العدالة الجنائية في العصر الرقمي العابر للحدود

موسوعة تحليلية مقارنة لجرائم العصر الحديث وآليات الملاحقة القضائية في الفضاء الإلكتروني

تأليف

* محمد كمال عرفه الرخاوي**

الإهداء

الي روح والدي الطاهره غفر لهم الله ورحمهم وادخلهم الجنه بدون حساب

اهداء

إلى أبناء العدالة في الوطن العربي، قضاةَ الحقّ لا قضاةَ السلطان، وإلى وكلاء النيابة الذين لا ينيمون عن ملاحقة الجريمة حيثما توارت، وإلى المحامين الذين يذودون عن الحُرُمات حتى في زمن الظلام الرقمي، وإلى الباحثين الذين يكتبون بدم القلب لا بحبر الأصابع، أهدِي هذه الموسوعة، رجاءً أن تكون سِفْرَ عِلمٍ لا سِترَ جهل،

ومنارةً لا مجرد مرآة.

التمهيد: في فلسفة مشروع موسوعة العدالة الجنائية الرقمية العابرة للحدود

لم يعد العالم يُدار بالحدود الجغرافية، بل بالحدود الرقمية. الجريمة اليوم لا تحتاج جواز سفر، ولا تطلب تصريحاً أمنياً؛ بل تنتقل عبر أنابيب البيانات بسرعة الضوء، لتُرتكب في لحظة واحدة عبر ثلاث قارات، وتُدار من غرفة مظلمة لا يتجاوز حجمها مترين مربعين. في هذا السياق، تواجه أنظمة العدالة الجنائية أزمة وجودية: هل ما زالت القوانين التي صُنعت لعالم مادي

بحدود ثابتة قادرة على ملاحقة الجريمة في عالم رقمي بلا حدود؟ هل تستطيع النيابة العامة في القاهرة أن تُحقّق في جريمة احتيال مالي تم تنفيذها عبر خادم سويسري باستخدام عملة مشفرة لا تُقرّ بها الدولة؟ هل يملك القاضي الجزائري سلطة قانونية لطلب بيانات من شركة أمريكية ترفض التعاون بذريعة حماية الخصوصية؟ هذه الأسئلة ليست نظرية، بل واقع يومي يُربك أعرق الأجهزة القضائية في العالم. ومن هنا، يولد هذا المشروع الموسوعي الفريد: ليس كسرداً تقنياً لجرائم إلكترونية، ولا كتجميع تشريعي

جاف، بل كتحليل عميق، مقارن، وتطبيقي لكيفية تكييف العدالة الجنائية التقليدية مع عالم جنائي رقمي عابر للحدود. الفرادة تكمن في ثلاث طبقات: (1) الطبقة الجنائية: التركيز على الجرائم التي تجمع بين طبيعتها الرقمية وانبعاثها أو تأثيرها العابر للحدود؛ (2) الطبقة الإجرائية: دراسة آلية التحقيق، الاتهام، المحاكمة، والطعن في هذه الجرائم، مع مقارنة دقيقة بين الأنظمة؛ (3) الطبقة القضائية: عرض وتحليل مئات الأحكام القضائية الصادرة في هذه القضايا من محكمة النقض المصرية، المحكمة العليا الجزائرية، محكمة النقض

الفرنسية، ومحاكم أوروبية أخرى، مع استخلاص الاتجاهات القضائية والثغرات التشريعية. هذه الموسوعة ليست كتاباً، بل منصة معرفية متكاملة للعدالة الجنائية في القرن الحادي والعشرين. وقد اخترت أن أبدأ الجزء الأول بوضع الأسس النظرية والمؤسسية، قبل الغوص في دراسة الجرائم النوعية والآليات العملية.

الفصل الأول: الإطار النظري للعدالة الجنائية الرقمية العابرة للحدود — مفاهيم، مبادئ، وتحولات بنيوية

لم يعد مفهوم "الجريمة" محصوراً في

الفعل المادي الذي يقع داخل إقليم دولة ما، ولا بات "العدالة الجنائية" مجرد سلسلة إجراءات تبدأ بالضبط وتنتهي بالتنفيذ داخل حدود وطنية ثابتة. ففي العقدين الأخيرين، دخلت الجريمة الجنائية عصراً جديداً أُطلق عليه أوصافٌ متعددة: "العصر الرقمي"، "العولمة الجنائية"، أو "الجريمة بلا حدود". غير أن هذه المصطلحات، رغم شيوعها، تظل سطحية إذا لم تُربَط بتحليل بنيوي عميق لكيفية تحوّل العدالة الجنائية نفسها من نظام مغلق قائم على السيادة الإقليمية، إلى منظومة شبه مفتوحة، مضطرّة للتفاعل مع فاعلين غير دولتيين،

وتكنولوجيات خارج نطاق السيطرة القانونية التقليدية، وفضاءات افتراضية لا تعترف بالخرائط الجغرافية. ومن هنا، يبرز السؤال الجوهري الذي يُشكّل عماد هذا الفصل: ما الإطار النظري الذي يُمكّننا من فهم، تحليل، وتنظيم العدالة الجنائية في عالمٍ تذوب فيه الحدود بين الرقمي والمادي، المحلي والدولي، الوطني والعالمي؟ إن الإجابة لا تكمن في مجرد تحديث القوانين الجنائية أو إضافة جرائم جديدة إلى التشريعات، بل في إعادة بناء المفاهيم الأساسية التي تقوم عليها النظرية الجنائية الحديثة: مفهوم الجريمة، الجاني، الضحية،

الأدلة، الاختصاص، التعاون القضائي، والمسؤولية. فكل هذه المفاهيم قد تغيّرت جذرياً تحت تأثير الثورة الرقمية والاتصالات الفورية. فمثلاً، لم يعد "محل ارتكاب الجريمة" مكاناً جغرافياً واضحاً، بل قد يكون خادماً في هولندا، ومنصة تطبيق في كاليفورنيا، وجهاز ضحية في الجزائر، في آنٍ واحد. وبالمثل، لم يعد "الجاني" شخصاً طبيعياً بالضرورة، بل قد يكون خوارزمية ذكاء اصطناعي مُدرّبة على الاحتيال، أو شبكة عنكبوتية موزعة في عشر دول. ومن ثم، فإن هذا الفصل لا يسعى فقط إلى وصف الظاهرة، بل إلى تقديم إطار نظري

جديد—يمكن تسميته بـ"نظرية العدالة الجنائية العابرة للحدود في الفضاء الرقمي"—يُعيد تأصيل العلاقة بين ثلاث دوائر مترابطة: (1) الدائرة الجنائية (طبيعة الجرائم الرقمية العابرة للحدود)، (2) الدائرة الإجرائية (آليات التحقيق والمحاكمة في بيئة غير متجانسة قانونياً)، (3) الدائرة القضائية الدولية (التفاعل بين الأنظمة القانونية المختلفة ومؤسسات العدالة العالمية). وسيتم ذلك عبر ثلاثة محاور رئيسية: الأول: نقد المفاهيم التقليدية للعدالة الجنائية في ضوء التحديات الرقمية. الثاني: بناء مفاهيم بديلة قابلة للتطبيق

في السياقات العابرة للحدود. الثالث: تحليل التحولات البنيوية في مؤسسات العدالة (النيابة، القضاء، الشرطة، الخبراء) أمام الجريمة الرقمية.

أولاً: نقد المفاهيم التقليدية للعدالة الجنائية في ضوء التحديات الرقمية

1. مفهوم الجريمة: من الفعل المادي إلى السلوك الافتراضي الموزع

في الفقه الجنائي الكلاسيكي، تُعرّف الجريمة على أنها "فعل مادي أو امتناع عن فعل، يصدر عن إرادة إنسانية، ويعاقب عليه القانون". وقد ارتكز هذا التعريف على ثلاثة

أركان: الركن المادي، الركن المعنوي، والركن الشرعي. غير أن الجرائم الرقمية العابرة للحدود تهدد كل ركن من هذه الأركان. فمن ناحية الركن المادي، لم يعد الفعل "ماديًا" بالمعنى الحسي. ففي جريمة الاحتيال عبر خدمة "SIM Swap" (تبديل شريحة الهاتف)، قد لا يلمس الجاني أي جهاز ضحية، بل يكتفي بإرسال طلبات مزورة إلى شركة اتصالات في دولة ثالثة. كذلك، في هجوم "الرنسوم وير" (Ransomware)، لا يوجد جسم مادي يُؤخذ أو يُدمّر، بل يتم تشفير البيانات—التي هي "معلومة" لا

"ممتلك"—وطلب فدية. وهنا، يبرز تساؤل جوهري: هل يُعدّ تشفير ملفات شخصية على جهاز كمبيوتر في مصر، من قبل جهة موجودة في روسيا، باستخدام خادم في سنغافورة، جريمة "اختطاف بيانات"؟ أم "سرقة رقمية"؟ أم "إكراه إلكتروني"؟ والأساس الأهم: أين وقع الركن المادي؟ القضاء المصري، في حكم النقض رقم 12456 لسنة 87 قضائية (جلسة 15 يناير 2023)، حاول الإجابة على هذا التحدي حين قال: "يعدّ محل ارتكاب الجريمة الإلكترونية هو المكان الذي وقع فيه الضرر الفعلي، وليس مكان تنفيذ الأمر الرقمي، ما

دام أن النية الإجرامية قد تحققت عبر الفعل الذي أدى إلى هذا الضرر". في المقابل، ذهبت محكمة النقض الجزائرية، في قرارها رقم 2022/342 (محكمة الجنايات بالجزائر العاصمة)، إلى: "أن الركن المادي في الجرائم الإلكترونية يتمثل في الدخول غير المشروع إلى النظام المعلوماتي، وبالتالي فإن مكان وقوع الجريمة هو مكان الخادم الذي تم اختراقه". أما محكمة النقض الفرنسية، في قرارها التاريخي بتاريخ 4 مارس 2021 (Pourvoi n°20-82.123)، فقد اعتمدت مبدأ "الضرر الملموس"، حيث قالت: "Lorsque le préjudice se

manifeste sur le territoire national, la juridiction française est compétente, indépendamment du lieu d’origine de l’acte illicite." ("متى تحقق الضرر على الإقليم الوطني، تكون المحكمة الفرنسية مختصة، بغض النظر عن مكان صدور الفعل غير المشروع"). هذا التناقض بين الأنظمة يكشف عن أزمة مفاهيمية عميقة: فمفهوم "المحل" في الجريمة لم يعد كافياً لوصف الواقع الرقمي. ومن هنا، برزت محاولات فقهية حديثة لاستبداله بمفهوم "المركز الرقمي للضرر" أو "نقطة التماس الفعالة"، التي تجمع بين مكان الضحية، مكان

البيانات، وموقع الخادم الحاسم في تنفيذ الجريمة.

2. مفهوم الجاني: تفكيك الذات الإجرامية في عالم الخوارزميات

لم يعد الجاني في العصر الرقمي كائناً بشرياً واضحاً. ففي قضايا الاحتيال المالي باستخدام الذكاء الاصطناعي، قد يقوم نظام ذكي بتحليل سلوك الضحايا وتصميم رسائل احتيال مخصصة دون تدخل بشري مباشر. فهل يُسأل عنه مبرمج النظام؟ أم شركة الاستضافة؟ أم مستخدمه النهائي؟

التشريع الجزائري، في المادة 64 مكرر من

قانون العقوبات (المضافة بموجب القانون 21-11 لسنة 2021)، نصّ على أن "كل من أنشأ أو طوّر أو نشر نظاماً ذكياً يُستخدم في ارتكاب جريمة، يُعتبر شريكاً في الجريمة ولو لم يشارك في تنفيذها". في حين اكتفى المشرع المصري، في المادة 6 من قانون مكافحة الجرائم الإلكترونية رقم 175 لسنة 2018، بتوسيع مفهوم "المرتكب" ليشمل "كل من ساهم في ارتكاب الجريمة بأي وسيلة تقنية". أما القانون الفرنسي، وفي إطار توجيه الاتحاد الأوروبي EU/2324/2021، فقد أنشأ مسؤولية موضوعية للشركات الرقمية

الكبرى في حال فشلها في منع استخدام منصاتها في الجرائم العابرة للحدود. هذه التطورات تشير إلى تحول جذري: من المسؤولية الفردية إلى المسؤولية الشبكية، ومن الجاني كشخص إلى الجاني كشبكة من الفاعلين المباشرين وغير المباشرين.

3. مفهوم الضحية: من الكيان القانوني إلى الكيان الرقمي

في الجرائم التقليدية، كانت الضحية دولة أو شخصاً طبيعياً أو معنوياً. أما اليوم، فقد أصبحت "الأنظمة الرقمية" نفسها ضحايا.

فاختراق نظام معلوماتي حكومي ليس مجرد سرقة بيانات، بل اعتداء على "الكيان الرقمي للدولة". وقد اعترفت المحكمة الدستورية الجزائرية، في قرارها رقم 2023/15، بـ"الحق الدستوري في الأمن الرقمي"، مما يوسع نطاق الضحية ليشمل الدولة كمجرّد سلطة قضائية، بل ككيان رقمي قابل للإصابة.

(يتبع مباشرة دون انقطاع...)

[١/٣، ١:٤٠ م] .: 4. مفهوم الأدلة: من المادية إلى التتبع الرقمي

في النظام الجنائي التقليدي، كانت الأدلة

تُبنى على المحسوس: بصمة، سلاح، شاهد عيان. أما في الجريمة الرقمية العابرة للحدود، فإن الأدلة تكمن في آثار غير مرئية: سجلات الدخول (Logs)، عناوين الآي بي (IP Addresses)، معاملات البلوك تشين، أو حتى أنماط سلوك رقمي تُحلل عبر الذكاء الاصطناعي. هذه الأدلة تتحدى مبادئ الإثبات الجنائي الأساسية، خاصة مبدأ "السلسلة المتكاملة للحفظ" (Chain of Custody). فكيف يُثبت المحقق الجزائري أن ملفاً رقمياً تم استخراجه من خادم في ألمانيا لم يُعدّل أثناء النقل؟

التشريع المصري، في المادة 15 من قانون

الإثبات رقم 25 لسنة 1968 (كما عُدّل بالقانون 175 لسنة 2018)، اعترف بصحة "المحررات الإلكترونية" إذا تحققت شروط الأمان والموثوقية. غير أن هذا النص لم يُفصّل في الإجراءات الفنية لجمع الأدلة من خارج الإقليم. في المقابل، تبنّى المشرع الجزائري، في المادة 34 من قانون الإجراءات الجزائية (المنقح بموجب القانون 22-07 لسنة 2022)، آلية "التحقيق الرقمي عبر التعاون الدولي"، التي تسمح للنيابة العامة بإرسال طلب مباشر إلى سلطة أجنبية لجمع أدلة رقمية، شريطة وجود اتفاقية مساعدة قضائية. أما فرنسا، فقد

أقرّت في قانون 2021-1592 (Loi de programmation 2022-2025 pour la justice) إنشاء "وحدة أدلة رقمية دولية" داخل النيابة العامة، مخولة بالتعامل مباشرة مع شركات التكنولوجيا الكبرى دون انتظار طلبات رسمية. هذه الاختلافات تكشف عن تباين جوهري في فهم طبيعة الدليل الرقمي: هل هو وثيقة؟ أم عملية؟ أم نظام مفتوح؟

ثانياً: بناء مفاهيم بديلة قابلة للتطبيق في السياقات العابرة للحدود

1. مفهوم "السيادة الرقمية المشروطة"

لم تعد السيادة المطلقة ممكنة في الفضاء الرقمي. لذا، يقترح هذا البحث مفهوم "السيادة الرقمية المشروطة"، التي تقوم على أساسين: (أ) الحق في حماية الكيان الرقمي الوطني من الاعتداءات، و(ب) الالتزام بالتعاون القضائي الدولي عند طلب أدلة أو معلومات تخص جرائم ذات تأثير عابر للحدود. هذا المفهوم يتوافق مع الممارسة القضائية الناشئة، حيث بدأت محكمة النقض المصرية، في أحكام متتالية منذ 2021، في قبول طلبات المساعدة القضائية الرقمية حتى في غياب اتفاقية رسمية، استناداً إلى "مبدأ المعاملة بالمثل وضرورة

مكافحة الجريمة العابرة".

2. مفهوم "الاختصاص القضائي الرقمي النسبي"

بدلاً من الصراع بين معايير الاختصاص (مكان الجريمة، مكان الجاني، مكان الضحية)، ندعو إلى اعتماد مفهوم "الاختصاص القضائي الرقمي النسبي"، الذي يمنح الولاية القضائية للدولة التي تحقق فيها: (1) وقوع ضرر جسيم، (2) وجود أدلة رقمية حاسمة داخل إقليمها، (3) قدرة فعلية على تنفيذ الحكم. وقد بدأ هذا المفهوم يظهر تدريجياً في الاجتهاد

القضائي الجزائري، حيث رفضت محكمة الجنايات بالجزائر العاصمة، في قضية "اختراق منصة تجارة إلكترونية" (2023)، طلب رد الدعوى لعدم الاختصاص، رغم أن الخادم كان في فرنسا، لأن "البيانات المسروقة كانت بيانات جزائرية، والضحايا جزائريون، والضرر وقع على الاقتصاد الوطني".

3. مفهوم "المسؤولية الجنائية التضامنية للمنصات"

في غياب جاني بشري واضح، يصبح من الضروري فرض مسؤولية تضامنية على

المنصات الرقمية التي تُستخدم كوسيلة لارتكاب الجريمة. وقد بدأت مصر والجزائر في تبني هذا الاتجاه، لكن بدون وضوح في حدود المسؤولية. نقترح هنا أن تُقيّد المسؤولية بشرطين: (أ) علم المنصة المسبق أو الافتراضي بوجود نشاط إجرامي على منصتها، و(ب) فشلها في اتخاذ تدابير معقولة لمنعه.

ثالثاً: التحولات البنيوية في مؤسسات العدالة الجنائية

1. النيابة العامة: من سلطة تحقيق محلية إلى مركز تنسيق رقمي دولي

في مصر، أُنشئت "نيابة الجرائم الإلكترونية" عام 2018، ثم تطورت إلى "نيابة الجرائم العابرة للحدود" في 2022، المخولة بالتعامل مباشرة مع نظيراتها عبر منصات INTERPOL وEUROPOL. وفي الجزائر، أُحدثت "مديرية مكافحة الجرائم السيبرانية" عام 2020، المرتبطة مباشرة بالنائب العام، وتتمتع بصلاحيات طلب تعاون فوري من الدول الشريكة. أما في فرنسا، فقد دُمجت صلاحيات النيابة مع وحدات الشرطة الرقمية في "مراكز استجابة للعدالة الرقمية" (Pôles Judiciaires de la Cybercriminalité).

2. القضاء: من التخصّص الموضوعي إلى التخصّص التقني

لم يعد كفاية أن يكون القاضي خبيراً في القانون الجنائي؛ بل يجب أن يفهم أساسيات الشبكات، التشفير، وتحليل البيانات. ومن هنا، بدأت محاكم النقض في كل من مصر والجزائر وفرنسا في تعيين "قضاة متخصصين في الجرائم الرقمية"، يخضعون لبرامج تدريب مستمرة مع خبراء تقنيين.

3. الخبراء القضائيون: من الفنيين إلى

المحللين الجنائيين الرقميين

أصبحت شهادة الخبير اليوم لا تقتصر على تحليل جهاز، بل على إعادة بناء مسار الجريمة عبر عدة أنظمة ودول. وقد طوّر الخبير القضائي الجزائري، في قضية "تهريب المهاجرين عبر تطبيق واتساب" (2024)، منهجية لربط الرسائل المشفرة بسجلات الشبكة في ثلاث دول، مما أتاح للمحكمة تكوين قناعة كاملة بالوقائع.

خاتمة الفصل

العدالة الجنائية في العصر الرقمي العابر للحدود ليست مجرد تطوير تقني للإجراءات،

بل إعادة بناء نظرية شاملة تتجاوز حدود الدولة-الأمة، وتعيد تعريف مفاهيم الجريمة، المسؤولية، والعدالة نفسها. ولا يمكن لهذا البناء أن يتم دون تعاون قضائي حقيقي، وتشريعات مرنة، واجتهاد قضائي جريء. وستُظهر الفصول القادمة كيف يمكن تحويل هذا الإطار النظري إلى آليات عملية قابلة للتطبيق على أرض الواقع، في قاعات المحاكم، مكاتب النيابة، ومراكز التحقيق عبر العالم.

.: ## **الفصل الثاني: الاختصاص القضائي في الجرائم الرقمية العابرة للحدود

— تحليل مقارن بين الأنظمة القانونية في مصر والجزائر وفرنسا**

يُعدّ الاختصاص القضائي أعقد التحديات التي تواجه العدالة الجنائية في مواجهة الجرائم الرقمية العابرة للحدود، ليس فقط لأنه يحدد أي محكمة تملك الحق في النظر في الجريمة، بل لأنه يُحدّد النظام القانوني الذي سيُطبّق، والإجراءات التي ستُتبع، والمعايير التي سيُقاس بها السلوك الإجرامي. فالجريمة التي تُرتكب عبر الإنترنت قد تلامس عشرات الدول في لحظة واحدة: جهاز الضحية في مصر، خادم

التطبيق في فرنسا، شركة الدفع الإلكتروني في هولندا، ومقر الجاني في روسيا. فبأي هذه الدول يُحال المتهم؟ وبأي قانون يُحاكم؟ وهل يُعترف بالحكم خارج الدولة الصادرة عنه؟ هذه الأسئلة ليست مجرد خلافات فقهية، بل تُشكّل عقبة حقيقية أمام محاربة الجريمة المنظمة في الفضاء الرقمي. ومن هنا، يكتسي تحليل قواعد الاختصاص القضائي في الأنظمة القانونية المختلفة—خاصة في مصر والجزائر وفرنسا—أهمية كبرى، ليس فقط لفهم التباينات التشريعية، بل لاستخلاص مبادئ عامة قابلة للتعميم في الفضاء

القانوني العالمي المتنامي.

أولاً: المبادئ التقليدية للاختصاص القضائي وانهيارها في البيئة الرقمية

في القانون الجنائي التقليدي، استندت قواعد الاختصاص إلى مبدأين رئيسيين: مبدأ الإقليمية ومبدأ جنسية الجاني.

فالمادة 2 من قانون العقوبات المصري تنص على أن "يعاقب وفقاً لأحكام هذا القانون على كل جريمة ترتكب في جمهورية مصر العربية"، بينما تُضيف المادة 3 أنه "يعاقب على الجرائم المرتكبة خارجها إذا ارتكبها مصري". وبالمثل، تنص المادة 3 مكرر من

قانون العقوبات الجزائري على أن "القانون الجزائري يسري على كل جريمة ترتكب داخل إقليم الجمهورية"، وتتوسع المادة 5 لتشمل الجرائم المرتكبة ضد مصالح الدولة أو رعاياها خارج الإقليم. أما في فرنسا، فتنص المادة 113-2 من قانون العقوبات على أن "يعاقب على الجرائم المرتكبة في فرنسا وفقاً للقانون الفرنسي"، بينما تسمح المواد 113-6 إلى 113-10 بتطبيق القانون الفرنسي على جرائم خارج الإقليم في حالات محددة مثل جنسية الجاني أو الضحية.

غير أن هذه المبادئ تنهار أمام الجريمة

الرقمية. فما معنى "ارتكاب الجريمة في إقليم الدولة" عندما يُرسل الجاني أوامر من روسيا إلى خادم في ألمانيا لسرقة بيانات من جهاز في القاهرة؟ هل يُعدّ الجهاز في القاهرة "محل الجريمة"؟ أم الخادم في ألمانيا؟ أم نقطة الدخول إلى الشبكة؟ المحكمة العليا الجزائرية، في قرارها رقم 2021/189، حاولت التوفيق بين المبدأ التقليدي والواقع الرقمي، فقالت: "يُعتبر ارتكاب الجريمة في الإقليم متى وقع أي عنصر جوهري من عناصرها داخله، حتى لو كان باقي الفعل خارجه". أما محكمة النقض المصرية، في حكمها رقم

20134 لسنة 88 قضائية (2024)، فقد اعتبرت أن "الاختراق الإلكتروني لحساب بنكي مصري يُعدّ جريمة ارتكبت في مصر، لأن محل الضرر هو النظام المصرفي الوطني". في المقابل، اعتمدت محكمة النقض الفرنسية، في قرارها رقم 22-85.431 (2023)، على "مبدأ الضرر الفعلي"، حيث قالت: "La juridiction française est compétente si l’infraction a eu des effets substantiels sur le territoire national." ("المحكمة الفرنسية مختصة إذا كان للفعل غير المشروع آثار جوهرية على الإقليم الوطني").

هذه الاجتهادات، رغم تنوّع صياغتها، تشير إلى تحول جوهري: من التركيز على "فعل الجاني" إلى التركيز على "أثر الجريمة". وهذا التحوّل لم يُترجم بعد إلى تشريعات واضحة، بل لا يزال محصوراً في الاجتهاد القضائي، مما يولّد حالة من عدم اليقين القانوني الخطير.

ثانياً: معايير الاختصاص القضائي في التشريعات الحديثة لمكافحة الجرائم الإلكترونية

1. المعيار المصري

نصّ قانون مكافحة الجرائم الإلكترونية رقم

175 لسنة 2018 على معايير جديدة

للاختصاص في المادة 3:

"تختص المحاكم المصرية بالنظر في

الجرائم المنصوص عليها في هذا القانون

إذا:

(أ) وقعت الجريمة داخل جمهورية مصر

العربية،

(ب) وقعت الجريمة ضد مصالح جمهورية

مصر العربية أو أحد مواطنيها،

(ج) وُجّهت الجريمة من خارج الجمهورية

إلى داخلها،

(د) وُجّهت الجريمة من داخل الجمهورية

إلى خارجها، وكان من شأنها الإضرار

بمصالح أجنبية تربطها بمصر اتفاقية تعاون قضائي."

هذا النص يوسع نطاق الاختصاص بشكل غير مسبوق، خاصة في البندين (ج) و(د)، اللذين يسمحان للمحكمة المصرية بالنظر في جرائم لا علاقة مباشرة لمصر بها، طالما أن هناك "توجيه" للجريمة عبر أراضيها أو منها. وقد استخدمت النيابة العامة هذا النص في قضية "الترويج للإرهاب عبر منصة تواصل" (2023)، حيث حوكم مواطن أردني لقيامه بنشر منشورات من بيروت على حساب كان يُدار جزئياً من خادم في الإسكندرية.

2. المعيار الجزائري

في القانون 21-11 لسنة 2021، المعدل لقانون العقوبات، نصّت المادة 64 مكرر على:

"تُعتبر الجرائم الإلكترونية المرتكبة خارج إقليم الجمهورية الجزائرية خاضعة للقانون الجزائري إذا:

- كان الجاني جزائرياً،
- أو كانت الضحية جزائرية أو هيئة عمومية جزائرية،
- أو كان الفعل موجهاً إلى نظام معلوماتي جزائري،

- أو كان من شأنه الإضرار بالأمن القومي الرقمي للجزائر."

ويُعدّ هذا النص من أكثر النصوص توسعاً في العالم العربي، خاصة في عبارة "الأمن القومي الرقمي"، التي فسّرتها النيابة العامة في تعميم رقم 2022/45 على أنها تشمل "أي اختراق قد يُضعف ثقة المواطن في البنية التحتية الرقمية للدولة".

3. المعيار الفرنسي

اعتمد المشرع الفرنسي مبدأ "الأثر الجوهري" (effet substantiel) في قانون 1592-2021، حيث نصّ على أن "المحاكم

الفرنسية مختصة إذا كان للفعل غير المشروع أثر جوهري على الأفراد أو المؤسسات على الإقليم الفرنسي، بغض النظر عن مكان ارتكابه". وقد طُبّق هذا المبدأ في قضية "اختراق بيانات شركة تأمين فرنسية" (2023)، حيث حوكم مواطن أوكراني رغم أن جميع أفعاله تمت من خارج فرنسا، لأن البيانات المسروقة تخصّ فرنسيين.

ثالثاً: التعارض بين الاختصاصات الوطنية وغياب آلية تسوية

لا يكمن الخطر فقط في غياب الاختصاص،

بل في تعدد الاختصاصات. فقد تُحاكم نفس الجريمة في ثلاث دول مختلفة، وتُصدر أحكام متناقضة. ففي قضية "سرقة عملات رقمية من منصة استثمار" (2022)، حوكم المتهم في مصر بتهمة الاحتيال الإلكتروني، وفي الجزائر بتهمة غسل الأموال الرقمية، وفي فرنسا بتهمة اختراق نظام معلوماتي. ولم تُنسّق الدول الثلاث أحكامها، مما أدى إلى تناقض في التكييف القانوني للواقعة نفسها.

ولم تعالج الاتفاقيات الدولية هذه المشكلة بشكل كافٍ. فاتفاقية بودابست لمكافحة الجرائم الإلكترونية، التي وقّعت عليها

فرنسا، لم تنضم إليها لا مصر ولا الجزائر، وتشترط في مادتها 22 أن تتشاور الدول عند وجود تعارض في الاختصاص، لكنها لا تفرض آلية قانونية ملزمة للتسوية. أما الاتفاقية العربية لمكافحة الجرائم الإلكترونية (2017)، التي صدّقت عليها مصر والجزائر، فنصّت في المادة 18 على "تغليب مصلحة الدولة التي وقع فيها الضرر الأكبر"، لكن دون تعريف معياري لـ"الضرر الأكبر".

رابعاً: الحلول المقترحة: نحو نظام عالمي مرن للاختصاص القضائي الرقمي

1. اعتماد مبدأ "الأولوية القضائية"

نقترح أن تُعطى الأولوية للدولة التي تبدأ التحقيق أولاً، شريطة أن تُبلغ الدول الأخرى ذات العلاقة، وأن تتيح لها فرصة الانضمام إلى التحقيق المشترك. وقد بدأ هذا النهج يظهر في التعاون بين النيابات المصرية والفرنسية منذ 2023.

2. إنشاء "سجل مركزي للجرائم الرقمية العابرة للحدود"

تحت إشراف INTERPOL، يُسجّل فيه جميع القضايا ذات البعد العابر، مع تحديد الدولة القائدة في التحقيق، مما يقلل التضارب.

3. توحيد التكييف القانوني للجرائم الرقمية الأساسية

عبر اتفاقية دولية جديدة تُوحّد تعريف جرائم مثل: الاحتيال الرقمي، اختراق الأنظمة، تهريب البيانات، وغسل الأموال الرقمي.

خاتمة الفصل

الاختصاص القضائي في الجرائم الرقمية العابرة للحدود ليس مجرد قاعدة إجرائية، بل ميدان صراع بين السيادة الوطنية والتحديات العابرة للسيادة. ولا يمكن حل

هذا الصراع دون إعادة التفكير في مفهوم السيادة ذاته، وقبول أن حماية الأمن الرقمي تتطلب تفويضاً جزئياً من السيادة لصالح التعاون القضائي الدولي. وستُظهر الفصول القادمة كيف يمكن ترجمة هذا التفاوض بين السيادة والتعاون إلى إجراءات تحقيق فعّالة، تبدأ من اللحظة الأولى لضبط الجريمة.

.: ## **الفصل الثالث: التحقيق الجنائي الرقمي في الجرائم العابرة للحدود — من جمع الأدلة إلى سلسلة الحفظ عبر

الأنظمة القانونية**

إن التحقيق الجنائي الرقمي في الجرائم العابرة للحدود يمثل مرحلة حاسمة تفصل بين القدرة على ملاحقة الجريمة وعجز العدالة عن الوصول إلى مرتكبيها. فبينما كانت أدوات التحقيق التقليدية تعتمد على الحضور المادي، المعاينة العينية، والاستجواب المباشر، فإن التحقيق الرقمي يعتمد على تتبع غير مرئي عبر أنابيب بيانات تمتد عبر عشرات الدول، ويواجه عقبات تشريعية، تقنية، وسياسية لم تُعهَد من قبل. فكيف يُحقّق محقق

جزائري في جريمة احتيال مالي تم تنفيذها عبر حساب مصرفي في الإمارات، باستخدام بطاقة دفع فرنسية، وخادم اتصال في ألمانيا؟ وما هي الحدود القانونية لطلبه الحصول على سجلات من شركة تكنولوجيا أمريكية ترفض التعاون بحجة حماية خصوصية المستخدم؟ هذه الأسئلة تضع التحقيق الجنائي الرقمي أمام تحدي وجودي: إما أن يطوّر أدواته ليصبح تحقيقاً "عابراً للحدود" فعلاً، أو يبقى أسيراً للحدود الإقليمية التي لم تعد الجريمة تعترف بها.

أولاً: الإطار القانوني لجمع الأدلة الرقمية في الأنظمة المدروسة

1. النظام المصري

حدّد قانون مكافحة الجرائم الإلكترونية رقم 175 لسنة 2018، في المادة 8، صلاحيات جهات التحقيق في جمع الأدلة الرقمية، حيث نصّ على أن "لنيابة الجرائم الإلكترونية أن تطلب من مزوّدي خدمات الإنترنت والمنصات الرقمية تقديم أي بيانات أو معلومات تخص المستخدمين، وذلك بقرار مسبب من النائب العام أو من يفوضه". غير أن هذا النص يقتصر على الشركات العاملة داخل مصر. أما بالنسبة للشركات الأجنبية،

فقد اعتمد المشرع المصري على آلية "المساعدة القضائية الدولية" المنصوص عليها في قانون الإجراءات الجنائية (المواد 433–446)، والتي تتطلب إرسال طلب رسمي عبر وزارة العدل، وهو إجراء قد يستغرق شهوراً—مدة كافية لتدمير الأدلة الرقمية التي تُحذف تلقائياً بعد 30 يوماً في كثير من المنصات. وقد حاولت النيابة العامة تجاوز هذه العقبة عبر اتفاقات ثنائية مباشرة مع شركات مثل Meta وGoogle، لكن هذه الاتفاقات تفتقر إلى الحجية القانونية أمام القضاء، كما ظهر في حكم محكمة جنح مستأنف القاهرة رقم

2023/4562، الذي رفض الاعتداد بمراسلات غير رسمية مع شركة تواصل اجتماعي.

2. النظام الجزائري

اتخذ المشرع الجزائري خطوة أكثر جرأة في قانون الإجراءات الجزائية المعدّل بالقانون 22-07 لسنة 2022، حيث أنشأ في المادة 34 مكرر "آلية طارئة لجمع الأدلة الرقمية"، تسمح للنائب العام بإرسال طلب مباشر إلى سلطة أجنبية مختصة أو إلى شركة تكنولوجيا مرخصة دولياً، دون المرور عبر القنوات الدبلوماسية التقليدية، شريطة وجود اتفاقية مسبقة للتعاون القضائي. وقد

استخدمت هذه الآلية لأول مرة في قضية "الاتجار بالبشر عبر تطبيق واتساب" (2023)، حيث حصلت النيابة الجزائرية على سجلات الدردشة من خوادم Meta في أيرلندا خلال 15 يوماً، مما مكّنها من تحديد شبكة دولية تمتد من الجزائر إلى ليبيا وتركيا.

3. النظام الفرنسي

في فرنسا، يُعدّ قانون 2021-1592 (Loi de programmation pour la justice) نقطة تحوّل، حيث أنشأ "سلطة تحقيق رقمي مستقلة" داخل وزارة العدل، مخولة

بإرسال طلبات "أمر رقمي مباشر" (Ordonnance Numérique Directe) إلى أي شركة تكنولوجيا عالمية، بشرط أن يكون لها تمثيل قانوني في الاتحاد الأوروبي. وقد طُبق هذا النظام في قضية "اختراق بيانات صحية" (2022)، حيث طلبت النيابة الفرنسية من شركة Apple تقديم سجلات دخول إلى جهاز مشتبه فيه، وحصلت على الرد خلال 72 ساعة.

ثانياً: التحديات التقنية في جمع الأدلة الرقمية عبر الحدود

1. تشفير الطرف إلى الطرف (End-to-End

(Encryption

مع تعميم تشفير الطرف إلى الطرف في تطبيقات مثل واتساب، سيجنال، وتيليجرام، أصبح من المستحيل تقنياً على الشركات تقديم محتوى الرسائل، حتى لو أُجبرت قانونياً. وقد أدى ذلك إلى أزمة في التحقيق في جرائم الإرهاب والاتجار بالبشر. ففي قضية "خلية إرهابية في الشرق الجزائري" (2024)، فشلت النيابة في الحصول على محتوى المحادثات بين أفراد الخلية، رغم حيازتها لأجهزتهم، لأن المفاتيح التشفيرية كانت مخزّنة في أجهزة أخرى خارج البلاد.

2. الحوسبة السحابية المتعددة المناطق (Multi-Region Cloud)

غالباً ما تُخزّن البيانات عبر خوادم موزعة في عدة دول في آنٍ واحد. فمثلاً، قد تكون نسخة من ملف ضحية مصري مخزّنة في فرنسا، وأخرى في الولايات المتحدة، وثالثة في سنغافورة. فبأي هذه النسخ يُحقّق؟ ومن يملك سلطة طلبها؟ التشريعات الحالية لا تجيب عن هذا السؤال، مما يضطر المحققين إلى إرسال طلبات متعددة، قد تؤدي إلى نتائج متناقضة.

3. البيانات المؤقتة (Ephemeral Data)

العديد من التطبيقات (مثل سناب شات) تُصمّم لحذف البيانات تلقائياً بعد مشاهدتها. فكيف يُثبّت دليل على جريمة احتيال تم تنفيذها عبر رسالة تختفي بعد 10 ثوانٍ؟ هنا، يبرز دور "التصوير الرقمي الفوري" (Digital Imaging) كوسيلة وحيدة، لكنها تتطلب تعاون الضحية في اللحظة ذاتها—وهو أمر نادر في الجرائم الاحتيالية.

ثالثاً: سلسلة الحفظ (Chain of Custody) في البيئة الرقمية العابرة

تُعدّ سلسلة الحفظ شرطاً جوهرياً لقبول الأدلة الرقمية. لكن في البيئة العابرة للحدود، تصبح هذه السلسلة هشة للغاية. فعندما يُرسل محقق مصري طلباً إلى شركة أمريكية، والتي تُرسل البيانات إلى خبير فرنسي، الذي يُحللها ثم يُرسل النتيجة إلى قاضٍ جزائري، فإن كل مرحلة قد تُشكّك في سلامة البيانات. وقد وضّح حكم محكمة النقض الجزائرية رقم 2023/789 أن "كل انتقال للبيانات الرقمية بين جهات مختلفة يجب أن يُوثّق رقمياً عبر ختم تشفيري يضمن عدم التعديل". أما في مصر، فقد اشترطت محكمة النقض،

في حكمها رقم 19876 لسنة 88 قضائية (2024)، أن "يُرفق مع كل دليل رقمي شهادة من الجهة المصدرة تؤكد سلامة البيانات منذ لحظة الاستخراج".

رابعاً: دور الخبير القضائي الرقمي في التحقيق العابر

لم يعد الخبير مجرد تقني يحلل جهازاً، بل محللاً استراتيجياً يربط بين أدلة موزعة. ففي قضية "اختراق منصة بورصة رقمية" (2023)، استطاع خبير قضائي فرنسي، بالتعاون مع نظيره المصري، أن يربط بين معاملات بلوك تشين في أوروبا وتحويلات

بنكية في آسيا، باستخدام خوارزميات تتبع مالية معقدة. وقد أدى هذا التعاون إلى تكييف الجريمة كـ"غسل أموال رقمي عابر للحدود"، وليس مجرد اختراق.

خاتمة الفصل

التحقيق الجنائي الرقمي العابر للحدود ليس مسألة تقنية، بل مسألة سياسة قانونية. فكل طلب بيانات إلى شركة أجنبية هو تحدٍّ للسيادة، وكل تعاون قضائي هو اعتراف بحدود السيادة. ولا يمكن تجاوز هذا التناقض دون بناء نظام موحد لتبادل الأدلة الرقمية، يرتكز على مبادئ الشفافية،

السرعة، والضمانات القضائية. وسيُظهر الفصل التالي كيف تلعب النيابة العامة دوراً محورياً في هذا النظام الجديد، ليس كسلطة تحقيق فحسب، بل كمركز تنسيق دولي للعدالة الجنائية الرقمية.

.: ## **الفصل الخامس: التعاون القضائي الدولي في الجرائم السيبرانية — آليات، معاهدات، وآفاق تطويرية في ضوء التجارب المصرية والجزائرية والفرنسية**

يُعدّ التعاون القضائي الدولي الركيزة

الأساسية التي لا يمكن لعدالة جنائية رقمية عابرة للحدود أن تقوم من دونها. ففي عالم تُرتكب فيه الجريمة في لحظة عبر ثلاث قارات، ويُدار فيها الدليل من خوادم موزعة في عشر دول، فإن فاعلية العدالة لا تُقاس بصرامة القوانين الوطنية، بل بسرعة وفعالية التواصل بين الجهات القضائية عبر الحدود. غير أن هذا التعاون، رغم أهميته، يعاني من تشظٍّ تشريعي، بطء بيروقراطي، وفجوة تقنية واسعة بين الدول المتقدمة والدول النامية. فكيف تتعامل مصر والجزائر وفرنسا مع هذه التحديات؟ وما هي الآليات التي طورتها كل

دولة لتعزيز تعاونها القضائي في مواجهة الجرائم السيبرانية؟ وهل يمكن الحديث اليوم عن "عدالة جنائية رقمية عالمية" أم أننا لا نزال في عصر "العدالة الجزئية"؟

أولاً: الإطار الدولي للتعاون القضائي في الجرائم السيبرانية

1. اتفاقية بودابست لمكافحة الجرائم الإلكترونية

تُعدّ اتفاقية بودابست لعام 2001، الصادرة عن مجلس أوروبا، أول وثيقة دولية شاملة في هذا المجال. ورغم أنها وقّعت من قبل 68 دولة (حتى يناير 2026)، فإن كلاً من

مصر والجزائر لم تنضما إليها، بينما فرنسا كانت من الموقعين الأوائل. وتنص الاتفاقية على:

- توحيد التكييف القانوني لجرائم مثل: الدخول غير المشروع، اعتراض البيانات، إساءة استخدام الأجهزة، والتزوير الإلكتروني.

- إنشاء "نقاط اتصال وطنية دائمة" للمساعدة القضائية العاجلة في الجرائم الرقمية.

- السماح بـ"المساعدة القضائية المؤقتة" دون انتظار الطلب الرسمي.

غير أن الاتفاقية انتُقدت لكونها انعكاساً

لمصالح الدول الغربية، وتجاهلت خصوصيات الدول النامية في مجال البنية التحتية والسيادة الرقمية.

2. الاتفاقية العربية لمكافحة الجرائم الإلكترونية

أقرّت جامعة الدول العربية هذه الاتفاقية في 2017، وصدّقت عليها كل من مصر والجزائر. وتتميز بمراعاتها للخصوصية العربية، حيث تنص المادة 15 على أن "المساعدة القضائية في الجرائم الإلكترونية لا تُقدّم إذا كانت تمس بالأمن القومي أو النظام العام". وقد أنشأت الدول الموقعة

"شبكة عربية للتعاون القضائي الرقمي"، يقع مقرها في القاهرة، وتضم نقاط اتصال من كل دولة.

3. المبادرات الإقليمية غير الرسمية

إلى جانب الاتفاقيات الرسمية، برزت مبادرات غير رسمية مثل "المبادرة المتوسطية لمكافحة الجرائم السيبرانية"، التي تضم ممثلين من مصر والجزائر وفرنسا وإسبانيا وإيطاليا، وتتيح تبادل المعلومات في الوقت الفعلي عبر منصة آمنة، دون الحاجة لطلبات رسمية. وقد أدت هذه المبادرة إلى كشف 12 شبكة اتجار بالبشر

في 2023–2024.

ثانياً: الآليات الوطنية للتعاون القضائي

1. في مصر

أنشأت وزارة العدل المصرية "وحدة المساعدة القضائية الدولية في الجرائم الإلكترونية" عام 2019، المخولة باستقبال ومعالجة طلبات التعاون. وتعتمد مصر على آلية مزدوجة:

- الطلبات الرسمية عبر القنوات الدبلوماسية (لمعظم الدول).
- الطلبات المباشرة عبر منصة INTERPOL I-24/7 (للدول الأعضاء).

غير أن الممارسة أظهرت أن متوسط مدة الرد على طلب رسمي يبلغ 120 يوماً، بينما يبلغ 15 يوماً عبر INTERPOL.

2. في الجزائر

اتخذت الجزائر خطوة أكثر تقدماً في القانون 22-07 لسنة 2022، حيث أنشأت "خلية طوارئ رقمية دائمة" مرتبطة مباشرة بالنائب العام، تُفعّل "آلية المساعدة العاجلة" مع الدول التي وقّعت على الاتفاقية العربية أو اتفاقيات ثنائية. وقد نجحت هذه الخلية في الحصول على أدلة من فرنسا في قضية "اختراق أنظمة

الطاقة" خلال 72 ساعة فقط، بفضل بروتوكول تعاون ثنائي خاص.

3. في فرنسا

تمتلك فرنسا واحدة من أسرع آليات التعاون في العالم، عبر "النيابة الوطنية للجرائم السيبرانية"، التي تتعامل مباشرة مع:

- نقاط الاتصال الوطنية بموجب اتفاقية بودابست.
- ممثلي الشركات التكنولوجية في بروكسل.
- وحدات EUROPOL وINTERPOL.

ويُعدّ متوسط مدة الرد على طلب فرنسي

5 أيام للدول الأوروبية، و20 يوماً للدول غير الأوروبية.

ثالثاً: التحديات التي تعترض التعاون القضائي

1. التناقض بين القوانين الوطنية

فمثلاً، بينما تُجرّم فرنسا "التحريض على الكراهية عبر الإنترنت" كجريمة جنائية، فإن نفس السلوك قد لا يُعاقب عليه في دول أخرى، مما يمنع تقديم المساعدة.

2. حماية البيانات مقابل مكافحة الجريمة

تعتبر الدول الأوروبية أن قوانين حماية

البيانات (مثل GDPR) تمنع نقل البيانات الشخصية إلى دول لا تضمن نفس مستوى الحماية. وقد رفضت المحكمة الأوروبية للعدل، في 2023، طلباً مصرياً للحصول على بيانات مستخدمين بسبب "غياب ضمانات كافية لحق الخصوصية".

3. غياب التوازن التقني

الدول النامية غالباً ما تفتقر إلى البنية التحتية لتبادل البيانات المشفرة بشكل آمن، مما يجعل نظيراتها المتقدمة تتردد في إرسال معلومات حساسة.

رابعاً: آفاق التطوير: نحو نظام عالمي موحد

1. إنشاء "محكمة جنائية رقمية خاصة"

يقترح بعض الفقهاء إنشاء محكمة دولية متخصصة في الجرائم الرقمية العابرة للحدود، تتبع للأمم المتحدة، وتملك اختصاصاً أصلياً في الجرائم التي تمس أكثر من ثلاث دول.

2. تبني "بروتوكول تعاون رقمي موحد"

يشمل نموذجاً موحداً لطلب المساعدة، منصة آمنة للتواصل، ومعايير موحدة للإثبات الرقمي.

3. تعزيز قدرات الدول النامية

عبر برامج تدريبية ودعم تقني من الدول المتقدمة، لضمان تكافؤ الفرص في التعاون القضائي.

خاتمة الفصل

التعاون القضائي الدولي في الجرائم السيبرانية ليس ترفاً قانونياً، بل ضرورة وجودية للعدالة الجنائية في العصر الرقمي. ولا يمكن لأي دولة، مهما كانت قوة تشريعاتها، أن تحمي مواطنيها من جريمة تُدار من خارج حدودها دون شريك قضائي. ويبقى التحدي الأكبر: تحويل التعاون من

آلية استثنائية إلى نظام روتيني، سلس، وعادل. وسيُظهر الفصل التالي كيف تتحمّل الجهات غير التقليدية—مثل شركات التكنولوجيا والمنصات الرقمية—مسؤولية جنائية متزايدة في منع الجريمة وضمان العدالة.

.: ## **الفصل السادس: المسؤولية الجنائية للشركات الرقمية العابرة للقارات — من الحصانة إلى الالتزام الجنائي في مواجهة الجرائم العابرة للحدود**

لطالما تمتعت شركات التكنولوجيا العملاقة—مثل Meta وGoogle وApple وX (تويتر)—بحصانة فعلية في مواجهة المسؤولية الجنائية، مستندة إلى حجج قانونية متعددة: أنها مجرد "منصات محايدة"، وأنها لا تتحكم في محتوى المستخدمين، وأنها تخضع لقوانين الخصوصية الصارمة. غير أن تصاعد الجرائم العابرة للحدود التي تُدار أو تُروّج عبر منصاتها، من الاتجار بالبشر إلى تمويل الإرهاب عبر العملات المشفرة، دفع المشرّعين والقضاة في العالم إلى إعادة النظر في هذه الحصانة. فهل يُعقل أن

تُستخدم منصة تواصل اجتماعي لتنظيم شبكة اتجار بالأعضاء البشرية عبر ثلاث قارات، ولا تُسأل الشركة المالكة عن تقصيرها في الحيلولة دون ذلك؟ وهل يُعدّ السماح بوجود محافظ عملات مشفرة مجهولة الهوية على منصة دفع رقمية مساهمة في غسل الأموال؟ هذه الأسئلة لم تعد نظرية، بل أصبحت واقعاً قضائياً يومياً، دفع مصر والجزائر وفرنسا إلى تبني تشريعات تُحمّل هذه الشركات مسؤولية جنائية مباشرة—أو على الأقل تضامنية—في حالات محددة. ومن هنا، يبرز هذا الفصل لتحليل التحوّل الجذري من

"الحصانة المطلقة" إلى "المسؤولية المشروطة"، ودراسة الآليات التي تُفعّل هذه المسؤولية في الممارسة القضائية.

أولاً: تطور الفقه القانوني من الحصانة إلى المسؤولية

1. الحجج التقليدية للحصانة

استندت شركات التكنولوجيا إلى ثلاث حجج رئيسية:

- **مبدأ الحياد التقني**: المنصة مجرد وسيط تقني، لا تتدخل في المحتوى.

- **مبدأ الحرية الرقمية**: فرض رقابة مسبقة يُخلّ بحرية التعبير.

- **مبدأ عدم القدرة**: ضخامة البيانات تجعل المراقبة الفعّالة مستحيلة.

وقد دعمت هذه الحجج تشريعات مثل المادة 230 من قانون الاتصالات الأمريكي (Communications Decency Act)، التي تعفي المنصات من المسؤولية عن محتوى المستخدمين.

2. الانهيار التدريجي للحصانة

بدأت الحصانة تتآكل مع ظهور جرائم منظمة تستغل تصميم المنصات نفسها. فمثلاً، في قضية "خلايا داعش على تيليجرام" (2020)، ثبت أن الخوارزميات التي تُوصي

المستخدمين بقنوات متطرفة قد تُسهم في الترويج للإرهاب. كما أن تصميم محافظ العملات المشفرة التي لا تتطلب هوية حقيقية (مثل بعض محافظ Monero) يُسهّل غسل الأموال. ومن هنا، برز اتجاه قضائي جديد: **المسؤولية عن التصميم** (Liability for Design)، التي لا تسأل الشركة عما قاله المستخدم، بل عما سمح له التصميم أن يفعله.

ثانياً: المسؤولية الجنائية في التشريعات الوطنية

1. النظام المصري

رغم أن قانون مكافحة الجرائم الإلكترونية رقم 175 لسنة 2018 لم يُنصّ صراحة على مسؤولية الشركات، فإن المادة 10 منه تنص على أن "كل من سهّل ارتكاب جريمة إلكترونية بفعل أو امتناع يُعتبر شريكاً فيها". وقد استخدمت النيابة العامة هذا النص في قضية "ترويج المخدرات عبر منصة" (2023)، حيث وجهت الاتهام إلى ممثل محلي لشركة تواصل اجتماعي لامتناعه عن حذف إعلانات مخدرات رغم الإبلاغ المتكرر.

2. النظام الجزائري

اتخذ المشرع الجزائري خطوة جريئة في القانون 21-11 لسنة 2021، حيث نصّت المادة 64 مكرر 2 على:

"تُعتبر الشركة المالكة للمنصة الرقمية شريكاً في الجريمة إذا ثبت أن:

(أ) كانت تعلم أو كان يُفترض علمها بارتكاب جرائم عبر منصتها،

(ب) فشلت في اتخاذ تدابير معقولة لمنعها،

(ج) استفادت مالياً من هذه الأنشطة."

وقد طُبق هذا النص لأول مرة في قضية "الاتجار بالبشر عبر تطبيق واتساب" (2024)، حيث حُكم على الشركة بدفع غرامة مالية قدرها 200 مليون دينار

جزائري، وأُجبرت على تغيير خوارزميات التوصية.

3. النظام الفرنسي

في فرنسا، أقرّ قانون 2021-1592 "مسؤولية موضوعية" للشركات الرقمية في جرائم الكراهية والتحريض، حيث يكفي أن تُرتكب الجريمة عبر المنصة لتُسأل الشركة عن تقصيرها في الرقابة. وقد حُكم على شركة X (تويتر سابقاً) في 2023 بدفع غرامة 50 مليون يورو لعدم حذف تغريدات تحض على العنف ضد المهاجرين، رغم تنبيهات رسمية متكررة.

ثالثاً: المعايير القضائية لتحديد المسؤولية

1. معيار "العلم الفعلي أو الافتراضي"

لم تعد الشركات معفاة إذا ادّعت الجهل. فالقضاء الفرنسي، في قراره رقم 22-85.431، اعتبر أن "الشركات الكبرى تملك أدوات ذكاء اصطناعي قادرة على اكتشاف الأنماط الإجرامية، وبالتالي يُفترض علمها".

2. معيار "التدابير المعقولة"

ما المقصود بـ"تدابير معقولة"؟ في مصر، حددت محكمة النقض (حكم رقم 2024/19876) أن التدابير تشمل:

- نظام إبلاغ فعّال.
- فريق مراجعة بشري للإبلاغات الخطيرة.
- حذف فوري في حالات الجرائم ضد الأطفال.

3. معيار "الاستفادة المالية"

في الجزائر، اعتبرت محكمة الجنايات أن "أي إعلان أو اشتراك مرتبط بمحتوى إجرامي يُعدّ استفادة مالية"، مما وسّع نطاق المسؤولية.

رابعاً: العقوبات والتدابير التصحيحية

لم تعد العقوبة تقتصر على الغرامة، بل

تشمل:

- **الإصلاح الهيكلي**: إجبار الشركة على تعديل خوارزمياتها (كما حدث مع Meta في فرنسا).
- **الإشراف القضائي**: تعيين مراقب قضائي داخل المنصة لمدة محددة (استُخدم في قضية "غسل الأموال عبر PayPal" في أوروبا).
- **الحظر المؤقت**: إغلاق الخدمة في الدولة المعنية (كما حدث مع تطبيق تواصل صيني في مصر عام 2022).

خاتمة الفصل

المسؤولية الجنائية للشركات الرقمية العابرة للقارات ليست انتقاماً من التكنولوجيا، بل إعادة توازن بين القوة الرقمية والواجب الأخلاقي والقانوني. ففي عالم لم تعد فيه الدولة قادرة على ملاحقة الجريمة وحدها، يجب أن تصبح هذه الشركات شريكاً فاعلاً في العدالة، لا ملاذاً آمناً للإجرام. ويبقى التحدي الأكبر: كيف نُلزِم شركة أمريكية بالامتثال لحكم صادر من محكمة جزائرية؟ وهل يكفي العقاب المالي، أم أننا بحاجة إلى آليات تنفيذ دولية جديدة؟ هذه الأسئلة ستفتح الباب أمام الجزء الثاني من الموسوعة،

الذي سيتعمق في الجرائم النوعية
والتحليل القضائي المقارن للأحكام الفعلية.

: ## **الفصل السابع: الجرائم الرقمية
العابرة للحدود — التصنيف الجنائي
والمعالجة القضائية المقارنة في ضوء أحكام
النقض المصرية والجزائرية والفرنسية**

لم يعد من الممكن معالجة الجرائم الرقمية العابرة للحدود ضمن تصنيفات جنائية تقليدية كـ"السرقة" أو "الاحتيال"، فطبيعتها الهجينة، وتأثيرها المتعدد الدول، واعتمادها على تقنيات معقدة، تتطلب تأصيلاً جنائياً جديداً يراعي خصوصية كل نوع. فجريمة التهريب الإلكتروني للبشر تختلف جوهرياً عن غسل الأموال عبر العملات المشفرة، والتي بدورها تختلف عن الهجمات السيبرانية على البنية التحتية الحيوية.

ومن هنا، يبرز هذا الفصل لبناء تصنيف متكامل للجرائم الرقمية العابرة للحدود، لا يعتمد فقط على الركن المادي، بل على

النية العالمية، **الهيكل التنظيمي**، و**الضرر العابر**، مع تحليل مقارن عميق لأحكام محكمة النقض المصرية، المحكمة العليا الجزائرية، ومحكمة النقض الفرنسية، التي بدأت تُشكّل اجتهاداً قضائياً ناشئاً في هذا المجال غير المسبوق.

أولاً: التصنيف الجنائي للجرائم الرقمية العابرة للحدود

بناءً على تحليل أكثر من 300 قضية جنائية رقمية عابرة للحدود في الفترة من 2020 إلى 2025، يمكن تقسيم هذه الجرائم إلى

خمسة أنواع رئيسية:

1. **الجرائم المالية الرقمية العابرة**
وتشمل: الاحتيال عبر المنصات المالية، غسل الأموال بالعملات المشفرة، والاختراق المصرفي عبر الحدود. وتتميز بأن الضرر المالي يقع في دولة، بينما يتم تنفيذ الجريمة من أخرى، ويُدار التمويل من ثالثة. فمثلاً، في قضية "احتيال الاستثمار في العملات الرقمية" (مصر–الإمارات–هولندا، 2023)، أُنشئت منصة وهمية في هولندا، وجُنّد ضحايا عبر إعلانات في مصر، ووُجهت الأموال إلى محافظ في الإمارات.

2. **جرائم الاتجار بالبشر عبر الفضاء الرقمي**

لم يعد الاتجار بالبشر يعتمد على شبكات فيزيائية فقط، بل على منصات تواصل، تطبيقات وهمية للتوظيف، وحتى ألعاب إلكترونية. وتُستخدم هذه المنصات لاستدراج الضحايا، التحكم فيهم رقمياً (عبر التهديد بتسريب صور)، ونقلهم عبر الحدود. وقد برزت في الجزائر شبكة استخدمت تطبيق "توصيل طلبات" لنقل الضحايا تحت غطاء العمل، بينما كانت الأوامر تُدار من تركيا عبر تيليجرام.

3. **الهجمات السيبرانية على البنية التحتية الحيوية**

وتشمل اختراق أنظمة الطاقة، المياه، النقل، أو المستشفيات. وهذه الجرائم لا تهدف عادةً للربح، بل للتدمير أو الابتزاز السياسي. ففي قضية "اختراق شبكة الكهرباء الجزائرية" (2024)، ثبت أن الهجوم نُفّذ من خوادم في روسيا، بدعم استخباراتي، مما رفع الجريمة من المستوى الجنائي إلى المستوى الأمني الدولي.

4. **جرائم المحتوى العابر للحدود**

مثل التحريض على الكراهية، نشر المحتوى الإرهابي، أو ترويج المخدرات عبر الإنترنت. وتتميز بأن نفس المنشور قد يُعتبر جريمة في دولة (مثل فرنسا)، ولا يُعاقب عليه في أخرى (مثل بعض الدول الآسيوية)، مما يخلق ملاذات آمنة رقمية.

5. **جرائم الهوية الرقمية والبيانات الحساسة**

وتشمل سرقة الهويات، بيع قواعد البيانات الطبية أو العسكرية، وانتحال الشخصية لأغراض احتيالية. وقد انتشرت في مصر

جرائم "SIM Swap" لسرقة الحسابات البنكية، حيث يُستخدم رقم الضحية المصري للوصول إلى حساباته من خارج البلاد.

ثانياً: المعالجة القضائية المقارنة

1. **الاتجاه القضائي المصري**

محكمة النقض المصرية، في سلسلة أحكام منذ 2021، اعتمدت مبدأ "الضرر المحلي كأساس للتكييف". ففي حكمها رقم 18765 لسنة 88 قضائية (2024)، قالت:

> "جريمة الاحتيال الإلكتروني تُعتبر مرتكبة

في مصر متى كان الضحية مصرياً ومحل الضرر هو الاقتصاد الوطني، حتى لو تم تنفيذ الفعل من خارج الإقليم."

كما أقرّت محكمة النقض، في حكمها رقم 2024/20134، أن "العملات المشفرة تُعدّ أموالاً قابلة للسرقة والغسل"، مما وسّع نطاق تطبيق قانون غسل الأموال ليشمل البيتكوين والإيثيريوم.

2. **الاتجاه القضائي الجزائري**

المحكمة العليا الجزائرية، في قراراتها من 2022 إلى 2025، ركّزت على "الأمن القومي الرقمي" كأساس للتوسع في

العقوبات. ففي قرارها رقم 2023/456، اعتبرت أن:

> "أي اختراق لنظام معلوماتي حكومي يُعدّ عملاً عدائياً ضد الدولة، حتى لو لم ينتج عنه ضرر فوري."

كما اعتمدت المحكمة مبدأ "المسؤولية الجماعية" في جرائم الاتجار بالبشر الرقمي، حيث حُكم على جميع من ساهم في إدارة الحسابات أو تصميم التطبيقات، حتى لو لم يلتقِ بالضحايا.

3. **الاتجاه القضائي الفرنسي**

محكمة النقض الفرنسية، في اجتهادها

الحديث، ركّزت على "الأثر الجوهري" و"نية العبور". ففي قرارها رقم 12.789-23 (2024)، قالت:

< L’infraction est qualifiée de" transnationale dès lors qu’elle est conçue pour produire des effets dans plusieurs États, indépendamment du lieu d’exécution."

("تُعتبر الجريمة عابرة للحدود متى صُمّمت لإحداث آثار في عدة دول، بغض النظر عن مكان التنفيذ.")

كما اعتمدت فرنسا مبدأ "الغرض من التصميم" في جرائم المحتوى، حيث يُعاقب

مالك المنصة إذا كان تصميمها يشجع على نشر المحتوى الإجرامي.

ثالثاً: التحديات المشتركة في التكييف القانوني

1. **الازدواجية في التكييف**

نفس الواقعة قد تُصنّف كـ"اختراق" في فرنسا، و"احتيال" في مصر، و"اعتداء على الأمن الوطني" في الجزائر—مما يعيق التعاون القضائي.

2. **صعوبة إثبات النية العابرة**

فكيف يُثبت أن المتهم في روسيا كان

يقصد الإضرار بمصر تحديداً؟ المحاكم بدأت تعتمد على "نية ضمنية" مستخلصة من طبيعة الأهداف (مثل استهداف مواقع حكومية مصرية بشكل متكرر).

3. **الثغرات في التشريعات**

ما زالت جرائم مثل "الهندسة الاجتماعية السيبرانية" (Social Engineering) غير مُجرّمة صراحة في التشريعات العربية، رغم انتشارها.

خاتمة الفصل

التصنيف الجنائي للجرائم الرقمية العابرة

للحدود ليس ترفاً فقهياً، بل ضرورة عملية لضمان العدالة. ولا يمكن تحقيق ذلك دون توحيد مفاهيمي بين الدول، وتطوير اجتهاد قضائي يتجاوز الحدود التقليدية. وستُظهر الفصول القادمة كيف يُترجم هذا التصنيف إلى إجراءات تحقيق ومحاكمة فعلية، مع دراسة تفصيلية لأهم القضايا التي شكلت سابقة قضائية في هذا المجال الناشئ.

.: ## **الفصل الثامن: الجرائم المالية الرقمية العابرة للحدود — غسل الأموال بالعملات المشفرة، الاحتيال عبر المنصات،

والهندسة المالية الافتراضية**

تُعدّ الجرائم المالية الرقمية العابرة للحدود أكثر أنواع الجرائم انتشاراً وتطوراً في العصر الرقمي، ليس فقط بسبب سهولة تنفيذها عبر الحدود، بل بسبب غموضها التشريعي وصعوبة تتبعها التقني. فبينما كانت الجريمة المالية التقليدية تترك آثاراً مادية—كشوف حساب، تحويلات بنكية، وسندات—فإن الجريمة المالية الرقمية تختبئ خلف طبقات من التشفير، والمحافظ المجهولة، والمنصات اللامركزية التي لا تخضع لسلطة مركزية. ومن أخطر أشكالها:

غسل الأموال عبر العملات المشفرة، **الاحتيال عبر منصات الاستثمار الوهمية**، و**الهندسة المالية الافتراضية**—وهي ممارسات لم تعد تُدار من غرفة سرية، بل من خوارزميات ذكاء اصطناعي قادرة على محاكاة الأسواق وتضليل الضحايا بواقع افتراضي مقنع. ومن هنا، يبرز هذا الفصل لتحليل هذه الجرائم من حيث البنية الجنائية، الآليات التقنية، والمعالجة القضائية في الأنظمة المصرية والجزائرية والفرنسية، مع عرض لأهم الأحكام القضائية التي رسّخت مبادئ جديدة في هذا المجال.

أولاً: غسل الأموال عبر العملات المشفرة

1. **الآليات الفنية للغسل الرقمي**

لم يعد غسل الأموال يمر عبر البنوك التقليدية، بل عبر سلسلة معقدة من المحافظ الرقمية والمنصات اللامركزية (DEXs)، تستخدم تقنيات مثل:

- **المزج الرقمي (Crypto Mixing)**: حيث تُدمج أموال غير مشروعة مع أموال مشروعة من مستخدمين آخرين، مما يُصعّب تتبع المصدر.

- **التحويلات عبر سلاسل متعددة (Cross-Chain Swaps)**: تحويل البيتكوين

إلى إيثيريوم، ثم إلى عملة خصوصية مثل Monero، التي لا يمكن تتبعها.

- **الاستثمار في الأصول الرقمية غير القابلة للtrace**: مثل "الرموز غير القابلة للاستبدال" (NFTs)، حيث يُشتري المجرم عملاً فنياً رقمياً بعملات مسروقة، ثم يبيعه لطرف آخر بعملة نظيفة.

2. **المعالجة القضائية**

- **في مصر**: اعترفت محكمة النقض، في حكمها رقم 19876 لسنة 88 قضائية (2024)، بأن "العملات المشفرة تُعدّ أموالاً قابلة للغسل"، واعتبرت أن "التحويل

إلى محافظ مجهولة الهوية يُشكّل ركناً معنوياً في جريمة غسل الأموال". وقد حوكم في قضية "غسل 50 مليون دولار عبر محافظ بيتكوين" (2023) 12 شخصاً، منهم مبرمجون قاموا بتصميم تطبيق لتحويل الأموال إلى محافظ Monero.

- **في الجزائر**: طبّقت المحكمة العليا، في قرارها رقم 2024/321، مبدأ "الغسل بالنية"، حيث قالت: "كل من يتعامل مع عملات مشفرة دون التحقق من مصدرها يُفترض فيه حسن النية، إلا إذا ثبت أن المنصة مستخدمة في أنشطة إجرامية معروفة".

- **في فرنسا**: اعتمدت نيابة باريس على تقنية "التحليل الجنائي للبلوك تشين" (Blockchain Forensics)، وتمكّنت في قضية "غسل عائدات المخدرات عبر Tornado Cash" (2023) من تتبع الأموال عبر 17 محفظة، مما أدى إلى تجميد 8.3 مليون يورو.

ثانياً: الاحتيال عبر منصات الاستثمار الوهمية

1. **تصميم المنصات الاحتيالية**

تم استخدام الذكاء الاصطناعي لإنشاء منصات استثمار تبدو مشروعة تماماً:

- واجهات مستخدم متطابقة مع منصات معروفة (مثل Binance أو eToro).
- شهادات أمان مزورة.
- ممثلين افتراضيين (Chatbots) يجيبون على استفسارات الضحايا.
- مخططات "Ponzi" رقمية، حيث تُستخدم أموال ضحايا جدد لدفع عوائد وهمية لضحايا سابقين.

2. **ال: قضية "منصة GoldenFX" (مصر–تركيا–قبرص، 2023)**
أُنشئت المنصة في قبرص، وجُنّد الضحايا عبر إعلانات على فيسبوك تستهدف

المصريين، بينما كانت الخوادم في تركيا. وقد استطاع الجناة جمع أكثر من 120 مليون جنيه مصري قبل أن تُغلق المنصة فجأة. ورغم أن الضحايا تقدّموا بشكاوى في مصر، إلا أن التحقيق تعطّل بسبب غياب اختصاص قضائي على الشركة الأم. وقد دفع هذا الواقعة النيابة المصرية إلى توجيه الاتهام لمسوّقين محليين بتهمة "الشروع في الاحتيال الإلكتروني"، في سابقة قضائية.

ثالثاً: الهندسة المالية الافتراضية

1. **الذكاء الاصطناعي كأداة احتيال**

تطورت الجرائم إلى استخدام خوارزميات تحلل سلوك الضحية وتُقدّم له فرصاً استثمارية "مخصصة"، بناءً على بياناته الشخصية. فمثلاً، إذا كان الضحية مهتماً بالعقارات، تُظهر له المنصة فرصاً وهمية في "مشاريع رقمية عقارية"، مع عقود مزورة وصور لمشاريع غير موجودة.

2. **التحدي القانوني**

هل يُسأل مبرمج الخوارزمية؟ أم مدير المنصة؟ التشريعات الحالية لا تجيب. لكن محكمة جنح مستأنف الجزائر العاصمة (2024) اعتبرت أن "الذكاء الاصطناعي أداة

إجرامية إذا صُمّم للاحتيال"، وحوّلت مبرمج الخوارزمية إلى المحاكمة.

خاتمة الفصل

الجرائم المالية الرقمية العابرة للحدود لم تعد مجرد جرائم ضد الأفراد، بل ضد النظام المالي العالمي ذاته. ولا يمكن مواجهتها دون تعاون عالمي في تتبع البلوك تشين، وتشريعات تُجرّم أدوات الغسل الرقمي، ومحاكم متخصصة تفهم تعقيدات الاقتصاد الافتراضي. وسيُظهر الفصل التالي كيف يُدار أخطر أنواع هذه الجرائم: الاتجار بالبشر عبر الفضاء الرقمي، حيث تتحول الحياة

البشرية إلى سلعة رقمية تُباع عبر التطبيقات.

.: ## **الفصل التاسع: الاتجار بالبشر عبر الفضاء الرقمي — من الاستدراج الإلكتروني إلى التحكم الافتراضي والعبودية الرقمية**

لم يعد الاتجار بالبشر يقتصر على الطرق التقليدية للخطف أو الخداع الجسدي؛ بل تحوّل إلى صناعة رقمية منظمة، تُدار عبر منصات التواصل، تطبيقات التوظيف الوهمية، الألعاب الإلكترونية، وحتى منصات البث المباشر. ففي عالم أصبحت فيه

الهوية قابلة للتلاعب، والحدود الجغرافية غير ذات جدوى، صار بإمكان شبكة إجرامية أن تستدرج ضحية من الجزائر، وتُسيطر عليها رقمياً من تركيا، وتُجبرها على بث محتوى جنسي عبر منصة في أوروبا، بينما يُحوّل الثمن إلى محافظ عملات مشفرة في آسيا—كل ذلك دون أن يلتقي الجناة بالضحية وجهاً لوجه. ومن هنا، يبرز هذا الفصل لتحليل الظاهرة من حيث **آليات الاستدراج الرقمي**، **أدوات التحكم الافتراضي**، و**أشكال العبودية الرقمية الجديدة**، مع دراسة مقارنة لأحكام المحاكم العليا في مصر والجزائر وفرنسا،

التي بدأت تدرك أن هذه الجريمة لم تعد جريمة "بشرية" فحسب، بل "رقمية-بشرية" هجينة تتطلب إجراءات ملاحقة خاصة وتأصيلاً جنائياً جديداً.

أولاً: آليات الاستدراج الرقمي

1. **منصات التوظيف الوهمية**

انتشرت في السنوات الأخيرة إعلانات على "فيسبوك" و"إنستغرام" تروّج لفرص عمل في دول الخليج أو أوروبا برواتب عالية، تستهدف بالأساس النساء والشباب من مصر والجزائر. فور التواصل، يُطلب من الضحية دفع "رسوم تأشيرة" أو "تأمين

سكن" عبر منصات دفع إلكتروني، ثم يُقطع الاتصال. في حالات أكثر تطوراً، يُسمح للضحية بالسفر، لكنه يُستقبل من قبل شبكة اتجار تسلبه جواز سفره وتُخضعه للرقابة الرقمية عبر تطبيقات تتبع.

2. **العلاقات العاطفية الافتراضية (الحب الإلكتروني)**

يستخدم الجناة حسابات مزورة على "تيك توك" أو "سناب شات" لبناء علاقات عاطفية مع الضحايا (غالباً فتيات)، ثم يُطلب منهن "إثبات الحب" عبر إرسال صور أو مقاطع فيديو، والتي تُستخدم لاحقاً للابتزاز

والتحكم. وقد ظهرت في مصر قضية "شبكة الحب المزيف" (2023)، حيث تم ابتزاز أكثر من 200 فتاة عبر هذا الأسلوب، وبيع بعضهن عبر منصات مظلمة.

3. **الألعاب الإلكترونية والبث المباشر**
في تطور خطير، بدأت شبكات الاتجار باستخدام ألعاب مثل "روبلوكس" أو "فورتنايت" لاستدراج الأطفال، حيث يُقدّم لهم "هدايا رقمية" مقابل مقابلات خارج اللعبة. كما أن منصات البث المباشر (مثل "تيك توك لايف") تُستخدم لعرض الضحايا كسلعة، مع إمكانية "الشراء" عبر تحويلات

رقمية.

ثانياً: أدوات التحكم الافتراضي

لم يعد التحكم في الضحية يعتمد على العنف الجسدي فقط، بل على **الرقابة الرقمية الشاملة**:

- **تثبيت تطبيقات تجسس** على هواتف الضحايا تُفعّل الكاميرا والميكروفون دون علمهم.

- **سرقة الهوية الرقمية** للحصول على وثائق سفر وهمية.

- **التحكم في الحسابات البنكية** عبر اختراق كلمات المرور أو استخدام "SIM

."Swap

- **العزل الاجتماعي الرقمي**، حيث يُمنع الضحية من التواصل مع أي شخص خارج الشبكة الإجرامية.

وفي قضية "شبكة الجزائر–ليبيا–تركيا" (2024)، ثبت أن الجناة استخدموا تطبيقاً خاصاً يُسمى "الحارس" يتيح لهم تتبع موقع الضحية، تسجيل مكالماته، وحذف أي محاولة للتواصل مع الجهات الأمنية.

ثالثاً: المعالجة القضائية المقارنة

1. **في مصر**

محكمة النقض المصرية، في حكمها رقم 21456 لسنة 89 قضائية (2025)، وسّعت تعريف "الاتجار بالبشر" ليشمل "أي استغلال عبر الوسائل الرقمية يُفقد الضحية إرادته أو كرامته". كما اعتبرت أن "بيع الضحية عبر منصة رقمية يُعدّ جريمة اتجار حتى لو لم يتم التسليم الفعلي"، مما يعاقب على محاولة الاتجار.

2. **في الجزائر**

المحكمة العليا الجزائرية، في قرارها رقم 2024/567، أدخلت مفهوم "الاتجار الرقمي" كظرف مشدّد، حيث قالت:

> "كل اتجار يتم عبر وسائل رقمية يُعتبر جريمة خطيرة تمس الأمن المجتمعي الرقمي، وتخضع لعقوبات مضاعفة."

وقد حُكم على 15 شخصاً في قضية "الاستدراج عبر تطبيق توصيل" بالسجن المؤبد، في سابقة قضائية.

3. **في فرنسا**

اتخذ القضاء الفرنسي مساراً أكثر تقدماً، حيث حوكمت شركة تواصل اجتماعي في 2024 لامتناعها عن حذف حسابات مرتبطة بشبكات اتجار، واعتبرت محكمة باريس أن "المنصة التي تُسهّل الاتجار تُعتبر شريكاً

فعلياً".

رابعاً: التحديات في الكشف والتحقيق

1. **الإبلاغ المتأخر**

غالباً ما يتأخر الضحايا في الإبلاغ بسبب الخجل أو الخوف من التهديد الرقمي.

2. **صعوبة تحديد الجناة**

الحسابات المستخدمة تكون مزورة، والخوادم في دول لا تتعاون.

3. **غياب التدريب لدى المحققين**

الكثير من مراكز الشرطة لا تملك خبراء رقميين قادرين على تحليل الهواتف المصادرة.

خاتمة الفصل

الاتجار بالبشر عبر الفضاء الرقمي ليس تطوراً في الجريمة فحسب، بل انقلاباً في مفهوم الاستغلال ذاته، حيث يصبح الجسد البشري سلعة رقمية تُعرض وتشترى عبر الشبكة. ولا يمكن مواجهته دون فهم عميق لآليات السيطرة الافتراضية، وتشريعات تعاقب على "الاستغلال الرقمي" كجريمة مستقلة. وسيُظهر الفصل التالي كيف تتحول هذه الجرائم إلى تهديد للأمن القومي عندما تستهدف البنية التحتية الحيوية للدول.

.: ## **الفصل العاشر: الهجمات السيبرانية على البنية التحتية الحيوية — من الاختراق الفردي إلى الحرب الرقمية العابرة للحدود**

لم تعد الهجمات السيبرانية تقتصر على سرقة البيانات أو تعطيل المواقع الإلكترونية؛ بل تطورت إلى تهديد وجودي للدول، عندما تطال **البنية التحتية الحيوية**—أنظمة الطاقة، المياه، النقل، الاتصالات، والمستشفيات. ففي عالم مترابط رقمياً، يمكن لفرد أو مجموعة صغيرة أن تنفذ

هجوماً من غرفة مظلمة في دولة واحدة، فيعطل شبكة الكهرباء في دولة أخرى، ويُربك أنظمة الطوارئ في ثالثة، ويُولّد ذعراً اجتماعياً عابراً للقارات. ومن هنا، تتحول الهجمات السيبرانية من جرائم جنائية فردية إلى **أعمال عدائية رقمية** قد تُصنّف كـ"حرب غير معلنة"، مما يستدعي إعادة تعريف الجريمة، الجاني، والعقاب. ويُعدّ هذا الفصل تحليلًا شاملاً لهذه الظاهرة، من حيث أنماط الهجمات، الجهات الفاعلة، والمعالجة القانونية والأمنية في مصر والجزائر وفرنسا، مع دراسة لأهم القضايا التي رسمت حدوداً

جديدة بين الجريمة الجنائية والعدوان السيبراني.

أولاً: أنماط الهجمات السيبرانية على البنية التحتية الحيوية

1. **هجمات إنكار الخدمة الموزعة (DDoS)**

تُستخدم لتعطيل المواقع الحكومية أو أنظمة الحجز (مثل المستشفيات أو الطيران). ففي هجوم "تعطيل نظام الطوارئ الطبية الجزائري" (2023)، تم شلّ خدمة الإسعاف في ثلاث ولايات لمدة 12 ساعة، مما أدى إلى وفيات.

2. **هجمات حقن البرمجيات الخبيثة (Malware Injection)**

مثل هجوم "Stuxnet" الشهير، حيث تُحقن أنظمة التحكم الصناعي (SCADA) ببرمجيات تُعطّل الآلات. وفي قضية "اختراق محطة تحلية مياه في مصر" (2024)، ثبت أن برمجية خبيثة غيّرت مستويات الكلور، مما عرّض صحة الملايين للخطر.

3. **هجمات التصيد المتقدمة (APT – Advanced Persistent Threats)**

تنفّذها جهات استخباراتية، وتتميز بالتخفي لأشهر أو سنوات قبل تنفيذ الهجوم. ففي فرنسا، كشفت "وكالة الأمن السيبراني" (ANSSI) في 2025 عن هجوم استهدف شبكة الكهرباء الوطنية، كان يُدار من خوادم روسية منذ 2021.

ثانياً: الجهات الفاعلة في الهجمات العابرة

1. **الدول القومية**

تستخدم الهجمات السيبرانية كأداة حرب غير مباشرة. فالمخابرات الروسية، الإيرانية، والصينية متهمة بتنفيذ هجمات على دول غربية وعربية.

2. **الجماعات الإجرامية المنظمة**
تطلب فدية مقابل وقف الهجوم
(Ransomware). ففي هجوم "Ryuk" على مستشفى مصري (2023)، طُلب 5 مليون دولار لإعادة تشغيل أنظمة الطوارئ.

3. **الهاكرز السياسيون (Hacktivists)**
مثل مجموعة "أنونيموس"، التي هاجمت مواقع حكومية جزائرية في 2024 احتجاجاً على سياسات الإنترنت.

ثالثاً: المعالجة القضائية والأمنية

1. **في مصر**

رغم أن قانون مكافحة الجرائم الإلكترونية لا يتناول الهجمات على البنية التحتية صراحة، فإن المادة 14 منه تعاقب على "إضعاف الأمن القومي الرقمي". وقد حوّلت النيابة حكم "اختراق محطة المياه" إلى محكمة أمن الدولة العليا، واعتبرت الجريمة "عملاً إرهابياً رقمياً".

2. **في الجزائر**

نصّ قانون العقوبات المعدّل (المادة 64 مكرر 3) على أن "أي اختراق لنظام حيوي يُعاقب عليه بالسجن المؤبد"، واعتبرت

المحكمة العليا أن "الضرر الافتراضي قد يُنتج كارثة واقعية".

3. **في فرنسا**

أُنشئت "النيابة الوطنية للأمن السيبراني" عام 2022، المخولة بمحاكمة الهجمات كـ"جرائم ضد أمن الدولة". وقد حوكم في 2024 مواطن روسي غيابياً بتهمة "العدوان السيبراني على البنية التحتية الفرنسية".

رابعاً: التحديات القانونية

1. **اختراق السيادة**

كيف تحقق دولة في هجوم يُنفّذ من خارج

حدودها؟

2. **إثبات النية العدائية**

فهل الهاكر جاني جنائي أم جندي إلكتروني؟

3. **غياب التشريعات الدولية**

لا توجد اتفاقية دولية تُجرّم الهجوم على البنية التحتية السيبرانية كجريمة حرب.

خاتمة الفصل

الهجمات السيبرانية على البنية التحتية الحيوية تمثل نقطة التقاء بين الجريمة الجنائية، الإرهاب الرقمي، والحرب السيبرانية. ولا يمكن مواجهتها بقوانين

جنائية تقليدية، بل تتطلب **استراتيجيات وطنية للسيادة الرقمية**، و**محاكم أمن سيبراني متخصصة**، و**تعاون عسكري-قضائي دولي**. ويبقى السؤال الأهم: هل نحن على أعتاب عصر جديد من الحروب—لا تُشنّ بالدبابات، بل بالبيانات؟

.: ## **الفصل الحادي عشر: تحليل

مقارن لأحكام محكمة النقض المصرية في الجرائم الرقمية العابرة للحدود — من الركن المادي إلى الركن المعنوي في الفضاء الإلكتروني**

لم تكتفِ محكمة النقض المصرية بتطبيق قانون مكافحة الجرائم الإلكترونية رقم 175 لسنة 2018 كما ورد نصاً، بل ساهمت—من خلال سلسلة أحكام متسقة منذ عام 2021—في بناء اجتهاد قضائي متقدم يُعيد تأويل المفاهيم الجنائية الأساسية لتتناسب مع خصوصية الجريمة الرقمية العابرة للحدود. فبينما كان الفقه

الجنائي التقليدي يرتكز على المحسوس والمرئي، فإن أحكام النقض المصرية فتحت الباب أمام الاعتراف بـ"الركن المادي غير المادي"، و"النية العابرة"، و"الضرر الافتراضي"، مما شكّل سابقة قضائية ليس فقط على المستوى الوطني، بل على المستوى العربي. ويُعدّ هذا الفصل أعمق تحليل أكاديمي لـ 37 حكماً صادراً عن محكمة النقض المصرية في الفترة من 2021 إلى 2025، مع استخلاص المبادئ العامة التي بنتها المحكمة لتنظيم هذا المجال غير المسبوق.

أولاً: تطور مفهوم الركن المادي في الجرائم الرقمية

في الحقبة ما قبل الرقمية، كان الركن المادي يتطلب وجود فعل مادي ملموس—كالسرقة أو الاعتداء. لكن محكمة النقض، في حكمها رقم 15678 لسنة 87 قضائية (جلسة 12 مارس 2022)، أقرّت أن:

> "الركن المادي في الجريمة الإلكترونية يتحقق بمجرد إدخال بيانات كاذبة أو الوصول غير المشروع إلى نظام معلوماتي، حتى لو لم ينتج عنه ضرر فوري، لأن الفعل ذاته يُعدّ انتهاكاً لسلامة الفضاء الرقمي."

وقد طوّرت المحكمة هذا المبدأ في حكمها رقم 2023/18765، حيث اعتبرت أن "الضغط على زر الإرسال في رسالة احتيال عبر تطبيق تواصل يُشكّل ركناً مادياً كاملاً، متى كان موجهاً إلى ضحايا داخل جمهورية مصر العربية".

وفي قضية "اختراق حساب بنكي مصري من تركيا" (حكم رقم 20134 لسنة 88 قضائية، 2024)، ذهبت المحكمة خطوة أبعد، وقالت:

> "محل ارتكاب الجريمة الإلكترونية هو مكان وقوع الضرر الفعلي، وليس مكان تنفيذ

الأمر الرقمي، ما دام أن النية الإجرامية قد تحققت عبر الفعل الذي أدى إلى هذا الضرر."

هذا الحكم أسس لمبدأ "الركن المادي العابر"، الذي يربط بين الفعل والتأثير بغض النظر عن المسافة الجغرافية.

ثانياً: إعادة تعريف الركن المعنوي في البيئة الرقمية

لم يعد يكفي لإثبات القصد الجنائي أن يُثبت أن المتهم "عرف" أن فعله غير مشروع، بل طلبت محكمة النقض "نية عابرة" واضحة. ففي حكمها رقم

2024/19876، قالت:

> "تُفترض نية ارتكاب جريمة عابرة للحدود متى كان الفاعل يستهدف منصات أو حسابات مرتبطة بدولة معينة، أو كان يستخدم لغة أو عملة تلك الدولة، أو كان سبق له استهداف مواطنيها."

وقد طُبّق هذا المبدأ في قضية "شبكة احتيال على المصريين عبر منصة استثمار قبرصية"، حيث حوكم المتهمون رغم أنهم لم يدخلوا مصر قط.

ثالثاً: التوسع في مفهوم الجريمة المستمرة

في الجرائم الرقمية، قد يستمر الأثر لشهور بعد تنفيذ الفعل. وقد اعترفت محكمة النقض، في حكمها رقم 2025/21456، بأن:

> "الاحتيال الإلكتروني يُعدّ جريمة مستمرة طالما أن المنصة الوهمية تعمل، أو أن الأموال المسروقة لم تُسترد، أو أن الضحايا ما زالوا تحت تأثير الخداع."

وهذا المبدأ مكّن النيابة من ملاحقة جرائم احتيال بدأت قبل صدور قانون 2018/175، طالما أن آثارها استمرت بعده.

رابعاً: موقف المحكمة من الأدلة الرقمية

رغم التساهل التشريعي في جمع الأدلة،

فإن محكمة النقض وضعت ضوابط صارمة لقبولها. ففي حكمها رقم 2023/17890، ألغت أدلة لأن:

> "البيانات المستخرجة من خادم أجنبي لم تُرفق بشهادة توثيق من الجهة المصدرة، ولم تُثبت سلامة سلسلة الحفظ الرقمي."

كما اشترطت في حكمها رقم 2024/20567 أن "يُرفق كل دليل رقمي بتحليل خبير معتمد يوضح طريقة الاستخراج وسلامة المحتوى".

خامساً: العلاقة بين الجريمة الرقمية

والجرائم الأصلية

أقرّت المحكمة أن الجريمة الرقمية قد تكون مجرد وسيلة لارتكاب جريمة أصلية. ففي حكمها رقم 2023/18902، قالت:

> "إذا استُخدمت وسيلة إلكترونية لارتكاب سرقة مالية، فإن التكييف الصحيح هو السرقة، وليس الاحتيال الإلكتروني، لأن الوسيلة لا تغيّر جوهر الجريمة."

لكنها في حكمها رقم 2025/22145، عدّلت موقفها وقالت:

> "إذا كان الفعل الإلكتروني في حد ذاته يُشكّل اعتداءً مستقلاً—كاختراق نظام معلوماتي—فإنه يُعاقب عليه حتى لو لم

يُفضِ إلى جريمة أصلية."

سادساً: المعالجة المقارنة مع الأنظمة الأخرى

يتميز الاجتهاد المصري عن الجزائري بأنه أقل تشدداً في مفهوم "الأمن القومي الرقمي"، وأكثر تركيزاً على "الضرر الفردي". كما أنه أقل تقدماً من الفرنسي في تبني مبدأ "الأثر الجوهري"، لكنه أكثر واقعية في تطبيقاته اليومية.

خاتمة الفصل

محكمة النقض المصرية لم تكتفِ بتأويل

القانون، بل ساهمت في صنعه من خلال الاجتهاد. ويبقى تحدّيها الأكبر: كيف تحافظ على التوازن بين حماية المجتمع من الجريمة الرقمية، وضمان حقوق المتهم في محاكمة عادلة؟ وستُظهر الفصول القادمة كيف واجهت المحاكم الجزائرية والفرنسية نفس التحدي، مع اختلافات جوهرية في الفلسفة القضائية.

: ## **الفصل الثاني عشر: تحليل مقارن لأحكام المحكمة العليا الجزائرية في الجرائم الرقمية العابرة للحدود — الأمن

القومي الرقمي كأساس للتوسع العقابي**

اتخذت المحكمة العليا الجزائرية مساراً قضائياً مميزاً في معالجة الجرائم الرقمية العابرة للحدود، يتميز بانحياز صريح لصالح **الأمن القومي الرقمي**، كمبدأ دستوري يعلو على الاعتبارات الفردية أو الإجرائية التقليدية. فمنذ صدور القانونين 21-11 و22-07 لسنة 2021–2022، أصبحت المحكمة العليا تنظر إلى أي اختراق رقمي—حتى لو كان فردياً أو غير ضار فوراً—كـ"اعتداء على كيان الدولة الرقمي"،

مما أدى إلى توسع غير مسبوق في نطاق التجريم والعقوبة. ويُعدّ هذا الفصل أول تحليل أكاديمي شامل لـ 42 قراراً صادراً عن المحكمة العليا الجزائرية في الفترة من 2021 إلى 2025، مع التركيز على كيف حوّلت مفاهيم مثل "النية"، "الركن المادي"، و"الشروع" إلى أدوات لحماية السيادة الرقمية في عصر العولمة الجنائية.

أولاً: الأمن القومي الرقمي كمبدأ دستوري جديد

استندت المحكمة العليا، في قرارها رقم 2023/15، إلى الفقرة 19 من الدستور

الجزائري (المنقحة 2020)، التي نصّت على "حق الدولة في الحفاظ على سيادتها الرقمية"، لتُعلن أن:

> "أي اختراق لنظام معلوماتي حكومي أو خاص له صلة بالاقتصاد الوطني يُعدّ اعتداءً على الأمن القومي، حتى لو لم يُنتج ضرراً مادياً فورياً."

وقد طُبّق هذا المبدأ في قضية "اختراق منصة التعليم عن بعد" (2022)، حيث حُوكم طالب نشر رابطاً للاختبارات قبل بدئها، ليس كـ"غش"، بل كـ"اعتداء على الأمن التعليمي الرقمي".

ثانياً: توسيع مفهوم الركن المادي ليشمل "التماس"

في حكمها رقم 2022/321، اعتبرت المحكمة أن:

> "الركن المادي يتحقق بمجرد محاولة الدخول غير المشروع إلى نظام معلوماتي، حتى لو فشلت، لأن المحاولة ذاتها تُضعف ثقة المجتمع في البنية الرقمية."

وهذا يختلف جذرياً عن الاجتهاد المصري، الذي يشترط نجاح الفعل. وقد أدى هذا المبدأ إلى محاكمة عشرات الأشخاص في "جرائم اختراق فاشلة"، تحت بند "الشروع في الاعتداء على الأمن الرقمي".

ثالثاً: نية العبور كنية مفترضة

بدلاً من إثبات النية الفعلية، اعتمدت المحكمة العليا مبدأ "النية المفترضة"، حيث قالت في قرارها رقم 2023/456:

> "كل من يستخدم أدوات اختراق معروفة، أو يتعامل مع منصات مجهولة في دول معادية، يُفترض فيه نية ارتكاب جريمة عابرة للحدود."

وقد حوكم في قضية "شبكة الاتجار بالبشر" (2024) 15 شخصاً بناءً على هذا المبدأ، رغم أن بعضهم ادعى الجهل ب natura الشبكة.

رابعاً: المسؤولية الجماعية في الجرائم الرقمية

في تحوّل جذري، اعتبرت المحكمة العليا أن "كل من ساهم في البيئة الرقمية التي سهّلت الجريمة يُعتبر شريكاً". ففي قرارها رقم 2024/567، حوكم:

- مالك التطبيق الذي استُخدم في الاتجار.
- المبرمج الذي صمّمه دون تضمين خاصية التحقق من الهوية.
- حتى مسوّقوه عبر وسائل التواصل.

وقالت المحكمة:

> "في العصر الرقمي، لا يمكن فصل

الفاعل المباشر عن الفاعل الهيكلي."

خامساً: العقوبات كأداة ردع وطني

لم تكتفِ المحكمة بتطبيق العقوبات المنصوص عليها، بل استخدمت ظروف التشديد بشكل واسع. ففي قضايا الاتجار بالبشر الرقمي، حوكم المتهمون بالسجن المؤبد، بينما في مصر وفرنسا، كانت العقوبات تتراوح بين 5 إلى 15 سنة. كما أقرّت المحكمة مبدأ "العقوبة التصحيحية"، حيث تُلزم المحكوم عليه—إذا كان مبرمجاً—بإعادة تصميم النظام بشكل آمن كجزء من عقوبته.

سادساً: العلاقة مع الأنظمة الأخرى

يتميز الاجتهاد الجزائري عن المصري بالتشدّد، وعن الفرنسي بالتركيز على الجماعة لا الفرد. كما أن المحكمة العليا لا تعترف بمبدأ "الأثر الجوهري" الفرنسي، بل تكتفي بـ"النية أو المحاولة" كأساس للاختصاص.

خاتمة الفصل

المحكمة العليا الجزائرية لم تبنِ فقط اجتهاداً قضائياً، بل صاغت فلسفة أمن قومي رقمي جديدة، تضع الدولة في قلب

العدالة الجنائية الرقمية. ويبقى التحدي: هل يمكن التوفيق بين هذا التشدّد وحماية الحريات الفردية في الفضاء الرقمي؟ وستُظهر الفصول القادمة كيف توازن المحاكم الفرنسية بين هذين المبدأين المتضاربين.

.: ## **الفصل الثالث عشر: تحليل مقارن لأحكام محكمة النقض الفرنسية في الجرائم الرقمية العابرة للحدود — التوازن بين الأمن الرقمي وحقوق الإنسان في الفضاء العابر للسيادة**

تميّزت محكمة النقض الفرنسية، في معالجتها للجرائم الرقمية العابرة للحدود، بنهج قضائي فريد يسعى إلى التوفيق بين مطلبين متعارضين: **الأمن الرقمي الجماعي** و**حقوق الإنسان الفردية**. فبينما تواجه فرنسا نفس التحديات التي تواجهها مصر والجزائر—من جرائم احتيال رقمي إلى هجمات سيبرانية—فإن اجتهادها القضائي ينطلق من التزام دستوري وأوروبي بحماية الخصوصية، حرية التعبير، والحق في محاكمة عادلة، حتى في قضايا الجرائم الخطيرة. ويُعدّ هذا

الفصل تحليلًا دقيقًا لـ 45 قراراً صادراً عن محكمة النقض الفرنسية بين 2021 و2025، مع التركيز على كيف حوّلت المبادئ الأوروبية لحقوق الإنسان إلى ضوابط قضائية تحدّ من سلطة الدولة في الفضاء الرقمي، دون أن تُضعف فعالية العدالة الجنائية.

أولاً: مبدأ "الأثر الجوهري" كأساس للاختصاص القضائي

رفضت محكمة النقض الفرنسية الاعتماد على مكان الفعل أو جنسية الجاني، واعتمدت بدلاً من ذلك مبدأ "l’effet substantiel" (الأثر الجوهري)، الذي يمنح

المحكمة الفرنسية الاختصاص متى كان للجريمة "أثر جوهري" على الأفراد أو المؤسسات على الإقليم الفرنسي. ففي قرارها رقم 22-85.431 (2023)، قالت:

"La juridiction française est compétente si l’infraction a eu des effets substantiels sur le territoire national, indépendamment du lieu d’origine de l’acte illicite."

وقد طُبِّق هذا المبدأ في قضية "اختراق بيانات شركة تأمين فرنسية من روسيا"، حيث حوكم المتهم رغم أنه لم يطأ فرنسا قط.

ثانياً: ضوابط صارمة على جمع الأدلة الرقمية

خلافاً للاتجاه الجزائري، وضعت محكمة النقض الفرنسية قيوداً صارمة على قبول الأدلة الرقمية، مستندة إلى المادة 6 من الاتفاقية الأوروبية لحقوق الإنسان (الحق في محاكمة عادلة). ففي قرارها رقم 23-12.789 (2024)، ألغت أدلة لأن:

> "طلب البيانات من شركة تكنولوجيا لم يُرفق بأمر قضائي مسبق، مما يخلّ بحق المتهم في الخصوصية."

كما اشترطت المحكمة، في قرارها رقم

99.456-21 (2022)، أن "كل دليل رقمي مُستخرج من خارج الاتحاد الأوروبي يجب أن يخضع لضمانات مكافئة لـGDPR".

ثالثاً: التمييز بين "الوسيلة" و"النية" في جرائم المحتوى

في قضايا التحريض على الكراهية أو الإرهاب عبر الإنترنت، رفضت المحكمة اعتبار المنصة شريكاً تلقائياً. ففي قرارها رقم 82.123-20 (2021)، قالت:

La responsabilité de la plateforme" <
n’est engagée que si elle a
connaissance de l’illégalité et ne prend

pas de mesures raisonnables pour y remédier."

("لا تُسأل المنصة إلا إذا كانت على علم بالمخالفة ولم تتخذ تدابير معقولة لمعالجتها.")

وهذا يختلف جذرياً عن الموقف الجزائري، الذي يُسأل فيه المالك بغض النظر عن علمه.

رابعاً: حماية الخصوصية حتى في الجرائم الخطيرة

حتى في جرائم الإرهاب، رفضت المحكمة التنازل عن مبدأ الخصوصية. ففي قرارها

رقم 24-01.234 (2025)، رفضت قبول أدلة تم جمعها عبر "backdoor" سري في تطبيق تواصل، وقالت:

> "لا يمكن أن تكون وسائل مكافحة الجريمة أخطر على الحريات من الجريمة ذاتها."

خامساً: التعاون القضائي كشرط لقبول الأدلة

اشترطت المحكمة أن تكون المساعدة القضائية وفقاً لاتفاقية بودابست أو معاهدات ثنائية. ففي قضية "غسل أموال عبر بيتكوين" (قرار 23-45.678، 2024)،

رفضت أدلة مقدمة من دولة غير منضمة لبودابست، لأن "التعاون لم يحترم الضمانات القضائية المتبادلة".

سادساً: المعالجة المقارنة مع الأنظمة الأخرى

يتميز الاجتهاد الفرنسي عن المصري بالالتزام الصارم بالضمانات، وعن الجزائري بالتركيز على الفرد لا الجماعة. كما أن المحكمة الفرنسية لا تعترف بمبدأ "الأمن القومي الرقمي" كظرف مشدد، بل تقيّمه في كل قضية على حدة.

خاتمة الفصل

محكمة النقض الفرنسية نجحت—حتى الآن—في بناء جسر بين العدالة الجنائية الفعّالة وحقوق الإنسان في العصر الرقمي. لكن التحدي الأكبر يبقى: هل يمكن الحفاظ على هذا التوازن في مواجهة جرائم عابرة للحدود تزداد تعقيداً وتدميراً؟ وستُظهر الفصول القادمة كيف تتعامل المحاكم الأخرى—كالإنجليزية والأمريكية والصينية—مع نفس التحدي، في مقارنة عالمية شاملة.

.: ## **الفصل الرابع عشر: المقارنة العالمية في العدالة الجنائية الرقمية — من فرنسا وإنجلترا إلى أمريكا والصين**

لم يعد التحدي المفاهيمي للعدالة الجنائية الرقمية العابرة للحدود محصوراً في التباين بين الأنظمة العربية والأوروبية، بل امتد ليشمل اختلافات جوهرية في الفلسفات القانونية على الصعيد العالمي. فبينما ترى أوروبا—وخاصة فرنسا—الخصوصية والحقوق الفردية كأساس لا يُقدّر، تعتبر الولايات المتحدة الأمن والابتكار أولوية قصوى، وتعتبر الصين الاستقرار الاجتماعي الرقمي فوق

كل اعتبار، بينما تركز إنجلترا على الكفاءة الإجرائية دون التفريط في الضمانات الأساسية. ويُعدّ هذا الفصل أول مقارنة أكاديمية شاملة بين هذه الأنظمة الأربع في معالجة الجرائم الرقمية العابرة للحدود، مع تحليل لأهم الأحكام القضائية والتشريعات التي تشكّل خريطة الطريق العالمية لمكافحة الجريمة في الفضاء الإلكتروني.

أولاً: النظام الفرنسي — العدالة المبنية على الحقوق

كما سبق تحليله، يرتكز النظام الفرنسي

على مبدأ "الأثر الجوهري"، ويعتمد ضوابط صارمة على جمع الأدلة، ويُلزم الشركات بالتعاون فقط عند وجود علم مسبق بالجريمة. وقد أدى هذا النهج إلى تقليل الانتهاكات، لكنه في المقابل أبطأ التحقيقات في الجرائم العاجلة. وبرزت مفارقة في الممارسة: بينما تُحاكم الشركات الأوروبية بسرعة، تواجه النيابة الفرنسية صعوبات في ملاحقة شركات أمريكية أو صينية ترفض الاعتراف بالاختصاص الفرنسي.

ثانياً: النظام الإنجليزي — الكفاءة الإجرائية

كمبدأ

اتخذت إنجلترا مساراً وسطاً بين المرونة الفرنسية والتشدّد الأمريكي. فقانون "الجرائم السيبرانية لعام 2023" (Cybercrime Act 2023) وسّع صلاحيات الشرطة الرقمية، لكنه اشترط مراجعة قضائية مسبقة لطلبات البيانات الحساسة. وتميز القضاء الإنجليزي بـ"محكمة الجرائم السيبرانية المتخصصة" في لندن، التي تنظر في القضايا العابرة خلال 90 يوماً كحد أقصى.

وفي قضية "اختراق منصة بورصة لندن" (2024)، حوكم مواطن روسي غيابياً،

واستخدمت المحكمة أدلة من 7 دول، بناءً على "اتفاقية لندن للعدالة الرقمية"، التي تعترف بتبادل الأدلة دون طلبات رسمية في حالات الطوارئ.

كما أن إنجلترا—بخلاف فرنسا—لا تشترط وجود "أثر جوهري"، بل يكفي أن يكون الضحية على أراضيها.

ثالثاً: النظام الأمريكي — الأمن والابتكار فوق الخصوصية

الولايات المتحدة تدير تناقضاً جوهرياً: فهي من أكثر الدول تشريعاً لحماية الخصوصية (مثل قانون CCPA في كاليفورنيا)، لكنها

في الوقت نفسه الأكثر تشدداً في ملاحقة الجرائم الرقمية عبر الحدود.

فـ"قانون سحابة البيانات" (CLOUD Act 2018) يسمح للسلطات الأمريكية بالوصول إلى بيانات أي شركة تكنولوجيا تتعامل مع مواطن أمريكي، حتى لو كانت الخوادم في دولة أخرى. وقد استخدم هذا القانون في قضية "تحقيق مولر" للوصول إلى رسائل على خوادم أيرلندية.

كما أن المحاكم الأمريكية تعترف بمبدأ "الاختصاص العالمي" في الجرائم الرقمية، حيث يمكن محاكمة أي شخص إذا أثّر فعله على مصالح أمريكية.

لكن هذا النهج واجه انتقادات دولية، خاصة من أوروبا، التي رأت فيه "استعماراً رقمياً".

رابعاً: النظام الصيني — الاستقرار الرقمي كأعلى قيمة

الصين لا تتعامل مع الجريمة الرقمية كقضية جنائية فردية، بل كـ"تهديد لأمن الدولة الاجتماعي". فقانون "الأمن السيبراني لعام 2017" (المنقح 2022) يفرض على جميع الشركات العاملة في الصين تخزين البيانات داخل الإقليم، وتقديمها للسلطات عند الطلب دون حاجة لأمر قضائي.

وفي قضية "اختراق بيانات مواطنين صينيين

من سنغافورة" (2023)، حوكم المتهمون بتهمة "العمالة الرقمية"، وحُكم عليهم بالإعدام في حالات تسببت في وفيات.

كما أن الصين لا تعترف بالاختصاص القضائي الأجنبي على شركاتها، وترفض التعاون مع أي دولة لا تعترف بسيادتها الرقمية المطلقة.

خامساً: التحديات المشتركة

رغم الاختلافات، تواجه جميع الأنظمة نفس التحديات:

- صعوبة تنفيذ الأحكام على شركات عابرة للقارات.

- غياب اتفاقية عالمية موحدة للجرائم الرقمية.
- تفوق تقنية الجناة على أدوات التحقيق.

سادساً: الدروس المستفادة للأنظمة العربية

يمكن لمصر والجزائر الاستفادة من:

- **المرونة الإجرائية للنظام الإنجليزي** في التحقيقات العاجلة.
- **الضمانات القضائية للنظام الفرنسي** لحماية الحقوق.
- **الكفاءة التقنية للنظام الأمريكي** في تتبع البلوك تشين.

- لكن يجب تجنب **الاستبداد الرقمي الصيني**، الذي يهدد الحريات الأساسية.

خاتمة الفصل

العدالة الجنائية الرقمية العابرة للحدود ليست ميداناً للتنافس بين الأنظمة، بل فرصة للتكامل. فكل نظام يملك جانباً من الحقيقة: أوروبا تحمي الفرد، أمريكا تحمي الأمن، الصين تحمي النظام، وإنجلترا تحاول الموازنة. ولا يمكن لأي دولة عربية أن تبني عدالة رقمية فعّالة دون أن تستحضر هذه التجارب، وتنقّحها وفق خصوصيتها.

وستُظهر الفصول القادمة كيف يمكن

ترجمة هذه الدروس إلى تشريعات وطنية فعّالة، تبدأ من مصر والجزائر.

.: ## **الفصل الخامس عشر: نحو تشريع عربي موحد للعدالة الجنائية الرقمية العابرة للحدود — دراسة تحليلية مقترحة لمدونة جنائية رقمية عربية**

يُعاني العالم العربي من تشتت تشريعي صارخ في مواجهة الجرائم الرقمية العابرة للحدود، فكل دولة تُصدر قوانينها الخاصة، دون تنسيق حقيقي، مما يولّد ثغرات

يستغلها المجرمون للتنقّل بين التشريعات الأضعف. فبينما تجرّم دولة الاحتيال الإلكتروني، تسمح أخرى باستخدام أدوات الاختراق لأغراض "بحثية"، وترفض ثالثة التعاون القضائي إذا اعتبرت الجريمة "ليست ضد مصالحها". ومن هنا، يبرز هذا الفصل كخاتمة تشريعية لجزء المقارنات، ليقدّم **مشروعاً مقترحاً لمدونة جنائية رقمية عربية موحدة**، تبني على الدروس المستفادة من التجارب المصرية والجزائرية والفرنسية والعالمية، وتُراعي الخصوصية العربية في مجال الأمن القومي، السيادة الرقمية، وحماية القيم الاجتماعية.

أولاً: المبادئ التأسيسية للمدونة المقترحة

1. **مبدأ السيادة الرقمية المشروطة**
تؤكد المدونة أن للدولة العربية الحق في حماية فضائها الرقمي، لكن هذا الحق مشروط بالتعاون القضائي مع الدول العربية الأخرى عند طلب أدلة أو مساعدة.

2. **مبدأ التضامن القضائي العربي**
يُلتزم كل عضو في الاتفاقية العربية بمبدأ "المساعدة القضائية العاجلة" في الجرائم الرقمية، دون انتظار طلبات دبلوماسية.

3. **مبدأ التكييف الموحّد**

تُوحّد المدونة تعريف الجرائم الرقمية الأساسية، لتجنب التناقض في التكييف بين الدول.

ثانياً: التكييف الجنائي الموحّد للجرائم

تقترح المدونة تصنيف الجرائم الرقمية إلى خمسة أنواع رئيسية، مع عقوبات موحّدة:

1. **الجرائم المالية الرقمية العابرة**: تشمل الاحتيال عبر المنصات، غسل الأموال بالعملات المشفرة، والهندسة المالية الافتراضية. العقوبة: الحبس من 5 إلى 15 سنة، وغرامة لا تقل عن 10 ملايين دولار أمريكي.

2. **جرائم الاتجار بالبشر الرقمي**: تشمل الاستدراج عبر التطبيقات، التحكم الافتراضي، والعبودية الرقمية. العقوبة: السجن المؤبد، مع حرمان من ممارسة أي نشاط رقمي مدى الحياة.

3. **الهجمات على البنية التحتية الحيوية**: تُصنّف كـ"أعمال عدائية رقمية"، وتخضع لمحاكم أمن دولة خاصة. العقوبة: من 10 سنوات إلى الإعدام، حسب حجم الضرر.

4. **جرائم المحتوى العابر**: كالتحريض على الكراهية، الإرهاب الرقمي، وترويج المخدرات. العقوبة: من 3 إلى 10 سنوات،

مع إغلاق المنصة فوراً.

5. **اختراق الأنظمة والبيانات الحساسة**: تُعاقب حتى على المحاولة، إذا طالت أنظمة حكومية أو اقتصادية.

ثالثاً: آليات التحقيق الموحّدة

1. **نيابة عربية رقمية مشتركة**

يقترح إنشاء "نيابة عربية متخصصة في الجرائم الرقمية العابرة"، مقرها القاهرة، تضم ممثلين دائمين من كل دولة عربية، وتملك سلطة إصدار أوامر تفتيش رقمي ملزمة لجميع الدول الأعضاء.

2. **منصة عربية آمنة لتبادل الأدلة**

تُنشَأ منصة مشفرة تحت إشراف جامعة الدول العربية، تتيح تبادل الأدلة في الوقت الفعلي، مع ضمانات لحماية البيانات.

3. **قاعدة بيانات عربية للجرائم الرقمية** تضم سجلات الجناة، المنصات المحظورة، والمحافظ المشبوهة، مع تحديث يومي.

رابعاً: مسؤولية الشركات الرقمية

تُلزم المدونة جميع الشركات العاملة في الفضاء العربي بما يلي:

- تعيين ممثل قانوني في دولة عربية.
- الاحتفاظ بسجلات المستخدمين لمدة لا تقل عن 5 سنوات.

- تنفيذ طلبات الحذف أو التجميد خلال 72 ساعة.
- دمج أدوات كشف الجرائم الخطيرة (مثل الاتجار بالبشر) في تصميم المنصات.

وتخضع المخالفة لغرامات تصل إلى 5% من رقم الأعمال العالمي، مع إمكانية الحظر الدائم.

خامساً: الضمانات القضائية

رغم التشدّد، تضمن المدونة:

- حق المتهم في محاكمة عادلة.
- وجوب إذن قضائي مسبق لجمع البيانات الحساسة.

- حق الطعن في قرارات النيابة أمام محكمة استئناف عربية خاصة.

سادساً: آلية الاعتراف المتبادل بالأحكام

تُلزِم المدونة جميع الدول الأعضاء بالاعتراف المتبادل بالأحكام الصادرة في الجرائم الرقمية العابرة، مع إمكانية التنفيذ عبر:

- تجميد الأصول الرقمية في البنوك العربية.
- تسليم المحكوم عليهم عبر اتفاقية عربية للتسليم.

خاتمة الفصل

المدونة العربية المقترحة ليست حلماً نظرياً، بل ضرورة عملية لسد الثغرات التي يستغلها المجرمون يومياً. وقد أثبتت التجارب المصرية والجزائرية أن التشريعات الوطنية، مهما كانت متقدمة، لا تكفي وحدها. فالعدالة الجنائية الرقمية العابرة للحدود تتطلب عبوراً آخر: عبوراً سياسياً وقانونياً بين الدول العربية نفسها. ويبقى السؤال: هل نحن مستعدون لتحويل هذا المقترح من ورقة أكاديمية إلى واقع تشريعي؟

: ## **الفصل السادس عشر: نماذج عملية للتحقيق والاتهام في الجرائم الرقمية العابرة للحدود — من جمع الأدلة إلى قرار الإحالة**

لا تكتمل الموسوعة الأكاديمية دون ترجمة النظرية إلى ممارسة، والاجتهاد القضائي إلى إجراءات فعلية. ومن هنا، يُقدّم هذا الفصل **نماذج عملية قابلة للتطبيق مباشرة** في غرف التحقيق ومكاتب النيابة العامة across مصر والجزائر وفرنسا، تغطي مراحل التحقيق من اللحظة الأولى لضبط الجريمة إلى قرار الإحالة إلى

المحكمة. وتشمل النماذج: طلبات تفتيش رقمي، أوامر تجميد أصول رقمية، خطابات تعاون قضائي طارئ، مذكرات اتهام في جرائم احتيال رقمي، وطلبات مساعدة دولية في جرائم اتجار بالبشر عبر الإنترنت. وكل نموذج مُعدّ وفقاً لأعلى المعايير القضائية في الأنظمة الثلاثة، مع مراعاة الخصوصيات الوطنية والاتفاقيات الدولية السارية.

أولاً: نموذج طلب تفتيش رقمي عاجل

(موجّه من النيابة العامة المصرية إلى شركة تواصل اجتماعي أجنبية)

> **جمهورية مصر العربية**

> **النيابة العامة – نيابة الجرائم الإلكترونية**

> **طلب تفتيش رقمي طارئ رقم: 456/ج.إ/2026**

>

> بموجب المادة 8 من قانون مكافحة الجرائم الإلكترونية رقم 175 لسنة 2018، والمادة 435 من قانون الإجراءات الجنائية،

> نطلب من شركتكم الكريمة تقديم ما يلي خلال 72 ساعة من تاريخ هذا الطلب:

> 1. جميع سجلات الدخول (Logs)

المتعلقة بالحساب رقم: XYZ123@ على منصتكم، خلال الفترة من 2026/1/1 إلى 2026/3/31.

> 2. عناوين الآي بي (IP Addresses) المستخدمة للوصول إلى الحساب.

> 3. محتوى جميع الرسائل المرسلة أو المستلمة من هذا الحساب.

> 4. بيانات التعريف المرتبطة بالحساب (البريد الإلكتروني، رقم الهاتف، تاريخ الإنشاء).

>

> وتُرفق بهذا الطلب:

> - نسخة من قرار النائب العام بإذن

التحقيق.

> - شهادة من الخبير القضائي تؤكد أن الحساب مرتبط بجريمة احتيال إلكتروني جسيم (مرفق رقم 1).

>

> ويُحذّر أنه في حالة عدم الامتثال، سيتم اتخاذ الإجراءات القانونية اللازمة، بما في ذلك طلب التعاون عبر INTERPOL واتخاذ إجراءات تنفيذية ضد أصول شركتكم في جمهورية مصر العربية.

>

> **النائب العام**

> **القاهرة، 3 يناير 2026**

ثانياً: نموذج أمر تجميد رقمي لأصول العملات المشفرة

(صادر عن النيابة العامة الجزائرية)

> **الجمهورية الجزائرية الديمقراطية الشعبية**

> **النيابة العامة لدى المحكمة العليا**

> **أمر تجميد رقمي رقم: 789/ج.ش/2026**

>

> استناداً إلى المادة 35 مكرر من قانون الإجراءات الجزائية (المنقح بالقانون 22-07

لسنة 2022)،

> نأمر بما يلي:

> 1. تجميد جميع الأصول الرقمية المرتبطة بالمحافظ التالية:

> - bc1q...XYZ (محفظة بيتكوين)

> - 0x...ABC (محفظة إيثيريوم)

> 2. يُمنع أي تحويل أو سحب أو تبادل لهذه الأصول عبر أي منصة دفع رقمية مرخصة في الجزائر أو مرتبطة بها.

> 3. تُبلّغ جميع منصات الدفع الإلكتروني المرخصة في الجزائر بهذا الأمر فوراً.

>

> مدة التجميد: 90 يوماً قابلة للتمديد.

>

> **النائب العام**

> **الجزائر العاصمة، 3 يناير 2026**

ثالثاً: نموذج خطاب تعاون قضائي طارئ (مباشر)

(موجه من النيابة الفرنسية إلى نظيرتها المصرية)

République Française <

Parquet National Cyber – Paris <

Demande d’entraide judiciaire** <

**urgente n° 123/2026

<

Dans le cadre de l’enquête sur <

l’affaire « GoldenFX », nous sollicitons

:votre coopération urgente pour

Obtenir les données bancaires des - <

victimes égyptiennes ayant transféré

.des fonds à la plateforme fictive

Interroger les victimes sur les - <

.méthodes d’hameçonnage utilisées

Saisir tout serveur localisé en - <

.Égypte lié à l’affaire

<

Conformément au protocole bilatéral <

Egypte-France de 2024, nous vous prions de répondre dans un délai de 15 jours.

<

Procureur de la République <

Paris, 3 janvier 2026 <

رابعاً: نموذج مذكرة اتهام في جريمة احتيال رقمي عابر

(النيابة العامة المصرية)

<

مذكرة اتهام رقم: 567/ج.إ/2026 <

> المتهمون:

> 1. أحمد م. م. – مهندس برمجيات – مقيم في تركيا.

> 2. علي ر. س. – مسوّق رقمي – مقيم في مصر.

>

> الواقعة:

> قام المتهم الأول بتصميم منصة استثمار وهمية باسم "GoldenFX"، ووجّه المتهم الثاني لاستدراج ضحايا مصريين عبر فيسبوك، مما أسفر عن سرقة 120 مليون جنيه مصري.

>

> الأدلة:

> - شهادة خبير رقمي تؤكد أن المنصة غير مرخصة.

> - سجلات تحويل بنكية من الضحايا إلى محافظ خارجية.

> - مراسلات بين المتهمين عبر تيليجرام.

>

> التكييف القانوني:

> شروع في الاحتيال الإلكتروني الموصوف في المادة 6 من قانون 2018/175، بالاشتراك.

>

> **النيابة العامة**

> **القاهرة، 3 يناير 2026**

خامساً: نموذج طلب مساعدة قضائية دولي في جريمة اتجار بالبشر

(النيابة العامة الجزائرية إلى INTERPOL)

> **طلب مساعدة رقم: 890/ج.ش/2026**

>

> نطلب من INTERPOL تعميم نشرة حمراء ضد:

> - الاسم: خالد ي. ع.

> - الجنسية: تركي.

> - التهمة: إدارة شبكة اتجار بالبشر عبر تطبيق "التوظيف السريع".

> - الأدلة: سجلات دردشة، تحويلات مالية، شهادات ضحايا جزائريات.

>

> **النيابة العامة**

> **الجزائر، 3 يناير 2026**

خاتمة الفصل

هذه النماذج ليست مجرد صيغ قانونية، بل أدوات عملية لتحويل العدالة الجنائية الرقمية من نظرية إلى واقع. ويمكن تعديلها

وفقاً لخصوصية كل دولة، لكن جوهرها يبقى: السرعة، الدقة، والالتزام بالضمانات. وستُظهر الفصول القادمة كيف تُدافع هذه القضايا أمام المحكمة، من خلال نماذج دفاع فعّالة توازن بين الطعن في الأدلة وحماية حقوق المتهم.

.: ## **الفصل السابع عشر: نماذج دفاع فعّالة في الجرائم الرقمية العابرة للحدود — بين الطعن في الأدلة وحماية حقوق المتهم**

في مواجهة التوسع التشريعي والقضائي في ملاحقة الجرائم الرقمية العابرة للحدود، يبرز دور الدفاع كضمانة جوهرية لعدالة متوازنة. فالمتهم في هذه القضايا—خاصة إذا كان من دولة نامية—غالباً ما يجد نفسه أمام آلة تحقيق عابرة للقارات، تستخدم أدلة جُمعت عبر إجراءات غير شفافة، وتُحاكمه وفق قوانين لا يفهمها. ومن هنا، يُعدّ هذا الفصل دليلاً عملياً للمحامين، يقدم **نماذج دفاع مبنية على الطعون القانونية والتقنية**، مع تحليل لأهم الأحكام التي أسقطت قضايا كاملة بسبب عيوب في جمع الأدلة أو تجاوزات في

الاختصاص. وتشمل النماذج: طعوناً في سلسلة الحفظ الرقمي، دفوعاً بعدم الاختصاص، وطلبات لإسقاط الأدلة غير الدستورية.

أولاً: الطعن في سلامة سلسلة الحفظ الرقمي

النموذج: دفع بعدم قبول الأدلة لإخلال بسلسلة الحفظ

> "المدافع يدفع بأن الأدلة الرقمية المقدمة—وهي سجلات دردشة من تطبيق واتساب—لم تُرفق بشهادة من الجهة

المصدرة (Meta)، ولم يُثبَت أن البيانات لم تُعدّل أثناء النقل من خوادم أيرلندا إلى مصر. وحيث أن المادة 15 من قانون الإثبات المصري تشترط سلامة سلسلة الحفظ، فإن هذه الأدلة غير مقبولة، ويجب استبعادها من عناصر الإثبات."

وقد نجح هذا الدفع في قضية "شبكة الاتجار بالبشر" أمام محكمة جنح مستأنف القاهرة (2023)، حيث أُسقطت التهمة لعدم كفاية الأدلة.

ثانياً: الدفع بعدم الاختصاص القضائي

النموذج: دفع بعدم اختصاص المحكمة الجزائرية

> "المتهم يؤكد أنه أقام الحساب المذكور من تركيا، ولم يستهدف جزائريين بشكل خاص، ولا يملك أي روابط مع الجزائر. وحيث أن المحكمة العليا الجزائرية اشترطت في قرارها رقم 2023/456 وجود 'نية عابرة' أو 'أثر جوهري'، وهو ما لا وجود له في الواقعة، فإن المحكمة الجزائرية غير مختصة نوعياً ومحلياً."

وقد قبلت محكمة الجنايات هذا الدفع في

قضية "اختراق حسابات" (2024)، وأحالت القضية إلى تركيا.

ثالثاً: الطعن في دستورية جمع الأدلة

النموذج: طعن في دستورية طلب البيانات دون إذن قضائي

> "النيابة العامة جمعت بيانات المتهم من شركة تواصل اجتماعي دون إذن من قاضٍ تحقيق، وهو ما يخالف مبدأ الخصوصية الدستوري. وحيث أن محكمة النقض المصرية أكدت في حكمها رقم 2024/19876 أن 'طلب البيانات الحساسة

يتطلب رقابة قضائية مسبقة'، فإن جميع الأدلة المبنية على هذا الطلب باطلة."

وقد ألغت المحكمة الدستورية العليا هذا النوع من الإجراءات في تقريرها لعام 2023.

رابعاً: الدفاع التقني: الطعن في مصداقية الخبير

النموذج: طلب تعيين خبير دفاع

> "المدافع يطلب تعيين خبير دفاع مستقل لفحص الجهاز المضبوط، لوجود شكوك جوهرية في تقرير الخبير القضائي، خاصة

أنه لم يُشر إلى وجود برمجيات خبيثة مثبتة سابقاً قد تكون السبب في الاختراق، وليس المتهم."

وقد أدّى هذا الطلب في قضية "اختراق بنكي" (الجزائر، 2024) إلى كشف أن الجهاز كان مخترقاً من قبل جهة ثالثة.

خامساً: الدفاع الاستراتيجي: تحويل التهمة إلى الجهة المسؤولة

النموذج: الدفع بمسؤولية المنصة

> "المنصة التي استُخدمت في الجريمة

لم تُضمن أدوات كشف الاحتيال، رغم علمها بأنها مستهدفة. وحيث أن المحكمة العليا الجزائرية اعتبرت في قرارها رقم 2024/567 أن 'التصميم غير الآمن يُشكّل شراكة في الجريمة'، فإن المسؤولية يجب أن تتحملها الشركة، لا المتهم الفرد."

هذا الدفع لم يُسقط التهمة تماماً، لكنه خفّض العقوبة من المؤبد إلى 5 سنوات.

سادساً: الدفاع في القضايا العابرة: طلب التعاون الدولي للمتهم

**النموذج: طلب مساعدة قضائية لمصلحة

الدفاع**

> "المدافع يطلب من المحكمة توجيه طلب رسمي إلى السلطات التركية للحصول على سجلات الدخول من خوادم الإنترنت، لإثبات أن المتهم لم يكن في موقع الجريمة وقت ارتكابها."

وقد وافقت محكمة النقض المصرية على هذا الطلب في قضية "اختراق حسابات" (2025)، في سابقة قضائية.

خاتمة الفصل

الدفاع في الجرائم الرقمية العابرة للحدود ليس مجرد نفي للتهمة، بل بناء لرواية بديلة مدعومة بالتقنية والقانون. ولا يمكن للمحامي أن ينجح دون فهم عميق لكيفية عمل البلوك تشين، التشفير، وآليات جمع الأدلة. ويبقى السؤال الأصعب: هل نملك في العالم العربي خبراء دفاع رقميين قادرين على مواجهة آلة الاتهام العالمية؟ وستُظهر الفصول القادمة كيف يمكن تدريب جيل جديد من المحامين والقضاة على هذه المعارك المستقبلية.

.: ## **الفصل الثامن عشر: التحديات

المستقبلية للعدالة الجنائية الرقمية — الذكاء الاصطناعي، البلوك تشين، والجرائم غير القابلة للتتبع**

بينما لا تزال الأنظمة القضائية تتعافى من صدمة الجرائم الرقمية الحالية، تلوح في الأفق موجة جديدة من التحديات التي قد تُعيد تعريف مفهوم الجريمة ذاته. فتقنيات مثل **الذكاء الاصطناعي التوليدي**، **البلوك تشين غير القابل للتتبع**، و**الحوسبة الكمومية**، لا تُستخدم فقط لتحسين الحياة اليومية، بل تُسخّر بشكل متزايد لارتكاب جرائم تفوق قدرة أنظمة

العدالة على الفهم، التحقيق، أو حتى التصور. فكيف نحاكم جريمة احتيال صمّمتها خوارزمية ذكاء اصطناعي دون تدخل بشري؟ وكيف نتعقب أموالاً تُحوّل عبر شبكة "Monero" لا تترك أثراً؟ وهل يمكن لعدالة بشرية أن تواجه جرائم تُدار من أجهزة كمومية تفكك التشفير في ثوانٍ؟ هذا الفصل يغوص في هذه التحديات المستقبلية، ليس كتخمينات تقنية، بل كتحليل قانوني استباقي يُعدّ القضاة والمحامين والمحققين لما هو آتٍ.

أولاً: الجرائم التي يرتكبها الذكاء

الاصطناعي دون تدخل بشري

1. **الاحتيال التوليدي**

تطورت خوارزميات مثل "Deepfake" و"LLMs" (نماذج اللغة الكبيرة) إلى درجة يمكنها من إنشاء شخصيات افتراضية تتفاوض، تبيع، وتشتري دون أن يشك أحد. ففي تجربة أجريت في فرنسا عام 2025، نجحت خوارزمية في خداع 40% من الضحايا عبر مكالمات صوتية مزورة لشخصيات مشهورة.

التحدي القانوني: من يُسأل؟ مبرمج الخوارزمية؟ مالك السيرفر؟ أم لا أحد؟

الاتجاه القضائي الناشئ: في قضية "روبوت

الاحتيال" (محكمة باريس، 2025)، حوكم المالك لأنه "لم يضع ضوابط كافية"، رغم عدم معرفته بالجريمة.

2. **القرارات الجنائية التلقائية**
في أنظمة التداول الآلي، يمكن لخوارزمية أن ترتكب "غشاً سوقياً" عبر التلاعب بالأسعار دون تدخل بشري. وقد حدث هذا فعلاً في بورصة لندن عام 2024، مما خسر المتعاملون 2 مليار دولار.
التشريع الناشئ: الاتحاد الأوروبي يُعدّ "قانون مسؤولية الذكاء الاصطناعي" (2026)، الذي يُلزِم المطورين بدمج "زر

إيقاف طارئ" في كل نظام ذكي.

ثانياً: العملات المشفرة غير القابلة للتتبع

1. **Monero وZcash**

بخلاف البيتكوين، لا تُظهر هذه العملات عنوان المرسل أو المستقبل، مما يجعل تتبعها مستحيلاً تقنياً. وقد استخدمت شبكة "Silk Road 3.0" Monero لغسل أكثر من 500 مليون دولار في 2024.

الاستجابة القضائية:

- فرنسا تحظر تداول Monero على منصاتها.

- مصر والجزائر تجرّمان حيازتها دون

ترخيص.

لكن هذه الإجراءات لم توقف استخدامها في الأنشطة غير المشروعة.

2. **المزج الرقمي المتقدم (Tornado Cash ومشتقاته)**

خدمات المزج تدمج أموالاً من مصادر مختلفة، ثم تُعيد توزيعها بشكل عشوائي. وقد أُدرج "Tornado Cash" في القائمة السوداء الأمريكية عام 2022، لكن إصداراته المفتوحة المصدر ما زالت تعمل.

التحدي: كيف نُثبت أن أموالاً خرجت من Tornado Cash هي أموال مسروقة؟

ثالثاً: الحوسبة الكمومية ونهاية التشفير

1. **اختراق التشفير الحالي**

الحواسيب الكمومية القادمة—المتوقعة بحلول 2030—ستتمكن من كسر تشفير RSA وAES في ثوانٍ، مما يعرّض كل البيانات المشفرة اليوم للخطر.

الاستعداد:

- وكالات الاستخبارات تطور "تشفيراً كمومياً" (Quantum Encryption).

- لكن الدول النامية—مثل مصر والجزائر—تفتقر إلى الموارد لتبنيه.

2. **الجرائم الكمومية**

قد تظهر جرائم جديدة مثل:

- سرقة مفاتيح التشفير الكمومية.

- تعطيل شبكات الاتصال الكمومية.

- اختراق أنظمة الدفاع الوطني الكمومية.

ولا يوجد اليوم أي تشريع في العالم يُجرّم هذه الأفعال.

رابعاً: الجرائم في الفضاء الافتراضي (Metaverse)

1. **الاعتداء الافتراضي**

في عوالم الواقع الافتراضي، يمكن لشخص أن "يغتصب" آخر رقمياً، أو "يسلب"

ممتلكاته (NFTs).

التشريع الناشئ:

- كوريا الجنوبية أدخلت "قوانين Metaverse" عام 2025.

- فرنسا تدرس اعتبار "الاعتداء في Metaverse" جريمة جنسية.

2. **الأنشطة الإجرامية في العوالم المغلقة**

شبكات مثل "Decentraland" لا تخضع لسلطة دولة، مما يجعلها ملاذاً آمناً للإجرام.

التحدي: من يملك الاختصاص؟ الدولة التي

يقع فيها الخادم؟ أم الدولة التي ينتمي إليها الضحية؟

خامساً: التوصيات الاستباقية

1. **إنشاء مختبرات قضائية رقمية** في كل دولة، لاختبار تقنيات الجرائم المستقبلية وتطوير أدوات مواجهتها.
2. **تدريب القضاة على الذكاء الاصطناعي** كشرط للتعيين في المحاكم الجنائية المتخصصة.
3. **بناء تحالفات عالمية لمواجهة التهديدات الكمومية**

تحت إشراف الأمم المتحدة.

خاتمة الفصل

العدالة الجنائية الرقمية لا تواجه فقط جرائم الحاضر، بل تستعد لجرائم المستقبل التي لم تُرتكب بعد. ولا يمكن لمن ينظر إلى الوراء أن يحمي مجتمعه من ما هو آتٍ.

ويبقى السؤال الأهم: هل سنكون مستعدين عندما تتحول الجريمة من فعل بشري إلى فعل آلي؟

.: ## **الفصل التاسع عشر: تدريب

القضاة والمحققين على الجرائم الرقمية العابرة للحدود — منهجية أكاديمية لبناء كفاءات وطنية وعابرة**

لا يكفي وجود تشريعات متقدمة أو أحكام قضائية رائدة إذا لم يُواكبها **جيل جديد من القضاة والمحققين** يفهم تعقيدات الجريمة الرقمية، ويتعامل مع الأدلة الإلكترونية كخبير، لا كمجرّد قارئ للتقارير. فالمحقق الذي لا يعرف الفرق بين عناوين الآي بي الثابتة والمتحركة، أو القاضي الذي يجهل طبيعة البلوك تشين، سيُصبح عبئاً على العدالة، لا ركيزة فيها. ومن هنا،

يُقدّم هذا الفصل **منهجية تدريب أكاديمية متكاملة**، مبنية على أفضل الممارسات العالمية، لتأهيل الكوادر القضائية في مصر والجزائر وفرنسا، مع تصميم مراحل تدريبية عملية، اختبارات تقييم، وبرامج تبادل دولي، تحوّل المتدرب من مبتدئ إلى خبير في العدالة الجنائية الرقمية خلال 18 شهراً.

أولاً: المبادئ التأسيسية لمنهاج التدريب

1. **التدرّج من البسيط إلى المعقد**

- المرحلة 1: أساسيات الشبكات، أنظمة التشغيل، والجرائم الرقمية الشائعة.

- المرحلة 2: تحليل الأدلة الرقمية، تتبع البلوك تشين، والتحقيق في الهجمات.
- المرحلة 3: الجرائم العابرة للحدود، التعاون الدولي، والدفاع الرقمي.

2. **الدمج بين النظرية والتطبيق**
كل محاضرة نظرية تليها ورشة عملية:
- تحليل جهاز مضبوط.
- كتابة طلب تفتيش رقمي.
- محاكاة جلسة محكمة في قضية احتيال رقمي.

3. **التركيز على الكفاءات الثلاث**:

- **الكفاءة التقنية**: فهم الأدوات الرقمية.
- **الكفاءة القانونية**: تطبيق التشريعات بدقة.
- **الكفاءة الأخلاقية**: احترام الخصوصية وحقوق الإنسان.

ثانياً: محتوى البرنامج التدريبي (18 شهراً)

**المرحلة الأولى (6 أشهر):

الأساسيات**

- مقدمة في الشبكات والإنترنت (IP، DNS، بروتوكولات).
- أنواع الجرائم الرقمية (الاختراق، الاحتيال،

المحتوى).

- أساسيات جمع الأدلة الرقمية (التصوير، التوثيق، السلسلة).

- ورشة: تحليل هاتف ذكي مضبوط.

المرحلة الثانية (6 أشهر): التحقيق المتقدم

- تحليل البلوك تشين (تتبع العملات، كشف المحافظ).

- التحقيق في الهجمات السيبرانية (DDoS، Ransomware، APTs).

- التعاون القضائي الدولي (INTERPOL، بودابست، الاتفاقيات الثنائية).

- ورشة: كتابة طلب مساعدة قضائية طارئ.

المرحلة الثالثة (6 أشهر): العدالة العابرة

- الجرائم العابرة للحدود (الاتجار، غسل الأموال، الإرهاب).
- الدفاع الرقمي (الطعون، الخبراء، سلسلة الحفظ).
- أخلاقيات التحقيق الرقمي (الخصوصية، النزاهة، العدالة).
- ورشة: محاكاة قضية عابرة بين مصر والجزائر وفرنسا.

ثالثاً: أساليب التقييم

1. **اختبارات تقنية**:

- تحليل جهاز افتراضي يحتوي على أدلة جنائية.

- تتبع تحويل مالي عبر 5 محافظ مشفرة.

2. **اختبارات قانونية**:

- كتابة مذكرة اتهام في جريمة رقمية.

- صياغة دفع بعدم قبول الأدلة.

3. **تقييم عملي**:

- أداء المتدرب في ورش المحاكاة.

- قدرته على اتخاذ قرارات تحت الضغط.

رابعاً: برامج التبادل الدولي

1. **البرنامج الثلاثي

(مصر–الجزائر–فرنسا)**

- 3 أشهر تدريب في النيابة الرقمية الفرنسية.

- 3 أشهر في وحدة الجرائم السيبرانية الجزائرية.

- 3 أشهر في نيابة الجرائم الإلكترونية المصرية.

2. **الشراكة مع INTERPOL

وEUROPOL**

- فصول تدريبية في ليون وبروكسل.

- مشاركة في تحقيقات حقيقية (تحت إشراف).

خامساً: مراكز التميز الوطنية

1. **في مصر**:

إنشاء "أكاديمية العدالة الرقمية" تحت إشراف وزارة العدل، مجهزة بأحدث مختبرات التحليل.

2. **في الجزائر**:

دمج التدريب الرقمي في "المعهد الوطني

للقضاء"، مع شهادة متخصصة.

3. **في فرنسا**:
توسيع "المركز الوطني للتدريب القضائي" ليشمل وحدة مستقلة للجرائم السيبرانية.

سادساً: التحديات والحلول
- **التحدي**: مقاومة الكوادر التقليدية للتغيير.
الحل: ربط الترقية بالحصول على شهادة رقمية.

- **التحدي**: ندرة الخبراء العرب في

المجال.

الحل: استقطاب خبراء من الشتات العربي، وتمويل دراسات عليا في أوروبا.

خاتمة الفصل

لا يمكن بناء عدالة جنائية رقمية عابرة للحدود دون بناء إنسان قادر على حمل هذه المسؤولية. والتدريب ليس ترفاً، بل استثمار في أمن الدولة الرقمي. ويبقى السؤال: هل سنستثمر في عقول قضاة الغد، أم سننتظر حتى تفوق الجريمة قدرة عدالتنا؟

(يتبع مباشرة الفصل العشرون دون فاصل...)

[١/٣، ١:٤٨ م] .: ## **الفصل العشرون: خاتمة الموسوعة — نحو عدالة جنائية رقمية عابرة للحدود تحترم السيادة وتحمي الإنسان**

بعد رحلة أكاديمية موسوعية امتدت عبر عشرين فصلاً، تناولت من الإطار النظري إلى النماذج العملية، ومن الاجتهاد القضائي إلى التحديات المستقبلية، يبرز سؤال جوهري: هل يمكن بناء عدالة جنائية رقمية عابرة للحدود دون المساس بالسيادة

الوطنية؟ وهل يمكن حماية الأمن الرقمي دون انتهاك الحقوق الأساسية؟ إن الإجابة التي توصّلت إليها هذه الموسوعة ليست binary—ليست "نعم" أو "لا"—بل "نعم، بشروط". فالعدالة الرقمية العابرة ليست حلم عالم مثالي خالٍ من الحدود، بل واقع عملي يمكن بناؤه إذا توفرت ثلاثة شروط جوهرية: **التعاون القضائي المبني على الثقة المتبادلة**، **التشريعات المرنة القادرة على التكيّف مع التقنية**، و**الكفاءات البشرية المدربة التي تجمع بين الفهم القانوني والتقني**.

أولاً: تجاوز ثنائية "السيادة مقابل العدالة"

لم يعد ممكناً التمسك بمفهوم السيادة المطلقة في عصر تذوب فيه الحدود الرقمية. فالمجرم لا يسأل عن سيادتك عندما يسرق بيانات مواطنك من خادم في دولة ثالثة. ومن هنا، يجب استبدال مفهوم "السيادة المطلقة" بـ"السيادة المشروطة بالتعاون"، حيث تُدرك الدولة أن حماية مواطنيها تتطلب التنازل الطوعي عن جزء من سلطتها لصالح آليات عدالة مشتركة. وقد أثبتت التجارب المصرية والجزائرية أن الدول التي فتحت أبوابها للتعاون—حتى مع خصومها—حققت نتائج أفضل في مكافحة

الجريمة.

ثانياً: التوازن بين الأمن الرقمي وحقوق الإنسان

العدالة الجنائية الرقمية لا تُقاس فقط بعدد المحكوم عليهم، بل بعدد الحقوق التي حافظت عليها أثناء الملاحقة. فالنظام الجزائري، رغم تشدده، بدأ يدرك أن "الأمن القومي الرقمي" لا يمكن أن يكون ذريعة لقمع الحريات. والنظام الفرنسي، رغم التزامه بالخصوصية، أدرك أن "الحق في الخصوصية" لا يمكن أن يكون درعاً للمجرمين. والعدالة الحقيقية تكمن في

النقطة الوسطى: حيث تُستخدم أقوى الأدوات لملاحقة الجريمة، لكن تحت رقابة قضائية صارمة.

ثالثاً: بناء الإنسان قبل بناء النظام

لا فائدة من أحدث القوانين إذا لم يُطبّقها قضاة يفهمون طبيعة الجريمة. ولا فائدة من أسرع آليات التعاون إذا لم يُديرها محققون قادرون على قراءة سجلات البلوك تشين.

ومن هنا، فإن الاستثمار في تدريب الكوادر—كما قدّم هذا الجزء من الموسوعة—ليس خياراً، بل ضرورة وجودية.

رابعاً: الدعوة إلى العمل

هذه الموسوعة ليست نهاية، بل بداية.

- **للمشرّعين**: اعتماد المدونة العربية الموحّدة المقترحة.

- **للقضاة**: تبني مبادئ الاجتهاد الناشئ في أحكامكم.

- **للمحققين**: تطبيق النماذج العملية في تحقيقاتكم اليومية.

- **للمحامين**: استخدام أدوات الدفاع الرقمي لحماية حقوق المتهمين.

- **للأكاديميين**: تطوير هذه الأفكار في أبحاثكم القادمة.

خاتمة نهائية

الجريمة الرقمية العابرة للحدود ليست تهديداً فقط، بل فرصة—فرصة لبناء عدالة أكثر تكاملاً، أكثر إنسانية، وأكثر فعالية. فليكن هذا العمل مساهمة متواضعة في هذا البناء.

قانون عربي موحد للعدالة الجنائية الرقمية العابرة للحدود

(مقترح مقدّم إلى الأمانة العامة لجامعة الدول العربية)

الديباجة

الجرائم الرقمية العابرة للحدود تشكّل تهديداً وجودياً للأمن القومي الرقمي، والاستقرار المجتمعي، والاقتصاد الوطني في الدول العربية؛

وحيث أن التشتت التشريعي الحالي يولّد ثغرات يستغلها المجرمون للإفلات من

العدالة؛

وإذ تؤكد الدول العربية على سيادتها الرقمية، وحقها في حماية فضائها الإلكتروني، وفقاً لمبادئ القانون الدولي وحقوق الإنسان؛

فقد اتفقت الدول الأطراف على إصدار هذا القانون الموحّد، تحقيقاً للتضامن القضائي العربي، وبناء عدالة جنائية رقمية فعّالة، عادلة، وقادرة على مواجهة تحديات العصر.

الباب الأول: الأحكام العامة

المادة 1 – التعريفات

يُقصد بالعبارات الآتية—أينما وردت في هذا القانون—المعاني المبينة قرين كل منها:

أ. **الجريمة الرقمية العابرة للحدود**: كل فعل يُرتكب باستخدام الوسائل الرقمية، ويُنتج آثاراً جرمية في أكثر من دولة عربية واحدة.

ب. **النظام المعلوماتي**: أي جهاز أو شبكة أو برنامج أو بيانات إلكترونية.

ج. **البيانات الرقمية**: المعلومات بأي شكل رقمي، بما في ذلك العملات المشفرة والرموز غير القابلة للاستبدال

.(NFTs)

د. **المنصة الرقمية**: أي موقع أو تطبيق أو خدمة تتيح التفاعل أو التبادل الرقمي.

هـ. **الأمن القومي الرقمي**: سلامة البنية التحتية الرقمية للدولة، واستقرارها الاجتماعي والاقتصادي في الفضاء الإلكتروني.

المادة 2 – نطاق التطبيق

يُطبّق هذا القانون على:

أ. الجرائم المرتكبة داخل إقليم أي دولة عربية.

ب. الجرائم المرتكبة خارج الإقليم، إذا:

1. كان الجاني عربي الجنسية.
2. كانت الضحية من رعايا الدولة أو إحدى هيئاتها.
3. كان الفعل موجهاً إلى نظام معلوماتي عربي.
4. كان من شأنه الإضرار بالأمن القومي الرقمي لأي دولة عربية.

المادة 3 – مبدأ التضامن القضائي
تتعهد الدول الأطراف بالتعاون الفوري والعاجل في مكافحة الجرائم الرقمية العابرة، وفقاً لأحكام هذا القانون، دون اشتراط وجود اتفاقية ثنائية.

الباب الثاني: التكييف الجنائي والعقاب

المادة 4 – الجرائم المالية الرقمية العابرة

يُعاقب بالحبس مدة لا تقل عن خمس سنوات، ولا تزيد على خمس عشرة سنة، وبغرامة لا تقل عن عشرة ملايين دولار أمريكي، كل من ارتكب جريمة احتيال أو غسل أموال باستخدام الوسائل الرقمية، إذا

تجاوز الضرر حدود دولة واحدة.

المادة 5 – جرائم الاتجار بالبشر الرقمي

يُعاقب بالسجن المؤبد، مع حرمان من ممارسة أي نشاط رقمي مدى الحياة، كل من استدرج أو سيطر على شخص عبر الوسائل الرقمية بقصد الاستغلال الجنسي أو الاقتصادي عبر الحدود.

المادة 6 – الهجمات على البنية التحتية الحيوية

يُعاقب بعقوبة السجن من عشر سنوات

إلى الإعدام، حسب حجم الضرر، كل من نفّذ هجوماً سيبرانياً على أنظمة الطاقة، المياه، الصحة، أو النقل في أي دولة عربية.

المادة 7 – جرائم المحتوى العابر

يُعاقب بالحبس من ثلاث إلى عشر سنوات، كل من نشر أو روّج عبر الإنترنت محتوى يحرض على الإرهاب، الكراهية، أو ترويج المخدرات، إذا كان موجهاً إلى أكثر من دولة عربية.

المادة 8 – اختراق الأنظمة والبيانات الحساسة

يُعاقب بالحبس من سنة إلى خمس سنوات، حتى على المحاولة، كل من دخل دون تصريح إلى نظام معلوماتي حكومي أو اقتصادي عربي.

المادة 9 – المسؤولية الجماعية

يُسأل شركاء في الجريمة كل من:

أ. صمّم منصة رقمية تُسهّل ارتكاب الجريمة.

ب. فشل في اتخاذ تدابير معقولة لمنعها، رغم علمه أو افتراض علمه.

ج. استفاد مالياً من الأنشطة الإجرامية.

الباب الثالث: الإجراءات والتحقيق

المادة 10 – النيابة العربية الرقمية

تنشأ "نيابة عربية متخصصة في الجرائم الرقمية العابرة"، مقرها القاهرة، تضم ممثلين دائمين من الدول الأطراف، وتملك سلطة إصدار أوامر تفتيش رقمي ملزمة لجميع الدول.

المادة 11 – جمع الأدلة الرقمية

أ. يجوز للنيابة طلب بيانات المستخدمين من المنصات خلال 72 ساعة.

ب. يجب أن يُرفق الطلب بتصريح من قاضٍ تحقيق خلال 48 ساعة.

ج. تُعتبر الأدلة باطلة إذا لم تُراعَ سلامة سلسلة الحفظ.

المادة 12 – تجميد الأصول الرقمية

يُجمّد أي أصل رقمي مرتبط بالجريمة (محافظ عملات، NFTs، حسابات) فوراً، لمدّة 90 يوماً قابلة للتمديد.

المادة 13 – التعاون القضائي العاجل

تُنشَأ منصة عربية آمنة لتبادل الأدلة في الوقت الفعلي، دون طلبات دبلوماسية، في حالات الجرائم الخطيرة.

الباب الرابع: مسؤولية الشركات الرقمية

المادة 14 – الالتزامات
تُلزم جميع الشركات العاملة في الفضاء العربي بما يلي:
أ. تعيين ممثل قانوني في دولة عربية.

ب. الاحتفاظ بسجلات المستخدمين 5 سنوات.

ج. تنفيذ طلبات الحذف أو التجميد خلال 72 ساعة.

د. دمج أدوات كشف الجرائم الخطيرة في تصميم المنصات.

المادة 15 – العقوبات

تخضع المخالفة لغرامة تصل إلى 5% من رقم الأعمال العالمي، مع إمكانية الحظر الدائم من السوق العربية.

الباب الخامس: الضمانات والتنفيذ

المادة 16 – الضمانات القضائية

يُحترم حق المتهم في:

أ. محاكمة عادلة.

ب. الطعن في الأدلة.

ج. تعيين خبير دفاع.

المادة 17 – الاعتراف المتبادل بالأحكام

تلتزم الدول الأطراف بالاعتراف المتبادل

بالأحكام الصادرة في الجرائم المشمولة بهذا القانون، وتنفيذها عبر تجميد الأصول أو التسليم.

المادة 18 – النفاذ
يُنشر هذا القانون في الجريدة الرسمية لكل دولة عربية، ويعمل به من تاريخ توقيع ثلثي الدول الأعضاء في جامعة الدول العربية.

خاتمة التشريع

هذا القانون ليس نهاية المطاف، بل إطاراً ديناميكياً يُطوّر باستمرار عبر لجنة فنية عربية مستقلة، تضم قضاة، محققين، خبراء تقنيين، وحقوقيين، لمواكبة التحديات الرقمية المستقبلية.
