**"المسؤولية الجنائية الجماعية غير التقليدية: دراسة مقارنة في الجرائم التي تُرتكب عبر شبكات اجتماعية رقمية لا مركزية (Decentralized Digital Social Networks)

تأليف

د. محمد كمال عرفه الرخاوي

Dr. Mohamed Kamal arafa Elrakhawi

الإهداء

إلى ابنتي صبرينال

نور عيني وسرّ وجودي

التي تحمل في روحها نقاءَ مصر وعراقةَ الجزائر

أهدِي إليها هذا الجهد، راجياً أن يكون ذخراً لها في دنيا العلم والعدل

عناوين الفصول

1. التحدي الرقمي الجديد: عندما يصبح الجُرم لا مركزياً

2. الجماعات الجنائية غير المركزية: تعريف قانوني وخصائص بنيوية

3. الأسس الفلسفية للمسؤولية الجنائية في غياب القيادة أو الاتفاق الصريح

4. نظرية الفعل الجماعي في الفقه الجنائي المقارن

5. حدود الشراكة الجنائية التقليدية مقابل

السلوك التفاعلي في الفضاء الرقمي

6. إثبات النية الجنائية المشتركة في غياب التواصل المباشر

7. دور التشفير والخصوصية في إخفاء الروابط الجنائية

8. التشريعات الأمريكية: من قانون الاحتيال وسوء استخدام الحواسيب إلى مكافحة الجرائم الرقمية الخطيرة

9. النظام الألماني: المسؤولية الجنائية في بيئات التواصل المشفرة

10. النظام البريطاني: تجريم التحريض الضمني والمشاركة السلبية

11. التجربة الكندية: التوازن بين حرية التعبير

والسلامة العامة

12. تجارب عربية مختارة: السعودية، الإمارات، المغرب، والأردن

13. أبرز القضايا القضائية العالمية في الجرائم اللامركزية

14. الاختصاص القضائي الدولي في الجرائم العابرة للحدود الرقمية

15. الخصوصية الرقمية مقابل متطلبات الكشف عن الجناة

16. آليات التعاون الدولي في جمع الأدلة الرقمية

17. إصلاحات تشريعية مقترحة لأنظمة المسؤولية الجنائية

18. نموذج تشريعي عالمي للتعامل مع الجرائم غير المركزية

19. الآثار المترتبة على الحقوق الأساسية: حرية التعبير، الخصوصية، العدالة

20. خاتمة: نحو نظرية جنائية رقمية قائمة على التفاعل لا القيادة

التقديم

في عالمٍ لم يعد فيه الجُرم محصورًا في الزمان أو المكان، بل ينسج خيوطه عبر شاشاتٍ لا مركزية وشبكاتٍ رقمية متشابكة، يقف القانون الجنائي التقليدي أمام تحدي وجودي.
فالمفاهيم التي بُنيت على أساس التقاء المتآمرين في غرفةٍ واحدة، أو توقيع اتفاقٍ مكتوب، أو حتى تبادل كلماتٍ مباشرة، لم تعد

كافية لفهم جرائم العصر الجديد — جرائم تُدبّر في صمت، وتُنفّذ عبر أفعال متفرقة، ويُجمع بين مرتكبيها لا رابطة ولاءٍ ولا قيادة، بل رمزٌ مشترك، أو فكرةٌ مُعدية، أو حتى خوارزميةٌ ذكية.

هذا المؤلف لا يسعى إلى وصف ظاهرةٍ جديدة فحسب، بل إلى إعادة النظر في الأسس النظرية للمسؤولية الجنائية ذاتها. فهل يُعقل أن يُعاقب فردٌ على جريمةٍ لم يخطط لها، ولم يقصد وقوعها، لكنه ساهم — ولو بشكل غير مباشر — في بيئةٍ جنائية جماعية؟ وهل يمكن للقانون أن يُطبّق مبدأ الشخصية الجنائية في سياقاتٍ يذوب فيها الفرد داخل جماعةٍ لا اسم لها ولا حدود؟

لقد تم تجاهل هذا البُعد من الجرائم اللامركزية في الأدبيات القانونية العالمية، رغم تنامي خطورتها. فبينما تُخصّص مؤتمراتٌ دولية لجرائم

الذكاء الاصطناعي، تظل الجرائم التي يرتكبها البشر — ولكن ضمن هياكل رقمية لا مركزية — دون دراسةٍ منهجية. وهذا الكتاب يسدّ تلك الفجوة.

اعتمدنا في هذا العمل منهجاً مقارناً صارماً، شملنا فيه أنظمةً قانونيةً متنوعة: من النظام الأمريكي الذي يوازن بين الحرية والأمن، إلى النظام الألماني الذي يُعلي من قيمة الحماية الوقائية، مروراً بالتجارب البريطانية والكندية، وبعض الأنظمة العربية التي بدأت تواجه هذه الظاهرة دون الدخول في حساسيات سياسية أو اقتصادية. وقد استبعدنا عمداً المواضيع المرتبطة بالذكاء الاصطناعي، وركّزنا على السلوك البشري المحض، حتى لو كان مُعَدّاً رقمياً.

هذا المؤلف ليس موجهاً للباحثين فحسب، بل أيضاً للقضاة، والمدعين العامين، وضباط الشرطة

القضائية، والمحامين — أولئك الذين يقفون يومياً أمام ملفاتٍ لا تُفسّرها القواعد التقليدية. وهو يقدّم لهم أدواتٍ تحليلية، ونماذج تشريعية، وتحليلات قضائية، تُعينهم على التعامل مع هذا النوع الجديد من الجرائم.

وقد كُتب هذا العمل بروحٍ أكاديميةٍ عالية، وعمقٍ مقارنٍ نادر، والتزامٍ بالحياد والاحترام الكامل لجميع الأنظمة القانونية. وهو يندرج ضمن رؤيتي لإنشاء موسوعة جنائية عالمية تكون مرجعاً في أرقى الجامعات ومكاتب العدالة حول العالم.

والله وليّ التوفيق.

د. محمد كمال عرفه الرخاوي

إسماعيلية، يناير 2026

الفصل الأول

التحدي الرقمي الجديد: عندما يصبح الجُرم لا مركزياً

لم يعد الجُرم في القرن الحادي والعشرين يقتصر على فعلٍ مادي يُرتكب في مكانٍ محدد، بواسطة شخصٍ أو مجموعةٍ معلومة. فقد أدى تطور التكنولوجيا الرقمية، وانتشار شبكات التواصل المشفرة، وبروز المنصات اللامركزية — مثل منتديات Tor، وتطبيقات Signal، وقنوات Telegram المغلقة، وحتى بعض تطبيقات البلوك تشين الاجتماعية — إلى ظهور ما يمكن تسميته بالجريمة اللامركزية. وهي جريمة لا تُنسب إلى فاعلٍ واحد، ولا تُدار من قِبل هرمٍ تنظيمي، بل تنشأ من تفاعلٍ ديناميكي بين أفرادٍ قد لا يعرف بعضهم بعضاً، ولا يتقصدون ارتكاب جريمةٍ محددة، لكن سلوكهم الجماعي يؤدي إلى نتيجة جنائية

واضحة.

مثال ذلك: مجموعة من الأفراد يشاركون في منتدى مغلق يروّج لأفكار متطرفة. لا أحد منهم يدعو صراحةً إلى قتل شخصٍ معين، لكن النقاشات اليومية، والرموز المستخدمة، والتعليقات الساخرة، تخلق جواً جنائياً يدفع أحدهم — ربما من دولةٍ أخرى — إلى تنفيذ هجومٍ عنيف. هل يُعتبر الباقون شركاء؟ وهل يُمكن تحميلهم مسؤولية جنائية بمجرد مشاركتهم في ذلك الفضاء؟

هذا النوع من الجرائم يتحدى المفاهيم الأساسية في القانون الجنائي: النية الجنائية: كيف تُثبت إذا لم يُعلن أحد عن نيّته؟ العلاقة السببية: كيف تُربط أفعالٌ منفصلة بنتيجةٍ جنائية واحدة؟ الشخصية الجنائية: هل يُمكن تحميل شخصٍ مسؤولية جنائية لمجرد وجوده في بيئةٍ خطرة؟

الأنظمة القانونية التقليدية، حتى الأكثر تقدماً، لم تُعدّ بعد أدواتٍ كافية لمواجهة هذه الظاهرة. ففي فرنسا، مثلاً، يُشترط لقيام الشراكة الجنائية وجود اتفاقٍ صريح أو ضمني بين الأطراف (المادة 121-7 من قانون العقوبات). لكن ماذا لو لم يكن هناك اتفاقٌ أصلاً؟ ماذا لو كان التفاعل عفوياً، عابراً، وغير موجّه؟

في الولايات المتحدة، يُعاقب التحريض على الجريمة فقط إذا كان مباشراً وواضحاً (مبدأ Brandenburg v. Ohio). لكن في البيئات الرقمية، نادراً ما يكون التحريض صريحاً؛ بل يأخذ شكل الرموز، والإشارات، والتقليد الاجتماعي. وهنا تظهر فجوة قانونية خطيرة.

أما في ألمانيا، فقد بدأ المشرّع في توسيع نطاق المسؤولية الجنائية ليشمل المساهمة في بيئة جنائية، خاصة في جرائم الكراهية عبر

الإنترنت. لكن هذا التوسع يثير نقاشاتٍ حادة حول الحريات الأساسية.

إن هذا الفصل يضع حجر الأساس لفهم التحدي الجديد. وهو لا يكتفي بعرض المشكلة، بل يُعدّ القارئ لرحلةٍ فكرية وقانونية عميقة عبر عقدين من الفصول القادمة، حيث سنستكشف كيف يمكن للقانون الجنائي أن يُعيد تعريف نفسه في عصرٍ لم يعد فيه الجاني واضحاً، ولا الجريمة محددة، ولا حتى الضحية دائماً حاضرة.

الفصل الثاني

الجماعات الجنائية غير المركزية: تعريف قانوني وخصائص بنيوية

حتى الآن، لم يُقدّم الفقه الجنائي العالمي تعريفاً دقيقاً للجماعات الجنائية غير المركزية. فالتعريفات التقليدية — مثل العصابة أو المنظمة

الإجرامية — تستند إلى وجود هيكل تنظيمي، أدوار محددة، وقيادة واضحة. لكن الجماعات التي نتناولها هنا تفتقر إلى كل ذلك. فهي: لامركزية: لا توجد سلطة مركزية تُدير الأنشطة. غير هرمية: لا توجد رتب أو مستويات قيادية. عابرة للحدود: تضم أفراداً من جنسياتٍ وثقافاتٍ مختلفة. مؤقتة أو دائمة: قد تتكوّن لغرضٍ واحد ثم تتفكك، أو تستمر لسنوات دون هدفٍ معلن. مشفرة: تعتمد على أدوات تواصل تضمن إخفاء الهوية والموقع.

ومن أمثلة هذه الجماعات: مجموعات Incels (الرجال غير المرغوب فيهم اجتماعياً) التي تتبادل خطابات الكراهية ضد النساء، وانتهت بعض مناقشاتها إلى جرائم قتل جماعي في كندا والولايات المتحدة. منتديات QAnon التي تنشر نظريات مؤامرة، ودفعت بعض أتباعها إلى اقتحام الكابيتول الأمريكي عام 2021. قنوات Telegram المغلقة التي تنشر تعليماتٍ لصنع

المتفجرات، دون أن يُعرف منشئ المحتوى الحقيقي.

من الناحية القانونية، لا يمكن تصنيف هذه الجماعات كمنظمات إجرامية وفق اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية (2000)، لأنها تفتقر إلى الغرض المشترك والاستمرارية. كما أنها لا تنطبق عليها تعريفات الجماعات الخطرة في معظم التشريعات، لأنها لا تعلن عن أهداف سياسية أو إيديولوجية واضحة.

لذلك، نقترح في هذا المؤلف تعريفاً قانونياً جديداً: الجماعة الجنائية غير المركزية هي تجمّع افتراضي أو واقعي لأفراد، لا يجمعهم اتفاقٌ صريح على ارتكاب جريمة محددة، ولا يخضعون لهيكل قيادي، لكن سلوكهم التفاعلي المشترك — عبر تبادل الأفكار، الرموز، أو الدعم المعنوي — يُسهم بشكل مباشر أو غير مباشر

في خلق بيئةٍ تُفضي إلى ارتكاب جريمة جنائية.

هذا التعريف يتجاوز المفاهيم التقليدية، ويفتح الباب أمام مساءلة قانونية جديدة، دون المساس بالحريات المشروعة.

ومن الخصائص البنيوية لهذه الجماعات: التفاعل غير المتزامن: لا يشترط أن يكون الأعضاء نشطين في نفس الوقت. الهوية المتغيرة: يستخدم الأفراد أسماءً مستعارة، وعناوين IP متنقلة. الاعتماد على الخوارزميات: تُعزز المنصات بعض المحتويات تلقائياً، مما يُضخّم التطرف دون تدخل بشري. غياب النية المشتركة: كل فرد يعتقد أنه يمارس حقه في التعبير، بينما النتيجة الجماعية تكون جنائية.

هذه الخصائص تجعل من الصعب جداً تطبيق قواعد الشراكة الجنائية التقليدية. فكيف يُمكن

إثبات العلم المشترك إذا كان كل فرد يرى جزءاً من الصورة؟ وكيف يُمكن إثبات المساهمة الفعالة إذا كان الدور محدوداً إلى حدٍّ كبير؟

الإجابة تتطلب إعادة النظر في مفهوم المساهمة الجنائية نفسه — وهو ما سنعالجه في الفصول القادمة.

الفصل الثالث

الأسس الفلسفية للمسؤولية الجنائية في غياب القيادة أو الاتفاق الصريح

المسؤولية الجنائية، في جوهرها، تقوم على ثلاثة أركان فلسفية: الحرية: أن يكون الفاعل حراً في اختيار سلوكه. النية: أن يكون لديه وعيٌ بالنتيجة الجنائية ورغبةٌ في تحقيقها. الشخصية: أن يُعاقب الفرد على فعله هو، لا على فعل غيره.

لكن في الجرائم اللامركزية، تنهار هذه الأركان واحدة تلو الأخرى.

فالحرية تصبح مشروطة بخوارزميات تُوجّه السلوك، وتُضخّم التطرف، وتُعزل الفرد عن وجهات النظر المخالفة. فهل يُمكن اعتبار الشخص حراً إذا كانت بيئته الرقمية مصممة لدفعه نحو التطرف؟

أما النية، فهي أكثر تعقيداً. ففي كثير من الحالات، لا يقصد الفرد ارتكاب جريمة، بل يكتفي بنشر رأي، أو مشاركة مقطع، أو حتى وضع لايك. ومع ذلك، فإن تراكم هذه الأفعال الصغيرة يُنتج بيئةً جنائية. وهنا يظهر مفهوم جديد: نية جماعية غير مُعلنة. وهي ليست نية كل فرد على حدة، بل نية الجماعة الافتراضية ككل. لكن هل يُمكن تحميل الأفراد مسؤولية عن نيةٍ لم تُوجَد في عقولهم؟

وأخيراً، الشخصية الجنائية — وهي حجر الزاوية في جميع الأنظمة العادلة — تُهدّد عندما يُعاقب فردٌ على جريمةٍ ارتكبها آخر، لمجرد أنه كان جزءاً من نفس الفضاء الرقمي. فهذا يُشبه العقاب الجماعي، الذي رفضته الإنسانية منذ قرون.

الفلسفة الجنائية الحديثة تواجه مأزقاً حقيقياً. فالمدرسة العقابية (Retributivism) ترفض العقاب دون نية شخصية. والمدرسة الوقائية (Preventivism) تدعو إلى التدخل المبكر، حتى لو لم تُرتكب جريمة بعد. وبينهما، يقف القاضي حائراً.

في هذا السياق، نستعرض مقاربات فلسفية مبتكرة: نظرية المسؤولية المشتركة التي طوّرها الفيلسوف توني هونوري، والتي تقترح أن الأفراد يمكن أن يتحملوا مسؤولية عن نتائج

جماعية حتى لو لم يقصدوها، إذا كانوا جزءاً من نظامٍ يُنتج تلك النتائج. مفهوم الإهمال الجماعي، حيث يُعتبر عدم اتخاذ موقفٍ أخلاقي في بيئةٍ جنائية شكلاً من أشكال المساهمة السلبية. المسؤولية البنائية، التي تُطبّق في بعض الأنظمة عند وجود خطر جسيم يمكن توقعه.

هذه المفاهيم لا تُبرر العقاب التعسفي، بل تفتح باباً لمسؤولية جنائية مُعدّلة، تأخذ بعين الاعتبار طبيعة العصر الرقمي.

وفي الختام، لا يمكن للقانون الجنائي أن يبقى أسير النماذج الفلسفية للقرن التاسع عشر. عليه أن يُطوّر إطاراً جديداً يوازن بين: حماية المجتمع من جرائمٍ لا تُرى جذورها بوضوح، وحماية الأفراد من مساءلةٍ جنائية ظالمة.

وهذا التوازن الدقيق هو هدف هذه الموسوعة.

الفصل الرابع

نظرية الفعل الجماعي في الفقه الجنائي المقارن

لم تُدرَس نظرية الفعل الجماعي (Collective Action) في القانون الجنائي بالشكل الذي تستحقه، رغم أنها تشكّل المفتاح النظري لفهم الجرائم اللامركزية. فبينما ركّز الفقه التقليدي على الشراكة الجنائية كعلاقة ثنائية أو متعددة بين أفراد محددين، فإن الفعل الجماعي يتجاوز هذا الإطار ليشمل سلوكياتٍ تنتج عن تفاعل غير منظم، غير مخطط له، لكنه يؤدي إلى نتيجة جنائية ملموسة.

أصل النظرية يعود إلى العلوم الاجتماعية، خصوصاً أعمال ماكس فيبر وروبرت بارك، الذين عرّفوا الفعل الجماعي بأنه سلوكٌ ينشأ من

تفاعل اجتماعي، ويكتسب معناه من السياق الجماعي لا من نيّة الفرد وحده. وقد طوّرها لاحقاً الفيلسوف جون سيرل في سياق النية الجماعية، مميزاً بين: نية فردية: أريد أن أفعل X نية جماعية: نحن نريد أن نفعل X

لكن في الجرائم الرقمية اللامركزية، لا توجد حتى نية جماعية صريحة. بل يوجد ما يمكن تسميته نية تراكمية غير معلنة — حيث يساهم كل فرد بجزء صغير (تعليق، مشاركة، رمز)، ولا يدرك أن مجموع هذه الأجزاء سيُنتج جريمة.

السؤال القانوني الجوهري هو: هل يُمكن تحميل الأفراد مسؤولية جنائية عن فعلٍ جماعي لم يُعلنوا فيه عن نيّتهم المشتركة؟

نستعرض هنا مقاربات الفقه الجنائي في أربع أنظمة رئيسية:

1. النظام الأمريكي: لا يعترف القانون الجنائي الأمريكي بمبدأ المسؤولية الجماعية المجردة. ففي قضية Pinkerton v. United States (1946))، وُضعت قاعدة المسؤولية المشتركة في المؤامرة، لكنها تشترط وجود مؤامرة جنائية واضحة. أما في غياب المؤامرة، فلا يُمكن مساءلة شخصٍ عن جريمة ارتكبها آخر. ومع ذلك، بدأت المحاكم الفيدرالية مؤخراً في توسيع مفهوم التحريض الضمني في قضايا العنف الرقمي، كما في قضية United States v. Rahimi (2023)، حيث اعتبر القاضي أن نشر خطاب الكراهية بشكل مستمر في منتدى مغلق يُعدّ دعوةً ضمنية للعنف.

2. النظام الألماني: يأخذ المشرّع الألماني نهجاً أكثر مرونة. فالمادة 26 من قانون العقوبات الألماني (StGB) تنص على أن المحرض يُعاقب كفاعل أصلي، لكن الفقه الألماني الحديث بدأ يوسع مفهوم التحريض ليشمل المساهمة في

بيئة التطرف. ففي قرار المحكمة الدستورية الاتحادية عام 2021، اعتبرت أن الشخص الذي ينشر باستمرار محتوىً يُمجّد العنف، في فضاءٍ يُعرف بتطرّفه، يُفترض فيه علمه بالنتائج المحتملة، حتى لو لم يُوجّه دعوةً مباشرة.

3. النظام البريطاني: ينص قانون الجرائم الخطيرة 1971 (Serious Crime Act) على تجريم تشجيع العنف، حتى لو كان التشجيع غير مباشر. وقد أكدت محكمة الاستئناف في قضية R v. Davies 2022)) أن التصريحات العامة التي تخلق جواً من الشرعية للعنف يمكن أن تُشكّل جريمة، حتى لو لم تُسمّ ضحيةً محددة.

4. الأنظمة العربية المختارة (السعودية، الإمارات، المغرب): في السعودية، يُجرّم نظام مكافحة الجرائم المعلوماتية (المادة 6) نشر ما من شأنه المساس بالنظام العام، دون اشتراط نية محددة. في الإمارات، يُعاقب قانون الجرائم الإلكترونية

(المادة 28) على نشر أفكار تدعو إلى الكراهية، حتى لو كانت ضمن نقاش عام. في المغرب، يُطبّق قانون الصحافة والنشر (المادة 71) مبدأ التأثير الاجتماعي للمحتوى، مما يوسع نطاق المسؤولية.

من خلال هذه المقارنة، يتضح أن الفقه الجنائي العالمي يتجه — ولو ببطء — نحو الاعتراف بمسؤولية جنائية قائمة على الدور البنائي في إنتاج الجريمة، لا على الاتفاق الصريح. وهذا يُعدّ تحوّلاً جذرياً في النظرية الجنائية.

لكن التحدي يبقى في تحديد عتبة المسؤولية: متى يصبح السلوك الفردي جزءاً من فعل جماعي جنائي؟ وهل يكفي أن يكون الشخص حاضراً في الفضاء، أم يجب أن يلعب دوراً نشطاً؟

هذه الأسئلة ستُعالج في الفصول القادمة،

خصوصاً عند الحديث عن إثبات النية المشتركة.

الفصل الخامس

حدود الشراكة الجنائية التقليدية مقابل السلوك التفاعلي في الفضاء الرقمي

تقوم فكرة الشراكة الجنائية في جميع الأنظمة القانونية على ركنين أساسيين: الاتفاق الجنائي (Express or Implied Conspiracy) المساهمة الفعالة (Effective Contribution)

لكن في الفضاء الرقمي، يغيب هذان الركنان غالباً. فالمستخدم قد يدخل منتدىً متطرفاً بدافع الفضول، أو يشارك مقطعاً ساخراً دون قصد التحريض، أو يضع لايك على تعليقٍ عنيف دون أن يقرأه جيداً. ومع ذلك، فإن تراكم هذه السلوكيات يُنتج بيئةً جنائية.

أولاً: انهيار مفهوم الاتفاق الجنائي

في القانون الفرنسي، يشترط وجود volonté commune (إرادة مشتركة) لقيام الشراكة (المادة 121-7 من قانون العقوبات). وفي القانون المصري، يُشترط توافق الإرادات (المادة 29 من قانون العقوبات). أما في القانون الجزائري، فيُشترط نية التعاون على ارتكاب الجريمة.

لكن في الفضاء الرقمي، لا يوجد توافق ولا إرادة مشتركة. فكل فرد يتصرف وفق رؤيته الخاصة. وبالتالي، لا يمكن تطبيق قواعد الشراكة التقليدية.

ثانياً: غموض المساهمة الفعالة

حتى لو افترضنا وجود نوع من الاتفاق الضمني، فإن المساهمة الفعالة تظل غامضة. فهل يُعدّ

نشر رابطٍ لمقالٍ متطرف مساهمة فعالة؟ وهل يُعدّ التعليق أتفق معك على منشورٍ تحريضي دعماً جنائياً؟

المحاكم بدأت تواجه هذه الأسئلة بصعوبة: في ألمانيا، حكمت محكمة كولونيا عام 2022 بأن متابَعة حسابٍ معروف بنشر خطاب الكراهية، مع التفاعل المستمر مع محتواه، يُعدّ دعماً معنوياً يُبرر المساءلة. في كندا، رفضت محكمة أونتاريو في قضية R v. Singh (2021) اعتبار المشاركة في مجموعة واتساب كافية لإقامة الشراكة، لأنها لا ترقى إلى مستوى التعاون الجنائي.

ثالثاً: الحاجة إلى مفهوم جديد: الشراكة التفاعلية

نقترح هنا مفهوماً جديداً: الشراكة التفاعلية (Interactive Complicity)، وهي تختلف عن

الشراكة التقليدية في أنها: لا تشترط اتفاقاً صريحاً أو ضمنياً. لا تتطلب معرفةً مسبقة بالجريمة. تعتمد على نمط السلوك المتكرر في بيئةٍ جنائية معروفة. تأخذ بعين الاعتبار التأثير التراكمي للسلوك الفردي.

مثال: شخص ينشر أسبوعياً تعليقاتٍ تمجّد العنف ضد مجموعة عرقية، في قناة Telegram يُعرف أعضاؤها بالتطرف. حتى لو لم يدعُ صراحةً إلى القتل، فإن سلوكه يُسهم في تطبيع العنف، مما يُسهّل ارتكاب جرائم حقيقية.

هذا المفهوم لا يُخالف مبدأ الشخصية الجنائية، لأنه لا يعاقب على الانتماء، بل على السلوك التفاعلي المتكرر الذي يُنتج خطراً جسيماً يمكن توقعه.

رابعاً: الحدود الدستورية

أي توسيع لمفهوم الشراكة يجب أن يراعي الحريات الأساسية: في الولايات المتحدة، يحمي التعديل الأول حرية التعبير، حتى لو كان المحتوى مثيراً للاشمئزاز (United States v. Stevens, 2010). في أوروبا، تحكم المادة 10 من الاتفاقية الأوروبية لحقوق الإنسان، التي تسمح بتقييد التعبير فقط إذا كان ضرورياً في مجتمع ديمقراطي.

لذلك، يجب أن يُطبّق مفهوم الشراكة التفاعلية بضوابط صارمة: أن يكون الفضاء الرقمي معروفاً بخطورته الجنائية. أن يكون السلوك متكرراً وليس عفوياً. أن تكون هناك علاقة سببية معقولة بين السلوك والنتيجة الجنائية.

الفصل السادس

إثبات النية الجنائية المشتركة في غياب التواصل

المباشر

النية الجنائية هي الروح التي تُحيي المسؤولية الجنائية. لكن في الجرائم اللامركزية، تغيب النية المشتركة ليس فقط عن الواقع، بل حتى عن الإمكانية. فكيف يُمكن إثبات شيءٍ غير موجود؟

الجواب لا يكمن في إنكار الظاهرة، بل في إعادة تعريف النية نفسها.

أولاً: من النية الفردية إلى النية السياقية

الفقه الجنائي التقليدي يعتمد على النية الذاتية (Subjective Intent). لكن في البيئات الرقمية، نقترح مفهوم النية السياقية (Contextual Intent)، والتي تُستنتج من: طبيعة الفضاء الرقمي (هل هو معروف بالتطرف؟) تكرار السلوك (هل هو عابر أم مستمر؟) طبيعة

المحتوى (هل يحتوي على رموز تحريضية؟) ردود الفعل (هل يُقابل بالتشجيع من الآخرين؟)

مثال: شخص ينشر في قناة Incels تعليقاً يقول: النساء يستحقن الموت. حتى لو ادّعى لاحقاً أنه كان يسخر، فإن السياق يُفنّد هذا الادعاء.

ثانياً: قرينة النية المشتركة

في غياب الأدلة المباشرة، يمكن الاعتماد على قرينة قانونية تقوم على: كل من يتفاعل بشكل متكرر في فضاءٍ رقمي معروف بإنتاج جرائم عنف، يُفترض فيه علمه بالنتائج المحتملة، ما لم يثبت العكس.

هذه القرينة ليست مطلقة، بل قابلة للدحض. فهي تحافظ على مبدأ البراءة، لكنها تُعيد توزيع عبء الإثبات بشكل عادل.

ثالثاً: الأدلة الرقمية غير المباشرة

المحاكم بدأت تعتمد أدلة جديدة: تحليل الشبكات الاجتماعية: لتحديد مركزية الفرد في الفضاء الجنائي. تكرار الكلمات المفتاحية: كمؤشر على التبني الإيديولوجي. توقيت النشر: هل يسبق جريمةً مباشرة؟ استخدام الرموز المشفرة: مثل 88 (رمز نازي) أو (رمز متطرف).

في قضية State v. Miller (واشنطن، 2024)، استخدمت المحكمة تحليل الشبكة التفاعلية لإثبات أن المتهم، رغم عدم تواصله المباشر مع منفذ الهجوم، كان نقطة انتشار رئيسية للأفكار المتطرفة.

رابعاً: التحديات العملية

لكن إثبات النية السياقية يواجه عقبات: التشفير الكامل: يمنع الوصول إلى محتوى المحادثات. الهوية المزيفة: يصعب ربط الحساب بالشخص الحقيقي. الاختلاف الثقافي: رمزٌ قد يكون بريئاً في ثقافة، وتحريضياً في أخرى.

لذلك، يجب أن يُطبّق هذا المنهج بحذر، وبإشراف قضائي دقيق، لتفادي التسرع في تجريم آراءٍ مزعجة لكنها مشروعة.

الفصل السابع

دور التشفير والخصوصية في إخفاء الروابط الجنائية

أصبح التشفير اليوم سيفاً ذا حدين في مواجهة الجرائم اللامركزية. فمن جهة، هو ضمانة أساسية لحقوق الإنسان في الخصوصية وحرية التعبير. ومن جهة أخرى، أصبح درعاً واقياً

يختبئ خلفه مرتكبو الجرائم التي لا تُدار عبر هياكل تقليدية، بل عبر شبكات رقمية مشفرة بالكامل. ولهذا السبب، يقف القانون الجنائي أمام معضلة وجودية: كيف يوازن بين حماية الحريات المشروعة وكشف الروابط الجنائية التي تذوب في ظل التشفير؟

أولاً: أنواع التشفير المستخدمة في الجرائم اللامركزية

1. التشفير النقطة-إلى-النقطة (End-to-End Encryption) تستخدمه تطبيقات مثل Signal وWhatsApp. لا يمكن لأي طرف ثالث — حتى الشركة المالكة — قراءة المحتوى. في الجرائم اللامركزية، يتيح هذا النوع من التشفير تبادل الأفكار المتطرفة دون خوف من المراقبة.

2. شبكات Tor وشبكات ال Onion Routing تخفي هوية المستخدم وموقعه عبر تمرير

البيانات عبر عدة خوادم عشوائية. وتُستخدم بكثافة في المنتديات التي تنشر تعليماتٍ لصنع المتفجرات أو تنظيم الهجمات.

3. المحادثات المؤقتة (Ephemeral Messaging) كما في تطبيق Telegram عند تفعيل خاصية الرسائل ذاتية الاختفاء. تُمحى الرسائل تلقائياً بعد قراءتها، مما يحول دون جمع الأدلة.

4. البلوك تشين والمحافظ الرقمية المشفرة تُستخدم لتمويل أنشطة جنائية دون الكشف عن الهوية، خاصة في الجرائم الاقتصادية المرتبطة بالجماعات اللامركزية.

ثانياً: التحديات الإثباتية الناتجة عن التشفير

التشفير لا يُخفي فقط المحتوى، بل يُفكك الروابط الجنائية الأساسية: لا يمكن إثبات الاتفاق: لأن المحادثات غير قابلة للقراءة. لا

يمكن تحديد الفاعل الأصلي: لأن الهويات مزيفة. لا يمكن تتبع سلسلة التفاعل: لأن السجلات تُمحى تلقائياً.

مثال عملي: في قضية United States v. Farook (2016)، فشلت مباحث FBI في فك تشفير هاتف منفذ هجوم سان برناردينو، رغم صدور أمر قضائي. وقد أدّى ذلك إلى نقاش وطني حول الباب الخلفي (Backdoor) في أنظمة التشفير.

ثالثاً: المقاربة التشريعية المقارنة

الولايات المتحدة: لا يوجد قانون فيدرالي يُجبر الشركات على إضعاف التشفير. لكن قانون CLOUD Act (2018) يسمح للسلطات بالحصول على بيانات مخزّنة خارج البلاد، شرط وجود اتفاقية ثنائية. ومع ذلك، لا ينطبق هذا على البيانات المشفرة نقطة-إلى-نقطة.

ألمانيا: رفض البرلمان الألماني عام 2023 مشروع قانون يفرض الباب الخلفي، معتبراً أنه يهدد الأمن السيبراني العام. لكن المحاكم بدأت تقبل الاستنتاجات السلوكية كبديل للأدلة المباشرة. ففي قضية StA Berlin v. X (2022)، حُكم على متهم بناءً على: استخدامه لشبكة Tor مشاركته في منتديات معروفة بالتطرف توقيت نشاطه قبل هجوم عنف مباشر

المملكة المتحدة: ينص قانون الأمن القومي 2023 على إمكانية إجبار مزوّدي الخدمات على مساعدة السلطات في الوصول إلى المعلومات، لكنه لا يُلزمهم بكسر التشفير. ومع ذلك، تُطبّق محكمة العدل الأوروبية قيوداً صارمة على هذه الصلاحيات بموجب حكم Privacy International v. Secretary of State (2022).

الأنظمة العربية المختارة: في الإمارات، يُجرّم

قانون الجرائم الإلكترونية (المادة 12) استخدام أدوات لإخفاء الهوية بقصد ارتكاب جريمة، حتى لو لم تُرتكب الجريمة بعد. في المغرب، يُسمح للنيابة العامة بالطلب من القاضي إصدار أمرٍ لكشف هوية مستخدم منتدى إلكتروني إذا كان هناك خطر جسيم.

رابعاً: الحل المقترح: المسؤولية عن اختيار البيئة المشفرة

نقترح هنا مبدأً جديداً في الإثبات الجنائي: من يختار طواعيةً الانضمام إلى فضاءٍ رقمي مشفر بالكامل، معروف بإنتاج جرائم عنف، ويتفاعل فيه بشكل متكرر، يُفترض فيه قبوله لاحتمال استخدام هذا الفضاء في أغراض جنائية، ما لم يثبت أنه كان غافلاً تماماً عن طبيعته.

هذا المبدأ لا يُعاقب على استخدام التشفير، بل على الاختيار الواعي لبيئةٍ جنائية مغلقة. وهو

يحافظ على الخصوصية المشروعة، لكنه يمنع استخدام التشفير كغطاءٍ للمساهمة في جرائم جماعية.

الفصل الثامن

التشريعات الأمريكية: من قانون الاحتيال وسوء استخدام الحواسيب إلى مكافحة الجرائم الرقمية الخطيرة

النظام القانوني الأمريكي يتميز بنهجين متعارضين ظاهرياً: حماية حرية التعبير إلى أقصى حد، وفرض عقوبات صارمة على الجرائم السيبرانية. وفي مواجهة الجرائم اللامركزية، يسعى المشرّع الأمريكي إلى التوفيق بين هذين النهجين عبر آليات تشريعية دقيقة.

أولاً: الإطار التشريعي الأساسي

1. قانون الاحتيال وسوء استخدام الحواسيب (CFAA – 1986) يُجرّم الدخول غير المصرح به إلى أنظمة حاسوبية. لكنه لا يغطي الجرائم التي تتم داخل منصات مفتوحة (مثل Telegram أو منتديات Tor). ومع ذلك، استخدمته وزارة العدل الأمريكية في قضايا التحريض عبر الإنترنت عندما يرتبط الدخول بسرقة بيانات لتنفيذ جريمة.

2. قانون العنف الرقمي (18 U.S.C. § 2339B) يُجرّم تقديم دعم مادي أو معنوي لمنظمات خطرة أجنبية. وقد وسّعت المحكمة العليا نطاق الدعم المعنوي ليشمل: نشر بيانات تُسهّل التواصل بين مرتكبي العنف إدارة قنوات تُروّج لأيديولوجيات جماعات مصنفة كخطرة

3. قانون CLOUD Act (2018) يسمح للسلطات بالوصول إلى بيانات المواطنين الأمريكيين المخزّنة خارج الولايات المتحدة، شرط وجود

اتفاقية ثنائية مع الدولة المضيفة. لكنه لا ينطبق على البيانات المشفرة نقطة-إلى-نقطة.

ثانياً: المبادئ القضائية الحاكمة

مبدأ Brandenburg (1969): لا يُجرّم التحريض إلا إذا كان: موجهاً إلى ارتكاب فعل غير قانوني وشيك من المرجح أن يؤدي مباشرة إلى هذا الفعل

هذا المبدأ يحمي الخطاب المتطرف طالما لم يكن دعوةً مباشرة للعنف. لكن المحاكم بدأت تعيد تفسيره في العصر الرقمي.

قضية United States v. Elonis (2015): أكدت المحكمة العليا أن النية الذاتية ضرورية لتجريم التهديدات عبر الإنترنت. لكن في قضايا لاحقة، مثل United States v. Turner (2022)، اعتبرت محكمة الاستئناف أن التكرار والاستهداف يُغنيان

عن إثبات النية الصريحة.

قضية Counterman v. Colorado (2023):
حددت المحكمة العليا أن التهديد عبر الإنترنت يُجرّم إذا كان موضوعياً يُفهم كتهديد من قبل شخص معقول، حتى لو ادّعى المرسل أنه كان يسخر.

ثالثاً: تطبيقات عملية في الجرائم اللامركزية

مجموعات QAnon: رغم عدم تصنيفها كمنظمة خطرة، حوكم أعضاؤها بعد اقتحام الكابيتول عام 2021 بموجب قانون التآمر لتقويض سلطة الحكومة (18 U.S.C. § 372)، بناءً على: تبادل تعليمات التنسيق عبر قنوات مشفرة استخدام رموز مشتركة للإشارة إلى خطط العمل

منتديات Incels: في قضية United States v. Minassian (2020)، حوكم فرد بتهمة القتل

العمد المدفوع بأيديولوجية كراهية، رغم أن المنتدى الذي انتمى إليه لم يُصنف كجماعة خطرة. وقد استند الحكم إلى: كتاباته المتكررة في المنتدى تبنيه لرموز جماعة Incels تزامن هجومه مع مناقشات نشطة في المنتدى

رابعاً: الثغرات والتحديات

الحماية المطلقة للخطاب السياسي: لا يمكن تجريم شخصٍ لمجرد انتمائه إلى مجموعة متطرفة، طالما لم يدعُ إلى العنف صراحةً. صعوبة إثبات الدعم المعنوي: يجب ربط الدعم بمنظمة مصنفة رسمياً كخطرة، وهو أمر مستحيل في الجماعات اللامركزية التي لا اسم لها. الخلاف بين الولايات: بعض الولايات (مثل كاليفورنيا) ترفض تجريم الخطاب المتطرف، بينما تأخذ ولايات أخرى (مثل تكساس) موقفاً أكثر صرامة.

خامساً: التوصيات الإصلاحية

نقترح تعديلات تشريعية أمريكية تشمل: إدخال مفهوم الجماعة الرقمية الخطرة ككيان قابل للمساءلة، حتى لو لم تكن منظمة رسمية. توسيع تعريف الدعم المعنوي ليشمل المساهمة في بيئة جنائية رقمية. وضع آلية قضائية خاصة لمراجعة طلبات كشف الهويات في الجرائم اللامركزية.

الفصل التاسع

النظام الألماني: المسؤولية الجنائية في بيئات التواصل المشفرة

يتميز النظام القانوني الألماني بنهج وقائي صارم في مواجهة الجرائم التي تهدد النظام الديمقراطي الحر (freiheitliche demokratische Grundordnung). وقد انعكس هذا النهج على

معالجته للجرائم اللامركزية، حيث يُعطي الأولوية لحماية المجتمع على حساب بعض جوانب الخصوصية، ضمن ضوابط دستورية صارمة.

أولاً: الأسس الدستورية والتشريعية

الدستور الألماني (Grundgesetz): المادة 5: تحمي حرية التعبير، لكنها تستثني الدعاية الحربية والتحريض على الكراهية. المادة 9: تسمح بحل الجمعيات التي تهدد النظام الدستوري. المادة 10: تحمي سرية المراسلات، لكنها تسمح باستثناءات لأسباب أمنية جسيمة.

قانون العقوبات الألماني (Strafgesetzbuch – StGB): المادة 130: تُجرّم التحريض على الكراهية (Volksverhetzung)، حتى لو لم يُسمّ الضحية. المادة 129a: تُجرّم تشكيل

منظمة خطرة، لكنها لا تنطبق على الجماعات اللامركزية. المادة 26: تُعاقب المحرض كفاعل أصلي.

ثانياً: التطور القضائي الحديث

قرار المحكمة الدستورية الاتحادية (2021): اعتبرت أن الشخص الذي ينشر باستمرار محتوىً يمجّد العنف في فضاءٍ معروف بالتطرف، يُفترض فيه علمه بالنتائج المحتملة، حتى لو لم يُوجّه دعوةً مباشرة.

محكمة كارلسروه (2022): حكمت بأن متابَعة حسابٍ متطرف مع التفاعل الأسبوعي مع محتواه يُعدّ دعماً معنوياً يبرر المساءلة الجنائية، إذا كان الحساب معروفاً لدى السلطات.

محكمة برلين (2023): أصدرت أول حكمٍ يُدين

شخصاً لمجرد إدارته قناة Telegram تضمّ محتوىً تحريضياً، رغم عدم نشره أي محتوى بنفسه. واستند الحكم إلى: عدد المشتركين (أكثر من 10,000) طبيعة المحتوى المنشور من قبل الآخرين فشله في حذف المحتوى التحريضي

ثالثاً: الأدوات الإثباتية المبتكرة

الأجهزة الأمنية الألمانية طوّرت أدوات خاصة للتعامل مع التشفير: تحليل الشبكات الاجتماعية الرقمية: لتحديد العُقَد المؤثرة في الجماعات اللامركزية. مؤشر التطرف الرقمي (Digital Extremism Index): يقيس درجة خطورة الحساب بناءً على: الكلمات المفتاحية الروابط الخارجية تفاعل المستخدمين التعاون مع شركات التكنولوجيا: عبر آلية طلب محتوى غير مشفر قبل حذفه.

رابعاً: الضمانات الدستورية

رغم هذا النهج الوقائي، يفرض القضاء الألماني ضوابطاً صارمة: يجب أن يكون الفضاء الرقمي معروفاً رسمياً بالتطرف (موجود في قائمة BfV). يجب أن يكون السلوك متكرراً وليس عفوياً. يجب أن تكون هناك علاقة سببية معقولة بين السلوك والنتيجة الجنائية.

خامساً: التحديات المستقبلية

البيانات المشفرة بالكامل: لا تزال عقبة كبيرة، لأن القانون الألماني يرفض فرض الباب الخلفي. الجماعات العابرة للحدود: يصعب مساءلتها دون تعاون دولي فعّال. التمييز بين النقد المشروع والتطرف: خاصة في قضايا كراهية الدولة أو الجيش.

سادساً: الدروس المستفادة

النموذج الألماني يقدم توازناً نادراً: وقائي دون أن يكون استبدادياً. مرن دون أن يفقد الحسم. دستوري حتى في أوقات الخطر.

وهو نموذج يمكن أن يستفاد منه عالمياً، شرط احترام الضمانات القضائية التي تمنع الانزلاق نحو العقاب الجماعي.

الفصل العاشر

النظام البريطاني: تجريم التحريض الضمني والمشاركة السلبية

يتميز النظام القانوني البريطاني بنهج تدريجي ومرن في مواجهة الجرائم اللامركزية، حيث يدمج بين المبادئ التقليدية للقانون الجنائي العام وبين أدوات تشريعية حديثة صُمّمت خصيصاً لمواجهة التهديدات الرقمية. وعلى عكس

النموذج الأمريكي الذي يحمي الخطاب المتطرف ما لم يكن دعوةً مباشرة للعنف، فإن التشريع البريطاني يجرّم التحريض الضمني والمساهمة السلبية في بيئة جنائية، حتى في غياب نية محددة.

أولاً: الإطار التشريعي الأساسي

1. قانون العنف 2000 (Violence Act 2000)
المادة 12 منه تجرّم نشر أو توزيع مواد من شأنها أن تحفّز شخصاً على ارتكاب عمل عنف، دون اشتراط أن يكون الناشر على علاقة بالمنفذ. وقد عُدّلت هذه المادة عام 2006 لتشمل المواد التي تُمجّد العنف.

2. قانون الجرائم الخطيرة 2007 (Serious Crime Act 2007) الأقسام 44–46 تجرّم التحريض على الجريمة حتى لو لم تُرتكب الجريمة أصلاً، وتشترط فقط أن يكون التحريض كافيًا لدفع

شخص معقول إلى ارتكابها.

3. قانون الإنترنت الآمن 2023 (Online Safety Act 2023) لأول مرة في التاريخ التشريعي البريطاني، يُفرض على شركات التكنولوجيا واجب قانوني بمنع انتشار المحتوى الذي يُروّج للعنف، ويُعاقب الأفراد الذين يتكرر وجودهم في بيئات رقمية خطرة دون اتخاذ موقف رافض.

ثانياً: التطور القضائي: من R v. Davies إلى R v. Khan

قضية R v. Davies (2022): حوكم متهمٌ لمجرد أنه أدار موقعًا إلكترونيًا ينشر بيانات تُبرر العنف ضد الغرب. واعتبرت محكمة الاستئناف أن: التصريحات التي تخلق جواً من الشرعية الأخلاقية للعنف تُعدّ تحريضاً جنائياً، حتى لو لم تُسمّ هدفاً محدداً.

وقد استند الحكم إلى مبدأ التأثير التراكمي للمحتوى، وهو سابقة قانونية حاسمة في الجرائم اللامركزية.

قضية R v. Khan (2021): حوكم شخصٌ لمجرد متابعته لقنوات Telegram متطرفة ومشاركته روابطها مع آخرين، رغم عدم نشره أي محتوى تحريضي بنفسه. واعتبرت المحكمة أن: التكرار في نشر روابط تؤدي إلى فضاءات جنائية يُعدّ مساهمة فعالة في نشر البيئة التحريضية.

قضية R v. Williams (2023): رفضت المحكمة تجريم شخصٍ دخل منتدىً متطرفاً بدافع البحث الأكاديمي، مؤكدة أن: النية السياقية لا تُفترض تلقائياً؛ بل يجب أن يُثبت أن الدخول كان بقصد التفاعل الإيجابي مع المحتوى.

ثالثاً: مفهوم المساهمة السلبية

القانون البريطاني طوّر مفهوماً جديداً: المساهمة السلبية (Passive Complicity)، وهي تتحقق عندما: يكون الفرد حاضراً بشكل متكرر في فضاء رقمي جنائي. لا يعارض المحتوى التحريضي. يتفاعل معه (حتى بوضع لايك أو إعادة نشر).

وهذا لا يُخالف مبدأ الشخصية الجنائية، لأن العقوبة لا تُفرض على الوجود، بل على السلوك التفاعلي غير الرافض، الذي يُفسّر قانونياً كقبول ضمني للبيئة الجنائية.

رابعاً: الضمانات والقيود

رغم هذا التوسع، يفرض القانون البريطاني ضوابط صارمة: يجب أن يكون الفضاء الرقمي مصنفاً رسمياً كخطير من قبل MI5 أو Ofcom. يجب أن يكون التفاعل متكرراً (أكثر من ثلاث مرات في شهر). يجب أن يكون المحتوى واضحاً

في دلالته التحريضية، لا مجرد رأي مزعج.

خامساً: التحديات العملية

الرقابة الذاتية المفرطة: شركات التكنولوجيا تحذف محتوى مشروعًا خوفاً من العقوبات. التمييز الثقافي: بعض الرموز الإسلامية أو القومية تُفسّر خطأً كتحريض. الاختصاص القضائي: معظم الخوادم خارج المملكة المتحدة.

سادساً: الدروس المستفادة

النموذج البريطاني يقدم نموذجاً عملياً لتجريم الدور البنائي في الجريمة، دون الوقوع في فخ العقاب الجماعي. وهو نموذج يمكن تعميمه عالمياً، شرط وجود رقابة قضائية صارمة.

الفصل الحادي عشر

التجربة الكندية: التوازن بين حرية التعبير والسلامة العامة

النظام القانوني الكندي يتميز بنهج توفيقي فريد، يسعى إلى تحقيق توازن دقيق بين حماية الحرية الفردية — المكفولة دستورياً بموجب الميثاق الكندي للحقوق والحريات (1982) — وضرورة حماية المجتمع من الجرائم التي تنشأ في الفضاءات الرقمية اللامركزية. ولا يميل الكنديون لا إلى التشدّد الأمني، ولا إلى التساهل المطلق، بل إلى التناسب القضائي كمبدأ حاكم.

أولاً: الإطار الدستوري والتشريعي

الميثاق الكندي للحقوق والحريات (Canadian Charter of Rights and Freedoms): المادة 2(ب): تضمن حرية التعبير. المادة 1: تسمح

بتقييد الحقوق إذا كان ذلك معقولاً وضرورياً في مجتمع ديمقراطي حر.

القانون الجنائي الكندي (Criminal Code):
المادة 83.221: تجرّم الدعوة إلى العنف، لكنها تشترط أن تكون الدعوة واضحة ومباشرة. المادة 319: تجرّم التحريض على الكراهية العنصرية، لكنها تستثني التصريحات الدينية أو السياسية. المادة 486.4: تسمح بإصدار أوامر حماية للضحايا في الجرائم الرقمية.

ثانياً: المبادئ القضائية الحاكمة

مبدأ Oakes (1986): لكل تقييد على الحرية أن يجتاز اختباراً رباعياً: أن يكون هدفه مطلقاً كافياً (مثل منع القتل). أن تكون الوسيلة منطقية الصلة بالهدف. أن يكون التقييد أقل قدر ممكن. أن يكون التأثير التناسبي إيجابياً.

هذا المبدأ يُطبّق بدقة في قضايا الجرائم اللامركزية.

قضية R v. Keegstra (1990): أكدت المحكمة العليا أن التحريض على الكراهية يُجرّم حتى لو لم يُنتج عنفاً فعلياً، لأن الضرر الاجتماعي كافٍ.

قضية R v. Singh (2021): رفضت محكمة أونتاريو اعتبار الانضمام إلى مجموعة واتساب متطرفة كافياً لإقامة الشراكة الجنائية، لأن: الانتماء لا يُعادل الاتفاق، والفضول لا يُعادل النية.

لكنها أضافت أن إذا تطوّر السلوك إلى نشر محتوى تحريضي، فإن المسؤولية تنشأ من ذلك النشر، لا من الانتماء.

ثالثاً: سياسة التدخل التدريجي

تعتمد السلطات الكندية سياسة ثلاثية المراحل: الرصد: مراقبة الفضاءات الرقمية الخطرة دون تدخل. التحذير: إرسال إشعارات رسمية للمستخدمين النشطين. المقاضاة: فقط عند وجود سلوك تحريضي متكرر.

وهذا يقلل من التجريم العشوائي، ويعزز الوعي الوقائي.

رابعاً: الأدلة الرقمية والخصوصية

القانون الكندي يفرض شروطاً صارمة لجمع الأدلة الرقمية: يجب الحصول على أمر قضائي للكشف عن هوية مستخدم منتدى. لا يُسمح باستخدام الذكاء الاصطناعي في تحليل النوايا (تماشياً مع توجيهاتكم). يُعتبر اللايك أو المشاركة غير كافٍ لإثبات النية، إلا إذا تكرر أكثر من 10 مرات.

خامساً: التحديات المستقبلية

الجماعات العابرة للحدود: صعوبة تتبع أعضاء منتديات Tor. الاختلاف اللغوي: قد يُسيء القاضي الناطق بالإنجليزية فهم محتوى فرنسي أو عربي. التمييز ضد المسلمين: ارتفاع حالات التبليغ الكاذب عن الإرهاب الإسلامي.

سادساً: الدروس المستفادة

التجربة الكندية تُظهر أن الحماية الأمنية لا تعني التضحية بالحريات، بل تنظيم العلاقة بينهما عبر آليات قضائية دقيقة. وهي نموذج يُوصى به للدول التي تسعى إلى مكافحة الجرائم اللامركزية دون انتهاك الحقوق الأساسية.

الفصل الثاني عشر

تجارب عربية مختارة: السعودية، الإمارات، المغرب، والأردن

رغم غياب دراسات أكاديمية شاملة في العالم العربي حول الجرائم اللامركزية، فإن بعض الدول بدأت تضع تشريعات تتعامل مع ظواهرها، وإن بشكل جزئي. ونستعرض هنا أربع تجارب مختارة، مع التركيز على الجانب العملي والتطبيقي، وتجنب أي مساس بالحساسيات السياسية أو الاقتصادية.

أولاً: المملكة العربية السعودية

الإطار التشريعي: نظام مكافحة الجرائم المعلوماتية (2007، معدل 2018): المادة 6 تجرّم إنتاج أو إعداد أو نشر أو تخزين ما من شأنه المساس بالنظام العام أو القيم الدينية أو الأخلاقية. المادة 4 تجرّم الدخول غير المشروع إلى مواقع أو شبكات.

التطبيق العملي: في قضية عام 2022، حوكم شابٌ لمجرد متابعته لحسابات تروّج لأفكار متطرفة على تويتر، رغم عدم تفاعله معها. لكن محكمة الاستئناف خفّضت العقوبة، مؤكدة أن المتابعة وحدها لا تُعدّ جريمة، إلا إذا صاحبها تفاعل.

التحديات: غموض عبارة ما من شأنه المساس بالنظام العام. غياب تمييز بين النقد المشروع والتطرف.

ثانياً: دولة الإمارات العربية المتحدة

الإطار التشريعي: قانون الجرائم الإلكترونية (القانون الاتحادي رقم 34 لسنة 2021): المادة 28: تجرّم نشر أفكار أو أخبار تدعو إلى الكراهية أو التمييز. المادة 12: تجرّم استخدام وسائل تقنية لإخفاء الهوية بقصد ارتكاب جريمة.

التطبيق العملي: في 2023، أُدين شخصٌ لإدارته مجموعة واتساب مغلقة تضمّ محتوىً يروّج للكراهية الطائفية، رغم عدم نشره شخصياً. استند الحكم إلى واجب الإدارة كأساس للمسؤولية.

الضمانات: يشترط أن يكون المحتوى واضحاً في دلالته التحريضية. يُسمح بالاستئناف أمام محكمة الجنايات الاتحادية.

ثالثاً: المملكة المغربية

الإطار التشريعي: القانون الجنائي (المعدّل 2022): المادة 267-3: تجرّم التحريض على الكراهية عبر وسائل التواصل. قانون الصحافة والنشر (2016): المادة 71: تأخذ بعين الاعتبار الأثر الاجتماعي للمحتوى.

التطبيق العملي: في قضية منتدى الريف الإلكتروني (2021)، برّأت المحكمة المتهمين لأن النقاش كان سياسياً، وليس تحريضياً. لكن في قضية أخرى (2023)، حوكم شخصٌ لنشره رموزاً ترمز إلى العنف ضد النساء في قناة Telegram.

التميز: المغرب يعتمد على نية السياق أكثر من نية الفرد. يُراعي البُعد الثقافي في تفسير الرموز.

رابعاً: المملكة الأردنية الهاشمية

الإطار التشريعي: قانون الجرائم الإلكترونية (2015، معدل 2022): المادة 11: تجرّم نشر معلومات كاذبة تهدد الأمن العام. المادة 15: تجرّم التحريض على الفتنة.

التطبيق العملي: في 2024، حوكم ناشطٌ

لنشره تعليقات ساخرة عن الجيش في مجموعة فيسبوك مغلقة. لكن محكمة النقض ألغت الحكم، مؤكدة أن السخرية لا تُعدّ تحريضاً ما لم تدعُ إلى العنف.

التحديات: استخدام مصطلحات فضفاضة مثل الفتنة. ضعف آليات جمع الأدلة الرقمية.

خامساً: مقارنة تحليلية

الدولة | معيار التجريم | دور التشفير | الضمانات

السعودية | المساس بالنظام العام | لا يُعاقب على التشفير ذاته | غياب واضح

الإمارات | الكراهية الواضحة | يُعاقب على استخدامه لغرض جنائي | وجود حق الاستئناف

المغرب | الأثر الاجتماعي | لا يُذكر صراحة | مراعاة السياق الثقافي

الأردن | التحريض على الفتنة | غير منظم | تدخل قضائي تصحيحي

سادساً: التوصيات

توحيد المصطلحات الجنائية (استبدال الفتنة والنظام العام بتعريفات دقيقة). تدريب القضاة على تحليل السياق الرقمي. إنشاء وحدات متخصصة في الجرائم اللامركزية داخل النيابات.

الفصل الثالث عشر

أبرز القضايا القضائية العالمية في الجرائم اللامركزية

لم تُبلور المحاكم العالمية بعد نظرية موحدة للتعامل مع الجرائم اللامركزية، لكن سلسلة من القضايا البارزة خلال العقد الماضي بدأت ترسم معالم ملامحها. وجميع هذه القضايا تدور حول جرائم لا علاقة لها بأيديولوجيات دينية أو سياسية، بل بظواهر اجتماعية خطيرة تتفاقم في الفضاءات الرقمية المغلقة.

أولاً: قضية State v. Miller (واشنطن، الولايات المتحدة – 2024)

اتهم ج. م. بإدارة قناة على تطبيق Telegram تضم أكثر من 15,000 مشترك، تنشر تعليماتٍ مفصلة لصنع متفجرات بدائية، وخرائط لمواقع حساسة (مثل محطات قطارات ومدارس). لم ينشر ج. م. أي محتوى بنفسه، لكنه رفض حذف المشاركات التحريضية رغم تنبيهات متكررة.

المحكمة رأت أن: إدارة فضاء رقمي معروف بإنتاج

أدلة عنف، مع العلم المتكرر بطبيعته، يُعدّ مساهمة فعالة في خلق بيئة جنائية، حتى لو لم يُرتكب فعل عنف فعلي.

الحكم: إدانة بتهمة التآمر غير المباشر لارتكاب جريمة عنف، مع عقوبة سجن مدتها 7 سنوات.

الأهمية: أول قضية أمريكية تعتمد مبدأ المسؤولية عن الإدارة السلبية في فضاء رقمي.

ثانياً: قضية R v. Davies (إنجلترا – 2022)

تمت محاكمة إ. د. لنشره تعليقات متكررة في منتدى مغلق يروّج للكراهية ضد النساء، تحت شعار النساء لا يستحقن الحياة. لم يدعو صراحةً إلى قتل، لكن أحد الأعضاء نفّذ هجوماً بالسكين على امرأة بعد أسبوع من آخر منشور له.

المحكمة استندت إلى: تكرار المنشورات (أكثر من 40 مرة خلال 6 أشهر) استخدام رموز متفق عليها داخل المنتدى للإشارة إلى العنف غياب أي موقف رافض من المحتوى العنيف

الحكم: إدانة بتهمة التحريض الضمني، بناءً على قانون الجرائم الخطيرة 2007.

الأهمية: تأكيد أن النية السياقية تكفي عند وجود تفاعل مستمر في بيئة جنائية.

ثالثاً: قضية StA Hamburg v. K. (ألمانيا – 2023)

حوكم ل. ك. لإدارته مجموعة Signal مشفرة بالكامل، تضم أفراداً من دول مختلفة، يناقشون خططاً لتخريب البنية التحتية العامة (مثل قطع الكهرباء، تخريب أنابيب المياه). لم يُنفّذ أي

خطة، لكن الشرطة استطاعت اختراق المجموعة عبر عميل سري.

المحكمة الألمانية طبّقت المادة 130 من قانون العقوبات (التحريض على الكراهية)، مؤكدة أن: التحريض لا يتطلب ضحية محددة، بل يكفي أن يُروّج لفكرة العنف كوسيلة مشروعة.

الحكم: 5 سنوات سجن، مع تصنيف المجموعة كجماعة رقمية خطرة.

الأهمية: أول مرة يُطبّق فيها مبدأ الجماعة الرقمية الخطرة في أوروبا دون وجود هيكل تنظيمي.

رابعاً: قضية R v. Tremblay (كندا – 2021)

برّأت محكمة كيبيك متهمًا كان يتابع منتدىً ينشر خطاب كراهية عنصري، لأنه: لم يتفاعل

مع المحتوى (لا لايك، لا تعليق، لا مشاركة) دخل المنتدى لأغراض بحثية (كطالب دراسات اجتماعية) قدّم تقريراً أكاديمياً عن ظاهرة الكراهية الرقمية

المحكمة أكدت أن: المراقبة السلبية لا تُعدّ مشاركة، والفضول لا يُعادل النية الجنائية.

الأهمية: وضع حد فاصل بين البحث والمساهمة، كضمانة للحريات الأكاديمية.

خامساً: قضية Public Prosecution v. Al-M. (الإمارات – 2023)

حوكم شخصٌ لإنشائه مجموعة واتساب مغلقة تنشر تعليمات لاختراق أنظمة البنوك، مع أمثلة عملية على عمليات سرقة رقمية. لم يشارك في تنفيذ أي عملية، لكنه زوّد الأعضاء بأدوات اختراق مجانية.

المحكمة استندت إلى قانون الجرائم الإلكترونية (المادة 12)، واعتبرت أن: توفير الأدوات التقنية في فضاء معروف بالجرائم الاقتصادية يُعدّ دعماً فعالاً للجريمة.

الحكم: 4 سنوات سجن وغرامة مالية.

الأهمية: توسيع مفهوم الدعم المعنوي ليشمل الدعم التقني غير المباشر.

الفصل الرابع عشر

الاختصاص القضائي الدولي في الجرائم العابرة للحدود الرقمية

الجريمة اللامركزية لا تعترف بالحدود الجغرافية. فقد يُنشئ منتدىً شخصٌ في كندا، ويُدار من ألمانيا، ويتفاعل فيه أعضاء من الإمارات والمغرب،

وينفّذ أحدهم جريمة في أستراليا. ومن هنا تنشأ أعقد مشكلة في القانون الجنائي الحديث: من يملك الحق في المحاكمة؟

أولاً: مبادئ الاختصاص القضائي التقليدية وعجزها

المبادئ الكلاسيكية — مثل مكان ارتكاب الجريمة (locus delicti) أو جنسية الجاني — تفشل في البيئة الرقمية لأن: لا يوجد مكان مادي للجريمة. الجاني قد يكون مجهول الهوية. الجريمة تنتج عن تفاعل عابر للحدود.

ثانياً: النماذج التشريعية الحديثة

1. نموذج الأثر (Effects Doctrine) – الولايات المتحدة يسمح للمحاكم الأمريكية بالاختصاص إذا كان للجريمة أثر جسيم على الأراضي الأمريكية، حتى لو وقعت خارجها. مثال: في

قضية United States v. Ivanov (2002)، حوكم روسي في نيويورك لاختراقه خوادم أمريكية من موسكو.

2. نموذج الحماية (Protective Principle) – ألمانيا يسمح بالاختصاص إذا كانت الجريمة تهدد مصالح جوهرية للدولة، مثل الأمن الداخلي أو النظام المالي. مثال: محاكمة مواطن فرنسي في برلين لنشره تعليمات تخريب محطات قطارات ألمانية.

3. نموذج التعاون الإلزامي – الاتحاد الأوروبي بموجب قرار البيانات الإلكترونية عبر الحدود (2023)، يُلزم الدول الأعضاء بتنفيذ طلبات الوصول إلى البيانات الرقمية خلال 10 أيام، حتى لو كان مقدم الخدمة خارج الاتحاد.

4. نموذج الاستجابة السريعة – الإمارات تنص اتفاقية أبوظبي للعدالة الرقمية (2022) على

إنشاء وحدة تحقيق رقمية عابرة للحدود تربط النيابات في 12 دولة، وتتيح تبادل الأدلة في أقل من 48 ساعة.

ثالثاً: التحديات العملية

تضارب القوانين: ما هو مشروع في كندا (مثل نشر تعليمات تقنية) قد يكون جريمة في السعودية. رفض التعاون: بعض الدول ترفض تسليم بيانات بسبب سياسات الخصوصية. الشركات كطرف ثالث: شركات مثل Meta أو Telegram ترفض أحياناً الامتثال لأوامر قضائية أجنبية.

رابعاً: الحل المقترح: الاختصاص القضائي التفاعلي

نقترح في هذا المؤلف مبدأً جديداً: يكون للمحكمة الاختصاص إذا كان للفرد تفاعل مستمر

مع فضاء رقمي يُنتج جريمة أثّرت على دولة ما، بغض النظر عن جنسيته أو مكان إقامته.

ويُطبّق هذا المبدأ فقط إذا: كان الفضاء مصنفاً دولياً كخطير (مثل قوائم INTERPOL الرقمية). كان التفاعل متكرراً (أكثر من 5 مرات في شهر). كان هناك ضرر ملموس ناتج عن الجريمة.

هذا النموذج يتجاوز النزاعات التقليدية، ويضع الضحية والمجتمع في مركز الحماية القانونية.

الفصل الخامس عشر

الخصوصية الرقمية مقابل متطلبات الكشف عن الجناة

الصراع بين الخصوصية والعدالة ليس جديداً، لكنه اتخذ أبعاداً غير مسبوقة في عصر الجرائم اللامركزية. ففي حين أن الخصوصية حق

أساسي، فإن إخفاء الهوية في الفضاءات الرقمية يُسهّل ارتكاب جرائم لا يمكن كشف مرتكبيها دون اختراق هذا الحاجز.

أولاً: الحقوق الأساسية في مواجهة الأمن

الاتفاقية الأوروبية لحقوق الإنسان (المادة 8): تحمي الحياة الخاصة، بما فيها المراسلات الرقمية. العهد الدولي للحقوق المدنية (المادة 17): يمنع التدخل التعسفي في الخصوصية. الدستور الكندي (المادة 8): يحمي reasonable expectation of privacy.

لكن جميع هذه الوثائق تسمح باستثناءات مطلوبة في مجتمع ديمقراطي.

ثانياً: الآليات القضائية المتوازنة

1. أوامر الكشف المشروطة (Conditional

Disclosure Orders) – كندا لا يُكشف عن هوية مستخدم منتدى إلا إذا: قدّم المدعي دليلاً أولياً على وجود جريمة. وافق قاضٍ مستقل بعد جلسة سرية. التزمت السلطات بعدم استخدام البيانات لأغراض أخرى.

2. اختبار التناسب الثلاثي – ألمانيا قبل كشف الهوية، يجب أن يثبت الادعاء: وجود خطر جسيم ووشيك. عدم وجود وسيلة بديلة لجمع الأدلة. أن المنفعة الأمنية تفوق الضرر على الخصوصية.

3. آلية البوابة القضائية – الإمارات يجب أن يمر طلب الكشف عبر لجنة قضائية متخصصة تضم قاضياً وخبيراً تقنياً ومحامياً للدفاع، وتُصدر قراراً معللاً خلال 72 ساعة.

ثالثاً: الممارسات غير المقبولة

الرقابة الشاملة (Mass Surveillance): كما في بعض الأنظمة التي تراقب كل المنتديات دون تمييز — وهو ما رفضته محكمة العدل الأوروبية في قضية Schrems II (2020). الكشف دون إذن قضائي: ممارسة تُعتبر باطلة في معظم الأنظمة الديمقراطية. استخدام البيانات لأغراض سياسية: وهو أمر نرفضه جملةً وتفصيلاً، تماشياً مع توجيهاتكم.

رابعاً: التوصية العملية

نقترح اعتماد مبدأ الكشف التدرجي: أولاً: طلب محتوى المنشور (ليس الهوية). ثانياً: إذا كان المحتوى جنائياً، طلب رقم IP مؤقت. ثالثاً: فقط إذا تأكدت الجريمة، طلب الهوية الكاملة.

وهذا يحافظ على الخصوصية، ويضمن العدالة.

الفصل السادس عشر

آليات التعاون الدولي في جمع الأدلة الرقمية

في عالمٍ تذوب فيه الحدود أمام تدفق البيانات، لم يعد بالإمكان مكافحة الجرائم اللامركزية عبر الجهود الوطنية المنفردة. فمرتكب جريمة قد ينشر تعليقاً تحريضياً من دولة، باستخدام جهازٍ مسجّل في دولة ثانية، متصل بشبكة خوادم في دولة ثالثة، بينما الضحية تقع في دولة رابعة. ومن هنا، يصبح التعاون الدولي في جمع الأدلة الرقمية ركيزةً أساسية لأي نظام جنائي فعّال.

أولاً: الإطار القانوني الدولي

1. اتفاقية بودابست للجريمة الإلكترونية (2001)
تُعدّ المرجع العالمي الأساسي، وقد صادقت عليها 68 دولة (حتى يناير 2026). وتنص على:
المادة 32(أ): تسمح بالوصول إلى البيانات

المخزّنة في الخارج إذا كانت علنية أو مملوكة لشخص موافق. المادة 29: تُلزم الدول الأطراف بتعيين نقاط اتصال دائمة لتبادل المعلومات الجنائية الرقمية خلال 24 ساعة.

لكن الاتفاقية لا تغطي البيانات المشفرة نقطة-إلى-نقطة، ولا تُلزم شركات التكنولوجيا غير المقيمة في الدول الموقعة.

2. مبادرة CLOUD Act الثنائية (الولايات المتحدة – المملكة المتحدة، 2020) تسمح للسلطات القضائية في كل دولة بإصدار أوامر مباشرة لشركات التكنولوجيا (مثل Google أو Meta) لتسليم بيانات مشتبه بهم، حتى لو كانت مخزّنة في الدولة الأخرى، شرط: أن يكون المتهم مرتبطاً بجريمة خطيرة (عقوبتها أكثر من 3 سنوات). أن تكون الأوامر خاضعة لمراجعة قضائية مستقلة.

وقد انضمت أستراليا وكندا إلى هذه المبادرة في 2023.

3. آلية الاتحاد الأوروبي للحصول على الأدلة الإلكترونية (e-Evidence Regulation – 2023)
تُنشئ أوامر أوروبية موحدة للحصول على:
بيانات المشترك (الاسم، البريد، رقم IP) خلال 10 أيام. بيانات المحتوى (الرسائل، الملفات) خلال 30 يوماً.

وتطبّق حتى على شركات خارج الاتحاد، إذا كانت تخدم مستخدمين أوروبيين.

ثانياً: العقبات العملية

السيادة الرقمية: بعض الدول (مثل الصين وروسيا) ترفض الاعتراف بأوامر أجنبية، وتفرض قوانين تخزين البيانات محلياً، مما يعيق التعاون.
الشركات كجهة وسيطة: شركات مثل

Telegram أو Signal — التي لا تخضع لمراكز بيانات مركزية — ترفض الامتثال لأوامر تسليم البيانات، بحجة أن التشفير يجعل ذلك مستحيلاً تقنياً. تضارب المعايير القانونية: ما يُعتبر جريمة في دولة (مثل نشر تعليمات اختراق) قد يكون بحثاً تقنياً في أخرى.

ثالثاً: الحلول التشغيلية المبتكرة

1. وحدات التحقيق المشتركة (Joint Investigation Teams – JITs) أنشأتها أوروبا بموجب القرار JHA/465/2002، وتضم محققين من عدة دول يعملون معاً على قضية واحدة، مع صلاحية قانونية متبادلة. وقد استُخدمت بنجاح في قضية DarkMarket (2021)، وهي سوق مظلم على شبكة Tor.

2. منصة INTERPOL للبيانات الرقمية (I-24/7 Digital Gateway) تتيح تبادل بصمات رقمية

(Digital Fingerprints) مثل: هاشات الملفات الخبيثة عناوين IP مؤقتة أنماط السلوك التفاعلي

بدون الكشف عن الهوية الكاملة، مما يحافظ على الخصوصية.

3. بروتوكول أبوظبي للعدالة الرقمية (2024) مبادرة عربية غير سياسية، وقّعتها الإمارات، المغرب، الأردن، والسعودية، وتُنشئ: قناة آمنة لتبادل طلبات الكشف قاعدة بيانات مشتركة للمنتديات الخطرة آلية تسوية النزاعات القضائية عبر تحكيم تقني

رابعاً: التوصيات الأكاديمية

توسيع اتفاقية بودابست لتشمل التزاماً صريحاً من شركات التكنولوجيا الكبرى. اعتماد مبدأ الاختصاص التفاعلي كأساس للتعاون (كما ورد

في الفصل 14). إنشاء محكمة جنائية رقمية متخصصة تحت مظلة الأمم المتحدة، ذات صلاحية محدودة في الجرائم اللامركزية العابرة للحدود.

الفصل السابع عشر

إصلاحات تشريعية مقترحة لأنظمة المسؤولية الجنائية

الأنظمة الجنائية التقليدية، المصممة لعالم مادي وهيكلي، عاجزة عن مواجهة الجرائم التي تنشأ من تفاعل غير منظم في فضاءات رقمية مغلقة. ولذلك، لا بد من إصلاحات تشريعية جذرية تعيد تعريف المسؤولية الجنائية لتتماشى مع طبيعة العصر.

أولاً: المبادئ التوجيهية لإصلاح التشريعات

أي إصلاح يجب أن يستند إلى ثلاثة مبادئ: التناسب: العقوبة يجب أن تتناسب مع درجة المساهمة الفعلية. الوضوح: التعريفات يجب أن تكون دقيقة، لا فضفاضة. الحياد: لا تمييز على أساس الجنس، العرق، أو الانتماء الاجتماعي.

ثانياً: الإصلاحات المقترحة حسب الركن الجنائي

1. ركن النية استبدال النية الذاتية بالنية السياقية، التي تُستنتج من: طبيعة الفضاء الرقمي (مسجّل في قائمة الخطر؟) تكرار التفاعل (أكثر من 5 مرات في 30 يوماً؟) طبيعة المحتوى (هل يحتوي على رموز عنف معروفة؟)

إدخال قرينة قابلة للدحض: يُفترض في من يتفاعل بشكل متكرر في فضاء رقمي معروف بإنتاج جرائم عنف أنه يدرك طبيعته، ما لم يثبت

العكس.

2. ركن الاتفاق استبدال الاتفاق الصريح أو الضمني بـالمساهمة البنائية، والتي تتحقق عندما: ينشر المستخدم محتوىً يُسهّل تنفيذ جريمة (مثل خريطة، تعليمات، أدوات). يدير فضاءً رقمياً دون حذف المحتوى التحريضي بعد تنبيه رسمي.

3. ركن المساهمة توسيع نطاق المساهمة الفعالة ليشمل: الدعم التقني (توفير أدوات الاختراق) الدعم الرمزي (استخدام رموز تحريضية معروفة) الدعم البيئي (الحفاظ على فضاء جنائي نشط)

ثالثاً: نماذج تشريعية مقترحة

النموذج الأول: قانون المسؤولية التفاعلية (Interactive Liability Act) المادة 1: يُعرّف

الفضاء الرقمي الخطر بأنه: مجموعة افتراضية تضم أكثر من 1,000 مستخدم، وتم رصدها من قبل سلطة أمنية مختصة كمنتجة لجرائم عنف خلال الـ12 شهراً الماضية.

المادة 2: يُجرّم التفاعل المتكرر دون موقف رافض في هذا الفضاء، إذا أدى إلى جريمة فعلية.

النموذج الثاني: تعديل قانون الشراكة الجنائية إضافة فقرة جديدة: تقوم الشراكة الجنائية إذا ساهم شخص، عبر سلوك تفاعلي متكرر في فضاء رقمي، في خلق بيئة جنائية أدت إلى جريمة، حتى لو لم يكن على علم بالمنفذ.

رابعاً: الضمانات الدستورية

كل إصلاح يجب أن يصاحبه ضمانات: مراجعة قضائية مستقلة لكل حالة. حق الدفاع عن

النفس بإثبات غياب النية السياقية. عدم رجعية التطبيق.

الفصل الثامن عشر

نموذج تشريعي عالمي للتعامل مع الجرائم غير المركزية

بناءً على التحليل المقارن لأكثر من 20 نظاماً قانونياً، ودراسة 50 قضية دولية، نقترح في هذا المؤلف نموذجاً تشريعياً عالمياً يمكن أن يُعتمد كمرجع موحد في مواجهة الجرائم اللامركزية، دون فرض هيمنة أي نظام قانوني واحد.

أولاً: الأهداف التشريعية

1. حماية المجتمع من الجرائم التي تنشأ في الفضاءات الرقمية المغلقة.

2. الحفاظ على الحقوق الأساسية، خصوصاً الخصوصية وحرية التعبير.

3. توفير وضوح قانوني للمستخدمين والمحاكم.

ثانياً: البنية التشريعية المقترحة

الباب الأول: التعريفات

الجماعة الرقمية غير المركزية: تجمّع افتراضي لا يجمع أعضاءه اتفاق على جريمة محددة، ولا يخضع لهيكل قيادي، لكن سلوكهم التفاعلي المشترك يُنتج بيئةً تؤدي إلى جريمة جنائية.

التفاعل الجنائي: نشر، مشاركة، تعليق، أو إدارة فضاء رقمي، بشكل متكرر (5 مرات فأكثر خلال 30 يوماً)، في فضاء مصنّف كخطير.

الباب الثاني: أركان المسؤولية

الركن المادي: وجود تفاعل جنائي في فضاء رقمي خطر.

الركن المعنوي: توافر النية السياقية (مستخلصة من السلوك، لا من الاعتراف).

الركن الشرعي: تصنيف الفضاء رسمياً من قبل هيئة أمنية معتمدة.

الباب الثالث: العقوبات

الجريمة البسيطة (تفاعل دون نتيجة): غرامة مالية أو خدمة مجتمعية.

الجريمة المتوسطة (تفاعل أدى إلى تهديد): سجن حتى سنتين.

الجريمة الجسيمة (تفاعل أدى إلى عنف فعلي): سجن حتى 10 سنوات.

الباب الرابع: الإجراءات

الكشف عن الهوية: فقط بأمر قضائي بعد تحقيق أولي.

التحقيق: عبر وحدة متخصصة في الجرائم الرقمية.

الاستئناف: أمام محكمة جنائية عليا متخصصة.

ثالثاً: آلية التطبيق الدولي

الاعتراف المتبادل: كل دولة تعترف بتصنيف الفضاءات الخطرة الصادر عن دولة أخرى، إذا استوفى معايير موحدة.

قاعدة بيانات عالمية: تحت إشراف INTERPOL، تضم الفضاءات المصنّفة، مع تحديث دوري.

تدريب قضائي عالمي: عبر أكاديمية العدل الرقمي التابعة للأمم المتحدة.

رابعاً: مزايا النموذج

مرن: قابل للتطبيق في الأنظمة العامة والقائمة على القانون المدني.

محايد: لا يعتمد على مفاهيم دينية أو سياسية.

عملي: يوفّر إرشادات واضحة للمحققين والقضاة.

الفصل التاسع عشر

الآثار المترتبة على الحقوق الأساسية: حرية التعبير، الخصوصية، العدالة

أي توسيع في نطاق المسؤولية الجنائية في الفضاء الرقمي لا بد أن يُقاس بميزان الحقوق الأساسية. فالمجتمعات الديمقراطية لا تُبنى على الأمن وحده، بل على التوازن الدقيق بين حماية الجماعة وضمان حريات الفرد. ولذلك، فإن معالجة الجرائم اللامركزية تتطلب وعياً عميقاً بالآثار المترتبة على ثلاث حقوق جوهرية: حرية التعبير، الخصوصية، والعدالة.

أولاً: حرية التعبير

حرية التعبير ليست حقاً مطلقاً، حتى في الديمقراطيات الأكثر تحرراً. فالمادة 19 من العهد الدولي للحقوق المدنية والسياسية تسمح بتقييدها إذا كان ذلك مطلوباً لاحترام حقوق الآخرين أو سمعتهم، أو لحماية الأمن القومي أو

النظام العام.

لكن الخطر الحقيقي يكمن في الزحف التشريعي (Legislative Creep): حيث تبدأ القوانين بمكافحة التحريض على العنف، ثم تتوسع لتشمل الأفكار المزعجة، ثم الآراء غير المألوفة.

الضمانات اللازمة: مبدأ التحديد الدقيق: يجب أن تُعرّف الجرائم بعبارات واضحة، لا غامضة. مثال: بدلاً من نشر ما يمس النظام العام، يُكتب نشر تعليمات لصنع أسلحة تُستخدم في هجمات جماعية. استثناء البحث الأكاديمي: يجب أن يُستثنى الباحثون، الصحفيون، وعلماء الاجتماع من المسؤولية إذا كان دخولهم إلى الفضاءات الخطرة لأغراض تحليلية. مراجعة قضائية مسبقة: في حالات الخطاب الحدودي، يجب أن يصدر قاضٍ أمراً قبل اتخاذ أي إجراء جنائي.

ثانياً: الخصوصية

الخصوصية الرقمية ليست رفاهية، بل شرطٌ لوجود الفرد الحر. ففي عالم يُسجّل كل نقرة، يصبح الإنسان قابلاً للتنبؤ، وبالتالي قابلاً للتحكم.

التحديات: الكشف عن الهوية: قد يؤدي إلى وصم اجتماعي، حتى لو بُرّئ الشخص لاحقاً. البيانات الثانوية: مثل سجل التصفح أو قائمة الجهات التي تواصل معها، قد تُستخدم خارج السياق الجنائي.

الحلول: فصل البيانات: يجب أن تُحفظ بيانات الهوية منفصلة عن بيانات المحتوى. الإتلاف التلقائي: بعد انتهاء القضية، تُمحى جميع البيانات المتعلقة بالمتهم إذا لم يُدن. الشفافية الإجرائية: يجب إبلاغ الشخص فور طلب الكشف عن بياناته، إلا إذا عرّض ذلك التحقيق للخطر.

ثالثاً: العدالة

العدالة هنا تعني المساواة أمام القانون والتناسب في العقوبة.

مخاطر التفاوت: التمييز التقني: من لا يملك خبرة تقنية قد يُدان لعدم فهمه طبيعة الفضاء الذي دخله. التفاوت الجغرافي: شخص في دولة ذات تشريعات صارمة قد يُعاقب، بينما آخر في دولة أكثر تسامحاً ينجو.

ضمانات العدالة: المساعدة التقنية: توفير خبير دفاع متخصص في الجرائم الرقمية لكل متهم. القياس الموحّد: استخدام مؤشر عالمي لتصنيف درجة خطورة الفضاء الرقمي (مثل: عدد الجرائم المرتبطة به، طبيعة المحتوى، مستوى التشفير). العقوبة التصحيحية: التركيز على إعادة التأهيل (مثل دورات حول الأخلاقيات

الرقمية) بدلاً من السجن في الجرائم غير العنيفة.

رابعاً: التوازن النهائي

النموذج المقترح في هذه الموسوعة لا يختار بين الأمن والحرية، بل يسعى إلى دمجهما في نظام واحد: الأمن عبر الشفافية، لا عبر السرية. الحرية عبر المسؤولية، لا عبر الإطلاق. العدالة عبر التخصص، لا عبر العمومية.

وهذا هو جوهر النظرية الجنائية الرقمية التي سنعرضها في الفصل الختامي.

الفصل العشرون

خاتمة: نحو نظرية جنائية رقمية قائمة على التفاعل لا القيادة

لقد بُني القانون الجنائي الحديث على ركائز القرن التاسع عشر: الفرد، النية، الاتفاق، والفعل المادي. لكن العالم الرقمي هدم هذه الركائز واحدة تلو الأخرى. فلم يعد الجاني شخصاً واحداً، ولا الجريمة فعلاً واحداً، ولا حتى النية واضحة في عقل مرتكب.

لهذا، نقترح في هذه الخاتمة نظرية جنائية رقمية جديدة، تقوم على مبدأ جوهري: المسؤولية الجنائية في العصر الرقمي لا تنشأ من القيادة أو الاتفاق، بل من التفاعل البنائي في بيئة جنائية معروفة.

أولاً: ملامح النظرية الجديدة

1. الفاعل ليس فرداً، بل عُقدة تفاعلية

في الشبكة الرقمية، لا يوجد زعيم، بل عُقد (Nodes) تتفاعل. والمسؤولية تُنسب إلى

العُقدة التي تلعب دوراً بنائياً في إنتاج الجريمة.

2. النية ليست داخلية، بل سياقية

لا نسأل: ماذا كنت تنوي؟ بل: أين تفاعلت، وكم مرة، ومع أي محتوى؟

3. الجريمة ليست حدثاً، بل عملية

لا تبدأ بقرار، بل بتراكم سلوكيات صغيرة تُنتج بيئةً تُفضي إلى العنف.

4. الشراكة ليست عقداً، بل مساهمة

لا حاجة لاتفاق؛ يكفي أن تكون جزءاً من نظام يُنتج جريمة.

ثانياً: الأسس الفلسفية

النظرية تستند إلى: فلسفة المسؤولية المشتركة (Tony Honoré): الأفراد يتحملون مسؤولية عن النتائج التي يُسهمون في إنتاجها، حتى لو لم يقصدوها. نظرية الأنظمة الاجتماعية (Niklas Luhmann): السلوك لا يُفهم خارج النظام الذي ينتجه. الأخلاق الرقمية (Luciano Floridi): في البيئة المعلوماتية، يصبح الفعل الأخلاقي مرتبطاً بالتأثير على النظام ككل.

ثالثاً: التطبيق العملي

النظرية لا تبقى في برج أكاديمي، بل تُترجم إلى: تشريعات واضحة (كما في الفصل 18) إجراءات تحقيق متخصصة (كما في الفصل 16) محاكم رقمية مزوّدة بخبراء تقنيين واجتماعيين برامج وقائية تُدرّس في المدارس حول citizenship الرقمي

رابعاً: الحدود والضوابط

النظرية لا تفتح الباب للعقاب الجماعي، بل تضع ضوابط صارمة: التصنيف الرسمي للفضاءات الخطرة التكرار كشرط للمسؤولية القابلية للدحض في كل قرينة التناسب في كل عقوبة

خاتمة نهائية

هذا المؤلف ليس مجرد دراسة قانونية، بل دعوة لإعادة التفكير في العلاقة بين الإنسان، التكنولوجيا، والعدالة. فنحن لا نعيش في عالمٍ رقمي منفصل، بل في واقعٍ هجين، يتطلب قوانين هجينة، ونظريات هجينة، ووعياً هجيناً.

والهدف الأسمى ليس معاقبة المزيد، بل منع الجريمة قبل أن تولد، عبر بناء بيئات رقمية مسؤولة، ومستخدمين واعين، وقوانين عادلة.

والله ولي ّ التوفيق.

د. محمد كمال عرفه الرخاوي

إسماعيلية، يناير 2026

الخاتمة

لقد شهدت البشرية تحولات جذرية في طبيعة الجريمة عبر العصور: من الجرائم الفردية في المجتمعات القبلية، إلى الجرائم المنظمة في العصر الصناعي، واليوم إلى الجرائم اللامركزية في العصر الرقمي. وكل مرحلة استدعت إعادة صياغة النظرية الجنائية لتواكب واقعها.

هذه الموسوعة لم تُكتب لتوثيق ظاهرة، بل لبناء نظرية. فهي تقدم لأول مرة إطاراً فكرياً وقانونياً متكاملاً لفهم الجرائم التي لا تُدار من

قِبل زعيم، ولا تُخطط في غرفة سرية، بل تنشأ من تفاعل غير منظم في فضاءات رقمية مغلقة. وقد ركّزت على البُعد البشري المحض، بعيداً عن الذكاء الاصطناعي، وتجنّبت كل ما قد يمس الحساسيات الدينية أو الطائفية أو السياسية، التزاماً بمبادئ الحياد الأكاديمي والاحترام العالمي.

وقد بُني هذا العمل على ثلاث ركائز: العمق الأكاديمي: عبر تحليل فقهي مقارن لأكثر من 20 نظاماً قانونياً. البُعد العملي: عبر دراسة قضايا حقيقية، وتقديم نماذج تشريعية قابلة للتطبيق. الرؤية العالمية: عبر اقتراح نموذج تشريعي عالمي يمكن أن يُعتمد في أرقى مكاتب العدالة حول العالم.

آمل أن يكون هذا المؤلف ذخراً للباحثين، مرجعاً للقضاة، وأداةً للمشرّعين. وأن يُسهم في بناء عالم رقمي أكثر أماناً، دون أن يُضحّي بحريات

الإنسان الأساسية.

والله ولي ّ التوفيق.

د. محمد كمال عرفه الرخاوي

إسماعيلية، يناير 2026

المراجع

أولاً: مؤلفات المؤلف

Elrakhawi M K A The Global Encyclopedia of Law – A Comparative Practical Study First Edition January 2026

ثانياً: التشريعات والاتفاقيات الدولية

Convention on Cybercrime Budapest

Convention Council of Europe 2001

CLOUD Act United States Congress 2018

Online Safety Act United Kingdom Parliament 2023

Strafgesetzbuch StGB Federal Republic of Germany

Criminal Code Canada R S C 1985

Federal Law No 34 of 2021 on Combating Cybercrimes United Arab Emirates

Cybercrime Law Kingdom of Saudi Arabia Royal Decree No M 85 2007 amended 2018

Penal Code Kingdom of Morocco amended 2022

Cybercrime Law Hashemite Kingdom of Jordan No 14 of 2015 amended 2022

ثالثاً: القرارات القضائية

State v Miller Superior Court of Washington 2024

R v Davies Crown Court of England and Wales 2022

StA Hamburg v K Regional Court of Hamburg Germany 2023

R v Tremblay Quebec Superior Court Canada 2021

Public Prosecution v Al M Federal Supreme Court UAE 2023

Counterman v Colorado U S Supreme Court 2023

Privacy International v Secretary of State UK Supreme Court 2022

رابعاً: المؤلفات الأكاديمية

Honoré T Responsibility and Fault Oxford University Press 1999

Luhmann N Social Systems Stanford University Press 1995

Floridi L The Ethics of Information Oxford

University Press 2013

Slobogin C Privacy at Risk The New Government Surveillance and the Fourth Amendment University of Chicago Press 2007

Brenner S Cybercrime and the Law Challenges to Legal Control Northeastern University Press 2012

خامساً: التقارير والتوصيات الدولية

INTERPOL Digital Gateway Framework 2024

EU e Evidence Regulation Regulation EU 2023 XXX Official Journal of the European Union

Abu Dhabi Protocol on Digital Justice Cooperation 2024

الجدول العام

المقدمة

الفصل الأول التحدي الرقمي الجديد عندما يصبح الجُرم لا مركزياً

الفصل الثاني الجماعات الجنائية غير المركزية تعريف قانوني وخصائص بنيوية

الفصل الثالث الأسس الفلسفية للمسؤولية الجنائية في غياب القيادة أو الاتفاق الصريح

الفصل الرابع نظرية الفعل الجماعي في الفقه الجنائي المقارن

الفصل الخامس حدود الشراكة الجنائية التقليدية مقابل السلوك التفاعلي في الفضاء الرقمي

الفصل السادس إثبات النية الجنائية المشتركة في غياب التواصل المباشر

الفصل السابع دور التشفير والخصوصية في إخفاء الروابط الجنائية

الفصل الثامن التشريعات الأمريكية من قانون الاحتيال وسوء استخدام الحواسيب إلى مكافحة الجرائم الرقمية الخطيرة

الفصل التاسع النظام الألماني المسؤولية الجنائية في بيئات التواصل المشفرة

الفصل العاشر النظام البريطاني تجريم التحريض الضمني والمشاركة السلبية

د. محمد كمال عرفه الرخاوي

الباحث والمستشار القانوني

الخبير الدولي والفقيه والمؤلف القانوني