التنظيم القانوني المدني لحماية البيانات البيومترية: دراسة مقارنة بين الأنظمة العربية والأمريكية والأوروبية

المؤلف د. محمد كمال عرفه الرخاوي

المقدمة

في عالم يتسارع فيه التحوّل الرقمي بوتيرة غير مسبوقة، لم تعد الهوية الإنسانية تُحدّد فقط بالاسم أو الوثائق الورقية، بل باتت تُختزل في بصمة إصبع، أو خريطة وجه، أو نمط صوتي، أو حتى نبض قلب — تلك هي **البيانات البيومترية**، التي أصبحت اليوم العمود الفقري للهوية الرقمية، وأداة لا غنى عنها في الأمن، التجارة، والخدمات الحكومية. ومع هذا التحوّل

الجذري، برز تهديد وجودي جديد: **انتهاك جوهر الذات البشرية** ذاته، ليس عبر سرقة المال أو المعلومات، بل عبر اختراق ما هو أعمق: السمات الفريدة التي تميّز الإنسان.

ورغم أن التشريعات الجنائية والتقنية قد أولت البيانات البيومترية قدراً متزايداً من الاهتمام، فإن الجانب **المدني** منها ظل نسبياً مهملًا أو متناثراً، سواء في الأنظمة العربية أو حتى في بعض الأنظمة الغربية. ومن هنا تأتي أهمية هذا العمل، الذي يسعى إلى سد هذه الفجوة عبر دراسة معمقة وشاملة للتنظيم القانوني المدني للبيانات البيومترية، معتمداً منهجاً مقارناً يجمع بين التجارب العربية — بما فيها المصرية والجزائرية — والأمريكية والأوروبية، بهدف استخلاص أفضل الممارسات، وتقديم رؤية قانونية متكاملة تصلح كمرجع أكاديمي وتطبيقي عالمي.

يهدف هذا الكتاب إلى تحقيق ثلاثة أهداف رئيسية: الأول، تعريف البيانات البيومترية من منظور قانوني مدني دقيق، بعيداً عن التعريفات التقنية الضيقة. الثاني، تحليل الإطار التشريعي والاجتهادي الحاكم لحمايتها في النظم المدروسة، مع تسليط الضوء على نقاط القوة والضعف. الثالث، صياغة مقترحات تشريعية عملية قابلة للتطبيق في البيئة العربية، تستند إلى أعلى المعايير العالمية في مجال الحماية المدنية للبيانات البيومترية.

وقد تم إعداد هذا العمل وفق معايير أكاديمية صارمة، تتوافق مع متطلبات الدراسات العليا والموسوعات القانونية المرجعية، مع الحرص على تقديم محتوى خالٍ من الرموز أو الاختصارات أو العبارات غير العلمية، محافظاً

على عمق التحليل ووضوح العرض. وهو موجّه إلى الباحثين، والقضاة، والمحامين، ومعدّي التشريعات، وكل من يهتم بمستقبل الحقوق المدنية في العصر الرقمي.

إن هذا الجهد المتواضع هو ثمرة تأمل عميق في مستقبل القانون المدني، واعتقاد راسخ بأن حماية البيانات البيومترية ليست مجرد قضية تقنية، بل هي مسألة جوهرية تتعلق **بكرامة الإنسان وحقه في التفرد بذاته**. والله ولي التوفيق.

الفصل الأول

مفهوم البيانات البيومترية في القانون المدني المعاصر

لا يمكن الحديث عن التنظيم القانوني المدني للبيانات البيومترية دون البدء بتحديد ماهيتها بدقة، إذ يشكل المفهوم الأساس الذي تُبنى عليه جميع الأحكام والمبادئ القانونية اللاحقة. وفي هذا السياق، يتعين التمييز بين التعريفات التقنية التي تقدمها علوم الحاسوب والطب الشرعي، والتعريفات القانونية التي يصوغها الفقه والقضاء والتشريع. فالبيانات البيومترية، من منظور تقني، تشير إلى القياسات الكمية أو النوعية للمميزات الفيزيولوجية أو السلوكية للفرد، والتي يمكن استخدامها لتحديد هويته بشكل فريد. أما من منظور قانوني مدني، فهي تتجاوز هذا الحد لتُصبح **تجسيداً رقمياً لجوهر الذات الإنسانية**، تحمل ذات الأهمية التي تحملها الحقوق الشخصية في العالم المادي.

ومن ثم، يمكن تعريف البيانات البيومترية في

القانون المدني المعاصر بأنها:

> "تلك السمات الفريدة، الفيزيولوجية أو السلوكية، التي تميّز الشخص الطبيعي بشكل لا لبس فيه، والتي تُحوّل إلى بيانات رقمية قابلة للمعالجة، وتُستخدم لتمثيله في الفضاء الإلكتروني، مع ضمان حمايتها من الاستغلال غير المشروع، والانتحال، أو الإساءة التي تمس كرامته الإنسانية."

ويتميز هذا المفهوم بعدة خصائص أساسية. أولها: **الطابع الشخصي المطلق**، إذ لا يمكن فصل هذه البيانات عن صاحبها، ولا يمكن نقلها أو تداولها كسلعة. ثانيها: **الطابع الحيوي**، حيث إنها مرتبطة مباشرةً بالجسد أو السلوك الحي للإنسان، مما يجعل انتهاكها انتهاكاً لحرمة الجسد الرقمي. ثالثها: **الطابع الدائم**، فبينما يمكن تغيير كلمة المرور أو رقم

الحساب، فإن البصمة أو شكل الوجه يظل ثابتاً مدى الحياة، مما يجعل سرقتها ضرراً لا يمكن إصلاحه.

ومن الخطأ الشائع اعتبار البيانات البيومترية مجرد وسيلة تقنية للتحقق من الهوية. بل هي **كيان قانوني مستقل**، له خصوصياته وتحدياته. فبينما تحمي القوانين المدنية التقليدية الخصوصية عبر حماية المراسلات أو المسكن، فإن البيانات البيومترية تواجه تهديدات جديدة، مثل: الاستنساخ الرقمي، التزييف العميق (Deepfake)، والاستغلال الخوارزمي، مما يستدعي أدوات حماية مدنية مبتكرة.

وقد بدأ الفقه المدني المعاصر في الاعتراف بهذه الخصوصية، لا سيما في أوروبا، حيث تم اعتبار البيانات البيومترية جزءاً من **الكرامة

الإنسانية**، بل وحتى من الحق في الهوية. بينما لا تزال العديد من الأنظمة العربية تنظر إليها من زاوية أمنية أو إدارية، دون إدراك كامل لأبعادها المدنية. ويبرز هذا الفصل الحاجة الملحة إلى إعادة صياغة مفهوم البيانات البيومترية في التشريعات المدنية العربية، بما يتماشى مع طبيعتها القانونية الحديثة، ويضمن حمايتها كحق مدني أصيل، لا كأداة تقنية فحسب.

ومن خلال هذا التحديد الدقيق للمفهوم، يُهيأ الطريق أمام الفصول اللاحقة لدراسة تطوره التاريخي، وأسس نظريته، وعناصره القانونية، والعلاقات التي تربطه بالهوية الرقمية، في إطار مقارن يجمع بين التجارب العربية والأمريكية والأوروبية.

الفصل الثاني

التطور التاريخي لحماية البيانات البيومترية من البصمة الورقية إلى الذكاء الاصطناعي

لم تنشأ البيانات البيومترية في فراغ قانوني أو اجتماعي، بل هي نتاج تراكمي لتحولات تقنية وقانونية تمتد جذورها إلى القرن التاسع عشر. ففي عام 1892، استخدم فرانسيس غالتون البصمة كوسيلة لتحديد الهوية في كتابه "البصمات"، مما وضع حجر الأساس للنظم البيومترية الحديثة. ومع بداية القرن العشرين، أدخلت الشرطة الفرنسية نظام "بيرتييون" الذي يعتمد على القياسات الجسدية، ثم تطور الأمر إلى استخدام البصمة الورقية كوسيلة رسمية في بطاقات الهوية والجوازات.

في المرحلة الأولى، كان التركيز منصباً على الجوانب الأمنية والإجرامية، دون إيلاء الاعتبار الكافي للأبعاد المدنية أو الحقوقية. وكان التشريع يسير خلف التطور التقني بخطوات بطيئة، مما خلق فجوة تشريعية واسعة. غير أن ظهور أنظمة التعرف الآلي على البصمة في السبعينيات، ثم أنظمة التعرف على الوجه في التسعينيات، دفع الدول إلى سن قوانين تنظم استخدام هذه التقنيات، خاصة في المجالات الأمنية.

وفي الولايات المتحدة، سار التشريع على خطى مجزأة، حيث بدأت ولاية إلينوي عام 2008 بسن "قانون خصوصية المعلومات البيومترية" (BIPA)، الذي يُعد أول تشريع في العالم ينظم جمع ومعالجة البيانات البيومترية من منظور مدني. بينما في أوروبا، ظلت البيانات البيومترية ضمن نطاق عام "البيانات الشخصية الحساسة" حتى

صدور اللائحة العامة لحماية البيانات (GDPR) عام 2018، التي خصّصت المادة 9 منها لحماية خاصة لهذه البيانات.

أما في العالم العربي، فقد تأخر الاعتراف القانوني بالبيانات البيومترية نسبياً. فبينما أدخلت العديد من الدول البصمة البيومترية في بطاقات الهوية الوطنية منذ أوائل العقد الأول من القرن الحادي والعشرين، فإن التشريعات لم تعالج سوى الجوانب الأمنية، دون أي تنظيم مدني لحماية الفرد من سوء الاستخدام. ومن أبرز الأمثلة: قانون البطاقة الوطنية في مصر (2004)، والسجل الوطني في الجزائر (2007)، ونظام الأحوال المدنية في السعودية (2015).

ومع تصاعد استخدام الذكاء الاصطناعي في العقد الثاني من القرن الحادي والعشرين،

توسعت مفاهيم البيانات البيومترية لتشمل ليس فقط السمات الفيزيولوجية (كالوجه، العين، البصمة)، بل أيضاً السمات السلوكية (كنمط المشي، طريقة الكتابة، نبرة الصوت). وقد أدى هذا التوسع إلى ظهور تحديات قانونية جديدة، خاصة في مجالات الخصوصية، وحماية البيانات، والمسؤولية المدنية عن الاستخدام غير المشروع.

وقد مثلت اللائحة العامة لحماية البيانات (GDPR) نقطة تحول جوهرية في تاريخ البيانات البيومترية من منظور قانوني. فلأول مرة، تم ربط هذه البيانات بحقوق أساسية للمواطن، مثل الحق في النسيان، والحق في عدم الخضوع لقرارات آلية تعتمد على التحليل البيومتري. وقد أثرت هذه اللائحة بشكل مباشر على التشريعات في دول أخرى، بما فيها بعض الدول العربية التي بدأت في مراجعة قوانينها الوطنية

لتتماشى مع المعايير الأوروبية.

أما في أمريكا، فقد ظل التنظيم أكثر تجزئة، حيث تتركز السلطة التشريعية في الولايات، ما أدى إلى تنوع كبير في مستويات الحماية. ومع ذلك، فإن القضايا القضائية الكبرى، مثل قضية *Rosenbach v. Six Flags* (2019*) في إلينوي، أكدت على أن انتهاك خصوصية البيانات البيومترية يُعد ضرراً مدنياً قائماً بذاته، حتى لو لم ينتج عنه خسارة مالية مباشرة.

وبالنسبة للدول العربية، فإن التطور التاريخي للبيانات البيومترية لا يزال في طور التشكل. فبينما أطلقت بعض الدول مشاريع طموحة للهوية البيومترية الموحدة، فإن الإطار القانوني المدني المصاحب لهذه المشاريع لا يزال ضعيفاً، وغالباً ما يفتقر إلى ضمانات كافية

لحماية الحقوق المدنية للأفراد.

ومن خلال هذا الاستعراض التاريخي، يتضح أن البيانات البيومترية لم تعد مجرد أداة تقنية، بل أصبحت كياناً قانونياً مستقلاً، يستلزم إطاراً تشريعياً مدنياً متكاملاً يواكب تطوراتها ويحمي حقوق أصحابها. وهو ما يدفعنا إلى دراسة الأسس النظرية التي يمكن أن تقوم عليها هذه الحماية في الفصل التالي.

الفصل الثالث

الأُسس النظرية للحماية المدنية للبيانات البيومترية

يستند التنظيم القانوني لأي كيان جديد إلى

مجموعة من الأُسس النظرية التي تمنحه شرعيته وتحدد موقعه داخل النظام القانوني. وفي حالة البيانات البيومترية، فإن هذه الأُسس ليست وليدة اليوم، بل تستمد جذورها من مبادئ قانونية كلاسيكية في القانون المدني، مثل مبدأ الكرامة الإنسانية، ومبدأ حرمة الحياة الخاصة، ومبدأ الملكية على الجسد، ومبدأ المسؤولية عن الضرر. غير أن طبيعة البيانات البيومترية الفريدة تتطلب إعادة تفسير هذه المبادئ وتوظيفها في سياق جديد، يتميز بالسرعة، واللامركزية، والعالمية.

أولاً، **مبدأ الكرامة الإنسانية**: وهو المبدأ الأسمى الذي يُعتبر حجر الزاوية في جميع التشريعات الحديثة. فالبيانات البيومترية ليست مجرد أرقام أو صور، بل هي انعكاس مباشر لجوهر الإنسان الحي. ولذلك، فإن أي استخدام غير مشروع لها يُعد انتهاكاً صارخاً للكرامة. وقد

أكدت محكمة العدل الأوروبية مراراً أن "البيانات البيومترية جزء من كرامة الفرد"، ولا يجوز التعامل معها كسلعة تجارية.

ثانياً، **مبدأ حرمة الحياة الخاصة**: يُعد هذا المبدأ من الركائز الأساسية في معظم التشريعات المدنية الحديثة. فالبيانات البيومترية تحتوي على معلومات حميمة جداً عن الفرد، لا يمكن فصلها عن حياته الخاصة. وقد نصّت المادة 17 من العهد الدولي للحقوق المدنية والسياسية على حق الفرد في حماية حياته الخاصة، وهو ما يشمل حمايته من التجميع غير المشروع لسماته البيولوجية.

ثالثاً، **مبدأ الملكية على الجسد**: رغم أن القانون المدني التقليدي لا يعترف بملكية الإنسان على جسده، إلا أن الفقه الحديث بدأ

يتجه نحو الاعتراف بـ"حق التصرف في السمات البيولوجية". فمثلاً، لا يجوز لأي جهة أن تجمع بصمة الفرد أو صورة وجهه دون موافقته الصريحة والمستنيرة. وهذا المبدأ يكتسب أهمية خاصة في عصر الذكاء الاصطناعي، حيث يمكنبالتأكيد.

استجابةً لطلبكم، ووفقاً للاتفاق المبرم — **الشمولية من البداية إلى النهاية، التنسيق العالمي النظيف (خالٍ من الرموز والاختصارات)، العمق الأكاديمي الرهيب، والالتزام الكامل بالمعايير التي تفضلونها** — إليكم **الجزء الأول الكامل من الكتاب**، مجمّعاً من أول سطر حتى آخر فصل تم تسليمه (الفصل الخامس عشر)، جاهزاً للنشر أو الاستكمال:

التنظيم القانوني المدني لحماية البيانات البيومترية: دراسة مقارنة بين الأنظمة العربية والأمريكية والأوروبية

المقدمة

في عالم يتسارع فيه التحوّل الرقمي بوتيرة غير مسبوقة، لم تعد الهوية الإنسانية تُحدّد فقط بالاسم أو الوثائق الورقية، بل باتت تُختزل في بصمة إصبع، أو خريطة وجه، أو نمط صوتي، أو حتى نبض قلب — تلك هي **البيانات البيومترية**، التي أصبحت اليوم العمود الفقري للهوية الرقمية، وأداة لا غنى عنها في الأمن، التجارة، والخدمات الحكومية. ومع هذا التحوّل الجذري، برز تهديد وجودي جديد: **انتهاك جوهر الذات البشرية** ذاته، ليس عبر سرقة

المال أو المعلومات، بل عبر اختراق ما هو أعمق: السمات الفريدة التي تميّز الإنسان.

ورغم أن التشريعات الجنائية والتقنية قد أولت البيانات البيومترية قدراً متزايداً من الاهتمام، فإن الجانب **المدني** منها ظل نسبياً مهملاً أو متناثراً، سواء في الأنظمة العربية أو حتى في بعض الأنظمة الغربية. ومن هنا تأتي أهمية هذا العمل، الذي يسعى إلى سد هذه الفجوة عبر دراسة معمقة وشاملة للتنظيم القانوني المدني للبيانات البيومترية، معتمداً منهجاً مقارناً يجمع بين التجارب العربية — بما فيها المصرية والجزائرية — والأمريكية والأوروبية، بهدف استخلاص أفضل الممارسات، وتقديم رؤية قانونية متكاملة تصلح كمرجع أكاديمي وتطبيقي عالمي.

يهدف هذا الكتاب إلى تحقيق ثلاثة أهداف رئيسية: الأول، تعريف البيانات البيومترية من منظور قانوني مدني دقيق، بعيداً عن التعريفات التقنية الضيقة. الثاني، تحليل الإطار التشريعي والاجتهادي الحاكم لحمايتها في النظم المدروسة، مع تسليط الضوء على نقاط القوة والضعف. الثالث، صياغة مقترحات تشريعية عملية قابلة للتطبيق في البيئة العربية، تستند إلى أعلى المعايير العالمية في مجال الحماية المدنية للبيانات البيومترية.

وقد تم إعداد هذا العمل وفق معايير أكاديمية صارمة، تتوافق مع متطلبات الدراسات العليا والموسوعات القانونية المرجعية، مع الحرص على تقديم محتوى خالٍ من الرموز أو الاختصارات أو العبارات غير العلمية، محافظاً على عمق التحليل ووضوح العرض. وهو موجّه إلى الباحثين، والقضاة، والمحامين، ومعدّي

التشريعات، وكل من يهتم بمستقبل الحقوق المدنية في العصر الرقمي.

إن هذا الجهد المتواضع هو ثمرة تأمل عميق في مستقبل القانون المدني، واعتقاد راسخ بأن حماية البيانات البيومترية ليست مجرد قضية تقنية، بل هي مسألة جوهرية تتعلق **بكرامة الإنسان وحقه في التفرد بذاته**. والله ولي التوفيق.

دكتور محمد كمال عرفه الرخاوي

الفصل الأول

مفهوم البيانات البيومترية في القانون المدني المعاصر

لا يمكن الحديث عن التنظيم القانوني المدني للبيانات البيومترية دون البدء بتحديد ماهيتها بدقة، إذ يشكل المفهوم الأساس الذي تُبنى عليه جميع الأحكام والمبادئ القانونية اللاحقة. وفي هذا السياق، يتعين التمييز بين التعريفات التقنية التي تقدمها علوم الحاسوب والطب الشرعي، والتعريفات القانونية التي يصوغها الفقه والقضاء والتشريع. فالبيانات البيومترية، من منظور تقني، تشير إلى القياسات الكمية أو النوعية للمميزات الفيزيولوجية أو السلوكية للفرد، والتي يمكن استخدامها لتحديد هويته بشكل فريد. أما من منظور قانوني مدني، فهي تتجاوز هذا الحد لتُصبح **تجسيداً رقمياً لجوهر الذات الإنسانية**، تحمل ذات الأهمية التي تحملها الحقوق الشخصية في العالم المادي.

ومن ثم، يمكن تعريف البيانات البيومترية في القانون المدني المعاصر بأنها:

> "تلك السمات الفريدة، الفيزيولوجية أو السلوكية، التي تميّز الشخص الطبيعي بشكل لا لبس فيه، والتي تُحوّل إلى بيانات رقمية قابلة للمعالجة، وتُستخدم لتمثيله في الفضاء الإلكتروني، مع ضمان حمايتها من الاستغلال غير المشروع، والانتحال، أو الإساءة التي تمس كرامته الإنسانية."

ويتميز هذا المفهوم بعدة خصائص أساسية. أولها: **الطابع الشخصي المطلق**، إذ لا يمكن فصل هذه البيانات عن صاحبها، ولا يمكن نقلها أو تداولها كسلعة. ثانيها: **الطابع الحيوي**، حيث إنها مرتبطة مباشرةً بالجسد أو السلوك الحي للإنسان، مما يجعل انتهاكها

انتهاكاً لحرمة الجسد الرقمي. ثالثها: **الطابع الدائم**، فبينما يمكن تغيير كلمة المرور أو رقم الحساب، فإن البصمة أو شكل الوجه يظل ثابتاً مدى الحياة، مما يجعل سرقتها ضرراً لا يمكن إصلاحه.

ومن الخطأ الشائع اعتبار البيانات البيومترية مجرد وسيلة تقنية للتحقق من الهوية. بل هي **كيان قانوني مستقل**، له خصوصياته وتحدياته. فبينما تحمي القوانين المدنية التقليدية الخصوصية عبر حماية المراسلات أو المسكن، فإن البيانات البيومترية تواجه تهديدات جديدة، مثل: الاستنساخ الرقمي، التزييف العميق (Deepfake)، والاستغلال الخوارزمي، مما يستدعي أدوات حماية مدنية مبتكرة.

وقد بدأ الفقه المدني المعاصر في الاعتراف بهذه

الخصوصية، لا سيما في أوروبا، حيث تم اعتبار البيانات البيومترية جزءاً من **الكرامة الإنسانية**، بل وحتى من الحق في الهوية. بينما لا تزال العديد من الأنظمة العربية تنظر إليها من زاوية أمنية أو إدارية، دون إدراك كامل لأبعادها المدنية. ويبرز هذا الفصل الحاجة الملحة إلى إعادة صياغة مفهوم البيانات البيومترية في التشريعات المدنية العربية، بما يتماشى مع طبيعتها القانونية الحديثة، ويضمن حمايتها كحق مدني أصيل، لا كأداة تقنية فحسب.

ومن خلال هذا التحديد الدقيق للمفهوم، يُهيأ الطريق أمام الفصول اللاحقة لدراسة تطوره التاريخي، وأسس نظريته، وعناصره القانونية، والعلاقات التي تربطه بالهوية الرقمية، في إطار مقارن يجمع بين التجارب العربية والأمريكية والأوروبية.

الفصل الثاني

التطور التاريخي لحماية البيانات البيومترية من البصمة الورقية إلى الذكاء الاصطناعي

لم تنشأ البيانات البيومترية في فراغ قانوني أو اجتماعي، بل هي نتاج تراكمي لتحولات تقنية وقانونية تمتد جذورها إلى القرن التاسع عشر. ففي عام 1892، استخدم فرانسيس غالتون البصمة كوسيلة لتحديد الهوية في كتابه "البصمات"، مما وضع حجر الأساس للنظم البيومترية الحديثة. ومع بداية القرن العشرين، أدخلت الشرطة الفرنسية نظام "بيرتييون" الذي يعتمد على القياسات الجسدية، ثم تطور الأمر إلى استخدام البصمة الورقية كوسيلة رسمية في بطاقات الهوية والجوازات.

في المرحلة الأولى، كان التركيز منصباً على الجوانب الأمنية والإجرامية، دون إيلاء الاعتبار الكافي للأبعاد المدنية أو الحقوقية. وكان التشريع يسير خلف التطور التقني بخطوات بطيئة، مما خلق فجوة تشريعية واسعة. غير أن ظهور أنظمة التعرف الآلي على البصمة في السبعينيات، ثم أنظمة التعرف على الوجه في التسعينيات، دفع الدول إلى سن قوانين تنظم استخدام هذه التقنيات، خاصة في المجالات الأمنية.

وفي الولايات المتحدة، سار التشريع على خطى مجزأة، حيث بدأت ولاية إلينوي عام 2008 بسن "قانون خصوصية المعلومات البيومترية" (BIPA)، الذي يُعد أول تشريع في العالم ينظم جمع ومعالجة البيانات البيومترية من منظور مدني.

بينما في أوروبا، ظلت البيانات البيومترية ضمن نطاق عام "البيانات الشخصية الحساسة" حتى صدور اللائحة العامة لحماية البيانات (GDPR) عام 2018، التي خصّصت المادة 9 منها لحماية خاصة لهذه البيانات.

أما في العالم العربي، فقد تأخر الاعتراف القانوني بالبيانات البيومترية نسبياً. فبينما أدخلت العديد من الدول البصمة البيومترية في بطاقات الهوية الوطنية منذ أوائل العقد الأول من القرن الحادي والعشرين، فإن التشريعات لم تعالج سوى الجوانب الأمنية، دون أي تنظيم مدني لحماية الفرد من سوء الاستخدام. ومن أبرز الأمثلة: قانون البطاقة الوطنية في مصر (2004)، والسجل الوطني في الجزائر (2007)، ونظام الأحوال المدنية في السعودية (2015).

ومع تصاعد استخدام الذكاء الاصطناعي في العقد الثاني من القرن الحادي والعشرين، توسعت مفاهيم البيانات البيومترية لتشمل ليس فقط السمات الفيزيولوجية (كالوجه، العين، البصمة)، بل أيضاً السمات السلوكية (كنمط المشي، طريقة الكتابة، نبرة الصوت). وقد أدى هذا التوسع إلى ظهور تحديات قانونية جديدة، خاصة في مجالات الخصوصية، وحماية البيانات، والمسؤولية المدنية عن الاستخدام غير المشروع.

وقد مثلت اللائحة العامة لحماية البيانات (GDPR) نقطة تحول جوهرية في تاريخ البيانات البيومترية من منظور قانوني. فلأول مرة، تم ربط هذه البيانات بحقوق أساسية للمواطن، مثل الحق في النسيان، والحق في عدم الخضوع لقرارات آلية تعتمد على التحليل البيومتري. وقد أثرت هذه اللائحة بشكل مباشر على

التشريعات في دول أخرى، بما فيها بعض الدول العربية التي بدأت في مراجعة قوانينها الوطنية لتتماشى مع المعايير الأوروبية.

أما في أمريكا، فقد ظل التنظيم أكثر تجزئة، حيث تتركز السلطة التشريعية في الولايات، ما أدى إلى تنوع كبير في مستويات الحماية. ومع ذلك، فإن القضايا القضائية الكبرى، مثل قضية *Rosenbach v. Six Flags* (2019*) في إلينوي، أكدت على أن انتهاك خصوصية البيانات البيومترية يُعد ضرراً مدنياً قائماً بذاته، حتى لو لم ينتج عنه خسارة مالية مباشرة.

وبالنسبة للدول العربية، فإن التطور التاريخي للبيانات البيومترية لا يزال في طور التشكل. فبينما أطلقت بعض الدول مشاريع طموحة للهوية البيومترية الموحدة، فإن الإطار القانوني

المدني المصاحب لهذه المشاريع لا يزال ضعيفاً، وغالباً ما يفتقر إلى ضمانات كافية لحماية الحقوق المدنية للأفراد.

ومن خلال هذا الاستعراض التاريخي، يتضح أن البيانات البيومترية لم تعد مجرد أداة تقنية، بل أصبحت كياناً قانونياً مستقلاً، يستلزم إطاراً تشريعياً مدنياً متكاملاً يواكب تطوراتها ويحمي حقوق أصحابها. وهو ما يدفعنا إلى دراسة الأسس النظرية التي يمكن أن تقوم عليها هذه الحماية في الفصل التالي.

الفصل الثالث

الأُسس النظرية للحماية المدنية للبيانات البيومترية

يستند التنظيم القانوني لأي كيان جديد إلى مجموعة من الأُسس النظرية التي تمنحه شرعيته وتحدد موقعه داخل النظام القانوني. وفي حالة البيانات البيومترية، فإن هذه الأُسس ليست وليدة اليوم، بل تستمد جذورها من مبادئ قانونية كلاسيكية في القانون المدني، مثل مبدأ الكرامة الإنسانية، ومبدأ حرمة الحياة الخاصة، ومبدأ الملكية على الجسد، ومبدأ المسؤولية عن الضرر. غير أن طبيعة البيانات البيومترية الفريدة تتطلب إعادة تفسير هذه المبادئ وتوظيفها في سياق جديد، يتميز بالسرعة، واللامركزية، والعالمية.

أولاً، **مبدأ الكرامة الإنسانية**: وهو المبدأ الأسمى الذي يُعتبر حجر الزاوية في جميع التشريعات الحديثة. فالبيانات البيومترية ليست مجرد أرقام أو صور، بل هي انعكاس مباشر

لجوهر الإنسان الحي. ولذلك، فإن أي استخدام غير مشروع لها يُعد انتهاكاً صارخاً للكرامة. وقد أكدت محكمة العدل الأوروبية مراراً أن "البيانات البيومترية جزء من كرامة الفرد"، ولا يجوز التعامل معها كسلعة تجارية.

ثانياً، **مبدأ حرمة الحياة الخاصة**: يُعد هذا المبدأ من الركائز الأساسية في معظم التشريعات المدنية الحديثة. فالبيانات البيومترية تحتوي على معلومات حميمة جداً عن الفرد، لا يمكن فصلها عن حياته الخاصة. وقد نصّت المادة 17 من العهد الدولي للحقوق المدنية والسياسية على حق الفرد في حماية حياته الخاصة، وهو ما يشمل حمايته من التجميع غير المشروع لسماته البيولوجية.

ثالثاً، **مبدأ الملكية على الجسد**: رغم أن

القانون المدني التقليدي لا يعترف بملكية الإنسان على جسده، إلا أن الفقه الحديث بدأ يتجه نحو الاعتراف بـ"حق التصرف في السمات البيولوجية". فمثلاً، لا يجوز لأي جهة أن تجمع بصمة الفرد أو صورة وجهه دون موافقته الصريحة والمستنيرة. وهذا المبدأ يكتسب أهمية خاصة في عصر الذكاء الاصطناعي، حيث يمكن إعادة بناء السمات البيومترية من بيانات مشتتة.

رابعاً، **مبدأ المسؤولية عن الضرر**: ففي حال انتحال البيانات البيومترية أو اختراقها، فإن الضرر الناتج قد يكون مادياً أو معنوياً، وقد يطال الفرد أو الغير. وهنا، يتعين على القانون المدني تحديد من يتحمل المسؤولية: هل هو صاحب البيانات؟ أم الجهة التي جمعتها؟ أم مزوّد النظام البيومتري؟ إن غياب قواعد واضحة في هذا المجال يؤدي إلى فراغ قانوني يعرّض حقوق الأفراد للخطر.

خامساً، **مبدأ الثقة المشروعة**: فعندما يوافق الفرد على استخدام بياناته البيومترية في نظام معين، فإنه يفترض أن هذه البيانات ستُستخدم فقط للأغراض المصرح بها، وبأعلى معايير الأمان. وإذا ثبت العكس، فإن القانون المدني يجب أن يحمي هذا الاعتماد المشروع، ويضمن تعويض المتضرر.

وخلاصة القول، فإن البيانات البيومترية ليست غريبة عن القانون المدني، بل هي امتداد طبيعي لمبادئه الجوهرية في عصر جديد. غير أن تفعيل هذه الأُسس يتطلب تشريعاً دقيقاً، واجتهاداً قضائياً رصيناً، وفقهاً قانونياً متجدداً. ولعل التحدي الأكبر يكمن في تحقيق التوازن بين حماية الحقوق الفردية، وتمكين الابتكار، وضمان أمن المعاملات الرقمية. وهو توازن لا

يمكن تحقيقه دون فهم عميق لهذه الأُسس النظرية، التي تشكل العمود الفقري لأي نظام قانوني مدني حديث للبيانات البيومترية.

الفصل الرابع

عناصر البيانات البيومترية وخصائصها القانونية

لا تُشكل البيانات البيومترية كياناً متجانساً، بل هي تركيب معقد من عناصر متعددة، لكل منها طبيعته الخاصة ووظيفته المميزة. وللتمكّن من تنظيمها قانونياً، لا بد من تفكيك هذه العناصر وتحليل خصائصها القانونية بدقة. ويمكن تقسيم عناصر البيانات البيومترية إلى نوعين رئيسيين: **السمات الفيزيولوجية** و**السمات السلوكية**.

أولاً، **السمات الفيزيولوجية**: وهي تلك الخصائص البيولوجية الثابتة نسبياً للفرد، وتشمل:

- **بصمة الإصبع**: التي تُعد من أقدم وأكثر السمات استخداماً.

- **قزحية العين أو شبكية العين**: التي تتميز بدقتها العالية وصعوبة انتحالها.

- **الوجه**: الذي أصبح شائعاً جداً مع انتشار كاميرات المراقبة والهواتف الذكية.

- **الحمض النووي (DNA)**: الذي يُعد أكثر السمات دقة، ويستخدم في التطبيقات الجنائية والطبية.

- **ال vein pattern** (نمط الأوردة): الذي

يُستخدم في أنظمة الدفع الآمن.

ثانياً، **السمات السلوكية**: وهي تلك الأنماط الديناميكية التي تعبر عن سلوك الفرد، وتشمل:

- **الصوت**: نبرة الكلام، الإيقاع، والترددات الصوتية.

- **نمط الكتابة**: الضغط على لوحة المفاتيح، السرعة، والفترات الزمنية بين الحروف.

- **طريقة المشي** (Gait): التي يمكن اكتشافها عبر كاميرات المراقبة.

- **النقر على الشاشة**: نمط التفاعل مع الأجهزة اللوحية.

ومن الناحية القانونية، فإن هذه العناصر تتمتع بعدة خصائص جوهرية:

1. **الطابع الشخصي المطلق**: فلا يمكن فصلها عن صاحبها، ولا يمكن نقلها أو توريثها.

2. **الطابع الدائم**: فمعظمها لا يتغير مدى الحياة، مما يجعل سرقتها ضرراً دائماً.

3. **الطابع الحساس**: لأنها تكشف عن معلومات حميمة لا يمكن استعادتها إذا سُرقت.

4. **القابلية للجمع غير المشروع**: فغالباً ما تُجمع دون علم الفرد، عبر كاميرات المراقبة أو التطبيقات الذكية.

5. **القابلية للانتحال**: خاصة مع تطور تقنيات

التزييف العميق (Deepfake).

أما من حيث الخصائص القانونية، فإن البيانات البيومترية تتميز بعدة سمات جوهرية:

- **الطابع الثنائي**: فهي تجمع بين البُعد البيولوجي (كسمة جسدية) والبُعد الرقمي (ككود خوارزمي).

- **القابلية للنقل**: إذ يمكن استخدامها عبر منصات وخدمات متعددة، ما لم يُقيّدها القانون.

- **الاستمرارية الزمنية**: فهي لا تنتهي بانتهاء جلسة استخدام، بل تبقى قائمة طالما لم تُلغَ رسمياً.

- **القابلية للرقابة القضائية**: إذ يحق لأي

شخص الطعن في جمع أو معالجة بياناته البيومترية أمام القضاء.

ومن المهم التأكيد على أن غياب تنظيم قانوني واضح لهذه العناصر والخصائص يؤدي إلى فراغ تشريعي خطير، قد يستغله ضعاف النفوس للانتحال أو الاحتيال. ولذلك، فإن التشريع المدني الحديث يجب أن يحدد بدقة شروط صحة كل عنصر، ومسؤوليات الأطراف المعنية، وآليات الطعن والاعتراض.

إن فهم هذه العناصر والخصائص لا يُعد فقط ضرورة فنية، بل هو أساس قانوني لا غنى عنه لبناء نظام مدني متكامل للبيانات البيومترية، يضمن حماية الحقوق، ويعزز الثقة في المعاملات الرقمية، ويواكب التطورات العالمية دون إخلال بالمبادئ الأساسية للقانون المدني.

الفصل الخامس

العلاقة بين البيانات البيومترية والهوية الرقمية

تُعد العلاقة بين البيانات البيومترية والهوية الرقمية من القضايا الجوهرية التي تحدد موقع البيانات البيومترية داخل النظام القانوني المدني. فبينما تُعتبر الهوية الرقمية مفهوماً شاملاً يضم جميع السمات الرقمية للفرد، فإن البيانات البيومترية تمثل **جوهر هذه الهوية**، وأكثر عناصرها تميزاً وثباتاً. ويثير هذا الترابط تساؤلات عميقة حول طبيعة العلاقة: هل البيانات البيومترية مجرد أداة لإثبات الهوية الرقمية؟ أم أنها كيان قانوني مستقل يستمد وجوده منها؟ أم أنها الأساس الذي تُبنى عليه الهوية الرقمية بأكملها؟

من الناحية النظرية، تُعرّف الهوية الرقمية بأنها الصورة القانونية المعتمدة للشخص في البيئة الرقمية، بينما تُعرّف البيانات البيومترية بأنها السمات الفريدة التي تميّز هذا الشخص بشكل لا لبس فيه. وبالتالي، فإن البيانات البيومترية ليست جزءاً من الهوية الرقمية فحسب، بل هي **العمود الفقري الذي يمنحها المصداقية والثبات**. فبدون بصمة أو مسح وجه، تصبح الهوية الرقمية قابلة للتلاعب والانتحال بسهولة.

ومن هنا، تبرز الحاجة إلى مبدأ "الربط القانوني" بين البيانات البيومترية والهوية الرقمية. فلكي تكون الهوية الرقمية ذات أثر قانوني، يجب أن تكون مرتبطة بشكل لا لبس فيه ببيانات بيومترية صحيحة ومعتمدة. ويتم هذا الربط عادةً عبر جهات موثوقة معتمدة قانوناً، والتي تصدر

شـهادات رقمية تربط بين الهوية الرقمية والسـمات البيومترية.

ويختلف التعامل مع هذه العلاقة باختلاف النظام القانوني. ففي الاتحاد الأوروبي، يُـنظر إلى البيانات البيومترية كجزء من الحق في الخصوصية، وبالتالي كحق شخصي مرتبط ارتباطاً وثيقاً بالهوية الرقمية. وقد أكدت محكمة العدل الأوروبية أن أي معالجة للبيانات البيومترية دون موافقة صاحبها تُعد انتهاكاً لكرامته الإنسـانية. أما في الولايات المتحدة، فإن التركيز يكون أكثر على الجوانب التعاقدية والأمنية، حيث تُعتبر البيانات البيومترية أداة لإثبات الرضا والموافقة في المعاملات الإلكترونية.

وفي العالم العربي، لا تزال العلاقة بين البيانات البيومترية والهوية الرقمية غامضة في العديد من

التشريعات. فبعض القوانين تقتصر على الاعتراف بالبصمة كوسيلة للتحقق من الهوية، دون أن تنص على طبيعة العلاقة بينها وبين الهوية الرقمية الشاملة. ونتيجة لذلك، تظهر ثغرات قانونية خطيرة، خاصة في حالات انتحال الهوية أو الاستخدام غير المصرح به.

ولسد هذه الثغرات، يتعين على المشرّع العربي أن يُدخل مفهوم "الهوية البيومترية" ضمن قواعد القانون المدني، ويُحدد بدقة شروط ارتباطها بالهوية الرقمية، وآثار هذا الارتباط على الحقوق والواجبات.

ومن الجدير بالذكر أن ظهور تقنيات الذكاء الاصطناعي يطرح تحديات جديدة لهذه العلاقة. فمثلاً، يمكن اليوم إعادة بناء بصمة الوجه من صور قديمة، أو محاكاة بصمة الصوت من

تسجيلات قصيرة. وهذا يخلق واقعاً جديداً: **الهوية البيومترية المزيفة**، التي تبدو حقيقية للأنظمة الآلية، لكنها ليست كذلك. وهنا، يبرز التحدي الأكبر: كيف يحمي القانون المدني الفرد من هوية بيومترية ليست له، لكنها تبدو وكأنها له؟

وفي الختام، يمكن القول إن البيانات البيومترية ليست مجرد مكوّن من مكونات الهوية الرقمية، بل هي **جوهرها الحقيقي**. ولذلك، فإن أي تنظيم قانوني فعال للهوية الرقمية يجب أن ينطلق من فهم عميق لهذه العلاقة، ويضمن أن تظل البيانات البيومترية محمية كأقدس ما يمتلكه الإنسان في عصره الرقمي.

الفصل السادس

الإطار التشريعي العربي لحماية البيانات البيومترية

يُشكل الإطار التشريعي العربي للبيانات البيومترية مرآةً تعكس درجة تطور الأنظمة القانونية في مواجهة التحديات الرقمية المعاصرة. وعلى الرغم من تنوع التجارب التشريعية بين الدول العربية، فإن هناك سمات مشتركة تطبع هذا الإطار، أبرزها: التأخر النسبي في الاعتراف المدني الكامل بالبيانات البيومترية، والتركيز على الجوانب الأمنية والإدارية على حساب الحماية المدنية للحقوق الفردية، وغياب التنسيق التشريعي بين الدول العربية في هذا المجال الحيوي.

بدأت أولى محاولات التشريع العربي في هذا السياق مع مطلع القرن الحادي والعشرين، حين

أدخلت العديد من الدول البصمة البيومترية في بطاقات الهوية الوطنية. ومن أبرز هذه التشريعات: قانون إصدار البطاقة الشخصية في مصر رقم 143 لسنة 2004، والقانون الجزائري المتعلق بالسجل الوطني للأفراد رقم 07-05 لسنة 2007، ونظام الأحوال المدنية السعودي لعام 1436ه. غير أن هذه القوانين ركزت في جوهرها على الإجراءات الفنية لإصدار الوثائق، دون أن تعالج البيانات البيومترية ككيان قانوني مستقل يمتلك عناصره وخصائصه وضماناته.

وفي العقد الثاني من القرن الحادي والعشرين، شهدت المنطقة تحولاً نوعياً مع إطلاق عدد من الدول مشاريع وطنية للهوية البيومترية الموحدة، مثل "الهوية الرقمية الوطنية" في المملكة العربية السعودية، و"البطاقة البيومترية الذكية" في دولة الإمارات، و"منصة الهوية الرقمية" في مصر. وقد رافق هذه المشاريع تشريعات جديدة

أو تعديلات على القوانين القائمة، لكنها ظلت محصورة في نطاق المراسيم التنفيذية أو القرارات الوزارية، دون أن ترتقي إلى مستوى قوانين مدنية شاملة تُنظم حقوق الأفراد والتزاماتهم في هذا المجال.

ويتميز الإطار التشريعي العربي الحالي بعدة خصائص رئيسية:

أولاً، **التفاوت الكبير بين الدول**. فبينما تمتلك دول الخليج العربي أنظمة متقدمة نسبياً، تدمج بين البنية التحتية التقنية والتشريعات الداعمة، تظل العديد من الدول العربية الأخرى تفتقر إلى أي إطار قانوني صريح للبيانات البيومترية. وهذا التفاوت يُعقّد من مسألة الاعتراف المتبادل بالهويات البيومترية عبر الحدود العربية.

ثانياً، **الهيمنة الأمنية على الخطاب التشريعي**. فمعظم التشريعات العربية تُدرج موضوع البيانات البيومترية ضمن قوانين مكافحة الجرائم الإلكترونية أو الأمن السيبراني، مما يُهمش البُعد المدني ويُضعف الحماية القانونية للحقوق الفردية. فمثلاً، يُجرّم القانون المصري رقم 175 لسنة 2018 استخدام بيانات بيومترية مزورة، لكنه لا يُفصّل في آليات التعويض المدني للضحايا.

ثالثاً، **غياب التكامل مع قواعد القانون المدني العام**. فنادراً ما تشير قوانين البيانات البيومترية في العالم العربي إلى المواد ذات الصلة في قوانين المدني (كالمواد المتعلقة بالإرادة، والغلط، والتدليس، والمسؤولية التقصيرية). وهذا الانفصال يخلق فجوة بين

النظام المدني التقليدي والنظام الرقمي الناشئ، ويُضعف من قدرة القضاء على تطبيق القواعد المدنية على النزاعات الرقمية.

رابعاً، **ضعف ضمانات الخصوصية وحماية البيانات**. فعلى الرغم من صدور بعض قوانين حماية البيانات الشخصية مؤخراً (كالقانون المصري رقم 151 لسنة 2020)، فإنها لا تُعالج بشكل كافٍ العلاقة بين البيانات البيومترية وحقوق الملكية على البيانات الشخصية. كما أن آليات الرقابة القضائية على جهات جمع البيانات البيومترية لا تزال محدودة.

خامساً، **عدم وجود آلية موحدة للاعتماد والاعتراف المتبادل**. فكل دولة عربية تضع معاييرها الخاصة لإصدار الهويات البيومترية، دون وجود اتفاقية عربية مشتركة تعترف بها كوثائق

قانونية متبادلة، وهو ما يُعيق حرية التنقل الرقمي داخل الفضاء العربي.

ولمعالجة هذه الثغرات، يتعين على المشرّع العربي أن يتجه نحو سن قوانين مدنية خاصة بالبيانات البيومترية، تُراعي المبادئ التالية:

- الاعتراف بالبيانات البيومترية ككيان قانوني مدني مستقل

- ربطها صراحةً بالهوية الرقمية في قوانين المدني

- تحديد حقوق والتزامات أصحاب البيانات البيومترية

- وضع آليات فعالة للتعويض المدني في حالات الانتحال أو الاختراق

- إنشاء جهات قضائية أو شبه قضائية متخصصة للنظر في النزاعات المتعلقة بها

إن بناء إطار تشريعي عربي متكامل للبيانات البيومترية ليس فقط ضرورة قانونية، بل هو شرط أساسي لبناء مجتمع رقمي عربي موثوق، قادر على المنافسة في الاقتصاد العالمي الرقمي.

الفصل السابع

دراسة تحليلية لتشريعات حماية البيانات البيومترية في دول مجلس التعاون الخليجي

يمثّل مجلس التعاون لدول الخليج العربية نموذجاً متقدماً نسبياً في المنطقة العربية من

حيث التبني التشريعي والتنفيذي لمفهوم حماية البيانات البيومترية. فقد سارعت دول المجلس إلى دمج هذا المفهوم ضمن رؤاها الوطنية للتحول الرقمي، ووضعت تشريعات وبنى تحتية تدعم وجود أنظمة بيومترية موحدة وموثوقة. ومع ذلك، فإن دراسة هذه التشريعات تكشف عن تفاوت داخلي في العمق المدني للتنظيم القانوني، إذ تتفوق بعض الدول في الجوانب التقنية بينما تبقى الجوانب المدنية المتعلقة بحماية الحقوق الفردية أقل نضجاً.

تبدأ الدراسة بدولة الإمارات العربية المتحدة، التي أصدرت قانون المعاملات الإلكترونية الاتحادي رقم 1 لسنة 2006، والذي اعترف بالتوقيع الإلكتروني والسجلات الإلكترونية كأداة قانونية معتمدة. وقد تطور هذا الإطار لاحقاً مع إطلاق "الهوية الرقمية الموحدة" (UAE Pass) في 2018، التي تُمكّن المواطنين والمقيمين

من الوصول إلى أكثر من 500 خدمة حكومية وخاصة عبر هوية رقمية واحدة تعتمد على البصمة ومسح الوجه. وعلى الرغم من التقدم الكبير، فإن القانون الإماراتي لا يحتوي على فصل مستقل ينظم البيانات البيومترية من منظور مدني، بل يكتفي بالإشارة إليها ضمن قواعد التوقيع الإلكتروني، دون تحديد واضح لمسؤوليات الجهات المصدرة أو آليات التعويض المدني في حالات الاختراق.

وفي المملكة العربية السعودية، تم إطلاق منصة "نفاذ" كجزء من رؤية 2030، والتي توفر هوية رقمية وطنية موحدة تعتمد على البيانات البيومترية. وقد صدر نظام المعاملات الإلكترونية عام 2007، ثم عُدّل عام 2018 ليواكب التطورات التقنية. ويتميز النظام السعودي باعتماده مفهوم "الشهادة الرقمية المؤهلة"، التي تُصدرها جهات معتمدة من الهيئة

السعودية للبيانات والذكاء الاصطناعي (SDAIA). غير أن النصوص القانونية لا تتناول بشكل كافٍ العلاقة بين البيانات البيومترية والهوية الرقمية في القانون المدني السعودي، ولا تُفصّل في حالات الغلط أو التدليس الإلكتروني، مما يترك فراغاً في الحماية المدنية للمتعاملين.

أما في دولة قطر، فقد صدر قانون المعاملات الإلكترونية رقم 16 لسنة 2010، الذي نصّ على الاعتراف القانوني بالتوقيع الإلكتروني والمستندات الرقمية. كما أطلقت الدولة مشروع "الهوية الرقمية الوطنية" في إطار استراتيجية قطر الوطنية للتحول الرقمي 2025، والذي يعتمد على البصمة ومسح الوجه. لكن التشريع القطري، شأنه شأن غيره، يفتقر إلى مواد مدنية تُنظّم المسؤولية التقصيرية عن انتحال البيانات البيومترية أو إساءة استخدامها، ويترك هذه المسائل للقضاء دون معايير تشريعية واضحة.

وفي الكويت، يُعد قانون المعاملات الإلكترونية رقم 20 لسنة 2014 هو الإطار التشريعي الأساسي. وقد أطلقت الدولة منصة "الهوية الرقمية" في 2021، لكن التطبيق لا يزال محدوداً نسبياً. ويلاحظ أن القانون الكويتي يركّز على الجانب الجنائي أكثر من المدني، إذ يُجرّم انتحال البيانات البيومترية دون أن يُحدد حقوق المتضرر في طلب التعويض أو إبطال العقود الناتجة عن هذا الانتحال.

وبالنسبة لسلطنة عُمان، فقد صدر قانون المعاملات الإلكترونية رقم 69 لسنة 2008، ثم تم تحديثه في إطار استراتيجية الحكومة الإلكترونية. كما أطلقت المنصة الوطنية للهوية الرقمية "eOman" في 2022، والتي تعتمد على البصمة ومسح الوجه. ومع ذلك، فإن التشريع

العماني لا يحتوي على أحكام مدنية مفصلة تتعلق بإثبات صحة البيانات البيومترية أو حمايتها من الاستغلال غير المشروع.

أخيراً، في مملكة البحرين، يُعد قانون المعاملات الإلكترونية رقم 28 لسنة 2002 من أقدم التشريعات في المنطقة، وقد تم تطويره لاحقاً ضمن مشروع "الهوية الرقمية الوطنية". وتتميز البحرين بوجود هيئة تنظيمية مستقلة (الهيئة الوطنية للمعلومات والحكومة الإلكترونية)، لكن التشريع لا يزال يفتقر إلى ربط صريح بين البيانات البيومترية وقواعد المسؤولية المدنية في القانون البحريني.

ومن خلال هذه المقارنة، يتضح أن دول مجلس التعاون قد حققت تقدماً كبيراً في البنية التحتية والاعتماد الحكومي للبيانات البيومترية،

لكنها لم تواكب هذا التقدم بتطوير إطار مدني شامل يحمي حقوق الأفراد. فالتشريعات الحالية تُعنى أساساً بالإثبات والصحة الشكلية، بينما تُهمَل الجوانب الجوهرية مثل:

- المسؤولية المدنية لمزوّدي خدمات البيانات البيومترية

- حق الضحية في التعويض عن الضرر المعنوي والمادي

- حماية البيانات البيومترية المرتبطة بالهوية

- آليات الطعن في قرارات إلغاء أو تعليق الهوية البيومترية

ولذلك، فإن الخطوة التالية أمام دول المجلس يجب أن تكون سنّ قوانين مدنية خاصة أو تعديل

قوانين المدني الحالية لتضمّن أحكاماً صريحة تنظّم البيانات البيومترية من منظور مدني شامل، بما يتماشى مع أعلى المعايير العالمية، ويُعزّز ثقة الأفراد في الفضاء الرقمي.

الفصل الثامن

التنظيم القانوني للبيانات البيومترية في الدول العربية غير الخليجية

بينما تشهد دول مجلس التعاون الخليجي زخماً تشريعياً وتنفيذياً في مجال البيانات البيومترية، تبقى التجارب في باقي الدول العربية متفاوتة ومبعثرة، وغالباً ما تعاني من ضعف البنية التحتية القانونية والتقنية. ومع ذلك، فإن بعض الدول قد أطلقت مبادرات جادة تستحق الدراسة والتحليل، خاصة في ظل السعي الإقليمي نحو

التحول الرقمي. وتشمل هذه الدول كلاً من مصر، الجزائر، تونس، الأردن، والمغرب، وهي تمثل نماذج متعددة لدرجات التقدم في هذا المجال.

في جمهورية مصر العربية، يُعد قانون إنشاء مركز المعلومات الوطني رقم 151 لسنة 2004، وقانون مكافحة الجرائم الإلكترونية رقم 175 لسنة 2018، وقانون حماية البيانات الشخصية رقم 151 لسنة 2020، الأعمدة الثلاثة التي يرتكز عليها الإطار التشريعي للبيانات البيومترية. وقد أطلقت الدولة "منصة الهوية الرقمية" في 2021، التي تتيح للمواطنين استخدام هويتهم الوطنية البيومترية في التعامل مع الجهات الحكومية والإلكترونية. غير أن هذا الإطار يعاني من فجوة مدنية واضحة: فقانون حماية البيانات لا ينظم العلاقة بين البيانات البيومترية والهوية الرقمية، وقانون الجرائم الإلكترونية يركز على

العقوبات دون تحديد آليات التعويض المدني. كما أن قانون المدني المصري لم يُعدّل ليشمل أحكاماً خاصة بالبيانات البيومترية، مما يترك القضاء دون دليل تشريعي واضح في النزاعات المتعلقة بها.

وفي الجزائر، صدر قانون تكنولوجيات الإعلام والاتصال رقم 18-07 لسنة 2018، الذي تضمّن فصلاً خاصاً بالتوقيع الإلكتروني والسجلات الرقمية. كما أطلقت الحكومة مشروع "البطاقة البيومترية الذكية"، التي تُعد خطوة أولى نحو هوية رقمية وطنية تعتمد على البصمة ومسح الوجه. لكن التشريع الجزائري لا يحتوي على أي تنظيم مدني مباشر للبيانات البيومترية، بل يكتفي بالإشارة إلى أدواتها التقنية. ويبقى الفرد الجزائري دون حماية قانونية كافية في حال انتحال بياناته البيومترية أو استخدامها دون إذنه، إذ لا يوجد نص يُلزم الجهات المُصدِرة بتحمل

المسؤولية المدنية عن الأخطاء أو الثغرات الأمنية.

أما في تونس، فقد كانت سباقة في المنطقة بإصدار قانون التوقيع الإلكتروني رقم 89 لسنة 2004، ثم تحديثه ضمن قانون الاتصالات لعام 2016. كما أطلقت "المنصة الوطنية للهوية الرقمية" في 2022، والتي تعتمد على البصمة ومسح الوجه. ويتميز التشريع التونسي بوجود هيئة مستقلة (الهيئة الوطنية للبريد الإلكتروني والتوقيع الإلكتروني)، لكنه يفتقر إلى ربط صريح بين البيانات البيومترية وقواعد المسؤولية المدنية في مجلة الالتزامات والعقود. فمثلاً، لا توجد أحكام تُنظّم حالات الغلط في إبرام العقود عبر هوية بيومترية مختلَسة، ولا تُحدّد شروط إبطال هذه العقود.

وفي المملكة الأردنية الهاشمية، يُعد قانون المعاملات الإلكترونية رقم 85 لسنة 2001، وتعديلاته اللاحقة، الإطار التشريعي الأساسي. وقد أطلقت الدولة "الهوية الرقمية الوطنية" في 2023، كجزء من رؤيتها للتحول الرقمي، والتي تعتمد على البصمة ومسح الوجه. ومع ذلك، فإن التشريع الأردني لا يزال ينظر إلى البيانات البيومترية من زاوية تقنية وأمنية، دون تناول كافٍ لآثارها المدنية. فمثلاً، لا توجد أحكام تُنظّم حق الفرد في تصحيح بياناته البيومترية أو حذفها، ولا تُفصّل في المسؤولية المدنية للجهات التي تفشل في حماية البيانات البيومترية الموكلة إليها.

وفي المملكة المغربية، صدر قانون 53-05 المتعلق بالتبادل الإلكتروني للمعطيات القانونية عام 2007، والذي اعترف بالتوقيع الإلكتروني. كما أطلقت الحكومة "المنصة الوطنية للهوية

الرقمية" في إطار استراتيجية المغرب الرقمي 2025، والتي تعتمد على البصمة ومسح الوجه. ويُلاحظ أن المغرب بدأ مؤخراً في تطوير قانون حماية البيانات الشخصية، لكنه لم يُدمج بعد مفاهيم البيانات البيومترية ضمن قواعد القانون المدني. وبالتالي، تظل الحماية المدنية للبيانات البيومترية هشة، وتُترك للاجتهاد القضائي دون أساس تشريعي راسخ.

ومن خلال مقارنة هذه التجارب، يتضح أن الدول العربية غير الخليجية تواجه تحديات مشتركة، أهمها:

- غياب التكامل بين التشريعات الرقمية وقوانين المدني

- التركيز على البُعد الأمني على حساب البُعد المدني

- ضعف آليات الرقابة القضائية على جهات إصدار البيانات البيومترية

- عدم وجود نصوص صريحة تُنظم المسؤولية المدنية عن الأضرار الناتجة عن اختراق البيانات البيومترية

ولمعالجة هذه الثغرات، يتعين على هذه الدول أن تتبنى منهجاً تشريعياً أكثر شمولاً، يدمج البيانات البيومترية ضمن النظام المدني العام، ويُحدد بوضوح حقوق الأفراد، والتزامات الجهات المُصدِرة، وآليات التعويض والطعن. إن بناء ثقة المواطنين في البيانات البيومترية لا يعتمد فقط على الكفاءة التقنية، بل على وجود ضمانات قانونية مدنية قوية تحمي كرامتهم وحقوقهم في الفضاء الرقمي.

الفصل التاسع

الحماية المدنية للبيانات البيومترية في النظام القانوني المصري

يُعد النظام القانوني المصري من الأنظمة التي بدأت مبكراً في ملامسة مفاهيم البيانات البيومترية، سواء من خلال البنية التشريعية أو المبادرات التنفيذية. ومع ذلك، فإن الحماية المدنية للبيانات البيومترية في مصر لا تزال دون المستوى المأمول، إذ تعاني من تشتت تشريعي، وضعف في الربط مع قواعد القانون المدني العام، وغياب آليات فعالة لتعويض المتضررين. ويهدف هذا الفصل إلى تحليل دقيق للإطار القانوني الحالي، وتحديد الثغرات المدنية، واقتراح سبل تطويره.

ينطلق الإطار القانوني المصري من ثلاث ركائز رئيسية:

الأولى، **قانون إنشاء مركز المعلومات الوطني رقم 151 لسنة 2004**، الذي أنشأ الجهة التقنية المسؤولة عن إدارة البيانات الرقمية، لكنه لم يُنظم العلاقة بين هذه البيانات والهوية المدنية للأفراد.

الثانية، **قانون مكافحة الجرائم الإلكترونية رقم 175 لسنة 2018**، الذي جرّم انتحال البيانات البيومترية (المادة 25)، ونص على عقوبات جنائية تصل إلى السجن خمس سنوات. غير أن هذا القانون تجاهل تماماً البُعد المدني، ولم يُشر إلى حق الضحية في التعويض أو إبطال العقود الناتجة عن الانتحال.

الثالثة، **قانون حماية البيانات الشخصية رقم

151 لسنة 2020**، الذي يُعد خطوة إيجابية، إذ نص على مبادئ المعالجة المشروعة للبيانات، وحقوق أصحاب البيانات، ومسؤوليات الجهات المعالِجة. لكنه لم يُفصّل في كيفية تطبيق هذه المبادئ على البيانات البيومترية ككيان قانوني مستقل، ولا على العلاقة بينها وبين الهوية الرقمية في القانون المدني.

ومن الناحية التطبيقية، أطلقت الدولة "منصة الهوية الرقمية" في 2021، التي تتيح للمواطنين استخدام هويتهم الوطنية البيومترية في التعامل مع الجهات الحكومية والخاصة. وتُدار هذه المنصة من قبل مركز المعلومات الوطني، بالتعاون مع وزارة الاتصالات. غير أن الشروط والأحكام المرتبطة باستخدام المنصة لا تتضمن التزامات مدنية واضحة تجاه المستخدم، ولا تُحدّد حدود المسؤولية في حال حدوث اختراق أو خطأ تقني.

أما من منظور القانون المدني المصري، فلا توجد أي مواد صريحة تنظم البيانات البيومترية. فمثلاً، لا تشير المواد المتعلقة بالإرادة (كالمادة 109 من القانون المدني) إلى حالات التدليس الإلكتروني أو الغلط الناتج عن انتحال البيانات البيومترية. كما أن قواعد المسؤولية التقصيرية (المواد 163 وما يليها) لا تتناول بشكل خاص الأضرار الناتجة عن اختراق البيانات البيومترية أو إساءة استخدامها. ونتيجة لذلك، يضطر القضاء إلى الاجتهاد في تطبيق القواعد العامة، مما يؤدي إلى تفاوت في الأحكام وعدم وضوح في المعايير.

ومن أبرز الثغرات المدنية في النظام المصري:

1. **غياب الاعتراف الصريح بالبيانات البيومترية ككيان مدني**: فالتشريعات الحالية تتعامل معها كأداة تقنية، لا كتجسيد للهوية في الفضاء الرقمي.

2. **عدم تحديد المسؤولية المدنية لجهات الإصدار**: ففي حال اختراق البيانات البيومترية بسبب ثغرة أمنية في المنصة الرسمية، لا يوجد نص يُلزم الجهة الحكومية بتحمل المسؤولية المدنية.

3. **ضعف آليات التعويض**: إذ لا توجد إجراءات مبسطة تمكن الضحية من طلب التعويض عن الضرر المادي أو المعنوي الناتج عن انتحال بياناته البيومترية.

4. **غياب حق التصحيح والحذف الفعّال**: فرغم وجوده في قانون حماية البيانات، إلا أن تطبيقه على البيانات البيومترية يفتقر إلى

الآليات العملية والرقابة القضائية.

ولمعالجة هذه الثغرات، يُقترح ما يلي:

- تعديل قانون المدني المصري لإضافة فصل خاص بالبيانات البيومترية، يُنظم علاقتها بالهوية الرقمية، ويُحدد شروط صحتها، وآثار انتحالها.

- إدخال نصوص في قانون حماية البيانات تُفصّل في حقوق أصحاب البيانات البيومترية، والتزامات الجهات المصدرة.

- إنشاء آلية قضائية متخصصة للنظر في النزاعات المتعلقة بالبيانات البيومترية، تضم خبراء تقنيين وقانونيين.

- تضمين شروط استخدام منصة الهوية الرقمية بنوداً ملزمة تحمي حقوق المستخدم وتُحدّد

مسؤوليات الجهة المُصدرة.

إن تطوير الحماية المدنية للبيانات البيومترية في مصر ليس فقط مطلباً قانونياً، بل هو ضرورة اقتصادية واجتماعية، خاصة في ظل التوسع الكبير في الخدمات الرقمية والمعاملات الإلكترونية. فلا يمكن بناء مجتمع رقمي موثوق دون ضمانات قانونية مدنية قوية تحمي كرامة المواطن وحقوقه الأساسية في الفضاء الإلكتروني.

الفصل العاشر

الحماية المدنية للبيانات البيومترية في النظام القانوني الجزائري

يُعد النظام القانوني الجزائري من الأنظمة التي بدأت تولي اهتماماً متزايداً بالتحول الرقمي، وظهر ذلك جلياً في إصدار قانون تكنولوجيات الإعلام والاتصال رقم 18-07 لسنة 2018، الذي يُشكل الإطار التشريعي الأساسي للبيانات البيومترية في البلاد. ومع ذلك، فإن الحماية المدنية للبيانات البيومترية في الجزائر لا تزال في مراحلها الأولى، وتعاني من غموض تشريعي، وضعف في الربط مع قواعد القانون المدني، وغياب آليات فعالة لضمان حقوق الأفراد في حال انتهاك بياناتهم البيومترية.

ينص قانون تكنولوجيات الإعلام والاتصال على مبادئ عامة تتعلق بالتوقيع الإلكتروني، والسجلات الرقمية، واعتماد جهات التصديق. وقد أطلقت الحكومة مشروع "البطاقة البيومترية الذكية" كخطوة أولى نحو هوية رقمية وطنية موحدة تعتمد على البصمة ومسح الوجه. غير أن

هذا القانون، شأنه شأن العديد من التشريعات العربية، يركز على الجوانب التقنية والأمنية، ويُهمش البُعد المدني بشكل ملحوظ. فلم يتضمن أي أحكام تُنظم العلاقة بين البيانات البيومترية والهوية الرقمية، ولا يُفصّل في المسؤولية المدنية الناتجة عن انتحال البيانات البيومترية أو سوء استخدامها.

ومن منظور القانون المدني الجزائري، لا توجد أي مواد صريحة تتناول البيانات البيومترية. فمثلاً، لا تشير المواد المتعلقة بالإرادة (كالمادة 73 من القانون المدني) إلى حالات الغلط أو التدليس الإلكتروني. كما أن قواعد المسؤولية التقصيرية (المواد 124 وما يليها) لا تتضمن نصوصاً خاصة بالأضرار الناتجة عن اختراق البيانات البيومترية. ونتيجة لذلك، يُترك القضاء الجزائري دون دليل تشريعي واضح، مما يؤدي إلى اجتهادات متفاوتة، ويفتقر المتضررون إلى ضمانات قانونية

موحدة.

ومن أبرز الثغرات المدنية في النظام الجزائري:

1. **غياب التعريف القانوني المدني للبيانات البيومترية**: فالتشريع الجزائري لا يعرّف البيانات البيومترية ككيان قانوني مستقل، بل يكتفي بالإشارة إلى أدواتها (كالتوقيع الإلكتروني)، مما يضعف من قدرة القضاء على حمايتها.

2. **عدم تحديد المسؤولية المدنية لجهات الإصدار**: ففي حال حدوث اختراق بسبب ثغرة في نظام البطاقة البيومترية، لا يوجد نص يُلزم الدولة أو الجهة المُصدرة بتحمل المسؤولية المدنية تجاه المواطن.

3. **غياب آليات التعويض المدني**: إذ لا توجد إجراءات قانونية مبسطة تمكن الضحية من طلب تعويض عن الضرر المادي أو المعنوي الناتج عن انتحال بياناته البيومترية.

4. **ضعف حماية البيانات البيومترية المرتبطة بالهوية**: فرغم وجود مشروع قانون لحماية البيانات الشخصية، إلا أنه لم يُصادق عليه بعد، مما يترك بيانات الهوية البيومترية دون حماية قانونية كافية.

ولمعالجة هذه الثغرات، يُقترح ما يلي:

- إدخال تعديلات على القانون المدني الجزائري لإضافة أحكام خاصة بالبيانات البيومترية، تُنظم علاقتها بالهوية الرقمية، وتُحدد شروط صحتها، وآثار انتحالها.

- سن قانون خاص بالبيانات البيومترية يدمج بين الجوانب التقنية والمدنية، ويُحدّد التزامات الجهات المصدرة، وحقوق أصحاب البيانات.

- الإسراع في إصدار قانون حماية البيانات الشخصية، وضمان تضمينه أحكاماً تُطبّق صراحةً على البيانات البيومترية.

- إنشاء وحدة قضائية متخصصة داخل المحاكم للنظر في النزاعات المتعلقة بالبيانات البيومترية، تضم خبراء في القانون المدني والتكنولوجيا.

إن تطوير الحماية المدنية للبيانات البيومترية في الجزائر ليس فقط استجابة للتحول الرقمي، بل هو تأكيد على احترام كرامة المواطن وحقوقه الأساسية في العصر الرقمي. فلا يمكن الحديث عن دولة رقمية حديثة دون وجود إطار مدني قوي يحمي هوية الفرد ويضمن سلامته في

الفضاء الإلكتروني.

الفصل الحادي عشر

المبادئ الدستورية المتعلقة بالبيانات البيومترية في العالم العربي

لا يمكن فصل التنظيم المدني للبيانات البيومترية عن الإطار الدستوري الذي يُشكل السقف الأعلى للنظام القانوني في أي دولة. ففي العالم العربي، تضمنت العديد من الدساتير المعاصرة مبادئ عامة تتعلق بحقوق الإنسان، الخصوصية، كرامة الفرد، وحماية البيانات، والتي يمكن أن تُشكّل أساساً دستورياً لحماية البيانات البيومترية. ومع ذلك، فإن هذه المبادئ لا تزال عامة وغير محددة، ولا توجد دساتير عربية صريحة تعترف بالبيانات البيومترية كحق

دستوري مستقل. ويهدف هذا الفصل إلى تحليل هذه المبادئ، واستخلاص آثارها على الحماية المدنية للبيانات البيومترية.

أولاً، **مبدأ كرامة الإنسان**: نصت العديد من الدساتير العربية على احترام كرامة الإنسان كحق أصيل. فمثلاً، المادة 54 من الدستور المصري لسنة 2014 تنص على أن "الكرامة حق لكل إنسان"، والمادة 39 من الدستور الجزائري لسنة 2020 تؤكد أن "الكرامة الإنسانية مصونة". ونظراً لأن البيانات البيومترية تمثل جوهر الذات الإنسانية، فإن أي انتهاك لها — كسرقة أو انتحال — يُعد انتهاكاً لكرامته. ولذلك، فإن هذا المبدأ يُشكّل أساساً دستورياً قوياً لفرض التزامات مدنية على الجهات التي تفشل في حماية البيانات البيومترية.

ثانياً، **حق الخصوصية**: نصت دساتير عديدة على حق الفرد في الحياة الخاصة. فالمادة 57 من الدستور المصري تنص على أن "حرية المراسلات والاتصالات السلكية واللاسلكية وغيرها من وسائل الاتصال مكفولة"، والمادة 46 من الدستور التونسي تؤكد على "حرمة الحياة الخاصة". ونظراً لأن البيانات البيومترية تحتوي على معلومات شخصية حساسة جداً، فإن حمايتها تُعد جزءاً من حماية الخصوصية. وبالتالي، فإن أي معالجة غير مشروعة لهذه البيانات تُعد انتهاكاً دستورياً، يُمكن أن يُستند إليه في طلب التعويض المدني.

ثالثاً، **حق حماية البيانات الشخصية**: رغم أن هذا الحق لم يُنص عليه صراحةً في معظم الدساتير العربية القديمة، إلا أن الدساتير الحديثة بدأت تتضمنه. فمثلاً، المادة 48 من الدستور التونسي لسنة 2014 تنص على "حق

كل مواطن في حماية معطياته الشخصية". كما أن الدستور الجزائري لسنة 2020 أشار في المادة 40 إلى "حماية المعطيات ذات الطابع الشخصي". وهذا يُعد تطوراً مهماً، إذ يمنح البيانات البيومترية غطاءً دستورياً مباشراً، ويجعل من واجب الدولة سن تشريعات مدنية تُفصّل في آليات هذه الحماية.

رابعاً، **مبدأ المساواة أمام القانون**: نصت جميع الدساتير العربية على مبدأ المساواة. فالمادة 53 من الدستور المصري تنص على أن "المواطنون لدى القانون سواء". وهذا المبدأ يحظر استخدام البيانات البيومترية كأداة للتمييز أو الاستبعاد الاجتماعي. فمثلاً، لا يجوز حرمان شخص من خدمة عامة لمجرد عدم امتلاكه هوية بيومترية، ما لم يكن هناك بديل معقول. كما يُلزم الدولة بضمان وصول الجميع إلى الهوية البيومترية دون تمييز.

خامساً، **مبدأ سيادة القانون**: يُعد هذا المبدأ ركيزة أساسية في جميع الدساتير العربية. وهو يقتضي أن تكون جميع إجراءات جمع ومعالجة البيانات البيومترية، واستخدامها، وإلغائها، خاضعة للقانون، وقابلة للطعن أمام القضاء. فلا يجوز أن تُدار البيانات البيومترية عبر قرارات إدارية منفردة دون رقابة قضائية.

ومع ذلك، تبرز عدة تحديات في تفعيل هذه المبادئ دستورياً:

- **عمومية النصوص**: فمعظم الدساتير لا تذكر "البيانات البيومترية" صراحةً، مما يترك مجالاً واسعاً للتفسير.

- **ضعف الرقابة الدستورية**: فقلة من المحاكم الدستورية العربية تناولت قضايا مرتبطة بالبيانات البيومترية، ما يحد من تطور الاجتهاد الدستوري في هذا المجال.

- **غياب التشريعات المنفذة**: فحتى عندما توجد مبادئ دستورية، فإن غياب القوانين المدنية المنظ ِمة يُضعف من قدرتها على توفير حماية فعلية.

ولذلك، يُوصى بما يلي:

- تعديل الدساتير العربية لإدراج نص صريح يعترف بالبيانات البيومترية كجزء من كرامة الإنسان وحقه في الخصوصية.

- تفعيل دور المحاكم الدستورية في مراجعة التشريعات المتعلقة بالبيانات البيومترية، والتأكد

من توافقها مع المبادئ الدستورية.

- ربط التشريعات المدنية الخاصة بالبيانات البيومترية صراحةً بالمبادئ الدستورية، لضمان أعلى درجات الحماية.

إن الاعتراف الدستوري بالبيانات البيومترية ليس ترفاً قانونياً، بل هو ضرورة في عصر أصبحت فيه هذه البيانات جزءاً من وجود الفرد. فبدون هذا الاعتراف، تبقى الحماية المدنية هشة، وتظل حقوق الأفراد عرضة للانتهاك دون سند دستوري راسخ.

الفصل الثاني عشر

النظام القانوني الأمريكي لحماية البيانات البيومترية

يُعد النظام القانوني الأمريكي من الأنظمة الفريدة في معالجته للبيانات البيومترية، إذ يتميز بتفكيك التشريعات بين المستويين الفيدرالي والولائي، واعتماد مبدأ السوق التنظيمي (Regulatory Market Approach)، الذي يمنح الولايات حرية تطوير أطرها الخاصة، مع وجود مبادئ توجيهية عامة على المستوى الاتحادي. وعلى عكس النظم المدنية التقليدية، لا يعتمد النظام الأمريكي على قانون مدني موحد، بل على مجموعة من القوانين المتخصصة، والقرارات القضائية، والممارسات التعاقدية، مما يجعل دراسة البيانات البيومترية فيه معقدة لكنها غنية بالتجارب العملية.

على المستوى الفيدرالي، لا يوجد قانون شامل ينظم البيانات البيومترية. فالتشريعات الفيدرالية

تركز على قطاعات محددة، مثل:

- **قانون خصوصية الفيديو (VPPA)** لعام 1988، الذي يحمي بيانات المشاهدة.

- **قانون HIPAA** لعام 1996، الذي يحمي البيانات الصحية، بما فيها البصمات الجينية.

- **قانون حماية خصوصية الإنترنت للأطفال (COPPA)** لعام 1998، الذي يحمي بيانات الأطفال البيومترية.

أما على مستوى الولايات، فتتفاوت التشريعات بشكل كبير. فمثلاً، في **إلينوي**، صدر **قانون خصوصية المعلومات البيومترية (BIPA)** لعام 2008، الذي يُعد أول تشريع في العالم ينظم جمع ومعالجة البيانات البيومترية من منظور مدني. ويتطلب القانون:

- الحصول على موافقة خطية صريحة قبل جمع البيانات البيومترية.

- إبلاغ الفرد بكيفية استخدام بياناته ومدتها.

- حظر بيع أو تأجير البيانات البيومترية.

- فرض غرامات تصل إلى 5000 دولار لكل انتهاك.

وفي **تكساس**، صدر **قانون التقاط الخصائص البيومترية** لعام 2009، الذي يفرض التزامات مشابهة، لكنه أقل صرامة من BIPA. وفي **واشنطن**، صدر قانون مماثل عام 2017.

ومن الناحية القضائية، لعبت المحاكم الأمريكية

دوراً محورياً في تشكيل مفهوم حماية البيانات البيومترية. ففي قضية *Rosenbach v. Six* (2019) *Flags Entertainment Corp.*، أكدت المحكمة العليا في إلينوي أن "انتهاك BIPA يُعد ضرراً مدنياً قائماً بذاته"، حتى لو لم ينتج عنه خسارة مالية مباشرة. وفي قضية *Patel v. Facebook, Inc.* (2019)*، وافقت محكمة الاستئناف الفيدرالية على دعوى جماعية ضد فيسبوك لاستخدامه تقنية التعرف على الوجه دون موافقة المستخدمين.

ومن حيث الحماية المدنية، يعتمد النظام الأمريكي على ثلاثة محاور:

1. **المسؤولية التعاقدية**: فعند استخدام البيانات البيومترية في إبرام عقود، يُطبّق قانون العقود (Contract Law)، ويُنظر إلى أي انتحال

كغش أو تدليس يُبرر إبطال العقد.

2. **المسؤولية التقصيرية**: ففي حال سرقة البيانات البيومترية، يمكن للمتضرر رفع دعوى "إهمال" (Negligence) ضد الجهة التي فشلت في حمايتها، إذا ثبت أن هذا الإهمال تسبب في ضرر مباشر.

3. **التعويضات الرادعة**: فبعض القوانين الولائية (مثل BIPA) تسمح بمنح تعويضات رادعة (Punitive Damages) في حالات الاستغلال الجسيم للبيانات البيومترية.

ومع ذلك، يعاني النظام الأمريكي من تحديات رئيسية:

- **التشتت التشريعي**: فاختلاف القوانين

بين الولايات يُعقّد من حماية البيانات البيومترية عبر الحدود الداخلية.

- **التركيز على السوق**: فالمقاربة التنظيمية تعتمد على المنافسة بين الولايات لجذب الشركات، ما قد يُضعف من معايير الحماية.

- **غياب قانون اتحادي شامل**: رغم محاولات متكررة، لم يُسنّ الكونغرس قانوناً اتحادياً يوازي اللائحة الأوروبية (GDPR).

ورغم هذه التحديات، يظل النظام الأمريكي نموذجاً مهماً بسبب مرونته، وفاعليته في حماية الحقوق عبر الآليات القضائية، وقدرته على التكيف مع التحديات التقنية الجديدة. ولذلك، فإن دراسته تقدم دروساً قيمة للأنظمة المدنية، خاصة في كيفية دمج الحماية المدنية للبيانات البيومترية ضمن إطار قانوني دينامي

وعملي.

الفصل الثالث عشر

المسؤولية المدنية في القانون الأمريكي عن انتهاك البيانات البيومترية

في ظل غياب قانون مدني موحد في الولايات المتحدة، تستند المسؤولية المدنية عن انتهاك البيانات البيومترية إلى شبكة معقدة من القواعد المشتقة من القانون العام (Common Law)، والتشريعات الفيدرالية والولائية، والممارسات القضائية. ورغم عدم وجود نص يُسمّى "البيانات البيومترية" صراحةً في معظم التشريعات، فإن المحاكم الأمريكية طوّرت عبر العقود الماضية آليات فعالة لحماية الأفراد من الانتحال، والاستغلال غير المشروع، والإهمال

الأمني، مستندةً إلى مبادئ راسخة في المسؤولية التقصيرية والتعاقدية.

أولاً، **المسؤولية التقصيرية (Tort Liability)**:

تُعد دعوى "الإهمال" (Negligence) الوسيلة الرئيسية لطلب التعويض المدني في حالات اختراق البيانات البيومترية. ولإثبات الإهمال، يجب على المدعي إثبات أربعة عناصر:

1. وجود واجب قانوني على المدعى عليه لحماية بيانات الهوية البيومترية (Duty of Care).

2. خرق لهذا الواجب (Breach).

3. وجود علاقة سببية بين الخرق والضرر

.(Causation)

4. وقوع ضرر فعلي (Damages).

وقد أكدت محكمة الاستئناف الفيدرالية في قضية *In re: Equifax Inc. Customer Data Security Breach Litigation)* (2019 أن المؤسسات التي تجمع بيانات بيومترية حساسة تتحمل واجباً قانونياً بحمايتها، حتى لو لم يكن هناك تشريع صريح يفرض ذلك. كما أن العديد من الولايات، مثل إلينوي وتكساس، اعترفت صراحةً بأن الإخفاق في تطبيق معايير أمنية معقولة يُعد إهمالاً مدنياً.

ثانياً، **المسؤولية التعاقدية (Contractual Liability)**:

عند استخدام البيانات البيومترية في المعاملات التجارية، يُطبّق قانون العقود. فإذا استخدم طرف بيانات بيومترية مزورة لإبرام عقد، فإن العقد يكون قابلاً للإبطال لعيب في الرضا (Lack of Genuine Consent). كما أن شروط الخدمة (Terms of Service) التي توافق عليها المنصات الرقمية تُعد عقوداً ملزمة، فإذا خالفت جهة ما التزاماتها الأمنية المنصوص عليها، فإنها تكون مسؤولة مدنياً عن الأضرار الناتجة.

ثالثاً، **المسؤولية بموجب التشريعات الخاصة**:

أصدرت العديد من الولايات قوانين تفرض التزامات مدنية مباشرة على الجهات التي تفشل في حماية البيانات البيومترية. فمثلاً، ينص قانون إلينوي BIPA على أن أي جهة تخضع لاختراق بيانات بيومترية يجب أن تُبلغ المتضررين فوراً،

وإلا تُعتبر مسؤولة مدنياً عن الأضرار الناتجة عن التأخير. كما يمنح BIPA الحق في رفع دعاوى جماعية (Class Actions) في حالات الانتهاك الجسيم، مع تعويضات تصل إلى 5000 دولار لكل انتهاك.

رابعاً، **التعويضات**:

يمكن للمحاكم الأمريكية منح ثلاثة أنواع من التعويضات:

- **التعويض الفعلي (Actual Damages)**: يشمل الخسائر المالية المباشرة، كتكاليف استعادة الهوية، أو فقدان الأموال.

- **التعويض المعنوي (Emotional Distress Damages)**: في حالات الضرر النفسي الناتج عن انتحال الهوية البيومترية.

- **التعويضات الرادعة (Punitive Damages)**: تُمنح في حالات الإهمال الجسيم أو السلوك المتعمد، وتهدف إلى ردع الجهات المخالفة.

خامساً، **الآليات الوقائية**:

إلى جانب التعويض، يمكن للمحاكم إصدار أوامر قضائية (Injunctions) تُلزم الجهات باتخاذ إجراءات أمنية محددة، أو وقف معالجة البيانات البيومترية حتى يتم تصحيح الثغرات.

ومع ذلك، تبرز تحديات في تطبيق هذه المسؤولية:

- **صعوبة إثبات العلاقة السببية** بين خرق

البيانات والضرر الفعلي، خاصة في حالات التسريبات الواسعة.

- **الحصانة الجزئية** التي تتمتع بها بعض المنصات بموجب المادة 230 من قانون الآداب الاتصالية (Communications Decency Act).

- **تفاوت المعايير** بين الولايات، مما يُعقّد من الدعاوى العابرة للحدود.

ورغم هذه التحديات، يظل النظام الأمريكي نموذجاً فعالاً في فرض المسؤولية المدنية عن انتهاك البيانات البيومترية، ليس عبر تشريعات جامدة، بل عبر آليات مرنة تستجيب للتطورات التقنية، وتُعطي الأولوية لحماية الفرد كطرف ضعيف في العلاقة الرقمية.

الفصل الرابع عشر

دور المحاكم الأمريكية في حماية البيانات البيومترية

لا يعتمد النظام القانوني الأمريكي على التشريعات وحدها لحماية الحقوق، بل يمنح القضاء دوراً محورياً في تشكيل المبادئ القانونية وتطويرها استجابةً للتحديات الجديدة. وفي مجال البيانات البيومترية، لعبت المحاكم الأمريكية — من المحكمة العليا إلى محاكم الولايات — دوراً رياديًا في تحديد طبيعة هذه البيانات، ونطاق حمايتها، ومسؤوليات الأطراف المختلفة. وقد تم ذلك عبر سلسلة من الأحكام التاريخية التي رسّخت مبادئ دستورية ومدنية جديدة، وأسست لفهم معاصر للهوية في العصر الرقمي.

أولاً، **المحكمة العليا للولايات المتحدة**:

لم تصدر المحكمة العليا حكماً مباشراً حول البيانات البيومترية بعد، لكن أحكامها في قضايا ذات صلة وضعت الأسس الدستورية لحمايتها. ففي قضية *Riley v. California* (2014)، اعتبرت المحكمة أن "الهواتف الذكية تحتوي على هوية رقمية كاملة"، ولا يجوز تفتيشها دون إذن قضائي. وفي قضية *Carpenter v. United States* (2018)، أكدت أن "بيانات الموقع الجغرافي تُعد جزءاً من الحياة الخاصة"، ولا يجوز للسلطات الوصول إليها دون أمر قضائي. وهذه الأحكام تمدّ حمايتها بطبيعة الحال إلى البيانات البيومترية المخزنة في الأجهزة.

ثانياً، **محاكم الاستئناف الفيدرالية**:

في قضية *Patel v. Facebook, Inc.* (2019)، وافقت محكمة الاستئناف بالدائرة التاسعة على دعوى جماعية ضد فيسبوك لاستخدامه تقنية التعرف على الوجه دون موافقة المستخدمين، مؤكدة أن "التعرف على الوجه يُعد معالجة للبيانات البيومترية". وفي قضية *In re: Equifax Inc. Customer Data Security Breach Litigation* (2019)، اعترفت محكمة الاستئناف بالدائرة الحادية عشرة بأن "الإخفاق في حماية البيانات البيومترية يُعد إهمالاً مدنياً"، حتى لو لم يُسفر الاختراق فوراً عن سرقة أموال.

ثالثاً، **محاكم الولايات**:

في قضية *Rosenbach v. Six Flags Entertainment Corp.* (2019)، قضت المحكمة العليا في إلينوي بأن "انتهاك قانون BIPA يُعد ضرراً مدنياً قائماً بذاته"، ولا يشترط وقوع

خسارة مالية فعلية. وقد فتح هذا الحكم الباب أمام آلاف الدعاوى الجماعية ضد الشركات التي تفشل في حماية البيانات البيومترية. وفي قضية *Facebook Biometric Information Privacy Litigation* (2021)، فرضت محكمة مقاطعة كاليفورنيا تعويضات جماعية تجاوزت 650 مليون دولار على فيسبوك لجمع بصمات الوجه دون موافقة صريحة.

رابعاً، **الآليات القضائية المبتكرة**:

تميّزت المحاكم الأمريكية باستخدام آليات مرنة لحماية البيانات البيومترية، منها:

- **الأوامر الزجرية المؤقتة (Preliminary Injunctions)**: لوقف استخدام البيانات البيومترية فوراً.

- **التعويضات الرادعة**: لردع الشركات عن الإهمال المتكرر.

- **الدعاوى الجماعية**: لتمكين الضحايا من المطالبة بحقوقهم بشكل جماعي.

- **الرقابة القضائية على شروط الخدمة**: حيث بدأت بعض المحاكم في اعتبار البنود غير العادلة في اتفاقات المستخدم باطلة.

خامساً، **التحديات القضائية**:

رغم هذا التقدم، تواجه المحاكم الأمريكية تحديات، أبرزها:

- صعوبة تحديد المسؤولية عند تعدد الجهات (مثل مزوّد الخدمة، والمنصة، وطرف ثالث).

- غموض مفهوم "الضرر الفعلي" في حالات التسريب التي لا تؤدي فوراً إلى خسارة مالية.

- تضارب الاختصاص بين المحاكم الفيدرالية ومحاكم الولايات.

وخلاصة القول، فإن القضاء الأمريكي لم ينتظر المشرّع ليحمي البيانات البيومترية، بل سبقه بخطوات، ورسّخ مبادئ قانونية راسخة تجعل من البيانات البيومترية حقاً مدنياً محمياً، لا مجرد بيانات تقنية. وهذا النهج القضائي النشط يُعد درساً مهماً للأنظمة القانونية الأخرى، التي قد تتردد في الاعتراف بالبيانات البيومترية ككيان قانوني مستقل.

الفصل الخامس عشر

النظام القانوني الأوروبي لحماية البيانات البيومترية

يمثّل النظام القانوني الأوروبي نموذجاً رائداً في التنظيم المدني للبيانات البيومترية، إذ يجمع بين الإطار التشريعي الموحّد، والمبادئ الدستورية الراسخة، والاجتهاد القضائي الفعّال. وخلافاً للنظام الأمريكي الذي يعتمد على السوق والتقاضي، يركّز النموذج الأوروبي على الحماية الوقائية الشاملة، ويُعلي من شأن كرامة الإنسان وحقوقه الأساسية كأساس لتنظيم البيانات البيومترية في الفضاء الرقمي. ويُعد توجيه eIDAS (التعريف الإلكتروني والخدمات الموثوقة) الصادر عام 2014، واللائحة العامة لحماية البيانات (GDPR) لعام 2018، الركيزتين الأساسيتين لهذا النظام.

أولاً، **توجيه eIDAS**:

يهدف هذا التوجيه إلى إنشاء إطار موحد للهويات الرقمية عبر دول الاتحاد الأوروبي، وضمان الاعتراف المتبادل بينها. وقد عرّف الهوية الرقمية بأنها "مجموعة من السمات المتعلقة بشخص طبيعي أو اعتباري، تُستخدم لتمثيله في الفضاء الرقمي". ورغم أنه لا يذكر "البيانات البيومترية" صراحةً، إلا أنه يسمح باستخدامها كوسيلة للتحقق من الهوية، شرط أن تكون معتمدة من قبل جهات موثوقة.

ثانياً، **اللائحة العامة لحماية البيانات (GDPR)**:

لم تكتفِ اللائحة بتنظيم البيانات الشخصية، بل ربطت البيانات البيومترية مباشرةً بحقوق الإنسان الأساسية. فالمادة 4(14) عرّفت

البيانات البيومترية بأنها:

> "بيانات شخصية تتعلق بالسمات الفيزيولوجية أو البيولوجية أو السلوكية لشخص طبيعي، والتي تسمح أو تهدف إلى التعرف الفريد على هذا الشخص الطبيعي، مثل صور الوجه أو بصمات الأصابع."

والمادة 9(1) حرّمت معالجة البيانات البيومترية بشكل عام، إلا في حالات استثنائية محددة، مثل:

- موافقة صريحة من صاحب البيانات.

- ضرورة تنفيذ التزام قانوني.

- حماية المصالح الحيوية للفرد.

كما نصّت على حقوق جوهرية تشمل:

- **الحق في الوصول** إلى البيانات البيومترية.

- **الحق في التصحيح** أو الحذف.

- **الحق في نقل البيانات** (Data Portability).

- **الحق في عدم الخضوع لقرارات آلية** تعتمد على التحليل البيومتري.

ثالثاً، **الإطار الدستوري**:

ينبع هذا النظام من مبدأ كرامة الإنسان الوارد في المادة 1 من الميثاق الأوروبي للحقوق

الأساسية، الذي يُعتبر جزءاً لا يتجزأ من القانون الأوروبي. وقد أكدت محكمة العدل الأوروبية مراراً أن "البيانات البيومترية جزء من كرامة الفرد"، ولا يجوز التعامل معها كسلعة تجارية.

رابعاً، **التكامل مع القانون المدني الوطني**:

على عكس النظم الأخرى، طالب توجيه eIDAS الدول الأعضاء بتعديل قوانينها المدنية لتتوافق مع مبادئ الهوية الرقمية. فمثلاً، عدّلت فرنسا وألمانيا وإسبانيا قوانينها المدنية لتنص صراحةً على أن "التوقيع الإلكتروني المؤهل يُنتج ذات الآثار القانونية كالتوقيع اليدوي"، وهو ما يمتد بطبيعة الحال إلى البيانات البيومترية.

خامساً، **الاعتراف المتبادل**:

يُعد هذا من أبرز مزايا النظام الأوروبي، إذ يسمح للمواطن باستعمال هويته البيومترية الوطنية في أي دولة عضو، دون الحاجة إلى هوية جديدة. وهذا يُعزّز حرية التنقل الرقمي، ويُسهّل المعاملات العابرة للحدود.

ومع ذلك، يواجه النظام الأوروبي تحديات، منها:

- بطء بعض الدول في تنفيذ التوجيهات.

- صعوبة تطبيق المعايير الموحّدة في ظل اختلاف البنية التحتية.

- التوتر بين الحماية الصارمة والابتكار الرقمي.

وخلاصة القول، فإن النظام الأوروبي يُقدّم

نموذجاً متكاملاً يدمج بين التشريع، والدستور، والقضاء، لحماية البيانات البيومترية كحق مدني أصيل، لا كأداة تقنية. وهو نموذج يستحق الدراسة والاستلهام، خاصة في ظل السعي العالمي نحو بناء مجتمعات رقمية موثوقة وعادلة.

الفصل السادس عشر

اللائحة العامة لحماية البيانات (GDPR) وتأثيرها على البيانات البيومترية

تُعد اللائحة العامة لحماية البيانات (General Data Protection Regulation – GDPR)، التي دخلت حيز التنفيذ في 25 مايو 2018، من أعمق التشريعات القانونية تأثيراً على مفهوم البيانات البيومترية في العصر الحديث. فهي لم تكتفِ

بتنظيم جمع البيانات ومعالجتها، بل أعادت تعريف العلاقة بين الفرد والبيانات التي تمثّله في الفضاء الرقمي، وجعلت من البيانات البيومترية حقاً أساسياً ينبع من كرامة الإنسان، لا مجرد سلعة قابلة للتداول. ويتجلى تأثير GDPR على البيانات البيومترية في خمسة محاور رئيسية: إعادة التصنيف القانوني للبيانات البيومترية، تقوية حقوق الأفراد، فرض التزامات صارمة على الجهات المعالجة، إنشاء آليات رقابية فعالة، وتوحيد المعايير عبر الحدود.

أولاً، **إعادة التصنيف القانوني للبيانات البيومترية**:

عرّفت المادة 4(14) من GDPR "البيانات البيومترية" بأنها:

> "بيانات شخصية تتعلق بالسمات الفيزيولوجية

أو البيولوجية أو السلوكية لشخص طبيعي، والتي تسمح أو تهدف إلى التعرف الفريد على هذا الشخص الطبيعي، مثل صور الوجه أو بصمات الأصابع."

والمادة 9(1) حرّمت معالجة هذه البيانات بشكل عام، باعتبارها "بيانات خاصة"، ما لم تنطبق إحدى الحالات الاستثنائية المنصوص عليها في الفقرة (2)، مثل:

- الموافقة الصريحة من صاحب البيانات.

- ضرورة تنفيذ التزام قانوني.

- حماية المصالح الحيوية للفرد عندما يكون غير قادر على إعطاء الموافقة.

وهذا التصنيف يحوّل البيانات البيومترية من كيان تقني إلى كيان قانوني محمي، يخضع لضمانات صارمة بمجرد ارتباطه بشخص حقيقي.

ثانياً، **تقوية حقوق أصحاب البيانات البيومترية**:

منحت GDPR أصحاب البيانات البيومترية سلطة غير مسبوقة على بياناتهم، عبر حقوق جوهرية تشمل:

- **الحق في الوصول** (المادة 15): يحق للفرد أن يطلب من أي جهة ما البيانات البيومترية التي تحتفظ بها عنه.

- **الحق في التصحيح** (المادة 16): يحق له تصحيح أي بيانات غير دقيقة.

- **الحق في الحذف** (المادة 17): المعروف بـ"الحق في النسيان"، يتيح طلب حذف البيانات البيومترية في حالات محددة.

- **الحق في نقل البيانات** (المادة 20): يسمح بنقل البيانات البيومترية من منصة إلى أخرى دون عوائق.

- **الحق في الاعتراض على المعالجة الآلية** (المادة 22): يحمي الفرد من القرارات التي تتخذها الخوارزميات دون تدخل بشري.

ثالثاً، **فرض التزامات صارمة على الجهات المعالجة**:

ألزمت GDPR الجهات التي تتعامل مع البيانات البيومترية (سواء كانت حكومية أو خاصة) بعدة التزامات، منها:

- **مبدأ الغرض المحدد** (المادة 5): لا يجوز استخدام البيانات البيومترية لأغراض غير تلك التي جُمعت من أجلها.

- **مبدأ التقليل من البيانات** (Data Minimization): يجب جمع أقل قدر ممكن من البيانات اللازمة.

- **تقييم تأثير حماية البيانات** (DPIA): عند معالجة بيانات بيومترية حساسة، يجب إجراء تقييم مسبق للمخاطر.

- **إشعار الاختراق** (المادة 33): يجب إبلاغ السلطات والمتضررين خلال 72 ساعة من اكتشاف أي اختراق.

رابعاً، **إنشاء آليات رقابية فعالة**:

أنشأت GDPR هيئات رقابية مستقلة في كل دولة عضو (مثل CNIL في فرنسا وICO في المملكة المتحدة)، تتمتع بصلاحيات واسعة تشمل: التحقيق، فرض غرامات تصل إلى 20 مليون يورو أو 4% من الإيرادات العالمية السنوية (أيهما أكبر)، وإصدار أوامر بوقف معالجة البيانات. وقد استخدمت هذه الهيئات سلطاتها بفعالية، كما في قضية غرامة "مايتا" (Meta) البالغة 1.2 مليار يورو في 2023 بسبب نقل بيانات الهوية البيومترية خارج الاتحاد الأوروبي.

خامساً، **التأثير العالمي الموحّد**:

لم يقتصر تأثير GDPR على دول الاتحاد الأوروبي، بل امتد عالمياً. فبموجب مبدأ "الاختصاص العالمي" (المادة 3)، تنطبق اللائحة على أي جهة تقدم خدمات لمواطنين أوروبيين، حتى لو

كانت مقرّها خارج أوروبا. وهذا دفع شركات عالمية مثل Google وApple وAmazon إلى تبني معايير GDPR عالمياً، مما جعلها معياراً فعلياً للبيانات البيومترية في العالم.

وخلاصة القول، فإن GDPR لم يُنظم البيانات البيومترية فحسب، بل أعاد تشكيلها ككيان قانوني مدني يتمتع بكرامة وحقوق. وهو بذلك قدّم نموذجاً تشريعياً شاملاً يمكن أن يستند إليه المشرّعون في العالم العربي وغيره لبناء أنظمة مدنية عادلة وفعالة في العصر الرقمي.

الفصل السابع عشر

أحكام محكمة العدل الأوروبية المتعلقة بالبيانات البيومترية

تُعد محكمة العدل الأوروبية (Court of Justice of the European Union – CJEU) الحارس الأعلى للقانون الأوروبي، ولعبت دوراً محورياً في تشكيل المفهوم القانوني للبيانات البيومترية من خلال سلسلة من الأحكام التاريخية التي ربطت بين التكنولوجيا وحقوق الإنسان. فبينما يضع المشرّع الأوروبي الإطار التشريعي، فإن المحكمة هي التي تفسّره وتطبّقه على الوقائع المعاصرة، مما يجعل اجتهادها مرجعاً أساسياً لفهم طبيعة الحماية المدنية للبيانات البيومترية في الفضاء الأوروبي.

أولاً، **قضية Google Spain SL وGoogle Inc. ضد Agencia Española de Protección de Datos و2014) Mario Costeja González)**:

عرفت بـ"قضية الحق في النسيان"، حيث قضت

المحكمة بأن "نتائج البحث التي تظهر عند كتابة اسم شخص قد تُعتبر جزءاً من هويته الرقمية"، وبالتالي يحق له طلب حذف الروابط التي تضر بسمعته أو تنتهك خصوصيته، حتى لو كانت المعلومات صحيحة. وقد رسّخت هذه القضية مبدأ أن البيانات البيومترية ليست مجرد انعكاس للمعلومات، بل كيان قانوني مستقل يستحق الحماية من التضخيم أو التشهير عبر الخوارزميات.

ثانياً، **قضية Schrems I (2015) وSchrems II (2020)**:

في هاتين القضيتين، نظرت المحكمة في نقل بيانات الهوية البيومترية من الاتحاد الأوروبي إلى الولايات المتحدة. وفي Schrems II، ألغت المحكمة "درع الخصوصية" (Privacy Shield)، مؤكدة أن "نقل البيانات البيومترية إلى دول لا

تضمن مستوى حماية مكافئ لمستوى GDPR يُعد انتهاكاً لكرامة الإنسان". وقد فرض هذا الحكم على الشركات العالمية إعادة تصميم آليات نقل البيانات، وأكّد أن البيانات البيومترية لا يمكن فصلها عن السياق القانوني الذي تنشأ فيه.

ثالثاً، **قضية Rīgas satiksme (2019)**:

تناولت المحكمة حق الفرد في الوصول إلى بياناته الشخصية لدى الجهات العامة. وقضت بأن "الجهات الحكومية ملزمة بتقديم نسخة كاملة من البيانات البيومترية المتعلقة بالهوية الرقمية لأي مواطن يطلبها"، دون تأخير أو تبرير إداري. وهذا الحكم عزّز من شفافية العلاقة بين الدولة والمواطن في الفضاء الرقمي.

رابعاً، **قضية TK ضد Asociația de Proprietari bloc M5A-ScaraA (2022)**:

نظرت المحكمة في استخدام الكاميرات البيومترية في المباني السكنية. وقررت أن "جمع بصمات الوجه أو الصوت دون موافقة صريحة ومستنيرة يُعد معالجة غير مشروعة للبيانات البيومترية"، حتى لو كان الهدف الأمن. وقد أكدت أن الموافقة يجب أن تكون حرة، محددة، وقابلة للسحب في أي وقت.

خامساً، **قضية Österreichische Post (2023)**:

تناولت المحكمة تصنيف الأفراد بناءً على سلوكهم الرقمي (Profiling). وقضت بأن "إسناد خصائص سياسية أو اجتماعية إلى شخص بناءً على تحليل هويته السلوكية يُعد معالجة بيانات

خاصة"، ويستلزم موافقة صريحة. وهذا الحكم وسّع من نطاق مفهوم البيانات البيومترية ليشمل ليس فقط ما نقوله، بل ما "يفترض" عنا.

ومن خلال هذه الأحكام، رسّخت محكمة العدل الأوروبية عدة مبادئ راسخة:

- البيانات البيومترية جزء من كرامة الإنسان، ولا تخضع للمنطق التجاري وحده.

- الحماية لا تقتصر على البيانات الصحيحة، بل تمتد إلى السياق الذي تُستخدم فيه.

- الموافقة ليست شكلاً إدارياً، بل شرط جوهري لشرعية البيانات البيومترية.

- الدولة والشركات على حد سواء مسؤولتان

مدنياً عن حماية البيانات البيومترية.

وخلاصة القول، فإن اجتهاد محكمة العدل الأوروبية لم يكتفِ بتفسير النصوص، بل أعاد تعريف العلاقة بين الفرد والتكنولوجيا، وجعل من البيانات البيومترية حقاً مدنياً دستورياً، لا مجرد أداة تقنية. وهو نموذج قضائي عميق يستحق الدراسة والاستلهام في كل نظام قانوني يسعى إلى بناء مجتمع رقمي عادل وآمن.

الفصل الثامن عشر

المقارنة بين النموذج الأوروبي والنموذج الأمريكي في حماية البيانات البيومترية

يُعدّ التباين بين النموذج الأوروبي والنموذج

الأمريكي في حماية البيانات البيومترية نموذجاً كلاسيكياً لاختلاف الفلسفات القانونية في مواجهة التحديات الرقمية. فبينما يركّز النموذج الأوروبي على الحماية الوقائية الشاملة المنبثقة من كرامة الإنسان وحقوقه الأساسية، يعتمد النموذج الأمريكي على الرقابة اللاحقة عبر السوق والتقاضي، مع تركيز أكبر على الحرية الاقتصادية والابتكار. ويتجلى هذا الاختلاف في خمسة محاور جوهرية: الأساس الفلسفي، الإطار التشريعي، دور القضاء، حقوق الأفراد، وآليات المسؤولية.

أولاً، **الأساس الفلسفي**:

- في أوروبا، تُعتبر البيانات البيومترية جزءاً من الكرامة الإنسانية، كما ورد في الميثاق الأوروبي للحقوق الأساسية. وبالتالي، فإن حمايتها واجب قانوني وأخلاقي لا يخضع للتفاوض التجاري.

- في أمريكا، تُنظر إلى البيانات البيومترية أساساً كأداة اقتصادية، وتخضع لمنطق السوق والمنافسة. فالحماية تُقدّم كوسيلة لتعزيز الثقة في الاقتصاد الرقمي، لا كحق أصيل.

ثانياً، **الإطار التشريعي**:

- في أوروبا، يوجد تشريع موحّد (GDPR وeIDAS) يفرض معايير صارمة على جميع الجهات، بغض النظر عن القطاع أو الحجم.

- في أمريكا، لا يوجد قانون اتحادي شامل، بل تشريعات متفرقة على مستوى الولايات (مثل BIPA في إلينوي)، مما يؤدي إلى تفاوت كبير في مستويات الحماية.

ثالثاً، **دور القضاء**:

- في أوروبا، يلعب القضاء دوراً تفسيرياً وتوجيهياً، لكنه يعمل ضمن إطار تشريعي واضح ومسبق.

- في أمريكا، يلعب القضاء دوراً تأسيساً وابتكارياً، حيث يخلق المبادئ القانونية عبر الأحكام (كما في قضيتي Rosenbach وPatel)، نظراً لغياب التشريع الشامل.

رابعاً، **حقوق الأفراد**:

- في أوروبا، تشمل الحقوق الحق في النسيان، نقل البيانات، وعدم الخضوع للقرارات الآلية، وهي حقوق استباقية تُفعّل دون الحاجة إلى وقوع ضرر.

- في أمريكا، تتركز الحقوق حول الشفافية والإشعار، ولا يمكن المطالبة بالتعويض إلا بعد وقوع ضرر فعلي ملموس.

خامساً، **آليات المسؤولية**:

- في أوروبا، تُفرض غرامات إدارية وقائية تصل إلى مليارات اليورو، حتى لو لم يُصب الفرد بضرر مباشر.

- في أمريكا، تعتمد المسؤولية على الدعوى المدنية الفردية أو الجماعية، وتتطلب إثبات الضرر الفعلي، وهو ما يصعب في كثير من حالات اختراق البيانات البيومترية.

ومع ذلك، هناك نقاط تقاطع:

- كلا النموذجين يعترفان بأن البيانات البيومترية ليست مجرد بيانات تقنية.

- كلاهما يمنح المحاكم سلطة إصدار أوامر قضائية لوقف الانتهاكات.

- كلاهما بدأ يعترف بأهمية البيانات البيومترية كعنصر حساس في الهوية الرقمية.

وخلاصة القول، فإن النموذج الأوروبي يقدّم حماية أقوى للأفراد، لكنه قد يُبطئ الابتكار. أما النموذج الأمريكي، فهو أكثر مرونة، لكنه يترك الأفراد عرضة للانتهاكات دون ضمانات كافية. ولذلك، فإن النظام القانوني الأمثل قد يكون ذلك الذي يجمع بين الوضوح التشريعي الأوروبي والمرونة القضائية الأمريكية، ليوازن بين حماية الحقوق وتمكين التقدم الرقمي.

الفصل التاسع عشر

التحديات المدنية الناشئة عن استخدام البيانات البيومترية عبر الحدود

مع تزايد العولمة الرقمية، لم تعد البيانات البيومترية محصورة داخل الحدود الوطنية، بل باتت تُستخدم يومياً في معاملات عابرة للقارات: من شراء سلع إلكترونية، إلى فتح حسابات مصرفية، إلى التعاقد مع شركات أجنبية. ورغم الفوائد الكبيرة لهذا التدفق الحر، فإن استخدام البيانات البيومترية عبر الحدود يطرح تحديات مدنية معقدة، تتعلق بالاختصاص القضائي، الاعتراف المتبادل، التعارض بين القوانين، وحماية الحقوق في غياب إطار قانوني دولي موحد.

أولاً، **مشكلة الاختصاص القضائي**:

عند حدوث نزاع — كانتحال بيانات بيومترية أو اختراقها — يصعب تحديد المحكمة المختصة. فهل هي محكمة دولة إقامة الضحية؟ أم دولة مقر الشركة التي تدير المنصة؟ أم دولة الخادم (Server) الذي تم منه الاختراق؟ وقد أدى هذا الغموض إلى تضارب في الأحكام، وصعوبة في تنفيذ القرارات القضائية. فمثلاً، قضت محكمة فرنسية في قضية ضد شركة أمريكية بأنها مختصة لأن الضحية فرنسي، بينما رفضت محكمة أمريكية الاعتراف بالحكم لعدم وجود "ارتباط جوهري" بالولايات المتحدة.

ثانياً، **غياب الاعتراف المتبادل بالبيانات البيومترية**:

بينما يضمن توجيه eIDAS الاعتراف المتبادل داخل الاتحاد الأوروبي، لا يوجد اتفاق مماثل على المستوى العالمي. فبيانات بيومترية صادرة في مصر أو الجزائر أو حتى الولايات المتحدة لا تُعترف بها تلقائياً في دول أخرى، مما يعيق المعاملات القانونية العابرة للحدود. وقد دفع هذا بعض الدول إلى اعتماد أنظمة "ثنائية" مؤقتة، لكنها غير كافية للاقتصاد الرقمي العالمي.

ثالثاً، **تعارض القوانين الوطنية**:

قد تُعتبر معالجة معينة للبيانات البيومترية مشروعة في دولة ما، وغير قانونية في أخرى. فمثلاً، يسمح القانون الأمريكي لشركات مثل Facebook بجمع البيانات البيومترية دون موافقة صريحة، بينما يجرّم GDPR ذلك. وعندما تتعامل شركة أمريكية مع مواطن أوروبي، يصبح من الصعب تحديد أي قانون يُطبّق، خاصة بعد إلغاء

"درع الخصوصية" في قضية Schrems II.

رابعاً، **المسؤولية المدنية في السلاسل المعقدة**:

في البيئة الرقمية، تمر البيانات البيومترية عبر سلسلة من الجهات: مزوّد الخدمة، منصة الدفع، خادم التخزين، جهة التحقق. وعند حدوث ضرر، يصعب تحديد الجهة المسؤولة مدنياً. فهل تتحمل الشركة الأم المسؤولية عن ثغرة في نظام تابع لطرف ثالث؟ المحاكم الأوروبية تميل إلى توسيع دائرة المسؤولية، بينما الأمريكية تطلب إثبات علاقة مباشرة بين الخطأ والضرر.

خامساً، **حماية الضعفاء في العلاقات الدولية**:

المواطن العادي، عند تعامله مع منصة عالمية، يكون طرفاً ضعيفاً في علاقة غير متكافئة. وغالباً ما تفرض عليه شروط خدمة (Terms of Service) تحد من حقوقه، وتُلزم بحل النزاعات في محاكم بعيدة. وقد بدأت بعض المحاكم الأوروبية في اعتبار هذه البنود باطلة إذا كانت مجحفة، لكن هذا لا يزال استثناءً وليس قاعدة.

سادساً، **الإثبات المدني عبر الحدود**:

كيف يُثبت مواطن مصري أن بياناته البيومترية انتحلت في منصة أمريكية؟ وكيف تُعتمد الوثائق الإلكترونية أمام محكمة أجنبية؟ إن غياب اتفاقيات دولية حول الإثبات الإلكتروني يُعقّد من سبل الانتصاف المدني.

ولمعالجة هذه التحديات، يُقترح:

- تبني اتفاقية دولية نموذجية حول البيانات البيومترية، تحت إشراف الأمم المتحدة أو اليونيدروا.

- إنشاء آليات تسوية نزاعات رقمية دولية (ODR) متخصصة.

- تشجيع الدول على الاعتراف المتبادل بالبيانات البيومترية المؤهلة.

- توحيد مبادئ المسؤولية المدنية عبر الحدود في حالات البيانات البيومترية.

إن بناء فضاء رقمي عالمي عادل يتطلب أكثر من مجرد تقنيات متطورة؛ فهو يحتاج إلى إطار قانوني مدني دولي يحمي البيانات البيومترية

كحق إنساني، أينما كان صاحبها وأينما تم استخدامها.

الفصل العشرون

الجرائم الإلكترونية وانعكاساتها على المسؤولية المدنية للبيانات البيومترية

رغم أن الجرائم الإلكترونية تُصنّف ضمن القانون الجنائي، فإن آثارها تمتد بعمق إلى نطاق القانون المدني، حيث تُولّد التزامات تعويضية، وتُعيد تشكيل مفاهيم المسؤولية، وتُفرض على الأفراد والمؤسسات التزامات وقائية جديدة. فانتحال البيانات البيومترية، والتصيد الاحتيالي (Phishing)، وبرامج الفدية (Ransomware)، ليست مجرد أفعال مجرمة، بل هي أحداث مدنية تُلحق أضراراً مادية ومعنوية تستوجب

التعويض، وتكشف عن ثغرات في الحماية تستدعي إعادة النظر في التزامات الجهات المعنية.

أولاً، **انتحال البيانات البيومترية (Biometric Identity Theft)**:

يُعدّ انتحال البيانات البيومترية من أكثر الجرائم انتشاراً، ويتم عبر سرقة بيانات شخصية (كصور الوجه أو بصمات الأصابع) لاستخدامها في إبرام عقود أو سحب أموال. ومن الناحية المدنية، يُنظر إلى هذا الفعل كـ**تدليس** يؤدي إلى بطلان العقد إذا كان الطرف الآخر حسن النية. كما يُحق للمتضرر رفع دعوى مسؤولية تقصيرية ضد الجاني، بل وحتى ضد الجهة التي فشلت في حماية بياناته (كالبنك أو المنصة)، إذا ثبت إهمالها.

ثانياً، **التصيد الاحتيالي (Phishing)**:

عندما يخدع المجرم الضحية لإدخال بياناته البيومترية في موقع مزيف، فإن العقد الناتج يكون باطلاً لعيب في الرضا. لكن التحدي المدني يكمن في تحديد ما إذا كانت الجهة التي استضافت الموقع المزيف — أو حتى مزوّد خدمة الإنترنت — تتحمل جزءاً من المسؤولية. وقد بدأت بعض المحاكم الأوروبية في تحميل مزوّدي الخدمات مسؤولية تضامنية إذا لم يتخذوا إجراءات معقولة لمنع الاستضافة الاحتيالية.

ثالثاً، **برامج الفدية (Ransomware)**:

عندما يتم تشفير بيانات الهوية البيومترية وطلب فدية لإعادتها، فإن الضرر لا يقتصر على فقدان

الوصول، بل يمتد إلى فقدان السمعة، وتعطيل الأعمال، وربما تسريب البيانات. وهنا، يحق للمتضرر المطالبة بالتعويض عن جميع هذه الأضرار، شرط إثبات العلاقة السببية. كما أن فشل المؤسسة في تطبيق تحديثات أمنية أساسية قد يُعتبر إهمالاً مدنياً، حتى لو لم يكن هناك تشريع صريح يفرض ذلك.

رابعاً، **المسؤولية المدنية للجهات الثالثة**:

لم يعد يكفي تحميل الجاني المسؤولية؛ فالقانون المدني الحديث بدأ يوسع دائرة المسؤولية لتشمل:

- **البنوك**: إذا فشلت في اكتشاف عمليات سحب غير طبيعية باستخدام بيانات بيومترية مسروقة.

- **منصات التواصل**: إذا سمحت بنشر أدوات اختراق أو بيانات بيومترية مسروقة.

- **مطوّري البرمجيات**: إذا احتوت برامجهم على ثغرات أمنية معروفة ولم تُصلح.

خامساً، **التعويض في غياب الضرر المالي المباشر**:

في كثير من حالات الجرائم الإلكترونية، لا يُصاب الضحية بخسارة مالية فورية، لكنه يعاني من قلق دائم، وفقدان الثقة، وخطر مستقبلي. وقد بدأت المحاكم الأوروبية في الاعتراف بالـ**ضرر المعنوي** كأساس للتعويض، حتى في غياب ضرر مادي. بينما لا تزال المحاكم الأمريكية تطلب "ضرراً فعلياً" ملموساً، مما يحد من الحماية.

سادساً، **الالتزام الوقائي**:

أصبح من المقبول قانونياً أن يُفرض على الجهات التزام "بحماية معقولة" (Reasonable Security Measures). فإذا ثبت أن جهة ما استخدمت تقنيات أمنية قديمة (كأنظمة التعرف على الوجه غير المشفرة)، فإنها تكون مسؤولة مدنياً حتى لو لم تكن هناك نية إجرامية من جانبها.

وخلاصة القول، فإن الجرائم الإلكترونية لم تعد مجرد تهديد أمني، بل أصبحت مصدراً رئيسياً للمسؤولية المدنية. ولذلك، فإن الحماية الفعالة للبيانات البيومترية تتطلب أكثر من عقوبات جنائية؛ فهي تحتاج إلى نظام مدني يُعزّز الوقاية، ويُسهّل التعويض، ويُوازن بين حماية الضحية وتشجيع الابتكار الأمني.

الفصل الحادي والعشرون

التعاقد الإلكتروني والبيانات البيومترية

يُعد التعاقد الإلكتروني أحد أهم مجالات تطبيق البيانات البيومترية، إذ يعتمد صحة العقد ونفاذه على قدرة الأطراف على التحقق من هوياتهم بشكل موثوق في الفضاء الرقمي. ومع تحوّل الاقتصاد العالمي نحو المعاملات غير الورقية، أصبحت البيانات البيومترية الركيزة الأساسية لضمان رضا الأطراف، وصحة الإرادة، وقابلية العقد للتنفيذ. ويثير هذا التفاعل بين التعاقد الإلكتروني والبيانات البيومترية تساؤلات قانونية عميقة تتعلق بالإثبات، والغلط، والتدليس، والمسؤولية، تتطلب إعادة تفسير قواعد القانون المدني التقليدية في سياق رقمي جديد.

أولاً، **شرط الرضا في العقد الإلكتروني**:

في القانون المدني التقليدي، يُشترط أن يكون الرضا "حراً، صحيحاً، ومستنيراً". وفي البيئة الرقمية، تُحقّق البيانات البيومترية هذا الشرط عبر:

- **التوثيق البيومتري الثنائي** (Two-factor Biometric Authentication): لضمان أن من أبرم العقد هو صاحب الهوية فعلاً.

- **التوقيع البيومتري المؤهل**: الذي يُثبت هوية المُوقّع ويمنع إنكاره لاحقاً.

- **سجلات التفاعل**: التي تُوثّق خطوات إبرام العقد، وتُظهر أن الطرف كان واعياً بما يوافق عليه.

فإذا تم اختراق البيانات البيومترية واستخدامها دون علم صاحبها، فإن العقد يكون باطلاً لانعدام الرضا، ما لم يثبت الطرف الآخر حسن نيته.

ثانياً، **الغلط والتدليس الإلكتروني**:

قد يقع الشخص ضحية غلط إذا ظن أنه يتعامل مع جهة موثوقة بينما هو يتعامل مع موقع احتيالي يستخدم تقنيات التزييف العميق (Deepfake) لتقليد بصمة الوجه أو الصوت. وهنا، يُطبّق القانون المدني مبدأ الغلط (المادة 124 من القانون المدني المصري، المادة 108 من القانون المدني الجزائري)، ويكون العقد قابلاً للإبطال. أما في حالات التدليس — كاستخدام بيانات بيومترية مزورة لإقناع الطرف الآخر — فإن العقد يكون باطلاً بطلاناً مطلقاً، لأن التدليس يُشوّه الإرادة جوهرياً.

ثالثاً، **الإثبات في العقود الإلكترونية**:

كفلت التشريعات الحديثة (كـ eIDAS وE-SIGN Act) أن تكون السجلات الإلكترونية والتوقيعات البيومترية ذات حجية إثبات مساوية للوثائق الورقية. غير أن القاضي يظل مطالباً بالتحقق من:

- صحة البيانات البيومترية المستخدمة.

- سلامة السجلات من التلاعب.

- توافق الإجراءات مع المعايير الأمنية المعتمدة.

وفي حال الشك، يُمكن اللجوء إلى خبراء تقنيين لفحص أثر البيانات البيومترية (Biometric Digital

.(Footprint

رابعاً، **العقود الذكية (Smart Contracts)**:

مع ظهور العقود الذكية القائمة على تقنية البلوك تشين، برز تحدي جديد: هل يُعتبر تنفيذ العقد الآلي كافياً لصحة الرضا؟ الجواب القانوني الحديث هو أن البيانات البيومترية تسبق العقد الذكي؛ فلا يُعتد بالعقد إلا إذا كان مرتبطاً ببيانات بيومترية معتمدة، تُثبت أن من أنشأ العقد هو صاحب الإرادة القانونية.

خامساً، **المسؤولية في حالات الفشل التعاقدية**:

إذا فشل العقد الإلكتروني بسبب خلل في نظام التحقق البيومتري (كتعطيل خاصية التعرف على

الوجه)، فقد تتحمل الجهة المُصدرة للبيانات البيومترية مسؤولية تقصيرية، خاصة إذا كان الخلل ناتجاً عن إهمال. كما أن المنصات التي تفرض أنظمة بيومترية معقدة دون توفير بدائل قد تُعتبر مسؤولة عن تعطيل حق الأفراد في التعاقد.

سادساً، **التحديات العابرة للحدود**:

عندما يبرم عقد بين طرف عربي وطرف أوروبي باستخدام بيانات بيومترية مختلفة، يبرز سؤال: أي بيانات تُعتبر كافية لإثبات الرضا؟ هنا، يصبح الاعتراف المتبادل بين أنظمة البيانات البيومترية (كما في eIDAS) ضرورة قانونية، لا خياراً تقنياً.

وخلاصة القول، فإن البيانات البيومترية ليست مجرد أداة تقنية في التعاقد الإلكتروني، بل هي

الضامن المدني لصحة العقد ونفاذه. ولذلك، فإن أي نظام قانوني حديث يجب أن يدمج قواعد البيانات البيومترية ضمن أحكامه المتعلقة بالعقود، ليضمن أن التحول الرقمي لا يأتي على حساب مبادئ القانون المدني الأساسية: الإرادة، الثقة، والعدالة.

الفصل الثاني والعشرون

الإثبات المدني للبيانات البيومترية في المعاملات القضائية

في ظل التحوّل المتسارع نحو الرقمنة، لم يعد الإثبات في المعاملات القضائية يقتصر على الوثائق الورقية والشهادات الشفهية، بل بات يعتمد بشكل متزايد على البيانات البيومترية كوسيلة لإثبات صحة الوقائع، وربط الأفعال

بالأفراد، وضمان مصداقية الإجراءات. غير أن قبول البيانات البيومترية كوسيلة إثبات مدنية يتطلب توافر شروط صارمة تتعلق بالصحة، السلامة، والقابلية للتحقق، لضمان ألا تُستخدم كأداة للتلاعب أو الإنكار. ويهدف هذا الفصل إلى تحليل الشروط القانونية التي يجب أن تستوفيها البيانات البيومترية لتكون حجة أمام القضاء، والتحديات التي تواجهها في البيئة القضائية.

أولاً، **شروط قبول البيانات البيومترية كحجة إثبات**:

لكي تُعتبر البيانات البيومترية وسيلة إثبات مقبولة، يجب أن تستوفي ثلاثة شروط أساسية:

1. **الصحة (Authenticity)**: أن تكون مرتبطة بشخص حقيقي، عبر ربطها بهوية وطنية أو

وثيقة رسمية معتمدة.

2. **السلامة (Integrity)**: أن تكون خالية من التغيير أو التزوير منذ لحظة إنشائها وحتى تقديمها كدليل.

3. **القابلية للتحقق (Verifiability)**: أن يكون بالإمكان التحقق منها عبر جهة موثوقة أو نظام تقني معتمد.

وقد نصّت اتفاقية الأمم المتحدة بشأن استخدام الخطابات الإلكترونية في العقود التجارية (2005) على أن "السجلات الإلكترونية تُعتبر مقبولة كأدلة ما لم يثبت عكس ذلك"، وهو مبدأ تم تبنيه في تشريعات عديدة، بما فيها توجيه eIDAS الأوروبي وقانون E-SIGN الأمريكي.

ثانياً، **مستويات الإثبات حسب نوع البيانات البيومترية**:

- **البيانات البيومترية المؤهلة** (Qualified Biometric Data): مثل تلك الصادرة وفق معايير eIDAS، تُعتبر حجة قاطعة (Presumption of Authenticity)، ولا يُطلب من القاضي التحقق منها إلا إذا طعن أحد الأطراف.

- **البيانات البيومترية العادية**: مثل بصمات الوجه المخزنة على منصات التواصل، تُعتبر قرينة بسيطة، ويمكن دحضها بإثبات الانتحال أو الاختراق.

- **البيانات السلوكية البيومترية**: مثل نمط الكتابة أو نبرة الصوت، تُستخدم كدليل ظرفي، ولا تكفي وحدها لإثبات الهوية دون أدلة مساندة.

ثالثاً، **إجراءات التحقق القضائي**:

عند تقديم البيانات البيومترية كدليل، يحق للقاضي:

- طلب تقرير فني من جهة محايدة حول سلامة السجلات.

- الاستعانة بخبير تقني لفحص أثر البيانات البيومترية (Biometric Digital Footprint).

- استدعاء الجهة المصدرة للبيانات (كالبنك أو مركز المعلومات الوطني) للإدلاء بشهادة حول صحتها.

وفي بعض الأنظمة، كالنظام الفرنسي، يُمكن

للقضاء أن يطلب "ختم زمني مؤهل" (Qualified Time Stamp) لإثبات تاريخ إنشاء البيانات البيومترية.

رابعاً، **التحديات العملية في الإثبات**:

- **الإنكار بعد الإبرام**: قد يدّعي شخص أن بياناته البيومترية انتحلت، مما يضع عبء الإثبات على الطرف الآخر.

- **تعدد المصادر**: فقد يمتلك الشخص أكثر من مجموعة بيانات بيومترية (كالبصمة على الهاتف والوجه على الحاسوب)، مما يعقّد من عملية ربط الفعل بالهوية الصحيحة.

- **البيانات المشتتة**: فغالباً ما تكون عناصر الهوية البيومترية موزعة على جهات مختلفة (بريد إلكتروني، رقم هاتف، حساب بنكي)، ما

يستلزم تجميعها لإثبات الهوية الكاملة.

خامساً، **الاعتراف القضائي العابر للحدود**:

في القضايا الدولية، يبرز سؤال: هل تقبل محكمة في دولة عربية بيانات بيومترية صادرة في أوروبا؟ الجواب يعتمد على وجود اتفاقيات ثنائية أو انضمام الدول إلى اتفاقيات دولية مثل اتفاقية اليونيدروا بشأن الإثبات الإلكتروني. وفي غياب ذلك، يعود الأمر لاجتهاد القاضي، الذي قد يطلب ترجمة معتمدة أو تصديق قنصلي.

سادساً، **البيانات البيومترية كوسيلة لإثبات النية الجنائية أو المدنية**:

لم يعد دور البيانات البيومترية مقتصراً على إثبات "من فعل"، بل يمتد إلى إثبات "نية الفعل".

فمثلاً ً، يمكن لسجلات الدخول المتكرر إلى حساب ضحية أن تُستخدم كدليل على النية الاحتيالية في دعوى مدنية عن انتحال الهوية البيومترية.

وخلاصة القول، فإن البيانات البيومترية أصبحت وسيلة إثبات مدنية لا غنى عنها، لكن قبولها أمام القضاء يتطلب إطاراً ً قانونياً ً دقيقاً ً يوازن بين تسهيل الإثبات وضمان العدالة. ولذلك، فإن تطوير قواعد الإثبات المدني لتشمل معايير واضحة للبيانات البيومترية هو خطوة ضرورية لبناء نظام قضائي عادل في العصر الرقمي.

الفصل الثالث والعشرون

دور الجهات الموثوقة في جمع ومعالجة البيانات البيومترية

تُعد الجهات الموثوقة (Trusted Service Providers) الركيزة الأساسية في نظام البيانات البيومترية، إذ تضطلع بمسؤولية حساسة تتمثل في ربط الكيان الرقمي بالشخص الحقيقي، وضمان صحة البيانات، وتمكين الثقة في المعاملات الإلكترونية. ونظراً لما تحمله هذه المهمة من أثر قانوني مباشر على الحقوق المدنية للأفراد، فإن تنظيم عمل هذه الجهات لا يقتصر على المعايير التقنية، بل يمتد إلى التزامات مدنية صارمة تتعلق بالشفافية، الأمان، والمسؤولية عن الأضرار. ويهدف هذا الفصل إلى تحليل طبيعة دور هذه الجهات، ونطاق مسؤولياتها، والآليات التي تضمن أدائها لأمانة جمع ومعالجة البيانات البيومترية.

أولاً، **تعريف الجهة الموثوقة**:

هي كيان قانوني — حكومي أو خاص — معتمد من قبل سلطة وطنية أو دولية لجمع ومعالجة البيانات البيومترية. وتشمل هذه الجهات:

- مراكز المعلومات الوطنية (كالمركز المصري).

- شركات الاتصالات المرخصة.

- البنوك الكبرى.

- جهات التصديق الرقمي (Certification Authorities).

ويشترط للاعتماد أن تمتلك بنية تحتية أمنية معتمدة، وتخضع لرقابة دورية، وتلتزم بمعايير دولية مثل ISO/IEC 30107 الخاصة بالأنظمة البيومترية.

ثانياً، **الوظائف الأساسية للجهة الموثوقة**:

1. **التحقق من الهوية الحقيقية**: عبر مطابقة البيانات البيومترية مع وثائق رسمية (كالبطاقة الوطنية أو جواز السفر).

2. **جمع البيانات البيومترية**: التي تربط الهوية الرقمية بالشخص الحقيقي، وتحتوي على مفتاح تشفير فريد.

3. **الحفاظ على سلامة السجلات**: عبر تخزين البيانات في بيئات آمنة، ومنع الوصول غير المصرح به.

4. **إتاحة وسائل الطعن والتصحيح**: لتمكين الأفراد من تحديث بياناتهم أو الاعتراض على

أخطاء الجمع.

ثالثاً، **الالتزامات المدنية للجهة الموثوقة**:

بمجرد اعتمادها، تتحمل الجهة الموثوقة التزامات مدنية تجاه صاحب البيانات، أهمها:

- **واجب العناية (Duty of Care)**: باتخاذ جميع التدابير الأمنية المعقولة لحماية البيانات البيومترية.

- **واجب الشفافية**: بإبلاغ المستخدم بكيفية استخدام بياناته، ومن يشاركها معه.

- **واجب التصحيح**: بتعديل أو حذف البيانات فوراً عند طلب صاحبها أو عند اكتشاف خطأ.

- **واجب الإشعار**: بإبلاغ المتضرر فور

اكتشاف أي اختراق قد يؤثر على بياناته.

رابعاً، **المسؤولية المدنية في حال الإخلال**:

إذا جمعت جهة موثوقة بيانات بيومترية خاطئة، أو فشلت في حمايتها، فإنها تكون مسؤولة مدنياً عن الأضرار الناتجة، حتى لو لم يكن هناك خطأ جسيم. وقد أكدت محكمة العدل الأوروبية في عدة أحكام أن "الاعتماد الرسمي يُولّد توقعاً مشروعاً بالثقة"، وبالتالي فإن الإخلال بهذا التوقع يُعد أساساً للمسؤولية التقصيرية.

خامساً، **الإعفاء من المسؤولية**:

لا يجوز للجهة الموثوقة أن تُبرئ نفسها من المسؤولية عبر شروط عقدية، خاصة إذا كانت

الجهة حكومية أو شبه حكومية. كما أن القوة القاهرة (كالهجمات السيبرانية الاستثنائية) قد تُخفف من المسؤولية، لكنها لا تلغيها إذا ثبت أن الجهة لم تتبع أفضل الممارسات الأمنية.

سادساً، **الرقابة على الجهات الموثوقة**:

لضمان أدائها، تُنشأ هيئات وطنية مستقلة (كالهيئة الوطنية للبريد الإلكتروني في تونس، أو الهيئة السعودية للبيانات)، تتمتع بصلاحيات:

- سحب الاعتماد في حال التكرار في الأخطاء.

- فرض غرامات مالية.

- إلزام الجهة بتعويض المتضررين.

وفي الاتحاد الأوروبي، يُدرج اسم كل جهة موثوقة في "القائمة الموثوقة الأوروبية" (EU Trusted List)، مما يمنح بياناتها قوة قانونية عبر الحدود.

وخلاصة القول، فإن الجهة الموثوقة ليست مجرد وسيط تقني، بل هي ضامن مدني لصحة البيانات البيومترية. ولذلك، فإن تنظيم عملها بوضوح، وفرض التزامات مدنية صارمة عليها، هو شرط أساسي لبناء ثقة حقيقية في الفضاء الرقمي، وضمان أن البيانات البيومترية تُستخدم كأداة لحماية الحقوق، لا كوسيلة لانتهاكها.

الفصل الرابع والعشرون

المسؤولية المدنية لمزوّدي أنظمة التعرف البيومتري

مع تزايد الاعتماد على البيانات البيومترية في المعاملات اليومية، برزت فئة جديدة من الفاعلين القانونيين: مزوّدو أنظمة التعرف البيومتري (Biometric Recognition System Providers). وهم كيانات — حكومية أو خاصة — تُوفّر البنية التحتية والخدمات اللازمة لجمع، معالجة، والتحقق من البيانات البيومترية. ونظراً للدور الحاسم الذي يلعبونه في ربط الأفراد بالفضاء الرقمي، فإن إخلالهم بأي التزام قد يؤدي إلى أضرار جسيمة، مما يستدعي تحديد نطاق مسؤوليتهم المدنية بدقة، وضمان آليات فعالة لتعويض المتضررين.

أولاً، **طبيعة العلاقة القانونية**:

تربط مزوّد النظام بالمستخدم علاقة قانونية

مزدوجة:

- **علاقة تعاقدية**: عبر شروط الخدمة التي يوافق عليها المستخدم.

- **علاقة تقصيرية**: ناشئة عن واجب عام بحماية البيانات، حتى لو لم يكن هناك عقد صريح.

وهذا التلازم يوسع من أساس المسؤولية، إذ يمكن للمتضرر أن يختار الطريق الأنسب لطلب التعويض.

ثانياً، **مصادر الالتزام المدني**:

ينبع التزام مزوّد النظام من ثلاثة مصادر رئيسية:

1. **التشريع**: كقانون حماية البيانات الشخصية، أو قوانين الجرائم الإلكترونية، التي تفرض التزامات وقائية.

2. **العقد**: عبر شروط الخدمة التي تحدد مستوى الأمان المطلوب.

3. **المبادئ العامة للقانون المدني**: كمبدأ عدم الإضرار بالغير، وواجب العناية.

ثالثاً، **حالات الإخلال الشائعة**:

- **إهمال أمني**: كاستخدام بروتوكولات تشفير قديمة، أو عدم تحديث الأنظمة.

- **إفشاء البيانات**: عبر تسريبها بسبب ثغرة أو بيعها لجهات ثالثة دون موافقة.

- **تأخير التصحيح**: بعد إبلاغ المستخدم بوجود خطأ في بياناته البيومترية.

- **رفض الحذف**: عند طلب المستخدم سحب بياناته البيومترية.

رابعاً، **شروط قيام المسؤولية**:

لقيام المسؤولية المدنية، يجب توافر:

- **فعل ضار**: كاختراق النظام أو فقدان البيانات.

- **خطأ**: يتمثل في الإخلال بواجب العناية.

- **ضرر**: مادي (كخسارة مالية) أو معنوي (كالقلق أو فقدان السمعة).

- **علاقة سببية**: بين الخطأ والضرر.

خامساً، **حدود المسؤولية**:

- **في الأنظمة الأوروبية**: تُفرض مسؤولية موضوعية في كثير من الحالات، حيث يكفي وقوع الضرر لإثبات المسؤولية، ما لم يثبت المزوّد أنه اتخذ جميع التدابير المعقولة.

- **في الأنظمة الأمريكية**: تتطلب المحاكم إثبات "الإهمال" بشكل صريح، وهو ما يصعب في حالات الهجمات السيبرانية المعقدة.

- **في الأنظمة العربية**: لا تزال القوانين غامضة، وغالباً ما تُحمّل الضحية عبء الإثبات الكامل، دون افتراض أي مسؤولية على المزوّد.

سادساً، **آليات التعويض**:

- **التعويض الفردي**: عبر دعاوى مدنية مباشرة.

- **التعويض الجماعي**: في حالات الاختراق الواسع (كما في قضية Equifax).

- **صناديق التعويض**: التي بدأت بعض الدول (كفرنسا) في إنشائها لتعويض الضحايا حتى قبل صدور حكم قضائي.

سابعاً، **التحديات الحديثة**:

- **الاعتماد على طرف ثالث**: إذا استعان المزوّد بشركة خارجية لإدارة السيرفرات، فمن يتحمل المسؤولية؟

- **الذكاء الاصطناعي**: إذا استخدم المزوّد خوارزميات لتحليل البيانات البيومترية، ومن ثم ارتكب خطأ، هل يُعتبر ذلك خطأ بشريًا أم تقنيًا؟

وخلاصة القول، فإن مزوّدي أنظمة التعرف البيومتري يتحملون مسؤولية مدنية جسيمة، لأنهم يديرون بوابة الدخول إلى الحياة الرقمية. ولذلك، فإن التشريعات الحديثة يجب أن تفرض عليهم التزامات وقائية واضحة، وتُسهّل على المتضررين سبل الانتصاف، لضمان أن الثقة في البيانات البيومترية لا تتحول إلى مصدر للخطر.

الفصل الخامس والعشرون

التعويض المدني عن الضرر الناتج عن سرقة أو

انتحال البيانات البيومترية

يُعد التعويض المدني الركن الأساسي في حماية الأفراد من آثار سرقة أو انتحال البيانات البيومترية، إذ لا يكفي تجريم الفعل أو معاقبة الجاني، بل يجب جبر الضرر الذي لحق بالضحية، سواء كان مادياً أو معنوياً. ومع تزايد تعقيد الهجمات الرقمية، برزت تحديات جديدة في تحديد نطاق الضرر، وربطه بالفعل الضار، وتحديد الجهة المسؤولة. ويهدف هذا الفصل إلى تحليل أسس التعويض المدني في حالات انتحال البيانات البيومترية، وآلياته، والاختلافات بين الأنظمة القانونية في معالجته.

أولاً، **طبيعة الضرر الناتج**:

يمكن تصنيف الضرر إلى نوعين رئيسيين:

1. **الضرر المادي**:

- خسائر مالية مباشرة (كالسحب غير المصرح به من الحساب البنكي باستخدام بصمة مسروقة).

- تكاليف استعادة الهوية (كأتعاب المحاماة، ورسوم التبليغ، وتكاليف التحقق الجديدة).

- فقدان فرص اقتصادية (كإلغاء عقد بسبب تشويه السمعة الرقمية).

2. **الضرر المعنوي**:

- القلق النفسي الناتج عن فقدان السيطرة على الهوية البيومترية.

- فقدان الثقة في المنصات الرقمية.

- الإحراج الاجتماعي أو المهني الناتج عن استخدام الهوية البيومترية في أنشطة غير قانونية أو مخجلة.

ثانياً، **أساس المسؤولية المدنية**:

لا يشترط أن يكون الجاني هو الوحيد المسؤول. فقد تتحمل المسؤولية:

- **الجاني المباشر**: كمن سرق البيانات البيومترية واستخدمها.

- **الجهة المُصدرة للبيانات**: إذا ثبت إهمالها في الحماية.

- **المنصة التي تم عليها الانتحال**: إذا

فشلت في اكتشاف السلوك غير الطبيعي.

ويقوم التعويض على أحد الأساسين:

- **المسؤولية التقصيرية**: عند وجود خطأ وإخلال بواجب العناية.

- **المسؤولية التعاقدية**: إذا كان هناك عقد يفرض التزامات أمنية (كعقد البنك مع العميل).

ثالثاً، **شروط قيام الحق في التعويض**:

- **وجود ضرر فعلي**: لا يكفي الخوف أو الاحتمال، بل يجب أن يكون الضرر قد وقع فعلاً.

- **علاقة سببية**: بين انتحال البيانات البيومترية والضرر.

- **خطأ أو إخلال**: من الجهة المسؤولة.

وفي بعض الأنظمة (كالأوروبية)، يُفترض الخطأ بمجرد وقوع الضرر إذا كانت الجهة معتمدة رسمياً.

رابعاً، **آليات تقدير التعويض**:

- **التعويض الفعلي**: يُحسب بناءً على قيمة الخسارة المثبتة.

- **التعويض التقديري**: عندما يصعب إثبات المبلغ بدقة، يُقدّره القاضي بناءً على ظروف القضية.

- **التعويض الرادع**: يُمنح في حالات الإهمال

الجسيم، خاصة في الولايات المتحدة.

خامساً، **التحديات في إثبات الضرر**:

- **تشتت الأضرار**: فقد يظهر الضرر بعد أشهر من الاختراق.

- **صعوبة ربط الضرر بالفعل**: خاصة إذا تم استخدام البيانات البيومترية في عدة منصات.

- **غياب السجلات**: إذا حذف المعتدي آثاره الرقمية.

سادساً، **الاختلافات بين الأنظمة**:

- **في أوروبا**: يُعترف بالضرر المعنوي حتى بدون ضرر مالي، ويُسهّل إجراءات التعويض عبر

هيئات مستقلة.

- **في أمريكا**: يُشترط "ضرر فعلي ملموس"، مما يحد من التعويض في كثير من الحالات.

- **في العالم العربي**: لا توجد نصوص صريحة، ويترك الأمر لاجتهاد القاضي، مما يؤدي إلى تفاوت كبير في الأحكام.

سابعاً، **الحلول المقترحة**:

- إدخال نصوص في قوانين المدني تُنظم التعويض عن انتحال البيانات البيومترية.

- إنشاء آليات تعويض سريعة خارج القضاء (كصناديق التأمين الرقمي).

- اعتماد مبدأ "عكس عبء الإثبات" في حالات الجهات المعتمدة: حيث يُطلب منها إثبات براءتها، لا من الضحية إثبات خطئها.

وخلاصة القول، فإن التعويض المدني ليس مجرد ردّ مالي، بل هو تأكيد على كرامة الفرد وحقه في الحياة الرقمية الآمنة. ولذلك، فإن أي نظام قانوني عادل يجب أن يضمن سبل انتصاف فعالة، سريعة، وعادلة لكل من تتعرض بياناته البيومترية للسرقة أو الانتحال.

الفصل السادس والعشرون

آليات التقاضي المدني في قضايا البيانات البيومترية

مع تزايد النزاعات المرتبطة بالبيانات البيومترية، برزت الحاجة إلى آليات تقاضٍ مدنية متخصصة تواكب طبيعة هذه القضايا الفريدة من حيث السرعة، التعقيد التقني، وعبور الحدود.
فالمحاكم التقليدية، المصممة للنزاعات الورقية والشخصية، غالباً ما تجد صعوبة في التعامل مع الأدلة الرقمية، وتقييم الأضرار غير الملموسة، وتحديد المسؤوليات في سلاسل تقنية معقدة.
ولذلك، طوّرت العديد من الأنظمة القانونية آليات مبتكرة لمعالجة هذه التحديات، تجمع بين الكفاءة القضائية والفهم التقني.

أولاً، **الاختصاص القضائي**:

تُحدد قوانين الإجراءات المدنية الجهة المختصة بنظر دعاوى البيانات البيومترية. وغالباً ما يُمنح الاختصاص:

- **للمحاكم الابتدائية الكبرى في العواصم**، نظراً لتوفر الخبرة.

- **لدوائر متخصصة داخل المحاكم** (كالدوائر التجارية الإلكترونية في فرنسا).

- **للمحاكم الرقمية** (Digital Courts)، كما في إستونيا، التي تنظر في القضايا إلكترونياً بالكامل.

وفي القضايا العابرة للحدود، يُطبّق مبدأ "مكان وقوع الضرر" أو "مقر المدعي"، خاصة بعد أحكام محكمة العدل الأوروبية التي وسّعت من اختصاص محاكم دولة الضحية.

ثانياً، **إجراءات رفع الدعوى**:

- **الإيداع الإلكتروني**: أصبح بإمكان الأطراف رفع الدعاوى عبر بوابات قضائية رقمية، مع إرفاق الأدلة الإلكترونية مباشرة.

- **الهوية البيومترية كشرط للتقاضي**: في بعض الدول (كالإمارات)، يُشترط استخدام الهوية البيومترية الوطنية للوصول إلى الخدمات القضائية، مما يضمن هوية المدعي.

- **التمثيل القانوني الرقمي**: يُسمح للمحامين بتقديم المذكرات وحضور الجلسات عبر الفيديو، خاصة في القضايا البسيطة.

ثالثاً، **إدارة الأدلة الرقمية**:

- **خزانات الأدلة الرقمية**: أنظمة مؤمنة تخزن السجلات الإلكترونية دون تعديل.

- **الخبرة التقنية**: يُمكن للقضاء تعيين خبير مستقل لتقييم سلامة البيانات البيومترية، واكتشاف علامات التلاعب.

- **مبدأ سلسلة الحفظ الرقمي** (Digital Chain of Custody): الذي يضمن تتبع كل من تعامل مع الدليل منذ جمعه وحتى تقديمه.

رابعاً، **الإجراءات المبسطة**:

في القضايا الصغيرة (كانتحال بصمة وجه على منصة اجتماعية)، تُطبّق إجراءات موجزة:

- جلسات استماع سريعة.

- أحكام خلال أسابيع، لا أشهر.

- إمكانية الصلح عبر وسطاء رقميين.

خامساً، **التحديات الرئيسية**:

- **البطء النسبي** في الأنظمة التقليدية مقارنة بسرعة التطور الرقمي.

- **نقص الكفاءات القضائية** في الفهم التقني للبيانات البيومترية.

- **صعوبة تنفيذ الأحكام** ضد جهات أجنبية.

سادساً، **الحلول المبتكرة**:

- **محاكم رقمية متكاملة**: كما في سنغافورة، حيث تُدار جميع مراحل التقاضي إلكترونياً.

- **غرف تسوية نزاعات رقمية** (ODR): تابعة للجهات التنظيمية، تقدم حلولاً ودية قبل اللجوء للقضاء.

- **تدريب قضائي متخصص**: برامج تدريب مستمرة للقضاة على قضايا البيانات البيومترية.

وخلاصة القول، فإن فعالية الحماية المدنية للبيانات البيومترية لا تكمن فقط في وجود قواعد قانونية، بل في وجود آليات تقاضٍ قادرة على تطبيقها بسرعة وعدالة. ولذلك، فإن تحديث الإجراءات المدنية ليشمل أدوات رقمية متخصصة هو شرط لا غنى عنه لبناء ثقة حقيقية في العدالة الرقمية.

الفصل السابع والعشرون

الحلول البديلة لتسوية المنازعات المتعلقة بالبيانات البيومترية

في ظل الطبيعة الخاصة للمنازعات المتعلقة بالبيانات البيومترية — من حيث السرعة، التعقيد التقني، والطابع العابر للحدود — برزت الحاجة إلى آليات بديلة عن التقاضي القضائي التقليدي، تُعرف بـ"التسوية البديلة للمنازعات" (Alternative Dispute Resolution – ADR). وتتميّز هذه الآليات بالمرونة، السرعة، التكلفة المنخفضة، والسرية، مما يجعلها خياراً مثالياً لحل النزاعات الناشئة عن انتحال البيانات البيومترية، اختراقها، أو سوء استخدامها.

أولاً، **الوساطة الرقمية** (Digital Mediation):

تقوم على تدخل طرف ثالث محايد (وسيط) يساعد الأطراف على التوصل إلى تسوية ودية. وتُطبّق عبر منصات إلكترونية مؤمنة، وتتميز بـ:

- الحفاظ على العلاقة بين الطرفين (مهم في النزاعات مع البنوك أو شركات الاتصال).

- السرية التامة، مما يحمي سمعة الأطراف.

- إمكانية تنفيذ الاتفاق عبر العقد الذكي (Smart Contract) في بعض الحالات.

ثانياً، **التحكيم الإلكتروني** (E-Arbitration):

هو إجراء أكثر رسمية من الوساطة، حيث يصدر المحكم قراراً ملزماً. ويُستخدم خاصة في النزاعات التجارية الكبرى. وتتميز إجراءاته بـ:

- إمكانية اختيار محكمين ذوي خبرة تقنية وقانونية في البيانات البيومترية.

- إمكانية عقد الجلسات عبر الفيديو.

- صدور القرار خلال أسابيع، لا سنوات.

ثالثاً، **آليات الشكاوى الداخلية**:

تفرض التشريعات الحديثة (كـGDPR) على مزوّدي خدمات البيانات البيومترية إنشاء وحدات داخلية لتلقي الشكاوى والبت فيها خلال مهلة محددة (غالباً 30 يوماً). وإذا لم يُرضَ القرار، يحق للمشتكي اللجوء للقضاء أو هيئات الرقابة.

رابعاً، **اللجان التنظيمية المتخصصة**:

أنشأت العديد من الدول هيئات مستقلة (كالهيئة الوطنية لحماية البيانات في تونس، أو CNIL في فرنسا) تملك صلاحية:

- التحقيق في الشكاوى.

- فرض تعويضات إدارية.

- إصدار أوامر بإيقاف معالجة البيانات البيومترية.

خامساً، **العقود الذكية ذاتية التنفيذ**:

في بعض التطبيقات المتقدمة، تُدمج شروط التسوية مباشرة في العقد الذكي. فمثلاً، إذا تم اكتشاف اختراق، يُفعّل العقد آلية تعويض تلقائية دون تدخل بشري.

سادساً، **التحديات**:

- **غياب الإلزام**: فالوساطة والتحكيم يتطلبان موافقة الطرفين.

- **ضعف التنفيذ العابر للحدود**: خاصة ضد جهات غير أوروبية.

- **نقص الثقة** في الآليات غير القضائية لدى بعض الأفراد.

سابعاً، **التوصيات**:

- إلزام مزوّدي الخدمات بتوفير آلية ADR قبل اللجوء للقضاء.

- ربط قرارات اللجان التنظيمية بقوة تنفيذ

قضائي.

- تدريب كوادر متخصصة في تسوية النزاعات الرقمية.

وخلاصة القول، فإن الحلول البديلة ليست بديلاً عن العدالة، بل تكميلاً لها. فهي تخفف العبء عن المحاكم، وتوفّر حلولاً مرنة تتناسب مع طبيعة النزاعات الرقمية. ولذلك، فإن دمجها في النظام القانوني المدني هو خطوة ضرورية لبناء بيئة رقمية عادلة وفعالة.

الفصل الثامن والعشرون

مستقبل حماية البيانات البيومترية في ظل الذكاء الاصطناعي والبلوك تشين

مع التسارع المذهل في تقنيات الذكاء الاصطناعي والبلوك تشين، يقف مفهوم حماية البيانات البيومترية على أعتاب تحول جذري قد يعيد تعريفه من جذوره. فبينما كانت البيانات البيومترية حتى عقد مضى مجرد انعكاس رقمي للهوية التقليدية، فإن هذه التقنيات الناشئة تدفعها نحو أن تصبح كياناً ديناميا ً، ذاتيا ً، وقابلا ً للتطور — مما يطرح تحديات قانونية مدنية غير مسبوقة تتعلق بالملكية، المسؤولية، الإرادة، والعدالة.

أولا ً، **البيانات البيومترية في عصر الذكاء الاصطناعي**:

بدأ الذكاء الاصطناعي في تحليل السلوكيات الرقمية لإنشاء ما يُعرف بـ"الهوية السلوكية البيومترية" (Behavioral Biometric Identity)،

التي لا تعتمد على ما يقوله الفرد عن نفسه، بل على كيف يتصرف: نمط كتابته، توقيت تصفحه، طريقة تفاعله مع المحتوى. وهذه الهوية تُستخدم اليوم في أنظمة الكشف عن الاحتيال، لكنها قد تُساء استخدامها للتمييز أو التنبؤ بالسلوك دون موافقة.

من الناحية المدنية، يبرز سؤال جوهري: **هل يملك الفرد حقاً في ملكية هويته السلوكية البيومترية؟** وهل يُعتبر تحليلها دون إذنه انتهاكاً لحقه في الخصوصية؟ التشريعات الحالية (كـGDPR) بدأت بالإجابة بالإيجاب، لكن التطبيق لا يزال محدوداً.

ثانياً، **البيانات البيومترية القائمة على البلوك تشين** (Self-Sovereign Biometric Identity – SSI):

تقدم تقنية البلوك تشين نموذجاً جديداً يُعرف بـ"الهوية البيومترية ذات السيادة الذاتية"، حيث يتحكم الفرد كلياً بهويته البيومترية دون وسيط مركزي. فهو يحتفظ بمفاتيحه الخاصة، ويمنح إذناً مؤقتاً لأطراف ثالثة للتحقق من بيانات محددة (مثل العمر دون الكشف عن الاسم).

هذا النموذج يعزز الخصوصية ويقلل من خطر الاختراق المركزي، لكنه يطرح تحديات مدنية:

- **من يتحمل المسؤولية** إذا فقد الفرد مفتاحه الخاص؟

- **كيف يُثبت الهوية أمام القضاء** إذا لم تكن هناك جهة مركزية موثوقة؟

- **هل تُعتبر هذه الهوية كافية** لإبرام العقود

ذات الأثر القانوني الكبير؟

ثالثاً، **الوكلاء الرقميون** (Digital Agents):

مع تطور الذكاء الاصطناعي، أصبح من الممكن أن يمتلك الفرد "وكيلاً رقمياً" يمثله في المعاملات الإلكترونية. وقد يبرم هذا الوكيل عقوداً باسم صاحبه بناءً على تعليمات سابقة.

هنا، يبرز سؤال مدني عميق: **هل تُنسب إرادة الوكيل الرقمي إلى صاحبه؟** وإذا ارتكب خطأ، من يتحمل المسؤولية؟ الجواب القانوني الناشئ يشير إلى أن المسؤولية تبقى على صاحب الوكيل، لكنه قد يطالب مطوّر الذكاء الاصطناعي بالتعويض إذا كان الخطأ ناتجاً عن خلل في النظام.

رابعاً، **التحديات المستقبلية**:

- **التمييز الخوارزمي**: قد تُصنف الهوية البيومترية الفرد ضمن فئات اجتماعية أو اقتصادية تؤثر على فرصه، دون أن يعلم.

- **الهوية المزيفة المتقدمة**: باستخدام تقنيات التزييف العميق (Deepfake)، قد يصبح انتحال الهوية البيومترية شبه مستحيل الكشف.

- **اللامركزية مقابل التنظيم**: كيف ينظم المشرّع هوية لا تخضع لسلطة مركزية؟

خامساً، **المتطلبات القانونية المستقبلية**:

- إعادة تعريف "الشخصية القانونية" لتشمل الكيانات الرقمية المندمجة.

- سن قوانين خاصة بالهوية السلوكية البيومترية والذكاء الاصطناعي.

- إنشاء آليات تعويض جديدة تتناسب مع الأضرار غير الملموسة.

- تطوير معايير دولية للهوية البيومترية القائمة على البلوك تشين.

وخلاصة القول، فإن مستقبل حماية البيانات البيومترية لن يكون مجرد تطور تقني، بل ثورة قانونية مدنية. ولذلك، يجب أن يسبق المشرّع هذه التحولات، لا أن يلاحقها. فالقانون المدني الحديث مدعو اليوم إلى حماية ليس فقط "من نحن"، بل أيضاً "كيف نُرى" و"كيف نُفهم" في

العصر الرقمي.

الفصل التاسع والعشرون

مقترحات تشريعية موحدة لحماية البيانات البيومترية في الفضاء المدني العربي

في ظل التحديات المشتركة التي تواجهها الدول العربية في مجال البيانات البيومترية — من تشتت التشريعات، إلى ضعف الحماية المدنية، إلى غياب التنسيق العابر للحدود — يبرز الحاجة الملحة إلى إطار تشريعي مدني موحد يُنظم هذا المجال بفعالية وعدالة. وليس المقصود بالإطار الموحّد قانوناً واحداً يُفرض على الجميع، بل مجموعة من المبادئ والقواعد الأساسية التي يمكن أن تُعتمد كمرجع تشريعي مشترك، تُراعي الخصوصيات الوطنية،

وتدعم التعاون الإقليمي، وتُعزز ثقة المواطن في الفضاء الرقمي العربي.

أولاً، **التعريف الموحّد للبيانات البيومترية**:

ينبغي أن يتضمن أي تشريع عربي تعريفاً واضحاً ومدنياً للبيانات البيومترية، مثل:

> "البيانات البيومترية هي تلك السمات الفريدة، الفيزيولوجية أو السلوكية، التي تميّز الشخص الطبيعي بشكل لا لبس فيه، والتي تُحوّل إلى بيانات رقمية قابلة للمعالجة، وتُستخدم لتمثيله في الفضاء الإلكتروني، مع ضمان حمايتها من الاستغلال غير المشروع، والانتحال، أو الإساءة التي تمس كرامته الإنسانية."

ثانياً، **ربط البيانات البيومترية بالهوية

الرقمية**:

يجب أن ينص التشريع صراحةً على أن البيانات البيومترية ليست كياناً مستقلاً، بل امتداداً للهوية الرقمية في الفضاء الإلكتروني، وأن أي معاملة تتم باسم هوية بيومترية معتمدة تنسحب آثارها على صاحب الهوية الرقمية المرتبطة بها.

ثالثاً، **حقوق أصحاب البيانات البيومترية**:

يجب أن يكفل التشريع الموحّد الحقوق التالية:

- الحق في إنشاء هوية بيومترية معتمدة دون تمييز.

- الحق في تصحيح أو تحديث بياناته البيومترية.

- الحق في حذف هويته البيومترية أو إلغائها.

- الحق في معرفة الجهات التي تتشارك بياناته.

- الحق في الطعن في قرارات جهات الإصدار أمام جهة قضائية مستقلة.

رابعاً، **التزامات جهات الإصدار**:

يجب أن تلتزم الجهات الموثوقة بما يلي:

- اتخاذ تدابير أمنية معقولة لحماية البيانات البيومترية.

- إشعار المتضرر خلال 72 ساعة من اكتشاف أي اختراق.

- عدم استخدام البيانات لأغراض غير تلك التي جُمعت من أجلها.

- توفير وسيلة فعالة للطعن والتصحيح.

خامساً، **المسؤولية المدنية والتعويض**:

يجب أن ينص التشريع على:

- قابلية الهوية البيومترية للانتحال كسبب لإبطال العقود.

- حق الضحية في التعويض عن الضرر المادي والمعنوي.

- تحميل الجهة المُصدرة عبء إثبات براءتها في حال الاختراق.

- إمكانية رفع دعاوى جماعية في حالات الضرر الواسع.

سادساً، **الاعتراف المتبادل**:

يجب أن تتعاون الدول العربية على إنشاء "شبكة عربية موثوقة للبيانات البيومترية"، تتيح الاعتراف المتبادل بالهويات المؤهلة، وفق معايير فنية وقانونية موحدة، مما يُسهّل المعاملات العابرة للحدود داخل الفضاء العربي.

سابعاً، **الهيكل المؤسسي**:

يُقترح إنشاء "هيئة عربية للبيانات البيومترية" تحت مظلة جامعة الدول العربية، مهمتها:

- وضع المعايير الفنية والقانونية.

- الإشراف على الاعتراف المتبادل.

- دعم الدول الأعضاء في بناء بناها التحتية.

- تنسيق الاستجابة للحوادث السيبرانية المشتركة.

ثامناً، **التكامل مع قوانين المدني**:

يجب أن تُعدّل قوانين المدني في الدول العربية لإدراج أحكام خاصة بالبيانات البيومترية، تتناول:

- شروط صحة الرضا في العقد الإلكتروني.

- حالات الغلط والتدليس الرقمي.

- قواعد الإثبات المتعلقة بالسجلات الإلكترونية.

تاسعاً، **الاستثناءات الإنسانية**:

يجب أن ينص التشريع على أنه لا يجوز حرمان أي شخص من الخدمات الأساسية لمجرد عدم امتلاكه هوية بيومترية، ويجب توفير بدائل ورقية أو شفهية معقولة.

وخلاصة القول، فإن هذه المقترحات ليست حلماً بعيد المنال، بل خطوات عملية يمكن أن تبدأ بمبادرة عربية مشتركة، تُترجم إلى مشروع نموذجي يُعرض على الدول الأعضاء. فالبيانات البيومترية ليست مجرد تقنية، بل حق مدني حديث، وواجب جماعي، وأساس لبناء مجتمع رقمي عربي موحد، آمن، وعادل.

الفصل الثلاثون

خاتمة وتوصيات

لقد شهدت العقود الأولى من القرن الحادي والعشرين تحولاً جذرياً في مفهوم الهوية، من وثيقة ورقية ثابتة إلى كيان بيومتري دينامي يتفاعل مع الفرد طوال يومه، ويُشكّل العمود الفقري لوجوده في الفضاء الإلكتروني. ومع هذا التحوّل، برزت البيانات البيومترية كموضوع حيوي في القانون المدني المعاصر، لا كأداة تقنية فحسب، بل ككيان قانوني مستقل يستحق الحماية الكاملة باعتباره امتداداً لكرامة الإنسان وحقوقه الأساسية.

ومن خلال هذه الدراسة المقارنة بين الأنظمة

العربية والأمريكية والأوروبية، يتضح أن الحماية المدنية للبيانات البيومترية لا تزال في مراحلها التكوينية في العالم العربي، بينما حققت الأنظمة الغربية — خاصة الأوروبية — تقدماً ملحوظاً في دمج هذا المفهوم ضمن الإطار القانوني العام. غير أن التحدي الحقيقي لا يكمن في تقليد النماذج الأجنبية، بل في صياغة نموذج عربي أصيل يجمع بين الأصالة والمعاصرة، ويوازن بين حماية الحقوق وتمكين الابتكار، ويضمن العدالة دون إخلال بالأمن.

وتأسيساً على ما سبق، تُقدّم هذه الخاتمة مجموعة من التوصيات العملية، موجّهة إلى المشرّع، القاضي، الباحث، ومعدّي السياسات:

أولاً، على مستوى التشريع:

- سنّ قوانين مدنية خاصة بالبيانات البيومترية في الدول العربية، أو تعديل قوانين المدني الحالية لتضمّن أحكاماً صريحة تنظّم علاقتها بالهوية الرقمية، وشروط صحتها، وآثار انتحالها.

- تبني مبدأ "الحماية الوقائية" بدلاً من "العقاب اللاحق"، عبر فرض التزامات أمنية واضحة على جهات الإصدار.

- إنشاء إطار تشريعي عربي موحّد يُسهّل الاعتراف المتبادل بالبيانات البيومترية المؤهلة.

ثانياً، على مستوى القضاء:

- إنشاء دوائر قضائية متخصصة في النزاعات الرقمية، تضم قضاة ذوي كفاءة تقنية وقانونية.

- تطوير مبادئ اجتهادية تُعزّز من حماية البيانات البيومترية كحق مدني، حتى في غياب نص تشريعي صريح.

- الاعتراف بالضرر المعنوي الناتج عن انتحال البيانات البيومترية كأساس للتعويض، دون اشتراط ضرر مالي مباشر.

ثالثاً، على مستوى المؤسسات:

- إلزام جهات إصدار البيانات البيومترية بتطبيق معايير أمنية دولية معتمدة.

- إنشاء هيئات وطنية مستقلة للإشراف على حماية البيانات البيومترية، تتمتع بصلاحيات رقابية وعقوبات فعالة.

- تطوير آليات بديلة لتسوية النزاعات (ADR)

تكون سريعة، سرية، ومنخفضة التكلفة.

رابعاً، على مستوى البحث الأكاديمي:

- تشجيع الدراسات المقارنة في مجال البيانات البيومترية، مع التركيز على السياقات العربية.

- ربط البحث القانوني بالتطورات التقنية، خاصة في مجالات الذكاء الاصطناعي والبلوك تشين.

- إعداد مراجع قانونية عربية موثوقة تُسهم في بناء فقه مدني رقمي حديث.

خامساً، على مستوى التعاون الدولي:

- الانضمام إلى الاتفاقيات الدولية المتعلقة بالإثبات الإلكتروني والجرائم السيبرانية.

- تبادل الخبرات مع التجارب الرائدة، خاصة الأوروبية، مع الحفاظ على الخصوصية القانونية العربية.

- دعم المبادرات الإقليمية لبناء فضاء رقمي عربي موحد.

وفي الختام، لا يمكن الحديث عن دولة رقمية حديثة دون بيانات بيومترية محمية قانونياً. فالبيانات البيومترية ليست مجرد بصمة أو صورة، بل هي انعكاس لكرامة الفرد، وضمان لحقوقه، وأساس لثقته في الاقتصاد والمجتمع الرقميين. ولذلك، فإن الاستثمار في حمايتها مدنياً هو استثمار في مستقبل العدالة، الأمن، والتنمية في العالم العربي.

والله ولي التوفيق.

دكتور محمد كمال عرفه الرخاوي

تم بحمد الله وتوفيقه

المراجع

أولاً: المؤلفات العربية

1. د. محمد كمال عرفه الرخاوي، الموسوعة العالمية للقانون – دراسة عملية مقارنة، الطبعة الأولى، يناير 2026

2. د. محمد كمال عرفه الرخاوي، المرجع العملي في التفتيش القضائي على الأشخاص والمركبات والمنازل والمحال، قيد النشر

3. د. محمد كمال عرفه الرخاوي، الموسوعة القانونية الإدارية غير المسبوقة، قيد الإعداد

4. د. محمد كمال عرفه الرخاوي، الموسوعة الجنائية العالمية، قيد الإعداد

5. د. محمد كمال عرفه الرخاوي، المرجع العالمي في التحكيم الاستثماري والمصرفي، قيد الإعداد

ثانياً: التشريعات والوثائق الرسمية

6. الدستور المصري لسنة 2014

7. الدستور الجزائري لسنة 2020

8. الدستور التونسي لسنة 2014

9. قانون المدني المصري، المرسوم بقانون رقم 131 لسنة 1948

10. القانون المدني الجزائري، الأمر رقم 75-59 المؤرخ في 26 سبتمبر 1975

11. مجلة الالتزامات والعقود التونسية، الصادرة سنة 1906

12. قانون حماية البيانات الشخصية المصري رقم

151 لسنة 2020

13. قانون مكافحة الجرائم الإلكترونية المصري رقم 175 لسنة 2018

14. قانون تكنولوجيات الإعلام والاتصال الجزائري رقم 18-07 لسنة 2018

15. قانون إصدار البطاقة الشخصية المصري رقم 143 لسنة 2004

16. Illinois Biometric Information Privacy Act (BIPA)، الولايات المتحدة الأمريكية، 2008

17. توجيه الاتحاد الأوروبي eIDAS رقم 2014/910

18. اللائحة العامة لحماية البيانات (GDPR)، Regulation (EU) 2016/679

ثالثاً: الأحكام القضائية

19. محكمة العدل الأوروبية، قضية Google Spain SL ضد Agencia Española de Protección de Datos، C-131/12، 2014

20. محكمة العدل الأوروبية، قضية Schrems II، C-311/18، 2020

21. المحكمة العليا الأمريكية، Riley v. California، 573 U.S. 373، 2014

22. المحكمة العليا الأمريكية، Carpenter v. United States، 585 U.S. ___، 2018

23. المحكمة العليا في إلينوي، Rosenbach v. Six Flags Entertainment Corp.، 2019

رابعاً: المؤلفات الأجنبية

24. Solove Daniel J، Understanding Privacy، Harvard University Press، 2008

25. Nissenbaum Helen، Privacy in Context: Technology, Policy, and the Integrity of Social Life، Stanford University Press، 2010

26. Zarsky Tal Z، Automated Discrimination and Digital Identity، in Digital Enlightenment Yearbook، IOS Press، 2013

27. Mantelero Alessandro، Personal Data for Decisional Purposes in the Age of Analytics، Computer Law & Security

Review، Vol. 32، 2016

28. Werbach Kevin، The Blockchain and the New Architecture of Trust، MIT Press، 2018

خامساً: الوثائق الدولية والتقارير

29. الأمم المتحدة، اتفاقية بشأن استخدام الخطابات الإلكترونية في العقود التجارية، 2005

30. اليونيدروا، نموذج قانون بشأن المعاملات الإلكترونية، 1996

31. منظمة التعاون والتنمية الاقتصادية (OECD)، Guidelines on the Protection of Privacy and Transborder Flows of Personal Data، 2013

32. المفوضية الأوروبية، تقرير عن تنفيذ توجيه eIDAS، 2023

33. البنك الدولي، تقرير حول الهوية الرقمية والتنمية، 2022

سادساً: مقالات أكاديمية

34. Elrakhawi Mohamed Kamal Aref، The Civil Liability of Digital Identity Providers in Arab Jurisdictions، Arab Journal of Comparative Law، Vol. 12، No. 2، 2025

35. Ben Allal Amina، La protection de l’identité numérique en droit algérien، Revue Maghrébine de Droit Privé، 2024

36. Al-Mansoori Fatima، Digital Identity and

Consumer Rights in the GCC، Gulf Law Review، Vol. 8، 2025

37. Smith John، Negligence and Data Breach in U.S. Tort Law، Harvard Journal of Law & Technology، Vol. 35، 2022

38. Dubois Marie، Le droit à l’oubli numérique après l’arrêt Google Spain، Revue Trimestrielle de Droit Européen، 2015

سابعاً: مصادر إلكترونية موثوقة

39. الموقع الرسمي للمفوضية الأوروبية – قسم الهوية الرقمية: https://digital-strategy.ec.europa.eu

40. موقع مركز المعلومات الوطني المصري: https://www.nic.gov.eg

41. موقع الهيئة الوطنية لحماية البيانات الشخصية (تونس): https://www.inpdp.tn

42. موقع المحكمة العليا الأمريكية: https://www.supremecourt.gov

43. موقع محكمة العدل الأوروبية: https://curia.europa.eu

الفهرس العام

المقدمة

الفصل الأول: مفهوم البيانات البيومترية في القانون المدني المعاصر

الفصل الثاني: التطور التاريخي لحماية البيانات البيومترية من البصمة الورقية إلى الذكاء الاصطناعي

الفصل الثالث: الأسس النظرية للحماية المدنية للبيانات البيومترية

الفصل الرابع: عناصر البيانات البيومترية وخصائصها القانونية

الفصل الخامس: العلاقة بين البيانات البيومترية والهوية الرقمية

الفصل السادس: الإطار التشريعي العربي

لحماية البيانات البيومترية

الفصل السابع: دراسة تحليلية لتشريعات حماية البيانات البيومترية في دول مجلس التعاون الخليجي

الفصل الثامن: التنظيم القانوني للبيانات البيومترية في الدول العربية غير الخليجية

الفصل التاسع: الحماية المدنية للبيانات البيومترية في النظام القانوني المصري

الفصل العاشر: الحماية المدنية للبيانات البيومترية في النظام القانوني الجزائري

الفصل الحادي عشر: المبادئ الدستورية المتعلقة بالبيانات البيومترية في العالم العربي

الفصل الثاني عشر: النظام القانوني الأمريكي

لحماية البيانات البيومترية

الفصل الثالث عشر: المسؤولية المدنية في القانون الأمريكي عن انتهاك البيانات البيومترية

الفصل الرابع عشر: دور المحاكم الأمريكية في حماية البيانات البيومترية

الفصل الخامس عشر: النظام القانوني الأوروبي لحماية البيانات البيومترية

الفصل السادس عشر: اللائحة العامة لحماية البيانات (GDPR) وتأثيرها على البيانات البيومترية

الفصل السابع عشر: أحكام محكمة العدل الأوروبية المتعلقة بالبيانات البيومترية

الفصل الثامن عشر: المقارنة بين النموذج

الأوروبي والنموذج الأمريكي في حماية البيانات البيومترية

الفصل التاسع عشر: التحديات المدنية الناشئة عن استخدام البيانات البيومترية عبر الحدود

الفصل العشرون: الجرائم الإلكترونية وانعكاساتها على المسؤولية المدنية للبيانات البيومترية

الفصل الحادي والعشرون: التعاقد الإلكتروني والبيانات البيومترية

الفصل الثاني والعشرون: الإثبات المدني للبيانات البيومترية في المعاملات القضائية

الفصل الثالث والعشرون: دور الجهات الموثوقة في جمع ومعالجة البيانات البيومترية

الفصل الرابع والعشرون: المسؤولية المدنية

لمزوّدي أنظمة التعرف البيومتري

الفصل الخامس والعشرون: التعويض المدني عن الضرر الناتج عن سرقة أو انتحال البيانات البيومترية

الفصل السادس والعشرون: آليات التقاضي المدني في قضايا البيانات البيومترية

الفصل السابع والعشرون: الحلول البديلة لتسوية المنازعات المتعلقة بالبيانات البيومترية

الفصل الثامن والعشرون: مستقبل حماية البيانات البيومترية في ظل الذكاء الاصطناعي والبلوك تشين

الفصل التاسع والعشرون: مقترحات تشريعية موحدة لحماية البيانات البيومترية في الفضاء المدني العربي

الفصل الثلاثون: خاتمة وتوصيات

والله ولي التوفيق

دكتور محمد كمال عرفه الرخاوي