قمة قطر الأولى للذكاء الاصطناعي والتميز المؤسسي

" نحو مؤسسات أكثر ذكاءً وكفاءةً واستدامة "

25-26 سبتمبر 2026 | الدوحة – دولة قطر

المسؤولية الجنائية عن جرائم بطاقات الدفع الإلكتروني والاحتيال المالي المدعوم بالذكاء الاصطناعي: دراسة قانونية مقارنة في ضوء التشريعات الوطنية والاتفاقيات الدولية والوقائع الجنائية المعاصرة

بحث علمي مقدم لقمة قطر الأولى للذكاء الاصطناعي والتميز المؤسسي

إعداد الباحث: علي أحمد محمد أحمد الإبراهيم

استشاري في مجال التقييم بالمدارس الحكومية بوزارة التربية والتعليم والتعليم العالي بدولة قطر

حاصل على درجة الماجستير في القانون، تخصص العدالة الجنائية الدولية، مسار مكافحة الجريمة السيبرانية والإلكترونية

باحث متخصص في جرائم بطاقات الدفع الإلكتروني والأمن السيبراني والتشريعات القانونية المرتبطة بها

اعتماد الملف العلمي

رئيس اللجنة العلمية – قمة قطر الأولى للذكاء الاصطناعي والتميّز المؤسسي

د. أمل علاونة

سبتمبر 2026

فهرس المحتويات

الإطار العلمي والمشكلة البحثية 3
أولاً: التحول في طبيعة الجريمة المالية 3
ثانياً: المؤشرات الدولية 3
ثالثاً: مشكلة البحث 4
رابعاً: أهداف البحث 4
خامساً: منهج البحث 4
الإطار النظري والتحليل القانوني المقارن 6
1. التنظيم الجنائي للاحتيال المالي وجرائم بطاقات الدفع في القانون القطري 6
2. المقارنة العربية: المملكة العربية السعودية وجمهورية مصر العربية 8
3. الولايات المتحدة الأمريكية وكندا: المسؤولية الجنائية عن الاحتيال المالي ووسائل الوصول الإلكتروني 12
4. (ألمانيا وفرنسا وسويسرا): التمييز بين الاحتيال على الإنسان والاحتيال على أنظمة معالجة البيانات 15
5. أستراليا والاتحاد الأوروبي: الحماية الجنائية لبيانات الدفع والوسائل المالية غير المادية 20
6. الاتفاقيات الدولية والأدلة الإلكترونية والتعاون الجنائي عبر الحدود 22
7. الإنتربول ومكتب التحقيقات الفيدرالي: العمليات الدولية والإحصاءات المالية 26
8. الوقائع الجنائية المعاصرة والتطبيق القانوني المقارن 30
النتائج القانونية والتوصيات التشريعية 35
أولاً: النتائج 35
ثانياً: التوصيات 37
الخاتمة 39
المراجع التشريعية والدولية الأساسية 45
أولاً: التشريعات الوطنية 45
ثانياً: الاتفاقيات والتشريعات الدولية 45
ثالثاً: التقارير والوقائع الدولية 46

الإطار العلمي والمشكلة البحثية

أولاً: التحول في طبيعة الجريمة المالية

أحدثت تقنيات الذكاء الاصطناعي تحولاً في أساليب ارتكاب الجرائم المالية الرقمية، ولا سيما من خلال محاكاة الأصوات وإنتاج الصور والمقاطع المرئية الاصطناعية. فلم يعد الاستيلاء على الأموال مرتبطاً بالضرورة بسرقة بطاقة مصرفية أو اختراق نظام بنكي؛ إذ يمكن للجاني انتحال هوية شخص يملك صلاحية التصرف المالي، وإقناع موظف مختص بتنفيذ تحويل مصرفي بناءً على تعليمات مزيفة.

ويثير هذا التطور إشكالية تتعلق بتحديد محل الاعتداء الجنائي؛ فقد يستهدف الجاني إرادة الشخص المخول بالتصرف، أو نظام معالجة البيانات، أو وسيلة الدفع الإلكتروني ذاتها.

وقد كشفت واقعة الاحتيال التي أعلنت عنها سلطات هونغ كونغ سنة 2024 عن خطورة هذا النمط، بعدما استُخدمت تقنيات التزييف العميق في اجتماع مرئي انتحل فيه الجناة شخصيات مسؤولين داخل مؤسسة، وترتبت عليه تحويلات مالية بلغت نحو 200 مليون دولار هونغ كونغي.

وتبرز أهمية الواقعة في أن التحويلات صدرت عن موظف مخول بتنفيذها، إلا أن قراره تأثر بخداع قائم على هوية اصطناعية.

ثانياً: المؤشرات الدولية

أورد تقرير مركز شكاوى جرائم الإنترنت الأمريكي IC3 لعام 2025 بيانات عن شكاوى تضمنت معلومات بشأن استخدام الذكاء الاصطناعي، بلغ عددها 22,364 شكوى، مع خسائر مبلغ عنها تقارب 893.3 مليون دولار أمريكي.

كما أشار تقييم الإنتربول العالمي لتهديد الاحتيال المالي لعام 2026 إلى تقديرات تفيد بأن الاحتيال المعزز بالذكاء الاصطناعي قد يكون أكثر ربحية بنحو 4.5 أضعاف مقارنة بأساليب غير معززة بهذه التقنية.

ولا تمثل هذه المؤشرات أحكاماً قضائية بثبوت الجرائم، بل تعكس بيانات شكاوى وتقديرات تتعلق بطبيعة التهديد المالي.

ثالثاً: مشكلة البحث

تتمثل مشكلة البحث في تحديد مدى استيعاب التشريعات الجنائية القائمة لصور الاحتيال المالي المدعوم بالذكاء الاصطناعي، خاصة عندما يتحقق الاستيلاء على الأموال نتيجة تضليل شخص مخول بالتصرف، دون اختراق النظام المصرفي أو الحصول على بيانات بطاقة دفع إلكتروني.

وينبثق عن ذلك التساؤل الرئيسي:

ما الأساس القانوني لتحديد المسؤولية الجنائية عن الاحتيال المالي المدعوم بالذكاء الاصطناعي، وكيف يمكن التمييز بين جرائم الاحتيال الإلكتروني والاحتيال الحاسوبي وجرائم بطاقات الدفع في التشريعات المقارنة.

رابعاً: أهداف البحث

يهدف البحث إلى تحليل النصوص الجنائية المنظمة للاحتيال الإلكتروني وجرائم بطاقات الدفع، وبيان الفروق بين تضليل الإنسان والتلاعب بمعالجة البيانات، ومقارنة التشريعات القطرية والعربية والأجنبية، ودراسة دور الاتفاقيات الدولية والإنتربول في مكافحة الجرائم المالية العابرة للحدود.

كما يسعى إلى اقتراح معيار قانوني يساعد على تحديد النص الجنائي المنطبق على صور الاحتيال المستحدثة.

خامساً: منهج البحث

يعتمد البحث المنهج التحليلي لدراسة النصوص الجنائية، والمنهج المقارن لبيان أوجه الاتفاق والاختلاف بين التشريعات، ومنهج دراسة الوقائع لتطبيق القواعد القانونية على حوادث احتيال معلنة.

وتنطلق الدراسة من فرضية مفادها أن حداثة وسيلة ارتكاب الجريمة لا تعني بالضرورة غياب النص الجنائي، وأن التكييف الصحيح يتطلب تحديد الفعل ومحل الاعتداء وأركانه قبل النظر في التقنية المستخدمة.

المراجع الأساسية: تقرير FBI–IC3 لعام 2025؛ تقييم الإنتربول العالمي لتهديد الاحتيال المالي لعام 2026؛ البيانات الرسمية لسلطات هونغ كونغ بشأن واقعة التزييف العميق.

الإطار النظري والتحليل القانوني المقارن

1. التنظيم الجنائي للاحتيال المالي وجرائم بطاقات الدفع في القانون القطري

أولاً: الإطار التشريعي

تخضع الجرائم المالية الرقمية في دولة قطر لأحكام تشريعية متعددة، من أهمها:

القانون رقم (14) لسنة 2014 بإصدار قانون مكافحة الجرائم الإلكترونية.

القانون رقم (11) لسنة 2004 بإصدار قانون العقوبات.

ويقتضي التطبيق القانوني تحديد النص الذي يستوعب الفعل المرتكب، دون افتراض أن استخدام وسيلة إلكترونية يؤدي تلقائياً إلى تطبيق جميع النصوص المتعلقة بالجرائم المعلوماتية.

ثانياً: المادة (11) من قانون مكافحة الجرائم الإلكترونية

تعالج المادة (11) صوراً من انتحال الهوية والاستيلاء على المال باستخدام الوسائل التقنية، وفق الأفعال والشروط التي يحددها النص.

وتقرر عقوبة تصل إلى الحبس ثلاث سنوات والغرامة مائة ألف ريال قطري، أو إحدى هاتين العقوبتين.

وتكتسب هذه المادة أهمية خاصة في حالات استخدام الذكاء الاصطناعي لمحاكاة صوت شخص أو صورته، ثم استعمال الهوية الاصطناعية لخداع موظف مصرفي أو مسؤول مالي.

غير أن مجرد إنتاج صوت اصطناعي لا يكفي وحده لإثبات الجريمة؛ إذ يتعين تحديد السلوك المجرّم، والقصد الجنائي، ومدى تحقق العناصر الأخرى التي يتطلبها النص.

ثالثاً: المادة (12) من القانون ذاته

تتناول المادة (12) جرائم مرتبطة ببطاقات التعامل الإلكتروني وبياناتها، بما في ذلك صور الحصول غير المشروع على البيانات والتزوير والاستعمال وفق الحالات التي تحددها.

وتصل العقوبة إلى الحبس ثلاث سنوات والغرامة مائتي ألف ريال قطري، أو إحدى العقوبتين.

وتظهر أهمية هذه المادة عند استخدام رسائل تصيد إلكتروني مولدة بالذكاء الاصطناعي للحصول على بيانات بطاقات الدفع.

لكن يجب التمييز بين استخدام الذكاء الاصطناعي في صياغة رسالة احتيالية وبين تحقق الجريمة المنصوص عليها في المادة؛ فالعبرة باستيفاء عناصر الفعل المحظور قانوناً.

رابعاً: التمييز بين المادتين (11) و(12)

إذا انتحل الجاني شخصية المدير المالي وأقنع موظفاً بتحويل أموال، فإن البحث يبدأ من النصوص المتعلقة بالاحتيال وانتحال الهوية.

أما إذا حصل الجاني دون حق على بيانات بطاقة مصرفية واستخدمها في عمليات دفع، فيقتضي الأمر فحص النصوص الخاصة ببطاقات التعامل الإلكتروني.

وقد تتعدد الأفعال في الواقعة الواحدة، إلا أن اجتماع النصوص يتوقف على تحقق أركان كل جريمة وقواعد التعدد المقررة قانوناً.

خامساً: قانون العقوبات القطري

تُعد المواد (381–384) من قانون العقوبات القطري ذات صلة بالبحث في الاعتداءات المرتبطة ببطاقات التعامل الإلكتروني.

غير أن تطبيقها يتطلب مطابقة الوقائع مع الأفعال المحددة في كل مادة، والتحقق من العلاقة بينها وبين النصوص الواردة في قانون مكافحة الجرائم الإلكترونية.

ولا يجوز افتراض أن جميع هذه المواد تتناول الفعل ذاته أو تقرر العقوبة نفسها.

سادساً: الإشكالية التطبيقية

إذا استخدم شخص صورة وصوتاً اصطناعيين لانتحال شخصية صاحب حساب مصرفي، وأقنع موظفاً بإجراء تحويل مالي دون الحصول على بيانات البطاقة، فإن المسألة القانونية لا تتعلق بمجرد إثبات استخدام الذكاء الاصطناعي.

بل تتطلب الإجابة عن الأسئلة الآتية:

هل وقع انتحال هوية معاقب عليه؟ وهل تحققت صورة من صور الاحتيال المنصوص عليها؟ وهل وقع اعتداء مستقل على بيانات بطاقة الدفع؟ وهل ترتبت خسارة مالية يمكن ربطها بالسلوك الإجرامي؟

النتيجة: يتمثل جوهر الحماية الجنائية في تحديد الأفعال التي جرمها المشرع، وليس في تسمية التقنية المستخدمة.

المرجع التشريعي: القانون القطري رقم (14) لسنة 2014، المادتان (11) و(12)، والقانون رقم (11) لسنة 2004، المواد (381–384)..

2. المقارنة العربية: المملكة العربية السعودية وجمهورية مصر العربية

أولاً: المملكة العربية السعودية

صدر نظام مكافحة جرائم المعلوماتية بالمرسوم الملكي رقم (م/17) بتاريخ 1428/3/8هـ.

وتُعد المادة الرابعة من النصوص الأساسية المتعلقة بالاعتداءات المالية باستخدام الوسائل المعلوماتية.

وتشمل صوراً من الاستيلاء على المال بطريق الاحتيال أو اتخاذ اسم كاذب أو انتحال صفة غير صحيحة، وكذلك الوصول غير المشروع إلى بيانات بنكية أو ائتمانية في الحالات التي يحددها النظام.

وتقرر المادة عقوبة تصل إلى السجن ثلاث سنوات والغرامة مليوني ريال سعودي، أو إحدى العقوبتين.

أما المادة الخامسة، فتتناول صوراً من الاعتداء على البيانات والأنظمة المعلوماتية، وتصل عقوبتها إلى السجن أربع سنوات والغرامة ثلاثة ملايين ريال سعودي، أو إحدى العقوبتين.

ثانياً: المقارنة مع القانون القطري

وجه المقارنة	قطر	السعودية
التشريع	القانون 2014/14	نظام مكافحة جرائم المعلوماتية 1428هـ
الاحتيال وانتحال الهوية	المادة 11	المادة الرابعة
الحد الأقصى للعقوبة السالبة للحرية في النصين	3سنوات	3سنوات
الحد الأقصى للغرامة	100,000ريال قطري	2,000,000ريال سعودي
بيانات الدفع	المادة 12	من صور المادة الرابعة

وتكشف المقارنة اختلافاً في مقدار الغرامة، مع ضرورة مراعاة اختلاف عناصر الجرائم عند تقييم السياسة العقابية.

فلا يصح اعتبار النص السعودي أشد من النص القطري في جميع الحالات اعتماداً على قيمة الغرامة وحدها؛ إذ يتعين فحص الظروف المشددة والأحكام العامة وسائر النصوص ذات الصلة.

ثالثاً: جمهورية مصر العربية

صدر القانون رقم (175) لسنة 2018 بشأن مكافحة جرائم تقنية المعلومات.

وتتناول المادة (23) جرائم مرتبطة ببطاقات البنوك والخدمات وأدوات الدفع الإلكترونية.

وتتدرج العقوبات بحسب طبيعة السلوك والقصد والنتيجة، وفق النص القانوني.

ومن المؤشرات العقابية الواردة في المادة:

صورة الجريمة	الحد الأدنى للحبس	الغرامة
الوصول غير المشروع إلى بيانات أدوات الدفع	3أشهر	30–50ألف جنيه مصري
قصد استخدام البيانات للحصول على أموال أو خدمات	6أشهر	50–100ألف جنيه
تحقق الاستيلاء على الأموال أو الخدمات	سنة	100–200ألف جنيه

وتتناول المادة (24) صوراً من اصطناع الحسابات أو المواقع أو البريد الإلكتروني ونسبتها زوراً إلى أشخاص آخرين، وفق الشروط القانونية المحددة

رابعاً: المقارنة القانونية

تظهر ثلاث اتجاهات تشريعية:

1. **الاتجاه القطري:** التمييز بين النص المتعلق بالاحتيال وانتحال الهوية والنص الخاص ببطاقات التعامل الإلكتروني.
2. **الاتجاه السعودي:** إدراج صور من الاحتيال المالي والوصول إلى البيانات البنكية ضمن المادة الرابعة.
3. **الاتجاه المصري:** تنظيم خاص لبعض جرائم أدوات الدفع الإلكترونية مع تدرج عقابي يرتبط بالفعل ونتيجته.

خامساً: التطبيق على الذكاء الاصطناعي

إذا استخدم الجاني الذكاء الاصطناعي لإنشاء موقع مصرفي مزيف يستدرج بيانات البطاقات، فقد تثار أحكام خاصة ببيانات الدفع.

أما إذا استخدم صوتاً اصطناعياً لخداع صاحب الحساب ودفعه إلى تحويل المال، فإن التكييف يقتضي بحث نصوص الاحتيال وانتحال الهوية.

النتيجة المقارنة: لا يتحدد التكييف القانوني بمجرد وجود الذكاء الاصطناعي، وإنما بطبيعة الفعل الذي استُخدم لتحقيقه.

المراجع التشريعية: نظام مكافحة جرائم المعلوماتية السعودي، المادتان الرابعة والخامسة؛ القانون المصري رقم (175) لسنة 2018، المادتان (23) و.(24)

3. الولايات المتحدة الأمريكية وكندا: المسؤولية الجنائية عن الاحتيال المالي ووسائل الوصول الإلكتروني

أولاً: التشريع الجنائي الاتحادي الأمريكي

يتميز النظام القانوني الأمريكي بتعدد النصوص الجنائية التي يمكن تطبيقها على جرائم الاحتيال المالي، بحسب طبيعة الفعل ووسيلة ارتكابه وتوافر شروط الاختصاص الاتحادي.

ومن أبرز هذه النصوص:

النص القانوني	الجريمة	العقوبة الأساسية
U.S.C. 1029(a)(1)18	إنتاج أو استخدام أو الاتجار بوسائل وصول مزورة بقصد الاحتيال	السجن حتى 10 سنوات في الحالة الأساسية
U.S.C. 1029(a)(2)18	استخدام وسائل وصول غير مصرح بها للحصول على أشياء ذات قيمة تتجاوز 1,000 دولار خلال سنة، وفق شروط النص	السجن حتى 10 سنوات في الحالة الأساسية
U.S.C. 1030(a)(2)18	الوصول غير المصرح به إلى حاسوب للحصول على معلومات محمية قانوناً	تختلف العقوبة بحسب الظروف ونوع المخالفة
U.S.C. 134318	الاحتيال باستخدام الاتصالات السلكية أو اللاسلكية أو الإلكترونية	السجن حتى 20 سنة في الحالة الأساسية

وتوجد عقوبات مشددة وحالات خاصة في هذه النصوص، لذلك لا يجوز تطبيق الحد الأقصى المذكور على جميع الوقائع دون تمييز.

ثانياً: المادة 1029 وحماية وسائل الوصول المالي

تكتسب المادة 18 U.S.C. 1029 أهمية خاصة لأنها لا تقتصر على البطاقة المصرفية المادية.

فالتعريف القانوني لوسيلة الوصول (Access Device) يشمل، وفق شروط النص، البطاقات والأرقام والرموز وغيرها من الوسائل التي يمكن استخدامها للحصول على المال أو السلع أو الخدمات.

ويتيح ذلك دراسة الاعتداء على وسائل الدفع الإلكترونية حتى عندما لا تكون هناك بطاقة بلاستيكية مسروقة.

وتبرز أهمية المادة 1029 (a)(2)في اشتراط حصول الجاني على أشياء ذات قيمة يبلغ مجموعها 1,000 دولار أو أكثر خلال سنة واحدة، إلى جانب بقية عناصر الجريمة.

ثالثاً: المادة 1343 والاحتيال عبر الاتصالات

تُعد المادة 18 U.S.C. 1343 من النصوص المهمة عند دراسة الاحتيال الذي يستخدم رسائل البريد الإلكتروني أو الاتصالات الرقمية.

فإذا استخدم الجاني تسجيلاً صوتياً اصطناعياً لإقناع مسؤول مالي بإرسال الأموال، فقد يقتضي الأمر فحص هذه المادة، متى تحققت عناصر الجريمة ومتطلبات الاختصاص الاتحادي.

ولا يُشترط افتراض وقوع اختراق إلكتروني لمجرد أن وسيلة الاحتيال كانت رقمية.

رابعاً: التشريع الجنائي الكندي

يتضمن القانون الجنائي الكندي Criminal Code, R.S.C. 1985, c. C-46 أحكاماً تتصل بالاحتيال والاستخدام غير المصرح به للحاسوب.

المادة 380(1): الاحتيال

تتناول الاستيلاء على المال، أو الممتلكات، أو الخدمات باستخدام الخداع ،أو الوسائل الاحتيالية.

وفي الحالات التي تتجاوز فيها قيمة موضوع الجريمة 5,000 دولار كندي، قد تصل العقوبة إلى 14 سنة سجناً.

المادة 342.1: الاستخدام غير المصرح به للحاسوب

تعالج صوراً محددة من الاستخدام الاحتيالي أو غير المصرح به لخدمات الحاسوب أو البيانات.

وقد تصل العقوبة في المسار الاتهامي إلى 10 سنوات سجناً.

خامساً: المقارنة القانونية

تختلف الحماية الجنائية باختلاف محل الاعتداء:

- الاعتداء على وسيلة الوصول المالي يستدعي فحص المادة الأمريكية 1029.
- الاحتيال باستخدام الاتصالات يستدعي فحص المادة الأمريكية 1343.
- الاحتيال الموجه إلى إرادة الشخص يستدعي فحص المادة الكندية 380.

- الاستخدام غير المصرح به للحاسوب يستدعي فحص المادة الكندية 342.1.

سادساً: النتيجة العلمية

تكشف المقارنة أن الاحتيال المالي المدعوم بالذكاء الاصطناعي قد يتحقق دون وقوع دخول غير مشروع إلى نظام معلوماتي.

فقد يكون الفعل الإجرامي قائماً على تضليل شخص يملك صلاحية إصدار التحويل، وهو ما يستدعي التمييز بين النصوص المتعلقة بالاحتيال وتلك المتعلقة بالوصول غير المصرح به إلى الحواسيب.

المراجع التشريعية1343 ,1030 ,181029 United States Code, Title :؛ Canadian Criminal Code380, 342.1. .

4. (ألمانيا وفرنسا وسويسرا): التمييز بين الاحتيال على الإنسان والاحتيال على أنظمة معالجة البيانات

أولاً: قانون العقوبات الألماني

يقدم قانون العقوبات الألماني (Strafgesetzbuch (StGB تمييزاً مهماً بين الاحتيال التقليدي والاحتيال الحاسوبي.

المادة (263): الاحتيال

تجرم إحداث ضرر مالي عن طريق تضليل شخص بشأن وقائع معينة، بقصد الحصول على منفعة مالية غير مشروعة، وفق عناصر النص.

وتقرر عقوبة أساسية تصل إلى السجن خمس سنوات أو الغرامة.

المادة :(263a) الاحتيال الحاسوبي

تتناول إحداث ضرر مالي من خلال التأثير غير المشروع في نتيجة معالجة البيانات، وفق الصور المحددة في النص.

وتقرر عقوبة أساسية تصل إلى السجن خمس سنوات أو الغرامة.

المادة (269): تزوير البيانات ذات القيمة الإثباتية

تعالج صوراً من حفظ البيانات أو تغييرها أو استخدامها على نحو يحقق عناصر تزوير البيانات ذات القيمة الإثباتية.

وتصل العقوبة الأساسية إلى السجن خمس سنوات أو الغرامة.

ثانياً: الأهمية القانونية للتمييز الألماني

لنفترض أن شخصاً استخدم تقنية التزييف العميق لانتحال صوت المدير المالي، ثم طلب من موظف تحويل مبلغ إلى حساب معين.

في هذه الحالة، ينصب التأثير الاحتيالي على إرادة الموظف.

أما إذا تدخل الجاني بصورة غير مشروعة في نظام معالجة البيانات المصرفية لتغيير نتيجة المعالجة، فإن محل الاعتداء يختلف.

ومن هنا تظهر أهمية التمييز بين المادتين 263 و263a.

ولا يجوز افتراض انطباق المادة الخاصة بالاحتيال الحاسوبي لمجرد أن التحويل نُفذ باستخدام نظام مصرفي إلكتروني.

ثالثاً: قانون العقوبات الفرنسي

يتضمن قانون العقوبات الفرنسي Code pénal نصوصاً مهمة في هذا المجال.

المادة 313-1: الاحتيال

تتناول استخدام اسم كاذب أو صفة غير صحيحة أو وسائل احتيالية لحمل شخص على تسليم أموال أو ممتلكات أو تقديم خدمة، وفق شروط النص.

وتقرر عقوبة أساسية تبلغ:

السجن خمس سنوات وغرامة 375,000 يورو.

المادة 323-1: الدخول أو البقاء غير المشروع في نظام معالجة بيانات آلي

تتناول الدخول أو البقاء بطريق احتيالي داخل نظام لمعالجة البيانات آلياً.

وتقرر عقوبة أساسية تبلغ:

السجن ثلاث سنوات وغرامة 100,000 يورو، مع تشديد العقوبة في الحالات التي يحددها النص.

رابعاً: قانون العقوبات السويسري

يتميز القانون السويسري بالفصل بين الاحتيال التقليدي وإساءة الاستخدام الاحتيالي لنظام معالجة البيانات.

المادة 146: الاحتيال

تتعلق بالحصول على منفعة مالية غير مشروعة عن طريق الخداع، وفق عناصر النص.

المادة 147: إساءة الاستخدام الاحتيالي لنظام معالجة البيانات

تتناول التأثير غير المشروع في عمليات معالجة البيانات لتحقيق منفعة مالية والإضرار بأموال الغير.

المادة 143 :bisالدخول غير المشروع إلى نظام معالجة البيانات

تعالج الدخول غير المصرح به إلى نظام محمي، وفق الشروط القانونية.

خامساً: المقارنة الأوروبية

المسألة القانونية	ألمانيا	فرنسا	سويسرا
الاحتيال على الإنسان	26	313-1	146
الاحتيال المرتبط بمعالجة البيانات	263a	تُفحص النصوص المنطبقة بحسب الفعل	147
الدخول غير المشروع إلى النظام	202aوما يرتبط بها	323-1	143bis
تزوير البيانات	269	بحسب طبيعة الفعل والنص المنطبق	بحسب طبيعة الفعل والنص المنطبق

سادساً: الإضافة المقارنة

توضح التجربتان الألمانية والسويسرية أن الاحتيال على الإنسان والاحتيال على المعالجة الآلية ليسا بالضرورة جريمة واحدة.

فقد يتحقق الضرر المالي من خلال قرار يصدر عن شخص مخدوع، أو من خلال التأثير غير المشروع في نتيجة معالجة البيانات.

ويؤثر هذا الاختلاف في تحديد الركن المادي، وطبيعة الدليل المطلوب، والنص الجنائي المنطبق.

النتيجة: يمثل تحديد الجهة التي استهدفها السلوك الاحتيالي، الإنسان أم نظام معالجة البيانات، مدخلاً مهماً للتكييف الجنائي المقارن.

المراجع التشريعية German Criminal Code 263, 263a, 269 ؛ French Penal Code Articles 313-1, 323-1؛ Swiss Criminal Code Articles 146, 147, 143bis.

الموضوع	المادة
الاستخدام الاحتيالي لوسائل الدفع غير النقدية	3
الجرائم المتعلقة بوسائل الدفع المادية	4
الجرائم المتعلقة بوسائل الدفع غير المادية	5
الاحتيال المرتبط بأنظمة المعلومات	6
الأدوات المستخدمة لارتكاب الجرائم	7
التحريض والمساعدة والشروع	8
العقوبات المفروضة على الأشخاص الطبيعيين	9
مسؤولية الأشخاص الاعتباريين	10

5. أستراليا والاتحاد الأوروبي: الحماية الجنائية لبيانات الدفع والوسائل المالية غير المادية

أولاً: التشريع الأسترالي

يتضمن القانون الجنائي الاتحادي الأسترالي Criminal Code Act 1995 أحكاماً تتعلق بالمعلومات المالية الشخصية.

ومن أبرزها:

موضوع التجريم	العقوبة	المادة
الحصول غير النزيه على المعلومات المالية الشخصية أو التعامل فيها، وفق شروط النص	السجن حتى 5 سنوات	480.4
حيازة أو السيطرة على أشياء بقصد استخدامها في ارتكاب جريمة المادة 480.4 أو تسهيلها	السجن حتى 3 سنوات	480.5
استيراد أشياء بقصد استخدامها في ارتكاب الجريمة المحددة بالمادة 480.4 أو تسهيلها	السجن حتى 3 سنوات	480.6

وتكتسب المادة 480.4 أهمية خاصة في الجرائم التي تستهدف البيانات المالية، حتى عندما لا تقع سرقة بطاقة مصرفية مادية.

ثانياً: التوجيه الأوروبي 713/2019أصدر الاتحاد الأوروبي التوجيه:

Directive (EU) 2019/713 of 17 April 2019

بشأن مكافحة الاحتيال وتزوير وسائل الدفع غير النقدية.

ويُعد من أهم النصوص المقارنة المتعلقة بجرائم بطاقات الدفع والوسائل المالية الرقمية.

ثالثاً: المادة الخامسة

تتناول المادة (5) الجرائم المتعلقة بوسائل الدفع غير المادية.

وتشمل صوراً من الحصول غير المشروع على وسيلة الدفع غير المادية، وتزويرها، وحيازتها أو تداولها بقصد الاستخدام الاحتيالي، وفق الأحكام الواردة فيها.

وتبرز أهميتها في الانتقال من التركيز على البطاقة المادية إلى حماية وسائل الدفع الرقمية.

رابعاً: المادة السادسة

تتناول المادة (6) الاحتيال المرتبط بأنظمة المعلومات، بما يشمل إحداث تحويل مالي أو نقل قيمة مالية بطريقة تسبب خسارة غير مشروعة، من خلال أفعال غير مصرح بها تتعلق بالنظام أو البيانات، وفق شروط النص.

وتتيح هذه المادة التمييز بين استخدام بيانات الدفع بصورة احتيالية وبين التدخل غير المشروع في عمليات المعالجة المعلوماتية.

خامساً: المقارنة مع القانون القطري

تنص المادة (12) من القانون القطري رقم (14) لسنة 2014 على تجريم صور محددة من الاعتداء على بطاقات التعامل الإلكتروني وبياناتها.

أما التوجيه الأوروبي 713/2019، فيميز صراحة بين وسائل الدفع المادية وغير المادية.

ويثير ذلك مسألة تستحق البحث:

هل يحقق نطاق النص القطري الحماية الجنائية المطلوبة لجميع صور وسائل الدفع الرقمية المستحدثة، أم توجد حالات تحتاج إلى معالجة تشريعية أكثر تحديداً؟

ولا يصح الجزم بوجود فراغ تشريعي قبل تحليل ألفاظ المادة القطرية ومقارنتها بالتعريفات الواردة في التوجيه الأوروبي.

سادساً: النتيجة العلمية

يُظهر التنظيم الأوروبي أهمية صياغة النص الجنائي بصورة تستوعب التطور التقني في وسائل الدفع.

لكن اتساع الحماية لا ينبغي أن يؤدي إلى تجاوز مبدأ الشرعية الجنائية أو التوسع في تفسير النصوص العقابية على حساب المتهم.

النتيجة: تستلزم الحماية الفعالة الجمع بين وضوح النص الجنائي ومرونته في استيعاب صور الاعتداء على وسائل الدفع غير المادية.

المراجعDirective (EU) 2019/713, ؛: Australian Criminal Code Act 1995480.4–480.6

Articles 3–10.

6. الاتفاقيات الدولية والأدلة الإلكترونية والتعاون الجنائي عبر الحدود

أولاً: اتفاقية بودابست بشأن الجريمة السيبرانية

فُتحت اتفاقية بودابست للتوقيع بتاريخ 23 نوفمبر 2001، ودخلت حيز النفاذ في 1 يوليو 2004.

رقم الاتفاقية.ETS No. 185 :

وتتضمن أحكاماً تتعلق بتجريم بعض الأفعال المرتبطة بالحاسوب، والإجراءات المتعلقة بالأدلة الإلكترونية، والتعاون الدولي.

الموضوع	المادة
التزوير المرتبط بالحاسوب	7
الاحتيال المرتبط بالحاسوب	8
الحفظ العاجل للبيانات الحاسوبية المخزنة	16
أوامر تقديم البيانات	18
الحفظ العاجل للبيانات المخزنة في إطار التعاون الدولي	29
شبكة الاتصال المتاحة طوال اليوم وعلى مدار الأسبوع	35

ثانياً: المادة الثامنة

تكتسب المادة (8) أهمية خاصة لأنها تتعلق بالاحتيال المرتبط بالحاسوب.

وتتناول إحداث خسارة مالية من خلال أفعال معينة تؤثر في البيانات أو عمل أنظمة الحاسوب، بقصد الحصول على منفعة اقتصادية غير مشروعة، وفق شروطها.

وتظهر أهمية هذه المادة عند مقارنتها بالمادة 263 aالألمانية والمادة 147 السويسرية.

ثالثاً: الحفظ العاجل للأدلة

تتيح المادة (16) إطاراً لحفظ البيانات الحاسوبية المخزنة بصورة عاجلة.

وتبرز أهمية الحفظ العاجل في الجرائم المالية الرقمية؛ لأن البيانات المرتبطة بالتحويلات والحسابات والاتصالات قد تتغير أو تُحذف خلال فترة قصيرة.

أما المادة (35)، فتتناول إنشاء شبكة اتصال تعمل على مدار الساعة لتسهيل التعاون العاجل.

ويجب التمييز بين الحفظ العاجل للبيانات وبين الحصول عليها أو استخدامها دليلاً أمام المحكمة؛ فلكل إجراء شروطه القانونية.

رابعاً: البروتوكول الإضافي الثاني

رقمه.CETS No. 224 :

فُتح للتوقيع في 12 مايو 2022.

ويتناول تعزيز التعاون الدولي والكشف عن الأدلة الإلكترونية، مع مراعاة الضمانات والقيود الواردة فيه.

ولا يجوز افتراض سريان التزاماته على دولة لم تصبح طرفاً فيه وفق الإجراءات القانونية المطلوبة.

خامساً: اتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية

اعتمدت الجمعية العامة للأمم المتحدة الاتفاقية بموجب القرار:

243/79 بتاريخ 24 ديسمبر 2024.

وتتناول الاتفاقية مسائل التجريم والإجراءات الجنائية والتعاون الدولي والمساعدة القانونية المتبادلة والأدلة الإلكترونية.

وتنظم المادة 65(1) شروط دخولها حيز النفاذ، المرتبطة بإيداع وثيقة التصديق، أو القبول، أو الموافقة، أو الانضمام الأربعين، وانقضاء المدة المحددة بعد ذلك.

وينبغي التحقق من حالة نفاذ الاتفاقية وعدد الدول الأطراف في تاريخ تقديم البحث، وعدم الخلط بين الاعتماد، والتوقيع، والتصديق، والنفاذ.

سادساً: قانون الذكاء الاصطناعي الأوروبي

صدر التنظيم الأوروبي:

Regulation (EU) 2024/1689

المعروف بقانون الذكاء الاصطناعي الأوروبي.

ومن مواده ذات الصلة:

المادة (5): تتناول ممارسات محظورة للذكاء الاصطناعي وفق شروط محددة.

المادة (50): تتناول التزامات الشفافية لبعض أنظمة الذكاء الاصطناعي والمحتويات الاصطناعية، ومنها التزييف العميق.

ولا يُعد هذا التنظيم بديلاً عن النصوص الجنائية الخاصة بالاحتيال أو جرائم بطاقات الدفع.

سابعاً: الضمانات الإجرائية

يقرر العهد الدولي الخاص بالحقوق المدنية والسياسية، المعتمد بقرار الجمعية العامة 2200 A (XXI) لعام 1966، ضمانات تتصل بالمحاكمة العادلة والخصوصية.

ومن أهم مواده:

المادة (14): المحاكمة العادلة.

المادة (17): الحماية من التدخل التعسفي أو غير القانوني في الخصوصية.

ثامناً: النتيجة القانونية

لا تتحقق فعالية مكافحة الاحتيال المالي العابر للحدود بمجرد تجريم الأفعال.

بل تتطلب المحافظة على الأدلة الرقمية، وتحديد السلطات المختصة، وسرعة تبادل المعلومات، ومراعاة الضمانات الإجرائية.

النتيجة: تمثل الأدلة الإلكترونية والتعاون الدولي امتداداً ضرورياً للحماية الجنائية الموضوعية، لا بديلاً عنها.

المراجعBudapest Convention ETS 185؛ Second Additional Protocol CETS 224؛ UNGA Resolution 79/243؛ Regulation (EU) 2024/1689.

7. الإنتربول ومكتب التحقيقات الفيدرالي: العمليات الدولية والإحصاءات المالية

أولاً: تقييم الإنتربول العالمي لعام 2026

أصدر الإنتربول في 16 مارس 2026 تقريراً بعنوان:

INTERPOL Global Financial Fraud Threat Assessment 2026

وتناول تطور الاحتيال المالي الدولي، بما في ذلك استخدام الذكاء الاصطناعي في تطوير أساليب الخداع.

ومن أبرز المؤشرات الواردة فيه تقدير بأن الاحتيال المعزز بالذكاء الاصطناعي قد يكون أكثر ربحية بنحو 4.5 أضعاف مقارنة بالأساليب التقليدية غير المعززة به.

ولا يمثل هذا الرقم نسبة ثابتة لجميع الجرائم، بل تقديراً ينبغي فهمه في سياق التقرير ومنهجيته.

ثانياً: عمليةHAECHI VI

أعلن الإنتربول نتائج العملية بتاريخ 24 سبتمبر 2025.

وشملت العملية 40 دولة وإقليماً، من بينها دولة قطر.

المؤشر	النتيجة
الأموال التقليدية المستردة	342مليون دولار
الأصول المادية والافتراضية المستردة	97مليون دولار
إجمالي الأموال والأصول المستردة	439مليون دولار
الحسابات المصرفية المحجوبة	أكثر من 68,000 حساب
محافظ العملات المشفرة المجمدة	نحو 400 محفظة

وشملت العملية أنماطاً متعددة من الاحتيال المالي الإلكتروني، منها الاحتيال الاستثماري والتصيد الصوتي والاحتيال عبر البريد الإلكتروني التجاري.

ولا يجوز نسبة جميع نتائج العملية إلى جرائم استخدمت الذكاء الاصطناعي؛ إذ لم تقتصر العملية على هذا النوع من الجرائم.

ثالثاً: عملية First Light 2026

أعلن الإنتربول نتائج عملية First Light 2026 بتاريخ 9 يوليو 2026.

وتضمنت المؤشرات المعلنة:

المؤشر	النتيجة
الدول والأقاليم المشاركة	97
الأشخاص المقبوض عليهم	5,811
قيمة الأصول التي جرى اعتراضها	293مليون دولار

وتكشف هذه النتائج عن أهمية التعاون الدولي في مواجهة شبكات الاحتيال التي تستهدف الضحايا في دول متعددة.

رابعاً: آلية I-GRIP

يستخدم الإنتربول آلية تعرف باسم:

Global Rapid Intervention of Payments – I-GRIP

وتهدف إلى تسهيل التدخل السريع في المدفوعات المرتبطة بالاحتيال، من خلال التعاون بين السلطات المختصة.

وتبرز أهميتها في الحالات التي تُحوّل فيها الأموال بسرعة عبر حسابات متعددة أو ولايات قضائية مختلفة.

ولا تعني الاستفادة من هذه الآلية أن الإنتربول يحل محل السلطات القضائية الوطنية في إصدار الأوامر أو مباشرة إجراءات المصادرة.

خامساً: تقرير FBI لعام 2025

أورد التقرير السنوي لمركز شكاوى جرائم الإنترنت IC3 بيانات عن الشكاوى التي تضمنت معلومات مرتبطة باستخدام الذكاء الاصطناعي.

ومن أبرزها:

- 22,364 شكوى.
- 893,346,472 دولاراً من الخسائر المبلغ عنها.

وتوضح هذه الأرقام أن الذكاء الاصطناعي أصبح عنصراً مؤثراً في بعض صور الاحتيال الإلكتروني.

لكن الخسائر المبلغ عنها لا تعادل بالضرورة قيمة الأموال التي ثبت الاستيلاء عليها بموجب أحكام قضائية نهائية.

سادساً: التحليل القانوني

تختلف وظيفة كل جهة:

FBI: يجمع بيانات الشكاوى والتحقيقات وفق اختصاصاته.

الإنتربول: يسهل التعاون الشرطي الدولي وتبادل المعلومات والتنسيق بين الدول.

السلطات القضائية الوطنية: تختص بتطبيق النصوص الجنائية وإصدار الأحكام واتخاذ الإجراءات القضائية وفق القانون.

سابعاً: النتيجة

تكشف العمليات الدولية أن مكافحة الاحتيال المالي تتطلب التدخل قبل اكتمال نقل الأموال إلى حسابات يصعب تعقبها.

النتيجة القانونية: يجب أن تتكامل إجراءات التحقيق والإثبات مع آليات التعاون الدولي السريع، دون الإخلال بالاختصاص القضائي أو ضمانات المحاكمة العادلة.

المراجعHAECHI VI ؛: INTERPOL Global Financial Fraud Threat Assessment 2026

First Light 2026؛2025 ؛

FBI IC3 Annual Report 2025.

8. الوقائع الجنائية المعاصرة والتطبيق القانوني المقارن

أولاً: واقعة الاحتيال بالتزييف العميق في هونغ كونغ

أعلنت سلطات هونغ كونغ سنة 2024 تفاصيل واقعة استخدم فيها محتالون تقنيات التزييف العميق لانتحال شخصيات مسؤولين داخل مؤسسة.

وقد تعرض أحد الموظفين للخداع من خلال اجتماع مرئي اصطناعي، ترتبت عليه تحويلات مالية بلغت نحو:

200 مليون دولار هونغ كونغي.

وتكمن الأهمية القانونية في أن التحويلات صدرت عن موظف يملك صلاحية تنفيذها، لكنه اتخذ قراره بناءً على معلومات وهوية مزيفتين.

وهذه واقعة جنائية معلنة، ولا تُعرض هنا باعتبارها حكماً قضائياً نهائياً.

ثانياً: التكييف وفق القانون القطري

إذا افترضنا وقوع واقعة مماثلة ضمن نطاق تطبيق القانون القطري، فإن التحليل يبدأ بفحص المادة (11) من القانون رقم (14) لسنة 2014.

ويتطلب ذلك بحث:

الفعل المادي: استخدام وسيلة تقنية في انتحال الهوية أو الاحتيال، وفق شروط النص.

القصد الجنائي: العلم والإرادة المتطلبان قانوناً.

النتيجة: تحقق الاستيلاء على المال في الصورة التي يشترط فيها النص ذلك.

علاقة السببية: ارتباط التحويل المالي بالخداع الذي مارسه الجاني.

أما المادة (12) المتعلقة ببطاقات التعامل الإلكتروني، فلا يُفترض انطباقها ما لم تثبت أفعال تدخل ضمن نطاقها.

ثالثاً: التكييف وفق القانون الألماني

إذا انصب الخداع على إرادة الموظف، فإن المادة 263 المتعلقة بالاحتيال تكون ذات صلة.

أما المادة 263 aالخاصة بالاحتيال الحاسوبي، فتتطلب فحص وجود تدخل غير مشروع في نتيجة معالجة البيانات وفق شروطها.

وتظهر أهمية التمييز في أن استخدام النظام المصرفي لتنفيذ التحويل لا يعني بالضرورة أن النظام نفسه كان محل التلاعب.

رابعاً: التكييف وفق القانون الفرنسي

تقتضي الواقعة فحص المادة 313-1 من قانون العقوبات الفرنسي.

فقد يتحقق الاحتيال باستخدام صفة غير صحيحة أو وسائل احتيالية لحمل شخص على تسليم الأموال، متى استوفت الواقعة عناصر النص.

أما المادة 323-1 الخاصة بالدخول غير المشروع إلى نظام معالجة البيانات، فلا تُطبق تلقائياً إذا لم يقع دخول غير مشروع.

خامساً: التكييف وفق القانون الأمريكي

قد تثار المادة 18 U.S.C1343 المتعلقة بالاحتيال باستخدام وسائل الاتصالات الإلكترونية، إذا تحققت عناصرها ومتطلبات الاختصاص الاتحادي.

أما المادة §1029 المتعلقة بوسائل الوصول المالي، فتتطلب إثبات الأفعال والشروط المحددة فيها.

سادساً: التكييف وفق القانون الكندي

قد تُبحث المادة 380 المتعلقة بالاحتيال.

أما المادة 342.1 المتعلقة بالاستخدام غير المصرح به للحاسوب، فتتطلب إثبات عناصرها الخاصة.

سابعاً: المقارنة التطبيقية

النص الذي يُبحث تطبيقه ابتداءً	الدولة المسألة الحاسمة	الدولة
المادة 11	تحقق انتحال الهوية أو الاحتيال وفق النص	قطر
المادة الرابعة	تحقق صورة من صور الاحتيال المنصوص عليها	السعودية
263	تضليل شخص وإحداث ضرر مالي	ألمانيا
1-313	استخدام وسائل احتيالية لحمل شخص على تسليم المال	فرنسا
U.S.C134318	تحقق عناصر الاحتيال عبر الاتصالات والاختصاص الاتحادي	الولايات المتحدة
380	تحقق الاحتيال وفق عناصر القانون	كندا

ثامناً: الإشكالية الإثباتية

يتعين في الجرائم التي تستخدم التزييف العميق إثبات صلة المتهم بالمحتوى الاصطناعي واستعماله الاحتيالي.

ومن الأدلة التي قد تكون ذات صلة:

1. سجلات الاتصالات والرسائل الإلكترونية .

2. البيانات الفنية المتعلقة بإنشاء المحتوى وتداوله .

3. سجلات الحسابات المستقبلة للتحويلات .

4. الأدلة المتعلقة بالأجهزة والبرامج المستخدمة .

5. القرائن التي تربط المتهم بإصدار التعليمات أو الاستفادة من الأموال .

ولا يكفي إثبات أن التسجيل مزيف لإثبات هوية منشئه أو تحديد مسؤوليته الجنائية.

تاسعاً: النتيجة

تؤكد الواقعة أن الاحتيال المالي المدعوم بالذكاء الاصطناعي قد يستهدف الثقة البشرية التي تسبق المعاملة المصرفية، دون أن يستهدف بالضرورة سلامة النظام المصرفي نفسه.

المرجع: البيانات الرسمية لحكومة هونغ كونغ بشأن وقائع الاحتيال باستخدام التزييف العميق، 2024.

النتائج القانونية والتوصيات التشريعية

أولاً: النتائج

النتيجة الأولى: استقلال التكييف الجنائي عن الوسيلة التقنية

لا يكفي استخدام الذكاء الاصطناعي لقيام جريمة مستقلة ما لم ينص القانون على ذلك أو تتحقق عناصر إحدى الجرائم القائمة.

فالعبرة بطبيعة السلوك المجرّم، والقصد الجنائي، والنتيجة، وعلاقة السببية حيث يتطلبها النص.

النتيجة الثانية: التمييز بين محل الاعتداء

تكشف المقارنة عن ثلاثة محال محتملة للاعتداء:

إرادة الشخص المخول بالتصرف المالي، ونظام معالجة البيانات، ووسيلة الدفع أو بياناتها.

ويترتب على اختلاف المحل اختلاف النصوص الجنائية التي يتعين فحصها.

النتيجة الثالثة: أهمية النصوص القطرية القائمة

تتيح المادتان (11) و(12) من القانون القطري رقم (14) لسنة 2014 أساساً لدراسة صور متعددة من الاحتيال الإلكتروني وجرائم بطاقات التعامل الإلكتروني.

غير أن تحديد مدى استيعابهما للصور المستحدثة يتطلب تطبيق عناصر كل نص على الوقائع، وليس الاكتفاء بعمومية وصف الجريمة.

النتيجة الرابعة: أهمية التمييز الألماني والسويسري

يساعد الفصل بين الاحتيال التقليدي والاحتيال الحاسوبي في ألمانيا وسويسرا على تجنب الخلط بين تضليل الإنسان والتأثير غير المشروع في معالجة البيانات.

النتيجة الخامسة: تطور مفهوم وسيلة الدفع

يبرز التوجيه الأوروبي 713/2019 أهمية التمييز بين وسائل الدفع المادية وغير المادية، وهو تمييز مفيد عند تقييم نطاق الحماية الجنائية لبيانات الدفع والوسائل الرقمية.

النتيجة السادسة: الطبيعة العابرة للحدود

تكشف عمليات الإنتربول عن أن الجرائم المالية قد تتوزع عناصرها بين عدة دول، بما يستلزم سرعة حفظ الأدلة وتبادل المعلومات وتتبع الأموال.

النتيجة السابعة: تحديات الأدلة الاصطناعية

لا يثبت استخدام التزييف العميق بذاته هوية الجاني؛ إذ يتعين إثبات الصلة بين المحتوى الاصطناعي والفعل الاحتيالي والمتهم والنتيجة المالية.

ثانياً: التوصيات

التوصية الأولى: مراجعة تشريعية محددة

إجراء دراسة تطبيقية للمادتين (11) و(12) من القانون القطري رقم (14) لسنة 2014، لقياس مدى استيعابهما صور الاحتيال القائمة على انتحال الهوية الاصطناعية ووسائل الدفع غير المادية.

التوصية الثانية: تطوير قواعد التعامل مع الأدلة الاصطناعية

تعزيز إجراءات التحقق الفني من التسجيلات الصوتية والمرئية، مع توثيق مصدر الدليل وسلسلة حيازته وسلامته.

التوصية الثالثة: الاستفادة من التوجيه الأوروبي

دراسة التمييز بين وسائل الدفع المادية وغير المادية الوارد في المادتين (4) و(5) من التوجيه الأوروبي 713/2019، لتقييم الحاجة إلى مزيد من الوضوح التشريعي.

التوصية الرابعة: تعزيز التعاون الدولي

تطوير إجراءات التنسيق بين الجهات المختصة في الجرائم المالية العابرة للحدود، والاستفادة من الآليات المتاحة لدى الإنتربول وفق القوانين الوطنية والاتفاقيات السارية.

التوصية الخامسة: التحقق المستقل من التعليمات المالية

اعتماد إجراءات تحقق إضافية قبل تنفيذ التحويلات المالية الحساسة، بحيث لا يكون الصوت أو الصورة وحدهما وسيلة كافية لإثبات هوية صاحب التعليمات.

التوصية السادسة: التدريب القضائي والفني

إعداد برامج متخصصة للعاملين في التحقيق الجنائي والقطاع المالي تتناول تحليل المحتوى الاصطناعي، وجرائم وسائل الدفع، والتعامل مع الأدلة الإلكترونية.

الخاتمة

تكشف الدراسة أن الجرائم المالية المدعومة بالذكاء الاصطناعي لا تشكل نموذجاً جنائياً واحداً؛ فقد تستهدف إرادة الإنسان، أو سلامة معالجة البيانات، أو وسائل الدفع وبياناتها.

ويقتضي التكييف القانوني الصحيح تحديد موضع الاعتداء والأفعال التي تحققت فعلاً، ثم تطبيق النص الجنائي المناسب دون توسع يخالف مبدأ شرعية الجرائم والعقوبات.

وتتمثل النتيجة المركزية في أن التطور التقني يستلزم تطوير أدوات التحليل القانوني والإثبات والتعاون الدولي، دون افتراض أن كل وسيلة مستحدثة تستوجب بالضرورة إنشاء جريمة جديدة.

الإضافة العلمية للباحث: الحدود الفاصلة بين الاحتيال بالذكاء الاصطناعي والاحتيال الحاسوبي وجرائم بطاقات الدفع الإلكتروني

نحو معيار قانوني مقارن لتحديد المسؤولية الجنائية في الجرائم المالية المستحدثة

أولاً: الإشكالية القانونية المستحدثة

تثير تقنيات الذكاء الاصطناعي إشكالية تتجاوز الصور التقليدية لجرائم بطاقات الدفع الإلكتروني؛ إذ أصبح بالإمكان الاستيلاء على الأموال دون سرقة البطاقة المصرفية، أو الحصول على بياناتها، أو الدخول غير المشروع إلى النظام البنكي.

وتتمثل الصورة الأكثر تعقيداً في استخدام تقنية التزييف العميق لانتحال شخصية صاحب الحساب أو المدير المالي، وإقناع موظف مختص بتنفيذ تحويل مصرفي صحيح من الناحية التقنية، لكنه صدر نتيجة خداع جنائي.

وهنا يبرز تساؤل قانوني جوهري:

هل يتحدد الوصف الجنائي للجريمة بطبيعة الوسيلة التقنية المستخدمة، أم بمحل الاعتداء والطريقة التي تحقق بها الاستيلاء على المال.

ثانياً: المعيار القانوني المقترح من الباحث

يقترح الباحث اعتماد معيار محل التأثير الاحتيالي للتمييز بين ثلاثة أنماط من الجرائم المالية الرقمية:

النمط الأول: الاحتيال الموجه إلى الإرادة البشرية.

يتحقق عندما يستخدم الجاني الذكاء الاصطناعي لتضليل شخص يملك صلاحية التصرف المالي، فيحمله على تحويل الأموال.

ومن النصوص التي يمكن بحث انطباقها:

- قطر: المادة (11) من القانون رقم (14) لسنة 2014 .
- السعودية: المادة (4) من نظام مكافحة جرائم المعلوماتية .
- ألمانيا: المادة (§263) من قانون العقوبات .
- فرنسا: المادة (313-1) من قانون العقوبات .
- كندا: المادة (380) من القانون الجنائي .

النمط الثاني: الاحتيال الموجه إلى المعالجة الآلية للبيانات.

يتحقق عندما ينصب السلوك غير المشروع على معالجة البيانات أو نتائجها، دون أن يكون تضليل شخص بشري هو الآلية الأساسية للاستيلاء.

ومن النصوص المقارنة:

- ألمانيا: المادة (§263a) من قانون العقوبات .

- سويسرا: المادة (147) من قانون العقوبات .
- الاتحاد الأوروبي: المادة (6) من التوجيه. .2019/713 (EU)

النمط الثالث: الاعتداء على وسيلة الدفع أو بياناتها.

يتحقق عندما يكون محل السلوك الإجرامي بطاقة الدفع أو بياناتها أو إحدى وسائل الوصول المالي المحمية قانوناً.

ومن النصوص المقارنة:

- قطر: المادة (12) من القانون رقم (14) لسنة 2014 .
- مصر: المادة (23) من القانون رقم (175) لسنة 2018 .
- الولايات المتحدة: المادة .(18 U.S.C. §1029)
- أستراليا: المادة (480.4) من القانون الجنائي الاتحادي .
- الاتحاد الأوروبي: المادتان (4) و(5) من التوجيه .2019/713 (EU)

ولا يعني هذا التصنيف أن الأنماط الثلاثة متنافية بالضرورة؛ فقد تجتمع في الواقعة الواحدة أفعال مستقلة تستوفي أركان جرائم متعددة، وفق أحكام كل تشريع.

ثالثاً: الاختبار القانوني المقترح

لتطبيق المعيار، يقترح الباحث طرح خمسة أسئلة متتابعة:

السؤال	الأثر القانوني
1 .هل وقع انتحال هوية أو تقديم معلومات مضللة لشخص؟	فحص نصوص الاحتيال وانتحال الهوية
2 .هل تدخل الجاني بصورة غير مشروعة في معالجة البيانات؟	فحص نصوص الاحتيال الحاسوبي
3 .هل حصل الجاني على بيانات بطاقة دفع أو استخدمها دون حق؟	فحص النصوص الخاصة بوسائل الدفع
4 .هل أدى الفعل إلى الاستيلاء على المال أو إحداث خسارة مالية؟	تحديد النتيجة وعلاقة السببية وفق النص المنطبق
5 .هل تتوافر أدلة تربط الفعل التقني بالمتهم؟	بحث الإسناد الجنائي وسلامة الأدلة الإلكترونية

ويمنع هذا الاختبار افتراض أن استخدام الذكاء الاصطناعي يحقق بذاته جميع أركان الجريمة.

رابعاً: التطبيق على واقعة افتراضية مركبة

يفترض الباحث أن شخصاً استخدم برنامجاً للذكاء الاصطناعي لإنتاج صورة وصوت مطابقين ظاهرياً لمدير مؤسسة مالية، ثم عقد اجتماعاً مرئياً مزيفاً مع موظف مخول بالتحويلات، وأقنعه بإرسال مبلغ إلى حساب يسيطر عليه الجاني.

المرحلة الأولى: إنشاء الهوية الاصطناعية.

يُبحث ما إذا كان إنشاء المحتوى واستخدامه قد حققا عناصر انتحال الهوية أو أي جريمة أخرى منصوص عليها، مع التمييز بين مجرد إنتاج المحتوى واستعماله الاحتيالي.

المرحلة الثانية: التأثير في إرادة الموظف.

ينصب الخداع هنا على شخص طبيعي، لا على برنامج المعالجة المصرفية.

المرحلة الثالثة: تنفيذ التحويل.

قد يكون أمر التحويل صحيحاً من حيث إجراءات النظام، لكنه صدر نتيجة التضليل.

المرحلة الرابعة: تحقق الاستيلاء.

يُبحث انتقال المال، والجهة المستفيدة، وعلاقة السببية بين الخداع والتحويل.

المرحلة الخامسة: الإسناد الجنائي.

يلزم إثبات صلة المتهم بإنشاء المحتوى أو استخدامه وبالحسابات المستقبلة للأموال، مع فحص الأدلة وفق القواعد الإجرائية المعمول بها.

خامساً: القيمة العلمية للإضافة

تكمن القيمة العلمية للمعيار المقترح في الفصل بين التقنية المستخدمة في ارتكاب الجريمة والبنية القانونية للجريمة نفسها.

فالتزييف العميق قد يمثل وسيلة لارتكاب الاحتيال، لكنه لا يثبت وحده وقوع جريمة متعلقة ببطاقات الدفع، كما أن تنفيذ تحويل مصرفي عبر نظام معلوماتي لا يعني بالضرورة تحقق جريمة الاحتيال الحاسوبي.

ويتيح هذا التمييز تجنب التوسع غير المنضبط في تفسير النصوص الجنائية، بما يتفق مع مبدأ شرعية الجرائم والعقوبات.

سادساً: النتيجة العلمية المستخلصة

يرى الباحث أن التحدي القانوني الأبرز في الاحتيال المالي المدعوم بالذكاء الاصطناعي لا يتمثل دائماً في غياب التجريم، وإنما في تحديد موضع التدخل الاحتيالي داخل العملية المالية، وإثبات صلته بالنتيجة الإجرامية.

وبناءً عليه، يقترح الباحث أن يبدأ التكييف الجنائي بتحديد ما إذا كان الاعتداء قد انصب على إرادة الإنسان، أو معالجة البيانات، أو وسيلة الدفع، ثم فحص أركان النصوص المنطبقة وإمكان اجتماعها.

ويمثل هذا المعيار إطاراً تحليلياً مقترحاً يحتاج إلى اختباره على أحكام قضائية ووقائع إضافية قبل الجزم بقدرته على تفسير جميع صور الاحتيال المالي المستحدث.

المراجع التشريعية والدولية الأساسية

أولاً: التشريعات الوطنية

1. دولة قطر: القانون رقم (14) لسنة 2014 بإصدار قانون مكافحة الجرائم الإلكترونية، المواد (11) و (12).
2. دولة قطر: القانون رقم (11) لسنة 2004 بإصدار قانون العقوبات، المواد (384–381).
3. المملكة العربية السعودية: نظام مكافحة جرائم المعلوماتية، المرسوم الملكي رقم (م/17) لسنة 1428هـ، المادتان الرابعة والخامسة .
4. جمهورية مصر العربية: القانون رقم (175) لسنة 2018 بشأن مكافحة جرائم تقنية المعلومات، المادتان (23) و (24).
5. الولايات المتحدة الأمريكية. United States Code, Title 18 §§ 1029, 1030, 1343 :
6. كندا. Criminal Code, R.S.C. 1985, c. C-46, ss. 380, 342.1 :
7. ألمانيا. Strafgesetzbuch §§ 263, 263a, 269 :
8. فرنسا. Code pénal, Articles 313-1, 323-1 :
9. سويسرا. Swiss Criminal Code, Articles 146, 147, 143bis :
10. أستراليا. Criminal Code Act 1995, ss. 480.4–480.6 :

ثانياً: الاتفاقيات والتشريعات الدولية

11. Convention on Cybercrime, Budapest, 2001, ETS No. 185.
12. Second Additional Protocol to the Convention on Cybercrime, 2022, CETS No. 224.

13. United Nations Convention against Cybercrime, UN General Assembly Resolution 79/243, 24 December 2024.

14. Directive (EU) 2019/713 of the European Parliament and of the Council, 17 April 2019.

15. Regulation (EU) 2024/1689, Artificial Intelligence Act.

16. International Covenant on Civil and Political Rights, UN General Assembly Resolution 2200A (XXI), 1966.

ثالثاً: التقارير والوقائع الدولية

17. Federal Bureau of Investigation, Internet Crime Complaint Center, 2025 IC3 Annual Report.

18. INTERPOL, Global Financial Fraud Threat Assessment 2026.

19. INTERPOL, HAECHI VI, September 2025.

20. INTERPOL, First Light 2026, July 2026.

21. Hong Kong Government, official statements concerning deepfake-enabled financial fraud, June 2024.