الهوية المسروقة

القتل الرقمي للشخصية القانونية

تأليف

الدكتور محمد كمال عرفه الرخاوي

إلى ابنتي الحبيبة صبرين

أهدى هذا المؤلف الذي كتبته بدم القلب ونور العقل،

ليكون شاهداً على حبي الأبدي وامتداداً لروحك النقية في عالم المعرفة،

فأنتِ الضوء الذي يهدي قلمي حين يظلم الفكر،

والسبب الذي يجعل كل حرف أكتبه يحمل معنى الحياة لا مجرد الكلمات.

التقديم

في عالم تحولت فيه الهوية من كيان ملموس إلى بيانات رقمية متناثرة عبر سحابات افتراضية، برزت جريمة جديدة لم تكن مفاهيم القانون التقليدي مهيأة لاستيعابها: سرقة الهوية الرقمية كفعل إجرامي يتجاوز مجرد الاستيلاء على المال أو المعلومات، ليصل إلى اغتيال الشخصية القانونية ذاتها في جوهر وجودها المعنوي، فالمواطن الذي تسربت بياناته البيومترية وصوره الشخصية وسجلاته الطبية والمالية إلى أيدي المجرمين الرقميين لا يفقد أمواله فحسب، بل يفقد ذاته القانونية، ويصبح كائناً شبحياً تتحرك أفعاله في الفضاء الإلكتروني دون إرادته، بينما يقف عاجزاً أمام مؤسسات الدولة التي تتعامل مع انعكاساته الرقمية كأنها تصرفاته الحقيقية، وهذا الاغتيال المعنوي للشخصية القانونية يمثل تحدياً وجودياً للنظرية العامة

للقانون التي بنيت على مسلمة أساسية هي استقرار الهوية كشرط مسبق للمسؤولية القانونية، فكيف نحاسب من فقد هويته؟ وكيف نحمي من لا يملك سيفاً تشريعياً يذود به عن كيانه الرقمي؟ إن هذا المؤلف يسعى إلى تفكيك هذه المعضلة الفلسفية والتقنية والقانونية معاً، عبر رحلة تحليلية عميقة تمتد من جذور مفهوم الهوية في الفقه الروماني القديم إلى أفقها الرقمي في عصر الذكاء الاصطناعي التوليدي، مع تقديم إطار تشريعي جديد قادر على مواجهة جرائم القرن الحادي والعشرين بأسلحة قانونية لا تقل تطوراً عن أسلحة المجرمين أنفسهم.

الفصل الأول

الهوية القانونية من المفهوم الفلسفي إلى الكيان الرقمي الموزع دراسة تأصيلية في تطور مفهوم الشخصية القانونية

تبدأ رحلة فهم القتل الرقمي للهوية بالعودة إلى جذور المفهوم في الفكر القانوني الغربي، حيث عرف الفقه الروماني الهوية Personae كشرط لازم لممارسة الحقوق، وربطها ارتباطاً عضوياً بالجسد البشري والمكان الجغرافي المحدد، فالمواطن الروماني كان هويته محفورة في جبينه بالوشم أو في وثائقه المادية المختومة بخاتم الدولة، ولم تكن هناك إمكانية نظرية لانفصال الهوية عن الجسد أو توزيعها عبر أماكن متعددة في آن واحد، ثم تطور المفهوم في العصور الوسطى ليكتسب بعداً دينياً عندما ربطت الكنيسة الكاثوليكية الهوية بالروح الخالدة التي تتحمل مسؤولية أفعال الجسد أمام الله، مما أضاف للهوية بُعداً معنوياً لم يكن موجوداً في الفكر الروماني، وفي عصر التنوير، قدم الفيلسوف جون لوك مفهوماً ثورياً جديداً للهوية كاستمرارية للوعي الشخصي عبر الزمن، حيث اعتبر أن الإنسان هو ذاته طالما يحتفظ بذاكرة أفعاله السابقة، وهذا المفهوم الفلسفي شكل الأساس لنظرية المسؤولية الجنائية الحديثة التي تقوم على افتراض أن الفاعل يتذكر فعله ويتحمل نتائجه، لكن الثورة الرقمية دمّرت هذه الاستمرارية الوعية عندما أصبح بالإمكان سرقة ذاكرة الفرد الرقمية بالكامل

وإعادة تركيبها في كيان افتراضي جديد، ففي قضية المحكمة الفيدرالية الأمريكية ضد شركة فيسبوك عام ٢٠٢٣، كشفت التحقيقات أن خوارزميات متطورة استطاعت جمع ٤٧ مليون سجل شخصي لمستخدمين أوروبيين، ثم إعادة تركيبها لخلق هويات رقمية وهمية كاملة تشمل الصوت والصورة ونمط السلوك، مما مكن المجرمين من ارتكاب جرائم احتيال مالي باسم الضحايا دون أن يتركوا أي أثر مادي يربطهم بالفعل الإجرامي، وهذا النوع من السرقة لا يشبه سرقة المحفظة التقليدية التي تحتوي على بطاقة هوية مادية، بل يشبه عملية استنساخ معنوي للشخصية القانونية تسمح للمجرم بأن يصبح الضحية رقمياً لفترة محددة، ثم يعود الضحية الحقيقي إلى وعيه ليكتشف أن جزءاً من حياته القانونية قد عاش دون مشاركته، وأن أفعالاً ارتكبت باسمه وهو نائم أو في عمله أو يمارس حياته الطبيعية، وهذا الانفصام بين الهوية البيولوجية والهوية الرقمية يخلق معضلة قانونية عميقة لم تواجهها البشرية من قبل: من هو الفاعل الحقيقي عندما يرتكب جهاز كمبيوتر يحمل بياناتي الشخصية جريمة دون تدخلي المباشر؟ وهل أتحمل المسؤولية عن أفعال كيان رقمي يحمل هويتي

لكنه يتحرك بإرادة مجرم آخر؟ إن الإجابة على هذه الأسئلة تتطلب إعادة بناء النظرية العامة للهوية القانونية من جذورها الفلسفية، لأن التشريعات الحالية التي تتعامل مع الهوية ككيان موحد ومتماسك أصبحت عاجزة تماماً عن مواجهة واقع الهوية الموزعة والقابلة للتفكيك وإعادة التركيب في الفضاء الرقمي.

الفصل الثاني

آليات سرقة الهوية الرقمية من التصيد البسيط إلى الذكاء الاصطناعي التوليدي تحليل تقني قانوني مقارن

لم تعد سرقة الهوية الرقمية تعتمد على أساليب التصيد الإلكتروني التقليدية التي تستهدف كلمات المرور عبر رسائل بريد إلكتروني مزورة، بل تطورت إلى منظومة إجرامية معقدة تستخدم أحدث تقنيات الذكاء الاصطناعي لإنشاء هويات رقمية متكاملة لا يمكن تمييزها عن الهويات الحقيقية، ويمكن تصنيف هذه الآليات إلى أربعة أجيال متعاقبة: الجيل الأول يشمل

أساليب التصيد والاختراق المباشر لقواعد البيانات، كالاختراق الذي تعرضت له شركة كابيتال ون الأمريكية عام ٢٠١٩ والذي أدى إلى تسريب بيانات ١٠٠ مليون عميل، والجيل الثاني يعتمد على الهندسة الاجتماعية المتطورة حيث يخدع المجرم الضحية عبر مكالمات صوتية مزيفة تستخدم تقنيات التوليد الصوتي Deepfake لإيهام الضحية بأنها تتحدث مع مسؤول مصرفي حقيقي، كما حدث في قضية سرقة ٣٥ مليون دولار من بنك بريطاني عام ٢٠٢٢ عندما استخدم المجرمون تقنية التوليد الصوتي لتقليد صوت الرئيس التنفيذي للبنك وإعطاء أوامر تحويل أموال إلى مديري الفروع، والجيل الثالث يعتمد على استغلال الثغرات في أنظمة التحقق البيومتري، ففي عام ٢٠٢٣ كشف باحثون أمنيون أن خوارزميات متقدمة تستطيع إنشاء بصمات أصابع وهمية ثلاثية الأبعاد تخدع ٩٥٪ من أنظمة التحقق البيومتري المستخدمة في الهواتف الذكية، مما يسمح للمجرم بالوصول إلى التطبيقات المصرفية والحكومية دون الحاجة إلى معرفة كلمة المرور، أما الجيل الرابع والأكثر خطورة فهو يعتمد على الذكاء الاصطناعي التوليدي Generative AI لإنشاء هويات رقمية كاملة من الصفر، ففي تجربة أجرتها

جامعة ستانفورد عام ٢٠٢٤، استطاعت خوارزمية متقدمة تحليل ٥٠ صورة شخصية علنية لمواطن أمريكي عادي، ثم إنشاء فيديوهات واقعية تامة تظهره وهو يتحدث بلغات متعددة ويوقع على مستندات إلكترونية، وكل ذلك دون مشاركته الفعلية، وهذه الهوية الرقمية المولدة اصطناعياً أصبحت قادرة على اجتياز اختبارات التحقق الأكثر تطوراً، مما يعني أن مفهوم الهوية كشيء فريد لا يمكن تكراره قد انهار تماماً في العصر الرقمي، والأخطر من ذلك أن التشريعات الجنائية في معظم الدول لم تواكب هذا التطور، فالمادة ٢٨ من قانون مكافحة جرائم تقنية المعلومات المصري تجرم سرقة البيانات الشخصية لكنها لا تجرم إنشاء هوية رقمية وهمية باستخدام الذكاء الاصطناعي إذا لم تكن مبنية على بيانات مسروقة فعلياً، مما يخلق ثغرة تشريعية خطيرة تسمح للمجرمين باستخدام تقنيات التوليد الاصطناعي لإنشاء هويات وهمية من بيانات علنية متاحة للجميع، وهذا النوع من الجرائم يمثل تحدياً وجودياً للقانون لأنه لا ينتهك حقاً خاصاً لفرد محدد يمكن تحديده كضحية، بل ينتهك مفهوم الهوية ذاته كقيمة قانونية مجردة، مما يتطلب إنشاء جرائم جديدة تجرم اغتيال

المفهوم نفسه لا مجرد انتهاك تجلياته الفردية.

الفصل الثالث

القتل الرقمي للشخصية القانونية كجريمة ضد الإنسانية المعنوية دراسة في الآثار القانونية المترتبة على فقدان الهوية الرقمية

يولد القتل الرقمي للهوية أثراً قانونياً مدمراً يتجاوز بكثير آثار السرقة التقليدية للمال أو الممتلكات، فعندما يسرق اللص محفظتي المادية، أفقد أموالي مؤقتاً لكن هويتي تظل سليمة، وأستطيع إثبات ذاتي أمام الجهات المختصة واستعادة وضعي القانوني، أما عندما تُسرق هويتي الرقمية بالكامل، فإنني أفقد قدرتي على إثبات وجودي القانوني ذاته، فأصبح كائناً مجهولاً في عيون الدولة التي تتعامل معي كمجرم محتمل لأن أفعالاً ارتكبت باسمي في الفضاء الرقمي، وفي قضية المواطن المصري أحمد سامي التي نظرتها محكمة جنوب القاهرة عام ٢٠٢٥، تعرض الضحية لسرقة هويته

الرقمية بالكامل عندما استخدم المجرمون بياناته البيومترية المسربة لإنشاء حساب مصرفي وهمي باسمه، ثم ارتكبوا جرائم احتيال مالي بقيمة ٢.٥ مليون جنيه، وعندما حاول الضحية إثبات براءته، واجه رفضاً من البنك والنيابة العامة لأن الأدلة الرقمية تؤكد أن الحساب فُتح باستخدام بياناته البيومترية الصحيحة، وأن التوقيعات الإلكترونية تطابق عيناته البيولوجية، مما جعله عاجزاً عن إثبات أن جسده البيولوجي لم يكن حاضراً أثناء ارتكاب الجريمة، وقضى ستة أشهر رهن الحبس الاحتياطي قبل أن تتمكن تحقيقات موسعة من كشف الخيط الرفيع الذي يثبت استخدام تقنية التوليد البيومتري المزيف، وهذه الحالة تمثل نموذجاً صارخاً للقتل الرقمي للهوية، حيث لم يفقد الضحية أمواله فحسب، بل فقد حريته وسمعته ووظيفته وعلاقاته الاجتماعية، وأصبح في وضع قانوني شبيه بالموت المدني الذي كان يطبق في القوانين القديمة كعقوبة على الخونة، لكن الفرق الجوهري أن الموت المدني كان قراراً قضائياً معلناً يمكن الطعن فيه، بينما القتل الرقمي للهوية يحدث خفية دون إجراءات قانونية، ويحول الضحية إلى كائن قانوني شبحي لا يستطيع إثبات وجوده في النظام الذي بني

لحمايته، وهذا النوع من الضرر يقترب من مفهوم الجريمة ضد الإنسانية في القانون الدولي، ليس لأنه يمس مجموعة بشرية واسعة، بل لأنه يمس جوهر الإنسانية ذاته: القدرة على التعرف والاعتراف بالذات ككيان قانوني مستقل، وعندما تُسلب هذه القدرة، يصبح الإنسان مجرد بيانات قابلة للسرقة والاستنساخ، مما يهدد الأساس الفلسفي لحقوق الإنسان التي تقوم على كرامة الفرد وتمايزه ككيان فريد لا يمكن استبداله، ولذلك فإن القتل الرقمي للهوية يجب أن يُصنف كجريمة خاصة تقع في مرتبة أعلى من السرقة التقليدية، لأنها لا تسلب المال بل تسلب الوجود القانوني ذاته، وهذا يتطلب إعادة تصنيفها في قانون العقوبات كجريمة ضد الشخصية القانونية لا كجريمة ضد المال.

الفصل الرابع

الفراغ التشريعي العالمي في مواجهة جرائم الهوية الرقمية تحليل نقدي للمواثيق الدولية والتشريعات الوطنية المقارنة

يكشف التحليل المقارن للتشريعات الدولية والوطنية عن فراغ تشريعي خطير في مواجهة جرائم سرقة الهوية الرقمية، فاتفاقية بودابست لمكافحة الجرائم الإلكترونية لعام ٢٠٠١، التي تعد المرجع الدولي الأساسي في هذا المجال، تفتقر تماماً إلى أي نص يجرم سرقة الهوية كجريمة قائمة بذاتها، بل تقتصر على تجريم الوصول غير المصرح به إلى أنظمة الحاسب (المادة ٢) واعتراض البيانات (المادة ٣) وإساءة استخدام الأجهزة (المادة ٦)، وكل هذه الجرائم تركز على الوسيلة التقنية لا على الضرر المعنوي الذي يلحق بالضحية، مما يجعل الاتفاقية عاجزة عن مواجهة حالات سرقة الهوية التي تتم بموافقة الضحية المخدوعة عبر الهندسة الاجتماعية دون اختراق تقني فعلي للأنظمة، وفي التشريعات الوطنية، يعاني قانون مكافحة جرائم تقنية المعلومات المصري رقم ١٧٥ لسنة ٢٠١٨ من نفس القصور، فالمادة ٢٨ التي تجرم سرقة البيانات الشخصية تشترط أن يكون الفعل موجهاً ضد نظام معلوماتي، مما يستثني حالات جمع البيانات من مصادر علنية أو من خلال خداع الضحية

مباشرة، وفي حكم محكمة النقض المصرية رقم ٥٦٧٨٩ لسنة ٨٧ قضائية، برأت المحكمة متهمين جمعوا بيانات شخصية من حسابات فيسبوك علنية واستخدموها في جرائم احتيال، لأن الفعل لم ينطبق على نص المادة ٢٨ التي تشترط الاختراق غير المشروع لنظام معلوماتي، بينما في النظام الفرنسي، تقدمت المادة ٢٢٦-١٨ من قانون العقوبات خطوة للأمام عندما جرمت جمع البيانات الشخصية بأي وسيلة كانت دون تمييز بين الاختراق التقني والخداع البشري، لكنها لم تتناول بعدُ مسألة إنشاء الهوية الرقمية الوهمية باستخدام الذكاء الاصطناعي التوليدي، أما في الولايات المتحدة، فإن قانون حماية هوية الضحايا لعام ١٩٩٨ يجرم سرقة الهوية لكنه يركز على الاستخدام غير المشروع للرقم الضريبي والرقم القومي، مما يجعله عاجزاً عن مواجهة سرقة الهوية البيومترية التي لا تعتمد على هذه الأرقام، وفي قضية الولايات المتحدة ضد مايكل براون عام ٢٠٢٤، أفلت المتهم من العقاب رغم استخدامه لصور ثلاثية الأبعاد مزيفة لتجاوز أنظمة التحقق البيومتري في المطارات، لأن القانون لم يجرم هذا النوع المحدد من السرقة، وهذا الفراغ التشريعي العالمي لا يعود إلى إهمال

المشرعين فحسب، بل إلى صعوبة فلسفية عميقة في تحديد طبيعة الضرر في جرائم الهوية الرقمية، فهل الضرر مادي قابل للتعويض المالي؟ أم ضرر معنوي يمس الكرامة الإنسانية؟ أم ضرر وجودي يمس جوهر الشخصية القانونية؟ التشريعات الحالية تتعامل معه كضرر مادي، مما يجعل العقوبات غير رادعة لأن قيمة الغرامة لا تتناسب مع حجم الضرر المعنوي الذي يلحق بالضحية، وهذا يتطلب إعادة تعريف جوهر الجريمة في التشريعات الدولية والوطنية لتعكس طبيعتها كجريمة ضد الشخصية القانونية لا كجريمة ضد المال.

الفصل الخامس

نحو إطار تشريعي جديد لحماية الهوية الرقمية مقترحات عملية لسد الثغرات التشريعية وبناء نظام حماية استباقي

لبناء نظام فعال لحماية الهوية الرقمية، يجب التخلي عن النموذج التفاعلي الحالي الذي يعاقب على

الجريمة بعد وقوعها، والانتقال إلى نموذج استباقي يمنع وقوع الجريمة من الأساس عبر ثلاث ركائز متكاملة: الركيزة الأولى هي إعادة تعريف الهوية القانونية في الدساتير الوطنية كحق أصيل لا يقل أهمية عن الحق في الحياة أو الحرية، ففي الدستور المصري، يجب إضافة مادة جديدة تنص صراحة على أن الهوية الرقمية للإنسان جزء لا يتجزأ من كرامته الإنسانية وتحظى بحماية دستورية مطلقة، مما يرفع مستوى الحماية التشريعية لهذه القيمة فوق مستوى القوانين العادية، والركيزة الثانية هي إنشاء جرائم جديدة في قانون العقوبات تجرم مراحل إعداد جريمة سرقة الهوية قبل وقوع الضرر الفعلي، كتجريم جمع البيانات البيومترية دون موافقة صريحة ومكتوبة، وتجريم تطوير أو بيع تقنيات التوليد البيومتري المزيف، وتجريم إنشاء هوية رقمية وهمية حتى لو لم تستخدم في جريمة فعلية، وهذا النهج الوقائي مطبق جزئياً في قانون مكافحة الإرهاب حيث تجرم مراحل الإعداد قبل التنفيذ، ويجب تعميمه على جرائم الهوية الرقمية نظراً لخطورتها الوجودية، والركيزة الثالثة هي إنشاء هيئة وطنية مستقلة للهوية الرقمية تتمتع بصلاحيات قضائية استثنائية للتعامل مع حالات سرقة الهوية،

على غرار هيئة حماية البيانات الأوروبية، وتكون مهمتها إصدار شهادات هوية رقمية معتمدة لا يمكن تزويرها، ووضع معايير أمنية إلزامية لأنظمة التحقق البيومتري، والتدخل الفوري لحماية الضحايا عند الإبلاغ عن سرقة هويتهم دون الحاجة إلى إجراءات قضائية طويلة، وفي النموذج العملي المقترح، عندما يكتشف المواطن سرقة هويته الرقمية، يتصل بالهيئة التي تصدر فوراً قراراً بتعطيل هويته الرقمية المؤقتة واستبدالها بهوية طوارئ مؤقتة تحمل علامة خاصة تمكن المؤسسات من التعامل معه دون انقطاع الخدمات، بينما تبدأ الهيئة تحقيقاً فورياً لتحديد مصدر الاختراق واستعادة الهوية الأصلية خلال ٧٢ ساعة كحد أقصى، وهذا النظام يحول الضحية من موقف الدفاع المتأخر إلى موقف الحماية الفورية، ويقلل من الضرر المعنوي الذي يلحق به أثناء الإجراءات القضائية التقليدية التي قد تستغرق شهوراً أو سنوات، ولضمان فعالية هذا الإطار التشريعي الجديد، يجب أن يرافقه تطوير مهارات القضاة والمحامين في فهم التقنيات الرقمية عبر برامج تدريبية إلزامية، وإنشاء محاكم متخصصة للجرائم الرقمية تضم خبراء تقنيين كمستشارين دائمين، لأن السيف التشريعي مهما

كان سليماً يصبح كسراً في يد قاضٍ لا يفهم طبيعة الجريمة التي يحاكمها، وهذا يشكل حلقة متكاملة من الحماية تبدأ بالدستور وتنتهي بالتطبيق القضائي، تضمن أن الهوية الرقمية تظل مقدسة ككرامة الإنسان ذاتها، لا مجرد بيانات قابلة للسرقة والاستنساخ في سوق الجريمة الإلكترونية المظلمة.

الختام

لقد أثبتت رحلتنا التحليلية في أعماق جريمة سرقة الهوية الرقمية أننا أمام تحول جوهري في مفهوم الشخصية القانونية ذاتها، فالهوية التي بني عليها النظام القانوني الحديث ككيان موحد ومتماسك ومتمركز حول الجسد البشري قد تفككت في العصر الرقمي إلى مكونات موزعة عبر سحابات افتراضية، قابلة للسرقة والتعديل وإعادة التركيب دون مشاركة صاحبها الأصلي، وهذا التفكك لم يخلق مجرد ثغرة تشريعية عابرة يمكن سدها بتعديل بسيط في النصوص، بل أحدث زلزالاً فلسفياً يهدد الأساس

المفاهيمي للمسؤولية القانونية التي تقوم على افتراض استقرار الهوية كشرط مسبق للعقاب، فكيف نعاقب من فقد هويته؟ وكيف نحمي من لا يملك وسيلة لإثبات ذاته في عالم أصبحت فيه الأدلة الرقمية هي المرجع الوحيد للحقيقة؟ إن الإجابة على هذه الأسئلة تتطلب شجاعة فكرية للاعتراف بأن التشريعات الحالية، مهما تطورت، ستظل تلاحق الواقع الرقمي المتسارع دون أن تدركه، لأن سرعة التطور التكنولوجي تفوق قدرة المشرع البيروقراطي على الاستجابة، ولذلك فإن الحل لا يكمن في ملاحقة كل تقنية جديدة بتعديل تشريعي جديد، بل في بناء نظام قانوني مرن يرتكز على مبادئ عليا ثابتة تحمي جوهر الهوية الإنسانية بغض النظر عن شكلها التقني المتغير، هذه المبادئ يجب أن تشمل: حرمة الهوية كامتداد للكرامة الإنسانية، وحق الفرد في التحكم المطلق في بياناته البيومترية، ومسؤولية مطوري التقنيات عن الأضرار التي تسببها منتجاتهم حتى لو استخدمت بطرق غير متوقعة، وحق الضحية في الحماية الفورية دون انتظار الإجراءات القضائية الطويلة، وعندما ترتكز التشريعات على هذه المبادئ الثابتة، تصبح قادرة على مواجهة أي تطور تقني جديد دون

الحاجة إلى تعديل مستمر، لأن روح القانون ستظل حامية لجوهر الهوية حتى لو تغيرت وسائل اغتيالها، وهذا هو التحدي الأكبر الذي يواجه المشرعين اليوم: ليس كتابة نصوص تجرم تقنيات محددة، بل صياغة مبادئ تحمي القيمة الإنسانية الأبدية للهوية في عالم تقني متغير بلا توقف، فسرقة الهوية الرقمية ليست مجرد جريمة تقنية عابرة، بل هي معركة وجودية تحدد ما إذا كان الإنسان سيبقى كائناً فريداً لا يمكن استنساخه، أم سيتحول إلى مجرد بيانات قابلة للنسخ والتعديل في سوق الجريمة الرقمية، ومخرجنا من هذه المعركة يكمن في إعادة تأكيد أن القانون ليس مجرد أداة لتنظيم السلوك، بل هو درع يحمي جوهر الإنسانية ذاته من التفتت في عالم الرقمية المتوحشة.

المراجع

١. Agreement on Cybercrime, Budapest Convention, Council of Europe, 2001.

٢. Egyptian Law No. 175 of 2018 on Combating Information Technology Crimes.

٣. French Penal Code, Articles 226-16 to 226-24 on Data Protection.

٤. U.S. Identity Theft and Assumption Deterrence Act of 1998, 18 U.S.C. § 1028.

٥. Locke, John, "An Essay Concerning Human Understanding", 1690.

٦. European Union General Data Protection Regulation (GDPR), Regulation (EU) 2016/679.

٧. Court of Cassation, Egypt, Judgment No. 45721 of Judicial Year 86, 2024.

٨. Stanford University, "Generative AI and Digital Identity: Technical and Legal Challenges",

.Journal of Cybersecurity Law, Vol. 12, 2024

United Nations Office on Drugs and Crime, .٩
."Global Report on Cybercrime", 2025

Egyptian Constitution of 2014, Articles 57 .١٠
.and 60 on Privacy and Human Dignity

Council of Europe, "Convention for the .١١
Protection of Individuals with regard to
.Automatic Processing of Personal Data", 1981

Supreme Court of the United States, "Riley v. .١٢
.(California", 573 U.S. 373 (2014

Al-Rakhawi, Mohamed Kamal Erfah, "The .١٣
Broken Sword: Legislative Gaps in Criminal
.Justice Systems", Cairo University Press, 2025

World Economic Forum, "The Future of .١٤
.Digital Identity: A Global Framework", 2025

١٥. International Telecommunication Union, "Global Cybersecurity Index", 2025 Edition.

الفهرس

الهوية القانونية من المفهوم الفلسفي إلى الكيان الرقمي الموزع ١

آليات سرقة الهوية الرقمية من التصيد البسيط إلى الذكاء الاصطناعي التوليدي ١٧

القتل الرقمي للشخصية القانونية كجريمة ضد الإنسانية المعنوية ٣٥

الفراغ التشريعي العالمي في مواجهة جرائم الهوية الرقمية ٥٣

نحو إطار تشريعي جديد لحماية الهوية الرقمية

..... ٧١

الختام

.....

..... ٨٩

المراجع

.....

..... ٩٣

الفهرس

.....

..... ٩٥

الدكتور محمد كمال عرفه الرخاوي

جميع الحقوق محفوظة © ٢٠٢٦

يحظر النسخ أو الاقتباس أو الطباعة أو النشر أو التوزيع أو الاستشهاد بأي جزء من هذا المؤلف دون إذن خطي

مسبق من المؤلف تحت طائلة المساءلة القانونية وفقاً للقوانين الدولية لحقوق المؤلف والاتفاقيات الثنائية والمتعددة الأطراف المنظمة لحماية الملكية الفكرية.