الجريمة في زمن العولمة الرقمية: تحولات عميقة وتحديات مستعصية

مراجعة مقال Subject Rview

م.م. أمير علي هادي

amer.ali@uokerbala.edu.iq

جامعة كربلاء/ كلية التربية للعلوم الانسانية

الملخص

شهدت العقود الأخيرة تحولات جذرية بفعل العولمة الرقمية، التي غيرت طبيعة الجريمة بشكل جذري. لم تعد الجرائم محلية أو محدودة بالحدود الجغرافية، بل أصبحت عابرة للقارات ومعقدة، مستفيدة من التكنولوجيا والإنترنت والهواتف الذكية. من أبرز مظاهر هذه الجرائم: الجريمة المنظمة العابرة للحدود، الجرائم الإلكترونية، الاتجار بالبشر، وغسيل الأموال. وبالتالي أصبحت مكافحة هذه الجرائم تحديًا كبيرًا بسبب صعوبة تتبعها، فوضى التشريعات القانونية بين الدول، ضعف التنسيق الدولي، التطور التكنولوجي السريع، العوامل الاقتصادية والاجتماعية، والطبيعة العابرة للحدود لهذه الجرائم. ومع ذلك، يمكن الحد من آثارها عبر استراتيجيات ذكية تشمل التعاون الدولي الفعال، توحيد وتطوير التشريعات، توظيف التكنولوجيا كأداة دفاعية وهجومية، تعزيز التوعية المجتمعية، وتطوير كوادر متخصصة قادرة على التعامل مع التحديات الرقميةز

الكلمات المفتاحية: الجريمة، العولمة، التحول الرقمي.

Crime in the Age of Digital Globalization: Profound Transformations and Intractable Challenges

M.M. Amir Ali Hadi

University of Karbala / College of Education for Human Sciences / Department of Educational and Psychological Sciences

Abstract

The last few decades have witnessed radical transformations due to digital globalization, which has fundamentally altered the nature of crime. Crimes are no longer local or confined by geographical boundaries, but have become

transnational and complex, leveraging technology, the internet, and smartphones. Among the most prominent manifestations of these crimes are transnational organized crime, cybercrime, human trafficking, and money laundering. Combating these crimes has become a major challenge due to the difficulty of tracking them, the disparity in legal frameworks between countries, weak international coordination, rapid technological development, economic and social factors, and the transnational nature of these crimes. However, their impact can be mitigated through smart strategies that include effective international cooperation, harmonizing and developing legislation, employing technology as a defensive and offensive tool, enhancing community awareness, and developing specialized personnel capable of addressing digital challenges.

Keywords: Crime, Globalization, Digital Transformation

المقدمة

منذ مطلع التسعينات، والعالم يعيش حالة من التكثيف المتسارع لما بات يعرف بالعولمة، وهذه الظاهرة التي بدأت كحلم بقرية كونية واحدة، سرعان ما كشفت عن وجهها الآخر لم تعد الحدود الجغرافية تشكل عائقاً أمام حركة السلع والأفكار فقط، بل أصبحت أيضاً ممرات مفتوحة لأنماط جديدة من النشاط الإجرامي. ولعل المفارقة الأكثر إيلاماً تكمن في أن الأدوات ذاتها التي جعلت العالم أكثر تواصلاً وانفتاحاً، هي نفسها التي وفرت للجريمة غطاءً من التعقيد والإفلات من الملاحقة، فلم يعد المجرم ذلك الشخص الذي نعرفه في أفلام الأبيض والأسود، بل تحول إلى كيان افتراضي قد يعبر القارات بضغطة زر، مخلفاً وراءه ملايين الضحايا دون أن تغادر قدماه غرفته، لذلك لم يعد مقاربة ظاهرة الجريمة اليوم ممكنة من خلال عدسات علم الإجرام التقليدي وحدها، نحن اليوم إزاء تحول جذري يتطلب منا إعادة التفكير في كل شيء من تعريف الجريمة ذاتها، وصولاً إلى آليات مكافحتها على المستويين المحلي والدولي.

أولًا: مفهوم الجريمة في ظل العولمة الرقمية:

عند النظر إلى الجريمة في سياق العولمة، يمكن القول إنها لم تعد محصورة داخل حدود دولة واحدة، بل أصبحت نشاطًا يتجاوزها بسهولة، ويرتبط ذلك ارتباطًا وثيقًا بالتطور التكنولوجي المتسارع، إلى جانب سهولة التنقل والتواصل بين مختلف أنحاء العالم، فالتطور التكنولوجي وتحديداً انتشار الإنترنت فائق السرعة والهواتف الذكية حول الجريمة إلى صناعة عالمية، صحيح أن جرائم تقليدية كالسرقة والسطو لا تزال قائمة، لكن اللافت هو ذلك التحول النوعي نحو جرام أكثر تعقيداً مثل الجرائم الإلكترونية التي تستهدف البنى التحتية، والاتجار بالبشر الذي أصبح تجارة مربحة تفوق تجارة السلاح في بعض المناطق، وعمليات غسل الأموال التي تجيد التخفي خلف متاهات من الشركات الوهمية والحسابات المشفرة. ما يزيد

الطين بلة هو صعوبة تتبع هذه الجرائم. ففي الماضي، كان المحقق يحتاج إلى بصمات أو شهود. الآن، يحتاج إلى فريق من خبراء التكنولوجيا الماليين والمحللين الرقميين، وكل ذلك في سباق مع الزمن قبل أن تتبدد الأدلة في الفضاء الإلكتروني.

ثانيًا: مظاهر الجريمة في زمن العولمة الرقمية:

١. **الجريمة المنظمة:** لم تعد هذه الجريمة تقتصر على العائلات الإجرامية التقليدية التي شاهدناها في أفلام هوليوود، لقد ظهرت شبكات جديدة تعمل بتنسيق عالٍ، تمتد خيوطها من أميركا اللاتينية إلى أوروبا مروراً بإفريقيا وآسيا وهذه الشبكات تتاجر بالمخدرات والأسلحة وتستغل بدورها أي ثغرة في الحدود أو في التنسيق الأمني بين الدول، لكن الأخطر بلا شك هو ذلك العالم الموازي الذي نسميه "الإنترنت المظلم"، إذ يمكن للمرء أن يشتري أي شيء أسلحة، مخدرات، بطاقات ائتمان مسروقة، بل وحتى خدمات قراصنة محترفين لاختراق أي هدف، كل ذلك بعملات رقمية مشفرة، يصعب تتبعها، وتحت غطاء من إخفاء الهوية يجعل من المستحيل تقريباً كشف هوية الأطراف المتعاملة.

٢. **جريمة الاتجار بالبشر:** ولا يمكننا هنا تجاهل هذه جريمة التي تمثل وصمة عار في جبين الإنسانية، إذ إنها ليست مجرد جريمة عابرة للحدود، بل هي انتهاك صارخ لكرامة الإنسان، تحوله إلى سلعة تباع وتشترى في سوق سوداء عالمية، فالمهاجرون، الفقراء، والأطفال هم الأكثر عرضة لهذه الشبكات التي تجيد استغلال الأحلام واليأس في آن معاً.

٣. **غسيل الأموال:** فهو ذلك الشريان الذي يغذي كل هذه الأنشطة، فهو عملية معقدة تهدف إلى تبييض الأموال القذرة، وإضفاء الشرعية عليها عبر استثمارات وهمية وحسابات مصرفية معقدة، وكلما تطورت تقنيات المراقبة المصرفية، ابتكر المجرمون طرقاً أكثر دهاءً للالتفاف عليها.

ثالثًا: لماذا أصبحت مكافحة الجريمة أقرب إلى المستحيل؟

إذا كنت تتساءل لماذا لا تزال الجريمة متفشية رغم كل التطور التكنولوجي والأمني، فالإجابة تكمن في سلسلة من التحديات المترابطة التي تجعل من مكافحتها معركة غير متكافئة، يمكن تلخيص أبرز هذه التحديات على النحو التالي:

١. **صعوبة التتبع والملاحقة** في الماضي، كان المحقق يعتمد على الأدلة المادية مثل البصمات أو الشهود لتحديد هوية الجاني، اليوم الجريمة أصبحت رقمية ومعقدة، تخيل مجرمًا يسرق بيانات ملايين البطاقات البنكية، ويبيعها على الإنترنت المظلم خلال دقائق، ثم يحول الأموال إلى عملات رقمية ويوزعها على محافظ إلكترونية متعددة في دول مختلفة. وعند اكتشاف الضحية للسرقة، تكون الأموال قد اختفت تمامًا في شبكة معقدة من المعاملات الرقمية، لا يمكن اختراقها بسهولة، وهذا يجعل جهود الشرطة التقليدية في التتبع والملاحقة غير كافية، ويتطلب تدخل فرق متخصصة في التحليل الرقمي والأمن السيبراني، وفي سباق دائم مع الزمن قبل أن تختفي الأدلة الرقمية نهائيًا.

٢. **فوضى الأنظمة القانونية:** أن اختلاف التشريعات بين الدول يشكل عقبة ضخمة ما يعتبر جريمة في دولة معينة قد يكون قانونيًا أو مخالفة بسيطة في دولة أخرى، وهذا الاختلاف يسمح للمجرمين بالتحرك بحرية مستغلين الثغرات القانونية بين الدول المختلفة، فعلى سبيل المثال بعض الدول يمكن أن تصبح "ملاذات آمنة" للمجرمين الدوليين، ليس لأنها تشجع الإجرام، بل لأنها لم تطور تشريعاتها الرقمية بعد أو لأنها تفتقر إلى الإرادة السياسية للتعاون مع الدول الأخرى، كما أن تنازع الاختصاصات القضائية يطرح سؤالًا معقدًا: أي دولة لها الحق في محاكمة الجاني؟ الدولة التي يعيش فيها؟ أم الدولة التي حدثت فيها الجريمة؟ أو الدولة التي تقع فيها الخوادم الرقمية؟ هذه الفوضى القانونية تزيد من صعوبة تحقيق العدالة بسرعة وفعالية.

٣. **فشل التنسيق الدولي:** رغم وجود مؤسسات دولية مثل الإنتربول، إلا أن التعاون بين الدول لا يزال متأثرًا بالاعتبارات السياسية والدبلوماسية، لأن بعض الدول ترفض تسليم المطلوبين لأسباب سياسية، بينما تتردد أجهزة الأمن في مشاركة معلومات حساسة خوفًا من تسريبها، وكل هذا يمنح المجرمين مساحة كبيرة للتحرك بحرية، وكأنهم "طيور مهاجرة" تتنقل دون قيود، ما يجعل بعض الدول فعليًا ملاذًا آمنًا لهم، ويعقد عمل الأجهزة الأمنية في متابعة الجرائم العابرة للحدود.

٤. **التطور التكنولوجي السريع:** التكنولوجيا أوجدت أدوات جديدة للجريمة لا يستطيع القانون التقليدي مجاراتها بسهولة، فالمجرمون اليوم يستخدمون الذكاء الاصطناعي لتزوير الهويات، أو إنشاء مقاطع فيديو مزيفة، بالإضافة إلى الهجمات الإلكترونية المؤتمتة التي يمكن أن تعطل أنظمة مالية أو حكومية بالكامل. أما التشريعات التقليدية، فهي تستغرق سنوات لتعديل نفسها لمواكبة هذه الابتكارات، ما يمنح المجرمين دائمًا خطوة أمام القانون، ويجعل حماية المجتمعات من هذه الجرائم أمرًا بالغ الصعوبة.

٥. **العوامل الاقتصادية والاجتماعية:** الظروف الاقتصادية الصعبة تزيد من هشاشة المجتمع أمام الجريمة. الفقر، البطالة، والفرص المحدودة تدفع الشباب للانخراط في أنشطة غير مشروعة، سواء عبر التهريب، تجارة المخدرات، أو المشاركة في هجمات إلكترونية لتحقيق مكاسب سريعة. بالإضافة لذلك، قلة الوعي الرقمي لدى بعض الأفراد تجعلهم هدفًا سهلًا للاستغلال في الجرائم الرقمية، مثل الابتزاز الإلكتروني أو الاحتيال المالي عبر الإنترنت.

٦. **الطبيعة العابرة للحدود:** شبكات الجريمة الحديثة لا تعرف الحدود. عندما تمتد شبكات من كولومبيا إلى أوروبا مرورًا بغرب إفريقيا، يصبح محاربتها أشبه بمحاربة وحش متعدد الرؤوس؛ فالقضاء على جزء واحد لا يعني القضاء على الشبكة بأكملها. هذه العمليات تشمل جمع البيانات، الهجمات الإلكترونية، تحويل الأموال، أو الاتجار بالبشر، مما يتطلب استجابة دولية متكاملة تعتمد على التعاون الوثيق بين الدول والمنظمات الدولية.

رابعاً: كيف نواجه وحشاً بلا حدود؟

السؤال المحوري الآن: هل نحن عاجزون حقاً أمام هذه الظاهرة؟ الإجابة ليست بيضاء أو سوداء. هناك أمل، لكنه أمل مشروط بتبني استراتيجيات ذكية ومبتكرة ومن هذه السبل والاستراتيجيات لمواجهة الجريمة هي على النحو التالي:

٧. **تعزيز التعاون الدولي والاستخباراتي:** لا بديل عن تعاون دولي حقيقي. ليس التعاون الشكلي الذي نراه في المؤتمرات والندوات، بل تعاون استخباراتي يومي، حيث أن تفعيل اتفاقيات تسليم المجرمين بسرعة، وإنشاء قواعد بيانات دولية موحدة يمكن الرجوع إليها فورياً عند الاشتباه بأي حركة مشبوهة للمجرمين عبر الحدود. هذا يتطلب تجاوز الأنانية الوطنية، والاقتناع بأن أمن أي دولة هو جزء من الأمن الجماعي. وهذا الأمر يقلل من الفرص التي يستغلها المجرمون للهروب من العدالة، وإنشاء قواعد بيانات دولية موحدة تسمح بمشاركة المعلومات في الوقت الفعلي، بحيث يمكن متابعة تحركات العناصر الإجرامية عبر المطارات والموانئ والمنافذ الحدودية بشكل مباشر، وتطوير أنظمة إنذار مبكر تعتمد على التعاون الاستخباراتي لتبادل التحذيرات حول التهديدات الإلكترونية والهجمات المحتملة قبل وقوعها، كما يمكن للعلاقات الدبلوماسية القوية بين الدول أن تلعب دوراً محورياً في تذليل العقبات السياسية التي قد تعيق التعاون، وهو ما يخلق بيئة دولية أقل ملاذاً آمناً للمجرمين.

٨. **يجب توحيد التشريعات وتطويرها:** لا يمكن لدولة أن تبقى متخلفة عن ركب التشريعات الرقمية. يجب أن تعترف القوانين بمفاهيم جديدة كالأصول الرقمية، والجرائم السحابية، والإرهاب الإلكتروني، والأهم من ذلك العمل على تقريب التشريعات بين الدول بحيث لا توجد "جنة قانونية" يمكن للمجرمين الاختباء فيها. فالعقوبات يجب أن تكون رادعة، لكن أيضاً يجب أن تكون قابلة للتنفيذ عبر الحدود. على سبيل المثال، يجب أن تشمل التشريعات الحديثة مفاهيم مثل "الأصول الرقمية"، و"الهجمات السحابية"، و"الإرهاب السيبراني"، بحيث يمكن تصنيف أي نشاط إجرامي يتعلق بهذه المجالات كجريمة يعاقب عليها القانون، كما أن العمل على الاتفاقيات الإطارية الدولية لتوحيد تعريف الجريمة عبر الدول يمكن أن يمنع المجرمين من استغلال التباين القانوني بين دولة وأخرى، ويخلق أرضية قانونية متسقة، ويجب أن تكون هذه التشريعات مرنة بما يكفي لتواكب الابتكارات المستقبلية، مثل استخدام تقنيات الذكاء الاصطناعي في الجرائم، أو الهجمات الإلكترونية المركبة، بحيث لا تتطلب كل جريمة جديدة تعديلاً تشريعياً كبيراً، مما يقلل الوقت الذي يستغرقه القانون لمواكبة التطورات الإجرامية.

٩. **استخدام التكنولوجيات كدرع وسلاح:** لماذا لا نستخدم الذكاء الاصطناعي لرصد الأنماط الإجرامية قبل وقوعها؟ في عصر تتسارع فيه الابتكارات التقنية بشكل مذهل، أصبح استخدام التكنولوجيا أداة دفاعية وهجومية في الوقت نفسه لمواجهة الجريمة المعولمة، ويشمل ذلك توظيف الذكاء الاصطناعي لتحليل الأنماط الإجرامية والتنبؤ بالمخاطر قبل وقوعها، بحيث يمكن لأجهزة الأمن استباق الجرائم الإلكترونية أو الجرائم المنظمة، كما يمكن الاستفادة من تقنية البلوكشين لتأمين السجلات الحيوية وسلاسل التوريد، ومنع التلاعب أو التهريب، حيث توفر هذه التقنية سجلاً رقمياً ثابتاً وشفافاً يصعب تغييره أو تزويره، بالإضافة

إلى تطوير أنظمة مراقبة مالية متقدمة قادرة على رصد عمليات غسل الأموال والتمويل غير المشروع بشكل تلقائي فور ظهور أي سلوك مالي مشبوه، مما يساهم في كشف الجرائم قبل أن تتحول إلى عمليات كبيرة ومعقدة.

١٠.**التوعية المجتمعية والتحصين الداخلي:** الفرد غالباً ما يكون الحلقة الأضعف في سلسلة الجرائم الحديثة، خاصة في الجرائم الرقمية التي تعتمد على الهندسة الاجتماعية والاحتيال النفسي، لذلك فإن نشر ثقافة الوعي الأمني الرقمي في المدارس والجامعات والمؤسسات الحكومية والخاصة يصبح أمراً حيوياً، حيث يمكن للبرامج التوعوية المتقدمة تعليم الأفراد كيفية حماية بياناتهم الشخصية، والتعامل بحذر مع الرسائل والمكالمات المشبوهة، بالإضافة إلى تنظيم حملات إعلامية تهدف إلى رفع مستوى فهم المجتمع لمخاطر الابتزاز الإلكتروني والقرصنة، مما يقلل من نجاح محاولات المجرمين في استغلالهم، ويعزز من قدرة المجتمع على الصمود أمام الهجمات الرقمية المتقدمة.

١١.**تطوير الكوادر رقمية متخصصة:** أن تطوير القدرات البشرية أصبح ضرورة ملحة لمواجهة الجريمة المعولمة، حيث يجب تحويل رجل الأمن التقليدي إلى محقق رقمي قادر على تحليل الأدلة الرقمية واختراق الشبكات الإجرامية من الداخل، بالإضافة إلى الاستثمار في وحدات خاصة مدربة على التعامل مع الإنترنت المظلم واستخدام التقنيات الحديثة لفك الشفرات وتحليل البيانات المشفرة، كما يمكن للعلاقات الاستراتيجية بين القطاع العام والقطاع الخاص أن تعزز القدرة على صد الهجمات المعقدة من خلال تبادل الخبرات وتطوير أدوات مبتكرة، وهو ما يخلق جيشاً من الخبراء الرقميين القادرين على التصدي للتهديدات المستقبلية بشكل أكثر فاعلية وكفاءة.

التوصيات

١. يجب العمل على تعزيز التعاون الاستخباراتي اليومي بين الدول، بعيدًا عن مجرد المشاركة الشكلية في المؤتمرات والندوات. الهدف هو تحقيق تبادل معلوماتي استخباراتي فوري وفعّال يتيح التصرف بسرعة حيال التهديدات المحتملة.

٢. كما ينبغي إنشاء قواعد بيانات دولية موحدة، تسهّل تتبع تحركات العناصر الإجرامية عبر المنافذ الحدودية والموانئ، مما يعزز قدرة السلطات على الاستجابة لأي نشاط مشبوه بشكل دقيق وسريع.

٣. في الوقت نفسه، من الضروري تطوير أنظمة إنذار مبكر لرصد التهديدات السيبرانية والهجمات الإلكترونية قبل وقوعها، مما يمنح الجهات المختصة هامش تصرف أكبر لحماية البنية التحتية الحيوية.

٤. ولا يمكن تجاهل الدور الحيوي للعلاقات السياسية القوية في تسهيل اتفاقيات تسليم المجرمين، ومنع ظهور ملاذات آمنة لهم، وهو ما يعزز الأمن على المستوى الدولي.

٥. كما يجب تحديث القوانين لتواكب الابتكار والتقدم، مع إدخال مفاهيم حديثة تشمل الأصول الرقمية، الجرائم السحابية، والإرهاب السيبراني ضمن الإطار العقابي.

٦. على صعيد مالي، ينبغي إنشاء أنظمة متقدمة لرصد عمليات غسل الأموال والتمويل غير المشروع بشكل تلقائي وفوري، لضمان استقرار الأنظمة الاقتصادية ومنع استغلالها في أنشطة إجرامية.

٧. وأخيرًا، لا بد من إدراج التوعية بالأمن الرقمي في المناهج الدراسية والجامعية، لتجهيز الأفراد بالمعرفة والأدوات اللازمة لحماية أنفسهم من الابتزاز والاحتيال الإلكتروني.

المصادر

١. حاتم عبد الرحمن منصور الشحات: الإجرام المعلوماتي، دار النهضة العربية، مصر، ٢٠٠٣.

٢. جميل عبد الباقي الصغير، القانون الجنائي والتكنولوجيا الحديثة، الكتاب الأول من الجرائم الناشئة عن استخدام الحاسب الآلي، دار النهضة العربية، القاهرة، مصر، ٢٠١٢.

٣. محسن الخضيري، غسيل الأموال الظاهر والأسباب والعلاج، مجموعة النيل العربية، بيروت، لبنان، ٢٠٠٠٣.

4. Almohammadi, A. (2021). Basic Concepts of Digital Transformation, Digital Government Authority, Riyadh, Saudi Arabia.

5. martin (d) ,la criminalite informatique , cybercrime: sabotage, piratage.. ect . evolution jet repression, paris, puf .1ed ,1997.