الإطار القانوني للهوية الرقمية وحماية البيانات الحيوية

The Legal Framework of Digital Identity and Biometric Data Protection

تأليف

د. محمد كمال عرفه الرخاوي

١

الإهداء

إلى ابنتي الحبيبة صبرينال

نور عيني وفخر جبيني

التي تجمع بين روح النيل الخالد

وساحل البحر الأبيض المتوسط

وجبال الأوراس الشامخة

إليكِ أهدي هذا الجهد المتواضع

تعبيراً عن حبّي العميق وفخري الأبدي

واعتزازي بانتمائك إلى ضفتي الأصالة

مصر أم الدنيا والجزائر بلد المليون شهيد

فلتبقى يداكِ نبع خير

وقلبكِ معيناً للعطاء

وعقلكِ سراجاً للحق والعدل

وصبرينال يا ابنتي

أنتِ المستقبل المشرق

والحاضر العطوف

والماضي الممجد

فلكِ من أبيكِ كل الحب

ومن قلبه كل الدعاء

أن يحفظكِ الله ويرعاكِ

ويجعلكِ ذخراً لوطنكِ ولأمتكِ

د. محمد كمال عرفه الرخاوي

٢

التقديم

في عصر التحول الرقمي المتسارع، أصبحت الهوية الرقمية البوابة الأساسية

للمشاركة في الحياة الاقتصادية والاجتماعية

والسياسية، حيث تُستخدم لفتح الحسابات

البنكية، والتسجيل في الخدمات الحكومية، والتصويت الإلكتروني، وحتى السفر عبر

المطارات دون تدخل بشري، وتستند هذه الهوية في جوهرها إلى ما يسمى بالبيانات

الحيوية أو البيومترية، كالبصمة، وقزحية العين، وبصمة الوجه، والصوت، وهي بيانات

تتميز بطابعها الفريد وغير القابل للتغيير، مما يجعلها أداة تعريف فعالة، لكنها في

نفس الوقت تشكل تهديداً وجودياً لخصوصية الفرد إذا تم اختراقها أو استغلالها

بدون رقابة قانونية صارمة، ورغم أهمية هذه البيانات، فإن التشريعات الوطنية لا

تزال تعاني من تأخر كبير في تنظيم جمعها وتخزينها واستخدامها، إذ تفتقر العديد

من القوانين إلى تعريف دقيق للهوية الرقمية، أو تحديد واضح لحدود استخدام البيانات

الحيوية، أو فرض عقوبات رادعة على انتهاكها، ومن هذا المنطلق، يأتي هذا العمل

الأكاديمي العملي ليقدم لأول مرة على المستوى العربي تحليلاً شاملاً ومتعمقاً للإطار

القانوني للهوية الرقمية وحماية البيانات الحيوية في ثلاث أنظمة قانونية مدنية رئيسية

هي مصر والجزائر وفرنسا، مع مقارنات دقيقة مع المعايير الدولية، بهدف استخلاص

أفضل الممارسات وتقديم توصيات تشريعية عملية، ويستند البحث إلى دراسة ميدانية

لأحكام قضائية فعلية، وتحليل فقهي دقيق للنصوص التشريعية الحديثة، مع التركيز على

الجوانب العملية التي تهم المواطن والمحامي والقاضي، كآليات الموافقة، وحقوق الحذف

والتصحيح، وآليات الرقابة على قواعد البيانات الوطنية، كما يتناول البحث الإشكاليات

النظرية المتعلقة بطبيعة البيانات الحيوية كملكية خاصة، ويبحث في العلاقة بين الأمن

القومي وحقوق الإنسان في سياق جمع هذه البيانات، ويخصص فصولاً خاصة لدراسة

ظاهرة الاحتيال البيومتري، وتحديات حماية الأطفال، ودور الشركات الخاصة في إدارة

الهوية الرقمية، ويبقى أن هذا الموضوع يمثل تحدياً قانونياً وأخلاقياً غير مسبوق

يتطلب توازناً دقيقاً بين الكفاءة الرقمية وحماية الكرامة الإنسانية

٣

الفصل الأول

مفهوم الهوية الرقمية والبيانات الحيوية في الفقه القانوني الحديث

يُعد تحديد المفهوم الدقيق للهوية الرقمية

والبيانات الحيوية الخطوة الأولى والأساسية

لأي دراسة قانونية متعمقة، إذ أن غموض
المصطلح يؤدي حتماً إلى غموض في التنظيم

وخلل في التطبيق القضائي، ويُعرّف الفقه
القانوني الحديث الهوية الرقمية بأنها مجموعة

من السمات والبيانات التي تمثل شخصاً
طبيعياً أو اعتبارياً في الفضاء الرقمي، وتسمح

بتحديده بشكل فريد والتحقق من هويته دون
الحاجة إلى وثائق ورقية، وتشمل هذه

السمات الاسم، رقم الهوية، العنوان الرقمي،
بالإضافة إلى البيانات الحيوية التي تشكل

جوهر الهوية الرقمية الحديثة، أما البيانات
الحيوية أو البيومترية، فتُعرف بأنها بيانات

شخصية تتعلق بالخصائص الجسدية أو الفسيولوجية أو السلوكية للفرد، والتي تسمح

بتحديده بشكل فريد، مثل بصمة الإصبع، وقزحية العين، وبصمة الوجه، وشكل الأذن

والصوت، ونمط المشي، وحتى الحمض النووي، وتتميز هذه البيانات بعدة خصائص

جوهرية، أولها الطابع الفريد، الذي يجعل من المستحيل تقليدها أو مشاركتها مع غيرها

وثانيها الطابع الثابت، الذي لا يتغير مع مرور الزمن، وثالثها الطابع الحساس، الذي

يكشف عن معلومات عميقة عن حياة الفرد الخاصة، ورابعها الطابع غير القابل للإلغاء

فإذا تم اختراق بصمة إصبعك، فلا يمكنك تغييرها كما تغير كلمة المرور، مما يجعل

من انتهاكها كارثة دائمة، ومن الناحية التقنية، تعتمد أنظمة الهوية الرقمية على عدة

مكونات، منها قاعدة البيانات المركزية التي تخزن المعلومات، وأنظمة جمع البيانات

الحيوية عند نقاط التسجيل، وخوارزميات المطابقة التي تتحقق من الهوية عند كل استخدام

وقد تطورت هذه الأنظمة بشكل كبير في السنوات الأخيرة، بفضل الذكاء الاصطناعي

الذي يزيد من دقة المطابقة، لكنه في نفس الوقت يزيد من مخاطر التحيز والتمييز

ومن الجدير بالذكر أن الهوية الرقمية لا تقتصر على الأفراد فقط، بل قد تمتد إلى

الشركات والمؤسسات، حيث تُستخدم لتوقيع العقود الإلكترونية والتعامل مع الجهات

الحكومية، وهو ما يوسع من نطاق الحماية القانونية المطلوبة، ويبقى أن فهم هذه

المفاهيم بدقة هو المفتاح لبناء نظام قانوني فعال يحمي الحقوق دون أن يعيق الابتكار

٤

الفصل الثاني

الأسس النظرية لتنظيم الهوية الرقمية وحماية

البيانات الحيوية

لا يمكن تنظيم أي نظام قانوني للهوية الرقمية دون وجود أسس نظرية راسخة تبرره

وذلك انطلاقاً من مبدأ الشرعية الذي يقضي بعدم جواز التدخل في الحقوق دون نص

ومن هذا المنطلق، فإن تنظيم الهوية الرقمية يستند إلى مجموعة من الأسس النظرية

التي تتمثل في الحق في الخصوصية، وحماية الكرامة الإنسانية، وضرورة الأمن القومي

ومبدأ التناسب، وهذه الأسس هي التي تمنح المشرع الحق في التدخل لتنظيم هذه

الأنظمة الحساسة، وأول هذه الأسس هو الحق في الخصوصية، وهو حق دستوري مكفول

في جميع الدول المدنية الحديثة، حيث أن جوهر الهوية الرقمية هو جمع معلومات

شديدة الخصوصية عن الفرد، وهو ما يشكل اعتداءً صارخاً على حياته الخاصة إذا

تم دون رقابة، وثاني الأسس هو حماية الكرامة الإنسانية، إذ أن تحويل الإنسان إلى

مجموعة من البيانات الرقمية قد يجرده من إنسانيته ويعرضه للتمييز أو الاستغلال

وثالث الأسس هو ضرورة الأمن القومي، حيث أن أنظمة الهوية الرقمية تساعد في

مكافحة الإرهاب والجريمة المنظمة والهجرة غير الشرعية، مما يبرر جمع البيانات

الحيوية على نطاق واسع، ورابع الأسس هو مبدأ التناسب، الذي يقضي بأن يكون

التدخل في الحقوق مطلوباً ومتناسباً مع الهدف المنشود، فلا يجوز جمع بصمة الوجه

للحصول على بطاقة مكتبة، بينما قد يكون ذلك مبرراً للحصول على جواز سفر

ومن هنا، نجد أن التشريعات تختلف في كيفية تبنيها لهذه الأسس النظرية، فبعضها

مثل التشريع الفرنسي يعطي الأولوية للخصوصية وحقوق الإنسان، بينما يميل البعض

الآخر كالمصري في بداياته إلى إعطاء الأولوية للأمن القومي، وقد تطورت التشريعات

تدريجياً لتعكس توازناً أفضل بين هذه الأسس،

كما في حالة اللائحة الأوروبية GDPR

التي أصبحت معياراً عالمياً، ويبقى أن هذه الأسس النظرية لا تبرر التنظيم فحسب

بل تحدد أيضاً حدوده، فلا يجوز جمع بيانات حيوية لا تحقق شروط التناسب أو

الضرورة، حفاظاً على الحريات العامة وتجنب التوسع التعسفي في نطاق الدولة الرقمية

٥

الفصل الثالث

الهوية الرقمية والبيانات الحيوية في التشريع المصري

في مصر، شهدت السنوات الأخيرة تطوراً كبيراً في مجال الهوية الرقمية، مع إطلاق

مشروع بطاقة الهوية الوطنية الموحدة التي تعتمد على البيانات الحيوية، وصدر قانون

حماية البيانات الشخصية رقم 151 لسنة 2020 كخطوة تشريعية مهمة، إلا أن هذا القانون

لا يحتوي على نصوص خاصة بالبيانات الحيوية، بل يصنفها كبيانات شخصية حساسة

تحتاج إلى موافقة كتابية صريحة من صاحبها قبل جمعها أو معالجتها، ونصت المادة 21

من القانون على أنه يعاقب بالحبس مدة لا تقل عن سنة ولا تزيد على ثلاث سنوات

وبغرامة لا تقل عن مائتي ألف جنيه ولا تزيد على مليون جنيه كل من قام بمعالجة

بيانات شخصية حساسة دون موافقة صاحبها، وتشمل البيانات الحساسة البيانات الحيوية

إلا أن التشريع المصري يعاني من عدة ثغرات جوهرية، أبرزها غياب تعريف دقيق للهوية

الرقمية في التشريعات ذات الصلة، واختلاف التعريفات بين الجهات الحكومية المختلفة

كوزارة الداخلية ووزارة الاتصالات، مما يخلق بلبلة قانونية، كما أن القانون لا ينص

على آليات واضحة لحق الفرد في حذف بياناته الحيوية أو تصحيحها، ولا يحدد مدة

تخزين هذه البيانات في قواعد البيانات

الحكومية، مما يعرضها للاختراق أو الاستغلال

على المدى الطويل، بالإضافة إلى ذلك، فإن القانون يمنح جهات إنفاذ القانون سلطات

واسعة لجمع البيانات الحيوية دون موافقة في حالات الأمن القومي، دون وجود رقابة

قضائية فعالة على استخدام هذه السلطات، وقد أكدت محكمة القضاء الإداري في أكثر

من حكم على أن جمع البيانات الحيوية يجب أن يكون متناسباً مع الغرض منه، إلا أن

هذه المبادئ لم تُترجم بعد إلى نصوص تشريعية ملزمة، ويبقى أن التشريع المصري يحتاج

إلى مزيد من التطوير ليواكب المعايير الدولية،

خاصة في مجال حماية الأطفال وضمان

استقلالية هيئة حماية البيانات الشخصية التي أنشأها القانون

٦

الفصل الرابع

الهوية الرقمية والبيانات الحيوية في التشريع الجزائري

في الجزائر، شهدت السنوات الأخيرة تحركاً تشريعياً ملحوظاً في مجال الهوية الرقمية

مع إطلاق مشروع بطاقة التعريف البيومترية الوطنية، وصدور الأمر رقم 22-04 المتعلق

بحماية البيانات الشخصية في عام 2022، والذي يُعد خطوة تشريعية مهمة، ونص هذا الأمر

على تصنيف البيانات الحيوية كبيانات شخصية ذات طابع حساس، ويشترط الحصول على

موافقة صريحة من صاحبها قبل جمعها أو معالجتها، ونصت المادة 38 من الأمر على

عقوبات تصل إلى الحبس من سنة إلى خمس سنوات وغرامة من 500 ألف إلى 5 ملايين

دينار جزائري لكل من قام بمعالجة بيانات حساسة دون موافقة، إلا أن التشريع الجزائري

يعاني من عدة ثغرات جوهرية، أبرزها غياب تعريف دقيق للهوية الرقمية في النصوص القانونية

واختلاف الممارسات بين الجهات الحكومية مثل وزارة الداخلية ووزارة البريد والمواصلات

مما يخلق ازدواجية في النظام، كما أن الأمر لا ينص على آليات واضحة لحق الفرد في

حذف بياناته الحيوية أو تصحيحها، ولا يحدد المدة القصوى لتخزين هذه البيانات في قواعد

البيانات الحكومية، مما يعرضها لمخاطر الاختراق على المدى الطويل، بالإضافة إلى ذلك

فإن الأمر يمنح السلطات الأمنية سلطات واسعة لجمع البيانات الحيوية دون موافقة في

حالات الأمن القومي، دون وجود رقابة قضائية فعالة على استخدام هذه السلطات، وقد

أكدت المحكمة العليا الجزائرية في عدة قرارات على أن جمع البيانات يجب أن يكون

متناسباً مع الغرض منه، إلا أن هذه المبادئ لم تُترجم بعد إلى نصوص تشريعية ملزمة

ويبقى أن التشريع الجزائري يحتاج إلى مزيد من التطوير ليواكب المعايير الدولية، خاصة

في مجال حماية الأطفال وضمان استقلالية السلطة الوطنية لحماية البيانات التي أنشأها الأمر

كما أن غياب برامج توعية وطنية حول حقوق المواطنين في الهوية الرقمية يشكل عقبة

كبيرة أمام تمكين الأفراد من الدفاع عن خصوصيتهم في العصر الرقمي

٧

الفصل الخامس

الهوية الرقمية والبيانات الحيوية في التشريع الفرنسي

يُعد التشريع الفرنسي من أكثر التشريعات تقدماً في مجال تنظيم الهوية الرقمية وحماية

البيانات الحيوية، حيث يعتمد على إطار تشريعي مزدوج: القانون المحلي واللوائح الأوروبية

وخاصة اللائحة العامة لحماية البيانات GDPR، والتي تصنف البيانات الحيوية كبيانات

شخصية حساسة للغاية، وتشترط موافقة

صريحة ومستنيرة من صاحبها قبل أي معالجة

وتنص على عقوبات باهظة تصل إلى 20 مليون يورو أو 4% من رقم الأعمال السنوي

للشركة المخالفة، وتم تطوير هذا الإطار بموجب قانون الجمهورية الرقمية لعام 2016

وقانون الأمن الداخلي الشامل لعام 2021، الذي نظم استخدام تقنيات التعرف على الوجه

في الأماكن العامة، ونص على وجوب الحصول على إذن قضائي مسبق لاستخدامها

ومن الجدير بالذكر أن التشريع الفرنسي يتميز بوجود هيئة مستقلة قوية هي اللجنة الوطنية

للمعلوميات والحريات CNIL، التي تتمتع بصلاحيات واسعة للرقابة والتحقيق وفرض

العقوبات

على الجهات المخالفة، سواء كانت حكومية أو خاصة، كما أن القضاء الفرنسي يلعب دوراً

فعالاً في حماية الحقوق، حيث أكدت محكمة النقض الفرنسية في عدة أحكام على أن

جمع البيانات الحيوية يجب أن يكون ضرورياً ومتناسباً مع الغرض منه، وألغت عدة

مشاريع حكومية لخرقها هذا المبدأ، بالإضافة إلى ذلك، فإن التشريع الفرنسي يوفر آليات

فعالة لحقوق الأفراد، مثل حق الوصول إلى بياناتهم، وحق تصحيحها، وحق حذفها

وحتى حق نقلها إلى جهة أخرى، ويتميز أيضاً بوجود آليات وقائية قوية لحماية الأطفال

من خلال اشتراط موافقة أولياء الأمور على جمع بياناتهم الحيوية، ويبقى أن التشريع

الفرنسي رغم تقدمه لا يخلو من انتقادات، خاصة من جهات إنفاذ القانون التي ترى فيه

عائقاً أمام مكافحة الإرهاب، لكنه يظل معياراً عالمياً يُحتذى به في التوازن بين الأمن

وحقوق الإنسان

٨

الفصل السادس

مقارنة تشريعية في عناصر تنظيم الهوية الرقمية

وحماية البيانات الحيوية

تختلف التشريعات الثلاثة بشكل جوهري في التعامل مع الهوية الرقمية والبيانات الحيوية

ففي مصر، يعتمد التشريع على قانون حماية البيانات الشخصية لعام 2020، الذي يصنف

البيانات الحيوية كبيانات حساسة لكنه يفتقر إلى التفاصيل الدقيقة حول آليات الجمع

والتخزين والاستخدام، ويمنح سلطات واسعة للجهات الأمنية دون رقابة قضائية فعالة

وفي الجزائر، يعتمد الأمر رقم 22-04 لعام 2022 على نفس المبدأ، لكنه يعاني من غموض

أكبر في التعريفات وآليات التنفيذ، ويفتقر إلى هيئة رقابية مستقلة ذات صلاحيات واسعة

أما في فرنسا، فيتميز التشريع بحداثة واضحة حيث يدمج بين القانون المحلي واللوائح

الأوروبية GDPR، ويفرض قيوداً صارمة على جمع البيانات الحيوية، ويشترط موافقة

قضائية مسبقة لاستخدام تقنيات التعرف على الوجه، ويمنح هيئة CNIL صلاحيات واسعة

للرقابة والعقاب، وتشترك التشريعات الثلاثة في تصنيف البيانات الحيوية كبيانات حساسة

وتشترط موافقة صاحبها قبل المعالجة، لكنها تختلف في درجة هذه الموافقة، ففي فرنسا

يجب أن تكون صريحة ومستنيرة ومكتوبة، بينما في مصر والجزائر، قد تُعتبر الموافقة

ضمنية في بعض الحالات، وخاصة في الخدمات الحكومية، ومن حيث الحماية، فإن التشريع

الفرنسي يوفر حماية أوسع للأفراد من خلال آليات الرقابة المستقلة وحقوق الحذف والتصحيح

بينما لا تزال هذه الآليات غائبة أو ضعيفة في التشريعات العربية، ويبقى أن التشريعات

العربية تحتاج إلى مزيد من التطوير لمواكبة التجربة الفرنسية، خاصة في مجال إنشاء

هيئات رقابية مستقلة وتحديد مدد تخزين البيانات وضمان الرقابة القضائية على الاستخدامات

الأمنية، مع الحفاظ على التوازن بين الكفاءة الرقمية وحماية الحقوق الأساسية

٩

الفصل السابع

العقوبات والتدابير الجزائية في انتهاكات الهوية الرقمية والبيانات الحيوية

تختلف العقوبات والتدابير الجزائية المقررة لانتهاكات الهوية الرقمية والبيانات الحيوية

في الدول الثلاثة، ففي مصر، يعاقب قانون حماية البيانات الشخصية بالحبس مدة لا تقل

عن سنة ولا تزيد على ثلاث سنوات، وبغرامة لا تقل عن مائتي ألف جنيه ولا تزيد

على مليون جنيه، وهي عقوبة صارمة تهدف إلى الردع، كما يجوز للمحكمة أن تأمر

بمصادرة الأجهزة المستخدمة في الانتهاك، وحظر استخدام البيانات لمدة محددة

وفي الجزائر، يعاقب الأمر رقم 22-04 بالحبس من سنة إلى خمس سنوات، وبغرامة

من 500 ألف إلى 5 ملايين دينار جزائري، وهي عقوبة مماثلة من حيث المدة، لكن

الغرامة أقل رادعية بسبب انخفاض قيمتها الشرائية، كما أن التدابير التكميلية مثل

مصادرة الأجهزة غير منصوص عليها صراحة، مما يحد من فعاليتها، أما في فرنسا

فيعاقب الجاني بغرامات باهظة تصل إلى 20

مليون يورو أو 4% من رقم الأعمال السنوي

وهو ما يعطيها أثراً رادعاً قوياً، خاصة ضد الشركات الكبرى، كما يجوز للهيئة CNIL

فرض تدابير وقائية مثل إلزام الشركة بحذف البيانات فوراً، أو تعطيل النظام المخالف

أو تعيين مسؤول حماية بيانات مستقل، ويمكن تشديد العقوبة في حالات الانتهاكات

التي تستهدف الأطفال أو تتم باستخدام تقنيات متطورة، أو ترتكب في إطار شبكة

إجرامية منظمة، ويبقى أن فعالية العقوبة لا تعتمد فقط على شدتها، بل على مدى

قدرة السلطات الرقابية على كشف الانتهاكات وجمع الأدلة، وهو التحدي الأكبر الذي

يواجه الهيئات الناشئة في الدول العربية، والتي تفتقر إلى الخبرة التقنية والموارد

البشرية اللازمة لمواجهة الشركات العالمية التي تمتلك بنى تحتية تقنية متطورة

١٠

الفصل الثامن

الاختصاص القضائي في انتهاكات الهوية الرقمية العابرة للحدود

تُعد انتهاكات الهوية الرقمية من أبرز الجرائم العابرة للحدود، نظراً لطبيعة الفضاء الرقمي

الذي لا يعترف بالحدود الجغرافية، حيث قد تُجمع البيانات الحيوية في دولة، وتُخزن في خوادم

بدولة أخرى، وتُستخدم من قبل شركة في دولة ثالثة، مما يطرح تحديات كبيرة أمام العدالة

في تحديد المحكمة المختصة والهيئة الرقابية المختصة، ويختلف موقف التشريعات الثلاثة

في التعامل مع هذا التحدي، ففي مصر، يعتمد قانون حماية البيانات الشخصية على مبدأ

الاختصاص المحلي، حيث تكون المحكمة المختصة هي المحكمة التي وقع فيها الضرر أو

التي يوجد فيها موطن المتهم، إلا أن هذا المبدأ يواجه صعوبات كبيرة في تحديد مكان

وقوع الانتهاك بدقة، خاصة إذا كانت الشركة تستخدم خوادم وسيطة في دول أخرى، وفي

الجزائر، يعتمد الأمر رقم 22-04 على مبدأ مشابه، حيث تكون المحكمة المختصة هي

المحكمة التي وقع فيها الفعل المجرم أو التي يوجد فيها موطن المتهم، لكن القضاء الجزائري

لا يزال يفتقر إلى الخبرة في تطبيق هذا المبدأ على الانتهاكات العابرة للحدود، أما في فرنسا

فيتميز التشريع بمرونة أكبر، حيث يسمح للهيئة CNIL بطلب التعاون الدولي من الدول الأخرى

لجمع الأدلة وتحديد مكان الانتهاك، كما أن فرنسا عضو في اتفاقية بودابست للجرائم الإلكترونية

وملتزمة باللوائح الأوروبية GDPR التي تمنح المواطنين حق تقديم الشكوى في أي دولة

أوروبية ضد أي شركة تنتهك بياناتهم، وتشترك التشريعات الثلاثة في الاعتراف بمبدأ

الاختصاص العالمي في حالات الانتهاكات الخطيرة التي تهدد الأمن القومي أو تمس المواطنين

من الدولة، إلا أن تطبيق هذا المبدأ يتطلب وجود معاهدات ثنائية أو متعددة الأطراف، وهو ما

يغيب في كثير من الحالات، ويبقى أن غياب تنسيق قضائي عربي موحد يشكل عقبة كبيرة

أمام مكافحة انتهاكات الهوية الرقمية في المنطقة، وهو ما يستدعي إنشاء آلية تعاون قضائي

إقليمية لتبادل المعلومات وتحديد الاختصاص، خاصة في ظل تزايد استثمار الشركات العالمية

في المنطقة العربية وتشغيل أنظمتها عبر الحدود

١١

الفصل التاسع

جمع الأدلة في انتهاكات الهوية الرقمية: التحديات والآليات

يُعد جمع الأدلة في انتهاكات الهوية الرقمية من أصعب المهام التي تواجه السلطات الرقابية

نظراً لطبيعة الأدلة الرقمية التي تتميز بالهشاشة والقابلية للتلاعب والحذف، بالإضافة إلى

صعوبة تتبع مصدرها في ظل استخدام تقنيات الإخفاء مثل الشبكات الافتراضية الخاصة VPN

وفي مصر، تواجه هيئة حماية البيانات الشخصية صعوبات كبيرة في الحصول على بيانات

من شركات التكنولوجيا العالمية، بسبب غياب آليات قانونية واضحة للتعاون، رغم وجود

بعض الاتفاقيات الثنائية، وفي الجزائر، تفتقر السلطة الوطنية لحماية البيانات إلى الخبرة

التقنية اللازمة لتحليل الأدلة الرقمية، كما أن التشريع لا ينص على إجراءات محددة لجمع

هذه الأدلة، مما يؤدي إلى بطلانها في كثير من الأحيان، أما في فرنسا، فيتميز النظام

القضائي بوجود وحدات متخصصة في جمع الأدلة الرقمية المتعلقة بالبيانات الحيوية، كما

أن هناك تشريعاً ً واضحاً ً يلزم شركات التكنولوجيا بتقديم البيانات المطلوبة في إطار زمني

محدد، تحت طائلة فرض غرامات باهظة، بالإضافة إلى التعاون الوثيق مع وكالات الأمن

السيبراني الأوروبية، ومن بين التحديات الرئيسية التي تواجه جمع الأدلة، صعوبة الحفاظ

على سلسلة الحفظ Chain of Custody، التي تضمن عدم تغيير الأدلة منذ لحظة جمعها

حتى عرضها أمام المحكمة، وكذلك صعوبة إثبات هوية الجاني الحقيقي في ظل استخدام

حسابات وهمية وأسماء مستعارة، وصعوبة استرجاع البيانات المحذوفة من الخوادم، وللتغلب

على هذه التحديات، تم تطوير آليات تقنية متقدمة مثل برامج تحليل البيانات الرقمية، وأنظمة

تتبع عناوين الآي بي، وأدوات فك تشفير المراسلات، إلا أن فعالية هذه الآليات تعتمد على

وجود إطار قانوني ينظم استخدامها ويحمي حقوق الأفراد، وهو ما يغيب في كثير من التشريعات

العربية، مما يجعل جمع الأدلة عملية معقدة وغير مضمونة النتائج

١٢

الفصل العاشر

دور شركات التكنولوجيا في إدارة الهوية الرقمية وحماية البيانات الحيوية

تلعب شركات التكنولوجيا الكبرى دوراً محورياً في منظومة الهوية الرقمية، نظراً لكونها

المالكة للمنصات التي تُجمع عبرها البيانات الحيوية، ولامتلاكها القدرة التقنية على تخزينها

وتحليلها، إلا أن هذا الدور يختلف بشكل كبير بين الدول، ففي فرنسا، يفرض التشريع

على شركات التكنولوجيا التزامات صارمة بفحص أنظمتها قبل جمع البيانات الحيوية، والإبلاغ

عن أي ثغرات قد تؤدي إلى انتهاكات، وتقديم البيانات المطلوبة للهيئة CNIL في إطار زمني

محدد، تحت طائلة فرض غرامات تصل إلى ملايين اليوروهات، كما أن الشركات تتعاون بشكل

وثيق مع الوحدات الحكومية لمكافحة الانتهاكات، وتقدم أدوات للمواطنين للإبلاغ الفوري عن

أي خرق لبياناتهم، بينما في مصر، لا ينص قانون حماية البيانات الشخصية على التزامات

واضحة لشركات التكنولوجيا، بل يقتصر الأمر على طلبات تعاون غير ملزمة، مما يحد من

فعالية جهود الإنفاذ، وغالباً ما ترفض الشركات العالمية تقديم البيانات بحجة حماية خصوصية

المستخدمين أو غياب المعاهدات الثنائية، وفي الجزائر، يعاني الموقف من غموض أكبر، حيث

لا يوجد تشريع ينظم العلاقة بين السلطة الوطنية لحماية البيانات وهذه الشركات، مما يجعل

التعاون يعتمد على المبادرات الفردية، وهو أمر غير كافٍ لمواجهة التحديات الكبيرة، ومن الجدير

بالذكر أن بعض شركات التكنولوجيا بدأت تطور آليات وقائية داخلية، مثل خوارزميات كشف

اختراق البيانات الحيوية، وأنظمة الإبلاغ التلقائي عن الانتهاكات، إلا أن هذه الآليات لا تزال

محدودة الفعالية، وتحتاج إلى دعم تشريعي وقضائي لتعزيزها، ويبقى أن غياب التزام قانوني

ملزم لشركات التكنولوجيا في الدول العربية يشكل ثغرة كبيرة في منظومة حماية الهوية الرقمية

وهو ما يستدعي سن تشريعات جديدة تفرض على هذه الشركات التعاون مع السلطات الرقابية

كجزء من مسؤوليتها الاجتماعية والقانونية، وتحديد آليات واضحة لاستجابة الطوارئ عند حدوث

اختراقات جماعية للبيانات الحيوية

١٣

الفصل الحادي عشر

الوقاية من انتهاكات الهوية الرقمية: الإطار المؤسسي والتوعوي

لا يمكن الاعتماد على العقوبة وحدها لحماية الهوية الرقمية، بل يجب اعتماد استراتيجية وقائية

شاملة تجمع بين التوعية والتأهيل والرقابة التقنية، وفي هذا المجال، تختلف الدول في نهجها

الوقائي، ففي فرنسا، توجد استراتيجية وطنية للهوية الرقمية تشمل حملات توعية واسعة في

المدارس والجامعات، وبرامج تدريب للقضاة والمحققين، ووحدات متخصصة في الشرطة للتعامل

مع البلاغات، كما أن هناك منصة وطنية للإبلاغ عن الانتهاكات تتيح للمواطنين تقديم بلاغاتهم

بشكل سري وآمن، وفي مصر، بدأت الجهات المعنية في إطلاق حملات توعية، خاصة عبر وسائل

التواصل الاجتماعي، إلا أن هذه الحملات لا تزال محدودة التأثير، وتفتقر إلى الاستمرارية

والشمول، كما أن البرامج التدريبية للهيئات الرقابية غير كافية، ولا توجد وحدات متخصصة

في جميع المحافظات، أما في الجزائر، فتقتصر الجهود الوقائية على تصريحات إعلامية من

حين لآخر، دون وجود استراتيجية وطنية متكاملة، مما يجعل الوعي الرقمي لدى الجمهور منخفضاً

جداً، ومن بين أهم عناصر الاستراتيجية الوقائية، نشر ثقافة الخصوصية الرقمية، وتعليم الأفراد

كيفية حماية بياناتهم الحيوية، مثل عدم مشاركتها على وسائل التواصل الاجتماعي، واستخدام

أنظمة المصادقة الثنائية، بالإضافة إلى تطوير أدوات تقنية وقائية مثل برامج الحماية من

الاختراق

وأنظمة إنذار مبكر عن محاولات الوصول غير المصرح به إلى قواعد البيانات، ويبقى أن الوقاية

هي السلاح الأقوى في مواجهة انتهاكات الهوية الرقمية، لأنها تحمي المواطنين قبل وقوع الضرر

وتوفر على الدولة تكاليف الملاحقة القضائية، وهو ما يستدعي تخصيص ميزانيات كافية وبناء

شراكات فعالة بين القطاعين العام والخاص لتنفيذ هذه الاستراتيجية

١٤

الفصل الثاني عشر

حماية الضحايا في انتهاكات الهوية الرقمية والبيانات الحيوية

تُعد حماية الضحايا من أهم الركائز في مكافحة انتهاكات الهوية الرقمية، نظراً للأضرار الجسيمة

التي قد يتعرضون لها، والتي قد تكون مالية أو نفسية أو اجتماعية، وفي فرنسا، يتمتع الضحايا

بحماية قانونية قوية، حيث يحق لهم طلب حذف بياناتهم الحيوية من قواعد البيانات فوراً، وطلب

تعطيل النظام المسبب للانتهاك، كما يحق لهم الحصول على دعم نفسي واجتماعي من

جهات

حكومية متخصصة، بالإضافة إلى حقهم في التعويض المدني عن الأضرار التي لحقت بهم، أما

في مصر، فلا توجد آليات قانونية فعالة لحماية الضحايا، حيث يصعب الحصول على أوامر قضائية

عاجلة لحذف البيانات الحيوية المسروقة، وغالباً ما يتعرض الضحايا لصعوبات كبيرة في إثبات

الضرر ونسبته إلى الانتهاك، مما يضاعف معاناتهم، كما أن الدعم النفسي غير متوفر بشكل منظم

وفي الجزائر، يعاني الضحايا من وضع أسوأ، حيث لا توجد أي آليات قانونية لحمايتهم، بل إن بعض

الضحايا يتعرضون للمحاسبة بدلاً من الجناة، خاصة إذا كانت البيانات الحيوية تتعلق بمعاملات

شخصية، وهو ما يدفع العديد من الضحايا إلى الصمت وعدم الإبلاغ عن الانتهاك، خوفاً من العواقب

الاجتماعية، ومن الجدير بالذكر أن حماية الضحايا لا تقتصر على الجانب القانوني، بل تمتد إلى

الجانب الاجتماعي، حيث يجب تغيير النظرة المجتمعية التي تلوم الضحية بدلاً من الجاني، وتعزيز

ثقافة الدعم والتعاطف، ويبقى أن غياب آليات حماية فعالة في الدول العربية يشكل عقبة كبيرة

أمام مكافحة هذه الانتهاكات، وهو ما يستدعي إدخال تعديلات تشريعية عاجلة تضمن حقوق الضحايا

وتوفّر لهم الحماية الكاملة من لحظة الإبلاغ وحتى نهاية الإجراءات القضائية، مع إنشاء وحدات

دعم متخصصة داخل الهيئات الرقابية لمساعدتهم

١٥

الفصل الثالث عشر

الهوية الرقمية كأداة للتمييز والرقابة الاجتماعية

يُعد استخدام الهوية الرقمية كأداة للتمييز أو الرقابة الاجتماعية أحد أخطر تجليات هذه التكنولوجيا

حيث تُستخدم أنظمة التعرف على الوجه لاستهداف فئات معينة بناءً على عرقهم أو دينهم أو آرائهم

السياسية، مما يؤدي إلى انتهاكات جسيمة لحقوق الإنسان، وقد بدأت المحاكم في الدول المتقدمة

بالاعتراف بهذه الظاهرة كشكل من أشكال الانتهاك الجنائي، ففي فرنسا، تم تقييد استخدام أنظمة

التعرف على الوجه في الأماكن العامة، ويعاقب عليها القانون إذا استخدمت للتمييز ضد

الأقليات

ويُعتبر المسؤول عن النظام مسؤولاً جنائياً حتى لو لم يقصد التمييز صراحة، إذا ثبت أنه أهمل في

فحص الخوارزميات لاكتشاف التحيز، أما في مصر والجزائر، فلا توجد نصوص خاصة تجرّم هذا

السلوك، بل يتم التعامل معه كانتهاك إداري أو مدني، مما يخلق فجوة تشريعية خطيرة، وتشير

الدراسات إلى أن نسبة كبيرة من أنظمة الهوية الرقمية في المنطقة العربية تعاني من تحيز ضد

فئات معينة، وهو ما يهدد بتكريس عدم المساواة بشكل آلي وغير مرئي، ويبقى أن تصنيف

استخدام

الهوية الرقمية للتمييز كجريمة جنائية هو خطوة ضرورية لبناء منظومة حماية شاملة للفئات

الضعيفة، وهو ما يتطلب تعديلات تشريعية عاجلة وتدريبات قضائية وتوعية مجتمعية مكثفة، مع

فرض التزامات على الجهات الحكومية والخاصة باختبار أنظمتها بانتظام لاكتشاف أي تحيز

١٦

الفصل الرابع عشر

الهوية الرقمية في بيئة العملات المشفرة

والمعاملات المجهولة

أدى دمج الهوية الرقمية مع تقنيات البلوك تشين والعملات المشفرة إلى ظهور تناقض جوهري

بين مبدأ الشفافية الذي تقوم عليه الهوية الرقمية، ومبدأ الخصوصية المطلقة الذي تتبناه

العديد من منصات العملات المشفرة، حيث تسعى الحكومات إلى ربط المحافظ الرقمية بهوية

حقيقية لمنع غسل الأموال وتمويل الإرهاب، بينما يرفض العديد من المستخدمين هذا الربط

باسم الحرية المالية، وفي مصر، لا يزال التشريع يتعامل مع هذه البيئة بشكل تقليدي، دون

إدراك للتحديات التقنية التي تفرضها، مما يعيق

جهود مراقبة المعاملات المشفرة، وفي الجزائر

يعاني الموقف من غموض أكبر، حيث لا يوجد تشريع ينظم العملات المشفرة أصلاً، مما يجعل

من الصعب تكييف انتهاكات الهوية الرقمية في هذا السياق، أما في فرنسا، فقد طورت السلطات

الرقابية آليات متقدمة لربط المحافظ الرقمية بالهوية الوطنية، بالتعاون مع شركات تحليل البلوك

تشين، كما أن هناك تشريعاً خاصاً يلزم منصات التداول بفحص هوية عملائها قبل السماح لهم

بالتداول، ومن بين التحديات الرئيسية صعوبة تحديد هوية المالك الحقيقي للمحفظة الرقمية

نظراً لسهولة إنشاء محافظ وهمية، وللتغلب على هذه التحديات، تم تطوير أدوات تقنية متقدمة

مثل برامج تحليل تدفق العملات، وأنظمة ربط المحافظ بالهويات الرقمية، إلا أن فعالية هذه

الأدوات تعتمد على وجود إطار قانوني يسمح باستخدامها ويحمي حقوق الأفراد، ويبقى أن غياب

تنظيم قانوني للعملات المشفرة في الدول العربية يشكل ثغرة كبيرة في منظومة حماية الهوية

الرقمية، وهو ما يستدعي سن تشريعات جديدة تنظم هذه الأصول وتحدد آليات ربطها بالهوية

الوطنية، مع الحفاظ على التوازن بين الأمن المالي وحقوق الخصوصية

١٧

الفصل الخامس عشر

الهوية الرقمية للأطفال والمراهقين: خصوصية الحماية

يُعد الأطفال والمراهقون من أكثر الفئات عرضة لانتهاكات الهوية الرقمية، نظراً لضعف وعيهم

الرقمي وسهولة استغلال بياناتهم الحيوية عبر الإنترنت، حيث يتم جمع بصماتهم أو صور وجوههم

من خلال تطبيقات الألعاب أو منصات التعليم الإلكتروني دون موافقة أولياء أمورهم، وتشير

الإحصائيات إلى أن نسبة كبيرة من انتهاكات الهوية الرقمية في الدول العربية تطال القصر، وذلك

بسبب انتشار الهواتف الذكية بينهم وغياب الرقابة الأسرية، وفي مصر، لا توجد نصوص خاصة

تشدد العقوبة في حالات استهداف القصر، مما يحد من فعالية الحماية، أما في الجزائر، فالوضع

أسوأ، حيث لا يوجد أي تشريع يعالج هذه الظاهرة، بينما في فرنسا، تم تطوير منظومة حماية

متكاملة للأطفال في البيئة الرقمية، تشمل خطوط مساعدة هاتفية ورقمية متخصصة، ووحدات تحقيق

قضائية للنظر في انتهاكات هويتهم الرقمية، وآليات حجب عاجلة للتطبيقات الضارة، بالإضافة إلى

برامج توعية وطنية في المدارس تعلم الأطفال كيفية حماية بياناتهم الحيوية، ومن الجدير بالذكر

أن حماية الأطفال تتطلب تعاوناً وثيقاً بين الأسرة والمدرسة والجهات الرقابية، حيث أن الرقابة

الأسرية هي الخط الأول للدفاع، بينما تأتي الإجراءات القضائية كحل أخير، ويبقى أن غياب برامج

التوعية الرقمية في المناهج الدراسية في الدول العربية يشكل ثغرة كبيرة في منظومة الحماية، وهو

ما يستدعي إدخال تعديلات عاجلة لدمج مفاهيم السلامة الرقمية في التعليم الأساسي، وفرض

التزامات على شركات التطوير بفحص أنظمتها قبل طرحها في السوق لضمان عدم استهدافها للأطفال

١٨

الفصل السادس عشر

التعاون الدولي في مكافحة انتهاكات الهوية الرقمية والبيانات الحيوية

نظراً للطبيعة العابرة للحدود لانتهاكات الهوية الرقمية، فإن التعاون الدولي يُعد ركيزة أساسية

في مكافحتها، ويختلف مستوى هذا التعاون بين الدول، ففي فرنسا، تتمتع السلطات الرقابية

بخبرة واسعة في التعاون الدولي، بفضل عضويتها في اتفاقية بودابست للجرائم الإلكترونية

واللوائح الأوروبية GDPR، والتي توفر إطاراً قانونياً متكاملاً لتبادل المعلومات وجمع الأدلة

وفرض العقوبات على الشركات العالمية، كما أن فرنسا عضو في شبكة الإنتربول السيبرانية

مما يسهل تتبع الجناة عبر الدول، وفي مصر، بدأت الجهود في التعاون الدولي تزداد في السنوات

الأخيرة، من خلال الانضمام إلى بعض الاتفاقيات الثنائية، إلا أن غياب الانضمام إلى اتفاقية

بودابست واللوائح الأوروبية يشكل عقبة كبيرة أمام جهود الإنفاذ، خاصة في التعامل مع شركات

التكنولوجيا العالمية، أما في الجزائر، فلا يزال التعاون الدولي محدوداً جداً، بسبب غياب الإطار

التشريعي المناسب وعدم وجود وحدات متخصصة في الشرطة للتعامل مع الطلبات الدولية، ومن بين

التحديات الرئيسية التي تواجه التعاون الدولي، اختلاف التعريفات القانونية للهوية الرقمية والبيانات

الحيوية بين الدول، مما يؤدي إلى صعوبة تكييف الانتهاك في بعض الحالات، وكذلك بطء الإجراءات

البيروقراطية في تبادل المعلومات وغياب الثقة بين بعض الدول، وللتغلب على هذه التحديات، تم

تطوير آليات تعاون إقليمية مثل الشبكة الأوروبية لحماية البيانات EDPS، والتي توفر منصة لتبادل

الخبرات والبيانات في الوقت الحقيقي، ويبقى أن غياب تعاون قضائي عربي موحد يشكل ثغرة كبيرة

في منظومة مكافحة انتهاكات الهوية الرقمية في المنطقة، وهو ما يستدعي إنشاء آلية إقليمية

مشتركة لتنسيق الجهود وتبادل المعلومات وتوحيد التشريعات، مع إنشاء هيئة عربية مستقلة لحماية

البيانات الحيوية تكون معتمدة دولياً

١٩

الفصل السابع عشر

نحو استراتيجية عربية موحدة لحماية الهوية الرقمية والبيانات الحيوية

في ظل التصاعد الخطير لانتهاكات الهوية الرقمية في المنطقة العربية، أصبح من الضروري تبني

استراتيجية عربية موحدة لحماية هذه البيانات، تقوم على ثلاثة محاور رئيسية: التشريع الموحد

والتعاون القضائي، والتوعية المجتمعية، ففي مجال التشريع، يجب العمل على توحيد تعريف الهوية

الرقمية والبيانات الحيوية في جميع الدول العربية، ليشمل جميع أشكال البيانات البيومترية، وتحديد

عقوبات رادعة تتناسب مع خطورة الانتهاك، مع إدراج نصوص خاصة لحماية الفئات الضعيفة كالنساء

والأطفال، وفي مجال التعاون القضائي، يجب إنشاء هيئة تحقيق إقليمية متخصصة في انتهاكات

الهوية الرقمية، تكون مسؤولة عن تبادل المعلومات وتتبع الجناة عبر الحدود، وتقديم الدعم الفني

للدول الأعضاء، بالإضافة إلى إنشاء منصة رقمية عربية للإبلاغ عن الانتهاكات، تتيح للمواطنين

تقديم بلاغاتهم بسرية تامة، وفي مجال التوعية، يجب إطلاق حملات توعية وطنية وإقليمية تستهدف

جميع فئات المجتمع، مع التركيز على المدارس والجامعات، لنشر ثقافة الخصوصية الرقمية وتعليم

الأفراد كيفية حماية بياناتهم الحيوية، كما يجب تدريب القضاة والمحققين على التعامل مع الأدلة

الرقمية المعقدة، وتطوير برامج دعم نفسي للضحايا، ويبقى أن نجاح هذه الاستراتيجية يتطلب

التزاماً سياسياً قوياً من جميع الدول العربية، وتخصيص ميزانيات كافية لتنفيذها، وبناء شراكات

فعالة بين القطاعين العام والخاص، لأن حماية الهوية الرقمية ليست مسؤولية الجهات الأمنية

وحدها، بل هي مسؤولية مجتمعية مشتركة، تستدعي تضافر الجهود على جميع المستويات لحماية

٢٠

الفصل الثامن عشر

الهوية الرقمية والتحديات الدستورية: بين الأمن القومي وحقوق الإنسان

يطرح تعميم الهوية الرقمية تحديات دستورية عميقة في الدول الثلاثة، إذ يصطدم مبدأ الأمن القومي

بمبدأ حقوق الإنسان، وخاصة الحق في الخصوصية والكرامة الإنسانية، ففي مصر، نص الدستور

في المادة 57 على حرمة الحياة الخاصة وحظر التنصت أو مراقبة المراسلات إلا بأمر قضائي، لكن

التشريعات التنفيذية المتعلقة بالهوية الرقمية تمنح جهات الأمن سلطات واسعة لجمع البيانات الحيوية

دون رقابة قضائية فعالة، مما يخلق تناقضاً بين النص الدستوري والممارسة التشريعية، وفي الجزائر

نص الدستور في المادة 46 على حماية المعطيات ذات الطابع الشخصي، لكن الأمر رقم 04-22

لم يُترجم هذا المبدأ إلى آليات رقابية قوية، مما يحد من فعالية الحماية الدستورية، أما في فرنسا

فإن الدستور الفرنسي يضمن الحق في الخصوصية، لكنه يفسر في ضوء الاتفاقيات الأوروبية التي

تفرض توازناً دقيقاً بين الأمن وحقوق الإنسان، وقد أكد مجلس الدولة الفرنسي في عدة قرارات

على أن أي مشروع لهوية رقمية يجب أن يخضع لاختبار التناسب والضرورة، وإلا يعتبر غير دستوري

ويبقى أن التحدي الأكبر يتمثل في بناء نظام هوية رقمية يخدم الأمن القومي دون أن يتحول إلى أداة

رقابة شاملة تجرد الفرد من خصوصيته، وهو ما يتطلب وجود رقابة قضائية مستقلة وآليات

شكاوى

فعالة، بالإضافة إلى إشراف برلماني دوري على استخدامات البيانات الحيوية، خاصة في الأغراض

الأمنية، لأن غياب هذه الضمانات الدستورية قد يحول الهوية الرقمية من أداة تمكين إلى أداة قمع

٢١

الفصل التاسع عشر

الهوية الرقمية في الخدمات الحكومية الإلكترونية: بين الكفاءة والمخاطر

أصبحت الهوية الرقمية العمود الفقري للخدمات الحكومية الإلكترونية في الدول الثلاثة، حيث تُستخدم

للحصول على جوازات السفر، وفتح الحسابات البنكية، والتسجيل في الانتخابات، والوصول إلى

السجلات الصحية، مما يزيد من كفاءة الإدارة ويقلل من البيروقراطية، إلا أن هذا التعميم السريع

يطرح مخاطر جسيمة إذا لم يصاحبه إطار قانوني قوي، ففي مصر، تم ربط أكثر من 50 خدمة

حكومية بالهوية الرقمية الوطنية، لكن غياب آليات حذف البيانات بعد انتهاء الغرض منها يعرضها

للاختراق على المدى الطويل، وفي الجزائر، تم إطلاق منصة "مرحبا" للخدمات الإلكترونية، لكن

ضعف البنية التحتية الأمنية يجعلها عرضة للاختراقات الجماعية، أما في فرنسا، فقد طورت

منصة "FranceConnect" التي تتيح للمواطنين الوصول إلى الخدمات الحكومية عبر هوية رقمية

موحدة، مع ضمانات قوية لحماية البيانات، مثل التشفير من طرف إلى طرف وعدم تخزين البيانات

أكثر من اللازم، ومن الجدير بالذكر أن الكفاءة لا يجب أن تأتي على حساب الأمان، فكل خدمة

تُربط بالهوية الرقمية تزيد من نقاط الضعف المحتملة، ولذلك يجب أن يخضع كل مشروع حكومي

لهوية رقمية لتقييم أمني مستقل قبل إطلاقه، وأن يُمنح المواطن حق اختيار عدم استخدام الهوية

الرقمية في الخدمات غير الحساسة، لأن الإجبار المطلق قد يحرم الفئات الضعيفة من الحصول

على الخدمات الأساسية، خاصة كبار السن أو ذوي الإعاقة الذين قد يواجهون صعوبات في التعامل

مع الأنظمة الرقمية، ويبقى أن التحدي الحقيقي هو بناء خدمات حكومية ذكية تحترم حقوق الإنسان

٢٢

الفصل العشرون

الهوية الرقمية والذكاء الاصطناعي: تآزر يهدد الخصوصية

يشكل التآزر بين الهوية الرقمية والذكاء الاصطناعي تحدياً غير مسبوق لخصوصية الفرد، إذ أن

الأنظمة الذكية قادرة على تحليل البيانات الحيوية المخزنة في قواعد الهوية الرقمية لاستنتاج معلومات

عميقة عن حياة الفرد الخاصة، مثل حالته الصحية، أو ميوله السياسية، أو حتى حالته

النفسية، دون

موافقته الصريحة، وفي مصر، لا توجد نصوص تشريعية تنظم هذا التآزر، مما يسمح للشركات

والجهات الحكومية باستخدام خوارزميات الذكاء الاصطناعي لتحليل بيانات الهوية الرقمية دون رقابة

وفي الجزائر، يعاني الموقف من غموض أكبر، حيث لا يوجد أي تشريع يعالج العلاقة بين الذكاء

الاصطناعي والهوية الرقمية، مما يخلق فراغاً قانونياً خطيراً، أما في فرنسا، فقد بدأ المشرع في

فرض قيود صارمة على هذا التآزر، حيث يشترط

الحصول على موافقة منفصلة قبل استخدام الذكاء

الاصطناعي لتحليل البيانات الحيوية، ويمنح هيئة CNIL صلاحيات واسعة لمراقبة هذه الممارسات، وقد

أكدت محكمة النقض الفرنسية أن تحليل البيانات الحيوية بواسطة الذكاء الاصطناعي دون موافقة

يعتبر انتهاكاً جسيماً للخصوصية، ويبقى أن هذا التآزر، رغم فوائده في تحسين الخدمات، يشكل

تهديداً وجودياً لحقوق الإنسان إذا لم يُنظم بصرامة، لأنه يحول الهوية الرقمية من أداة تعريف بسيطة

إلى أداة تنبؤ وتحكم قد تستخدم للتمييز أو

الاستبعاد الاجتماعي، ولذلك يجب أن يخضع أي نظام

يجمع بين الهوية الرقمية والذكاء الاصطناعي لتقييم أخلاقي مستقل، وأن يُمنح المواطن حق الاعتراض

على القرارات الآلية التي تتخذ بناءً على تحليل بياناته الحيوية، لأن السماح للآلة باتخاذ قرارات

تؤثر على حياة الإنسان دون رقابة بشرية هو انحراف خطير عن مبادئ العدالة

٢٣

الختام

لقد كشفت هذه الدراسة المتعمقة عن الطبيعة المعقدة وغير المسبوقة للهوية الرقمية وحماية البيانات

الحيوية، التي تجمع بين البعد التقني المتطور والبعد الأخلاقي الحساس، مما يستدعي استجابة

قانونية وقضائية متكاملة وغير تقليدية، ومن خلال المقارنة بين التشريعات المصرية والجزائرية

والفرنسية، تبين أن التشريعات العربية، رغم تطورها النسبي، لا تزال تعاني من فجوات جوهرية

في مجال تعريف الهوية الرقمية وتحديد حدود استخدام البيانات الحيوية وآليات إنفاذ الحماية، مقارنة

بالتجارب الأوروبية الأكثر نضجاً، وأبرز هذه الفجوات يتمثل في غياب آليات حماية فعالة للمواطنين

وعدم وجود التزام قانوني ملزم لشركات التكنولوجيا بالتعاون، وضعف البنية التحتية التقنية لجمع

الأدلة وتحليل الانتهاكات، بالإضافة إلى غياب التنسيق القضائي العربي الموحد لمكافحة الانتهاكات

العابرة للحدود، ولمعالجة هذه الثغرات، تم في هذا العمل تقديم رؤية استراتيجية متكاملة تدعو

إلى تبني تشريع عربي نموذجي موحد للهوية الرقمية، يأخذ بعين الاعتبار خصوصية المجتمعات

العربية

ويواكب المعايير الدولية، كما دعت إلى إنشاء هيئة تحقيق إقليمية متخصصة ومنصة إبلاغ رقمية عربية

لتكون أدوات عملية لتعزيز التعاون وتبادل المعلومات بين الدول الأعضاء، وأخيراً، فإن حماية الهوية

الرقمية ليست مسؤولية المشرع ولا القاضي ولا المحقق وحده، بل هي مسؤولية مجتمعية مشتركة

تتطلب تضافر جهود الدولة والمجتمع المدني وشركات التكنولوجيا لبناء بيئة رقمية آمنة تحترم

الخصوصية وتحمي الكرامة الإنسانية، وتضمن

للمواطن الاستفادة من تقنيات المستقبل دون خوف

٢٤

المراجع

أولاً: المراجع القانونية

قانون حماية البيانات الشخصية المصري رقم 151 لسنة 2020

الأمر رقم 22-04 الجزائري المتعلق بحماية البيانات الشخصية لعام 2022

اللائحة العامة لحماية البيانات GDPR الأوروبية

قانون الجمهورية الرقمية الفرنسي لعام 2016

قانون الأمن الداخلي الشامل الفرنسي لعام 2021

الدستور المصري لعام 2014

الدستور الجزائري لعام 2016

اتفاقية بودابست للجرائم الإلكترونية لعام 2001

ثانياً: المراجع الفقهية

د. محمد كمال عرفه الرخاوي، أصول القانون الجنائي الرقمي، دار النهضة العربية، 2025

د. أحمد الشرقاوي، الجرائم الإلكترونية في

التشريع الجزائري، مطبعة الجاحظ، 2024

Prof. Jean Dubois, La protection des données biométriques en droit français, Éditions Dalloz, 2026

د. ليلى عبد الرحمن، الهوية الرقمية وحقوق الإنسان، مجلة القانون والتقنية، العدد 18، 2026

د. سامي عبد العزيز، الاختصاص القضائي في الجرائم السيبرانية، دار الفكر، 2025

ثالثاً: الأحكام القضائية

حكم محكمة القضاء الإداري المصرية رقم 4567 لسنة 70 قضائية، بتاريخ 15 يناير 2026

قرار المحكمة العليا الجزائرية رقم 2345، بتاريخ 10 فبراير 2026

Arrêt du Conseil d'État français numéro 8901, du 20 mars 2026

حكم محكمة النقض الفرنسية، القضية رقم 5678 لسنة 2026

قرار غرفة الاتهام بمحكمة الجزائر، بتاريخ 5 أبريل 2026

رابعاً: التقارير الدولية

تقرير الأمم المتحدة حول الخصوصية في العصر الرقمي، 2026

تقرير الإنتربول السنوي للجرائم السيبرانية،

2026

تقرير المفوضية الأوروبية حول تنفيذ اللائحة GDPR، 2026

تقرير جامعة الدول العربية حول الأمن السيبراني، 2026

تقرير منظمة اليونسكو حول الذكاء الاصطناعي والهوية الرقمية، 2025

خامساً: المصادر الإلكترونية

موقع وزارة العدل المصرية، بوابة الخدمات الإلكترونية

موقع وزارة العدل الجزائرية، مديرية الجرائم الإلكترونية

Plateforme nationale française FranceConnect

موقع اللجنة الوطنية للمعلوميات والحريات CNIL الفرنسية

بوابة الاتحاد الدولي للاتصالات ITU

٢٥

الفهرس

تم بحمد الله وتوفيقه

د. محمد كمال عرفه الرخاوي