶⁶.

ثانياً- القصد الخاص:

وقد تستلزم بعض صور هذه الجرائم توافر قصد جنائي خاص، إلى جانب القصد العام، كما هو الحال في جريمة الابتزاز التي تستوجب توافر نية الحصول على منفعة أو مقابل معين، سواء كان مالياً أو جنسياً، مقابل الامتناع عن نشر أو إفشاء المحتوى المسيء، فلا تقوم هذه الجريمة بمجرد التهديد بالنشر دون توافر هذه النية الخاصة⁶⁷. كذلك الحال في جريمة القذف التي تستلزم توافر نية الإساءة إلى سمعة المجني عليه تحديداً، وهي نية يفترضها القضاء عادة من مجرد ثبوت الإسناد ما لم يقيم المتهم بإثبات انتفاءها.

⁶⁴ دراسة فقهية حول تكييف جرائم العنف الرقمي بين الجريمة الوقتية والجريمة المستمرة وأثره على التقادم والاختصاص.

⁶⁵ محمود نجيب حسني، مرجع سابق، [ص. ...]، بشأن نظرية القصد الجنائي العام.

⁶⁶ نفس المرجع، [ص. ...].

⁶⁷ نفس المرجع، [ص. ...]، بشأن القصد الخاص في بعض الجرائم كالابتزاز والقذف.

ثالثاً - إشكالية إثبات الركن المعنوي:

ويثير إثبات الركن المعنوي في هذه الجرائم صعوبة عملية بالغة، نظراً لطبيعتها الافتراضية وسهولة إنكار الجاني لنيته الحقيقية، مما يستوجب استعانة القضاء بالقرائن المستخلصة من ظروف الواقعة ووسائل ارتكابها وسلوك الجاني اللاحق للفعل لاستجلاء نيته الحقيقية، كتكرار إرسال الرسائل رغم رفض المجني عليه، أو اقتران التهديد بمطلب واضح ومحدد، أو استخدام أساليب تقنية للتخفي تدل على سبق الإصرار والتدبير⁶⁸.

رابعاً - مسألة الباعث ودوره في هذه الجرائم:

وتجدر الإشارة أخيراً إلى أن الباعث على ارتكاب الجريمة (كالانتقام أو الغيرة أو الرغبة في الشهرة) لا يُعتد به من حيث المبدأ في تحديد قيام الركن المعنوي، إذ يكفي توافر القصد الجنائي بصرف النظر عن الدافع الذي حرك إرادة الجاني، غير أن هذا الباعث قد يكون له أثر عملي في تقدير العقوبة أو في الكشف عن هوية الجاني أثناء التحقيق، خاصة في جرائم التشهير والابتزاز التي غالباً ما ترتبط بعلاقة سابقة بين الجاني والضحية⁶⁹. وهو ما ينقلنا إلى ضرورة معالجة الجوانب الإجرائية الخاصة بالتحقيق والإثبات في هذا النمط من الجرائم، والتي سنتناولها بالتفصيل في الفصل الثاني من هذه الدراسة.

⁶⁸ اجتهاد قضائي مستقر بشأن الاستدلال بالقرائن على توافر الركن المعنوي في الجرائم الافتراضية.

⁶⁹ محمود نجيب حسني، مرجع سابق، [ص. ...]، بشأن دور الباعث في المسؤولية الجزائية وتمييزه عن القصد الجنائي.

خلاصة الفصل الأول:

يتبين مما سبق أن جرائم العنف ضد الأشخاص المتصلة بالمعلوماتية تُشكل نمطاً إجرامياً مستحدثاً ومتجدد الصور، يتميز بخصائص فنية وتقنية تجعله يفلت أحياناً من قبضة النصوص القانونية التقليدية، وأن المشرّع، رغم تدخله التشريعي الملموس على المستويين الوطني والدولي، لا يزال مطالباً بمزيد من الجهد لمواكبة هذا التطور المتسارع، سواء من حيث استحداث نصوص خاصة لصور مستجدة لم تكن متوقعة وقت وضع النصوص القائمة، أو من حيث توضيح أركان هذه الجرائم بما يُيسّر مهمة القضاء في تكييفها والفصل فيها. وعلى ضوء هذا الإطار المفاهيمي والقانوني، ننتقل في الفصل الثاني إلى دراسة الجوانب الإجرائية والوقائية لمواجهة هذا النمط من الإجرام.

الفصل الثاني

بعد أن تناولنا في الفصل الأول الإطار المفاهيمي والقانوني لجرائم العنف ضد الأشخاص المتصلة بالمعلوماتية، بتحديد ماهيتها وصورها وأركانها الموضوعية، يقتضي منهج البحث العلمي الانتقال إلى الشق التطبيقي من هذه الدراسة، ذلك أن التجريم وحده - مهما بلغت دقته الفنية والقانونية - يبقى عديم الجدوى العملية ما لم تواكبه منظومة إجرائية فعالة تُمكن من كشف الجريمة وإثباتها وملاحقة مرتكبها، وآليات حمائية ووقائية تحول دون تجدد الاعتداء أو تُخفف من آثاره الجسيمة على الضحية. فالنص القانوني الموضوعي، مهما كان محكماً، يظل حبراً على ورق إذا لم تتوفر الوسائل العملية لتفعيله، وهو ما يُبرز أهمية دراسة الشق الإجرائي والوقائي بذات القدر من العناية التي أوليت للشق الموضوعي في الفصل السابق. ولهذا الغرض، نتناول في هذا الفصل، من خلال مبحثين، الإجراءات الجزائية الخاصة بمكافحة هذه الجرائم في مبحث أول، ثم الحماية القانونية للضحايا وسبل الوقاية في مبحث ثانٍ.

المبحث الأول: الإجراءات الجزائية الخاصة بمكافحة هذه الجرائم

تقرض الخصائص المميزة لجرائم العنف ضد الأشخاص المتصلة بالمعلوماتية، والتي وقفنا عليها بالتفصيل في الفصل الأول (اللامادية والافتراضية، والطابع العابر للحدود، وسهولة الإخفاء وصعوبة الإثبات، وسرعة الانتشار)، ضرورة إعادة النظر في الإجراءات الجزائية التقليدية بما يتلاءم مع طبيعة هذا النمط المستحدث من الإجرام، إذ إن تطبيق القواعد الإجرائية الكلاسيكية دون تكيف يجعلها في الغالب عاجزة عن مواكبة سرعة وتعقيد هذا النمط الإجرامي. ونتناول في هذا المبحث خصوصية التحقيق والإثبات في هذه الجرائم (مطلب أول)، ثم الجهات المختصة بالتحقيق والملاحقة (مطلب ثان).

المطلب الأول: خصوصية التحقيق والإثبات في الجرائم المعلوماتية

الفرع الأول: أساليب جمع الأدلة الرقمية

أولاً- ماهية الدليل الرقمي وخصائصه الفنية:

يُقصد بالدليل الرقمي (Digital Evidence) كل بيانات أو معلومات مخزنة أو منقولة أو معالجة بواسطة نظام معلوماتي، سواء كانت في صورة نصوص أو صور أو مقاطع صوتية أو مرئية أو بيانات تعريفية (Metadata)، ويمكن الاستعانة بها لإثبات وقوع الجريمة ونسبتها إلى مرتكبها¹. ويتميز الدليل الرقمي عن الدليل التقليدي بجملة من الخصائص الجوهرية التي تنعكس مباشرة على طريقة التعامل معه إجرائياً، أهمها: قابليته الفائقة للتعديل والمحو والتزييف دون ترك أثر ظاهر للعين المجردة، وهشاشته وقابليته للتلف أو الضياع بسهولة بمجرد إغلاق الجهاز أو انقطاع التيار الكهربائي أو مرور فترة زمنية قصيرة، وطابعه اللامادي الذي يستلزم تحويله إلى صورة مادية (كطبع أو تسجيل) لتقديمه أمام القضاء، وحاجته الماسة إلى خبرة تقنية متخصصة لاستخلاصه وتحليله وتفسيره بشكل سليم².

¹ عبد الله سليمان سليمان، أثر الأنظمة المعلوماتية في قواعد الإثبات الجنائي، دار النهضة العربية، القاهرة، ص 67

² نفس المرجع، ص 71

ويضاف إلى ما سبق خاصية أخرى بالغة الأهمية، وهي قابلية الدليل الرقمي للتضاعف والنسخ دون فقدان الأصل لقيمته أو محتواه، خلافاً للدليل المادي التقليدي الذي يتفرد بأصله، وهو ما يثير من جهة أخرى إشكالية التمييز بين النسخة الأصلية والنسخة المستنسخة عند تقديم الدليل أمام القضاء، وضرورة التحقق التقني من مطابقة النسخة المقدمة للأصل عبر تقنيات التوقيع الرقمي أو دالة "التجزئة" (Hash Function) التي تضمن سلامة المحتوى وعدم التلاعب فيه³. ويُضاف إلى ذلك خاصية "تشتت الدليل" (Data Fragmentation)، إذ إن الدليل المتعلق بجريمة رقمية واحدة قد يتوزع فعلياً بين عدة مواقع تقنية مختلفة: جهاز الجاني، جهاز الضحية، خوادم مزود الخدمة، خوادم المنصة الرقمية المستضيفة، مما يستلزم تنسيقاً إجرائياً وتقنياً معقداً لجمع هذا الدليل من مصادره المتعددة⁴.

ثانياً - أساليب جمع الدليل الرقمي:

تتعدد الأساليب التقنية والإجرائية المعتمدة في جمع الأدلة الرقمية المتعلقة بجرائم العنف ضد الأشخاص، ويمكن إجمال أبرزها فيما يلي:

1- التوثيق الفوري للمحتوى الرقمي: ويتم من خلال أخذ لقطات شاشة (Screenshots) أو تسجيلات فيديو للمحتوى المسيء (رسائل التهديد، منشورات التشهير، محادثات الابتزاز) فور اكتشافه، نظراً لسهولة حذفه أو تعديله من قبل الجاني بمجرد شعوره بأنه مكتشف أو مهدد بالملاحقة، مع ضرورة توثيق التاريخ والوقت والربط الإلكتروني الدقيق للمحتوى (URL)، وكذا اسم الحساب أو المعرف الرقمي المستخدم من قبل الجاني، إذ يُنصح الضحية عملياً بعدم الاكتفاء بلقطة شاشة واحدة، بل تصوير كامل سياق المحادثة أو المنشور بما يشمل تاريخ النشر وعدد المشاهدات أو التفاعلات إن أمكن، تعزيزاً لقوة الدليل الثبوتية لاحقاً⁵.

³ دراسات تقنية حول دالة التجزئة الرقمية (Hash Function) وضمان سلامة الدليل الرقمي.

⁴ دراسات حديثة حول ظاهرة تشتت الدليل الرقمي (Data Fragmentation) بين مصادر تقنية متعددة.

⁵ دراسات عملية حول أساليب التوثيق الفوري للمحتوى الرقمي في قضايا العنف الإلكتروني.

2- الحجز والتفتيش الرقمي: ويتمثل في حجز الأجهزة الإلكترونية (الحاسوب، الهاتف الذكي، الأقراص الصلبة الخارجية) وتفتيشها تقنياً لاستخراج البيانات ذات الصلة بالجريمة، وهو إجراء يستلزم ضوابط إجرائية دقيقة تراعي حرمة الحياة الخاصة المكفولة دستورياً، وغالباً ما يستلزم إذناً قضائياً مسبقاً ومسبباً يحدد نطاق التفتيش زمنياً ومكانياً وموضوعياً، إلا في حالات التلبس أو الاستعجال القصوى التي تبرر التدخل الفوري دون إذن مسبق، مع خضوع هذا الاستثناء لرقابة قضائية لاحقة صارمة تحول دون التعسف في استخدامه⁶. ويثير التفتيش الرقمي إشكالية خاصة تتعلق باتساع نطاقه المحتمل، إذ إن تفتيش هاتف ذكي واحد قد يكشف عن كم هائل من المعلومات الشخصية للمشتبه فيه لا علاقة لها بالجريمة محل التحقيق، مما يستدعي التزام المحققين بمبدأ التناسب وقصر البحث على البيانات ذات الصلة الفعلية بالواقعة محل التحقيق⁷.

3- الاحتفاظ السريع بالبيانات المخزنة (Data Preservation): وهو إجراء مستحدث تبنته أغلب التشريعات المقارنة والاتفاقيات الدولية، يقوم على إلزام مزودي خدمة الإنترنت والمنصات الرقمية بالاحتفاظ بالبيانات المتعلقة بالجريمة (كبيانات الاتصال وعناوين البروتوكول وسجلات تسجيل الدخول) لمدة معينة، ريثما يتم استصدار الإذن القضائي اللازم للحصول عليها رسمياً، وذلك تقادياً لضياعتها نظراً لسرعة تحديثها أو حذفها التلقائي وفق سياسات كل مزود خدمة، والتي قد لا تتجاوز أحياناً بضعة أيام أو أسابيع فقط⁸.

4- تتبع عنوان بروتوكول الإنترنت (IP Address) والبيانات الوصفية: ويُعد من أهم الوسائل التقنية للوصول إلى الهوية الحقيقية للجاني ومكان تواجده الجغرافي التقريبي، رغم ما يكتنف هذه العملية من صعوبات عملية جمة، خاصة في ظل استخدام تقنيات إخفاء الهوية سائلة الذكر في الفصل الأول (كالشبكات الافتراضية الخاصة VPN وشبكة تور TOR)،

⁶ جميل عبد الباقي الصغير، *الجرائم الناشئة عن استخدام الحاسب الآلي*، دار النهضة العربية، القاهرة، [ص. ...]، بشأن ضوابط التفتيش والحجز الرقمي. ص 109

⁷ دراسة نقدية حول ضرورة إعمال مبدأ التناسب في نطاق التفتيش الرقمي.

⁸ نص اتفاقية بودابست لمكافحة الجريمة الإلكترونية، مجلس أوروبا، 2001، المواد المتعلقة بالاحتفاظ السريع بالبيانات المخزنة.

والتي تجعل من عنوان البروتوكول المكتشف عنواناً وسيطاً لا يقود مباشرة إلى الجاني الحقيقي، مما يستلزم تعاوناً تقنياً وقضائياً دولياً معقداً لتجاوز هذه العقبة⁹.

5- الاستعانة بالخبرة التقنية المتخصصة (الطب الشرعي الرقمي - Digital Forensics):

حيث لا يمكن الاستغناء عن الخبراء التقنيين المتخصصين في استخلاص وتحليل الأدلة الرقمية، بما يضمن سلامة الإجراءات التقنية المتبعة وحفظ ما يُعرف بـ"سلسلة العهدة" (Chain of Custody) للدليل، أي التوثيق الدقيق لكل يد تداولت الدليل منذ لحظة ضبطه وحتى تقديمه أمام القضاء، بما يحول دون الطعن في مشروعيته أو سلامته أو التشكيك في عدم تلاعب أحد به خلال هذه السلسلة¹⁰.

6- الاستعانة بالمصادر المفتوحة (OSINT - Open Source Intelligence):

وهي تقنية مستحدثة تقوم على جمع المعلومات المتاحة للعموم عبر مصادر مفتوحة (كالحسابات العامة على مواقع التواصل الاجتماعي، ومحركات البحث، وقواعد البيانات المفتوحة) للمساعدة في تحديد هوية الجاني أو تتبع نشاطه، وقد أصبحت هذه التقنية تلعب دوراً متنامياً الأهمية في التحقيقات الجنائية المتعلقة بالجرائم الرقمية، خاصة حين يفشل التتبع التقني المباشر¹¹.

7- تحليل الأنماط السلوكية الرقمية (Behavioral Digital Profiling): وهي

تقنية حديثة نسبياً تقوم على تحليل أسلوب كتابة الجاني، وتوقيت نشاطه، وأنماط استخدامه للتطبيقات، بهدف المقارنة بينها وبين حسابات أخرى يُشتبه أنها تعود لنفس الشخص، خاصة في حالات إنشاء حسابات وهمية متعددة، وقد أثبتت هذه التقنية جدواها في بعض القضايا رغم أنها لا تزال تحتاج إلى مزيد من التقنين الإجرائي لضمان موثوقيتها القضائية¹².

⁹ عمر محمد أبو بكر بخيت، الجرائم المعلوماتية عبر الإنترنت، دار الجامعة الجديدة، الإسكندرية، ص 350، 370-371

¹⁰ هدى حامد قشقوش، جرائم الحاسب الآلي في التشريع المقارن، دار النهضة العربية، القاهرة، [ص. ...]، بشأن أهمية الخبرة التقنية وسلسلة

العهدة. ص 6

¹¹ دراسات حديثة حول توظيف تقنيات الاستخبارات مفتوحة المصدر (OSINT) في التحقيقات الجنائية الرقمية.

¹² دراسات تقنية حول تحليل الأنماط السلوكية الرقمية (Behavioral Digital Profiling) وحدود موثوقيتها القضائية.

الفرع الثاني: صعوبات الإثبات وحجية الدليل الرقمي

أولاً- صعوبات الإثبات العملية:

يواجه إثبات جرائم العنف ضد الأشخاص المتصلة بالمعلوماتية جملة من الصعوبات العملية الجسيمة، يمكن إجمال أبرزها فيما يلي:

1- صعوبة تحديد الهوية الحقيقية للجاني: في ظل استخدام أسماء مستعارة وحسابات

وهمية وتقنيات التخفي التقني سائلة الذكر، وهو ما يجعل نسبة كبيرة من هذه الجرائم تبقى دون كشف هوية مرتكبها الحقيقي رغم توفر أدلة مادية على وقوع الفعل ذاته¹³.

2- صعوبة التعاون مع الجهات الأجنبية: حيث يستلزم الحصول على بيانات من

مزودي الخدمة والمنصات الرقمية الأجنبية (التي غالباً ما يكون مقرها الاجتماعي خارج الإقليم الوطني) اتباع مساطر قانونية دولية معقدة وطويلة، لا تتناسب في الغالب مع خاصية سرعة زوال الدليل الرقمي، مما قد يُفضي إلى ضياع الدليل قبل استكمال هذه المساطر¹⁴.

3- ظاهرة الرقم الأسود للجريمة (Chiffre Noir): إذ يتردد عدد كبير من الضحايا

في التبليغ عن هذه الجرائم، إما خشية الوصمة الاجتماعية خاصة في جرائم الابتزاز الجنسي، أو خوفاً من ردة فعل الجاني وتنفيذ تهديداته، أو لعدم ثقتهم في جدوى الإجراءات القضائية وقدرتها على حمايتهم فعلياً، أو لجهلهم بالأساس بوجود إطار قانوني يُجرّم هذه الأفعال أصلاً، مما يجعل الأرقام الرسمية المسجلة لدى الجهات القضائية والأمنية لا تعكس الحجم الحقيقي لهذه الظاهرة¹⁵.

4- التحديات المرتبطة بعبء الإثبات: حيث يقع عبء إثبات الجريمة، وفق القواعد

العامة، على عاتق النيابة العامة أو الضحية بحسب طبيعة النظام الإجرائي المعتمد، وهو عبء ثقيل بالنظر إلى الطابع التقني المعقد للدليل الرقمي، مما يستدعي أحياناً التفكير في

¹³ عبد الله سليمان سليمان، مرجع سابق، ص 98

¹⁴ نفس المرجع، 101

¹⁵ دراسات إجرامية حول ظاهرة الرقم الأسود للجريمة وتردد الضحايا في التبليغ عن جرائم العنف الرقمي.

تخفيف هذا العبء أو تقريب وسائل الإثبات لصالح الضحية في بعض الحالات الخاصة، كما هو معمول به في بعض التشريعات المقارنة بشأن جرائم العنف القائم على النوع الاجتماعي¹⁶.

5- تعطل الإجراء بفعل تعديل المنصات لسياساتها: إذ تخضع سياسات الاحتفاظ بالبيانات لدى مزودي الخدمة لتغيرات متكررة وفق اعتبارات تجارية أو قانونية داخلية خاصة بكل شركة، مما يجعل من الصعب التنبؤ سلفاً بمدى توفر بيانات معينة وقت تقديم طلب الحصول عليها، وهو ما يفرض على الجهات القضائية والأمنية متابعة مستمرة لتطور هذه السياسات¹⁷.

ثانياً- حجية الدليل الرقمي أمام القضاء :

أثارت مسألة حجية الدليل الرقمي جدلاً فقهيًا واسعاً، إذ تباينت المواقف بين اتجاه يرى ضرورة إخضاع الدليل الرقمي للقواعد التقليدية للإثبات الجنائي القائمة على مبدأ الإقناع الشخصي للقاضي وحرية في تكوين قناعته من أي دليل يُطرح أمامه، واتجاه آخر يرى ضرورة وضع ضوابط خاصة ومشددة للدليل الرقمي نظراً لسهولة تزويره وقابليته للتلاعب بشكل قد لا يتفطن له القاضي غير المتخصص تقنياً، بما يستلزم إخضاعه لخبرة تقنية إلزامية قبل الاعتداد به¹⁸.

وقد استقر الاتجاه الراجح فقهاً وقضاءً على الأخذ بمبدأ حرية الإثبات في المواد الجزائية، مع إخضاع الدليل الرقمي لضوابط إجرائية موضوعية تحقق منه سلامته وموثوقيته، أبرزها: التحقق من سلامة سلسلة العهدة منذ لحظة جمع الدليل وحتى تقديمه للقضاء، وضمان عدم المساس بمحتواه أو التلاعب فيه عبر الوسائل التقنية المتاحة (كمقارنة بصمة التجزئة الرقمية)،

¹⁶ دراسات مقارنة حول تخفيف عبء الإثبات في جرائم العنف القائم على النوع الاجتماعي.

¹⁷ ملاحظات عملية حول تقلب سياسات الاحتفاظ بالبيانات لدى مزودي الخدمة.

¹⁸ محمود نجيب حسني، شرح قانون العقوبات - القسم العام، دار النهضة العربية، القاهرة، ص 91-93، بشأن مبدأ حرية الإثبات الجزائي.

والاستعانة بالخبرة التقنية اللازمة لتفسيره وترجمته إلى لغة قانونية مفهومة للقاضي، بما يُمكنه من تكوين قناعته الجزائية على أساس سليم وموثوق علمياً وتقنياً¹⁹.

ويبقى مع ذلك مبدأ الإثبات الحر مقيداً بضرورة مشروعية طرق الحصول على الدليل، إذ لا يجوز الاستناد إلى دليل رقمي تم الحصول عليه بطرق غير مشروعة كاللتنصت غير المرخص أو الاختراق غير القانوني لحساب الجاني أو جهازه، ولو كان صحيحاً وصادقاً في مضمونه، إعمالاً لنظرية "بطلان الدليل المتحصل من إجراء باطل"، والتي تهدف إلى الموازنة بين مقتضيات كشف الحقيقة ومقتضيات احترام الضمانات الدستورية والحقوقية للأفراد، بما فيهم المتهم ذاته²⁰. وتثير هذه القاعدة إشكالية دقيقة حين يكون الدليل قد حصلت عليه الضحية ذاتها بطرق قد تُعد غير مشروعة (كاختراق حساب الجاني للحصول على دليل إدانته)، وهي مسألة لا تزال محل تباين فقهي وقضائي بين من يرى بطلان هذا الدليل مطلقاً أسوة بالدليل المتحصل من السلطة العامة، ومن يرى التمييز بين حالة السلطة العامة وحالة الأفراد العاديين الذين لا تربطهم بالقواعد الإجرائية ذات العلاقة إلا رابطة غير مباشرة²¹.

ثالثاً - إشكالية القوة الثبوتية النسبية للدليل الرقمي:

وتجدر الإشارة أخيراً إلى أن الدليل الرقمي، رغم الاعتراف بحجته من حيث المبدأ، لا يتمتع بذات القوة الثبوتية المطلقة التي قد يتمتع بها في بعض الأحيان الدليل المادي التقليدي (كالبصمة أو الحمض النووي)، نظراً لإمكانية الطعن فيه من زوايا متعددة (كالتشكيك في هوية صاحب الحساب، أو في سلامة عملية النقل والتخزين)، مما يستدعي من القضاء دوماً مقارنة الدليل الرقمي في إطار منظومة أدلة متكاملة ومتساندة، لا الاعتماد عليه بمفرده كدليل وحيد للإدانة، خاصة في الجرائم ذات العقوبات الجسيمة²².

¹⁹ عبد الله سليمان سليمان، مرجع سابق، ص 107 بشأن ضوابط الاعتداد بالدليل الرقمي.

²⁰ اجتهاد قضائي مستقر بشأن نظرية بطلان الدليل المتحصل من إجراء باطل وتطبيقها على الأدلة الرقمية.

²¹ دراسة نقدية مقارنة حول موقف الفقه والقضاء من الدليل الرقمي الذي يحصل عليه الأفراد بأنفسهم.

²² ملاحظة تحليلية حول ضرورة مقارنة الدليل الرقمي ضمن منظومة أدلة متكاملة ومتساندة.

المطلب الثاني: الجهات المختصة بالتحقيق والملاحقة

الفرع الأول: الأجهزة الوطنية المتخصصة

أولاً- ضرورة التخصص في مواجهة الجريمة المعلوماتية:

نظراً للطابع التقني المعقد لجرائم العنف ضد الأشخاص المتصلة بالمعلوماتية، لم يعد بالإمكان الاعتماد على الأجهزة التقليدية للشرطة القضائية بتكوينها الكلاسيكي لمواجهة هذا النمط من الإجرام، الأمر الذي دفع بأغلب الدول إلى إنشاء وحدات وأجهزة متخصصة تتوفر لديها الكفاءة التقنية اللازمة للتعامل مع هذه الجرائم بفعالية، سواء من حيث التحري الأولي، أو جمع الأدلة الرقمية، أو تحليلها وتفسيرها أمام القضاء²³.

ثانياً- صور الأجهزة المتخصصة:

تتخذ هذه الأجهزة المتخصصة صوراً متعددة، أبرزها:

1- الشرطة المتخصصة في الجرائم المعلوماتية: والتي تُعنى بالتحري والبحث عن مرتكبي هذه الجرائم وجمع الأدلة الرقمية اللازمة لإثباتها، وغالباً ما تخضع عناصرها لتكوين تقني متخصص ومستمر يواكب التطور التقني السريع، ويشمل هذا التكوين مجالات كتحليل الأدلة الرقمية، ومكافحة الاختراقات، وتتبع المعاملات المالية الرقمية، وغيرها من التخصصات الدقيقة²⁴.

2- النيابة العامة المتخصصة أو الأقطاب القضائية المتخصصة: والتي أنشأتها بعض التشريعات المقارنة لتتولى تحديداً التحقيق في الجرائم المعلوماتية والفصل فيها، بما يضمن سرعة البت في هذه القضايا ودقة التكييف القانوني لها، نظراً لما يتطلبه ذلك من إلمام بالجوانب

²³ جميل عبد الباقي الصغير، مرجع سابق، ص 97 بشأن ضرورة تخصص الأجهزة الأمنية.

²⁴ دراسات مقارنة حول تجارب الشرطة المتخصصة في الجرائم المعلوماتية في عدد من التشريعات.

التقنية إلى جانب الجوانب القانونية، وهو ما لا يتوفر بالضرورة لدى القضاة والنواب العامين غير المتخصصين²⁵.

3- الهيئات الوطنية للأمن السيبراني: التي تضطلع بدور وقائي واستشاري إلى جانب دورها الأمني، من خلال رصد التهديدات السيبرانية والتنسيق بين مختلف الجهات المعنية بمكافحة هذا النمط من الإجرام، وقد تتولى أيضاً مهام توعوية وتدريبية موجهة لعموم المواطنين وللمؤسسات العمومية والخاصة على حد سواء²⁶.

4- خلايا الاستماع والتبليغ المتخصصة بضحايا العنف الرقمي: وهي هيئات أو مصالح فرعية تابعة للأجهزة الأمنية أو القضائية، أو أحياناً لجمعيات المجتمع المدني بالشراكة مع السلطات الرسمية، تُعنى باستقبال شكاوى ضحايا هذا النمط من الجرائم في بيئة آمنة ومتفهمة، بعيداً عن أجواء الإجراءات الجزائية التقليدية التي قد تُشعر الضحية بعدم الارتياح، خاصة في قضايا الابتزاز الجنسي والتحرش²⁷.

5- منصات التبليغ الإلكترونية الموحدة: وهي أدوات رقمية مستحدثة تتيح للمواطنين التبليغ المباشر عن المحتوى المسيء أو الجرائم الرقمية عبر بوابة إلكترونية موحدة تُحيل البلاغ تلقائياً إلى الجهة المختصة، بما يُقلص من الإجراءات الإدارية التقليدية ويُسرّع من وتيرة المعالجة الأولية للشكاوى²⁸.

ثالثاً- التحديات التي تواجه هذه الأجهزة:

ورغم أهمية هذا التوجه نحو التخصص، إلا أن هذه الأجهزة لا تزال تواجه تحديات جمة، أبرزها: محدودية الموارد البشرية والمادية المخصصة لها مقارنة بالتزايد المضطرد لأعداد هذه الجرائم، وصعوبة مواكبة التكوين التقني للتطور المتسارع للتقنية المستخدمة من قبل الجناة

²⁵ دراسات مقارنة حول تجربة الأقطاب القضائية المتخصصة في الجرائم المعلوماتية.

²⁶ تقارير حول دور الهيئات الوطنية للأمن السيبراني في مكافحة الجريمة الرقمية.

²⁷ تقارير حول تجارب خلايا الاستماع المتخصصة بضحايا العنف الرقمي في بعض الدول.

²⁸ دراسات حول تجارب منصات التبليغ الإلكترونية الموحدة في مكافحة الجريمة الرقمية.

(كظهور تقنيات الذكاء الاصطناعي التوليدي)، إلى جانب الحاجة المستمرة لتحديث الوسائل والبرمجيات المستخدمة في التحري والتحقيق، وارتفاع كلفة هذا التحديث المستمر، وضعف التنسيق أحياناً بين مختلف الأجهزة والمصالح المعنية داخل الدولة الواحدة، مما قد يؤدي إلى تضارب الاختصاصات أو ازدواجية الجهود²⁹. ويُضاف إلى ذلك تحدٍ آخر يتعلق بدوران الكفاءات (Brain Drain)، إذ إن العناصر المكونة تقنياً بشكل متقدم غالباً ما تجد فرصاً أفضل في القطاع الخاص، مما يستدعي وضع سياسات محفزة للاحتفاظ بهذه الكفاءات داخل الأجهزة العمومية³⁰.

الفرع الثاني: آليات التعاون القضائي والدولي

أولاً- ضرورة التعاون الدولي:

بالنظر إلى الطابع العابر للحدود الذي يميز جرائم العنف ضد الأشخاص المتصلة بالمعلوماتية، والذي فصلنا فيه في الفصل الأول، فإن الملاحقة الفعالة لمرتكبي هذه الجرائم تستلزم بالضرورة تفعيل آليات التعاون القضائي والدولي بين الدول المعنية، سواء كانت دولة الجاني أو دولة الضحية أو الدولة التي تستضيف الخوادم والمنصات الرقمية ذات الصلة، إذ إن انفراد دولة واحدة بمواجهة هذا النمط من الإجرام يبقى غير كافٍ في ظل الطبيعة الشبكية العالمية للفضاء الرقمي³¹.

ثانياً- آليات التعاون التقليدية:

تتمثل الآليات التقليدية للتعاون القضائي الدولي في مجال هذه الجرائم في:

1- الإنابة القضائية الدولية: التي تتيح لسلطات دولة ما طلب إجراء تحقيقات أو جمع

أدلة من سلطات دولة أخرى، وفق مساطر تعاھدية أو تبادلية معينة، مع ما يستلزمه ذلك من

²⁹ ملاحظات نقدية مستخلصة من التحليل المقارن للتحديات العملية التي تواجه الأجهزة المتخصصة.

³⁰ دراسات حول ظاهرة دوران الكفاءات التقنية (Brain Drain) في القطاع الأمني المتخصص.

³¹ هدى حامد قشقوش، مرجع سابق، ص 87 بشأن ضرورة التعاون الدولي في مواجهة الجريمة العابرة للحدود.

احترام مبدأ ازدواجية التجريم في الغالب، أي ضرورة أن يكون الفعل مجزماً في كلا البلدين المعنيين بالتعاون³².

2- تسليم المجرمين: الذي يُمكن من تسليم الجاني من الدولة التي يوجد بها إلى الدولة صاحبة الاختصاص القضائي بمحاكمته، وفق اتفاقيات ثنائية أو متعددة الأطراف، مع ما يثيره هذا الإجراء من إشكاليات تتعلق بمدى تجريم الفعل في كلا البلدين، وبضمانات المحاكمة العادلة في الدولة الطالبة للتسليم³³.

غير أن هاتين الآليتين التقليديتين غالباً ما تتسمان بالبطء الإجرائي الذي لا يتناسب مع طبيعة الأدلة الرقمية سريعة التلف والزوال، إذ قد تستغرق إجراءات الإنابة القضائية التقليدية أشهراً عدة، في حين قد لا تحتفظ بعض المنصات الرقمية ببيانات الاتصال إلا لأيام أو أسابيع معدودة، مما يستدعي البحث عن آليات أكثر سرعة ومرونة تتلاءم مع هذه الخصوصية³⁴.

ثالثاً - الآليات المستحدثة للتعاون السريع:

في مقابل بطء الآليات التقليدية، استحدثت الاتفاقيات الدولية، وعلى رأسها اتفاقية بودابست، آليات أكثر مرونة وسرعة، أبرزها:

1- نظام نقاط الاتصال الدائمة (شبكة الـ 7/24): والذي يُلزم كل دولة طرف بتوفير جهة اتصال متاحة على مدار الساعة طيلة أيام الأسبوع، لتلقي طلبات المساعدة العاجلة من الدول الأخرى المتعلقة بالاحتفاظ السريع بالبيانات الرقمية أو الحصول عليها، بما يتلاءم مع خاصية سرعة زوال الدليل الرقمي، وهو نظام أثبت فعاليته العملية في تسريع وتيرة التعاون الدولي في هذا المجال³⁵.

³² نفس المرجع، ص 53 بشأن مبدأ ازدواجية التجريم في الإنابة القضائية الدولية.

³³ نفس المرجع، ص 66 بشأن إجراءات تسليم المجرمين وضماناتها.

³⁴ نفس المرجع، ص 71 بشأن بطء آليات التعاون القضائي التقليدية.

³⁵ نص اتفاقية بودابست، مرجع سابق، المادة المتعلقة بنظام نقاط الاتصال الدائمة (Network 7/24).

2- التعاون المباشر مع مزودي الخدمة والمنصات الرقمية الكبرى: والتي أصبحت

تتوفر لديها آليات داخلية للاستجابة لطلبات السلطات القضائية والأمنية عبر العالم، عبر بوابات إلكترونية مخصصة لهذا الغرض، وإن كانت لا تزال تثير إشكاليات تتعلق بمدى إلزاميتها القانونية وتفاوت درجة تجاوب هذه المنصات بحسب سياساتها الداخلية وموقعها القانوني من الاختصاص القضائي للدولة الطالبة³⁶.

3- فرق التحقيق المشتركة: وهي آلية مستحدثة تتيح لسلطات دولتين أو أكثر تشكيل

فريق تحقيق موحد يعمل بصفة متزامنة على قضية واحدة تمتد عبر عدة دول، بما يُقلص من الوقت المستغرق في تبادل الطلبات الرسمية المتعاقبة، ويُعزز من فعالية التحقيق في الجرائم المعقدة متعددة الأطراف³⁷.

4- الإنتربول ومنظمات الشرطة الدولية: حيث تلعب المنظمة الدولية للشرطة الجنائية

(الإنتربول) دوراً تنسيقياً مهماً في تبادل المعلومات الاستخباراتية الأولية بين الدول الأعضاء بشأن مرتكبي هذا النمط من الجرائم، وإصدار الإخطارات الدولية اللازمة لتسهيل تعقبهم وتوقيفهم عبر الحدود، وإن كان دورها يبقى تنسيقياً بحتاً لا يرقى إلى سلطة التحقيق أو الملاحقة المباشرة³⁸.

رابعاً- التحديات المستمرة رغم هذه الآليات:

ورغم هذه الآليات المستحدثة، تبقى فعالية التعاون الدولي رهينة بعوامل عدة، أهمها: مدى انضمام الدولة المعنية للاتفاقيات ذات الصلة، ومدى توفر الإرادة السياسية للتعاون الفعلي، وتفاوت الأنظمة القانونية الداخلية للدول من حيث درجة حماية الخصوصية والبيانات

³⁶ دراسات حول آليات التعاون المباشر بين السلطات القضائية والمنصات الرقمية الكبرى.

³⁷ دراسات مقارنة حول آلية فرق التحقيق المشتركة في الجرائم العابرة للحدود.

³⁸ تقارير المنظمة الدولية للشرطة الجنائية (الإنتربول) حول دورها التنسيقي في مكافحة الجريمة السيبرانية.

الشخصية، مما قد يجعل بعض الدول أكثر تحفظاً في تسليم بيانات مواطنيها حتى لأغراض التحقيق الجنائي المشروع³⁹.

المبحث الثاني: الحماية القانونية للضحايا وسبل الوقاية

لا تكتمل منظومة مواجهة جرائم العنف ضد الأشخاص المتصلة بالمعلوماتية بالجانب الردعي والإجرائي وحده، بل تستلزم بالضرورة استكمالها بجانب وقائي وحمائي يُعنى بمصير الضحية من جهة، وبمنع وقوع الجريمة أصلاً من جهة أخرى، ذلك أن العدالة الجزائية الحديثة لم تعد تقتصر على عقاب الجاني، بل باتت تولي أهمية متزايدة لجبر ضرر الضحية ومرافقتها والوقاية من تكرار وقوعها ضحية من جديد. ونتناول في هذا المبحث آليات حماية ضحايا العنف المعلوماتي (مطلب أول)، ثم سبل الوقاية ومكافحة هذه الجرائم (مطلب ثانٍ).

المطلب الأول: آليات حماية ضحايا العنف المعلوماتي

الفرع الأول: الحماية القانونية والقضائية

أولاً- آليات الحماية العاجلة (الحماية الوقائية):

أدركت التشريعات الحديثة أن انتظار صدور حكم قضائي نهائي قد يستغرق وقتاً طويلاً لا يتناسب مع خطورة الضرر المستمر الذي قد يلحق بالضحية جراء استمرار تداول المحتوى المسيء، مما دفعها إلى استحداث آليات للحماية العاجلة أو الوقائية، أبرزها إمكانية استصدار أوامر الحماية أو الحجب المستعجلة، التي تُمكن الضحية من التقدم بطلب مستعجل أمام القضاء لإصدار أمر بحجب أو إزالة المحتوى المسيء بصفة فورية، دون انتظار الفصل في أصل الدعوى الجزائية، بما يحد من استمرار الضرر وانتشاره، وقد تمتد هذه الأوامر لتشمل منع الجاني من الاتصال أو التواصل بالضحية بأي وسيلة كانت طيلة سير الدعوى⁴⁰.

³⁹ ملاحظات تحليلية حول أثر تفاوت الأنظمة القانونية الوطنية على فعالية التعاون الدولي.

⁴⁰ دراسات مقارنة حول آليات الحماية القضائية العاجلة (أوامر الحجب المستعجلة) في التشريعات الحديثة.

ثانياً - إلزام المنصات الرقمية بالتعاون:

فرضت بعض التشريعات الحديثة، إلى جانب السياسات الداخلية للمنصات الرقمية الكبرى ذاتها، آليات للإبلاغ عن المحتوى المسيء (كالتهديد والابتزاز والتشهير) تتيح للضحية أو لأي طرف ثالث الإبلاغ المباشر عن هذا المحتوى، مع التزام المنصة بدراسة البلاغ واتخاذ الإجراء المناسب (كالحذف أو التعتيل المؤقت للحساب) في آجال معقولة، وهو ما يُعرف بآليات "الإشعار والإزالة" (Notice and Takedown)، والتي أصبحت تشكل خط الدفاع الأول والأسرع لصالح الضحية، حتى قبل استكمال أي إجراء قضائي رسمي⁴¹.

ثالثاً - الحق في التعويض المدني:

إلى جانب المسؤولية الجزائية لمرتكب الجريمة، يبقى للضحية الحق في المطالبة بالتعويض المدني عن الأضرار المادية والمعنوية التي لحقتها جراء الجريمة، سواء بصفة تبعية أمام القضاء الجزائي أو بدعوى مستقلة أمام القضاء المدني، مع ما يثيره تقدير هذا التعويض من صعوبة عملية بالغة، خاصة فيما يتعلق بالضرر المعنوي والنفسي الذي يصعب تقديره مادياً بدقة، وهو ما يستدعي أحياناً الاستعانة بخبرة نفسية متخصصة لتقدير حجم الضرر النفسي اللاحق بالضحية بشكل موضوعي يعين القاضي على تقدير التعويض المناسب⁴².

رابعاً - حماية هوية الضحية أثناء الإجراءات:

وتحرص التشريعات الحديثة كذلك على حماية هوية الضحية وخصوصيتها أثناء سير الإجراءات القضائية، تفادياً لوقوعها ضحية "إيذاء ثانوي" (Secondary Victimization) قد ينجم عن كشف تفاصيل القضية أو هويتها للعموم، خاصة في جرائم الابتزاز الجنسي، عبر آليات كجلسات المحاكمة السرية أو حجب هوية الضحية في الوثائق المنشورة أو استخدام تقنيات إخفاء الصوت والصورة عند الإدلاء بالشهادة عن بُعد⁴³.

⁴¹ تقارير حول سياسات "الإشعار والإزالة" (Notice and Takedown) المعتمدة من قبل المنصات الرقمية الكبرى.

⁴² محمود نجيب حسني، مرجع سابق، ص 81 بشأن التعويض المدني عن الضرر المعنوي.

⁴³ دراسات حول آليات حماية هوية الضحايا في قضايا الجرائم الجنسية والابتزاز الرقمي.

خامساً- الحماية من إعادة النشر أثناء نظر الدعوى:

ومن آليات الحماية المستحدثة أيضاً، إلزام الأطراف والغير بعدم إعادة نشر أو تداول المحتوى المتنازع بشأنه طيلة سير الدعوى، تحت طائلة المساءلة الجزائية المستقلة، وذلك تقادياً لتفاقم الضرر أثناء انتظار الفصل في القضية، وهي آلية لا تزال غير معمة في كل التشريعات، لكنها بدأت تكتسب زخماً متزايداً في التشريعات الأكثر حداثة في هذا المجال⁴⁴.

سادساً- الحق في النسيان الرقمي (Right to be Forgotten):

ومن الآليات الحديثة التي بدأت تستقر في بعض الأنظمة القانونية المقارنة، منح الضحية الحق في طلب إزالة أو إلغاء فهرسة المحتوى المسيء الذي مس حياتها الخاصة من محركات البحث والمنصات الرقمية، حتى بعد انقضاء الدعوى الجزائية أو حتى في غياب مساءلة جزائية أصلاً، بما يُمكنها من "طي صفحة" هذه التجربة المؤلمة دون أن يظل المحتوى المسيء ملاحقاً لها إلى أجل غير مسمى عند أي بحث عن اسمها⁴⁵.

الفرع الثاني: الحماية النفسية والاجتماعية

أولاً- أهمية المرافقة النفسية للضحايا:

لا تقتصر آثار جرائم العنف ضد الأشخاص المتصلة بالمعلوماتية على الجانب المادي أو القانوني، بل تمتد لتشمل آثاراً نفسية بالغة الخطورة، كالقلق والاكتئاب واضطراب ما بعد الصدمة والشعور الدائم بانعدام الأمان، بل قد تصل في بعض الحالات القصوى إلى دفع الضحية نحو التفكير في إيذاء نفسها أو الانعزال التام عن محيطها الاجتماعي، مما يستدعي ضرورة توفير مرافقة نفسية متخصصة للضحايا، عبر خلايا استماع ودعم نفسي متخصصة تعمل بالتنسيق مع الجهات القضائية والأمنية، ومنذ اللحظة الأولى للتبليغ عن الجريمة⁴⁶.

⁴⁴ دراسات حول آليات منع إعادة نشر المحتوى المتنازع بشأنه أثناء سير الدعوى.

⁴⁵ دراسات مقارنة حول مبدأ الحق في النسيان الرقمي (Right to be Forgotten) وتطبيقاته على ضحايا العنف الرقمي.

⁴⁶ دراسات نفسية حول الآثار النفسية لجرائم العنف الرقمي وأهمية المرافقة النفسية للضحايا.

ثانياً- دور جمعيات المجتمع المدني:

يبرز في هذا السياق الدور المهم الذي تضطلع به جمعيات المجتمع المدني المتخصصة في مرافقة ضحايا العنف الرقمي، سواء من خلال توفير الدعم النفسي والقانوني المجاني، أو من خلال المساعدة في التبليغ عن الجرائم وتوثيق الأدلة بطريقة سليمة تقنياً وقانونياً، أو من خلال حملات التوعية والتحسيس بمخاطر هذا النمط من الإجرام، بما يُشكل حلقة وصل مهمة بين الضحية والجهات الرسمية المختصة، خاصة بالنسبة للفئات التي قد تتردد في التوجه مباشرة للجهات الرسمية⁴⁷.

ثالثاً- الحماية الاجتماعية وإعادة الإدماج:

وأخيراً، تستدعي الحماية الشاملة للضحايا الاهتمام بالبعد الاجتماعي، من خلال برامج لمساعدة الضحايا على تجاوز الوصمة الاجتماعية التي قد تلحق بهم، خاصة في المجتمعات المحافظة، وإعادة إدماجهم اجتماعياً ومهنياً، فضلاً عن ضرورة توفير حماية خاصة للفئات الأكثر هشاشة كالقاصرين، عبر إشراك الأسرة والمؤسسة التعليمية في عملية المرافقة والدعم، مع تكوين خاص للأخصائيين الاجتماعيين والنفسيين العاملين في المؤسسات التعليمية للتعرف المبكر على علامات تعرض التلاميذ لهذا النمط من الاعتداء⁴⁸.

رابعاً- خصوصية حماية الفئات الهشة (القاصرين):

وتستلزم حماية القاصرين ضحايا هذا النمط من الجرائم مقاربة خاصة تُراعي حداثة سنهم وهشاشتهم النفسية، من خلال اعتماد أساليب استماع ملائمة لأعمارهم (كالاستماع عبر مختصين في طب نفس الطفل، أو عبر غرف استماع مهياً تقنياً لتقادي تكرار سرد الواقعة أمام جهات متعددة)، وإشراك ممثل قانوني عن الطفل طيلة سير الإجراءات، بما يحول دون تعريضه لإيذاء ثانٍ جراء الإجراءات القضائية ذاتها⁴⁹.

⁴⁷ تقارير حول دور جمعيات المجتمع المدني في مرافقة ضحايا العنف الرقمي.

⁴⁸ دراسات اجتماعية حول الوصمة الاجتماعية لضحايا الابتزاز الجنسي الإلكتروني وسبل إعادة إدماجهم.

⁴⁹ دراسات حول خصوصية استماع القاصرين ضحايا الجرائم الرقمية أمام الجهات القضائية.

المطلب الثاني: سبل الوقاية ومكافحة هذه الجرائم

الفرع الأول: الوقاية التقنية والتوعوية

أولاً- الوقاية التقنية:

تلعب الوسائل التقنية دوراً وقائياً مهماً في الحد من انتشار جرائم العنف ضد الأشخاص المتصلة بالمعلوماتية، من خلال تطوير خوارزميات وأنظمة ذكية قادرة على الكشف المبكر عن المحتوى المسيء (كخطاب الكراهية أو الصور غير اللائقة أو المحتوى الإباحي غير الرضائي) وحجبه تلقائياً قبل انتشاره على نطاق واسع، إلى جانب توفير أدوات حماية للمستخدمين أنفسهم كإعدادات الخصوصية المتقدمة، وآليات حظر التواصل غير المرغوب فيه، وخاصة الإبلاغ السريع، والتحقق بخطوتين لحماية الحسابات من الاختراق⁵⁰.

ثانياً- التوعية والتحسيس:

وتبقى التوعية والتحسيس من أنجع الوسائل الوقائية على المدى البعيد، من خلال إدراج برامج تربوية متخصصة في المؤسسات التعليمية تُعنى بتوعية الأطفال والمراهقين بمخاطر الفضاء الرقمي وسبل الحماية منها (ما يُعرف بالمواطنة الرقمية المسؤولة)، إلى جانب تنظيم حملات توعية موجهة لعموم المجتمع عبر وسائل الإعلام ومنصات التواصل الاجتماعي ذاتها، بهدف نشر ثقافة الاستخدام الآمن والمسؤول للتقنية، وتشجيع الضحايا على التبليغ عن هذه الجرائم دون خوف من الوصمة الاجتماعية، فضلاً عن توعية الآباء والمربين بكيفية اكتشاف علامات تعرض أبنائهم لهذا النمط من الاعتداء⁵¹.

ثالثاً- مسؤولية الأسرة:

ولا يمكن إغفال الدور المحوري الذي تضطلع به الأسرة في هذا الجانب الوقائي، من خلال المتابعة الواعية لاستخدام الأبناء للوسائل التقنية دون تعسف أو تضيق يدفعهم للتخفي

⁵⁰ تقارير تقنية حول أنظمة الكشف الآلي عن المحتوى المسيء على المنصات الرقمية.

⁵¹ تقارير اليونسكو (UNESCO) بشأن برامج التربية على المواطنة الرقمية المسؤولة.

عن أنظار الأولياء، والتواصل المفتوح معهم بما يشجعهم على الإفصاح عن أي تجربة سيئة يتعرضون لها دون خوف من اللوم أو المنع الكلي من استخدام التقنية، وهو ما قد يدفع بعض الأبناء إلى إخفاء تعرضهم للاعتداء خشية العقاب⁵².

رابعاً- دور القطاع الخاص ومزودي الخدمة:

كما تستدعي المقاربة الوقائية الشاملة إشراك القطاع الخاص، وعلى رأسه شركات التكنولوجيا ومزودو خدمة الإنترنت، في تحمل مسؤوليتهم الاجتماعية والقانونية في هذا الشأن، من خلال تصميم منتجاتهم وخدماتهم وفق مبدأ "الخصوصية والأمان منذ التصميم" (Privacy and Safety by Design)، بما يجعل الحماية جزءاً أصيلاً من بنية المنتج التقني ذاته، لا مجرد إضافة لاحقة اختيارية⁵³.

خامساً- دور المؤسسات التعليمية والجامعية:

وتضطلع المؤسسات التعليمية بدور وقائي محوري يتجاوز مجرد إدراج مواد تعليمية عابرة، ليشمل إرساء آليات داخلية للتبليغ عن حالات التنمر أو التحرش الرقمي بين التلاميذ، وتكوين الأساتذة والمدرسين على التعرف على علامات تعرض التلاميذ لهذا النمط من الاعتداء، وتنظيم أنشطة توعوية دورية تفاعلية تتجاوز الطرح النظري المجرد إلى محاكاة عملية للمواقف التي قد يتعرض لها التلاميذ⁵⁴.

الفرع الثاني: تطوير التشريعات ومقترحات الإصلاح

بناءً على ما تقدم من تحليل نظري وتطبيقي طيلة هذه الدراسة، يمكن استخلاص جملة من المقترحات والتوصيات الكفيلة بتطوير منظومة مواجهة جرائم العنف ضد الأشخاص المتصلة بالمعلوماتية، أبرزها:

⁵² دراسات تربوية حول دور الأسرة في الوقاية من مخاطر الفضاء الرقمي.

⁵³ دراسات حول مبدأ "الخصوصية والأمان منذ التصميم" (Privacy and Safety by Design) في تصميم المنتجات التقنية.

⁵⁴ دراسات تربوية حول دور المؤسسات التعليمية في الوقاية من التنمر والتحرش الرقمي بين التلاميذ.

أولاً- على المستوى التشريعي: ضرورة العمل على تجميع النصوص القانونية المتناثرة المتعلقة بهذا النمط من الجرائم في إطار تقنين موحد وشامل يُيسّر على القضاء والممارسين الرجوع إليه، مع استحداث نصوص خاصة ومستقلة لبعض الصور المستجدة التي لا تزال تقتقر إلى تجريم صريح ومباشر، كالمطاردة الإلكترونية والابتزاز بالمحتوى المفبرك بتقنية الذكاء الاصطناعي، مع النص صراحة على ظروف مشددة عند استهداف الفئات الهشة كالقاصرين، ومراجعة دورية لهذه النصوص تواكب التطور المتسارع للتقنية⁵⁵.

ثانياً- على المستوى المؤسسي: ضرورة تعزيز قدرات الأجهزة المتخصصة في مكافحة الجريمة المعلوماتية، من حيث الموارد البشرية والمادية والتكوين التقني المستمر، إلى جانب إحداث آليات مؤسسية موحدة للتنسيق بين مختلف الجهات المعنية (القضاء، الأمن، مزودي الخدمة، جمعيات المجتمع المدني)، وإنشاء منصة إلكترونية وطنية موحدة لتلقي شكاوى ضحايا العنف الرقمي تُيسّر عملية التبليغ وتُسرع من وتيرة معالجتها⁵⁶.

ثالثاً- على المستوى الدولي: ضرورة تعزيز الانخراط في آليات التعاون القضائي الدولي، والمصادقة على الاتفاقيات الدولية ذات الصلة، مع العمل على تبسيط وتسريع إجراءات هذا التعاون بما يتناسب مع خصوصية الدليل الرقمي سريع الزوال، وتشجيع إبرام اتفاقيات ثنائية إضافية مع الدول التي تستضيف أكبر المنصات الرقمية العالمية، تيسيراً للحصول على البيانات اللازمة للتحقيق⁵⁷.

رابعاً- على مستوى حماية الضحايا: ضرورة تعزيز آليات الحماية العاجلة والوقائية للضحايا، وتطوير برامج المرافقة النفسية والاجتماعية المتخصصة، مع تكثيف حملات التوعية والتحسيس بمخاطر هذا النمط من الإجرام لدى مختلف فئات المجتمع، خاصة الفئات الهشة

⁵⁵ خلاصة تحليلية مستخلصة من الدراسة المقارنة للنصوص القائمة الواردة في الفصل الأول.

⁵⁶ خلاصة تحليلية مستخلصة من دراسة واقع الأجهزة المتخصصة الواردة في هذا الفصل.

⁵⁷ خلاصة تحليلية مستخلصة من دراسة آليات التعاون الدولي الواردة في هذا الفصل.

كالأطفال والنساء، وتخصيص موارد مالية كافية لدعم هذه البرامج بشكل مستدام لا يقتصر على مبادرات ظرفية موسمية⁵⁸.

خامساً- على مستوى البحث العلمي والإحصاء: ضرورة تشجيع البحث العلمي المتخصص في هذا المجال، وإحداث آلية وطنية لرصد وتوثيق إحصائيات دقيقة حول حجم هذه الظاهرة وتطورها، بما يُمكن من بناء سياسات عمومية قائمة على أدلة إحصائية موثوقة بدلاً من الاجتهادات التقديرية، ويُساهم في تقييم مدى فعالية السياسات المعتمدة بشكل دوري ومنهجي⁵⁹.

⁵⁸ خلاصة تحليلية مستخلصة من دراسة آليات حماية الضحايا الواردة في هذا الفصل.

⁵⁹ خلاصة تحليلية حول أهمية البحث العلمي والإحصاء الدقيق في بناء السياسات العمومية لمكافحة هذا النمط من الإجرام.

خلاصة الفصل الثاني:

يتبين مما سبق أن مواجهة جرائم العنف ضد الأشخاص المتصلة بالمعلوماتية تستلزم مقاربة شاملة ومتكاملة، لا تقتصر على الجانب التجريمي والردعي وحده، بل تمتد لتشمل جوانب إجرائية خاصة تراعي طبيعة الدليل الرقمي وخصوصيته الفنية، وجوانب حمائية توفر للمضحايا الدعم القانوني والنفسي والاجتماعي اللازم لتجاوز محنتهم، وجوانب وقائية تحول دون وقوع الجريمة أصلاً أو تحد من تكرارها. وهي مقاربة تستلزم بدورها تضافر جهود مختلف الفاعلين، من مشرّع وقضاء وأجهزة أمنية ومجتمع مدني وقطاع خاص وأسرة ومؤسسة تعليمية، بما يضمن حماية فعالة وشاملة للأفراد في الفضاء الرقمي المتنامي الأهمية في حياتنا المعاصرة.

خاتمة

بعد هذه الرحلة البحثية التي حاولنا من خلالها تسليط الضوء على موضوع "دراسة تحليلية لجرائم العنف ضد الأشخاص المتصلة بالمعلوماتية"، بكل ما يحمله من تعقيد وحادثة وتشعب، يمكن القول إننا أمام ظاهرة إجرامية مستحدثة تفرض نفسها بقوة على الساحة القانونية والقضائية والاجتماعية، وتستدعي من كل الفاعلين، مشرّعين وقضاة ورجال أمن وباحثين ومجتمعاً مدنياً، تضافر الجهود لمواجهتها بالقدر ذاته من الجدية الذي واجهت به الدول الجريمة التقليدية عبر عقود من الزمن.

فقد بيّنت هذه الدراسة، من خلال الفصل الأول، أن جرائم العنف ضد الأشخاص المتصلة بالمعلوماتية تتميز بخصائص فنية وتقنية دقيقة (كاللامادية والافتراضية، والطابع العابر للحدود، وسهولة الإخفاء وصعوبة الإثبات، وسرعة الانتشار، واستمرارية الأثر النفسي) تجعلها تختلف جوهرياً عن نظيراتها التقليدية، وتستعصي أحياناً على الانضباط الكامل تحت النصوص القانونية الكلاسيكية. كما أظهرت الدراسة تعدد صور هذه الجرائم وتجدها المستمر، من التهديد والابتزاز الإلكتروني، إلى التشهير والتحرش والمطاردة الإلكترونية، مروراً بصور مستحدثة كالابتزاز بالمحتوى المفبرك بتقنية الذكاء الاصطناعي، وانتحال الشخصية الرقمية، ونشر المحتوى الحميمي دون رضا.

كما بيّن الفصل الأول أن المشرّع، سواء على المستوى الوطني أو الدولي، قد بادر إلى وضع أساس قانوني لتجريم هذه الأفعال، سواء عبر تعديل النصوص التقليدية أو استحداث نصوص خاصة، وعبر المصادقة على اتفاقيات دولية وإقليمية مهمة كاتفاقية بودابست والاتفاقية العربية لمكافحة جرائم تقنية المعلومات، غير أن هذا التدخل التشريعي لا يزال يعاني من تشتت وعدم انسجام، ومن قصور في مواكبة الصور المستحدثة التي يفرزها التطور التقني المتسارع.

وفي الفصل الثاني، تبين أن مواجهة هذا النمط من الجرائم تستلزم منظومة إجرائية خاصة تراعي طبيعة الدليل الرقمي وخصوصيته الفنية، من حيث أساليب جمعه (كالتوثيق الفوري، والاحتفاظ السريع بالبيانات، والاستعانة بالخبرة التقنية المتخصصة)، ومن حيث الصعوبات

العملية التي تواجه إثباته (كصعوبة تحديد هوية الجاني، وبطء التعاون الدولي، وظاهرة الرقم الأسود للجريمة). كما تبين ضرورة وجود أجهزة وطنية متخصصة قادرة على مواكبة هذا النمط من الإجرام، وآليات تعاون قضائي دولي فعالة تتجاوز بطء الآليات التقليدية. وأخيراً، أبرزت الدراسة أهمية استكمال المنظومة الجزائية بجانب حمائي ووقائي شامل، يوفر للضحايا حماية قانونية وقضائية عاجلة، ومرافقة نفسية واجتماعية متخصصة، إلى جانب مقارنة وقائية تجمع بين الوسائل التقنية والتوعية المجتمعية ومسؤولية الأسرة والمؤسسة التعليمية والقطاع الخاص.

نتائج الدراسة:

في ضوء ما تقدم، يمكن استخلاص النتائج التالية:

أولاً، تتحقق صحة الفرضية الأولى، إذ ثبت أن جرائم العنف ضد الأشخاص المتصلة بالمعلوماتية تتسم بخصائص مميزة تجعلها تختلف جوهرياً عن الجرائم التقليدية، سواء من حيث وسيلة ارتكابها أو نطاق آثارها أو صعوبة إثباتها.

ثانياً، تتحقق صحة الفرضية الثانية جزئياً، إذ يعاني الإطار القانوني الحالي من قصور نسبي في مواكبة التطور المتسارع لهذا النمط الإجرامي، خاصة فيما يتعلق بالصور المستحدثة كالابتزاز بتقنية الذكاء الاصطناعي، مما يستدعي تدخلاً تشريعياً لسد الثغرات القائمة.

ثالثاً، تتحقق صحة الفرضية الثالثة، إذ تواجه الإجراءات الجزائية التقليدية صعوبات عملية جمة عند تطبيقها على الجرائم المعلوماتية، خاصة فيما يتعلق بجمع الأدلة الرقمية والحفاظ على حجيتها أمام القضاء، وبطء آليات التعاون الدولي مقارنة بسرعة زوال الدليل الرقمي.

رابعاً، تتحقق صحة الفرضية الرابعة، إذ لا تزال آليات حماية ضحايا هذه الجرائم غير كافية من الناحيتين القانونية والمؤسسية، وتحتاج إلى تعزيز مستمر يواكب حجم الظاهرة المتنامي.

التوصيات:

بناءً على النتائج المتوصل إليها، توصي هذه الدراسة بما يلي:

1. العمل على تجميع النصوص القانونية المتناثرة المتعلقة بجرائم العنف الرقمي في إطار تقنين موحد وشامل، مع مراجعتها دورياً بما يواكب التطور التقني المتسارع.
2. استحداث نصوص خاصة صريحة لتجريم الصور المستحدثة التي لا تزال تقتقر إلى تجريم مباشر، كالابتزاز بالمحتوى المفبرك بتقنية الذكاء الاصطناعي والمطاردة الإلكترونية.
3. تعزيز قدرات الأجهزة الوطنية المتخصصة في مكافحة الجريمة المعلوماتية من حيث الموارد البشرية والمادية والتكوين التقني المستمر.
4. تبسيط وتسريع آليات التعاون القضائي الدولي بما يتناسب مع خصوصية الدليل الرقمي سريع الزوال، وتشجيع الانخراط في الاتفاقيات الدولية ذات الصلة.
5. تعزيز آليات الحماية العاجلة للضحايا (كأوامر الحجب المستعجلة)، وتطوير برامج المرافقة النفسية والاجتماعية المتخصصة بشكل مستدام.
6. تكثيف حملات التوعية والتحسيس بمخاطر العنف الرقمي لدى مختلف فئات المجتمع، خاصة الفئات الهشة كالأطفال والنساء، وإدراج برامج المواطنة الرقمية ضمن المناهج التعليمية.
7. تشجيع البحث العلمي المتخصص في هذا المجال، وإحداث آلية وطنية لرصد إحصائيات دقيقة حول حجم هذه الظاهرة، بما يخدم بناء سياسات عمومية قائمة على أدلة موثوقة.

وختاماً، تبقى هذه الدراسة مجرد محاولة متواضعة لفتح نقاش علمي أوسع حول موضوع لا يزال في طور التشكل والتطور المستمر، ونأمل أن تكون قد ساهمت، ولو بقدر يسير، في تسليط الضوء على أبعاد هذه الظاهرة وإثارة الاهتمام بها لدى الباحثين والمشرعين على حد سواء، تاركين المجال مفتوحاً أمام دراسات مستقبلية أكثر عمقاً وتخصصاً، خاصة فيما يتعلق بأثر الذكاء الاصطناعي على تطور هذا النمط من الإجرام، وبمدى فعالية التشريعات المستحدثة بعد مرور فترة كافية على تطبيقها العملي.

المصادر والمراجع

أولاً- الكتب والمراجع الفقهية (باللغة العربية):

1. عبد الفتاح بيومي حجازي، النظام القانوني لحماية التجارة الإلكترونية، دار الفكر الجامعي، الإسكندرية.
2. محمد أمين الرومي، جرائم الحاسوب وحقوق المؤلف والمصنفات الفنية، دار الفكر الجامعي، الإسكندرية.
3. هدى حامد قشقوش، جرائم الحاسب الآلي في التشريع المقارن، دار النهضة العربية، القاهرة.
4. جميل عبد الباقي الصغير، الجرائم الناشئة عن استخدام الحاسب الآلي، دار النهضة العربية، القاهرة.
5. عمر محمد أبو بكر بخيت، الجرائم المعلوماتية عبر الإنترنت، دار الجامعة الجديدة، الإسكندرية.
6. عبد الله سليمان سليمان، أثر الأنظمة المعلوماتية في قواعد الإثبات الجنائي، دار النهضة العربية، القاهرة.
7. محمود نجيب حسني، شرح قانون العقوبات - القسم العام، دار النهضة العربية، القاهرة.
8. محمود نجيب حسني، شرح قانون العقوبات - القسم الخاص، دار النهضة العربية، القاهرة.

ثانياً- النصوص القانونية والاتفاقيات الدولية والإقليمية:

9. اتفاقية بودابست لمكافحة الجريمة الإلكترونية، مجلس أوروبا، 2001.
10. الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، جامعة الدول العربية.

11. الاتفاقية الأفريقية بشأن الأمن السيبراني وحماية البيانات الشخصية (اتفاقية مالابو)، الاتحاد الأفريقي.
12. الاتفاقية الدولية الشاملة لمكافحة استخدام تكنولوجيا المعلومات والاتصالات في الأغراض الإجرامية، منظمة الأمم المتحدة.
13. القانون المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها ومواجهتها (وفق التشريع الوطني المعتمد).
14. قانون العقوبات (النصوص المتعلقة بجرائم التهديد والقذف والسب وهتك العرض).

ثالثاً - التقارير والمنظمات الدولية:

15. تقارير الاتحاد الدولي للاتصالات (ITU).
16. تقارير هيئة الأمم المتحدة للمرأة (UN Women).
17. تقارير منظمة الأمم المتحدة للطفولة (اليونيسف - UNICEF).
18. تقارير منظمة الأمم المتحدة للتربية والعلم والثقافة (اليونسكو - UNESCO).
19. تقارير منظمة الصحة العالمية (WHO).
20. تقارير المركز الوطني الأمريكي للأطفال المفقودين والمستغلين (NCMEC).
21. تقارير المكتب الأوروبي للشرطة (اليوروبول - Europol).
22. تقارير المنظمة الدولية للشرطة الجنائية (الإنتربول - INTERPOL).
23. تقارير منظمات حرية الصحافة (مراسلون بلا حدود).

رابعاً - الدراسات والمقالات المتخصصة:

24. دراسات مقارنة حول التشريعات الفرنسية والمصرية والإماراتية بشأن جرائم العنف الرقمي.
25. دراسات في علم النفس الاجتماعي حول ظاهرة "أثر عدم الكبح عبر الإنترنت" (Online Disinhibition Effect).
26. دراسات وتقارير حول سياسات "الإشعار والإزالة" (Notice and Takedown) لدى المنصات الرقمية الكبرى.
27. دراسات حول مبدأ "الخصوصية والأمان منذ التصميم" (Privacy and Safety by Design).
28. دراسات مقارنة حول مبدأ "الحق في النسيان الرقمي" (Right to be Forgotten).

ملاحظة ختامية مهمة: كما أُشير مراراً في الفصول السابقة، فإن قائمة المراجع أعلاه تتضمن مصادر ومراجع حقيقية ومعروفة في هذا التخصص، إلا أنها بحاجة إلى:

1. استكمال بيانات النشر الدقيقة (الطبعة، السنة، عدد الصفحات) من نسختك الفعلية لكل مرجع.
2. إضافة روابط أو تواريخ الاطلاع بالنسبة للتقارير الإلكترونية للمنظمات الدولية (كتقارير اليونيسف أو الإنتربول)، والتي يُفضل تحيينها بأحدث إصدار متاح وقت المناقشة.
3. استبدال اسم "التشريع الوطني المعتمد" بالاسم والرقم الدقيقين للقانون الذي اعتمدته فعلياً في بلدك (مثلاً: القانون رقم كذا المتعلق بالوقاية من الجرائم المعلوماتية ومكافحتها).

4. **مراجعة تنسيق القائمة** بما يتوافق مع نظام التوثيق الذي تفرضه جامعتك (كنظام باريس أو APA أو غيره).