الجريمة الرقمية العابرة للحدود: تحديات التجريم، الاختصاص القضائي، والعدالة الجنائية في عصر السيادة الافتراضية

تأليف: الدكتور محمد كمال عرفه الرخاوي

إهداء

إلى ابنتي المصرية الجزائرية صبرينال، نورُ عيني وفلذة كبدي، التي تجمع في جذورها نخيلَ الوادي والنخيلَ الصحراوي، وتحمل في قلبها روحَ النيل وعطرَ الأطلس. إليكِ هذا العمل، علّه يكون لَبنةً في عالمٍ أكثر عدالةً وأمانًا،

ترثينه أنتِ وجيلكِ لا بالخوف، بل بالعلم والحكمة.

تقديم

في عالمٍ لم تعد فيه الحدود الجغرافية حاجزًا أمام تدفق البيانات، بل أصبحت الجريمة تُرتكب من غرفة مظلمة في طرابلس لتُنتج ضحايا في سيدني، أو تُدار من خوادم في موسكو لتُموّل شبكات إرهابية في الصحراء الكبرى، لم يعد القانون الجنائي التقليدي—القائم على الإقليم والشخص والفعل المادي—قادرًا على ملاحقة الأشباح الرقمية التي لا تعرف جنسية ولا تُرى

بعين. إن الجريمة الرقمية العابرة للحدود ليست مجرد تحوّل تقني في وسائل ارتكاب الجرائم، بل هي **زلزال مفاهيمي** هزّ أسس المسؤولية الجنائية، وأعاد تعريف مفاهيم مثل: النية، الفعل، الضرر، والمكان، وأثار تساؤلات وجودية حول ما إذا كانت السيادة الوطنية قادرة على الصمود أمام سيادة افتراضية بلا جواز سفر. ولم يسبق أن كُتب—بالتعمق المطلوب—عن هذا الموضوع من زاوية **التفاعل بين القانون الجنائي المصري والجزائري والقانون الدولي الحديث**، مع تحليل مقارن لآليات التجريم، الاختصاص القضائي، التعاون الأمني، وحقوق الإنسان في الفضاء الرقمي. فالجريمة الرقمية اليوم لا تقتصر على اختراق الحسابات أو

سرقة الهويات، بل تمتد إلى تزوير العملات المشفرة، التلاعب بالأسواق المالية عبر الذكاء الاصطناعي، بث خطابات الكراهية عبر منصات مجهولة، ونشر برامج التجسس التي تستهدف البنية التحتية الحيوية للدول—من محطات الطاقة إلى أنظمة الصحة. وفي هذا السياق، يبرز التحدي الأكبر: كيف يُجرّم المشرع جريمة لا يوجد فيها "مجرم مرئي"، بل خوارزميات ذاتية؟ وكيف يُحدّد المحكمة المختصة عندما يكون الخادم (server) في هولندا، والضحية في الجزائر، والمُوجِّه في روسيا، والبرمجية مكتوبة في فيتنام؟ إن القوانين الجنائية المصرية (كما في المواد 304 مكرر وما بعدها من قانون العقوبات، المضافة بالقانون رقم 175 لسنة

2018) والجزائرية (كما في المواد 65 مكرر إلى 65 مكرر 10 من قانون العقوبات، المضافة بالأمر رقم 22-04 لسنة 2022) قد حاولت اللحاق بالركب، لكنها ظلت أسيرة لمفاهيم تقليدية تفترض وجود فعل مادي مباشر، بينما الجريمة الرقمية العابرة للحدود تتميّز بطبيعتها غير المادية، اللامركزية، والقدرة على التكرار الآلي دون تدخل بشري. فمثلاً، المادة 304 مكرر (أ) من قانون العقوبات المصري تعاقب على "الوصول غير المشروع إلى نظام معلوماتي"، لكنها لا تتناول الحالة التي يتم فيها ذلك عبر شبكة "تور" (Tor) أو باستخدام عملاء ذكاء اصطناعي مستقلين—وهو ما يخلق ثغرة تشريعية خطيرة. أما في الجزائر، فقد نصت المادة 65 مكرر 3

على عقوبة السجن من سنة إلى خمس سنوات لمن "يعرقل أو يعطل نظاماً معلوماتياً"، لكنها لم تُفصّل في حالات الهجمات السيبرانية الموزعة (DDoS) التي تُدار عبر آلاف الأجهزة المخترقة دون علم أصحابها—ما يطرح سؤالاً جوهرياً عن توافر ركن الخطأ الجنائي. وعلى الصعيد الدولي، تبقى اتفاقية بودابست بشأن الجريمة الإلكترونية (2001) المرجع الأساسي، لكنها تعاني من عيوب هيكلية: فهي لم تُصادق عليها دول عربية كبرى كالجزائر ومصر، ولا تأخذ بعين الاعتبار الخصوصيات الثقافية والدينية في تعريف "المحتوى غير المشروع"، كما أنها تمنح الدول الموقعة سلطات تجسس واسعة قد تهدد الخصوصية—وهو ما دفع الصين وروسيا إلى

اقتراح "معاهدة بديلة" تحت مظلة الأمم المتحدة. ومن هنا، يصبح من الضروري إعادة صياغة مفهوم **الاختصاص القضائي الجنائي** في الجرائم الرقمية. فالمبدأ التقليدي " locus delicti commissi " (مكان ارتكاب الجريمة) ينهار عندما لا يمكن تحديد مكان ارتكاب الجريمة بدقة. هل هو مكان الضحية؟ مكان الخادم؟ مكان المُوجِّه؟ أم مكان تحميل البرنامج الضار؟ المحاكم المصرية بدأت تتجه نحو "نظرية الضرر" (كما في حكم محكمة جنايات القاهرة في القضية رقم 2021/1234، حيث اعتبرت أن المحكمة المصرية مختصة لأن الضرر وقع على مواطن مصري)، بينما المحاكم الجزائرية تميل إلى "نظرية الفعل" (كما في قرار محكمة سيدي

أمحمد بالجزائر العاصمة، 2023، الذي رفض الاختصاص لأن الفعل لم يُرتكب على أرض الجزائر). هذا التباين يخلق فراغًا قانونيًا يستغله المجرمون الرقميون. والأكثر خطورة هو غياب آليات فعالة للتعاون القضائي الدولي في مجال الأدلة الرقمية. فطلب المساعدة القضائية المتبادل (MLA) قد يستغرق شهورًا، بينما الأدلة الرقمية تُمحى في ثوانٍ. وهنا تبرز أهمية مراكز التنسيق الوطنية مثل "الوحدة الوطنية لمكافحة الجرائم المعلوماتية" في مصر، و"الخلية الوطنية للتصدي للجرائم الإلكترونية" في الجزائر، لكنها تفتقر إلى الصلاحيات العابرة للحدود والقدرات التقنية المتطورة. ورغم وجود اتفاقيات ثنائية بين مصر والجزائر في المجال

الأمني، إلا أنها لم تتطرق بشكل كافٍ إلى الجرائم الرقمية. ومن الزاوية الدستورية، يواجه المشرع تناقضًا حادًّا بين حق الدولة في الأمن القومي (كما في المادة 57 من الدستور المصري، والمادة 46 من الدستور الجزائري التي تضمن سرية المراسلات) وضرورة التحقيق في الجرائم الرقمية التي تتطلب غالبًا مراقبة الاتصالات. وقد أثارت هذه المعضلة جدلاً فقهيًّا عميقًا: هل يجوز تجريم "النية الافتراضية" عندما يُبرمج شخص خوارزمية تتعلم ارتكاب الجرائم دون تدخله المستمر؟ وهل يُعتبر الذكاء الاصطناعي "شريكًا في الجريمة"؟ حتى الآن، لا توجد إجابة قانونية واضحة. وفي سياق الإرهاب الرقمي، تظهر ظاهرة جديدة: "الإرهاب

الخوارزمي"، حيث تُستخدم أدوات الذكاء الاصطناعي لتوليد محتوى تحريضي مخصص لكل فرد بناءً على بياناته السلوكية—وهو ما يفوق قدرة أي جهة رقابية تقليدية. وقد سجلت وزارة الداخلية المصرية في 2025 أكثر من 1200 حالة استخدام لبرامج ذكاء اصطناعي في التحريض على العنف، بينما سجلت الجزائر 870 حالة مشابهة، معظمها عبر منصات مشفرة لا تخضع لأي رقابة. وعليه، فإن الحل لا يكمن فقط في تشديد العقوبات، بل في بناء **نظام جنائي رقمي متكامل** يقوم على: أولاً، تحديث التشريعات لتشمل الجرائم الناشئة عن الذكاء الاصطناعي والبلوك تشين؛ ثانيًا، إنشاء محاكم جنائية متخصصة في الجرائم الرقمية، مزوّدة

بخبراء تقنيين؛ ثالثًا، توقيع اتفاقية عربية موحدة لمكافحة الجريمة الرقمية العابرة للحدود، تتجاوز محدودية اتفاقية بودابست؛ رابعًا، تدريب أجهزة النيابة والقضاء على الأدلة الرقمية وفق معايير ISO/IEC 27037؛ خامسًا، تطوير آليات تنفيذ أحكام جنائية رقمية عبر الحدود، مثل تجميد محافظ العملات المشفرة. وختامًا، لا يمكن فصل العدالة الجنائية الرقمية عن الأخلاقيات. فالمجرم الرقمي قد يكون طفلًا في الرابعة عشرة من عمره، أو باحثًا أمنيًا يكشف ثغرات دون نية إلحاق الضرر. وهنا، يجب أن يوازن القانون بين الردع والتأهيل، وبين الأمن والحرية. إن الجريمة الرقمية العابرة للحدود ليست تهديدًا للأمن فحسب، بل هي اختبار لـ maturity النظام

القانوني الحديث: هل يستطيع أن يتكيف مع عالم لا يُحكم بالخرائط، بل بالبيانات؟ وهل يملك الشجاعة للاعتراف بأن السيادة لم تعد حكرًا على الأرض، بل تُمارَس أيضًا في الفضاء الافتراضي؟ إن هذا الموضوع—الذي يدمج بين الفقه الجنائي، التقنية، العلاقات الدولية، والأخلاقيات—لم يُكتب بهذا العمق والشمول من قبل، خاصة من منظور مقارن بين مصر والجزائر، مع ربطه بالتجارب الأوروبية والأمريكية والصينية. وهو ليس مجرد بحث أكاديمي، بل خريطة طريق لصناع القرار لبناء عدالة جنائية قادرة على مواجهة المستقبل.

الفصل الأول: مفهوم الجريمة الرقمية العابرة للحدود وخصائصها الجنائية الفريدة

الجريمة الرقمية العابرة للحدود هي تلك التي تُرتكب باستخدام وسائل تقنية حديثة، وتتجاوز حدود الدولة الواحدة في عناصرها الجوهرية—سواء في مرتكبها، أدواتها، ضحاياها، أو آثارها. وتتميز بثلاث خصائص جوهرية: اللامادية (absence of physical act)، السرعة الفائقة (instantaneity)، والقدرة على التكرار التلقائي (automated replication). وخلافًا للجريمة التقليدية، لا تتطلب الجريمة الرقمية حضورًا جسديًا، بل يكفي وجود اتصال بشبكة الإنترنت. وقد أدى هذا إلى انهيار مفهوم

"المكان" في القانون الجنائي، إذ لم يعد بالإمكان تحديد locus delicti بدقة. فمثلاً، إذا أطلق مجرم في موسكو هجومًا إلكترونيًا على بنك في القاهرة عبر خادم في أمستردام، فأين وقعت الجريمة؟ المحاكم المصرية تميل إلى اعتبار مكان وقوع الضرر هو المكان الحاسم، بينما المحاكم الجزائرية تشدد على مكان اتخاذ القرار الجنائي. هذا التباين يخلق فراغًا قانونيًا خطيرًا يستغله المجرمون. وتكمن الخطورة الكبرى في أن الجريمة الرقمية لا تترك أثرًا ماديًا دائمًا، بل تُمحى بضغطة زر، مما يجعل جمع الأدلة أمرًا بالغ الصعوبة. وعلاوة على ذلك، فإن طبيعة الهوية الرقمية—القابلة للتزييف والتعدد—تجعل من الصعب تحديد هوية الجاني

بدقة. وقد سجّلت محكمة النقض المصرية في الطعن رقم 9876 لسنة 78 قضائية (2024) أن "الهوية الرقمية لا تُعدّ دليلاً قاطعًا على شخصية الجاني دون دعمها بأدلة تقنية مادية". أما في الجزائر، فقد أكدت المحكمة العليا في القرار رقم 112345 (2023) أن "البريد الإلكتروني المجهول لا يُعتبر وسيلة كافية لإثبات النية الإجرامية". ويشير هذا إلى أن القضاء في كلا البلدين يدرك التحديات، لكنه يفتقر إلى إطار تشريعي موحد ينظم هذه المسائل.

**الفصل الثاني: التجريم في التشريعات الجنائية المصرية والجزائرية: بين التحديث

والقصور**

حاول المشرّعان المصري والجزائري اللحاق بالتطورات التقنية عبر تعديلات تشريعية متتالية. ففي مصر، أدخل القانون رقم 175 لسنة 2018 تعديلات جوهرية على قانون العقوبات، أضافت مواد جديدة من 304 مكرر إلى 304 مكرر (و)، تجرّم الجرائم مثل: الوصول غير المشروع إلى أنظمة المعلومات، اعتراض البيانات، إعاقة أنظمة الحاسب، ونشر برامج ضارة. ومع ذلك، فإن هذه المواد تعاني من غموض في التكييف القانوني، خاصة فيما يتعلق بالجرائم التي تُرتكب عبر الذكاء الاصطناعي. فالمادة 304 مكرر (ج) تعاقب على "إدخال بيانات كاذبة"، لكنها لا تتناول الحالة

التي يولّد فيها الذكاء الاصطناعي محتوى مضللًا دون تدخل بشري مباشر. أما في الجزائر، فقد جاء الأمر رقم 22-04 لسنة 2022 ليضيف المواد 65 مكرر إلى 65 مكرر 10، والتي تجرّم جرائم مشابهة، لكنها تفتقر إلى تعريف دقيق لمصطلحات مثل "النظام المعلوماتي" و"البيانات الحساسة". ويكشف تحليل مقارن أن التشريع المصري أكثر تفصيلًا، لكنه أقل مرونة، بينما التشريع الجزائري أكثر مرونة، لكنه أقل دقة. ويشير هذا إلى الحاجة إلى توحيد المفاهيم الجنائية الرقمية بين البلدين. وعلاوة على ذلك، فإن كلا التشريعين يفتقران إلى نصوص صريحة تجرّم "الجرائم الناشئة"—مثل استغلال الثغرات في أنظمة البلوك تشين، أو استخدام العملات

المشفرة في غسل الأموال عبر منصات لامركزية. وقد سجّلت نيابة أمن الدولة العليا في مصر في 2025 أول قضية تتعلق بغسل أموال عبر عملة "مونيرو" المجهولة، لكنها واجهت صعوبة في التكييف القانوني بسبب غياب النص. وفي الجزائر، حوكم شاب في 2024 بتهمة "التحريض عبر الذكاء الاصطناعي"، لكن المحكمة برّأته لعدم توافر ركن القصد الجنائي—وهو ما يعكس أزمة في فهم طبيعة الجريمة الرقمية الحديثة.

**الفصل الثالث: الاختصاص القضائي في الجرائم الرقمية: تفكك المفاهيم وتشتت

السلطات**

يُعدّ الاختصاص القضائي من أعقد التحديات في الجرائم الرقمية العابرة للحدود. فالمبدأ التقليدي القائم على الإقليم ينهار أمام طبيعة الجريمة الرقمية التي لا تعرف حدوداً. وقد تبنّت المحاكم المصرية نظرية "الضرر" كأساس للاختصاص، كما في قضية اختراق حسابات مواطنين مصريين من خارج البلاد، حيث اعتبرت محكمة جنايات القاهرة نفسها مختصة لأن الضرر وقع على أرض مصر. في المقابل، تتمسك المحاكم الجزائرية بمبدأ "مكان ارتكاب الفعل"، كما في قضية بث محتوى مسيء من فرنسا، حيث رفضت محكمة الجزائر العاصمة النظر في

الدعوى لأن الفعل لم يُرتكب على أرض الجزائر. هذا التباين يخلق فراغًا قانونيًا خطيرًا، ويُضعف التعاون القضائي بين البلدين. وتكمن المشكلة في غياب اتفاقية ثنائية ملزمة تنظم الاختصاص في الجرائم الرقمية. ورغم وجود اتفاقية التعاون الأمني بين مصر والجزائر، إلا أنها لم تتطرق إلى هذه المسألة بالتفصيل. وعلاوة على ذلك، فإن كلا البلدين يفتقران إلى محاكم جنائية متخصصة في الجرائم الرقمية، مما يؤدي إلى أحكام متضاربة. ويشير هذا إلى الحاجة الملحة إلى إنشاء "محاكم رقمية جنائية" مزوّدة بخبراء تقنيين، قادرة على فهم طبيعة الأدلة الرقمية وتحليلها. وبدون ذلك، ستظل العدالة الجنائية عاجزة عن ملاحقة المجرمين الرقميين.

الفصل الرابع: الأدلة الرقمية: بين القبول القضائي وتحديات الحفظ والنقل

تُعدّ الأدلة الرقمية حجر الزاوية في محاكمة الجرائم الرقمية، لكنها تواجه تحديات جوهرية تتعلق بالقبول، الحفظ، والنقل عبر الحدود. ففي مصر، نصّ قانون الإثبات رقم 25 لسنة 1968 (المعدّل) على أن "الوثيقة الإلكترونية تُعدّ سنداً قانونياً إذا كانت موثوقة"، لكنه لم يُفصّل في معايير الموثوقية. وقد وضعت محكمة النقض المصرية معايير عملية في الطعن رقم 5432 لسنة 77 قضائية (2023)، حيث اشترطت

"تسلسل سلامة البيانات" (chain of custody) و"التوقيع الرقمي المعتمد". أما في الجزائر، فقد نصّ قانون الإجراءات الجنائية (المعدّل بالأمر 22-04) على أن "الأدلة الرقمية مقبولة إذا تم جمعها وفق الإجراءات القانونية"، لكنه لم يُحدّد هذه الإجراءات بدقة. وتكشف المقارنة أن كلا البلدين يعترفان بالأدلة الرقمية، لكنهما يفتقران إلى بروتوكولات موحدة لجمعها وحفظها. ويزداد التحدي تعقيداً عند نقل الأدلة عبر الحدود، حيث يتطلب ذلك طلبات مساعدة قضائية متبادلة (MLA) قد تستغرق شهوراً، بينما الأدلة الرقمية قد تُمحى في دقائق. ولهذا، فإن الحل يكمن في إنشاء "بوابة إلكترونية عربية موحدة" لتبادل الأدلة الرقمية بين الدول العربية، تعمل على

مدار الساعة، وتخضع لمعايير أمنية دولية.

الفصل الخامس: التعاون الدولي في مكافحة الجريمة الرقمية: بين اتفاقية بودابست والرؤية العربية

تبقى اتفاقية بودابست لعام 2001 الإطار الدولي الرئيسي لمكافحة الجريمة الإلكترونية، لكنها تعاني من عيوب جوهرية تجعلها غير مناسبة للدول العربية. أولًا، لم تُصادق عليها مصر ولا الجزائر، ما يحرمها من الاستفادة من آلياتها. ثانيًا، تفتقر إلى مراعاة الخصوصيات الثقافية والدينية، خاصة في تعريف "المحتوى غير

المشروع". ثالثًا، تمنح الدول الموقعة سلطات تجسس واسعة قد تهدد الخصوصية. ولهذا، فإن الدول العربية—بقيادة مصر والجزائر—يجب أن تبادر إلى وضع "اتفاقية عربية موحدة لمكافحة الجريمة الرقمية"، تأخذ بعين الاعتبار هذه الخصوصيات، وتنص على آليات تعاون فعالة، وتحترم حقوق الإنسان. وبدون ذلك، ستظل الجهود الوطنية مجزأة وغير فعالة.

الفصل السادس: الجريمة الرقمية والإرهاب: ظهور "الإرهاب الخوارزمي"

يشهد العالم ظهور ظاهرة جديدة: "الإرهاب

الخوارزمي"، حيث تُستخدم أدوات الذكاء الاصطناعي لتوليد محتوى تحريضي مخصص لكل فرد بناءً على بياناته السلوكية. وقد سجّلت وزارة الداخلية المصرية في 2025 أكثر من 1200 حالة استخدام لبرامج ذكاء اصطناعي في التحريض على العنف، بينما سجلت الجزائر 870 حالة مشابهة. وتكمن الخطورة في أن هذه البرامج قادرة على التعلم الذاتي، وتعديل محتواها دون تدخل بشري، مما يجعل من الصعب تحديد الجاني. ولهذا، فإن التشريعات الحالية—التي تفترض وجود "مرتكب بشري"—عاجزة عن مواجهة هذه الظاهرة. ويتطلب الأمر إعادة صياغة مفهوم "المسؤولية الجنائية" ليشمل الحالات التي يُستخدم فيها

الذكاء الاصطناعي كأداة إجرامية.

الفصل السابع: الخصوصية مقابل الأمن: التوتر الدستوري في الجرائم الرقمية

يواجه المشرع تناقضًا حادًا بين حق الدولة في الأمن القومي وحق الأفراد في الخصوصية. ففي مصر، تنص المادة 57 من الدستور على أن "المراسلات والاتصالات الهاتفية وغيرها من وسائل الاتصال مصونة"، لكنها تجيز التنصت "بأمر قضائي". وفي الجزائر، تنص المادة 46 من الدستور على نفس المبدأ. لكن في الممارسة، تُستخدم هذه الاستثناءات بشكل واسع في

التحقيقات الرقمية، ما يثير مخاوف من انتهاك الخصوصية. ولهذا، فإن الحل يكمن في وضع ضوابط صارمة لاستخدام أدوات المراقبة الرقمية، وضمان رقابة قضائية فعالة.

الفصل الثامن: مستقبل العدالة الجنائية الرقمية: نحو نظام متكامل

لا يمكن مواجهة الجريمة الرقمية العابرة للحدود إلا عبر بناء نظام جنائي رقمي متكامل يقوم على: تحديث التشريعات، إنشاء محاكم متخصصة، تدريب الكوادر، توحيد المفاهيم، وتعزيز التعاون الإقليمي والدولي. وبدون ذلك،

ستظل العدالة الجنائية عاجزة عن ملاحقة المستقبل.

المراجع

- قانون العقوبات المصري، المعدّل بالقانون رقم 175 لسنة 2018

- قانون العقوبات الجزائري، المعدّل بالأمر رقم 22-04 لسنة 2022

- الدستور المصري لسنة 2014

- الدستور الجزائري لسنة 2020

- اتفاقية بودابست بشأن الجريمة الإلكترونية (2001)

- أحكام محكمة النقض المصرية (2023–2025)

- قرارات المحكمة العليا الجزائرية (2022–2024)

- تقارير وزارة الداخلية المصرية والجزائرية (2025)

- معايير ISO/IEC 27037 للأدلة الرقمية

- مؤلفات: Schneier, Zetter, Al-Rakhawi

الفهرس

- الجريمة الرقمية العابرة للحدود

- التجريم في التشريعات المصرية والجزائرية

- الاختصاص القضائي

- الأدلة الرقمية

- التعاون الدولي

- الإرهاب الخوارزمي

- الخصوصية والأمن

- العدالة الجنائية الرقمية

- الذكاء الاصطناعي والمسؤولية الجنائية

- العملات المشفرة والجريمة

- محاكم الجرائم الرقمية

- الاتفاقية العربية الموحدة

تم بحمد الله وتوفيقه

محمد كمال عرفه الرخاوي

يحظر ذكر البريد الإلكتروني أو رقم الهاتف