Federal Foreign Office

Global Project Partners e.V.

secdev.foundation

KING HUSSEIN FOUNDATION مؤسسة الملك الحسين
مركز المعلومات والبحوث
INFORMATION AND RESEARCH CENTER

الدليل القانوني للتعامل مع قضايا العنف الرقمي ضد النساء

مرجع قانوني وعملي للممارسين والجهات ذات العلاقة

مركز المعلومات والبحوث - مؤسسة الملك الحسين

الدليل القانوني للتعامل مع قضايا العنف الرقمي ضد النساء في الأردن

إعداد

مركز المعلومات والبحوث - مؤسسة الملك الحسين

بدعم من

Global Project Partners e.V. (GPP)

في إطار مشروع ممول من وزارة الخارجية الاتحادية الألمانية

عمّان - الأردن

2026

فريق إعداد الدليل

فريق المركز

الأستاذ الدكتور أيمن هلسا مدير المركز	**الأستاذة سوسن زايدة** رئيسة قسم الأبحاث
الأستاذة روان ربيحات باحثة رئيسية	**الأستاذة جهينة زريقات** باحثة

المراجعة القانونية

يتقدم فريق إعداد الدليل بخالص الشكر والتقدير إلى:

المحامي الدكتور صخر الخصاونة

لما تفضل به من مراجعة قانونية متخصصة للدليل، وما قدمه من ملاحظات واقتراحات قيّمة استندت إلى خبرته الأكاديمية والعملية الواسعة، وأسهمت في تعزيز دقة المحتوى القانوني، ومواءمته مع التشريعات الأردنية والممارسات القضائية ذات الصلة.

تنويه

أُعد هذا الدليل لأغراض التوعية وبناء القدرات، ولا يُعد بديلاً عن الاستشارة القانونية أو التفسير القضائي للنصوص القانونية. وقد بذل فريق الإعداد أقصى درجات العناية لضمان دقة المعلومات الواردة فيه حتى تاريخ نشره، إلا أن تطبيق النصوص القانونية يظل خاضعاً للتشريعات النافذة وما يستقر عليه الاجتهاد القضائي.

شكر وتقدير

يتقدم مركز المعلومات والبحوث - مؤسسة الملك الحسين بخالص الشكر والتقدير إلى Global Project Partners e.V على دعمها لإعداد هذا الدليل، وذلك في إطار المشروع المنفذ بدعم من وزارة الخارجية الاتحادية الألمانية.

ويعكس هذا الدليل ثمرة تعاون مهني وبنّاء يهدف إلى تعزيز القدرات القانونية والمهنية في التعامل مع قضايا العنف الرقمي ضد النساء، من خلال توفير مرجع عملي يستند إلى التشريعات الأردنية والخبرات الوطنية والممارسات الفضلى في هذا المجال.

كما يتقدم المركز بالشكر والتقدير لجميع الخبراء والخبيرات، والمحامين والمحاميات، وممثلي الجهات الحكومية، ومؤسسات المجتمع المدني، الذين شاركوا في المقابلات وجلسات التشاور وإبداء الملاحظات، وأسهموا بخبراتهم العملية في تطوير هذا الدليل.

تنويه

إن الآراء والمحتوى الوارد في هذا الدليل تعبر عن المؤلفين، ولا تعكس بالضرورة وجهات نظر Global Project Partners e.V. أو وزارة الخارجية الاتحادية الألمانية.

عن الدليل

يأتي هذا الدليل ضمن إطار شراكة فنية بين مركز المعلومات والبحوث – مؤسسة الملك الحسين ومؤسسة SecDev في مجال العنف الرقمي ضد النساء، والذي شمل جهوداً بحثية وأنشطة لبناء القدرات وتطوير المعرفة والموارد ذات الصلة. وتعمل مؤسسة SecDev، وهي مؤسسة غير حكومية كندية، على تعزيز السلامة والمرونة الرقمية، يشمل ذلك العديد من المبادرات مثل مبادرة Salam@ المعنية بالعنف الرقمي ضد النساء. وقد أسهم التعاون الفني بين المؤسستين في دعم تطوير هذا الدليل بما يتلاءم مع السياق الأردني واحتياجات الممارسين والممارسات القانونيين.

أهمية الدليل

يشهد الأردن، شأنه شأن العديد من دول العالم، تزايداً في استخدام الوسائل الرقمية ومنصات التواصل الاجتماعي، وما رافق ذلك من بروز أنماط جديدة من الجرائم والانتهاكات التي تستهدف النساء والفتيات في الفضاء الرقمي. وقد أوجد هذا الواقع تحديات قانونية وعملية متزايدة أمام الممارسين القانونيين والجهات المعنية بالاستجابة لهذه القضايا، تتطلب فهماً متكاملاً للتشريعات الوطنية، وطبيعة الأدلة الرقمية، وآليات حماية الضحايا، والإجراءات العملية ذات الصلة، وطبيعة الأدلة الرقمية، وآليات حماية الضحايا، والإجراءات العملية الواجب اتباعها عند التعامل مع هذا النوع من القضايا.

ويأتي هذا الدليل استجابةً لهذه الحاجة، ليكون مرجعاً قانونياً وعملياً يساعد الممارسين القانونيين والجهات ذات العلاقة على فهم قضايا العنف الرقمي ضد النساء بصورة تراعي الجوانب القانونية والإجرائية والحقوقية، وتسهم في تعزيز الوصول إلى العدالة وحماية حقوق الضحايا.

الهدف من الدليل

يهدف هذا الدليل إلى توفير مرجع قانوني وعملي للتعامل مع قضايا العنف الرقمي ضد النساء في الأردن، من خلال توضيح الإطار القانوني الوطني، وأبرز الجوانب الإجرائية والإثباتية، والممارسات المهنية المرتبطة بالاستجابة لهذه القضايا.

الفئة المستهدفة

يستهدف هذا الدليل الممارسين القانونيين والجهات ذات العلاقة بالتعامل مع قضايا العنف الرقمي ضد النساء، بما في ذلك المحامين والمحاميات، ومقدمي المساعدة القانونية، والعاملين في جهات إنفاذ القانون والجهات الرسمية المختصة، كما يمكن أن يستفيد منه الباحثون ومؤسسات المجتمع المدني والجهات العاملة في مجالات الحماية والوصول إلى العدالة.

منهجية إعداد الدليل

اعتمد إعداد هذا الدليل على منهجية تشاركية جمعت بين المراجعة القانونية، والخبرة العملية، والتشاور مع الجهات ذات العلاقة، وشملت ما يلي:

مراجعة التشريعات الأردنية ذات الصلة، وفي مقدمتها قانون الجرائم الإلكترونية، وقانون العقوبات، وقانون حماية البيانات الشخصية، والتشريعات والإجراءات ذات العلاقة.

مراجعة الأدبيات الوطنية والدولية، والدلائل المهنية، والممارسات الفضلى المتعلقة بالتعامل مع قضايا العنف الرقمي ضد النساء.

إجراء مقابلات شبه منظمة مع ممثلين عن الجهات الحكومية ذات العلاقة، وفي مقدمتها وحدة مكافحة الجرائم الإلكترونية، إضافة إلى مقدمي الخدمات القانونية، ومؤسسات المجتمع المدني، والمحامين والمحاميات، والخبراء والخبيرات في المجالات القانونية والحقوقية.

مراجعة المسودة من قبل خبير قانوني متخصص، وإدماج الملاحظات القانونية لضمان دقة المحتوى واتساقه مع الإطار التشريعي الأردني.

عقد جلسة تشاورية (Validation Workshop) ضمت نخبة من المحامين والمحاميات والخبراء القانونيين لمناقشة واقع الممارسة العملية، والتحقق من مدى استجابة الدليل للاحتياجات الفعلية للممارسين القانونيين، والاستفادة من الملاحظات المطروحة في تطوير النسخة النهائية.

وقد اعتمد إعداد الدليل على منهجية تراعي التكامل بين الجوانب القانونية والعملية، بما يضمن أن يكون مرجعاً تطبيقياً يساعد المحامين والمحاميات في التعامل مع هذا النوع من القضايا.

حقوق النشر والاستخدام

© مركز المعلومات والبحوث - مؤسسة الملك الحسين، 2026.

جميع الحقوق محفوظة.

يُسمح بإعادة إنتاج هذا الدليل أو الاقتباس منه، كلياً أو جزئياً، لأغراض غير تجارية، شريطة الإشارة بوضوح إلى المصدر على النحو الآتي:

مركز المعلومات والبحوث، مؤسسة الملك الحسين. الدليل القانوني للتعامل مع قضايا العنف الرقمي ضد النساء في الأردن. عمّان، الأردن، 2026.

ويُمنع استخدام هذا الدليل أو أي جزء منه لأغراض تجارية دون الحصول على موافقة خطية مسبقة من مركز المعلومات والبحوث

قائمة المحتويات

فريق إعداد الدليل 2

المراجعة القانونية 2

شكر وتقدير 3

الفصل الأول: مدخل إلى العنف الرقمي ضد النساء 10

ثالثاً: الخصوصية الجندرية للعنف الرقمي 15

رابعاً: الشخصيات العامة وغير العامة 16

الفصل الثاني: الإطار القانوني الأردني الناظم لقضايا العنف الرقمي ضد النساء 20

أولاً: الأساس الدستوري للحماية 20

ثانيًا: قانون الجرائم الإلكترونية رقم 17 لسنة 2023 21

ثالثاً: تشريعات أخرى ذات صلة 26

الفصل الثالث: الأدلة الإلكترونية في قضايا العنف الرقمي ضد النساء 28

أولاً: أنواع الأدلة الإلكترونية في قضايا العنف الرقمي ضد النساء 28

ثانياً: حجية الأدلة الإلكترونية في القانون الأردني 31

ثالثاً: شروط قبول الدليل الإلكتروني أمام القضاء 32

رابعاً: الأخطاء الشائعة التي قد تضعف الدليل الإلكتروني 33

خامساً: إجراءات جمع الأدلة الإلكترونية وضبطها 34

سادساً: إزالة المحتوى وحفظ البيانات 34

سابعاً: جوانب عملية خاصة 35

الفصل الرابع: التعامل القانوني الأولي مع قضايا العنف الرقمي ضد النساء.....38
أولاً: المقابلة الأولية مع الضحية.....38
ثانياً: تقييم المخاطر.....39
ثالثاً: السرية وحماية المعلومات.....40
رابعاً: التواصل مع الجهات المختصة.....41
خامساً: التعامل المهني مع الضحية.....42
الفصل الخامس: الإحالة والدعم والحماية في قضايا العنف الرقمي ضد النساء.....44
أولاً: أهمية الدعم متعدد القطاعات.....45
ثانياً: دور المحامي أو مقدم المساعدة القانونية.....46
ثالثاً: التعامل مع المنصات الرقمية.....47
رابعاً: السلامة الرقمية للضحية.....48
خامساً: الجهات المختصة وجهات الدعم.....48
سادساً: التعامل مع المخاطر المستمرة.....49
الفصل السادس: الأدوات العملية والملاحق.....51
أولاً: نموذج مقابلة أولية مع الضحية.....51
ثانياً: قائمة تحقق أولية للأدلة الرقمية.....52
ثالثاً: قائمة تحقق أولية لتقييم المخاطر.....52
رابعاً: إرشادات أولية للسلامة الرقمية.....53
خامساً: إرشادات أولية للتعامل مع المنصات الرقمية.....53
سادساً: قائمة بالجهات المرجعية والداعمة.....53

سابعا: مصفوفة الجرائم الشائعة والتكييف القانوني الأولي في قضايا العنف الرقمي ضد النساء 55

ثامنا: مؤشرات تستدعي اتخاذ إجراءات عاجلة.....57

تاسعا: أبرز التحديات العملية في قضايا العنف الرقمي 58

عاشرا: تذكير عملي عند التعامل مع قضايا العنف الرقمي ضد النساء 59

حادي عشر: أهم التعريفات والمصطلحات أساسية.....59

قائمة المراجع: 70

الفصل الأول: مدخل إلى العنف الرقمي ضد النساء

أصبح الفضاء الرقمي جزءاً أساسياً من الحياة اليومية في الأردن، سواء في مجالات التواصل الاجتماعي أو التعليم أو العمل أو المشاركة العامة. ومع التوسع المتزايد في استخدام وسائل التواصل الاجتماعي والمنصات الرقمية، برزت أنماط جديدة من الانتهاكات والسلوكيات الضارة التي تُمارس عبر الوسائل الإلكترونية، بما في ذلك العنف الرقمي ضد النساء.

ولا يقتصر هذا النوع من العنف على الإساءة اللفظية أو التشهير فحسب، بل يشمل مجموعة واسعة من الأفعال التي قد تؤدي إلى الإضرار النفسي أو الاجتماعي أو المهني أو القانوني بالضحية، وقد تمتد آثارها لتؤثر على السلامة الشخصية والعلاقات الأسرية وفرص المشاركة العامة.

وفي كثير من الحالات، يتسم العنف الرقمي بسرعة الانتشار وصعوبة السيطرة على المحتوى المنشور، الأمر الذي يزيد من تعقيد التعامل القانوني معه، ويجعل من الضروري امتلاك الممارسين والجهات المعنية فهماً واضحاً لطبيعة هذه القضايا وخصوصيتها، سواء من حيث التكييف القانوني أو جمع الأدلة الرقمية أو تقييم المخاطر التي قد تتعرض لها الضحايا.

أولاً: مفهوم العنف الرقمي ضد النساء[1]

يشير العنف الرقمي ضد النساء إلى أي سلوك أو فعل يُرتكب باستخدام الوسائل الرقمية أو عبر الإنترنت ويستهدف النساء أو الفتيات بشكل يؤدي إلى الإساءة أو التهديد أو الابتزاز أو انتهاك الخصوصية أو الإضرار النفسي أو الاجتماعي أو المهني.[2]

ومن الناحية القانونية، لا يستخدم التشريع الأردني مصطلح "العنف الرقمي ضد النساء" بوصفه وصفاً قانونياً مستقلاً، وإنما تتوزع الأفعال المكوّنة لهذا النوع من العنف على عدد من الجرائم المنصوص عليها في التشريعات النافذة، وعلى رأسها قانون الجرائم الإلكترونية وقانون العقوبات والتشريعات ذات الصلة.

كما أن قانون الجرائم الإلكترونية يتعامل مع هذه الأفعال من خلال الأركان القانونية للجريمة والوسيلة المستخدمة في ارتكابها، دون تمييز بين النساء والرجال من حيث صفة المجني عليه. وبذلك فإن العنف الرقمي ضد النساء يشمل الجرائم

[1] United Nations Population Fund. "Technology-Facilitated Gender-Based Violence: A Growing Threat." Accessed May 9, 2026.

[2] قلعة الكرك، *سياسيات تحت القصف الرقمي: دراسة في أنماط ومصادر وآثار العنف الرقمي الذي واجهته المرشحات في الانتخابات البرلمانية الأردنية لعام 2024*، مؤسسة سيكديف (سلاما@) (عمّان، 2025)؛ المطيري، نورة. *العنف الرقمي ضد النساء في الكويت: تفكيك تجارب النساء*. مؤسسة سيكديف، (سلاما@). 2022.

والأفعال المرتكبة باستخدام الشبكة المعلوماتية أو تقنية المعلومات أو نظام المعلومات أو المواقع الإلكترونية أو منصات التواصل الاجتماعي، متى استهدفت النساء أو الفتيات وألحقت بهن ضرراً أو تهديداً أو انتهاكاً لحقوقهن.

وقد يتم هذا العنف من خلال:

منصات التواصل الاجتماعي.	تطبيقات التراسل الفوري.	البريد الإلكتروني.
المواقع الإلكترونية.	الحسابات الوهمية.	نشر أو إعادة نشر المحتوى الرقمي.

ولا يشترط أن يكون الفعل ذا طبيعة جنسية حتى يُعتبر عنفاً رقمياً ضد النساء، إذ قد يشمل أيضاً: [3]

الذم والقدح والتحقير الإلكتروني.	نشر الأخبار أو المعلومات الكاذبة أو المضللة.
التهديد.	الابتزاز الإلكتروني.
انتحال الهوية.	انتهاك الخصوصية.
نشر المعلومات أو الصور الخاصة.	حملات الإساءة المنظمة.
أشكال أخرى من السلوكيات الضارة التي تتم عبر الوسائل الرقمية.	

ومن الجدير بالملاحظة أن المشرع الأردني لم يضع نصوصاً خاصة بالعنف الرقمي ضد النساء باعتباره فئة مستقلة من الجرائم، كما لم يعتبر صفة المرأة ظرفاً مشدداً للعقوبة بحد ذاتها. وفي المقابل، فقد اعتبر القانون في بعض الحالات ظروفاً معينة تستوجب تشديد العقوبة، مثل الجرائم المرتكبة بحق الأطفال أو بعض الفئات المستضعفة التي منحها المشرع حماية إضافية. [4]

ويتميّز العنف الرقمي بعدد من الخصائص التي تزيد من خطورته، من أبرزها:

- سهولة الوصول إلى الضحية في أي وقت ومن أي مكان.
- السرعة الكبيرة في انتشار المحتوى وإعادة تداوله على نطاق واسع.

[3] Salam@, *Digital Violence Against Women in Algeria: Legal and Institutional Context* (2024)؛ Salam@, *Digital Violence Against Women in Yemen: Legal and Institutional Context* (2024).
(مؤسسة أنسم للحقوق الرقمية. الدليل الشامل للتعامل مع قضايا العنف الرقمي ضد النساء في العراق، مؤسسة سيكديف (سلاما@) (2025).

[4] Information and research Center – King Hussein Foundation. Jordan's Cybercrime Law: Balancing Protection and Freedom of Expression. SecDev Foundation (Amman, 2025).

- إمكانية إعادة نشر المحتوى بصور متعددة وإرفاقه بتعليقات أو تفسيرات شخصية قد تزيد من حجم الضرر.
- صعوبة إزالة المحتوى أو السيطرة عليه بصورة كاملة بعد نشره.
- إمكانية ارتكاب الانتهاك بصورة مجهولة أو باستخدام حسابات وهمية.
- إمكانية استخدام وسائل التمويه التقني أو ارتكاب الأفعال من خارج الإقليم الأردني، الأمر الذي قد يطرح تحديات إضافية تتعلق بالتتبع والملاحقة القانونية.
- استمرار الأثر النفسي والاجتماعي لفترات طويلة، حتى بعد إزالة المحتوى أو إغلاق الحسابات المستخدمة في الانتهاك.

كما أن بعض النساء قد يواجهن ضغوطاً اجتماعية إضافية عند التعرض للعنف الرقمي، حيث قد تتجه بعض البيئات الاجتماعية إلى لوم الضحية أو تحميلها جزءاً من المسؤولية، الأمر الذي يزيد من الآثار النفسية والاجتماعية المترتبة على الواقعة.[5]

ثانياً: أنماط العنف الرقمي ضد النساء[6]

تتعدد أشكال العنف الرقمي ضد النساء، وقد تتداخل أكثر من صورة في الواقعة الواحدة. كما قد تنتقل الواقعة من شكل إلى آخر مع تطورها، بحيث تبدأ بانتهاك للخصوصية ثم تتطور إلى ابتزاز أو تشهير أو تهديد.

ومن أبرز هذه الأنماط:

1. الذم والقدح والتحقير الإلكتروني

ويشمل إرسال أو نشر أو إعادة نشر بيانات أو معلومات أو تعليقات أو محتوى رقمي عبر الشبكة المعلوماتية أو تقنية المعلومات أو نظام المعلومات أو المواقع الإلكترونية أو منصات التواصل الاجتماعي، يتضمن عبارات أو أوصافاً من شأنها المساس بسمعة المرأة أو كرامتها أو مكانتها الاجتماعية.

ويُعد هذا النمط من أكثر أشكال العنف الرقمي شيوعاً، خاصة في البيئات المرتبطة بالنشاط العام أو المهني أو السياسي أو الاجتماعي.

2. الابتزاز الإلكتروني والتشهير

---

[5] قلعة الكرك، *سياسيات تحت القصف الرقمي: دراسة في أنماط ومصادر وآثار العنف الرقمي الذي واجهته المرشحات في الانتخابات البرلمانية الأردنية لعام 2024*، مؤسسة سيكديف (سلاما@) (عمّان، 2025)؛ شبكة مناهضة العنف الرقمي ضد الصحفيات في الأردن، مؤسسة الملك الحسين، *التأثيرات المهنية والقانونية على الصحفيات الأردنيات غير المنتسبات للنقابة في ظل تصاعد العنف الرقمي*، مؤسسة سيكديف (سلاما@) (عمّان، 2025).

[6] European Institute for Gender Equality. *Cyber Violence against Women and Girls*. Luxembourg: Publications Office of the European Union, 2017.

يُقصد بالابتزاز إجبار شخص على القيام بفعل أو الامتناع عنه أو تحقيق منفعة غير مشروعة للفاعل أو لغيره من خلال التهديد بإفشاء أمر أو نشر معلومات أو صور أو تسجيلات من شأنها الإضرار بسمعته أو شرفه أو مكانته الاجتماعية.

وفي البيئة الرقمية قد يتم الابتزاز من خلال:

- التهديد بنشر الصور أو التسجيلات الخاصة.
- التهديد بنشر محادثات شخصية.
- التهديد بالكشف عن معلومات خاصة أو حساسة.
- التهديد بالإساءة إلى السمعة أو التشهير بالضحية.

كما قد يشمل استخدام أو نشر أو إعادة نشر صور أو تسجيلات أو مقاطع فيديو حصل عليها الجاني بصورة مشروعة أو غير مشروعة بقصد التشهير أو الإساءة أو الحصول على منفعة أو ممارسة الضغط على الضحية.

3. انتهاك الخصوصية

يشمل هذا النمط نشر أو تداول الصور أو التسجيلات أو المعلومات الشخصية دون موافقة صاحبتها، أو الوصول غير المشروع إلى الحسابات أو البيانات الخاصة أو استخدامها بصورة تنتهك حق المرأة في الخصوصية.

وقد يتخذ انتهاك الخصوصية أشكالاً متعددة، من بينها:

- نشر الصور الشخصية دون إذن.
- نشر المحادثات الخاصة.
- مشاركة البيانات الشخصية أو العائلية.
- الدخول غير المشروع إلى الحسابات الإلكترونية.
- جمع المعلومات الشخصية أو تداولها دون موافقة صاحبتها.

4. انتحال الهوية الرقمية

ويتمثل في إنشاء حسابات أو صفحات أو ملفات شخصية باسم الضحية أو استخدام صورها أو بياناتها أو معلوماتها الشخصية بطريقة مضللة أو مسيئة، بما يؤدي إلى الإضرار بسمعتها أو خداع الآخرين أو ارتكاب أفعال باسمها.

وقد يستخدم انتحال الهوية لأغراض التشهير أو الاحتيال أو الإساءة أو الابتزاز أو الإضرار بالعلاقات الاجتماعية أو المهنية للضحية.

5. التحرش الإلكتروني

يشمل الرسائل أو التعليقات أو السلوكيات الرقمية غير المرغوب فيها التي تحمل طابعاً مسيئاً أو مهيناً أو جنسياً أو ترهيبياً، خاصة إذا كانت متكررة أو مستمرة أو تنطوي على تهديد أو ضغط نفسي.

وقد يحدث التحرش الإلكتروني عبر:

- الرسائل الخاصة.
- التعليقات العامة.
- المجموعات المغلقة.
- المكالمات الرقمية.
- المنصات الاجتماعية المختلفة.

6. التهديد والملاحقة الرقمية

ويشمل إرسال رسائل تهديد أو ترهيب، أو متابعة الضحية بصورة متكررة عبر الوسائل الرقمية، أو مراقبة نشاطها الإلكتروني، أو التواصل المستمر معها بصورة غير مرغوب فيها بما يسبب لها الخوف أو القلق أو الشعور بعدم الأمان.

وقد تتخذ الملاحقة الرقمية أشكالاً مختلفة، مثل:

- تتبع الحسابات الشخصية.
- مراقبة النشاط الإلكتروني.
- تكرار الرسائل أو الاتصالات.
- استخدام حسابات متعددة للتواصل مع الضحية.
- نشر معلومات شخصية بقصد التخويف أو الضغط.

7. حملات الإساءة المنظمة

وتتمثل في استهداف الضحية بشكل جماعي أو منظم من خلال نشر الإساءات أو التحريض أو تداول الشائعات أو المعلومات المضللة أو المحتوى المسيء بهدف الإضرار بسمعتها أو التأثير على نشاطها الشخصي أو المهني أو العام.

وغالباً ما تظهر هذه الحملات في سياقات العمل العام أو النشاط السياسي أو الإعلامي أو الحقوقي، وقد يشارك فيها أفراد أو مجموعات بصورة منسقة أو شبه منسقة.

8. الشعوذة الإلكترونية

يقصد بالشعوذة الإلكترونية استخدام المنصات الرقمية أو وسائل التواصل الاجتماعي للترويج لأعمال الشعوذة أو السحر أو قراءة الطالع أو الادعاء بامتلاك قدرات روحانية أو علاجية، بما يؤدي إلى استدراج النساء أو استغلالهن أو الإضرار بهن.

وقد تتضمن هذه الممارسات طلب صور أو معلومات شخصية أو أسرية، أو استغلال الظروف النفسية أو الاجتماعية للضحية، أو استخدامها لاحقاً في الابتزاز أو التهديد أو التشهير أو الاحتيال.

ورغم أن التشريعات الأردنية لا تتعامل مع "الشعوذة الإلكترونية" بوصفها وصفاً جرمياً مستقلاً، إلا أن الأفعال المرتبطة بها قد تشكل جرائم أخرى وفقاً لظروف كل حالة، مثل الابتزاز الإلكتروني أو الاحتيال أو انتهاك الخصوصية أو إساءة استخدام البيانات الشخصية. ولذلك ينبغي التعامل مع هذه الوقائع من خلال تحليل الأفعال المرتكبة والآثار المترتبة عليها لتحديد التكييف القانوني المناسب.

9. خطاب الكراهية في البيئة الرقمية

يقصد بخطاب الكراهية، في معناه العام، أي شكل من أشكال التعبير أو التواصل الشفهي أو الكتابي أو البصري الذي يتضمن التحريض على الكراهية أو التمييز أو العداء أو الازدراء تجاه شخص أو مجموعة من الأشخاص بسبب صفاتهم أو هوياتهم أو انتماءاتهم.

وفي سياق العنف الرقمي ضد النساء، قد يرتبط خطاب الكراهية باستهداف النساء بسبب الجنس أو النوع الاجتماعي أو الانتماء الديني أو العرقي أو غير ذلك من الخصائص الشخصية، بما يسهم في خلق بيئة عدائية أو مهينة أو تمييزية ضدهن.

ثالثاً: الخصوصية الجندرية للعنف الرقمي

رغم أن العنف الرقمي قد يستهدف مختلف الفئات، إلا أن النساء والفتيات يواجهن أشكالاً خاصة من الانتهاكات ترتبط غالباً بالنوع الاجتماعي والصور النمطية والأدوار الاجتماعية المفروضة عليهن. وتكتسب هذه الخصوصية أهمية خاصة في المجتمعات التي قد يترتب فيها على الانتهاك الرقمي آثار اجتماعية أو أسرية أو مهنية تتجاوز الضرر المباشر الناتج عن الفعل ذاته.

وفي كثير من الحالات، يرتبط العنف الرقمي ضد النساء بمحاولات:

- السيطرة أو الترهيب.
- الإساءة إلى السمعة أو الشرف.
- الحد من المشاركة العامة أو المهنية.
- فرض ضغوط اجتماعية أو أسرية.
- الانتقام من الضحية أو التأثير على قراراتها الشخصية أو المهنية.

كما أن بعض النساء قد يترددن في الإبلاغ عن الانتهاكات الرقمية بسبب:

- الخوف من الوصمة الاجتماعية.
- القلق من تحميل الضحية مسؤولية ما حدث.
- الخشية من انتشار المحتوى المسيء بصورة أوسع نتيجة إجراءات الشكوى أو التقاضي.

- ضعف الثقة بفعالية الحماية القانونية أو المجتمعية.
- الكلفة المالية المترتبة على بعض الإجراءات القانونية أو الفنية اللازمة لإثبات الانتهاك.
- طول الإجراءات القضائية في بعض الحالات.
- الخوف من المساس بالخصوصية أو كشف تفاصيل شخصية أو عائلية أثناء سير الإجراءات.

ومن المهم أن يدرك المحامون والمحاميات أن هذه العوامل قد تؤثر بصورة مباشرة على قرار الضحية بالإبلاغ أو الاستمرار في الإجراءات القانونية، وأن التعامل مع هذه القضايا يتطلب حساسية مهنية خاصة تراعي الأبعاد النفسية والاجتماعية إلى جانب الأبعاد القانونية.

ويُعد فهم هذه الخصوصية أمراً أساسياً عند تقييم المخاطر، وتحديد الأولويات القانونية، واختيار الاستراتيجية المناسبة للتعامل مع القضية. كما يقتضي ذلك من المحامي أو المحامية التعامل مع المرأة المتضررة بوصفها موكلة وضحية في آن واحد، بما يتطلب تخصيص الوقت الكافي للاستماع، وشرح الخيارات القانونية والإجرائية بوضوح، ومساعدتها على اتخاذ قرارات مستنيرة دون ضغط أو لوم أو أحكام مسبقة.

رابعاً: الشخصيات العامة وغير العامة

قد يستهدف العنف الرقمي النساء من مختلف الفئات، سواء كنّ شخصيات عامة أو غير عامة، إلا أن طبيعة المخاطر والآثار القانونية والاجتماعية قد تختلف باختلاف طبيعة الظهور العام ومستوى التعرض للفضاء الرقمي.

وتكتسب التفرقة بين الشخصيات العامة وغير العامة أهمية قانونية وعملية عند تقييم بعض الوقائع المرتبطة بالنشر الإلكتروني وحرية التعبير والحق في الخصوصية، وعند التمييز بين النقد المباح والأفعال التي تشكل ذماً أو قدحاً أو تحقيراً أو انتهاكاً للحياة الخاصة.

1. الشخصيات العامة[7]

تشمل الشخصيات العامة، على سبيل المثال لا الحصر، النساء العاملات في:

- الإعلام.
- العمل السياسي.
- النشاط العام.
- العمل الحقوقي.
- صناعة المحتوى الرقمي.

[7] Posetti, Julie, Nabeelah Shabbir, Kalina Bontcheva, Diana Maynard, and Nermine Aboulez. The Chilling: Global Trends in Online Violence against Women Journalists. Paris: UNESCO, 2021.

- الوظائف العامة أو المواقع القيادية ذات الصلة بالشأن العام.

كما قد تشمل الشخصيات العامة فئات أخرى تكتسب حضوراً عاماً أو تأثيراً مجتمعياً يجعل أنشطتها أو مواقفها محل اهتمام الرأي العام.

ويُلاحظ في الفقه والقضاء المقارن أن الشخصيات العامة قد تكون أكثر عرضة للنقد أو التعليق المرتبط بأدائها أو نشاطها العام، شريطة أن يتم ذلك في حدود القانون وبحسن نية وضمن إطار النقد الموضوعي المرتبط بالمصلحة العامة.

وفي هذا السياق، استقر الفقه القانوني على مجموعة من الضوابط التي تساعد في التمييز بين النقد المباح والاعتداء على السمعة أو الكرامة، ومن أبرزها:

- أن يستند النقد إلى وقائع أو معلومات ذات أساس واقعي.
- أن تكون الواقعة محل النقد ذات أهمية أو مصلحة عامة.
- أن يكون التعليق أو الرأي مرتبطاً بالواقعة محل النقاش.
- أن يكون النقد متناسباً مع الواقعة.
- أن يتم بحسن نية ودون قصد الإساءة أو التشهير.

ومع ذلك، فإن الصفة العامة للشخص لا تعني حرمانه من الحماية القانونية أو إباحة الإساءة إليه أو انتهاك خصوصيته أو ممارسة العنف الرقمي بحقه، إذ تظل الحماية القانونية مكفولة للجميع وفقاً لأحكام القانون.

وغالباً ما تكون الشخصيات العامة أكثر عرضة لحملات التشهير والإساءة المنظمة وخطاب الكراهية والهجمات الرقمية المرتبطة بآرائهن أو نشاطهن أو مواقفهن العامة.[8]

كما قد تظهر في بعض الحالات فئة يمكن وصفها بـ "الشخصيات العامة بالصدفة"، ويُقصد بها النساء اللواتي لا يمارسن نشاطاً عاماً أو سياسياً أو إعلامياً بصورة منتظمة، إلا أنهن يصبحن محل اهتمام عام مؤقت بسبب واقعة معينة، مثل انتشار قضية تخصهن، أو تداول مقطع أو صورة أو تصريح لهن، أو ارتباط أسمائهن بحدث اجتماعي أو قضائي أو إعلامي.

وفي هذه الحالات، لا يؤدي هذا الظهور المؤقت إلى سقوط حق المرأة في الخصوصية أو إباحة الإساءة إليها أو التشهير بها، وإنما يقتصر النقاش المشروع، إن وجد، على حدود الواقعة ذات الاهتمام العام وبالقدر اللازم لها، مع بقاء الحماية القانونية قائمة من الذم والقدح والتحقير وانتهاك الخصوصية وخطاب الكراهية وأي صور أخرى من العنف الرقمي.

2. غير الشخصيات العامة

تشمل هذه الفئة النساء اللواتي لا يرتبطن بظهور عام أو نشاط يجعل حياتهن أو مواقفهن محلاً للاهتمام العام.

[8] Posetti, Julie, Diana Maynard, and Nabeelah Shabbir. *Guidelines for Monitoring Online Violence against Female Journalists*. Vienna: OSCE Representative on Freedom of the Media, 2023.

وغالباً ما ترتبط الانتهاكات الرقمية التي تتعرض لها هذه الفئة بالعلاقات الشخصية أو الأسرية أو المهنية، ومن أبرز صورها:

- الابتزاز الإلكتروني.
- نشر الصور أو التسجيلات الخاصة.
- انتحال الهوية الرقمية.
- انتهاك الخصوصية.
- الإساءة عبر الحسابات المغلقة أو المجموعات الخاصة.
- التهديد أو الملاحقة الرقمية.

وتتمتع هذه الفئة بأعلى درجات الحماية فيما يتعلق بالحياة الخاصة والبيانات الشخصية والصور والمراسلات الخاصة، ويُعد التدخل غير المشروع في هذه الجوانب أو نشرها دون موافقة صاحبها من أكثر صور الاعتداء على الخصوصية شيوعاً في البيئة الرقمية.

وفي بعض الحالات، قد تكون الآثار الاجتماعية والنفسية للعنف الرقمي على غير الشخصيات العامة أكثر حدة بسبب محدودية الخبرة في التعامل مع هذه المواقف، وضعف شبكات الدعم، وقلة الوعي بالإجراءات القانونية المتاحة أو بوسائل الحماية الرقمية المناسبة.

خامساً: أثر البيئة الرقمية[9]

تتميز البيئة الرقمية بخصائص تجعل آثار العنف الرقمي أكثر تعقيداً مقارنة بالعديد من الانتهاكات التقليدية، وهو ما ينعكس بصورة مباشرة على طبيعة الضرر الذي يلحق بالضحية وعلى آليات التعامل القانوني مع القضية.

ومن أبرز هذه الخصائص:

- السرعة الكبيرة في تداول المحتوى.
- سهولة إعادة النشر والمشاركة عبر منصات متعددة.
- صعوبة الحذف الكامل للمحتوى بعد نشره.
- إمكانية التخفي أو استخدام هويات أو حسابات وهمية.
- اتساع نطاق الجمهور والوصول إلى أعداد كبيرة من المستخدمين خلال فترة زمنية قصيرة.

[9] Association for Progressive Communications. *Technology-Related Violence against Women: A Briefing Paper*. Johannesburg: Association for Progressive Communications, 2015

- إمكانية الاحتفاظ بالمحتوى أو نسخه أو أرشفته أو إعادة تداوله بعد حذفه من المصدر الأصلي.
- استمرار المحتوى أو آثاره لفترات طويلة، بما يؤدي إلى استمرار الضرر حتى بعد انتهاء الواقعة الأصلية.

كما أن بعض المنصات الرقمية تعتمد على خوارزميات تعزز انتشار المحتوى الأكثر إثارة للتفاعل، الأمر الذي قد يؤدي أحياناً إلى زيادة انتشار المحتوى المسيء أو إعادة تداوله بصورة أوسع وأسرع مما هو متوقع.

ويضاف إلى ذلك أن الطبيعة العابرة للحدود للفضاء الرقمي قد تطرح تحديات إضافية تتعلق بتحديد هوية الفاعلين أو مكان وجودهم أو الجهة القضائية المختصة أو آليات تنفيذ القرارات والإجراءات القانونية.

ولذلك، ينبغي على المحامين والمحاميات إدراك الخصائص التقنية والقانونية للبيئة الرقمية عند التعامل مع هذه القضايا، ولا سيما فيما يتعلق بـ:

- سرعة توثيق الأدلة الرقمية والمحافظة عليها.
- تقييم مخاطر استمرار انتشار المحتوى الضار.
- تقديم الطلبات المستعجلة عند الحاجة.
- طلب اتخاذ التدابير القانونية المناسبة للحد من الضرر أو وقفه.
- التعامل مع الجهات المختصة والمنصات الرقمية عند الضرورة.
- مراعاة الجوانب النفسية والاجتماعية المترتبة على استمرار المحتوى أو إعادة تداوله.

إن فهم طبيعة البيئة الرقمية وخصائصها يُعد من المتطلبات الأساسية لبناء استراتيجية قانونية فعّالة في قضايا العنف الرقمي ضد النساء، ويسهم في تعزيز فرص الحماية القانونية وتقليل الآثار المترتبة على الضحايا.

الفصل الثاني: الإطار القانوني الأردني الناظم لقضايا العنف الرقمي ضد النساء

شهدت المنظومة القانونية الأردنية خلال السنوات الأخيرة تطوراً ملحوظاً في تنظيم الجرائم المرتكبة باستخدام الوسائل الرقمية، لا سيما مع صدور قانون الجرائم الإلكترونية رقم (17) لسنة 2023، والذي تضمّن نصوصاً تتعلق بعدد من الأفعال المرتبطة بالعنف الرقمي، مثل انتحال الهوية الرقمية، والابتزاز الإلكتروني، ونشر المحتوى الخاص، والذم والقدح والتحقير الإلكتروني، وخطاب الكراهية، وغيرها من الجرائم المرتكبة عبر الشبكة المعلوماتية أو وسائل التواصل الاجتماعي.

ومن المهم الإشارة إلى أن المشرع الأردني لم يضع تشريعاً خاصاً بالعنف الرقمي ضد النساء بوصفه وصفاً جرمياً مستقلاً، كما أن النصوص الجزائية ذات الصلة لا تميز في الحماية الجنائية بين الرجل والمرأة، وإنما تنصرف في معظمها إلى حماية "الشخص" بوجه عام. ومع ذلك، فإن خصوصية الآثار الاجتماعية والنفسية والمهنية التي قد تترتب على الجرائم الرقمية الواقعة على النساء تجعل من الضروري فهم هذه النصوص وتطبيقها في ضوء الاعتبارات المرتبطة بالنوع الاجتماعي.

ولا يقتصر التعامل القانوني مع قضايا العنف الرقمي ضد النساء على قانون الجرائم الإلكترونية فقط، بل قد يتطلب الرجوع إلى مجموعة من التشريعات الأخرى، من أبرزها:

- الدستور الأردني.
- قانون العقوبات.
- قانون أصول المحاكمات الجزائية.
- قانون حماية البيانات الشخصية والتشريعات ذات الصلة بالخصوصية.
- المبادئ الدستورية والقضائية المتعلقة بالحياة الخاصة وحرية التعبير والكرامة الإنسانية.

ويهدف هذا الفصل إلى تقديم عرض عملي لأبرز النصوص القانونية ذات الصلة، بما يساعد على فهم الإطار القانوني الناظم لهذه القضايا وتحديد التكييف القانوني الأنسب بحسب طبيعة كل حالة والأدلة المتوافرة فيها.

أولاً: الأساس الدستوري للحماية

يشكل الدستور الأردني المرجعية الأساسية للحماية القانونية من مختلف أشكال العنف والانتهاكات، بما في ذلك الانتهاكات المرتكبة باستخدام الوسائل الرقمية.

فقد أرسى الدستور مجموعة من المبادئ الدستورية ذات الصلة المباشرة بقضايا العنف الرقمي ضد النساء، ومن أبرزها:

- مبدأ المساواة أمام القانون وعدم التمييز بين الأردنيين في الحقوق والواجبات.[10]
- التزام الدولة بحماية المرأة من جميع أشكال العنف والتمييز وتمكينها من المشاركة الفاعلة في المجتمع.[11]
- حماية الحرية الشخصية.[12]
- حماية حرمة الحياة الخاصة.[13]
- تجريم أي اعتداء على الحقوق والحريات العامة أو على الحياة الخاصة للأفراد.

وتكتسب هذه المبادئ أهمية خاصة عند التعامل مع قضايا الابتزاز الإلكتروني، وانتهاك الخصوصية، ونشر الصور أو المعلومات الشخصية، والتشهير، وغيرها من صور العنف الرقمي التي تمس الكرامة الإنسانية والحياة الخاصة للنساء.

وينبغي على الممارسين القانونيين استحضار هذه المبادئ الدستورية عند بناء الحجج القانونية أو تفسير النصوص التشريعية ذات الصلة أو الدفع بحماية الحقوق الأساسية للضحايا.

ثانيًا: قانون الجرائم الإلكترونية رقم 17 لسنة 2023

يُعد قانون الجرائم الإلكترونية الإطار التشريعي الرئيسي المنظم للجرائم المرتكبة باستخدام الوسائل الرقمية في الأردن. وقد تضمّن عدداً من النصوص التي يمكن الاستناد إليها في التعامل مع قضايا العنف الرقمي ضد النساء.

1. انتحال الهوية الرقمية والحسابات الوهمية

تنص المادة (5) من قانون الجرائم الإلكترونية على تجريم إنشاء حسابات أو صفحات أو قنوات ونسبها زوراً إلى شخص طبيعي أو معنوي.[14]

---

[10] نصت المادة 6 من الدستور الأردني لسنة 1052 وتعديلاته على (1) الاردنيون امام القانون سواء لا تمييز بينهم في الحقوق والواجبات وان اختلفوا في العرق او اللغة او الدين. (2) الدفاع عن الوطن وأرضه ووحدة شعبه والحفاظ على السلم الاجتماعي واجب مقدس على كل أردني. (3) تكفل الدولة العمل والتعليم ضمن حدود امكانياتها وتكفل الطمانينة وتكافؤ الفرص لجميع الاردنيين. (4) الأسرة أساس المجتمع قوامها الدين والأخلاق وحب الوطن، يحفظ القانون كيانها الشرعي ويقوي أواصرها وقيمها. (5) يحمي القانون حقوق الأشخاص ذوي الإعاقة ويعزز مشاركتهم واندماجهم في مناحي الحياة المختلفة ، كما يحمي الأمومة والطفولة والشيخوخة ويرعى النشء ويمنع الإساءة والاستغلال .(6) تكفل الدولة تمكين المرأة ودعمها للقيام بدور فاعل في بناء المجتمع بما يضمن تكافؤ الفرص على أساس العدل والإنصاف وحمايتها من جميع أشكال العنف والتمييز .(7) تكفل الدولة تعزيز قيم المواطنة والتسامح وسيادة القانون وتكفل ضمن حدود امكانياتها تمكين الشباب في المساهمة في الحياة السياسية والاقتصادية والاجتماعية والثقافية وتنمية قدراتهم ودعم ابداعاتهم وابتكاراتهم .

[11] المرجع السابق.

[12] نصت المادة 7/1 من الدستور الأردني على أن الحرية الشخصية مصونة.

[13] نصت المادة 18 من الدستور الأردني على أن تعتبر جميع المراسلات البريدية والبرقية والمخاطبات الهاتفية وغيرها من وسائل الاتصال سرية لا تخضع للمراقبة أو الإطلاع أو التوقيف أو المصادرة إلا بأمر قضائي وفق أحكام القانون.

[14] نصت المادة 5 من قانون الجرائم الالكترونية على " يعاقب كل من قام بإنشاء حساب أو صفحة أو مجموعة أو قناة أو ما يماثلها على منصات التواصل الاجتماعي ونسبها زورا إلى شخص طبيعي أو معنوي بالحبس مدة لا تقل عن ثلاثة أشهر أو بغرامة لا تقل عن (1500) ألف وخمسمائة دينار ولا تزيد على (15000) خمسة عشر ألف دينار أو بكلتا هاتين العقوبتين."

وتبرز أهمية هذا النص في الحالات التي يتم فيها:

- إنشاء حسابات وهمية باسم الضحية.
- استخدام صور الضحية أو بياناتها الشخصية دون موافقتها.
- انتحال شخصية الضحية بقصد الإساءة إليها أو تشويه سمعتها.
- استخدام الحسابات الوهمية لاستدراج الآخرين أو التواصل باسم الضحية.

وغالباً ما ترتبط هذه الأفعال بجرائم أخرى مثل الذم والقدح، أو الابتزاز، أو خطاب الكراهية، أو اغتيال الشخصية.

وعند التعامل مع هذه القضايا، ينبغي على المحامي التركيز على إثبات العلاقة بين الحساب أو الصفحة محل الشكوى وبين الشخص الذي قام بإنشائها أو إدارتها، والاستفادة من الأدلة الفنية والبيانات الرقمية المتاحة.

2. الذم والقدح والتحقير الإلكتروني

تشكل جرائم الذم والقدح والتحقير من أكثر الجرائم الرقمية شيوعاً في الممارسة العملية. ويُرجع في تعريف الذم والقدح إلى الأحكام الواردة في قانون العقوبات الأردني،[15] في حين جرّم قانون الجرائم الإلكترونية ارتكاب هذه الأفعال باستخدام الوسائل الرقمية والشبكات المعلوماتية ومنصات التواصل الاجتماعي. وتُستخدم المادة (15) من القانون في بعض الحالات المتعلقة بالذم والقدح الإلكتروني أو نشر الأخبار الكاذبة عبر المنصات الرقمية.[16]

وتظهر هذه الجرائم في صور متعددة، منها:

- نشر ادعاءات أو معلومات تمس السمعة أو الكرامة.
- توجيه عبارات مهينة أو حاطة من الكرامة.
- نشر محتوى يتضمن تحقيراً أو إساءة متعمدة.
- إعادة نشر المحتوى المسيء أو تداوله على نطاق واسع.

وفي هذا السياق، ينبغي على المحامي التمييز بين:

---

[15] عرف المشرع الاردني الذم والقدح في المادة 188 من قانون العقوبات والتي تنص: (1) الذم: هو اسناد مادة معينة الى شخص - ولو في معرض الشك والاستفهام - من شانها ان تنال من شرفه وكرامته او تعرضه الى بغض الناس واحتقارهم سواء اكانت تلك المادة جريمة تستلزم العقاب ام لا. (2) القدح : هو الاعتداء على كرامة الغير او شرفه او اعتباره - ولو في معرض الشك والاستفهام - من دون بيان مادة معينة. (3) واذا لم يذكر عند ارتكاب جرائم الذم والقدح اسم المعتدى عليه صريحا او كانت الاسنادات الواقعة مبهمة، ولكنه كانت هنالك قرائن لا يبقى معها تردد في نسبة تلك الاسنادات الى المعتدى عليه وفي تعيين ماهيتها ، وجب عندئذ ان ينظر الى مرتكب فعل الذم او القدح كانه ذكر اسم المعتدى عليه وكان الذم او القدح كان صريحا من حيث الماهية ".

[16] يعاقب المشرع بموجب قانون الجرائم الالكترونية على الذم والقدح الواقع بواسطة الوسائل الالكترونية بموجب المادة 15 منه والتي تنص " يعاقب كل من قام قصدا بإرسال أو اعادة إرسال أو نشر بيانات أو معلومات عن طريق الشبكة المعلوماتية أو تقنية المعلومات أو نظام المعلومات أو الموقع الإلكتروني أو منصات التواصل الاجتماعي تنطوي على أخبار كاذبة تستهدف الأمن الوطني والسلم المجتمعي أو ذم او قدح او تحقير أي شخص بالحبس مدة لا تقل عن ثلاثة أشهر أو بغرامة لا تقل عن (5000) خمسة آلاف دينار ولا تزيد على (20000) عشرين ألف دينار أو بكلتا هاتين العقوبتين.

- النقد المباح المرتبط بالمصلحة العامة.
- حرية التعبير المكفولة قانوناً.
- الأفعال التي تتجاوز حدود النقد المشروع وتشكل ذماً أو قدحاً أو تحقيراً يعاقب عليه القانون.

ويكتسب هذا التمييز أهمية خاصة في القضايا المتعلقة بالشخصيات العامة أو العاملات في المجال السياسي أو الإعلامي أو الحقوقي.

3. اغتيال الشخصية عبر الوسائل الرقمية

أفرد قانون الجرائم الإلكترونية نصاً خاصاً لاغتيال الشخصية من خلال المادة 16،[17] وهو من المستحدثات التشريعية المهمة في القانون الأردني.

ورغم أن المشرع لم يضع تعريفاً تشريعياً محدداً لمفهوم اغتيال الشخصية، إلا أنه يُقصد به بصورة عامة الأفعال الرقمية التي تستهدف النيل من سمعة الشخص أو مصداقيته أو مكانته الاجتماعية أو المهنية من خلال نشر معلومات أو ادعاءات أو محتوى مضلل أو مجتزأ أو غير صحيح بقصد الإضرار به.

وتُعد النساء العاملات في الشأن العام، والإعلام، والسياسة، والعمل الحقوقي، وصناعة المحتوى الرقمي من أكثر الفئات عرضة لهذا النوع من الاعتداءات.

وعند التعامل مع قضايا اغتيال الشخصية، ينبغي للمحامين الانتباه إلى:

- طبيعة المحتوى المنشور.
- توقيت النشر والظروف المحيطة به.
- طبيعة الضرر الواقع على الضحية.
- وجود قصد للإساءة أو الإضرار.
- التمييز بين النقد المباح واغتيال الشخصية.
- مراعاة معايير حرية التعبير في القضايا ذات الصلة بالشأن العام.

3. الابتزاز والتهديد الإلكتروني[18]

[17] تنص المادة 16 من قانون الجرائم الالكترونية على "كل من أشاع أو عزا أو نسب قصدا دون وجه حق إلى أحد الأشخاص أو ساهم في ذلك عن طريق الشبكة المعلوماتية أو تقنية المعلومات أو نظام المعلومات أو الموقع الإلكتروني أو منصات التواصل الاجتماعي أفعالا من شأنها اغتيال شخصيته يعاقب بالحبس مدة لا تقل عن ثلاثة أشهر أو بغرامة لا تقل عن (5000) خمسة آلاف دينار ولا تزيد على (20000) عشرين ألف دينار أو بكلتا هاتين العقوبتين.

[18] يُعرّف الابتزاز من منظور علمي تكاملي يجمع بين علمي النفس والاجتماع بأنه سلوك تلاعبي عدواني قائم على استغلال ميزان القوى غير المتكافئ لفرض السيطرة وتحقيق مآرب نفعية؛ حيث يتخذ سيكولوجياً وسلوكياً نمطاً من الاستغلال العاطفي والنفسي المنهجي الذي يستهدف إثارة مشاعر الخوف، والذنب، والقلق الحاد لدى الضحية من خلال رصد نقاط ضعفها واستغلالها بشكل متكرر، مما يؤدي إلى شلّ قدراتها الإدراكية والتفكير المنطقي، ويدفعها للرضوخ التام كوسيلة دفاعية وحيدة للتخلص من الضغط النفسي والانتهازي المسلط عليها. حول هذا الموضوع انظر:

تنص المادة (18) من القانون على تجريم الابتزاز أو التهديد باستخدام الوسائل الرقمية أو منصات التواصل الاجتماعي.[19]

وتُعد هذه الجرائم من أكثر الجرائم ارتباطاً بقضايا العنف الرقمي ضد النساء، نظراً لما قد يترتب عليها من آثار نفسية واجتماعية ومهنية خطيرة على الضحية.

وتظهر هذه الجرائم في صور متعددة، من أبرزها:

- التهديد بنشر الصور أو الفيديوهات أو التسجيلات الخاصة.
- التهديد بنشر المحادثات أو المراسلات الشخصية.
- إجبار الضحية على القيام بفعل أو الامتناع عنه.
- طلب منفعة مالية أو شخصية مقابل عدم النشر أو عدم الإفصاح عن معلومات معينة.
- التهديد بإسناد أمور خادشة للشرف أو الاعتبار.

وتكتسب هذه الجرائم خصوصية خاصة عندما تكون الضحية امرأة، نظراً لما قد يترتب على النشر أو التهديد بالنشر من آثار اجتماعية أو أسرية أو مهنية قد تفوق أحياناً الضرر المباشر الناتج عن الفعل الإجرامي ذاته.

ومن الناحية القانونية، تقوم جريمة الابتزاز على توافر مجموعة من العناصر الأساسية، أهمها:[20]

- وجود تهديد أو ضغط موجه إلى المجني عليها.
- ارتباط التهديد بطلب منفعة أو تحقيق غاية غير مشروعة.
- توافر القصد الجرمي لدى الفاعل، المتمثل في علمه بطبيعة فعله واتجاه إرادته إلى تحقيق المنفعة أو الضغط على الضحية.

وعند التعامل مع هذه القضايا، ينبغي على المحامين والمحاميات إعطاء أولوية خاصة لتوثيق الرسائل والمحادثات والتسجيلات والبيانات الرقمية التي تثبت التهديد أو الابتزاز، والعمل على اتخاذ الإجراءات القانونية بصورة سريعة للحد من تفاقم الضرر.

4. نشر الصور أو التسجيلات أو المحتوى الخاص

Susan Forward and Donna Frazier, Emotional Blackmail: When the People in Your Life Use Fear, Obligation, and Guilt to Manipulate You (New York: HarperCollins Publishers, 1997).

[19] تنص المادة 18 من قانون الجرائم الالكترونية على "(أ) يعاقب بالحبس مدة لا تقل عن سنة وبغرامة لا تقل عن (3000) ثلاثة آلاف دينار ولا تزيد على (6000) ستة آلاف دينار كل من ابتز او هدد شخصاً اخر لحمله على القيام بفعل او الامتناع عنه او للحصول على اي منفعة جراء ذلك من خلال استخدام نظام المعلومات او الشبكة المعلوماتية او موقع الكتروني او منصة تواصل اجتماعي او بأي وسيلة من وسائل تقنية المعلومات.
(ب) تكون العقوبة الاشغال المؤقتة وبغرامة لا تقل عن (5000) خمسة آلاف دينار ولا تزيد على (10000) عشرة آلاف دينار اذا كان التهديد بارتكاب جريمة او بإسناد امور خادشة للشرف او الاعتبار وكان ذلك مصحوباً بطلب صريح او ضمني للقيام بعمل او الامتناع عنه .

[20] الحكم رقم 1392 لسنة 2023 - بداية اربد بصفتها الإستئنافية الصادر بتاريخ 2023-02-22

تعالج المادة (20) من القانون الحالات المتعلقة بنشر أو استخدام الصور أو الفيديوهات أو التسجيلات الخاصة بقصد التشهير أو الإساءة أو الحصول على منفعة.[21]

يُعد نشر الصور أو التسجيلات أو الفيديوهات أو المعلومات الخاصة دون موافقة صاحبها من أكثر صور العنف الرقمي انتشاراً وتأثيراً على النساء.

وقد جرم قانون الجرائم الإلكترونية نشر أو استخدام الصور أو التسجيلات أو الفيديوهات التي يحرص الشخص على صونها وعدم إظهارها للعامة متى كان ذلك بقصد التشهير أو الإساءة أو الحصول على منفعة.

كما جرم القانون إجراء أي تعديل أو تركيب أو معالجة رقمية على الصور أو التسجيلات أو الفيديوهات بقصد الإساءة أو التشهير أو تحقيق منفعة غير مشروعة.

وتشمل هذه الأفعال على سبيل المثال:

- نشر الصور أو الفيديوهات الخاصة دون موافقة الضحية.
- نشر أو إعادة نشر التسجيلات الشخصية.
- تعديل الصور أو الفيديوهات بصورة مسيئة.
- تركيب محتوى مضلل أو مفبرك.
- استخدام أدوات الذكاء الاصطناعي لإنتاج محتوى مزيف أو معدّل بقصد الإضرار بالضحية.
- نشر أو تداول ما يعرف بالصور أو التسجيلات الحميمة دون موافقة أصحابها.

وتبرز أهمية هذا النص القانوني في حماية الخصوصية الرقمية للنساء، خاصة في الحالات التي يتم فيها استغلال العلاقات الشخصية أو الأسرية أو المهنية للحصول على محتوى خاص ثم استخدامه للإساءة أو الابتزاز أو التشهير.

5. خطاب الكراهية عبر الوسائل الرقمية

يشير خطاب الكراهية إلى أشكال التعبير أو المحتوى الذي يتضمن التحريض على الكراهية أو العنف أو التمييز أو الإقصاء تجاه أفراد أو مجموعات بسبب صفاتهم أو هوياتهم أو انتماءاتهم.[22]

---

[21] تنص المادة 20 من قانون الجرائم الالكترونية على "(أ) يعاقب بناء على الشكوى بالحبس مدة لا تقل عن ثلاثة أشهر وبغرامة لا تقل عن (20000) عشرين ألف دينار ولا تزيد على (40000) أربعين ألف دينار كل من استخدم شبكة معلوماتية أو تقنية المعلومات أو نظام المعلومات أو موقعا الكترونيا أو منصة تواصل اجتماعي لنشر تسجيل أو صورة أو فيديو لما يحرص الشخص على صونه وعدم اظهاره أو كتمانه عن العامة بقصد التشهير أو الإساءة أو الحصول على أية منفعة من جراء ذلك وإن كان قد حصل على تلك الصور أو التسجيلات أو الفيديوهات بصورة مشروعة. (ب) يعاقب بالحبس مدة لا تقل عن سنتين وبغرامة لا تقل عن (25000) خمسة وعشرين ألف دينار ولا تزيد على (50000) خمسين ألف دينار كل من استخدم شبكة معلوماتية أو تقنية المعلومات أو نظام المعلومات أو موقعا الكترونيا أو منصة تواصل اجتماعي لإجراء تركيب أو تعديل أو معالجة على تسجيل أو صورة أو مشهد أو فيديو لما يحرص الشخص على صونه وعدم اظهاره للعامة بقصد التشهير أو الإساءة أو الحصول على منفعة من جراء ذلك.

[22] يُقصد بخطاب الكراهية أي نوع من أنواع التواصل، الشفهي أو الكتابي أو السلوكي، الذي يهاجم أو يستخدم لغة ازدرائية أو تمييزية بالإشارة إلى شخص أو مجموعة من الأشخاص على أساس هويتهم، مثل الدين أو الأصل الإثني أو الجنسية أو العرق أو اللون أو النسب أو الجنس أو أي عامل

وقد جرم قانون الجرائم الإلكترونية نشر المحتوى الذي من شأنه إثارة الفتنة أو النعرات أو الحض على الكراهية أو الدعوة إلى العنف أو تبريره أو المساس بالسلم المجتمعي باستخدام الوسائل الرقمية من خلال المادة 17.[23]

وفي سياق العنف الرقمي ضد النساء، قد يظهر خطاب الكراهية في صور متعددة، منها:

- التحريض على العنف ضد النساء.
- الدعوة إلى إقصائهن من الحياة العامة أو المهنية.
- نشر محتوى يحض على التمييز أو الكراهية بسبب الجنس أو النوع الاجتماعي.
- استهداف النساء بحملات منظمة تتضمن محتوى عدائياً أو مهيناً أو تحريضياً.

ويجب التنبه إلى أن التكييف القانوني النهائي لأي محتوى باعتباره خطاب كراهية يخضع لتقدير القضاء في ضوء طبيعة العبارات المستخدمة، وسياق النشر، ومدى تأثيره على السلم المجتمعي أو الحقوق المحمية قانوناً.[24]

ثالثاً: تشريعات أخرى ذات صلة

إلى جانب قانون الجرائم الإلكترونية، قد تستدعي بعض قضايا العنف الرقمي ضد النساء الرجوع إلى تشريعات أخرى بحسب طبيعة الواقعة.

1. قانون العقوبات

يُرجع إلى قانون العقوبات في العديد من المسائل المتعلقة بالذم والقدح والتحقير والتهديد والابتزاز وغيرها من الجرائم التي قد ترتكب باستخدام الوسائل الرقمية، خاصة فيما يتعلق بالتعريفات القانونية والأركان الجرمية العامة.

2. قانون أصول المحاكمات الجزائية

ينظم قانون أصول المحاكمات الجزائية إجراءات الشكوى والتحقيق وجمع الأدلة وسماع الشهود والطعن في القرارات والأحكام، وهو الإطار الإجرائي الذي يحكم سير الدعوى الجزائية في قضايا العنف الرقمي.

3. قانون حماية البيانات الشخصية والتشريعات المتعلقة بالخصوصية

آخر محدِّد للهوية. ومع أن القانون الدولي لا يضع تعريفاً قانونياً موحداً لخطاب الكراهية، فإن مجابهته لا تعني تقييد حرية التعبير بل منع تصعيده إلى عنف. الأمم المتحدة، استراتيجية الأمم المتحدة وخطة عملها بشأن خطاب الكراهية (نيويورك: الأمم المتحدة، 2019).

[23] تنص المادة 17 من قانون الجرائم الالكترونية على " يعاقب كل من قام قصدا باستخدام الشبكة المعلوماتية أو تقنية المعلومات أو نظام المعلومات أو موقع الكتروني أو منصة تواصل اجتماعي لنشر ما من شأنه إثارة الفتنة أو النعرات أو تستهدف السلم المجتمعي أو الحض على الكراهية او الدعوة إلى العنف أو تبريره أو ازدراء الأديان بالحبس من سنة إلى ثلاث سنوات أو بغرامة لا تقل عن (5000) خمسة آلاف دينار ولا تزيد على (20000) عشرين ألف دينار أو بكلتا هاتين العقوبتين."

[24] استقر الاجتهاد القضائي الأردني على تحديد مضمون فكرة مفهوم السلم المجتمعي (هو حالة السلم والوئام داخل المجتمع ويعتبر هذا المفهوم من المفاهيم التي تخضع لتقدير قاضي الموضوع ويرتبط هذا التقدير بفحوى العبارات التي تم نشرها وزمانها ومكانها. الحكم رقم 953 لسنة 2024 - صلح جزاء عمان، الصادر بتاريخ 17-01-2024

تكتسب حماية البيانات الشخصية أهمية متزايدة في ظل التطور الرقمي المتسارع، خاصة في القضايا المرتبطة بجمع البيانات الشخصية أو معالجتها أو نشرها أو تداولها دون موافقة أصحابها.

كما تشكل المبادئ القانونية المتعلقة بحماية الحياة الخاصة والبيانات الشخصية مرجعاً مهماً عند التعامل مع قضايا نشر الصور أو المعلومات أو التسجيلات الخاصة.

4. المبادئ الدستورية والقضائية

تُعد المبادئ الدستورية المتعلقة بالكرامة الإنسانية والحياة الخاصة والمساواة أمام القانون وحرية التعبير من العناصر الأساسية التي يجب مراعاتها عند تفسير النصوص القانونية وتطبيقها على قضايا العنف الرقمي ضد النساء.

كما أن الاجتهادات القضائية الصادرة عن المحاكم الأردنية تسهم في توضيح كيفية تطبيق النصوص القانونية على الوقائع المستجدة المرتبطة بالفضاء الرقمي والتطورات التقنية الحديثة.

خلاصة عملية

لا يعتمد النجاح في التعامل مع قضايا العنف الرقمي ضد النساء على معرفة النصوص القانونية فقط، وإنما على القدرة على اختيار التكييف القانوني الصحيح، وسرعة جمع الأدلة الرقمية والمحافظة عليها، وتقييم المخاطر التي تواجه الضحية، والاستفادة من مختلف الأدوات والإجراءات القانونية المتاحة لحمايتها والحد من استمرار الضرر الواقع عليها.

الفصل الثالث: الأدلة الإلكترونية في قضايا العنف الرقمي ضد النساء

تُعد الأدلة الإلكترونية الركيزة الأساسية لإثبات الجرائم المرتكبة باستخدام الوسائل الرقمية، وتمثل في العديد من قضايا العنف الرقمي ضد النساء الدليل الرئيسي أو الوحيد لإثبات الواقعة وتحديد هوية الجاني وربط الأفعال المرتكبة به.

وتتميز الأدلة الإلكترونية بطبيعة خاصة تختلف عن الأدلة التقليدية، إذ قد تكون عرضة للحذف أو التعديل أو الإخفاء خلال فترة زمنية قصيرة، كما قد تكون موزعة بين عدة أجهزة أو حسابات أو منصات رقمية داخل المملكة أو خارجها. ولذلك فإن سرعة التعامل مع هذه الأدلة وتوثيقها والمحافظة عليها تعد من العناصر الحاسمة في نجاح الإجراءات القانونية.

يُقصد بالأدلة الرقمية (Digital Evidence) كل معلومة أو بيانات ذات قيمة إثباتية يتم إنشاؤها أو تخزينها أو معالجتها أو نقلها أو استخراجها بواسطة وسيلة إلكترونية أو رقمية، ويمكن الاستناد إليها أمام الجهات القضائية لإثبات الجريمة أو نفيها. [25]. وينسجم هذا التعريف الفقهي مع التوجه التشريعي الأردني الحديث، وتحديداً ما نصت عليه المادة (36) من قانون الجرائم الإلكترونية الأردني رقم 17 لسنة 2023، والمادة (5) من قانون المعاملات الإلكترونية الأردني رقم 15 لسنة 2015، اللتان أضفتا الحجية القانونية الكاملة على السجلات والبيانات الرقمية المستخرجة أمام جهات القضاء.

ويهدف هذا الفصل إلى التعريف بأهم أنواع الأدلة الإلكترونية، وشروط قبولها أمام القضاء، والأخطاء الشائعة التي قد تؤدي إلى إضعاف قيمتها الإثباتية، إضافة إلى الإجراءات القانونية المتعلقة بحفظ الأدلة وإزالة المحتوى الضار.

أولاً: أنواع الأدلة الإلكترونية في قضايا العنف الرقمي ضد النساء

قد تتخذ الأدلة الإلكترونية أشكالاً متعددة بحسب طبيعة الواقعة والأداة المستخدمة في ارتكابها، ومن أبرزها:

1. المعرفات الرقمية

وهي البيانات التي تساعد على تحديد هوية المستخدم أو الجهاز أو الحساب المرتبط بالفعل الجرمي، ومن أبرزها:

- العنوان البروتوكولي (IP Address) : هو معرف رقمي فريد يُمنح لكل جهاز (حاسوب، هاتف، طابعة) عند اتصاله بشبكة الإنترنت أو بشبكة محلية. يعمل هذا العنوان بمثابة "العنوان البريدي الرقمي" للجهاز، حيث يتيح للشبكة التعرف على مكان الجهاز وإرسال واستقبال البيانات من وإلى الوجهة الصحيحة.[26]

[25] جميل عبد الباقي الصغير، أدلة الإثبات الجنائي والتكنولوجيا الحديثة (القاهرة: دار النهضة العربية، 2018)، 112. محمد أمين الخوالدة، الدليل الإلكتروني وحجيته في الإثبات الجنائي: دراسة مقارنة (عمان: دار الثقافة للنشر والتوزيع، 2021)، 45.

[26] Internet Corporation for Assigned Names and Numbers (ICANN), Glossary of Standard Internet Terms (Los Angeles: ICANN, 2022), 14.

- الرقم الدولي المميز للجهاز (IMEI) : هو رقم تسلسلي فريد عالمياً ومكون عادة من 15 رقماً، يُخصص لتمييز الهواتف والأجهزة الخلوية عن بعضها البعض. هذا الرقم يرتبط بالجهاز (العتاد الصلب) نفسه وليس بشريحة الاتصال (SIM)، ويُستخدم لتتبع الهواتف، والتحقق من هويتها على شبكات الاتصال، وقفل الأجهزة المسروقة لمنعها من العمل. [27]

- أسماء المستخدمين (Usernames): هو اسم أو سلسلة من الحروف والأرقام يختارها الشخص (أو تُمنح له) لتمثّل هويته العلنية عند تسجيل الدخول إلى موقع، تطبيق، أو نظام تشغيل. يُشترط أن يكون فريداً داخل تلك المنصة فقط، ويُستخدم كواجهة مرئية للتعرف على الحساب وضمان عدم تداخل حسابات المستخدمين. [28]

- معرفات الحسابات الرقمية (User IDs): هو رمز رقمي أو أبجدي-رقمي فريد **يولده النظام أو خادم قاعدة البيانات تلقائياً** ويربطه بحساب المستخدم فور إنشائه. على عكس "اسم المستخدم" الذي يمكن تعديله، فإن معرف الحساب (User ID) يبقى ثابتاً ولا يتغير أبداً، وهو المعيَّن الأساسي الذي تعتمده الأنظمة والبرمجيات داخلياً للتعرف على بيانات المستخدم وسلوكه وربط عملياته التشغيلية. [29]

- عناوين البريد الإلكتروني: هو معرف رقمي فريد ومقنن دولياً، يُخصص لصندوق بريد إلكتروني محدد على شبكة الإنترنت يستطيع استقبال وإرسال الرسائل الرقمية. يتكون العنوان دائماً من جزأين أساسيين يفصل بينهما الرمز @؛ الجزء الأول هو اسم المستخدم المعين اختيارياً، والجزء الثاني هو اسم النطاق (Domain Name) الذي يحدد الخادم (Server) المستضيف للحساب. ويُعد البريد الإلكتروني وسيلة رسمية لتبادل البيانات والمعاملات، ورابطاً أساسياً لتوثيق الهويات الرقمية وإنشاء الحسابات على منصات التواصل الاجتماعي. [30]

وتكتسب هذه البيانات أهمية خاصة في القضايا التي يستخدم فيها الجاني حسابات وهمية أو أسماء مستعارة.

2. بيانات الاتصال المحفوظة

وتشمل السجلات الإلكترونية التي توثق عمليات التواصل الرقمي، مثل:

- سجلات المكالمات.
- سجلات الرسائل النصية.
- سجلات تطبيقات التراسل الفوري.
- سجلات الدخول والخروج من الحسابات.
- أوقات الاتصال ومدته.

[27] GSM Association (GSMA), Technical Standards for Mobile Device Identifiers (London: GSMA, 2021), 8.

[28] National Cyber Security Centre (NCSC), *Principles of Identity and Access Management* (London: NCSC, 2023), 22.

[29] Institute of Electrical and Electronics Engineers (IEEE), Standards for Digital Identity Software Architecture (New York: IEEE, 2020), 47.

[30] Internet Engineering Task Force (IETF), Architectural Principles of the Internet Mail System (Fremont: IETF, 2021), 33.

وقد تساعد هذه البيانات في إثبات التواصل بين الأطراف أو تحديد توقيت ارتكاب الجريمة.

3. المحتوى الرقمي المباشر

ويشمل المحتوى الذي يشكل موضوع الجريمة أو جزءاً من عناصرها، مثل:

- الرسائل النصية.
- المحادثات الإلكترونية.
- رسائل البريد الإلكتروني.
- التسجيلات الصوتية.
- الصور الرقمية.
- مقاطع الفيديو.
- المنشورات والتعليقات على منصات التواصل الاجتماعي.

وتُعد هذه الفئة من أكثر الأدلة استخداماً في قضايا الابتزاز الإلكتروني والتشهير وانتهاك الخصوصية وخطاب الكراهية.

4. بيانات الموقع الجغرافي

تشمل البيانات التي تساعد على تحديد مكان وجود المستخدم أو الجهاز، ومن ذلك:

- بيانات نظام تحديد المواقع (GPS): هي بيانات رقمية دقيقة تشتمل على الإحداثيات الجغرافية (خطوط الطول، دوائر العرض، والارتفاع) بالإضافة إلى الطابع الزمني. يتم توليد هذه البيانات عبر التقاط الأجهزة (كالهواتف والسيارات) لإشارات الأقمار الصناعية، وتُستخدم لتحديد الموقع الجغرافي الفعلي للجهاز ومسار حركته بدقة في وقت محدد.[31]
- البيانات الوصفية المرفقة بالصور والملفات (Metadata): تُعرف علمياً بأنها "بيانات عن البيانات"؛ وهي معلومات رقمية خفية ومدمجة تلقائياً داخل الملف أو الصورة عند إنشائه. تتضمن هذه البيانات تفاصيل فنية هامة مثل: تاريخ ووقت الالتقاط، نوع الجهاز المستخدم، إعدادات الكاميرا، وحجم الملف، وفي كثير من الأحيان تتضمن الموقع الجغرافي (GPS) الذي التقطت فيه الصورة، مما يجعلها أداة حاسمة في التحقيق الرقمي.[32]
- بيانات مواقع الاتصال بالشبكات: هي معلومات رقمية تُسجلها شبكات الاتصال (مثل أبراج التغطية الخلوية أو نقاط بث الواي فاي Wi-Fi Router) عند اتصال جهازك بها. هذه البيانات لا تعتمد على الأقمار الصناعية (GPS)،

[31] National Coordination Office for Space-Based Positioning, Navigation, and Timing (PNT), Global Positioning System Standard Positioning Service Performance Standard (Washington, DC: PNT, 2020), 19.

[32] National Institute of Standards and Technology (NIST), Guide to Digital Forensic Examination of Information Systems (Gaithersburg: NIST, 2022), 42.

بل تحدد موقع الجهاز بشكل تقريبي بناءً على النطاق الجغرافي لبرج الاتصال الذي التقط إشارة الهاتف، وتُستخدم لتتبع وتحديد مكان الأجهزة عبر سجلات شركات الاتصال.[33]

وقد تكون هذه البيانات ذات أهمية في ربط شخص معين بمكان أو زمان ارتكاب الفعل الجرمي.

5. الأدلة الفنية والتقارير الرقمية

وتشمل:

- التقارير الفنية الصادرة عن الجهات المختصة.
- تقارير خبراء الأدلة الجنائية الرقمية.
- نتائج الفحص الفني للأجهزة والحسابات.
- تقارير مزودي الخدمات والمنصات الرقمية.

وغالباً ما تلعب هذه الأدلة دوراً محورياً في تفسير البيانات الرقمية وإثبات سلامتها.

ثانياً: حجية الأدلة الإلكترونية في القانون الأردني

اعترف المشرع الأردني صراحة بحجية الأدلة الإلكترونية أمام الجهات القضائية.

فقد نصت المادة (36) من قانون الجرائم الإلكترونية رقم (17) لسنة 2023 على حجية الأدلة المقدمة أو المستمدة أو المستخرجة من الأجهزة أو المعدات أو الوسائط أو الشبكات المعلوماتية أو أنظمة المعلومات أو برامج الحاسوب أو مزودي الخدمة أمام الجهات القضائية.[34]

كما أقرت المادة ذاتها حجية البيانات والمعلومات الواردة من الجهات الرسمية في الدول الأخرى، واعتبرت العنوان البروتوكولي (IP Address) وسيلة من وسائل الإثبات أمام الجهات القضائية.

وتكمن أهمية هذه المادة في تأكيد القيمة القانونية للأدلة الرقمية وإزالة أي شك بشأن إمكانية الاستناد إليها في التحقيق والمحاكمة.

كما جرّم المشرع إخفاء الأدلة الإلكترونية أو العبث بها أو إتلافها أو إعاقة الجهات المختصة عن الوصول إليها، لما لذلك من أثر مباشر على سير العدالة وإثبات الجرائم الإلكترونية.

---

[33] Federal Communications Commission (FCC), Standards for Location-Based Services and Network Tracking (Washington, DC: FCC, 2021), 55.

[34] تنص المادة 36 من قانون الجرائم الالكترونية على " (أ) يكون للأدلة المقدمة أو المستمدة أو المستخرجة من الأجهزة أو المعدات أو الوسائط أو الشبكة المعلوماتية أو تقنية المعلومات أو نظام المعلومات أو برنامج الحاسوب أو مزود الخدمة حجية الاثبات أمام الجهات القضائية. (ب) تكون للبيانات والمعلومات التي يتم الحصول عليها من الجهات الرسمية من دول أخرى حجية الاثبات أمام الجهات القضائية الأردنية. (ج) لغايات تطبيق أحكام هذا القانون يعتبر العنوان البروتوكولي وسيلة من وسائل الاثبات أمام الجهات القضائية. (د) يعاقب كل من أخفى أو عبث أو أتلف الأدلة المشار اليها في هذه المادة أو آثارها أو أعاق عمل الجهات المختصة للوصول الى تلك الادلة بالحبس مدة لا تقل عن ثلاثة أشهر.

ثالثاً: شروط قبول الدليل الإلكتروني أمام القضاء

رغم الاعتراف بحجية الأدلة الإلكترونية، إلا أن قبولها أمام القضاء يتطلب توافر مجموعة من الشروط الأساسية لضمان سلامتها ومصداقيتها.

1. الأصالة والسلامة

يجب أن يكون الدليل الإلكتروني أصلياً وغير معدل أو محرف أو مفبرك.

ويتحقق ذلك عادة من خلال الفحص الفني المتخصص واستخدام الوسائل التقنية التي تثبت سلامة البيانات وعدم العبث بها، بما في ذلك التحقق من القيم الرقمية الخاصة بالملفات (Hash Values) عند الاقتضاء.

2. مشروعية الحصول على الدليل

يشترط أن يكون الحصول على الدليل قد تم وفقاً لأحكام القانون.

ومن الأمثلة على ذلك:

- الحصول على إذن من المدعي العام أو المحكمة المختصة عندما يتطلب القانون ذلك.[35]
- تسليم الضحية للجهاز أو البيانات طوعاً.
- الحصول على البيانات من الجهات المختصة أو مزودي الخدمة وفق الإجراءات القانونية.

وقد يؤدي الحصول على الدليل بوسائل غير مشروعة إلى الطعن في مشروعيته أو استبعاده من البينة.

3. استمرارية سلسلة الحيازة

يقصد بسلسلة الحيازة توثيق جميع الأشخاص الذين تعاملوا مع الدليل الإلكتروني منذ ضبطه وحتى تقديمه أمام المحكمة.

ويهدف ذلك إلى ضمان عدم العبث بالدليل أو استبداله أو التعديل عليه خلال مراحل التحقيق والفحص الفني.[36]

[35] في القانون الأردني والمقارن، أي دليل يُستمد من إجراء باطل (مثل التفتيش دون إذن أو اختراق الحسابات) يكون باطلاً وفق قاعدة "ما بني على باطل فهو باطل"، وتحديداً المادة (147) من قانون أصول المحاكمات الجزائية الأردني، والمادة (34) من قانون الجرائم الإلكترونية الأردني رقم 17 لسنة 2023 التي تنظم صلاحيات المدعي العام والضابطة العدلية.

[36] National Institute of Standards and Technology (NIST), Guide to Digital Forensic Examination: Maintaining Chain of Custody (Gaithersburg: NIST, 2020), 12.

رابعاً: الأخطاء الشائعة التي قد تضعف الدليل الإلكتروني

تظهر الممارسة العملية أن عدداً من الأخطاء المتكررة قد تؤدي إلى إضعاف القيمة الإثباتية للدليل أو تعقيد عملية إثبات الجريمة.

ومن أبرز هذه الأخطاء:

1. الاعتماد على لقطة الشاشة فقط (Screenshot)

رغم أهمية لقطات الشاشة في توثيق الواقعة، إلا أنها قد لا تكون كافية بمفردها لإثبات الجريمة، وقد يثار بشأنها ادعاء التعديل أو الفبركة.

لذلك يُفضل دعمها بوسائل إثبات أخرى، مثل:

- فحص الحساب أو الجهاز.
- حفظ الروابط الإلكترونية.
- استخراج البيانات الفنية عند الإمكان.

2. حذف المحادثات أو حظر الجاني قبل توثيق الأدلة

قد يؤدي قيام الضحية بحذف الرسائل أو حظر الجاني أو إغلاق الحسابات قبل توثيق الأدلة إلى فقدان معلومات مهمة يحتاجها التحقيق.

ولذلك ينبغي توجيه الضحية إلى المحافظة على المحتوى محل الشكوى وعدم اتخاذ أي إجراء قد يؤدي إلى فقدانه قبل استشارة الجهات المختصة.

3. العبث بالأجهزة أو إغلاقها بصورة غير صحيحة

في بعض الحالات، قد يؤدي التعامل غير السليم مع الأجهزة الإلكترونية إلى فقدان بيانات مهمة أو إتلاف معلومات قد تكون ضرورية للتحقيق.

ولهذا يُنصح بترك إجراءات الفحص والاستخراج الفني للجهات المختصة والخبراء المعتمدين.

خامساً: إجراءات جمع الأدلة الإلكترونية وضبطها

نظم قانون الجرائم الإلكترونية هذه المسألة في المادة (32)، حيث منح موظفي الضابطة العدلية، بعد الحصول على إذن من المدعي العام المختص أو المحكمة المختصة، صلاحية:[37]

[37] تنص المادة 32 من قانون الجرائم الالكترونية على " (أ) مع مراعاة الشروط والأحكام المقررة في التشريعات النافذة وحقوق المشتكى عليه الشخصية، لموظفي الضابطة العدلية، بعد الحصول على اذن من المدعي العام المختص أو من المحكمة المختصة:1- الدخول إلى أي مكان تشير

- الدخول إلى الأماكن التي تشير الدلائل إلى استخدامها في ارتكاب الجريمة.
- تفتيش وفحص الأجهزة والبرامج وأنظمة المعلومات والشبكات المستخدمة.
- ضبط الأجهزة والوسائط والأدوات المستخدمة في ارتكاب الجرائم الإلكترونية.
- التحفظ على البيانات والمعلومات المرتبطة بالجريمة.

كما أوجب القانون تنظيم محاضر رسمية تتضمن إجراءات التفتيش والفحص والضبط، بما يضمن سلامة الإجراءات وقابليتها للاحتجاج أمام القضاء.

سادساً: إزالة المحتوى وحفظ البيانات

من الخصائص المميزة لقضايا العنف الرقمي أن الضرر قد يستمر ويتفاقم طالما ظل المحتوى المسيء متاحاً أو قابلاً للتداول.

ولذلك منح قانون الجرائم الإلكترونية في المادة (33) المدعي العام المختص أو المحكمة المختصة صلاحيات واسعة تهدف إلى الحد من استمرار الضرر، ومن أبرزها:[38]

- إزالة المحتوى المخالف.
- حجب أو تعطيل المحتوى أو الحسابات المخالفة.

الدلائل الى استخدامه لارتكاب أي من الجرائم المنصوص عليها في هذا القانون وتفتيشها. 2- تفتيش وفحص الأجهزة والأدوات والبرامج وأنظمة التشغيل والشبكة المعلوماتية والوسائل التي تشير الدلائل في استخدامها لارتكاب أي من تلك الجرائم. (ب) على الموظف الذي قام بالتفتيش أو الفحص أن ينظم محضرا بذلك ويقدمه إلى المدعي العام أو المحكمة المختصة. (ج) 1- مع مراعاة الفقرة (أ) من هذه المادة وحقوق الغير حسن النية يجوز لموظفي الضابطة العدلية ضبط الأجهزة والأدوات والبرامج وأنظمة التشغيل والشبكة المعلوماتية والوسائل المستخدمة لارتكاب أي من الجرائم المنصوص عليها أو يشملها هذا القانون والأموال المتحصلة منها والتحفظ على المعلومات والبيانات المتعلقة بارتكاب أي منها. 2- يستثنى من أحكام البند (1) من هذه الفقرة، المرخص لهم وفق أحكام قانون الاتصالات ممن لم يشتركوا بأي جريمة منصوص عليها في هذا القانون.

[38] تنص المادة 33 من قانون الجرائم الالكترونية على " (أ) للمدعي العام المختص أو للمحكمة المختصة وعند قيام نظام المعلومات أو موقع الكتروني أو مزود الخدمة داخل المملكة أو خارجها أو منصات التواصل الاجتماعي أو الشخص المسؤول عن أي حساب أو صفحة عامة أو مجموعة عامة أو قناة أو ما يماثلها بنشر أي مواد مخالفة لأحكام هذا القانون أو التشريعات النافذة في المملكة اصدار أمر الى القائمين عليها لاتخاذ ما يلي: 1- إزالة او حظر أو إيقاف أو تعطيل أو تسجيل أو اعتراض خط سير البيانات أو أي منشور أو محتوى أو منع الوصول اليه أو حظر المستخدم أو الناشر مؤقتاً خلال المدة المحددة في القرار. 2- تزويدهما بجميع البيانات أو المعلومات اللازمة التي تساعد في اظهار الحقيقة ومنها بيانات مالك أو مستخدم الموقع الالكتروني أو نظام المعلومات التي تساعد في تحديد هويته واجراء الملاحقة القانونية. 3- الحفظ العاجل للبيانات والمعلومات اللازمة لإظهار الحقيقة وتخزينها والمحافظة على سلامتها. 4- الحفاظ على السرية. (ب) في حال عدم استجابة أو رفض القائمين على نظام المعلومات أو منصة التواصل الاجتماعي أو الموقع الإلكتروني أو مزود الخدمة للأمر المنصوص عليه في البند (1) من الفقرة (أ) من هذه المادة أو إذا اقتضت السرعة ذلك فيجوز للمدعي العام المختص او المحكمة المختصة وبقرار معلل اصدار أمر الى الجهات المختصة بحظر نظام المعلومات أو الموقع الالكتروني أو منصة التواصل الاجتماعي أو الخدمة عن الشبكة الوطنية أو حظر الوصول للمحتوى المخالف. (ج) يعاقب بغرامة لا تقل عن (15000) خمسة عشر ألف دينار ولا تزيد على (30000) ثلاثين ألف دينار كل من امتنع عن تنفيذ أوامر المدعي العام أو المحكمة المختصة أو خالفها.

- منع الوصول إلى المحتوى الضار.
- الحصول على البيانات اللازمة لتحديد هوية المستخدم أو الناشر.
- الحفظ العاجل للبيانات والمعلومات اللازمة لإظهار الحقيقة.
- المحافظة على سرية البيانات والإجراءات.

وتكتسب هذه الصلاحيات أهمية خاصة في حالات:

- الابتزاز الإلكتروني.
- نشر الصور أو التسجيلات الخاصة.
- التشهير الرقمي.
- خطاب الكراهية.
- انتحال الهوية.

وينبغي على المحامين والمحاميات تقييم الحاجة إلى اللجوء لهذه الإجراءات بصورة عاجلة عند وجود خطر حقيقي من استمرار انتشار المحتوى أو تفاقم الضرر الواقع على الضحية.

سابعاً: جوانب عملية خاصة

إلى جانب القواعد العامة المتعلقة بحجية الأدلة الإلكترونية وشروط قبولها، توجد مجموعة من الجوانب العملية التي ينبغي على المحامين والمحاميات مراعاتها عند التعامل مع قضايا العنف الرقمي ضد النساء.

1. توثيق الأدلة الرقمية

يُعد التوثيق السريع والدقيق من أهم مراحل التعامل مع قضايا العنف الرقمي، خاصة في الحالات التي يكون فيها المحتوى قابلاً للحذف أو التعديل خلال فترة قصيرة.

ورغم أهمية لقطات الشاشة (Screenshots)، إلا أنه لا يُنصح بالاعتماد عليها وحدها متى أمكن، إذ قد يثار بشأنها ادعاء التعديل أو الفبركة. لذلك يُفضّل دعمها بوسائل أخرى، مثل حفظ الروابط الإلكترونية، والاحتفاظ بالمحادثات الأصلية، وتوثيق أسماء الحسابات، وتاريخ ووقت النشر أو الرسائل، وأي بيانات قد تساعد في ربط المحتوى بالحساب أو المستخدم المعني.

2. الحسابات الوهمية وانتحال الهوية

تُعد الحسابات الوهمية أو المنتحلة من أبرز التحديات العملية في قضايا العنف الرقمي، خاصة في قضايا التشهير، والابتزاز، وحملات الإساءة المنظمة، ونشر الصور أو المعلومات الخاصة.

وتكمن الصعوبة في تحديد هوية المستخدم الحقيقي، وإثبات صلة المتهم بالحساب، والتعامل مع الحسابات المحذوفة أو المؤقتة، أو الوصول إلى البيانات المطلوبة من المنصات الرقمية.

وقد تتطلب هذه الحالات طلبات رسمية لحفظ البيانات، أو مخاطبة المنصات الرقمية، أو إجراءات فنية متخصصة لتتبع الحسابات أو الأجهزة المستخدمة.

3. التعامل مع الأجهزة الإلكترونية

قد تتطلب بعض التحقيقات المتعلقة بالجرائم الإلكترونية الاطلاع على الهواتف أو الأجهزة الإلكترونية ذات الصلة بالقضية، سواء لغايات التحقق من الأدلة، أو توثيق المحتوى، أو استخراج البيانات الرقمية، أو إجراء الخبرة الفنية اللازمة.

وفي هذا السياق، ينبغي توعية الضحية مسبقاً بإمكانية اتخاذ مثل هذه الإجراءات، ومناقشة أي مخاوف تتعلق بالخصوصية أو بالمعلومات الشخصية غير المرتبطة بالقضية.

كما ينبغي التنبيه إلى أهمية:

- عدم حذف المحتوى أو الرسائل قبل التوثيق.
- عدم العبث بالأجهزة أو إعادة ضبطها.
- الاحتفاظ بالأجهزة والبيانات المرتبطة بالقضية قدر الإمكان.

4. إزالة المحتوى وحفظ الأدلة

قد يكون استمرار نشر المحتوى الضار سبباً في تفاقم الضرر الواقع على الضحية، خاصة إذا تعلق الأمر بالصور الخاصة أو التسجيلات الشخصية أو حملات التشهير والإساءة المنظمة.

وتزداد أهمية اتخاذ إجراءات إزالة المحتوى أو حجبه أو حفظ البيانات في الحالات التي يكون فيها المحتوى سريع الانتشار أو قابلاً لإعادة النشر على نطاق واسع.

ومع ذلك، ينبغي الحرص على توثيق المحتوى وحفظ الأدلة المرتبطة به قبل اتخاذ أي خطوات قد تؤدي إلى حذفه أو إزالته، لأن فقدان المحتوى قبل توثيقه قد يؤثر على القدرة على الإثبات لاحقاً.

5. تحديات عملية في الإثبات

قد تواجه قضايا العنف الرقمي عدداً من التحديات العملية المتعلقة بالإثبات، من أبرزها:

- حذف المحتوى قبل توثيقه.
- استخدام حسابات وهمية أو أسماء مستعارة.
- صعوبة إثبات ملكية الحساب أو ربطه بالمتهم.
- استخدام تطبيقات تعتمد الرسائل المؤقتة أو المشفرة.

- تعدد المشاركين في النشر أو إعادة النشر.
- وجود أطراف خارج المملكة أو استخدام منصات أجنبية.

وفي بعض الحالات، قد تتطلب القضية خبرة فنية متخصصة، أو تعاوناً مع جهات تقنية، أو إجراءات قانونية إضافية للحصول على المعلومات اللازمة لإظهار الحقيقة.

خلاصة عملية

في قضايا العنف الرقمي ضد النساء، لا تكفي معرفة النصوص القانونية وحدها، بل إن نجاح القضية يعتمد بدرجة كبيرة على سرعة توثيق الأدلة الرقمية والمحافظة عليها، وفهم الإجراءات القانونية والفنية المرتبطة بجمعها وتحليلها وتقديمها أمام القضاء. ولذلك ينبغي إعطاء مسألة الأدلة الإلكترونية أولوية خاصة منذ اللحظات الأولى للتعامل مع القضية.

الفصل الرابع: التعامل القانوني الأولي مع قضايا العنف الرقمي ضد النساء

تتطلب قضايا العنف الرقمي ضد النساء تعاملاً قانونياً ومهنياً يراعي خصوصية هذا النوع من القضايا، سواء من حيث طبيعة الانتهاكات المرتكبة، أو حساسية المعلومات المتداولة، أو الآثار النفسية والاجتماعية والقانونية المترتبة على الضحية.

وفي كثير من الحالات، قد تؤثر طريقة التعامل الأولية مع الضحية أو مع الوقائع محل الشكوى بشكل مباشر على:

- سلامة الضحية.
- إمكانية إثبات الواقعة.
- فعالية الإجراءات القانونية.
- الحد من استمرار الضرر أو انتشار المحتوى الضار.
- قدرة الضحية على اتخاذ قرارات قانونية مدروسة.

لذلك، يُعد الدور الأولي للمحامي أو مقدّم المساعدة القانونية بالغ الأهمية، ليس فقط من الناحية القانونية، وإنما أيضاً من حيث إدارة المخاطر، وبناء الثقة مع الضحية، وتوجيهها نحو الخيارات القانونية المناسبة.

ويعرض هذا الفصل مجموعة من الإرشادات المتعلقة بالتعامل القانوني الأولي مع الضحية، مع التركيز بصورة خاصة على دور المحامي ومقدم المساعدة القانونية.

أولاً: المقابلة الأولية مع الضحية

تُعد المقابلة الأولى من أهم مراحل التعامل مع القضية، إذ تساعد على:

- فهم طبيعة الواقعة.
- تقييم درجة الخطورة.
- تحديد نوع الانتهاك المرتكب.
- تقدير الحاجة إلى إجراءات عاجلة.
- تحديد الأدلة المتوافرة.

- التعرف إلى الاحتياجات القانونية والحماية المطلوبة.

وينبغي أن تتم المقابلة في بيئة تراعي:

- الخصوصية.
- السرية.
- الاحترام.
- عدم إصدار الأحكام المسبقة.
- تجنب لوم الضحية أو التشكيك بروايتها.

كما يُفضل استخدام أسئلة واضحة ومباشرة، مع منح الضحية الوقت الكافي لشرح الوقائع دون ضغط أو مقاطعة، خاصة في القضايا المرتبطة بالصور الخاصة أو العلاقات الشخصية أو التهديد أو الابتزاز.

وينبغي للمحامي أو مقدّم المساعدة القانونية توضيح طبيعة الإجراءات القانونية المتوقعة وحدود دوره المهني منذ المراحل الأولى، بما يساعد الضحية على اتخاذ قرارات مستنيرة بشأن الخطوات اللاحقة.

ثانياً: تقييم المخاطر

قد تتضمن بعض قضايا العنف الرقمي مخاطر تتجاوز الجانب الإلكتروني، خاصة إذا كان الجاني:

- شريكاً حالياً أو سابقاً.
- أحد أفراد الأسرة.
- شخصاً يعرف الضحية بصورة مباشرة.
- شخصاً يمتلك معلومات شخصية أو صوراً أو تسجيلات خاصة.
- شخصاً لديه إمكانية الوصول إلى حسابات الضحية أو أجهزتها الإلكترونية.

وفي هذا السياق، ينبغي على المحامي أو مقدّم المساعدة القانونية تقييم عدد من الجوانب، منها:

- احتمالية تصعيد التهديد أو الابتزاز.
- استمرار نشر المحتوى أو إعادة تداوله.
- وجود تهديد مباشر للسلامة الجسدية للضحية أو أحد أفراد أسرتها.
- احتمالية الوصول إلى الحسابات أو الأجهزة الخاصة بالضحية.

- احتمالية تعرض الضحية لضغط اجتماعي أو أسري.
- مدى تأثير الواقعة على الوضع النفسي أو المهني أو التعليمي للضحية.

وقد تستدعي بعض الحالات اتخاذ إجراءات عاجلة، مثل:

- توثيق الوقائع بصورة فورية.
- تقديم شكوى للجهات المختصة.
- طلب إزالة المحتوى أو حفظ البيانات.
- التواصل مع الجهات المختصة بالحماية أو التحقيق.
- إحالة الضحية إلى خدمات الدعم النفسي أو الاجتماعي عند الحاجة.

ويجب أن يكون تقييم المخاطر عملية مستمرة ترافق القضية منذ بدايتها وحتى انتهاء الإجراءات القانونية، نظراً لإمكانية تغير الظروف أو تصاعد المخاطر بمرور الوقت.

ثالثاً: السرية وحماية المعلومات

تتميز قضايا العنف الرقمي بدرجة عالية من الحساسية، خاصة في الحالات المرتبطة بـ:

- الصور أو التسجيلات الخاصة.
- المحادثات الشخصية.
- الحسابات الإلكترونية.
- البيانات الشخصية.
- المعلومات العائلية أو المهنية.

ولذلك، ينبغي التعامل مع المعلومات والوثائق المتعلقة بالقضية بأعلى درجات السرية والمهنية، مع مراعاة:

- عدم مشاركة المعلومات دون موافقة الضحية ما لم يقتض القانون خلاف ذلك.
- حفظ الوثائق والأدلة بطريقة آمنة.
- الحد من تداول الصور أو التسجيلات أو البيانات الشخصية.
- استخدام وسائل اتصال آمنة عند الحاجة.
- عدم الاحتفاظ بنسخ غير ضرورية من المواد الحساسة.

كما ينبغي توضيح حدود السرية للضحية منذ البداية، وخاصة في الحالات التي قد تتطلب:

- تقديم المعلومات إلى الجهات القضائية أو التحقيقية.
- إبراز الأدلة أمام المحكمة.
- الاستعانة بخبراء أو جهات مختصة لأغراض الإثبات أو الحماية.

وتسهم الشفافية في هذا الجانب في تعزيز ثقة الضحية بالإجراءات القانونية وتجنب أي سوء فهم لاحق.

رابعاً: التواصل مع الجهات المختصة

قد تتطلب بعض القضايا التواصل المباشر أو السريع مع الجهات المختصة، بحسب طبيعة الواقعة ومستوى الخطورة والضرر المترتب عليها.

ومن أبرز الجهات التي قد يكون من الضروري التواصل معها:

- وحدة مكافحة الجرائم الإلكترونية.
- النيابة العامة.
- إدارة حماية الأسرة.
- المنصات الرقمية أو مزودو الخدمات الإلكترونية.
- الجهات المعنية بالدعم النفسي أو الحماية الاجتماعية.

ويجب أن يراعي المحامي أو مقدّم المساعدة القانونية عند اتخاذ هذه الخطوات:

- طبيعة الخطر القائم.
- رغبة الضحية ومصلحتها الفضلى.
- حجم الضرر الواقع أو المحتمل.
- احتمالية استمرار انتشار المحتوى.
- الحاجة إلى إجراءات عاجلة أو تحفظية.
- السياق الاجتماعي والأسري المحيط بالضحية.

كما ينبغي شرح الإجراءات المتوقعة للضحية بصورة مبسطة وواضحة، بما يساعدها على فهم المسار القانوني للقضية والنتائج المحتملة لكل إجراء.

خامساً: التعامل المهني مع الضحية

يتطلب التعامل مع ضحايا العنف الرقمي حساسية مهنية خاصة، نظراً لما قد تتعرض له الضحية من:[39]

- الخوف.
- القلق.
- الضغط الاجتماعي أو الأسري.
- الشعور بالذنب أو الإحراج.
- فقدان الثقة بالآخرين.
- القلق من الوصمة أو من استمرار انتشار المحتوى.

وفي هذا السياق، ينبغي على المحامي أو مقدّم المساعدة القانونية:

- تجنب لوم الضحية أو التشكيك في أقوالها.
- استخدام لغة مهنية ومحترمة تراعي كرامتها وخصوصيتها.
- احترام قرارات الضحية وخياراتها القانونية.
- عدم التقليل من أثر الانتهاك أو آثاره النفسية والاجتماعية.
- مراعاة الحالة النفسية للضحية أثناء المقابلات والإجراءات.
- تمكين الضحية من المشاركة في اتخاذ القرارات المتعلقة بقضيتها.
- توضيح الخيارات القانونية المتاحة بلغة واضحة ومفهومة.
- تجنب استخدام عبارات أو أسئلة قد تُفهم على أنها تحميل للضحية مسؤولية ما تعرضت له.

كما ينبغي تجنب تشجيع الضحية على مواجهة الجاني أو التواصل معه أو حذف المحتوى أو اتخاذ خطوات قد تؤثر على مسار القضية قبل تقييم الوضع القانوني بصورة مناسبة.

وقد يكون من المفيد، في بعض الحالات، إحالة الضحية إلى خدمات دعم نفسي أو اجتماعي أو قانوني متخصصة، بما يضمن حصولها على الحماية والمساندة اللازمة إلى جانب الدعم القانوني.

---

[39] مؤسسة أنسم للحقوق الرقمية. *الدليل الشامل للتعامل مع قضايا العنف الرقمي ضد النساء في العراق، مؤسسة سيكديف (سلاما@) 2025)).*

خلاصة عملية

إن التعامل الأولي مع قضايا العنف الرقمي ضد النساء لا يقتصر على تحديد الوصف القانوني للواقعة أو تقديم الشكوى، بل يشمل أيضاً بناء علاقة مهنية قائمة على الثقة والاحترام، وتقييم المخاطر، وحماية الخصوصية، وتوجيه الضحية نحو الإجراءات المناسبة في الوقت المناسب. وكلما كان التدخل الأولي مهنياً ومدروساً، زادت فرص حماية الضحية، والحفاظ على الأدلة، والحد من الضرر، وتعزيز فرص الوصول إلى العدالة بصورة فعالة وآمنة.

الفصل الخامس: الإحالة والدعم والحماية في قضايا العنف الرقمي ضد النساء

لا تقتصر آثار العنف الرقمي ضد النساء على الجانب القانوني فقط، بل قد تمتد لتشمل آثاراً نفسية واجتماعية ومهنية وأسرية قد تستمر لفترات طويلة، خاصة في الحالات التي تتضمن:

- التشهير العلني.
- نشر الصور أو التسجيلات أو المعلومات الخاصة.
- الابتزاز الإلكتروني.
- انتحال الهوية.
- التهديد أو الملاحقة الرقمية.
- حملات الإساءة المنظمة أو خطاب الكراهية.

وفي كثير من الحالات، لا يكون اللجوء إلى الإجراءات القانونية وحده كافياً لمعالجة الآثار المترتبة على الانتهاك، إذ قد تحتاج الضحية إلى أشكال مختلفة من الدعم والحماية، تشمل: [40]

- الدعم النفسي والاجتماعي.
- الحماية الأسرية والمجتمعية.
- الحماية الرقمية والتقنية.
- المساعدة القانونية.
- التعامل مع المنصات الرقمية.
- التنسيق مع الجهات المختصة.

ويهدف هذا الفصل إلى توضيح أهمية الاستجابة متعددة القطاعات في قضايا العنف الرقمي ضد النساء، والدور الذي يمكن أن يؤديه المحامي أو مقدم المساعدة القانونية في دعم الضحية وتوجيهها وإحالتها إلى الجهات المناسبة عند الحاجة. [41]

---

[40] *(مؤسسة أنسم للحقوق الرقمية. الدليل الشامل للتعامل مع قضايا العنف الرقمي ضد النساء في العراق، مؤسسة سيكديف (سلاما@) (2025.*

[41] مركز المعلومات والبحوث - مؤسسة الملك الحسين، *نحو منظومة آمنة وفعّالة للاستجابة للعنف الرقمي في الأردن، مؤسسة سيدكيف (سلاما@) (عمّان 2025.))*

أولاً: أهمية الدعم متعدد القطاعات

قد لا تكون الإجراءات القانونية وحدها كافية لمعالجة الآثار الناتجة عن العنف الرقمي، خاصة في الحالات التي تتعرض فيها الضحية إلى:

- ضغوط اجتماعية أو أسرية.
- تهديد مستمر أو متكرر.
- آثار نفسية مرتبطة بالخوف أو القلق أو الشعور بالوصمة.
- فقدان الشعور بالأمان أو الثقة بالآخرين.
- آثار مهنية أو تعليمية أو اجتماعية نتيجة انتشار المحتوى.

ولذلك، قد يكون من الضروري توفير أو تسهيل الوصول إلى:

- الدعم النفسي.
- الخدمات الاجتماعية.
- خدمات الحماية.
- الاستشارات التقنية أو الرقمية.
- المساعدة القانونية المتخصصة.

كما قد تختلف احتياجات الضحايا تبعاً لـ:

- العمر.
- طبيعة الانتهاك.
- مدى انتشار المحتوى.
- العلاقة مع الجاني.
- مستوى المخاطر المرتبطة بالقضية.
- الوضع الأسري والاجتماعي للضحية.

ومن المهم النظر إلى احتياجات الضحية بصورة شاملة، وعدم الاقتصار على الجانب القانوني فقط.

ثانياً: دور المحامي أو مقدم المساعدة القانونية

لا يقتصر دور المحامي أو مقدم المساعدة القانونية على تقديم المشورة القانونية أو متابعة الإجراءات القضائية، بل قد يشمل أيضاً:

- شرح الحقوق القانونية المتاحة للضحية.
- توضيح الإجراءات المتوقعة ومراحلها.
- المساعدة في تقييم المخاطر.
- المساهمة في وضع خطة أولية للحماية.
- توجيه الضحية نحو الجهات المختصة.
- التنسيق مع جهات الدعم المختلفة عند الحاجة.

كما ينبغي على المحامي أو مقدم المساعدة القانونية:

- مراعاة حساسية القضية.
- احترام خصوصية الضحية.
- تجنب أي سلوك أو أسلوب قد يؤدي إلى إعادة إيذائها نفسياً أو اجتماعياً.
- مراعاة مبدأ الموافقة المستنيرة عند مناقشة الخيارات القانونية أو الإحالات.

وفي بعض الحالات، قد يكون من المناسب اقتراح:

- الدعم النفسي.
- الدعم الاجتماعي.
- الحماية الأسرية.
- الاستشارات التقنية.
- الإحالة إلى مؤسسات متخصصة.

خاصة إذا ظهرت مؤشرات على وجود ضغط نفسي أو اجتماعي كبير أو خطر مستمر على الضحية.

ثالثاً: التعامل مع المنصات الرقمية

قد يكون من الضروري في بعض القضايا اتخاذ خطوات للتعامل مع المنصات الرقمية أو مواقع التواصل الاجتماعي، خاصة عندما يتعلق الانتهاك بـ:

- الصور أو الفيديوهات الخاصة.
- المحتوى المسيء أو التشهيري.
- الحسابات الوهمية أو المنتحلة.
- حملات التشهير أو التحريض أو خطاب الكراهية.
- انتحال الهوية الرقمية.

وقد تشمل هذه الخطوات:

- الإبلاغ عن المحتوى المخالف.
- طلب إزالة الصور أو التسجيلات أو المنشورات.
- طلب إغلاق الحسابات الوهمية أو المنتحلة.
- توثيق المحتوى قبل حذفه.
- حفظ الروابط والبيانات المرتبطة بالقضية.

كما ينبغي الانتباه إلى أن:

- سياسات المنصات تختلف من منصة إلى أخرى.
- بعض الإجراءات قد تستغرق وقتاً.
- بعض الطلبات قد لا تستجاب بصورة فورية.
- إزالة المحتوى من المنصة لا تعني اختفاءه نهائياً من البيئة الرقمية.

ومن المهم التأكيد على أن الإبلاغ عن المحتوى أو طلب إزالته لا يغني عن توثيق الأدلة أو اتخاذ الإجراءات القانونية اللازمة عندما تشكل الواقعة جريمة يعاقب عليها القانون.

رابعاً: السلامة الرقمية للضحية

في بعض الحالات، قد يكون من الضروري اتخاذ إجراءات عاجلة لتعزيز السلامة الرقمية للضحية، خاصة إذا كان هناك احتمال:

- لاستمرار التهديد أو الابتزاز.
- للوصول غير المشروع إلى الحسابات.
- لاستخدام البيانات أو المعلومات الشخصية بصورة مسيئة.
- لمراقبة النشاط الرقمي للضحية.

وقد تشمل إجراءات السلامة الرقمية ما يلي:

- تغيير كلمات المرور.
- استخدام كلمات مرور قوية ومختلفة للحسابات المهمة.
- تفعيل التحقق الثنائي (Two-Factor Authentication).
- مراجعة إعدادات الخصوصية.
- تأمين الحسابات والأجهزة.
- مراجعة التطبيقات المرتبطة بالحسابات.
- إزالة التطبيقات أو الصلاحيات غير الضرورية.
- مراجعة البريد الإلكتروني وأرقام الهواتف المرتبطة بالحسابات.
- مراجعة خيارات استرداد الحساب.
- تسجيل الخروج من الأجهزة غير المعروفة.
- الحد من مشاركة المعلومات الشخصية على الإنترنت.

كما ينبغي مراعاة أن بعض الضحايا قد يفتقرن إلى المعرفة التقنية الكافية، وقد يحتجن إلى دعم أو مساعدة عملية لفهم وتطبيق إجراءات الحماية الرقمية الأساسية.

خامساً: الجهات المختصة وجهات الدعم

قد تتطلب بعض الحالات التواصل أو التنسيق مع جهات مختلفة بحسب طبيعة القضية ومستوى الخطورة.

وفيما يلي أمثلة على الجهات التي قد يكون من المناسب اللجوء إليها:

الحاجة أو نوع الدعم	الجهة أو الخدمة المقترحة
الإبلاغ عن الجريمة الإلكترونية والتحقيق فيها	وحدة مكافحة الجرائم الإلكترونية
الحماية في الحالات التي تتضمن تهديداً أسرياً أو عنفاً داخل الأسرة	إدارة حماية الأسرة
الإجراءات القضائية ومتابعة الدعوى	النيابة العامة والمحاكم المختصة
إزالة المحتوى أو الحسابات المخالفة	المنصات الرقمية ومزودو الخدمات
المساعدة القانونية	المحامون أو مؤسسات المساعدة القانونية
الدعم النفسي والاجتماعي	المؤسسات والجهات المتخصصة بالدعم النفسي والاجتماعي
خدمات الحماية والإيواء عند الحاجة	الجهات والمؤسسات المختصة بالحماية

وفي بعض الحالات، قد يكون من المفيد:

- توثيق التواصل مع الجهات المختلفة.
- الاحتفاظ بسجل للإجراءات المتخذة.
- متابعة نتائج الإحالات.
- تنسيق الإحالات بصورة تراعي خصوصية الضحية وسلامتها.

سادساً: التعامل مع المخاطر المستمرة

قد لا ينتهي أثر العنف الرقمي بمجرد تقديم الشكوى أو إزالة المحتوى، إذ قد تستمر بعض المخاطر لفترات طويلة، ومن ذلك:

- إعادة نشر المحتوى من قبل أطراف أخرى.
- استمرار المضايقات أو التهديدات.
- إنشاء حسابات جديدة بعد إغلاق الحسابات السابقة.
- محاولات الانتقام بعد تقديم الشكوى.
- استمرار الضغط الاجتماعي أو النفسي على الضحية.
- بقاء بعض النسخ أو المواد المنشورة متداولة خارج المنصة الأصلية.

وفي هذا السياق، قد يكون من المهم:

- متابعة تطورات الحالة بصورة دورية.
- تحديث تقييم المخاطر عند الحاجة.
- مناقشة أي تطورات جديدة مع الضحية.
- مراجعة إجراءات الحماية الرقمية بصورة مستمرة.
- إعادة تقييم الحاجة إلى خدمات الدعم أو الحماية.

كما ينبغي الانتباه إلى أن بعض القضايا قد تتطلب:

- استجابة طويلة الأمد.
- تنسيقاً مستمراً بين أكثر من جهة.
- متابعة قانونية ونفسية واجتماعية متوازية.

خلاصة عملية

تتطلب قضايا العنف الرقمي ضد النساء استجابة شاملة لا تقتصر على الإجراءات القانونية وحدها، وإنما تشمل أيضاً الحماية والدعم النفسي والاجتماعي والرقمي. ويؤدي المحامي أو مقدم المساعدة القانونية دوراً محورياً في تقييم الاحتياجات، وتوجيه الضحية، وتنسيق الإحالات، والمساهمة في تعزيز سلامتها وحقوقها خلال مختلف مراحل التعامل مع القضية.

وكلما كانت الاستجابة مبكرة ومتكاملة ومبنية على التعاون بين الجهات المختلفة، زادت فرص الحد من الضرر وتعزيز الحماية والوصول إلى العدالة بصورة فعالة وآمنة.

الفصل السادس: الأدوات العملية والملاحق

يهدف هذا الفصل إلى توفير مجموعة من الأدوات العملية والإرشادية التي تساعد في التعامل المنظم والفعال مع قضايا العنف الرقمي ضد النساء، ويمكن للممارسين القانونيين والجهات ذات العلاقة الاستفادة منها وفقاً لطبيعة أدوارهم واختصاصاتهم.

ولا تُعد هذه النماذج أو القوائم بديلاً عن التقدير المهني أو الإجراءات القانونية المعمول بها، وإنما أدوات مساندة يمكن تكييفها بحسب طبيعة كل قضية والظروف المحيطة بها.

كما ينبغي مراعاة أن:

- بعض القضايا قد تتطلب إجراءات إضافية،
- أو استشارات تقنية أو قانونية متخصصة،
- أو تنسيقاً مع جهات أخرى بحسب طبيعة الانتهاك والمخاطر المرتبطة به.

أولاً: نموذج مقابلة أولية مع الضحية

يمكن أن تساعد المقابلة الأولية في:

- فهم طبيعة الواقعة،
- وتقييم المخاطر،
- وتحديد الخطوات القانونية المناسبة،
- وتوثيق المعلومات الأساسية المتعلقة بالقضية.

معلومات أولية مقترحة

- تاريخ المقابلة
- وسيلة التواصل
- طبيعة العلاقة بين الأطراف
- نوع الانتهاك المبلغ عنه
- المنصات أو التطبيقات المستخدمة

- وجود تهديد مستمر أو خطر عاجل
- وجود محتوى منشور أو قابل للنشر
- ما إذا تم توثيق الأدلة
- أي إجراءات تم اتخاذها مسبقاً

ثانياً: قائمة تحقق أولية للأدلة الرقمية

قبل تقديم الشكوى أو اتخاذ الإجراءات القانونية، يُستحسن التأكد من:

- توثيق المحتوى قبل حذفه أو اختفائه
- الاحتفاظ بلقطات شاشة واضحة
- حفظ الروابط الإلكترونية المرتبطة بالمحتوى
- توثيق تاريخ ووقت النشر أو الرسائل
- الاحتفاظ بالمحادثات الأصلية قدر الإمكان
- توثيق أسماء الحسابات أو الصفحات المستخدمة
- عدم تعديل الصور أو الرسائل أو قصها
- الاحتفاظ بأي بيانات أو معلومات قد تساعد في تحديد هوية المستخدم
- توثيق أي حسابات وهمية أو مرتبطة بالواقعة
- الاحتفاظ بنسخة احتياطية من الأدلة الرقمية عند الحاجة

ثالثاً: قائمة تحقق أولية لتقييم المخاطر

قد يكون من المهم تقييم ما إذا كانت القضية تتضمن:

- تهديداً مباشراً بالنشر أو الإيذاء
- خطراً على السلامة الشخصية للضحية
- وصول الجاني إلى الحسابات أو الأجهزة
- استمرار المضايقات أو الملاحقة الرقمية
- احتمال إعادة نشر المحتوى
- وجود ضغوط اجتماعية أو أسرية على الضحية
- استخدام حسابات متعددة أو وهمية
- احتمال تصعيد السلوك أو انتقاله إلى الواقع الفعلي

رابعاً: إرشادات أولية للسلامة الرقمية

قد يكون من المفيد مناقشة بعض الإجراءات الأساسية مع الضحية، مثل:

- تغيير كلمات المرور للحسابات المهمة
- تفعيل التحقق الثنائي
- مراجعة إعدادات الخصوصية
- تقليل مشاركة المعلومات الشخصية
- مراجعة التطبيقات والأجهزة المرتبطة بالحسابات
- الحذر من الروابط أو الرسائل المشبوهة
- الاحتفاظ بنسخ من الأدلة قبل حذف أي محتوى

خامساً: إرشادات أولية للتعامل مع المنصات الرقمية

عند التعامل مع المحتوى المسيء أو الحسابات المرتبطة بالقضية، قد يكون من المهم:

- توثيق المحتوى قبل الإبلاغ عنه أو حذفه
- استخدام أدوات الإبلاغ المتاحة في المنصات
- الاحتفاظ بروابط الحسابات أو المنشورات
- توثيق أي ردود أو تفاعلات مرتبطة بالمحتوى
- الانتباه لاحتمال إعادة النشر أو إنشاء حسابات بديلة

سادساً: قائمة بالجهات المرجعية والداعمة

يهدف هذا الملحق إلى تعريف المستخدم بأبرز الجهات التي قد تقدم خدمات الإبلاغ أو الحماية أو الدعم أو الإحالة في حالات العنف الرقمي ضد النساء والفتيات. وتختلف الجهة الأنسب بحسب طبيعة الحالة واحتياجات الضحية، وقد تستدعي بعض الحالات التواصل مع أكثر من جهة في الوقت نفسه.[42]

تنبيه مهم:
يُراعى مواكبة أي مستجدات تشريعية أو مؤسسية أو تقنية ذات صلة، والتحقق دوريًا من بيانات الاتصال وروابط الإبلاغ والخدمات المتاحة من خلال المصادر الرسمية للجهات والمنصات المعنية، لضمان الاستفادة من أحدث الإجراءات والمعلومات.

الجهة	طبيعة الخدمة
وحدة مكافحة الجرائم الإلكترونية / مديرية الأمن العام	استقبال البلاغات المتعلقة بالجرائم الإلكترونية، واتخاذ الإجراءات القانونية والتحقيقية وفق التشريعات النافذة.
إدارة حماية الأسرة والأحداث / مديرية الأمن العام	التعامل مع جميع القضايا التي يكون أحد أطرافها طفلًا (دون الثامنة عشرة)، إضافة إلى حالات العنف الأسري والحالات التي تستوجب تدابير الحماية وفق الاختصاص القانوني.
المجلس الوطني لشؤون الأسرة	تطوير السياسات الوطنية، وإصدار الأدلة والإجراءات الوطنية، وتعزيز التنسيق بين الجهات ذات العلاقة بحماية الأسرة والطفل والمرأة.
منظمات المجتمع المدني ومقدمو خدمات الدعم	تقديم خدمات الدعم النفسي والاجتماعي والقانوني، والسلامة الرقمية، والإيواء، والإحالة، وفق اختصاص كل جهة.

الإبلاغ عبر المنصات الرقمية

توفر معظم المنصات الرقمية أدوات للإبلاغ عن المحتوى أو الحسابات التي تنطوي على تهديد أو ابتزاز أو تحرش أو انتحال هوية أو نشر محتوى دون موافقة. وتشمل أبرزها:

1. مجموعة منصات ميتا (Meta)

- **فيسبوك:** مركز السلامة للإبلاغ عن التحرش والانتهاكات على فيسبوك
- **إنستغرام:** مركز المساعدة العام على إنستغرام
- **واتساب:** مركز مساعدة واتساب لحظر جهات الاتصال والإبلاغ عنها
- **ميسنجر:** إرشادات الإبلاغ عن السلوك المسيء على ميسنجر

[42] مركز المعلومات والبحوث - مؤسسة الملك الحسين، *نحو منظومة آمنة وفعّالة للاستجابة للعنف الرقمي في الأردن*، مؤسسة سيدكيف ((سلاما@)) (عمّان 2025).

2. منصات التواصل الاجتماعي الأخرى

- **إكس (تويتر سابقاً):** بوابة نماذج الدعم والسلامة الرسمية لـ إكس (لتقديم بلاغات التحرش وانتحال الشخصية)
- **تيك توك:** دليل السلامة والإبلاغ عن المشكلات والمحتوى في تيك توك
- **سناب شات:** بوابة الدعم والإبلاغ عن مخاوف السلامة في سناب شات
- **تليغرام:** نموذج الدعم والإبلاغ الرسمي عبر الويب لـ تليغرام (أو مراسلتهم مباشرة عبر: abuse@telegram.org)

3. خدمات جوجل ويوتيوب

- **يوتيوب:** إرشادات الإبلاغ عن المحتوى المخالف للسياسات في يوتيوب
- **جوجل:** نموذج طلب إزالة المعلومات الشخصية أو المحتوى المسيء من نتائج بحث جوجل (لإزالة حالات الابتزاز أو نشر صور دون موافقة)

سابعا: مصفوفة الجرائم الشائعة والتكييف القانوني الأولي في قضايا العنف الرقمي ضد النساء

يهدف هذا الملحق إلى تزويد المحامين والمحاميات بأداة عملية سريعة تساعد في تحديد التكييف القانوني الأولي لأكثر الوقائع شيوعاً في قضايا العنف الرقمي ضد النساء، وربطها بالنصوص القانونية ذات الصلة والإجراءات الأولية التي ينبغي مراعاتها.

ولا يُغني هذا الملحق عن دراسة ظروف كل قضية على حدة، إذ قد تتداخل عدة جرائم أو أوصاف قانونية في الواقعة الواحدة، كما أن التكييف القانوني النهائي يبقى خاضعاً لظروف القضية والأدلة المتوافرة والتقدير القضائي.

مصفوفة الجرائم الشائعة والتكييف القانوني الأولي			
الواقعة أو السلوك	التكييف القانوني الأولي المحتمل	النصوص القانونية ذات الصلة	ملاحظات عملية للمحامي
إنشاء حساب أو صفحة أو قناة باسم الضحية أو باستخدام صورها أو بياناتها دون موافقتها	انتحال هوية رقمية	المادة (5) من قانون الجرائم الإلكترونية	توثيق الحساب والرابط والصور المستخدمة قبل حذفها أو إغلاقها
استخدام حساب وهمي للتواصل مع الآخرين باسم الضحية أو الإساءة إليها	انتحال هوية رقمية وقد يرتبط بالتشهير أو الابتزاز	المادة (5) من قانون الجرائم الإلكترونية	ضرورة توثيق المحتوى المنشور وبيانات الحساب

نشر منشورات أو تعليقات أو محتوى يمس سمعة الضحية أو كرامتها	ذم أو قدح أو تحقير إلكتروني	المادة (15) من قانون الجرائم الإلكترونية والمادة (188) وما بعدها من قانون العقوبات	التمييز بين النقد المباح والمحتوى المجرم قانوناً
نشر شائعات أو معلومات غير صحيحة بقصد الإضرار بالضحية	تشهير إلكتروني أو اغتيال شخصية	المادتان (15) و(16) من قانون الجرائم الإلكترونية	أهمية إثبات الضرر والعلنية وانتشار المحتوى
نشر محتوى يسيء إلى السمعة المهنية أو الاجتماعية للضحية بصورة منظمة	اغتيال شخصية	المادة (16) من قانون الجرائم الإلكترونية	توثيق نمط الاستهداف وتكرار النشر
تهديد الضحية بنشر صور أو فيديوهات أو محادثات خاصة	ابتزاز إلكتروني	المادة (18) من قانون الجرائم الإلكترونية	لا يشترط وقوع النشر فعلياً لقيام الجريمة
طلب منفعة مالية أو شخصية مقابل عدم نشر محتوى خاص	ابتزاز إلكتروني	المادة (18) من قانون الجرائم الإلكترونية	الاحتفاظ بالرسائل والمحادثات وعدم حذفها
تهديد الضحية بالإيذاء أو التشهير أو الإضرار بعلاقاتها الأسرية أو المهنية	تهديد رقمي	قانون الجرائم الإلكترونية وقانون العقوبات بحسب الواقعة	تقييم مستوى الخطر وإمكانية تصعيد التهديد
نشر صور أو فيديوهات أو تسجيلات خاصة دون موافقة الضحية	انتهاك الخصوصية الرقمية	المادة (20) من قانون الجرائم الإلكترونية	قد تستدعي القضية إجراءات مستعجلة لإزالة المحتوى
تعديل الصور أو الفيديوهات أو تركيبها بقصد الإساءة أو التشهير	انتهاك الخصوصية الرقمية	المادة (20) من قانون الجرائم الإلكترونية	يشمل المحتوى المفبرك أو المعدل رقمياً
استخدام أدوات الذكاء الاصطناعي لإنشاء صور أو فيديوهات مزيفة للضحية	انتهاك الخصوصية وقد يرتبط بالتشهير أو الابتزاز	المادة (20) وغيرها بحسب ظروف الواقعة	قد تتطلب القضية خبرة فنية متخصصة
نشر بيانات شخصية أو عائلية أو مهنية دون موافقة الضحية	انتهاك الخصوصية الرقمية	المادة (20) وغيرها من النصوص ذات الصلة	لا يشترط أن تكون المعلومات ذات طبيعة جنسية

الدخول إلى حساب الضحية أو جهازها الإلكتروني دون إذن	دخول غير مشروع إلى نظام معلومات أو حساب إلكتروني	قانون الجرائم الإلكترونية	توثيق سجلات الدخول والتنبيهات التقنية
الحصول على محتوى من حساب مخترق ثم نشره أو استخدامه للإساءة	دخول غير مشروع وانتهاك خصوصية وقد يرتبط بالابتزاز	قانون الجرائم الإلكترونية	غالباً ما تتعدد الجرائم في الواقعة الواحدة
إرسال رسائل أو تعليقات متكررة غير مرغوب فيها تتضمن مضايقة أو إساءة	تحرش رقمي	بحسب ظروف الواقعة والنصوص القانونية المنطبقة	أهمية إثبات التكرار والاستمرارية
التواصل المتكرر مع الضحية رغم رفضها أو حظرها للحساب	ملاحقة رقمية	بحسب ظروف الواقعة	توثيق سجل التواصل وتوقيته
مراقبة نشاط الضحية الرقمي أو تتبع حساباتها بصورة متكررة ومزعجة	ملاحقة رقمية	بحسب ظروف الواقعة	تقييم المخاطر المرتبطة بالسلامة الشخصية
نشر محتوى يحرض على الكراهية أو العنف أو التمييز ضد النساء	خطاب كراهية	المادة (17) من قانون الجرائم الإلكترونية	يخضع التكييف النهائي لتقدير القضاء
تنظيم حملة منسقة للإساءة أو التشويه أو التحريض ضد الضحية	حملة إساءة منظمة	المواد (15)، (16)، (17) بحسب ظروف الواقعة	توثيق الحسابات المشاركة وتوقيت النشر
استخدام عدد كبير من الحسابات لإعادة نشر محتوى مسيء بصورة منسقة	إساءة منظمة وقد ترتبط بانتحال الهوية أو التشهير	بحسب ظروف الواقعة	يفيد إثبات التنسيق بين الحسابات
إعادة نشر محتوى مسيء منشور من قبل الغير	مساهمة أو اشتراك في الجريمة الأصلية	بحسب نوع الجريمة المرتكبة	إعادة النشر قد تنشئ مسؤولية قانونية مستقلة
استخدام الشعوذة الإلكترونية لاستدراج النساء والحصول على صور أو معلومات خاصة	قد يشكل ابتزازاً أو احتيالاً أو انتهاكاً للخصوصية	قانون الجرائم الإلكترونية وقانون العقوبات	التركيز على الفعل المرتكب وليس على التسمية المتداولة

ثامنا: مؤشرات تستدعي اتخاذ إجراءات عاجلة

ينبغي التفكير باتخاذ إجراءات عاجلة عند وجود واحد أو أكثر من المؤشرات التالية:

- وجود تهديد وشيك بنشر صور أو تسجيلات خاصة.
- استمرار تداول المحتوى الضار على نطاق واسع.
- وجود خطر فعلي على السلامة الجسدية للضحية.
- استخدام حسابات متعددة أو منظمة لتوسيع نطاق الإساءة.
- وجود ابتزاز مالي أو جنسي مستمر.
- وجود أطفال أو أفراد من الأسرة متأثرين بالواقعة.
- احتمال فقدان الأدلة أو حذفها خلال فترة قصيرة.

وقد تشمل الإجراءات العاجلة:

- توثيق الأدلة فوراً.
- تقديم شكوى للجهات المختصة.
- طلب الحفظ العاجل للبيانات.
- طلب إزالة المحتوى أو حجبه.
- تقييم الحاجة إلى إجراءات حماية إضافية.

تاسعا: أبرز التحديات العملية في قضايا العنف الرقمي

من أبرز التحديات التي قد تواجه المحامين والمحاميات أثناء التعامل مع هذه القضايا:

- حذف المحتوى قبل توثيقه.
- استخدام حسابات وهمية أو مستعارة.
- تعدد المشاركين في النشر أو إعادة النشر.
- صعوبة إثبات ملكية الحساب أو الجهاز.
- استخدام أرقام أو حسابات أو خوادم خارج المملكة.

- استخدام تطبيقات تعتمد الرسائل المؤقتة أو المشفرة.
- تردد الضحية في الاستمرار بالإجراءات القانونية.
- الضغوط الاجتماعية أو الأسرية أو محاولات الصلح.
- استمرار تداول المحتوى رغم حذفه من المصدر الأصلي.

عاشرا: تذكير عملي عند التعامل مع قضايا العنف الرقمي ضد النساء

عند التعامل مع أي قضية من قضايا العنف الرقمي ضد النساء، يُنصح بالتحقق من النقاط التالية منذ المرحلة الأولى:

- تحديد نوع الانتهاك أو الجريمة المحتملة.
- تقييم مستوى الخطر على الضحية.
- توثيق الأدلة الرقمية المتاحة.
- حفظ الروابط والحسابات والبيانات ذات الصلة.
- تقييم الحاجة إلى إجراءات مستعجلة.
- تحديد الجهات المختصة الواجب التواصل معها.
- مراعاة خصوصية الضحية وسرية المعلومات.
- دراسة احتمالية تداخل أكثر من جريمة في الواقعة الواحدة.
- تقييم الحاجة إلى خبرة فنية أو دعم نفسي أو اجتماعي.

ويُعد هذا الملحق أداة استرشادية تساعد في التقييم الأولي للقضايا، على أن يتم الرجوع إلى النصوص القانونية ذات الصلة والاجتهادات القضائية وظروف كل قضية عند اتخاذ القرار القانوني النهائي.

حادي عشر: أهم التعريفات والمصطلحات أساسية

لغايات هذا الدليل، تُستخدم المصطلحات التالية بالمعاني المبينة أدناه، مع مراعاة أن هذه التعريفات ذات طابع إرشادي وعملي، ولا تحل محل التعريفات القانونية الواردة في التشريعات النافذة.

المصطلح	التعريف
الابتزاز الإلكتروني	إجبار شخص على القيام بفعل أو الامتناع عنه أو تحقيق منفعة غير مشروعة للفاعل أو لغيره من خلال التهديد بإفشاء أمر أو نشر معلومات أو صور أو تسجيلات من شأنها الإضرار بسمعته أو شرفه أو مكانته الاجتماعية.

الإحالة	توجيه الضحية إلى جهة مختصة أخرى للحصول على خدمة قانونية أو نفسية أو اجتماعية أو حماية تتناسب مع احتياجاتها.[43]
انتحال الهوية الرقمية	هو استخدام اسم أو صورة أو بيانات أو حسابات أو أي عناصر تعريفية لشخص آخر عبر الوسائل الرقمية بما يؤدي إلى إيهام الغير بأنه ذلك الشخص.
انتهاك الخصوصية	نشر أو تداول الصور أو التسجيلات أو المعلومات الشخصية دون موافقة صاحبتها، أو الوصول غير المشروع إلى الحسابات أو البيانات الخاصة أو استخدامها بصورة تنتهك حق المرأة في الخصوصية.
اغتيال الشخصية	الأفعال الرقمية التي تستهدف النيل من سمعة الشخص أو مصداقيته أو مكانته الاجتماعية أو المهنية من خلال نشر معلومات أو ادعاءات أو محتوى مضلل أو مجتزأ بقصد الإضرار به.
البيانات الوصفية (Metadata)	هي بيانات تقنية مصاحبة للبيانات الإلكترونية الأصلية، تُظهر خصائصها وظروف إنشائها أو تعديلها أو إرسالها أو استقبالها أو تخزينها، وتشمل التاريخ والوقت والمصدر ونوع الجهاز والموقع الإلكتروني أو الجغرافي وسجل التعديلات المرتبطة بها.[44]
التتبع الرقمي	هو استخدام الوسائل التقنية أو البرمجيات أو أنظمة المعلومات لرصد أو مراقبة أو تحديد أو تسجيل النشاط الإلكتروني أو المواقع الجغرافية أو التحركات أو البيانات العائدة لشخص طبيعي أو اعتباري عبر الوسائط الرقمية.
التحرش الإلكتروني	الرسائل أو التعليقات أو السلوكيات الرقمية غير المرغوب فيها التي تحمل طابعاً مسيئاً أو مهيناً أو جنسياً أو ترهيبياً، خاصة إذا كانت متكررة أو مستمرة أو تنطوي على تهديد أو ضغط نفسي.[45]
التحقق الثنائي	هو إجراء أمني إلكتروني يُشترط بموجبه استخدام وسيلتين مستقلتين للتحقق من هوية المستخدم عند الدخول إلى حساب أو نظام إلكتروني بقصد تعزيز الحماية ومنع الوصول غير المصرح به.[46]

[43] UN Women, UNFPA, WHO, UNDP, and UNODC, Essential Services Package for Women and Girls Subject to Violence: Core Elements and Quality Guidelines (New York: United Nations Joint Global Programme on Essential Services for Women and Girls Subject to Violence, 2015).

[44] International Organization for Standardization, ISO 15489-1:2016: Information and Documentation — Records Management — Part 1: Concepts and Principles (Geneva: ISO, 2016).

[45] Council of Europe, Group of Experts on Action against Violence against Women and Domestic Violence (GREVIO), General Recommendation No. 1 on the Digital Dimension of Violence against Women (Strasbourg: Council of Europe, 2021).

[46] Paul A. Grassi et al., Digital Identity Guidelines: Authentication and Lifecycle Management, NIST Special Publication 800-63B (Gaithersburg, MD: National Institute of Standards and Technology, 2017, updated 2020).

التشهير الإلكتروني	هو نشر أو إعادة نشر أو تداول محتوى رقمي من شأنه الإضرار بسمعة شخص أو كرامته أو مكانته الاجتماعية، سواء تضمن معلومات غير صحيحة أو إفشاء معلومات خاصة بقصد الإساءة أو التشهير.[47]
التهديد الإلكتروني	هو أي نشاط عدائي أو خطر محتمل يُنفذ باستخدام الوسائل والشبكات الرقمية، ويسعى إلى إلحاق الضرر بالبنية التحتية المعلوماتية (عبر الاختراق، أو التعطيل، أو زرع البرمجيات الخبيثة)، أو استهداف الأفراد بشكل مباشر عبر ترهيبهم، أو ابتزازهم، أو انتهاك خصوصيتهم وتدمير سمعتهم، بغرض تحقيق مكاسب نفعية غير مشروعة أو فرض السيطرة والهيمنة.[48]
تقييم المخاطر	عملية تقدير مستوى التهديد أو الضرر الحالي أو المحتمل الذي قد تتعرض له الضحية نتيجة الواقعة أو تطوراتها اللاحقة. [49]
الجريمة الإلكترونية	هي كل فعل غير مشروع يُرتكب باستخدام الشبكة المعلوماتية أو نظام المعلومات أو وسائل تقنية المعلومات أو يكون موجهاً ضدها، ويترتب عليه اعتداء على الأشخاص أو الأموال أو البيانات أو الأنظمة الإلكترونية ويعاقب عليه القانون.
الحساب الوهمي	هو حساب إلكتروني يتم إنشاؤه أو استخدامه ببيانات أو معلومات غير صحيحة أو غير عائدة لمستخدمه الحقيقي بقصد إخفاء شخصيته أو تضليل الغير أو ممارسة نشاط إلكتروني دون إمكانية تحديد هويته الحقيقية.
حملات الإساءة المنظمة	استهداف الضحية بشكل جماعي أو منظم من خلال نشر الإساءات أو التحريض أو تداول الشائعات أو المعلومات المضللة أو المحتوى المسيء بهدف الإضرار بسمعتها أو التأثير على نشاطها الشخصي أو المهني أو العام.
حماية البيانات الشخصية	هي مجموعة القواعد والتدابير القانونية والتنظيمية والتقنية التي تنظم جمع البيانات الشخصية ومعالجتها وحفظها والإفصاح عنها، بما يكفل حماية حقوق أصحابها وفقاً للتشريعات النافذة.
خطاب الكراهية	يُقصد بخطاب الكراهية أي نوع من أنواع التواصل، الشفهي أو الكتابي أو السلوكي، الذي يهاجم أو يستخدم لغة ازدرائية أو تمييزية بالإشارة إلى شخص أو مجموعة من الأشخاص على أساس هويتهم، مثل الدين أو الأصل الإثني أو الجنسية أو العرق أو اللون أو النسب أو الجنس أو أي عامل آخر محدد للهوية. [50]

[47] Oxford University Centre for Socio-Legal Studies, Digital Defamation and Reputation Protection Law (Oxford: Oxford University Press, 2022), 47.

[48] Cybersecurity and Infrastructure Security Agency (CISA), Cybersecurity Framework and Threat Definitions (Washington, DC: CISA, 2022), 14.

[49] European Institute for Gender Equality, A Guide to Risk Assessment and Risk Management of Intimate Partner Violence against Women for Police (Luxembourg: Publications Office of the European Union, 2019).

[50] United Nations, United Nations Strategy and Plan of Action on Hate Speech (New York: United Nations, 2019).

الخصوصية الجندرية للعنف الرقمي	أشكال خاصة من الانتهاكات تواجهها النساء والفتيات وترتبط غالباً بالنوع الاجتماعي والصور النمطية والأدوار الاجتماعية المفروضة عليهن.
الدليل الإلكتروني	كل أثر رقمي أو معلومة رقمية يتم الحصول عليها من الحواسيب أو الهواتف الذكية أو الشبكات أو أنظمة المعلومات أو وسائل تقنية المعلومات، ويكون من شأنها المساهمة في كشف الحقيقة وإثبات الوقائع ذات الأهمية القانونية أمام القضاء.[51]
الذم والقدح والتحقير الإلكتروني	إرسال أو نشر أو إعادة نشر بيانات أو معلومات أو تعليقات أو محتوى رقمي عبر الوسائل الإلكترونية يتضمن عبارات أو أوصافاً من شأنها المساس بسمعة المرأة أو كرامتها أو مكانتها الاجتماعية.
الرابط الإلكتروني	هو عنوان أو مسار رقمي مخصص للوصول إلى موقع إلكتروني أو صفحة أو ملف أو محتوى أو خدمة عبر شبكة الإنترنت أو أي شبكة معلوماتية أخرى.
السلامة الرقمية	هي مجموعة الممارسات، والمهارات، والتدابير الوقائية التي يتخذها الأفراد أثناء استخدامهم للإنترنت والتكنولوجيا لحماية أنفسهم وهوياتهم من المخاطر الرقمية. وتشمل السلامة الرقمية تأمين الحسابات بكلمات مرور قوية، والحفاظ على خصوصية البيانات الشخصية، والوعي بكيفية التعامل مع التهديدات السلوكية مثل الابتزاز، والتحرش الإلكتروني، والاحتيال لضمان استخدام آمن للتقنيات الرقمية.[52]
الشخصيات العامة	النساء اللواتي يكتسبن حضوراً عاماً أو تأثيراً مجتمعياً يجعل أنشطتهن أو مواقفهن محل اهتمام الرأي العام.
الشخصيات العامة بالصدفة	النساء اللواتي لا يمارسن نشاطاً عاماً أو سياسياً أو إعلامياً بصورة منتظمة، إلا أنهن يصبحن محل اهتمام عام مؤقت بسبب واقعة معينة أو حدث أو قضية مرتبطة بهن.
الشعوذة الإلكترونية	استخدام المنصات الرقمية أو وسائل التواصل الاجتماعي للترويج لأعمال الشعوذة أو السحر أو قراءة الطالع أو الادعاء بامتلاك قدرات روحانية أو علاجية، بما يؤدي إلى استدراج النساء أو استغلالهن أو الإضرار بهن.
العنف الرقمي ضد النساء	أي سلوك أو فعل يُرتكب باستخدام الوسائل الرقمية أو عبر الإنترنت ويستهدف النساء أو الفتيات بشكل يؤدي إلى الإساءة أو التهديد أو الابتزاز أو انتهاك الخصوصية أو الإضرار النفسي أو الاجتماعي أو المهني.[53]

[51] Karen Kent et al., Guide to Integrating Forensic Techniques into Incident Response, NIST Special Publication 800-86 (Gaithersburg, MD: National Institute of Standards and Technology, 2006).

[52] World Health Organization (WHO), Guidelines on Digital Safety and Mental Well-being for Online Users (Geneva: WHO, 2023), 31.

[53] Council of Europe, Group of Experts on Action against Violence against Women and Domestic Violence (GREVIO), General Recommendation No. 1 on the Digital Dimension of Violence against Women (Strasbourg: Council of Europe, 2021).

غير الشخصيات العامة	النساء اللواتي لا يرتبطن بظهور عام أو نشاط يجعل حياتهن أو مواقفهن محلاً للاهتمام العام.
المحتوى الخاص	هو أي مادة رقمية (مثل: الصور الشخصية، مقاطع الفيديو، المراسلات النصية، السجلات الطبية، أو البيانات المالية) التي تعود لفرد أو مجموعة، والمحمية بموجب حق الخصوصية. هذا المحتوى لم يُنشر للعامة، ويحتفظ صاحبه بالحق الحصري في تحديد من يمكنه الاطلاع عليه أو مشاركته، ويُعد الوصول إليه أو نشره أو استغلاله دون سند قانوني أو موافقة صاحبه، متى توافرت أركان الجريمة، فعلاً قد يرتب مسؤولية قانونية.[54]
المحتوى الرقمي	كل نص أو صورة أو تسجيل صوتي أو فيديو أو ملف أو رسالة أو بيانات يتم إنشاؤها أو نشرها أو تداولها أو تخزينها باستخدام الوسائل الرقمية.
المصلحة الفضلى للضحية	مراعاة ما يحقق حماية الضحية وسلامتها وكرامتها وحقوقها عند اتخاذ القرارات أو اختيار الإجراءات المناسبة. [55]
الملاحقة الرقمية	متابعة الضحية بصورة متكررة عبر الوسائل الرقمية، أو مراقبة نشاطها الإلكتروني، أو التواصل المستمر معها بصورة غير مرغوب فيها بما يسبب لها الخوف أو القلق أو الشعور بعدم الأمان. [56]

ثاني عشر: سيناريوهات تطبيقية في التعامل القانوني مع قضايا العنف الرقمي ضد النساء

تهدف السيناريوهات الآتية إلى توضيح كيفية تطبيق عدد من الإرشادات القانونية والعملية الواردة في الدليل على حالات افتراضية، مع التركيز بصورة خاصة على دور المحامي ومقدم المساعدة القانونية في الاستجابة الأولية للقضية.

[54] United Nations Human Rights Office (OHCHR), The Right to Privacy in the Digital Age (Geneva: United Nations, 2022), 14.

[55] Committee on the Elimination of Discrimination against Women, General Recommendation No. 35 on Gender-Based Violence against Women, Updating General Recommendation No. 19, CEDAW/C/GC/35 (Geneva: United Nations, 2017).

[56] Council of Europe, Group of Experts on Action against Violence against Women and Domestic Violence (GREVIO), General Recommendation No. 1 on the Digital Dimension of Violence against Women (Strasbourg: Council of Europe, 2021).

السيناريو الأول: استخدام صور منشورة علناً لإنشاء حساب مسيء أو ابتزازي

وصف الحالة

راجعت شابة تبلغ من العمر 23 عاماً مكتب محاماة، وأفادت بأنها تعمل مدربة رياضية ولديها صفحة عامة على إحدى منصات التواصل الاجتماعي تنشر عليها صوراً عادية مرتبطة بعملها ونشاطها الرياضي. اكتشفت لاحقاً أن شخصاً مجهولاً قام بأخذ صورها المنشورة علناً واستخدامها في إنشاء حساب على منصة أخرى، وربط الصور بمحتوى مسيء يتضمن إيحاءات أو عبارات تمس سمعتها وكرامتها، وربما يستخدم صوتاً أو محتوى معدلاً رقمياً للإيحاء بأنها تقدم خدمات أو تتواصل مع الآخرين بصورة مسيئة.

أوضحت الضحية أنها لا تعرف من يقف خلف الحساب، وأنها تخشى إبلاغ أسرتها بسبب الحساسية الاجتماعية للموضوع، كما تخشى أن يؤدي تقديم الشكوى إلى انتشار المحتوى بصورة أوسع.

كيف يتعامل المحامي أو المحامية مع الحالة؟

1. استقبال الضحية وبناء الثقة

على المحامي في البداية أن يتعامل مع الضحية باعتبارها ضحية لانتهاك رقمي، وليس فقط موكلة في قضية قانونية. ويجب أن تتم المقابلة في بيئة آمنة وسرية، مع تجنب أي سؤال أو تعليق قد يُفهم منه لوم الضحية بسبب نشرها صوراً عامة على حسابها.

ينبغي طمأنة الضحية إلى أن استخدام صور منشورة علناً لا يبرر استغلالها أو تحريفها أو ربطها بمحتوى مسيء، وأن وجود الصور على حساب عام لا يعني التنازل عن الحق في الكرامة أو السمعة أو الخصوصية.

2. فهم الوقائع الأساسية

ينبغي على المحامي طرح أسئلة واضحة ومحددة، مثل:

- متى اكتشفت الضحية الحساب أو المحتوى المسيء؟
- ما المنصة المستخدمة؟
- هل الحساب ما زال فعالاً؟
- هل تم استخدام اسمها أو صورتها أو بياناتها؟
- هل توجد رسائل مباشرة أو تهديدات؟
- هل تم إرسال المحتوى إلى أشخاص تعرفهم؟
- هل هناك اشتباه بشخص معين؟
- هل تم الإبلاغ عن الحساب للمنصة أو للجهات المختصة؟

- هل قامت الضحية بحذف أي رسائل أو حظر الحساب؟

3. توثيق الأدلة قبل الإبلاغ أو الحذف

قبل طلب حذف الحساب أو المحتوى، يجب توثيق الأدلة قدر الإمكان، من خلال:

- أخذ لقطات شاشة واضحة للحساب والمحتوى.
- حفظ رابط الحساب أو الصفحة.
- توثيق اسم المستخدم وصورة الحساب وأي بيانات ظاهرة.
- توثيق تاريخ ووقت الاطلاع على المحتوى.
- حفظ أي رسائل أو تعليقات أو تفاعلات مرتبطة بالحساب.
- عدم تعديل الصور أو قصها أو إعادة إرسالها بطريقة قد تضعف قيمتها الإثباتية.

ولا يُنصح بالاعتماد على لقطات الشاشة وحدها إذا كان بالإمكان دعمها بروابط، أو بيانات حساب، أو فحص فني لاحق.

4. التكييف القانوني الأولي

قد تتضمن الواقعة أكثر من وصف قانوني محتمل، بحسب تفاصيل الحالة، ومنها:

- انتحال الهوية الرقمية، إذا تم إنشاء حساب أو صفحة باسم الضحية أو باستخدام صورها وبياناتها.
- الذم أو القدح أو التحقير الإلكتروني، إذا تضمن المحتوى إساءة إلى سمعتها أو كرامتها.
- اغتيال الشخصية، إذا كان المحتوى يهدف إلى النيل من مكانتها الاجتماعية أو المهنية.
- انتهاك الخصوصية أو استخدام محتوى خاص أو معدل، إذا تم تركيب الصور أو تعديلها أو معالجتها رقمياً.
- الابتزاز الإلكتروني، إذا ترافق الأمر مع تهديد أو طلب منفعة.

ويجب على المحامي عدم الاكتفاء بوصف عام مثل "إساءة إلكترونية"، بل تحديد الوقائع والأوصاف القانونية المحتملة بوضوح عند إعداد الشكوى.

5. تقييم المخاطر

ينبغي تقييم المخاطر المرتبطة بالحالة، بما في ذلك:

- احتمال توسع انتشار المحتوى.
- أثر الواقعة على عمل الضحية وسمعتها المهنية.
- احتمال معرفة الأسرة أو جهة العمل بالواقعة.

- وجود تهديد أو ابتزاز مباشر.
- احتمال أن يكون الفاعل شخصاً يعرف الضحية.
- الحالة النفسية للضحية وقدرتها على متابعة الإجراءات.

إذا ظهر أن المحتوى ينتشر بسرعة أو أن هناك تهديداً مباشراً، فقد تكون هناك حاجة إلى إجراءات عاجلة لحفظ البيانات أو طلب إزالة المحتوى.

6. الخيارات القانونية والعملية

بعد توثيق الأدلة، يمكن للمحامي مناقشة الخيارات التالية مع الضحية:

- تقديم شكوى إلى وحدة مكافحة الجرائم الإلكترونية أو النيابة العامة.
- طلب حفظ البيانات المرتبطة بالحساب.
- طلب إزالة المحتوى أو حجب الحساب وفق الإجراءات القانونية.
- تقديم بلاغ للمنصة الرقمية بعد حفظ الأدلة.
- دراسة الحاجة إلى دعم نفسي أو اجتماعي إذا كانت الضحية تحت ضغط شديد.

ويجب شرح النتائج المحتملة لكل خيار، وحدود السرية، واحتمال الحاجة إلى الاطلاع على هاتف الضحية أو حساباتها أو الأدلة الرقمية المرتبطة بالقضية.

7. تنبيه عملي

ينبغي نصح الضحية بما يلي:

- عدم التواصل مع صاحب الحساب.
- عدم إرسال تهديدات أو ردود غاضبة.
- عدم حذف الرسائل أو الصور قبل التوثيق.
- عدم نشر توضيحات عامة قد تزيد انتشار المحتوى.
- تعزيز إعدادات الخصوصية والسلامة الرقمية لحساباتها.

السيناريو الثاني: ابتزاز إلكتروني مرتبط بعلاقة سابقة أو محتوى خاص

وصف الحالة

راجعت امرأة مكتب محاماة وأفادت بأنها تتعرض لابتزاز من شخص كانت تربطها به علاقة معرفة أو علاقة شخصية سابقة. يحتفظ هذا الشخص بمحادثات أو صور أو تسجيلات خاصة، ويهدد بنشرها أو إرسالها إلى أفراد أسرتها أو زملائها أو محيطها الاجتماعي إذا لم تستجب لطلباته، سواء كانت مالية أو شخصية أو غير ذلك.

تخشى الضحية تقديم شكوى لأنها قلقة من معرفة أسرتها أو من أن تُسأل عن العلاقة السابقة أو تُحمّل مسؤولية ما حدث. كما أنها تفكر في حذف المحادثات أو حظر الشخص فوراً.

كيف يتعامل المحامي أو المحامية مع الحالة؟

1. التعامل الأولي مع الضحية

على المحامي أن يبدأ بالاستماع إلى الضحية دون لوم أو أحكام مسبقة. ولا يجوز أن يكون السؤال الأول موجهاً نحو سبب العلاقة أو سبب إرسال الصور أو المحادثات، بل يجب التركيز على الخطر الحالي، وطبيعة التهديد، والأدلة المتوافرة، وسلامة الضحية.

ينبغي توضيح أن وجود علاقة سابقة، إن وجدت، لا يبرر الابتزاز أو التهديد أو نشر المحتوى الخاص.

2. تحديد مستوى الخطر

ينبغي على المحامي تقييم الخطر بصورة عاجلة من خلال أسئلة مثل:

- هل هدد الجاني بالنشر خلال وقت محدد؟
- هل سبق أن نشر أي محتوى فعلاً؟
- هل طلب مالاً أو منفعة أو فعلاً معيناً؟
- هل يعرف أفراد أسرة الضحية أو مكان عملها؟
- هل لديه وصول إلى حساباتها أو هاتفها؟
- هل هناك خطر على السلامة الجسدية للضحية؟
- هل الضحية تحت ضغط نفسي شديد أو تفكر في الانسحاب من الإجراءات؟

إذا كان التهديد وشيكاً أو متكرراً أو يتضمن خطراً على السلامة، فينبغي التفكير بإجراءات عاجلة.

3. حفظ الأدلة وعدم حذف المحادثات

ينبغي تنبيه الضحية إلى عدم حذف المحادثات أو حظر الجاني قبل توثيق الأدلة، لأن ذلك قد يؤدي إلى فقدان معلومات مهمة.

تشمل الأدلة التي ينبغي حفظها:

- رسائل التهديد أو الابتزاز.
- المحادثات التي تتضمن الطلبات أو الضغوط.
- أرقام الهواتف أو أسماء الحسابات المستخدمة.
- الروابط أو الحسابات المرتبطة بالواقعة.
- أي تحويلات مالية أو طلبات دفع.
- أي محتوى تم نشره أو التهديد بنشره.
- تاريخ ووقت الرسائل والتهديدات.

ويجب حفظ الأدلة بطريقة آمنة، مع تقليل تداول الصور أو التسجيلات الحساسة إلى أضيق نطاق ممكن.

4. التكييف القانوني الأولي

قد تتضمن الواقعة أوصافاً قانونية متعددة، منها:

- الابتزاز الإلكتروني، إذا كان هناك تهديد لحمل الضحية على القيام بفعل أو الامتناع عنه أو للحصول على منفعة.
- التهديد الإلكتروني، إذا تضمن الفعل تهديداً بالإيذاء أو التشهير أو نشر محتوى خاص.
- انتهاك الخصوصية، إذا تم نشر أو استخدام صور أو تسجيلات أو معلومات خاصة.
- الذم والقدح أو التشهير، إذا تم نشر محتوى يمس السمعة أو الكرامة.
- جرائم أخرى بحسب طبيعة المحتوى وسن الضحية وظروف الواقعة.

ويجب أن تكون الشكوى واضحة من حيث الوقائع، والأدلة، والطلبات، والأوصاف القانونية الأولية المحتملة.

5. مناقشة قرار الشكوى مع الضحية

ينبغي للمحامي شرح الخيارات القانونية المتاحة للضحية بوضوح، بما في ذلك:

- تقديم شكوى رسمية.
- طلب إجراءات عاجلة لحفظ البيانات أو منع النشر.
- طلب إزالة المحتوى إذا تم نشره.
- طلب حماية أو إحالة إلى جهة مختصة إذا وُجد خطر أسري أو اجتماعي أو جسدي.
- الإحالة إلى دعم نفسي أو اجتماعي عند الحاجة.

ولا ينبغي دفع الضحية إلى تقديم شكوى دون أن تفهم آثارها المحتملة، ولا ينبغي كذلك إقناعها بالصمت إذا كان هناك خطر مستمر. المطلوب هو تمكينها من اتخاذ قرار مستنير بناءً على معرفة واضحة بالخيارات والمخاطر.

6. مرافقة الضحية أثناء الإجراءات

في مثل هذه القضايا، من المهم أن يرافق المحامي الضحية أثناء تقديم الشكوى أو مراجعة الجهات المختصة قدر الإمكان، لأن وجود المحامي قد يساعد في:

- شرح الوقائع بصورة منظمة.
- منع تكرار الأسئلة غير الضرورية.
- حماية خصوصية الضحية.
- التأكد من إرفاق الأدلة المتاحة.
- طلب السرية أو الإجراءات المناسبة عند الحاجة.
- متابعة مسار الشكوى وحفظ البيانات.

7. تجنب الخطوات التي قد تضر بالقضية

ينبغي تنبيه الضحية إلى تجنب ما يلي:

- الرد على الجاني بتهديد أو إساءة.
- الدخول في تفاوض غير مدروس معه.
- دفع المال دون تقييم قانوني للموقف.
- حذف المحادثات أو حظر الحساب قبل توثيق الأدلة.
- نشر القصة على وسائل التواصل.
- إرسال المحتوى الحساس لأشخاص غير معنيين.
- مواجهة الجاني مباشرة.

8. الدعم والحماية

إذا كانت الضحية تواجه ضغطاً نفسياً أو اجتماعياً كبيراً، أو تخشى ردة فعل الأسرة، أو توجد مخاطر فعلية على السلامة، فينبغي دراسة الإحالة إلى جهات دعم نفسي أو اجتماعي أو حماية، مع احترام رغبة الضحية وخصوصيتها، ودون مشاركة معلوماتها إلا بموافقتها أو وفق ما يقتضيه القانون.

تنبيه عملي

في قضايا الابتزاز المرتبطة بعلاقة سابقة، يجب أن يركز المحامي على الفعل الجرمي الحالي، أي التهديد أو الابتزاز أو نشر المحتوى، لا على تقييم سلوك الضحية أو علاقتها السابقة بالجاني. فالهدف هو حماية الضحية ووقف الضرر والحفاظ على الأدلة وتفعيل الحماية القانونية المناسبة.

قائمة المراجع:

أولاً: التشريعات الأردنية

- الدستور الأردني لسنة 1952 وتعديلاته.
- قانون أصول المحاكمات الجزائية رقم (9) لسنة 1961 وتعديلاته.
- قانون الجرائم الإلكترونية رقم (17) لسنة 2023.
- قانون العقوبات الأردني رقم (16) لسنة 1960 وتعديلاته.
- قانون حماية البيانات الشخصية رقم (24) لسنة 2023.

ثانياً: المراجع باللغة العربية

- أنسم للحقوق الرقمية، مؤسسة. الدليل الشامل للتعامل مع قضايا العنف الرقمي ضد النساء في العراق. مؤسسة سيكديف (سلاما@)، 2025.
- الخوالدة، محمد أمين. الدليل الإلكتروني وحجيته في الإثبات الجنائي: دراسة مقارنة. عمّان: دار الثقافة للنشر والتوزيع، 2021.
- شبكة مناهضة العنف الرقمي ضد الصحفيات في الأردن، مؤسسة الملك الحسين. التأثيرات المهنية والقانونية على الصحفيات الأردنيات غير المنتسبات للنقابة في ظل تصاعد العنف الرقمي. مؤسسة سيكديف (سلاما@). عمّان، 2025.
- الصغير، جميل عبد الباقي. أدلة الإثبات الجنائي والتكنولوجيا الحديثة. القاهرة: دار النهضة العربية، 2018.
- قلعة الكرك. سياسيات تحت القصف الرقمي: دراسة في أنماط ومصادر وآثار العنف الرقمي الذي واجهته المرشحات في الانتخابات البرلمانية الأردنية لعام 2024. مؤسسة سيكديف (سلاما@). عمّان، 2025.
- المطيري، نورة. العنف الرقمي ضد النساء في الكويت: تفكيك تجارب النساء. مؤسسة سيكديف، (سلاما@). 2022.
- مركز المعلومات والبحوث – مؤسسة الملك الحسين. نحو منظومة آمنة وفعّالة للاستجابة للعنف الرقمي في الأردن. مؤسسة سيكديف (سلاما@). عمّان، 2025.

ثالثاً: المراجع باللغة الإنجليزية

- Association for Progressive Communications. *Technology-Related Violence against Women: A Briefing Paper*. Johannesburg: Association for Progressive Communications, 2015.

- Committee on the Elimination of Discrimination against Women (CEDAW). *General Recommendation No. 35 on Gender-Based Violence against Women, Updating General Recommendation No. 19*. CEDAW/C/GC/35. Geneva: United Nations, 2017.
- Council of Europe. Group of Experts on Action against Violence against Women and Domestic Violence (GREVIO). *General Recommendation No. 1 on the Digital Dimension of Violence against Women*. Strasbourg: Council of Europe, 2021.
- Cybersecurity and Infrastructure Security Agency (CISA). *Cybersecurity Framework and Threat Definitions*. Washington, DC: CISA, 2022.
- European Institute for Gender Equality. *A Guide to Risk Assessment and Risk Management of Intimate Partner Violence against Women for Police*. Luxembourg: Publications Office of the European Union, 2019.
- European Institute for Gender Equality. *Cyber Violence against Women and Girls*. Luxembourg: Publications Office of the European Union, 2017.
- Federal Communications Commission (FCC). *Standards for Location-Based Services and Network Tracking*. Washington, DC: FCC, 2021.
- Forward, Susan, and Donna Frazier. *Emotional Blackmail: When the People in Your Life Use Fear, Obligation, and Guilt to Manipulate You*. New York: HarperCollins Publishers, 1997.
- GSM Association (GSMA). *Technical Standards for Mobile Device Identifiers*. London: GSMA, 2021.
- Institute of Electrical and Electronics Engineers (IEEE). *Standards for Digital Identity Software Architecture*. New York: IEEE, 2020.
- International Organization for Standardization (ISO). *ISO 15489-1:2016: Information and Documentation-Records Management-Part 1: Concepts and Principles*. Geneva: ISO, 2016.
- Information and research Center – King Hussein Foundation. Jordan's Cybercrime Law: Balancing Protection and Freedom of Expression. SecDev Foundation. Amman, 2025.
- Internet Corporation for Assigned Names and Numbers (ICANN). *Glossary of Standard Internet Terms*. Los Angeles: ICANN, 2022.
- Internet Engineering Task Force (IETF). *Architectural Principles of the Internet Mail System*. Fremont, CA: IETF, 2021.
- Kent, Karen, Suzanne Chevalier, Tim Grance, and Hung Dang. *Guide to Integrating Forensic Techniques into Incident Response*. NIST Special Publication 800-86. Gaithersburg, MD: National Institute of Standards and Technology, 2006.
- National Coordination Office for Space-Based Positioning, Navigation, and Timing (PNT). *Global Positioning System Standard Positioning Service Performance Standard*. Washington, DC: PNT, 2020.

- National Cyber Security Centre (NCSC). *Principles of Identity and Access Management*. London: NCSC, 2023.
- National Institute of Standards and Technology (NIST). *Guide to Digital Forensic Examination of Information Systems*. Gaithersburg, MD: NIST, 2022.
- National Institute of Standards and Technology (NIST). *Guide to Digital Forensic Examination: Maintaining Chain of Custody*. Gaithersburg, MD: NIST, 2020.
- Oxford University Centre for Socio-Legal Studies. *Digital Defamation and Reputation Protection Law*. Oxford: Oxford University Press, 2022.
- Paul A. Grassi, Michael Garcia, and James Fenton. *Digital Identity Guidelines: Authentication and Lifecycle Management*. NIST Special Publication 800-63B. Gaithersburg, MD: National Institute of Standards and Technology, 2017 (updated 2020).
- Posetti, Julie, Diana Maynard, and Nabeelah Shabbir. *Guidelines for Monitoring Online Violence against Female Journalists*. Vienna: OSCE Representative on Freedom of the Media, 2023.
- Posetti, Julie, Nabeelah Shabbir, Kalina Bontcheva, Diana Maynard, and Nermine Aboulez. *The Chilling: Global Trends in Online Violence against Women Journalists*. Paris: UNESCO, 2021.
- United Nations. *United Nations Strategy and Plan of Action on Hate Speech*. New York: United Nations, 2019.
- United Nations Human Rights Office (OHCHR). *The Right to Privacy in the Digital Age*. Geneva: United Nations, 2022.
- United Nations Population Fund (UNFPA). *Technology-Facilitated Gender-Based Violence: A Growing Threat*. Accessed May 9, 2026.
- UN Women, UNFPA, WHO, UNDP, and UNODC. *Essential Services Package for Women and Girls Subject to Violence: Core Elements and Quality Guidelines*. New York: United Nations Joint Global Programme on Essential Services for Women and Girls Subject to Violence, 2015.
- World Health Organization (WHO). *Guidelines on Digital Safety and Mental Well-being for Online Users*. Geneva: WHO, 2023.

يهدف هذا الدليل إلى توفير مرجع قانوني وعملي للتعامل مع قضايا العنف الرقمي ضد النساء في الأردن، من خلال توضيح الإطار القانوني الوطني، وأبرز الجوانب الإجرائية والإثباتية، والممارسات المهنية المرتبطة بالاستجابة لهذه القضايا.

يستهدف الدليل الممارسين القانونيين والجهات ذات العلاقة بالتعامل مع قضايا العنف الرقمي ضد النساء، بما في ذلك المحامين والمحاميات، ومقدمي المساعدة القانونية، والعاملين في جهات إنفاذ القانون والجهات الرسمية المختصة، كما يمكن أن يستفيد منه الباحثون ومؤسسات المجتمع المدني والجهات العاملة في مجالات الحماية والوصول إلى العدالة.

أيلول، 2026