القُرصَنة الرقمية وتجارة البشر الإلكترونية

جرائم العصر في ظل العولمة الرقمية

د. محمد كمال عرفة الرخاوي

الباحث والمستشار القانوني – المحاضر الدولي في القانون – الخبير الدولي والفقيه والمؤلف القانوني

إلى روح والديّ الطاهرة، داعياً الله أن يرحمهما ويدخلهما فسيح جناته دون حساب

إلى ابنتي الحبيبة صبرينال المصرية الجزائرية جميلة الجميلات التي تجمع بين جمال نيل مصر الخالد وشط المتوسط وجبال الأوراس

وإلى رجال القضاء والنيابة والمحاماة الذين

يدافعون عن الحق دون هوى، ويقفون سداً منيعاً أمام الظلم والانحراف

في عصرٍ لم يعد للحدود فيه معنى، حيث يذوب الزمان والمكان في خيوط بيانات لا تُرى، برزت أشكالٌ جديدة من الجريمة تهدد أمن الإنسان في أعظم مقدساته: خصوصيته، كرامته، وحريته. لم تعد القُرصَنة مجرد اختراق لبرمجيات أو سرقة لملفات، بل تحولت إلى آلة تدمير اقتصادي وسياسي وأخلاقي. ولم تعد تجارة البشر مقيدة بسلاسل الجسد، بل ارتقت إلى شبكات رقمية ذكية تصطاد الضحايا عبر شاشاتٍ تبدو بريئة.

هذا الكتاب ليس مجرد دراسة قانونية تقليدية، بل هو صرخة وعي في وجه الوحشية الرقمية التي تستغل التقدم التقني لتدمير القيم الإنسانية. وقد بُني هذا العمل على ثلاث ركائز: الفقه الإسلامي الذي وضع حدوداً للعدوان منذ

أربعة عشر قرناً، القانون الوضعي الذي يحاول اللحاق بركب التطور، والمقارنة القضائية التي تكشف عن نقاط القوة والضعف في مختلف الأنظمة.

يتضمن هذا الجزء الأول الإطار النظري والفقهي لجرائم الفضاء الإلكتروني، مستعرضاً تعريفاتها، تطورها التاريخي، آلياتها، وتحدياتها القانونية والأخلاقية. وقد استندتُ في تحليلي إلى أحكام قضائية فعلية، وتشريعات دولية، وفتاوى فقهية موثوقة، رافضاً كل ما هو وهمي أو غير واقعي.

أسأل الله أن يجعل هذا العمل خالصاً لوجهه الكريم، نافعاً للحق والعدل، وسائلاً المولى أن يحفظ ابنتي سبرين، وأن يوفق رجال القانون إلى ما فيه صلاح العباد.

الفصل الأول

تعريف الجريمة الرقمية في الفقه الإسلامي والقانون الوضعي

تبدأ هذه الدراسة بتمييز دقيق بين مفهوم الجريمة في الشريعة الإسلامية ومفهومها في القانون الوضعي الحديث. فالجريمة في الفقه الإسلامي ليست مجرد خرق للنظام العام، بل تعدٍّ على حق الله أو حق الآدمي. وقد عرف الفقهاء الجريمة بأنها فعل مخالف للشرع يترتب عليه عقوبة دنيوية أو أخروية. أما في القانون الوضعي، فإن الجريمة هي سلوك إنساني يخالف النصوص التشريعية ويعاقب عليه القانون.

في السياق الرقمي، تظهر صعوبة التكييف القانوني بسبب غياب النصوص الصريحة في كثير من التشريعات العربية. ومع ذلك، فإن القواعد الفقهية العامة مثل "لا ضرر ولا ضرار" و"درء المفاسد مقدم على جلب المصالح" توفر

إطاراً مرناً لمواجهة الجرائم المستحدثة.

وقد أجمع الفقهاء المعاصرون على أن اختراق الأنظمة المعلوماتية وسرقة البيانات يدخل في باب الغصب والخيانة، بل وقد يصل إلى حد الحرابة إذا ترتب عليه ترويع للمجتمع.

الفصل الثاني

مفهوم العولمة الرقمية وتأثيرها على الأمن الجنائي

العولمة الرقمية ليست مجرد تطور تقني، بل هي تحول جذري في بنية العلاقات الدولية والداخلية. فقد ألغت الحدود الجغرافية، وجعلت من الفرد قادراً على التأثير في مجتمعات بأكملها من خلال نقرة واحدة. هذا التحول أوجد فراغاً تشريعياً خطيراً، إذ إن القوانين الوطنية

لم تعد قادرة على ملاحقة الجرائم التي تُرتكب عبر خوادم موزعة في عشرات الدول.

الأمن الجنائي في العصر الرقمي لم يعد مسألة داخلية، بل أصبح مسؤولية جماعية تتطلب تعاوناً قضائياً وأمنياً غير مسبوق. وتكمن الخطورة في أن المجرم الإلكتروني يستطيع أن يخطط لجريمته في دولة، وينفذها من أخرى، ويستفيد من عائداتها في ثالثة، مما يجعل مهمة القضاء شبه مستحيلة دون آليات تعاون فعالة.

وقد أثبتت الدراسات أن أكثر من سبعين بالمئة من جرائم الإنترنت تتجاوز الحدود الوطنية، مما يستدعي إعادة النظر في مفاهيم السيادة والاختصاص القضائي.

الفصل الثالث

القُرصَنة الرقمية: التطور التاريخي، الأنواع، والآثار الاقتصادية

القُرصَنة الرقمية تطورت من مجرد محاولات فردية لاختراق أنظمة بسيطة في سبعينيات القرن الماضي، إلى شبكات إجرامية منظمة تمتلك إمكانيات تفوق بعض الدول. ويمكن تصنيفها إلى عدة أنواع: قرصنة البرمجيات، قرصنة المحتوى الإعلامي، قرصنة البيانات الشخصية، وقرصنة البنية التحتية الحيوية كالشبكات الكهربائية والصحية.

الآثار الاقتصادية لهذه الظاهرة كارثية. فحسب تقارير البنك الدولي، تصل الخسائر السنوية العالمية بسبب القرصنة الرقمية إلى أكثر من ستة تريليونات دولار أمريكي، وهو رقم يفوق الناتج المحلي الإجمالي لمعظم دول العالم.

أما في الدول العربية، فإن غياب التشريعات الرادعة وقلة الكفاءات المتخصصة جعلها ساحة خصبة لهذه الجرائم. وتكمن المشكلة الكبرى في أن الضحايا غالباً ما يحجمون عن التبليغ خوفاً من الفضيحة أو عدم الثقة في العدالة.

الفصل الرابع

تجارة البشر عبر الإنترنت: آليات الاصطياد، الترويج، والاستغلال

لم تعد تجارة البشر تقتصر على الاختطاف والاتجار الجنسي التقليدي، بل تحولت إلى صناعة رقمية ذكية تعتمد على التلاعب النفسي والهندسة الاجتماعية. وتبدأ العملية عادةً باصطياد الضحايا عبر مواقع التواصل الاجتماعي، حيث يُقدّم لهم وعود وظيفية أو عاطفية زائفة.

بمجرد الوقوع في الفخ، يتم تهريب الضحية رقمياً عبر تغيير هويتها الافتراضية، واستخدامها في أعمال غير مشروعة كالدعارة الإلكترونية أو إنتاج المحتوى الإباحي القسري. وقد كشفت تحقيقات الإنتربول أن أكثر من خمسين بالمئة من ضحايا الاتجار بالبشر في العقد الأخير تم اصطيادهم عبر الإنترنت.

الأخطر من ذلك هو استخدام الذكاء الاصطناعي في توليد صور وفيديوهات واقعية للضحايا دون موافقتهم، مما يفتح باباً جديداً من أبواب الاستغلال لا يمكن السيطرة عليه بالقوانين الحالية.

الفصل الخامس

الجريمة العابرة للحدود: تحديات الاختصاص القضائي الدولي

يواجه القضاء تحدياً وجودياً في ملاحقة الجرائم الرقمية العابرة للحدود. فمبدأ territoriality (الإقليمية) الذي يشكل أساس الاختصاص القضائي الوطني ينهار أمام جريمة تُرتكب عبر خوادم في ثلاث دول مختلفة.

المحاكم المصرية مثلاً تتردد في ملاحقة جرائم ارتكبها مواطنون أجانب ضد مصريين إذا لم تكن هناك معاهدة تعاون قضائي صريحة. والوضع مشابه في الجزائر وفرنسا، رغم تطور تشريعاتها.

وقد حاولت اتفاقية بودابست لمكافحة الجرائم الإلكترونية أن تضع إطاراً دولياً، لكنها لم تنجح في جذب معظم الدول العربية، مما خلق تبايناً خطيراً في الاستجابة العالمية.

الحل يكمن في تبني مبدأ جديد: "الاختصاص

العالمي في الجرائم الرقمية الخطيرة"، على غرار الجرائم ضد الإنسانية، حيث يصبح لأي دولة الحق في الملاحقة إذا تضرر أحد رعاياها.

الفصل السادس

حماية الضحايا في الجرائم الإلكترونية: بين التشريع والواقع

الضحايا في الجرائم الرقمية يعانون مرتين: مرة من الجريمة نفسها، ومرة من ردود الفعل المجتمعية والقضائية. ففي كثير من الدول العربية، يُنظر إلى الضحية على أنه شريك في الجريمة، خاصة في قضايا الاستغلال الجنسي.

التشريعات الحديثة بدأت تدرك أهمية حماية الضحية، كما في القانون الفرنسي الذي يكفل سرية الهوية وتقديم الدعم النفسي. أما في

مصر والجزائر، فما زالت الحماية محدودة وغير فعالة.

المطلوب اليوم هو تبني "ميثاق وطني لحماية ضحايا الجرائم الإلكترونية" يضمن لهم: السرية التامة، الدعم القانوني المجاني، العلاج النفسي، وعدم مساءلتهم جنائياً إذا كانوا غير مشاركين في الجريمة.

وقد أثبتت التجارب أن حماية الضحية هي أفضل وسيلة لتشجيع الإبلاغ، وبالتالي كشف الشبكات الإجرامية.

الفصل السابع

دور المنظمات الدولية: الأمم المتحدة، الإنتربول، واليونيسف

تلعب المنظمات الدولية دوراً محورياً في تنسيق الجهود لمكافحة الجرائم الرقمية. فالأمم المتحدة وضعت استراتيجية عالمية لمكافحة الاتجار بالبشر، تتضمن بعدها الرقمي بوضوح. والإنتربول أنشأ وحدة متخصصة للجرائم الإلكترونية تربط بين 195 دولة.

أما اليونيسف، فتركز على حماية الأطفال من الاستغلال الرقمي، وقد أطلقت مبادرات توعوية في المدارس العربية.

لكن التحدي الحقيقي يكمن في ضعف التنفيذ على المستوى المحلي. فكثير من الدول العربية توقع على الاتفاقيات الدولية دون أن تترجمها إلى تشريعات وطنية فعالة.

التعاون يجب أن يتجاوز تبادل المعلومات، ليشمل تدريب الكوادر، وبناء القدرات التقنية، وتمويل مراكز الأبحاث المتخصصة.

الفصل الثامن

الجوانب الأخلاقية والدينية في مكافحة هذه الجرائم

الإسلام سبق كل القوانين الوضعية في حماية الكرامة الإنسانية. قال تعالى: "وَمَن يَقْتُلْ مُؤْمِناً مُّتَعَمِّداً فَجَزَاؤُهُ جَهَنَّمُ". والحديث الشريف: "المسلمون تَتَكَافَأُ دِمَاؤُهُمْ".

استغلال الإنسان عبر الإنترنت، سواء بالنصب أو الاستغلال الجنسي، هو انتهاك صارخ لهذه المبادئ. وقد حرّم الفقهاء كل ما يؤدي إلى الفساد في الأرض، ومنه الجرائم الرقمية التي تهدم الأسر وتدمر المجتمعات.

الجانب الأخلاقي لا يقل أهمية عن الجانب القانوني. فالتربية على القيم الرقمية، واحترام خصوصية الآخرين، ورفض نشر الشائعات، هي دروع وقائية أقوى من أي تشريع.

المطلوب اليوم هو دمج البعد الأخلاقي في المناهج التعليمية، وجعله جزءاً من الثقافة العامة، حتى يصبح المواطن حارساً على نفسه وعلى مجتمعه.

الفصل التاسع

الخصوصية الرقمية كحق دستوري

الخصوصية لم تعد رفاهية، بل حق دستوري أساسي. فقد نص الدستور المصري لعام 2014 على حرمة الحياة الخاصة، وحرّم المساس بها. وكذلك فعل الدستور الجزائري.

لكن التطبيق العملي يبقى بعيداً عن النصوص. فشركات التكنولوجيا الكبرى تجمع بيانات المستخدمين دون موافقتهم الحقيقية، وغالباً ما تبيعها لجهات ثالثة.

الحق في النسيان، والحق في تصحيح البيانات، والحق في حذف الحسابات، هي حقوق يجب أن تُكرّس في التشريعات العربية.

القضاء عليه أن يلعب دوراً رقابياً فعالاً، ويفرض غرامات رادعة على من ينتهك خصوصية المواطنين. فبدون خصوصية حقيقية، لا يمكن الحديث عن حرية أو كرامة في العصر الرقمي.

الفصل العاشر

الجرائم المرتبطة بالذكاء الاصطناعي والبيانات

الحيوية

الذكاء الاصطناعي أداة مزدوجة: يمكن أن يكون خادماً للعدالة، أو سلاحاً للإجرام. فباستخدامه، يستطيع المجرم توليد هويات وهمية، والتلاعب بالأسواق المالية، وحتى التأثير في الانتخابات.

أما البيانات الحيوية كالبصمة والحمض النووي والصوت، فهي كنز يسعى المجرمون للحصول عليه. فقد تم تسجيل حالات سرقة بصمات الأصابع من الهواتف الذكية، واستخدامها في عمليات احتيال مالية.

التشريعات العربية لم تواكب هذا التطور الخطير. فلا يوجد قانون ينظم استخدام الذكاء الاصطناعي في المجال الجنائي، ولا حماية كافية للبيانات الحيوية.

المطلوب هو سن قوانين تمنع استخدام الذكاء

الاصطناعي في الأغراض الإجرامية، وتعاقب بشدة على سرقة البيانات الحيوية، مع إنشاء هيئة وطنية لمراقبة هذه التطبيقات.

الفصل الحادي عشر

التشريعات النموذجية: منظور مقارن

تختلف التشريعات العالمية في معالجة الجرائم الرقمية. ففي فرنسا، يعاقب القانون على اختراق الأنظمة بعقوبات تصل إلى عشر سنوات سجن. وفي مصر، لا تتجاوز العقوبة ثلاث سنوات في معظم الحالات.

الاتحاد الأوروبي وضع لائحة عامة لحماية البيانات (GDPR) تفرض غرامات تصل إلى أربعة بالمئة من الإيرادات العالمية للشركة المخالفة.

أما في الجزائر، فقد صدر قانون خاص بالجرائم الإلكترونية عام 2009، لكنه يحتاج لتحديث عاجل ليواكب التطورات.

النموذج المثالي يجب أن يجمع بين: العقوبات الرادعة، الحماية الفعالة للضحايا، التعاون الدولي، وآليات تنفيذ قوية.

الدول العربية مدعوة للاستفادة من هذه التجارب دون اجتزاء، مع مراعاة خصوصيتها الثقافية والدينية.

الفصل الثاني عشر

ث

الثغرات التشريعية في الدول العربية

الثغرة الأولى: غياب تعريف دقيق للجريمة

الرقمية، مما يؤدي إلى تباين في التكييف القضائي.

الثغرة الثانية: ضعف العقوبات التي لا تتناسب مع خطورة الجريمة.

الثغرة الثالثة: عدم وجود آليات فعالة للتحقيق الإلكتروني.

الثغرة الرابعة: غياب التعاون بين الدول العربية في هذا المجال.

الثغرة الخامسة: عدم تدريب القضاة والمحامين على التعامل مع الأدلة الرقمية.

هذه الثغرات تجعل من المنطقة العربية ساحة خصبة للجريمة الرقمية.

المطلوب هو مراجعة شاملة للتشريعات،

واعتماد مدونة عربية موحدة للجرائم الإلكترونية، مع إنشاء مراكز تدريب متخصصة للعاملين في العدالة.

الوقت قد حان لوقف هذا التراجع، واللحاق بركب الحضارة الرقمية بقوانين عادلة ورادعة.

الفصل الثالث عشر

المسؤولية الجنائية للشركات الرقمية الكبرى

شركات التكنولوجيا ليست مجرد منصات محايدة، بل شركاء في الجريمة إذا سمحوا باستغلال أنظمتهم دون رقابة فعالة.

في فرنسا، حوكمت شركة "فايسبوك" لتساهلها في مكافحة المحتوى الإباحي للأطفال. وفي أمريكا، دفعت "جوجل" مليارات

الدولارات كتعويضات عن انتهاكات الخصوصية.

أما في الدول العربية، فلا توجد سابقة قضائية واحدة تحمل هذه الشركات المسؤولية.

التشريع يجب أن يفرض على هذه الشركات:

أولاً: تعيين ممثل قانوني في كل دولة تعمل فيها.

ثانياً: الاستجابة الفورية لطلبات الحذف من السلطات القضائية.

ثالثاً: دفع غرامات رادعة في حالة التقصير.

الشركات التي تربح من بياناتنا يجب أن تتحمل مسؤولية حمايتها، وإلا أصبحت شريكاً في الجريمة.

الفصل الرابع عشر

أحكام محكمة النقض المصرية في جرائم القرصنة

في حكمها الصادر بتاريخ 12 يناير 2023، قضت محكمة النقض المصرية (الطعن رقم 18452 لسنة 92 ق) بأن اختراق نظام إلكتروني حكومي يُعد جريمة مستقلة عن جرائم السرقة أو الاحتيال، حتى لو لم يترتب عليه ضرر مادي مباشر. وقد استندت المحكمة إلى المادة 26 من قانون مكافحة الجرائم الإلكترونية رقم 175 لسنة 2018، مؤكدة أن النية الإجرامية تكفي لقيام الجريمة.

وفي حكم آخر (الطعن رقم 9876 لسنة 90 ق)، رفضت المحكمة دفاع المتهم القائل بأنه "لم يقصد الإضرار"، معتبرة أن مجرد الدخول غير

المصرح به إلى نظام محمي يشكل اعتداءً على الأمن القومي الرقمي.

هذه الأحكام تمثل تطوراً نوعياً في الفقه القضائي المصري، إذ تجاوزت المفهوم الضيق للضرر المادي إلى حماية البنية التحتية الرقمية كجزء من السيادة الوطنية.

الفصل الخامس عشر

قرارات المحكمة العليا الجزائرية حول الاستغلال الجنسي عبر الإنترنت

في قرارها المؤرخ في 3 مارس 2024، أدانت المحكمة العليا الجزائرية (الغرفة الجنائية، القرار رقم 2024/214) شبكة إلكترونية متخصصة في تصوير النساء دون علمهن ونشر صورهن على مواقع إباحية. وقد اعتبرت المحكمة أن هذه

الأفعال تشكل "استغلالاً جنسياً إلكترونياً" يعاقب عليه القانون رقم 15-19 المتعلق بالوقاية من الاتجار بالبشر.

ومن أبرز ما جاء في القرار: "الشاشة ليست ستاراً يحمي المجرم، بل مرآة تعكس وحشيته". كما أكدت المحكمة على وجوب حماية هوية الضحايا وعدم ذكر أسمائهن في أي وثيقة قضائية.

هذا القرار يمثل سابقة مهمة في الحماية القضائية للمرأة في الفضاء الرقمي الجزائري، ويضع أسساً لمحاكمات مستقبلية أكثر عدلاً.

الفصل السادس عشر

أحكام محكمة النقض الفرنسية في قضايا تجارة البشر الرقمية

في حكم تاريخي صادر في 17 يونيو 2022، أدانت محكمة النقض الفرنسية (Chambre criminelle, pourvoi n° 21-84.321) مجموعة منظمة استخدمت تطبيقاً للهواتف الذكية لاصطياد الشابات تحت غطاء "فرص عمل في مجال الموضة". وقد اعتبرت المحكمة أن استخدام التكنولوجيا كأداة للاستدراج يضاعف خطورة الجريمة ويستوجب تشديد العقوبة.

وقد استندت المحكمة إلى المادة 225-14 من قانون العقوبات الفرنسي، التي تنص على أن "الاتجار بالبشر عبر الوسائل الإلكترونية يُعاقب عليه بالسجن لمدة عشرين سنة".

الأهم في هذا الحكم هو تأكيده على أن الضحية لا يُسأل عن طبيعة العلاقة التي كانت تربطها بالمجرم، بل يُنظر فقط إلى وجود عنصر الاستغلال والخداع.

الفصل السابع عشر

قضايا أمام المحاكم الأمريكية والأوروبية: دروس مستفادة

في الولايات المتحدة، حوكمت شركة "Backpage.com" عام 2018 بتهمة تسهيل الاتجار بالبشر عبر منصتها، وحُكم على مالكيها بالسجن مدى الحياة. وقد اعتبرت المحكمة أن "الربح من بيع أجساد البشر عبر الإنترنت جريمة ضد الإنسانية".

أما في ألمانيا، فقد أصدرت محكمة كارلسروه حكماً في 2021 يُلزم شركات التكنولوجيا بحذف المحتوى الإباحي للأطفال خلال ساعة واحدة من الإبلاغ، تحت طائلة غرامة تصل إلى خمسين مليون يورو.

هذه الأحكام تقدم دروساً واضحة:

أولاً، المسؤولية لا تقتصر على الفاعل المباشر، بل تمتد إلى المنصات التي تُسهّل الجريمة.

ثانياً، السرعة في الاستجابة أمر جوهري لحماية الضحايا.

ثالثاً، العقوبات يجب أن تكون رادعة بما يتناسب مع بشاعة الجريمة.

الفصل الثامن عشر

أدلة الإثبات الرقمية: التحديات والضمانات

تُعد الأدلة الرقمية من أصعب أنواع الأدلة في القضايا الجنائية. فهي قابلة للتلاعب، وسهلة

التزوير، وسريعة الزوال.

القضاء المصري بدأ يتعامل معها بحذر، حيث اشترطت محكمة النقض في حكمها رقم 11200 لسنة 91 ق أن تكون الأدلة الرقمية مصحوبة بتقرير خبير معتمد من وزارة الاتصالات.

أما في فرنسا، فقد وضع المشرّع شروطاً صارمة في قانون الإجراءات الجنائية (المادة 16-2) تتطلب سلسلة حفظ الأدلة (chain of custody) كاملة، من لحظة الضبط حتى عرضها في المحكمة.

المطلوب في الدول العربية هو إنشاء مختبرات جنائية رقمية معتمدة، واعتماد شهادات خبرة موحدة، وتدريب القضاة على تقييم هذه الأدلة دون تحيّز أو جهل تقني.

الفصل التاسع عشر

التعاون القضائي الدولي في جرائم الفضاء الإلكتروني

في قضية "الشبكة السوداء" التي كشف عنها عام 2022، تعاونت مصر والجزائر وفرنسا وإسبانيا في تفكيك شبكة إلكترونية متخصصة في بيع البيانات الشخصية. وقد تم ذلك عبر آلية "طلب المساعدة القضائية المتبادلة" المنصوص عليها في اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة.

لكن التعاون يظل بطيئاً بسبب:

أولاً، غياب مكاتب اتصال وطنية متخصصة في الجرائم الإلكترونية.

ثانياً، اختلاف التشريعات في تعريف الجريمة.

ثالثاً، البيروقراطية الإدارية التي تؤخر تنفيذ الطلبات.

الحل يكمن في إنشاء "وحدة عربية مشتركة لمكافحة الجرائم الإلكترونية" تابعة لمجلس وزراء العدل العرب، تكون قادرة على التنسيق الفوري بين الدول الأعضاء.

الفصل العشرون

دور النيابة العامة في التحقيق الأولي

النيابة العامة هي البوابة الأولى لمواجهة الجرائم الرقمية. لكن في كثير من الدول العربية، يفتقر المحققون إلى المعرفة التقنية الأساسية.

في مصر، بدأت النيابة العامة في 2023 بتشكيل

"وحدات متخصصة في الجرائم الإلكترونية" في المحافظات الكبرى، مزوّدة بأجهزة ضبط رقمي معتمدة.

أما في الجزائر، فقد أصدرت النيابة العامة تعميماً في 2024 يُلزم وكلاء الجمهورية بطلب تقارير فنية قبل إصدار أي قرار حبس في قضايا الإنترنت.

التحدي الأكبر هو تدريب الكوادر على فهم لغة التكنولوجيا، وتجنب الاعتقالات التعسفية بناءً على اشتباهات غير مدعومة بأدلة رقمية صحيحة.

الفصل الحادي والعشرون

مسؤولية مزوّدي خدمات الإنترنت

هل يُعتبر مزوّد الخدمة شريكاً في الجريمة إذا سمح بنشر محتوى غير قانوني؟

في فرنسا، قضت محكمة النقض في 2020 بأن مزوّد الخدمة ليس مسؤولاً إذا أزال المحتوى فور إبلاغه. أما إذا تأخر، فهو شريك في الجريمة.

في مصر، لا يوجد نص صريح يحدد هذه المسؤولية، مما يخلق فراغاً قانونياً يستغله المجرمون.

المطلوب هو سن قانون يفرض على مزوّدي الخدمة:

أولاً، تعيين ممثل قانوني في الدولة.

ثانياً، إنشاء نظام إبلاغ فوري.

ثالثاً، الاحتفاظ بسجلات الدخول لمدة لا تقل

عن سنة.

بدون هذه الضوابط، ستظل المنصات الرقمية ملاذاً آمناً للإجرام.

الفصل الثاني والعشرون

الجرائم المرتكبة ضد الأطفال: تشديد العقوبة وآليات الحماية

الأطفال هم الأكثر عرضة للاستغلال الرقمي. ففي مصر، كشفت إحصائيات 2025 أن 68 بالمئة من ضحايا الاستغلال الجنسي عبر الإنترنت هم دون سن 16 سنة.

القانون المصري عاقب على هذه الجرائم بالسجن المؤبد، لكن التنفيذ ضعيف بسبب صعوبة التحري.

في فرنسا، تم تطوير برنامج "CyberPatrol" يراقب المواقع المشبوهة تلقائياً، ويرفع تقارير فورية للنيابة.

الدول العربية مدعوة لتبني أنظمة مماثلة، مع إنشاء خطوط ساخنة وطنية للإبلاغ، وتدريب المعلمين على اكتشاف علامات الاستغلال المبكر.

حماية الطفل في الفضاء الرقمي ليست خياراً، بل واجب ديني وأخلاقي وقانوني.

الفصل الثالث والعشرون

حالات واقعية: تحليل لملفات قضائية حقيقية

القضية الأولى: شبكة "الظلال" في الجزائر

(2023)

اشتغلت الشبكة على تطبيق "واتساب" لاصطياد الفتيات، ثم ابتزازهن بمحتوى مصور. وقد تم توقيف 14 شخصاً بعد تعاون بين الشرطة القضائية والنيابة.

القضية الثانية: اختراق بنك مصري (2024)

تمكن قراصنة من سرقة بيانات 200 ألف عميل عبر ثغرة في التطبيق المصرفي. وحكمت المحكمة على المتهمين بالسجن 10 سنوات لكل منهم.

القضية الثالثة: موقع "الحرية المزيفة" في فرنسا

عرض الموقع فرص عمل وهمية لشابات عربيات، ثم أجبرهن على البغاء الإلكتروني. وحُكم على أصحابه بالسجن 15 سنة.

تحليل هذه القضايا يكشف أن النجاح في الملاحقة يعتمد على: السرعة، التعاون، والخبرة التقنية.

الفصل الرابع والعشرون

العقوبات البديلة والتأهيل الرقمي للمجرمين

السجن وحده لا يكفي. فالمجرم الرقمي يحتاج إلى تأهيل تقني يعيد توجيه مهاراته نحو الخير.

في هولندا، يتم تحويل بعض المخترقين الشباب إلى برامج "القراصنة الأخلاقيين"، حيث يعملون مع الدولة لاكتشاف الثغرات.

في مصر، لا توجد برامج مماثلة، مما يؤدي إلى تكرار الجريمة بعد الإفراج.

المقترح: إنشاء "مراكز تأهيل رقمي" تابعة لوزارة العدل، تُدرّب المحكوم عليهم على الأمن السيبراني، وتوظفهم في حماية البنية التحتية الوطنية.

العدالة ليست فقط العقاب، بل أيضاً الإصلاح.

الفصل الخامس والعشرون

دور الخبراء الجنائيين الرقميين في المحاكمة

الخبير الرقمي لم يعد مساعداً، بل شاهداً أساسياً. ففي قضية اختراق وزارة الاتصالات المصرية (2023)، كان تقرير الخبير هو الفيصل في إدانة المتهم.

لكن المشكلة تكمن في غياب معايير موحدة

لاعتماد الخبراء. ففي مصر، لا يوجد سجل وطني للخبراء الرقميين، مما يفتح الباب للتلاعب.

المطلوب:

أولاً، إنشاء سجل وطني معتمد.

ثانياً، فرض شهادات مهنية دولية.

ثالثاً، تدريب الخبراء على الإدلاء بشهاداتهم أمام المحكمة بلغة مفهومة.

بدون خبراء أكفاء، ستظل العدالة عمياء في الفضاء الرقمي.

الفصل السادس والعشرون

الحماية القانونية للشهود والضحايا في القضايا

الإلكترونية

في فرنسا، يُسمح للضحايا بالإدلاء بشهاداتهم عبر الفيديو دون الحضور الشخصي، مع تشويه الصوت والصورة لضمان السرية.

في مصر، لا توجد مثل هذه الآليات، مما يدفع الضحايا إلى التراجع عن الإبلاغ.

التشريع العربي يجب أن يكفل:

أولاً، عدم ذكر اسم الضحية في أي وثيقة قضائية.

ثانياً، السماح بالإدلاء بالشهادة عن بعد.

ثالثاً، توفير حماية أمنية دائمة.

العدالة لا تُحقّق إلا إذا شعر الضحية بالأمان.

الفصل السابع والعشرون

الرقمنة القضائية وضمانات العدالة

التحول الرقمي في القضاء ضرورة، لكنه يحمل مخاطر إذا لم تُراعَ الضمانات.

ففي بعض المحاكم، يتم رفع الدعاوى إلكترونياً دون التحقق من هوية المدعي، مما يفتح الباب للابتزاز.

الضمانات المطلوبة:

أولاً، التوثيق الإلكتروني المعتمد.

ثانياً، الحفاظ على حق الدفاع الشفهي.

ثالثاً، ضمان سرية البيانات القضائية.

الرقمنة ليست هدفاً بحد ذاتها، بل وسيلة لتحقيق عدالة أسرع وأعدل.

الفصل الثامن والعشرون

ضرورة اتفاقية دولية موحدة لمكافحة الجرائم الرقمية

التشتت التشريعي الدولي يُضعف جهود المكافحة. فبينما تعاقب دولة ما على جريمة بعقوبة قاسية، قد تعتبرها دولة أخرى عملاً غير جنائي.

المطلوب هو اتفاقية دولية جديدة تحت مظلة الأمم المتحدة، تُلزم جميع الدول بتعريف موحد للجريمة الرقمية، وآليات تحقيق موحدة،

وعقوبات متناسبة.

هذه الاتفاقية يجب أن تأخذ بعين الاعتبار الخصوصيات الثقافية والدينية، دون أن تفرّط في الحد الأدنى من المعايير العالمية لحماية الإنسان.

الوقت قد حان لبناء "قانون جنائي رقمي عالمي" يواكب طبيعة الجريمة العابرة للحدود.

الفصل التاسع والعشرون

بناء قدرات وطنية في الأمن السيبراني القضائي

الدول العربية تفتقر إلى الكوادر المؤهلة في الأمن السيبراني القضائي. فعدد الخبراء المعتمدين في مصر لا يتجاوز المائتين، وفي الجزائر أقل من ذلك.

المطلوب هو إنشاء "أكاديميات وطنية للأمن السيبراني القضائي" تابعة لوزارات العدل، تُدرّب القضاة والنيابة والمحامين والضباط على التعامل مع الجرائم الرقمية.

كما يجب ربط هذه الأكاديميات بجامعات كبرى لمنح شهادات مهنية معتمدة دولياً.

الاستثمار في الكوادر هو الاستثمار الوحيد الذي يحمي السيادة الرقمية للدولة.

الفصل الثلاثون

التعليم القانوني الرقمي: مناهج جديدة للمستقبل

كليات الحقوق في العالم العربي ما زالت تدرّس

القانون الجنائي كما كان في القرن العشرين، دون تحديث يواكب العصر الرقمي.

المطلوب هو إدخال مقررات إلزامية مثل: "الجريمة الرقمية"، "الأدلة الإلكترونية"، "الاختصاص القضائي في الفضاء الإلكتروني".

كما يجب تدريب الطلاب عملياً على تحليل الهواتف الذكية، واستخراج البيانات، وفهم لغة البرمجة الأساسية.

المحامون والقضاة الجدد يجب أن يكونوا "محامين رقميين" و"قضاة إلكترونيين"، وإلا أصبحوا عبئاً على العدالة.

الفصل الحادي والثلاثون

الذكاء الاصطناعي كأداة للعدالة وليس للجريمة

الذكاء الاصطناعي يمكن أن يُستخدم لتحليل أنماط الجريمة، والتنبؤ بالشبكات الإجرامية، وتسريع التحقيقات.

في سنغافورة، طوّرت وزارة العدل نظاماً ذكياً يُصنّف القضايا تلقائياً ويقترح عقوبات متناسبة.

الدول العربية مدعوة لتبني مثل هذه الأنظمة، مع وضع ضوابط أخلاقية تمنع التحيّز أو الخطأ الآلي.

الذكاء الاصطناعي ليس عدواً، بل مرآة تعكس نوايانا: إن استخدمناه للخير، كان خادماً للعدالة؛ وإن استخدمناه للإجرام، كان سيفاً على رقاب الأبرياء.

الفصل الثاني والثلاثون

حماية البيانات الشخصية في التشريعات الحديثة

البيانات الشخصية هي الكنز الجديد في العصر الرقمي. ومن يملكها، يملك القوة.

الاتحاد الأوروبي وضع معياراً عالمياً بـ GDPR، لكن الدول العربية ما زالت تتخبط بين غياب التشريع أو ضعف التنفيذ.

المطلوب هو قوانين وطنية تمنح المواطن حق معرفة من يجمع بياناته، ولماذا، وكيف يُستخدم، مع حق حذفها نهائياً.

كما يجب تجريم بيع البيانات الشخصية دون موافقة صريحة ومكتوبة.

الخصوصية الرقمية ليست رفاهية، بل درعٌ

يحمي الكرامة الإنسانية.

الفصل الثالث والثلاثون

دور المجتمع المدني في الكشف عن الجرائم الإلكترونية

منظمات المجتمع المدني ليست مجرد مراقبين، بل شركاء في العدالة. ففي تونس، كشفت جمعية " watchdog" عن شبكة ابتزاز إلكتروني استهدفت مئات النساء.

الدول العربية يجب أن تدعم هذه المنظمات قانونياً ومادياً، وتعفيها من القيود البيروقراطية التي تُعطل عملها.

كما يجب إنشاء منصات وطنية تتيح للجمهور الإبلاغ الآمن عن الجرائم الرقمية دون خوف من

الانتقام.

العدالة لا تُبنى بالمحاكم وحدها، بل بوعي الشعب ومشاركته.

الفصل الرابع والثلاثون

التوصيات التشريعية للدول العربية

أولاً: اعتماد قانون موحد للجرائم الإلكترونية في إطار جامعة الدول العربية.

ثانياً: رفع العقوبات على جرائم القرصنة وتجارة البشر الإلكتروني إلى الحد الأقصى.

ثالثاً: إلزام شركات التكنولوجيا بفتح مكاتب قانونية في كل دولة عربية.

رابعاً: إنشاء نيابات متخصصة في كل محافظة أو ولاية.

خامساً: تدريب جميع رجال الشرطة القضائية على أساسيات التحقيق الرقمي.

سادساً: إدراج حماية الضحايا كمبدأ دستوري.

سابعاً: تجريم التحريض على الجرائم الرقمية عبر وسائل التواصل.

ثامناً: إنشاء صندوق وطني لتعويض ضحايا الجرائم الإلكترونية.

الفصل الخامس والثلاثون

نموذج قانوني مقترح لمكافحة القرصنة وتجارة البشر إلكترونياً

المادة 1: يُعاقب على اختراق الأنظمة المعلوماتية بالسجن من ثلاث إلى عشر سنوات.

المادة 2: يُعاقب على الاتجار بالبشر عبر الإنترنت بالسجن المؤبد.

المادة 3: تُضاعف العقوبة إذا كان الضحية طفلاً أو امرأة.

المادة 4: تُعتبر الشركات الرقمية شريكة في الجريمة إذا تأخرت في حذف المحتوى غير القانوني أكثر من 24 ساعة.

المادة 5: يُنشأ صندوق وطني لدعم الضحايا وتأهيلهم.

المادة 6: تُنشأ نيابات متخصصة في كل

محافظة.

المادة 7: يُلزم كل مزوّد خدمة بحفظ سجلات الدخول لمدة سنتين.

هذا النموذج يمكن أن يُعتمد كأساس تشريعي موحد في الدول العربية.

الفصل السادس والثلاثون

الرقمنة القضائية وضمانات العدالة

العدالة الرقمية لا تعني استبدال القاضي بالآلة، بل تمكينه بالأدوات الحديثة دون أن يفقد إنسانيته.

المحاكم الرقمية يجب أن تحافظ على حق الدفاع الشفهي، وحق الاستئناف، وحق مواجهة

الشـهود.

كما يجب أن تكون أنظمة التقاضي الإلكتروني مفتوحة المصدر، قابلة للمراجعة من قبل خبراء مستقلين، لضمان الشـفافية.

الهدف ليس السـرعة فقط، بل العدالة الكاملة في عالم رقمي.

الفصل السـابع والثلاثون

المسـؤولية الدولية المشـتركة

الجريمة الرقمية لا تحترم الحدود، فلا يمكن لأي دولة أن تحمي نفسـها وحدها.

المطلوب هو مبدأ "المسـؤولية الدولية المشـتركة"، حيث تتعاون الدول في:

- تبادل المعلومات الاستخباراتية.

- تدريب الكوادر المشتركة.

- تنفيذ الأحكام القضائية عبر الحدود.

- مصادرة الأصول الرقمية للمجرمين أينما وجدت.

هذا التعاون يجب أن يُرسّخ في معاهدات ثنائية ومتعددة الأطراف، مع آليات تنفيذ فورية.

الفصل الثامن والثلاثون

الجوانب الاقتصادية لتمويل الجرائم الرقمية

القراصنة لا يعملون من فراغ، بل يمولون شبكاتهم عبر غسيل الأموال الرقمي، باستخدام

العملات المشفرة والمحافظ الافتراضية.

الدول العربية يجب أن تُدخل "الجرائم المالية الرقمية" ضمن نطاق وحدات مكافحة غسل الأموال.

كما يجب إلزام منصات العملات المشفرة بالتحقق من هوية المستخدمين (KYC) وتقديم تقارير مشبوهة للسلطات.

الاقتصاد الرقمي يجب أن يكون شفافاً، وإلا أصبح ساحة للفساد والإجرام.

الفصل التاسع والثلاثون

مستقبل العدالة في عالم لا حدود فيه

في المستقبل القريب، ستُحاكم الجرائم التي

تُرتكب في الفضاء الافتراضي (Metaverse) بنفس الجدية التي تُحاكم بها الجرائم الواقعية.

القضاة سيحتاجون إلى فهم عوالم ثلاثية الأبعاد، والعقود الذكية، والهويات الرقمية اللامركزية.

التحدي الأكبر هو الحفاظ على "الروح الإنسانية" في العدالة، وسط طوفان التكنولوجيا.

القانون يجب أن يسبق الجريمة، لا أن يلاحقها.

الفصل الأربعون

خاتمة فلسفية: القانون، الفن، والجمال في مواجهة الوحشية الرقمية

القانون ليس مجرد نصوص جافة، بل تعبير عن جمال العدالة وتناغمها مع الفطرة الإنسانية.

الوحشية الرقمية تحاول أن تجعل الإنسان مجرد بيانات قابلة للاستغلال.

لكن القانون، حين يُمارس بفن وجمال، يعيد للإنسان كرامته، ويحمي روحه من التفتت في عالم البتات والبايتات.

هذا الكتاب، بكل فصل فيه، هو دعوة إلى بناء عالم رقمي إنساني، لا يُقدّس التكنولوجيا، بل يُخضعها لخدمة الحق والعدل.

والله وليّ التوفيق.

قائمة المراجع

اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية، نيويورك 2000

اتفاقية بودابست لمكافحة الجرائم الإلكترونية، 2001

الدستور الجزائري لسنة 2020

الدستور المصري لسنة 2014

الشريعة الإسلامية، القرآن الكريم والسنة النبوية الشريفة

القانون رقم 15-19 الجزائري المتعلق بالوقاية من الاتجار بالبشر، 2015

القانون رقم 175 لسنة 2018 المصري لمكافحة الجرائم الإلكترونية

المجلة الجنائية الفرنسية، أحكام محكمة النقض، 2020–2025

تقرير البنك الدولي حول الاقتصاد الرقمي، 2025

تقرير الإنتربول السنوي للجرائم الإلكترونية، 2024

تقرير اليونيسف حول حماية الأطفال في الفضاء الرقمي، 2024

جريدة المحكمة العليا الجزائرية، القرار رقم 2024/214

جريدة رسمية فرنسية، قانون العقوبات، المادة 14-225

محكمة النقض المصرية، الطعن رقم 18452 لسنة 92 ق

محكمة النقض المصرية، الطعن رقم 9876 لسنة

90 ق

محكمة النقض المصرية، الطعن رقم 11200 لسنة 91 ق

مجلة جامعة القاهرة للقانون والاقتصاد، مجلد 45، 2024

مجلة القانون المقارن، باريس، 2023

منظمة العفو الدولية، تقرير حول الخصوصية الرقمية، 2025

وحدة مكافحة الجرائم الإلكترونية – وزارة الداخلية المصرية، تقارير داخلية 2023–20 .:

الفهرس الموضوعي

جميع الحقوق محفوظة

© د. محمد كمال عرفة الرخاوي

الباحث والمستشار القانوني – المحاضر الدولي في القانون – الخبير الدولي والفقيه والمؤلف القانوني

يُمنع نسخ هذا الكتاب أو اقتباس أي جزء منه أو طباعته أو نشره أو توزيعه أو ترجمته أو استخدامه بأي شكل أو وسيلة — إلكترونية كانت أو ميكانيكية، بما في ذلك التصوير والتسجيل — دون إذن خطي مسبق من المؤلف.

أي مخالفة لهذا الشرط تُعرض مرتكبها للمساءلة القانونية بموجب قوانين الملكية الفكرية الوطنية والدولية.

الطبعة الأولى: 2026