**التنظيم القانوني المدني للهوية الرقمية: دراسة مقارنة بين الأنظمة العربية والأمريكية والأوروبية**

المؤلف د. محمد كمال عرفه الرخاوي

## الاهداء

اهدي هذا العمل لروح والدي رحمهم الله وغفر لهم وادخلهم الجنه بدون حساب يارب العالمين وابنتي الحبيبه صبرينال نور عيني المصريه الجزائريه جميله الجميلات التي تجمع بين جمال نهر النيل وجبال الاوراس وشط المتوسط

## المقدمه

في عالم يتسارع فيه التحوّل الرقمي بوتيرة غير مسبوقة، لم يعد مفهوم الهوية قاصراً على الوثائق الورقية أو السجلات المدنية التقليدية. بل تجاوز ذلك ليتشكل في فضاء افتراضي دينامي، يُعرف بالهوية الرقمية، التي باتت تُشكّل

العمود الفقري للتعاملات اليومية، من الخدمات الحكومية إلى المعاملات المالية، ومن التعليم عن بُعد إلى الرعاية الصحية الإلكترونية. ومع هذا التحوّل الجذري، برزت تحديات قانونية عميقة، خاصة في نطاق القانون المدني، الذي يُعنى بتنظيم العلاقات بين الأفراد، وحماية الحقوق الشخصية، وضمان سلامة المعاملات.

رغم أن التشريعات الجنائية والتقنية قد أولت الهوية الرقمية 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 للهوية الرقمية، 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 الهوية الرقمية من منظور قانوني مدني دقيق، بعيداً عن التعريفات التقنية الضيقة. الثاني، تحليل الإطار التشريعي والاجتهادي الحاكم لحماية الهوية الرقمية 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 للهوية الرقمية.

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 الهوية الرقمية ليست مجرد قضية تقنية، بل هي مسألة جوهرية تتعلق بكرامة الإنسان وحقوقه الأساسية. والله ولي التوفيق.

دكتور محمد كمال عرفه الرخاوي

## الفصل الأول
## مفهوم الهوية الرقمية في القانون المدني المعاصر

لا يمكن الحديث عن التنظيم القانوني المدني للهوية الرقمية 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، والتعريفات القانونية التي يصوغها الفقه والقضاء والتشريع. فالهوية الرقمية، من منظور تقني، تشير إلى مجموعة البيانات التي تمثّل شخصاً أو كياناً في الفضاء الإلكتروني، وتُستخدم للتحقق من هويته أثناء التفاعل مع الأنظمة الرقمية. أما من منظور قانوني مدني، فهي تتجاوز هذا الحد لتُصبح تجسيداً رقمياً للشخصية القانونية، تحمل ذات الأهمية التي تحملها الوثائق الرسمية في العالم المادي.

ومن ثم، يمكن تعريف الهوية الرقمية في القانون المدني المعاصر بأنها: تلك الصورة القانونية المُعترف بها للشخص الطبيعي أو الاعتباري في البيئة الرقمية، والتي تُعبّر عن صفاته الجوهرية، وتمكّنه من ممارسة حقوقه والتزاماته بشكل آمن وموثوق**التنظيم القانوني

## المدني للهوية الرقمية: دراسة مقارنة بين الأنظمة العربية والأمريكية والأوروبية**

## المقدمة

في عالم يتسارع فيه التحوّل الرقمي بوتيرة غير مسبوقة، لم يعد مفهوم الهوية قاصراً على الوثائق الورقية أو السجلات المدنية التقليدية. بل تجاوز ذلك ليتشكل في فضاء افتراضي دينامي، يُعرف بالهوية الرقمية، التي باتت تُشكّل العمود الفقري للتعاملات اليومية، من الخدمات الحكومية إلى المعاملات المالية، ومن التعليم عن بُعد إلى الرعاية الصحية الإلكترونية. ومع هذا التحوّل الجذري، برزت تحديات قانونية عميقة، خاصة في نطاق القانون المدني، الذي يُعنى بتنظيم العلاقات بين الأفراد، وحماية الحقوق الشخصية، وضمان سلامة المعاملات.

رغم أن التشريعات الجنائية والتقنية قد أولت

الهوية الرقمية 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 للهوية الرقمية، 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 الهوية الرقمية من منظور قانوني مدني دقيق، بعيداً عن التعريفات التقنية الضيقة. الثاني، تحليل الإطار التشريعي والاجتهادي الحاكم لحماية الهوية الرقمية 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 للهوية الرقمية.

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 الهوية الرقمية ليست مجرد قضية تقنية، بل هي مسألة جوهرية تتعلق بكرامة الإنسان وحقوقه الأساسية. والله ولي التوفيق.

دكتور محمد كمال عرفه الرخاوي

## الفصل الأول
## مفهوم الهوية الرقمية في القانون المدني المعاصر

لا يمكن الحديث عن التنظيم القانوني المدني للهوية الرقمية 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، والتعريفات القانونية التي يصوغها الفقه والقضاء والتشريع. فالهوية الرقمية، من منظور تقني، تشير إلى مجموعة البيانات التي تمثّل شخصاً أو كياناً في الفضاء الإلكتروني، وتُستخدم للتحقق من هويته أثناء التفاعل مع الأنظمة الرقمية. أما من منظور قانوني مدني، فهي تتجاوز هذا الحد

لتُصبح تجسيداً رقمياً للشخصية القانونية، تحمل ذات الأهمية التي تحملها الوثائق الرسمية في العالم المادي.

ومن ثم، يمكن تعريف الهوية الرقمية في القانون المدني المعاصر بأنها: تلك الصورة القانونية المُعترف بها للشخص الطبيعي أو الاعتباري في البيئة الرقمية، والتي تُعبّر عن صفاته الجوهرية، وتمكّنه من ممارسة حقوقه والتزاماته بشكل آمن وموثوق، وتُخوّله القدرة على التفاعل القانوني مع الآخرين عبر الوسائل الإلكترونية، مع ضمان حمايته من الانتحال أو التزوير أو الاستغلال غير المشروع.

ويتميز هذا المفهوم بعدة خصائص أساسية. أولها: الطابع القانوني، إذ لا يكفي أن تكون هناك بيانات رقمية عن الشخص، بل يجب أن تكون هذه البيانات مُعترفاً بها قانوناً، وقابلة للإثبات أمام الجهات القضائية والإدارية. ثانيها: الطابع

الدينامي، حيث إن الهوية الرقمية ليست ثابتة، بل تتغير باستمرار مع تطور أنشطة الشخص وتفاعله مع مختلف المنصات والخدمات. ثالثها: الطابع الشامل، إذ لا تقتصر على اسم أو رقم، بل تشمل مجموعة متكاملة من السمات، مثل العنوان الإلكتروني، بصمات السلوك الرقمي، السجلات المالية، وحتى التفضيلات الشخصية عند ارتباطها بمعاملات قانونية.

ومن الخطأ الشائع اعتبار الهوية الرقمية مجرد امتداد للهوية التقليدية. بل هي كيان قانوني مستقل، له خصوصياته وتحدياته. فبينما تحمي القوانين المدنية التقليدية الهوية من خلال السجلات الرسمية والشهادات الموثقة، فإن الهوية الرقمية تواجه تهديدات جديدة، مثل القرصنة، والانتحال الجماعي، واستغلال البيانات البيومترية، مما يستدعي أدوات حماية مدنية مبتكرة.

وقد بدأ الفقه المدني المعاصر في الاعتراف بهذه الخصوصية، لا سيما في أوروبا، حيث تم اعتبار الهوية الرقمية جزءاً من الحق في الخصوصية، بل وحتى من كرامة الإنسان. 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 الهوية الرقمية 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 بالشخصية القانونية، في إطار مقارن يجمع بين التجارب العربية والأمريكية والأوروبية.

## الفصل الثاني
## التطور التاريخي للهوية الرقمية من منظور قانوني

لم تنشأ الهوية الرقمية في فراغ قانوني أو اجتماعي، بل هي نتاج تراكمي لتحولات تقنية وقانونية تمتد جذورها إلى عقود مضت. فقبل ظهور الإنترنت كشبكة عالمية، كانت أنظمة المعلومات تُدار ضمن شبكات مغلقة، وكانت الهوية تُحدد عبر أرقام تعريف داخلية تابعة للجهات الحكومية أو المؤسسات الكبرى. ومع بروز شبكة الإنترنت في تسعينيات القرن العشرين، بدأت الحاجة إلى آليات جديدة للتعرف على الأفراد والكيانات في بيئة لا مركزية وغير موثوقة. وقد أدت هذه الحاجة إلى ولادة أولى صور الهوية الرقمية، مثل كلمات المرور، وأرقام التعريف الفريدة، والشهادات الرقمية.

في المرحلة الأولى، كان التركيز منصباً على

الجوانب الأمنية والتقنية، دون إيلاء الاعتبار الكافي للأبعاد القانونية. وكان التشريع يسير خلف التطور التقني بخطوات بطيئة، مما خلق فجوة تشريعية واسعة. غير أن ظهور التجارة الإلكترونية في أواخر التسعينيات دفع الدول إلى سن قوانين تنظم التعاملات الرقمية، ومن بينها قوانين التوقيع الإلكتروني، التي شكلت حجر الزاوية الأول في الاعتراف القانوني بالهوية الرقمية. فقد نصت اتفاقية الأمم المتحدة بشأن استخدام الخطابات الإلكترونية في العقود التجارية عام 2005، وكذلك توجيه الاتحاد الأوروبي رقم EC/93/1999، على مبدأ الاعتراف القانوني بالتوقيعات الإلكترونية، ما منح الهوية الرقمية أولى درجات الشرعية القانونية.

وفي الولايات المتحدة، سار التشريع على خطى مماثلة، إذ صدر قانون التوقيع الإلكتروني في المعاملات العالمية والوطنية (E-SIGN Act) عام 2000، والذي أقرّ بأن السجلات والتوقيعات

الإلكترونية لها نفس القوة القانونية كالسجلات والتوقيعات الورقية. أما في العالم العربي، فقد تأخر الاعتراف القانوني بالهوية الرقمية نسبياً، حيث لم تبدأ الدول العربية في سن تشريعات متكاملة إلا في أوائل العقد الأول من القرن الحادي والعشرين. ومن أبرز الأمثلة على ذلك قانون المعاملات الإلكترونية في الإمارات العربية المتحدة عام 2006، وقانون التوقيع الإلكتروني في تونس عام 2004، وقانون تكنولوجيا المعلومات في مصر عام 2004.

ومع تصاعد استخدام الشبكات الاجتماعية والخدمات السحابية في العقد الثاني من القرن الحادي والعشرين، توسعت مفاهيم الهوية الرقمية لتشمل ليس فقط هوية المستخدم الرسمية، بل أيضاً هويته السلوكية، المبنية على تتبع أنشطته وتفاعله مع المحتوى الرقمي. وقد أدى هذا التوسع إلى ظهور تحديات قانونية جديدة، خاصة في مجالات الخصوصية،

وحماية البيانات، والمسؤولية المدنية عن الاستخدام غير المشروع للمعلومات الشخصية.

وقد مثلت اللائحة العامة لحماية البيانات (GDPR) التي دخلت حيز التنفيذ في الاتحاد الأوروبي عام 2018 نقطة تحول جوهرية في تاريخ الهوية الرقمية من منظور قانوني. فلأول مرة، تم ربط الهوية الرقمية بحقوق أساسية للمواطن، مثل الحق في النسيان، والحق في نقل البيانات، والحق في عدم الخضوع لقرارات آلية. 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

Carpenter ضد الولايات المتحدة عام 2018، أكدت على أن البيانات الرقمية المتعلقة بالهوية تستحق حماية دستورية بموجب التعديل الرابع.

وبالنسبة للدول العربية، فإن التطور التاريخي للهوية الرقمية لا يزال في طور التشكل. فبينما أطلقت بعض الدول مشاريع طموحة للهوية الرقمية الموحدة، مثل مشروع الهوية الرقمية في السعودية ومصر، 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 الهوية الرقمية 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 للهوية الرقمية في القانون المدني

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

أولاً، يتعلق الأمر بمبدأ الشخصية القانونية.

فالقانون المدني التقليدي يربط الشخصية القانونية بوجود طبيعي أو اعتباري ملموس. ولكن الهوية الرقمية، رغم عدم ملموسيتها، تمثل هذا الوجود في الفضاء الإلكتروني. ولذلك، فإن الاعتراف بها كتجسيد للشخصية القانونية في البيئة الرقمية هو خطوة ضرورية لضمان اتساق النظام القانوني. وقد بدأ بعض الفقه الأوروبي في الحديث عن الشخصية الرقمية كامتداد ضروري للشخصية القانونية، وليس ككيان منفصل عنها.

ثانياً، يأتي مبدأ حرمة الحياة الخاصة، الذي يُعد من الركائز الأساسية في معظم التشريعات المدنية الحديثة. فالهوية الرقمية تحتوي على كم هائل من المعلومات الشخصية، التي إذا استُخدمت دون إذن، فإنها تشكل انتهاكاً صارخاً لهذا المبدأ. وقد أكدت محكمة العدل الأوروبية مراراً أن أي معالجة للبيانات الشخصية تُعد تدخلاً في الحق في الحياة الخاصة، ما لم

تكن مبررة قانوناً. وهذا المبدأ يكتسب أهمية خاصة في البيئة الرقمية، حيث يصعب على الفرد مراقبة كيفية استخدام بياناته.

ثالثاً، يبرز مبدأ المسؤولية عن الضرر. ففي حال انتحال الهوية الرقمية 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 الهوية؟ أم مزوّد الخدمة؟ أم جهة التحقق؟ إن غياب قواعد واضحة في هذا المجال يؤدي إلى فراغ قانوني يعرّض حقوق الأفراد للخطر.

رابعاً، هناك مبدأ الثقة المشروعة. فعندما يعتمد شخص على هوية رقمية معينة في إبرام عقد أو إجراء معاملة، فإنه يفترض أن هذه الهوية صحيحة وموثوقة. وإذا ثبت العكس، فإن القانون المدني يجب أن يحمي هذا الاعتماد المشروع، ويضمن تعويض المتضرر. وهذا المبدأ يكتسب

أهمية خاصة في المعاملات العابرة للحدود، حيث يصعب التحقق من الهوية يدوياً.

خامساً، يظهر مبدأ المساواة أمام القانون. فلا يجوز أن يُعامل الشخص الذي يمتلك هوية رقمية معتمدة معاملة مختلفة عن الشخص الذي لا يمتلكها، إلا إذا كان هناك مبرر قانوني وجيه. كما لا يجوز أن تُستخدم الهوية الرقمية كأداة للتمييز أو الاستبعاد الاجتماعي.

ومن خلال هذه الأُسس النظرية، يتضح أن الهوية الرقمية 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 للهوية الرقمية.

## الفصل الرابع
## عناصر الهوية الرقمية وخصائصها القانونية

لا تُشكل الهوية الرقمية 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 الهوية الرقمية إلى ثلاثة مستويات رئيسية: العناصر التعريفية، والعناصر الوثائقية، والعناصر السلوكية.

أولاً، العناصر التعريفية: وهي تلك البيانات الأساسية التي تميّز الشخص في الفضاء الرقمي، مثل الاسم الكامل، رقم الهوية الوطنية أو جواز السفر، تاريخ الميلاد، الجنسية، وعنوان

البريد الإلكتروني الرسمي. وهذه العناصر تُعد بمثابة العمود الفقري للهوية الرقمية، لأنها تربط الكيان الرقمي بالشخص الحقيقي في العالم المادي. ومن الناحية القانونية، فإن هذه العناصر تخضع لقواعد صارمة تتعلق بالصحة والدقة والتحديث. فمثلاً، لا يُعتد قانوناً بهوية رقمية تعتمد على اسم مستعار دون ربطه بهوية حقيقية معتمدة، خاصة في المعاملات ذات الأثر القانوني.

ثانياً، العناصر الوثائقية: وتشمل الشهادات الرقمية، التوقيعات الإلكترونية المؤهلة، والبيانات البيومترية (كالبصمة، ومسح الوجه، وقزحية العين). وهذه العناصر تلعب دوراً حاسماً في إثبات صحة الهوية وموثوقيتها. فالشهادة الرقمية، على سبيل المثال، تصدر عن جهة موثوقة معتمدة قانوناً، وتُستخدم للتحقق من أن صاحب الهوية هو من يدّعي أنه كذلك. أما التوقيع الإلكتروني المؤهل، فقد اكتسب قوة

قانونية مساوية للتوقيع الورقي في العديد من التشريعات، مثل توجيه الاتحاد الأوروبي eIDAS. ومن الناحية القانونية، فإن هذه العناصر تتمتع بحماية خاصة، إذ يُجرّم القانون**التنظيم القانوني المدني للهوية الرقمية: دراسة مقارنة بين الأنظمة العربية والأمريكية والأوروبية**

المقدمة

في عالم يتسارع فيه التحوّل الرقمي بوتيرة غير مسبوقة، لم يعد مفهوم الهوية قاصراً على الوثائق الورقية أو السجلات المدنية التقليدية. بل تجاوز ذلك ليتشكل في فضاء افتراضي دينامي، يُعرف بالهوية الرقمية، التي باتت تُشكّل العمود الفقري للتعاملات اليومية، من الخدمات الحكومية إلى المعاملات المالية، ومن التعليم عن بُعد إلى الرعاية الصحية الإلكترونية. ومع هذا التحوّل الجذري، برزت تحديات قانونية عميقة، خاصة في نطاق القانون المدني، الذي

يُعنى بتنظيم العلاقات بين الأفراد، وحماية الحقوق الشخصية، وضمان سلامة المعاملات.

رغم أن التشريعات الجنائية والتقنية قد أولت الهوية الرقمية 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 للهوية الرقمية، 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 الهوية الرقمية من منظور قانوني مدني دقيق، بعيداً عن التعريفات التقنية

الضيقة. الثاني، تحليل الإطار التشريعي والاجتهادي الحاكم لحماية الهوية الرقمية 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 للهوية الرقمية.

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 الهوية الرقمية ليست مجرد قضية تقنية، بل هي مسألة جوهرية تتعلق بكرامة الإنسان وحقوقه الأساسية. والله ولي التوفيق.

دكتور محمد كمال عرفه الرخاوي

## الفصل الأول
## مفهوم الهوية الرقمية في القانون المدني المعاصر

لا يمكن الحديث عن التنظيم القانوني المدني للهوية الرقمية 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، والتعريفات القانونية التي يصوغها الفقه والقضاء والتشريع. فالهوية الرقمية، من منظور تقني، تشير إلى

مجموعة البيانات التي تمثّل شخصاً أو كياناً في الفضاء الإلكتروني، وتُستخدم للتحقق من هويته أثناء التفاعل مع الأنظمة الرقمية. أما من منظور قانوني مدني، فهي تتجاوز هذا الحد لتُصبح تجسيداً رقمياً للشخصية القانونية، تحمل ذات الأهمية التي تحملها الوثائق الرسمية في العالم المادي.

ومن ثم، يمكن تعريف الهوية الرقمية في القانون المدني المعاصر بأنها: تلك الصورة القانونية المُعترف بها للشخص الطبيعي أو الاعتباري في البيئة الرقمية، والتي تُعبّر عن صفاته الجوهرية، وتمكّنه من ممارسة حقوقه والتزاماته بشكل آمن وموثوق، وتُخوّله القدرة على التفاعل القانوني مع الآخرين عبر الوسائل الإلكترونية، مع ضمان حمايته من الانتحال أو التزوير أو الاستغلال غير المشروع.

ويتميز هذا المفهوم بعدة خصائص أساسية.

أولها: الطابع القانوني، إذ لا يكفي أن تكون هناك بيانات رقمية عن الشخص، بل يجب أن تكون هذه البيانات مُعترفاً بها قانوناً، وقابلة للإثبات أمام الجهات القضائية والإدارية. ثانيها: الطابع الدينامي، حيث إن الهوية الرقمية ليست ثابتة، بل تتغير باستمرار مع تطور أنشطة الشخص وتفاعله مع مختلف المنصات والخدمات. ثالثها: الطابع الشامل، إذ لا تقتصر على اسم أو رقم، بل تشمل مجموعة متكاملة من السمات، مثل العنوان الإلكتروني، بصمات السلوك الرقمي، السجلات المالية، وحتى التفضيلات الشخصية عند ارتباطها بمعاملات قانونية.

ومن الخطأ الشائع اعتبار الهوية الرقمية مجرد امتداد للهوية التقليدية. بل هي كيان قانوني مستقل، له خصوصياته وتحدياته. فبينما تحمي القوانين المدنية التقليدية الهوية من خلال السجلات الرسمية والشهادات الموثقة، فإن الهوية الرقمية تواجه تهديدات جديدة، مثل

القرصنة، والانتحال الجماعي، واستغلال البيانات البيومترية، مما يستدعي أدوات حماية مدنية مبتكرة.

وقد بدأ الفقه المدني المعاصر في الاعتراف بهذه الخصوصية، لا سيما في أوروبا، حيث تم اعتبار الهوية الرقمية جزءاً من الحق في الخصوصية، بل وحتى من كرامة الإنسان. 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 الهوية الرقمية 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 بالشخصية القانونية، في إطار مقارن يجمع بين التجارب العربية والأمريكية والأوروبية.

## الفصل الثاني
## التطور التاريخي للهوية الرقمية من منظور قانوني

لم تنشأ الهوية الرقمية في فراغ قانوني أو اجتماعي، بل هي نتاج تراكمي لتحولات تقنية وقانونية تمتد جذورها إلى عقود مضت. فقبل ظهور الإنترنت كشبكة عالمية، كانت أنظمة المعلومات تُدار ضمن شبكات مغلقة، وكانت الهوية تُحدد عبر أرقام تعريف داخلية تابعة للجهات الحكومية أو المؤسسات الكبرى. ومع بروز شبكة الإنترنت في تسعينيات القرن العشرين، بدأت الحاجة إلى آليات جديدة للتعرف على الأفراد والكيانات في بيئة لا مركزية وغير موثوقة. وقد أدت هذه الحاجة إلى ولادة أولى

صور الهوية الرقمية، مثل كلمات المرور، وأرقام التعريف الفريدة، والشهادات الرقمية.

في المرحلة الأولى، كان التركيز منصباً على الجوانب الأمنية والتقنية، دون إيلاء الاعتبار الكافي للأبعاد القانونية. وكان التشريع يسير خلف التطور التقني بخطوات بطيئة، مما خلق فجوة تشريعية واسعة. غير أن ظهور التجارة الإلكترونية في أواخر التسعينيات دفع الدول إلى سن قوانين تنظم التعاملات الرقمية، ومن بينها قوانين التوقيع الإلكتروني، التي شكلت حجر الزاوية الأول في الاعتراف القانوني بالهوية الرقمية. فقد نصت اتفاقية الأمم المتحدة بشأن استخدام الخطابات الإلكترونية في العقود التجارية عام 2005، وكذلك توجيه الاتحاد الأوروبي رقم EC/93/1999، على مبدأ الاعتراف القانوني بالتوقيعات الإلكترونية، ما منح الهوية الرقمية أولى درجات الشرعية القانونية.

وفي الولايات المتحدة، سار التشريع على خطى مماثلة، إذ صدر قانون التوقيع الإلكتروني في المعاملات العالمية والوطنية (E-SIGN Act) عام 2000، والذي أقرّ بأن السجلات والتوقيعات الإلكترونية لها نفس القوة القانونية كالسجلات والتوقيعات الورقية. أما في العالم العربي، فقد تأخر الاعتراف القانوني بالهوية الرقمية نسبياً، حيث لم تبدأ الدول العربية في سن تشريعات متكاملة إلا في أوائل العقد الأول من القرن الحادي والعشرين. ومن أبرز الأمثلة على ذلك قانون المعاملات الإلكترونية في الإمارات العربية المتحدة عام 2006، وقانون التوقيع الإلكتروني في تونس عام 2004، وقانون تكنولوجيا المعلومات في مصر عام 2004.

ومع تصاعد استخدام الشبكات الاجتماعية والخدمات السحابية في العقد الثاني من القرن الحادي والعشرين، توسعت مفاهيم الهوية الرقمية لتشمل ليس فقط هوية المستخدم

الرسمية، بل أيضاً هويته السلوكية، المبنية على تتبع أنشطته وتفاعله مع المحتوى الرقمي. وقد أدى هذا التوسع إلى ظهور تحديات قانونية جديدة، خاصة في مجالات الخصوصية، وحماية البيانات، والمسؤولية المدنية عن الاستخدام غير المشروع للمعلومات الشخصية.

وقد مثلت اللائحة العامة لحماية البيانات (GDPR) التي دخلت حيز التنفيذ في الاتحاد الأوروبي عام 2018 نقطة تحول جوهرية في تاريخ الهوية الرقمية من منظور قانوني. فلأول مرة، تم ربط الهوية الرقمية بحقوق أساسية للمواطن، مثل الحق في النسيان، والحق في نقل البيانات، والحق في عدم الخضوع لقرارات آلية. 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 Carpenter ضد الولايات المتحدة عام 2018، أكدت على أن البيانات الرقمية المتعلقة بالهوية تستحق حماية دستورية بموجب التعديل الرابع.

وبالنسبة للدول العربية، فإن التطور التاريخي للهوية الرقمية لا يزال في طور التشكل. فبينما أطلقت بعض الدول مشاريع طموحة للهوية الرقمية الموحدة، مثل مشروع الهوية الرقمية في السعودية ومصر، 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 الهوية الرقمية 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 للهوية الرقمية في القانون المدني

يستند التنظيم القانوني لأي كيان جديد إلى مجموعة من الأُسس النظرية التي تمنحه شرعيته وتحدد موقعه داخل النظام القانوني. وفي حالة الهوية الرقمية، فإن هذه الأُسس ليست وليدة اليوم، بل تستمد جذورها من مبادئ قانونية كلاسيكية في القانون المدني، مثل مبدأ الشخصية القانونية، ومبدأ حرمة الحياة الخاصة، ومبدأ المسؤولية عن الضرر. غير أن طبيعة الهوية الرقمية الفريدة تتطلب إعادة

تفسير هذه المبادئ وتوظيفها في سياق جديد، يتميز بالسرعة، واللامركزية، والعالمية.

أولاً، يتعلق الأمر بمبدأ الشخصية القانونية. فالقانون المدني التقليدي يربط الشخصية القانونية بوجود طبيعي أو اعتباري ملموس. ولكن الهوية الرقمية، رغم عدم ملموسيتها، تمثل هذا الوجود في الفضاء الإلكتروني. ولذلك، فإن الاعتراف بها كتجسيد للشخصية القانونية في البيئة الرقمية هو خطوة ضرورية لضمان اتساق النظام القانوني. وقد بدأ بعض الفقه الأوروبي في الحديث عن الشخصية الرقمية كامتداد ضروري للشخصية القانونية، وليس ككيان منفصل عنها.

ثانياً، يأتي مبدأ حرمة الحياة الخاصة، الذي يُعد من الركائز الأساسية في معظم التشريعات المدنية الحديثة. فالهوية الرقمية تحتوي على كم هائل من المعلومات الشخصية، التي إذا

استُخدمت دون إذن، فإنها تشكل انتهاكاً صارخاً لهذا المبدأ. وقد أكدت محكمة العدل الأوروبية مراراً أن أي معالجة للبيانات الشخصية تُعد تدخلاً في الحق في الحياة الخاصة، ما لم تكن مبررة قانوناً. وهذا المبدأ يكتسب أهمية خاصة في البيئة الرقمية، حيث يصعب على الفرد مراقبة كيفية استخدام بياناته.

ثالثاً، يبرز مبدأ المسؤولية عن الضرر. ففي حال انتحال الهوية الرقمية 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 الهوية؟ أم مزوّد الخدمة؟ أم جهة التحقق؟ إن غياب قواعد واضحة في هذا المجال يؤدي إلى فراغ قانوني يعرّض حقوق الأفراد للخطر.

رابعاً، هناك مبدأ الثقة المشروعة. فعندما يعتمد شخص على هوية رقمية معينة في إبرام عقد أو

إجراء معاملة، فإنه يفترض أن هذه الهوية صحيحة وموثوقة. وإذا ثبت العكس، فإن القانون المدني يجب أن يحمي هذا الاعتماد المشروع، ويضمن تعويض المتضرر. وهذا المبدأ يكتسب أهمية خاصة في المعاملات العابرة للحدود، حيث يصعب التحقق من الهوية يدوياً.

خامساً، يظهر مبدأ المساواة أمام القانون. فلا يجوز أن يُعامل الشخص الذي يمتلك هوية رقمية معتمدة معاملة مختلفة عن الشخص الذي لا يمتلكها، إلا إذا كان هناك مبرر قانوني وجيه. كما لا يجوز أن تُستخدم الهوية الرقمية كأداة للتمييز أو الاستبعاد الاجتماعي.

ومن خلال هذه الأُسس النظرية، يتضح أن الهوية الرقمية 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 للهوية الرقمية.

## الفصل الرابع
## عناصر الهوية الرقمية وخصائصها القانونية

لا تُشكل الهوية الرقمية 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 الهوية الرقمية إلى ثلاثة مستويات رئيسية: العناصر التعريفية، والعناصر الوثائقية، والعناصر السلوكية.

أولاً، العناصر التعريفية: وهي تلك البيانات الأساسية التي تميّز الشخص في الفضاء الرقمي، مثل الاسم الكامل، رقم الهوية الوطنية أو جواز السفر، تاريخ الميلاد، الجنسية، وعنوان البريد الإلكتروني الرسمي. وهذه العناصر تُعد بمثابة العمود الفقري للهوية الرقمية، لأنها تربط الكيان الرقمي بالشخص الحقيقي في العالم المادي. ومن الناحية القانونية، فإن هذه العناصر تخضع لقواعد صارمة تتعلق بالصحة والدقة والتحديث. فمثلاً، لا يُعتد قانوناً بهوية رقمية تعتمد على اسم مستعار دون ربطه بهوية حقيقية معتمدة، خاصة في المعاملات ذات الأثر القانوني.

ثانياً، العناصر الوثائقية: وتشمل الشهادات الرقمية، التوقيعات الإلكترونية المؤهلة، والبيانات البيومترية (كالبصمة، ومسح الوجه، وقزحية العين). وهذه العناصر تلعب دوراً حاسماً في إثبات صحة الهوية وموثوقيتها. فالشهادة الرقمية،

على سبيل المثال، تصدر عن جهة موثوقة معتمدة قانوناً، وتُستخدم للتحقق من أن صاحب الهوية هو من يدّعي أنه كذلك. أما التوقيع الإلكتروني المؤهل، فقد اكتسب قوة قانونية مساوية للتوقيع الورقي في العديد من التشريعات، مثل توجيه الاتحاد الأوروبي eIDAS. ومن الناحية القانونية، فإن هذه العناصر تتمتع بحماية خاصة، إذ يُجرّم القانون أي تزوير أو انتحال لها، ويُحمّل الجهات المصدرة مسؤولية مدنية في حال إصدارها لهوية غير صحيحة.

ثالثاً، العناصر السلوكية: وهي تلك البيانات التي تُجمع من خلال تتبع سلوك المستخدم في الفضاء الرقمي، مثل سجلات التصفح، أنماط الكتابة، مواقع الدخول، وتفاعلات الشبكات الاجتماعية. وعلى الرغم من أن هذه العناصر لا تُستخدم عادةً في إثبات الهوية الرسمية، إلا أنها أصبحت أداة فعالة في أنظمة التحقق المتعدد العوامل (Multi-factor Authentication).

ومن الناحية القانونية، فإن هذه العناصر تثير إشكاليات كبيرة تتعلق بالخصوصية وحقوق الملكية الفكرية. فهل يملك الفرد حقاً في منع جمع هذه البيانات؟ وهل يُعتبر استخدامها دون موافقته انتهاكاً للحق في الحياة الخاصة؟ إن الإجابة على هذه الأسئلة تتطلب تحديداً دقيقاً لطبيعة العلاقة القانونية بين صاحب الهوية ومزوّد الخدمة.

أما من حيث الخصائص القانونية، فإن الهوية الرقمية تتميز بعدة سمات جوهرية:

1. الطابع الثنائي: فهي تجمع بين البُعد التقني (كالرمز الرقمي) والبُعد القانوني (كالاعتراف الرسمي بها).
2. القابلية للنقل: إذ يمكن استخدامها عبر منصات وخدمات متعددة، ما لم يُقيّدها القانون.
3. القابلية للتفكيك: حيث يمكن فصل بعض عناصرها عن البعض الآخر حسب الغرض من

الاستخدام.
4. الاستمرارية الزمنية: فهي لا تنتهي بانتهاء جلسة استخدام، بل تبقى قائمة طالما لم تُلغَ رسمياً.
5. القابلية للرقابة القضائية: إذ يحق لأي شخص الطعن في صحة هويته الرقمية 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 للهوية الرقمية، يضمن حماية الحقوق، ويعزز الثقة في المعاملات

الرقمية، ويواكب التطورات العالمية دون إخلال بالمبادئ الأساسية للقانون المدني.

## الفصل الخامس
## العلاقة بين الهوية الرقمية والشخصية القانونية

تُعد العلاقة بين الهوية الرقمية والشخصية القانونية من القضايا الجوهرية التي تحدد موقع الهوية الرقمية داخل النظام القانوني المدني. فبينما تُعتبر الشخصية القانونية مفهوماً تقليدياً راسخاً في جميع التشريعات المدنية، فإن الهوية الرقمية تمثل تجسيداً جديداً لهذه الشخصية في بيئة غير مادية، مما يثير تساؤلات عميقة حول طبيعة هذه العلاقة: هل الهوية الرقمية مجرد أداة لإثبات الشخصية؟ أم أنها كيان قانوني مستقل يستمد وجوده منها؟ أم أنها امتداد طبيعي لها في العصر الرقمي؟

من الناحية النظرية، تُعرّف الشخصية القانونية

بأنها الأهلية التي يتمتع بها الشخص الطبيعي أو الاعتباري لممارسة الحقوق وتحمل الواجبات. وهي تبدأ من لحظة الولادة للشخص الطبيعي، ومن تاريخ التأسيس للشخص الاعتباري، ولا تنتهي إلا بالوفاة أو الانقضاء. أما الهوية الرقمية، فهي لا تنشأ تلقائياً، بل تتطلب إجراءات إنشاء وتوثيق عبر جهات معتمدة، وقد تُلغى أو تُعلّق دون أن تنتهي الشخصية القانونية ذاتها. وهذا الفارق الجوهر يدفع إلى القول إن الهوية الرقمية ليست هي الشخصية القانونية، بل هي وسيلة رقمية لتمثيلها.

غير أن هذا التمثيل ليس مجرد انعكاس سلبي، بل هو تفاعل دينامي يحمل آثاراً قانونية مباشرة. فمثلاً، عندما يُبرم عقد إلكتروني باسم هوية رقمية معتمدة، فإن الآثار القانونية لهذا العقد تنسحب على صاحب الشخصية القانونية المرتبطة بتلك الهوية. وبالتالي، فإن الهوية الرقمية تكتسب قوة قانونية مشتقة من

الشخصية، لكنها في الوقت نفسه تُضفي على هذه الشخصية بعداً رقمياً جديداً، يُمكن من خلاله ممارسة الحقوق والتزام الواجبات في الفضاء الإلكتروني.

ومن هنا، تبرز الحاجة إلى مبدأ "الربط القانوني" بين الهوية الرقمية والشخصية القانونية. فلكي تكون الهوية الرقمية ذات أثر قانوني، يجب أن تكون مرتبطة بشكل لا لبس فيه بشخصية قانونية قائمة. ويتم هذا الربط عادةً عبر وثائق رسمية (كبطاقة الهوية أو جواز السفر) وبيانات بيومترية، ويتم توثيقه من قبل جهات موثوقة معتمدة قانوناً. وفي حال انقطاع هذا الربط — كأن تُستخدم هوية رقمية مسروقة أو مزورة — فإن المعاملات التي تتم باسمها تكون قابلة للإبطال، ما لم يثبت حسن نية الطرف الآخر.

ويختلف التعامل مع هذه العلاقة باختلاف النظام القانوني. ففي الاتحاد الأوروبي، يُنظر إلى

الهوية الرقمية كجزء من الحق في الخصوصية، وبالتالي كحق شخصي مرتبط ارتباطاً وثيقاً بالشخصية القانونية. وقد أكدت محكمة العدل الأوروبية أن أي معالجة للهوية الرقمية دون موافقة صاحبها تُعد انتهاكاً لكرامته الإنسانية. أما في الولايات المتحدة، فإن التركيز يكون أكثر على الجوانب التعاقدية والأمنية، حيث تُعتبر الهوية الرقمية أداة لإثبات الرضا والموافقة في المعاملات الإلكترونية.

وفي العالم العربي، لا تزال العلاقة بين الهوية الرقمية والشخصية القانونية غامضة في العديد من التشريعات. فبعض القوانين تقتصر على الاعتراف بالتوقيع الإلكتروني دون تحديد طبيعة العلاقة بينه وبين الشخصية القانونية. 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 "الشخصية الرقمية"

ضمن قواعد القانون المدني، ويُحدد بدقة شروط ارتباطها بالشخصية القانونية، وآثار هذا الارتباط على الحقوق والواجبات.

ومن الجدير بالذكر أن ظهور الكيانات الافتراضية (مثل الحسابات الذكية أو الوكلاء الرقميين) يطرح تحديات جديدة لهذه العلاقة. فهل يمكن لكيان رقمي غير بشري أن يمتلك هوية رقمية؟ وإذا كان كذلك، فهل يُنسب إليه شخصية قانونية؟ إن الإجابة على هذه الأسئلة تتطلب إعادة النظر في مفاهيم أساسية في القانون المدني، مثل الإرادة، والمسؤولية، والأهلية.

وفي الختام، يمكن القول إن الهوية الرقمية ليست بديلاً عن الشخصية القانونية، بل هي وعاء رقمي لها، يُمكّنها من الوجود والتفاعل في العصر الرقمي. ولذلك، فإن أي تنظيم قانوني فعال للهوية الرقمية يجب أن ينطلق من فهم عميق لهذه العلاقة، ويضمن أن تظل الشخصية

القانونية هي المصدر الوحيد للحقوق والواجبات، حتى في الفضاء الإلكتروني.

## الفصل السادس
## الإطار التشريعي العربي للهوية الرقمية

يُشكل الإطار التشريعي العربي للهوية الرقمية 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 بالهوية الرقمية، 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

أصدرت بعض الدول قوانين المعاملات الإلكترونية أو التوقيع الإلكتروني. ومن أبرز هذه التشريعات: قانون التجارة الإلكترونية في الإمارات العربية المتحدة لعام 2006، وقانون التوقيع الإلكتروني في تونس لعام 2004، وقانون إنشاء مركز المعلومات الوطني في مصر لعام 2004، وقانون تكنولوجيات الإعلام والاتصال في الجزائر لعام 2009. غير أن هذه القوانين ركزت في جوهرها على إضفاء الصفة القانونية على الوثائق والتوقيعات الإلكترونية، دون أن تتناول الهوية الرقمية 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 الرقمية الموحدة، مثل "الهوية الرقمية الوطنية" في المملكة العربية السعودية، و"بطاقة الهوية الرقمية" 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 للهوية الرقمية. وهذا التفاوت يُعقّد من مسألة الاعتراف المتبادل بالهويات الرقمية عبر الحدود العربية.

ثانياً، الهيمنة الأمنية على الخطاب التشريعي.

فمعظم التشريعات العربية تُدرج موضوع الهوية الرقمية 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 هوية رقمية مزورة، لكنه لا يُفصّل في آليات التعويض المدني للضحايا.

ثالثاً، غياب التكامل مع قواعد القانون المدني العام. فنادراً ما تشير قوانين الهوية الرقمية 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 الهوية الرقمية وحقوق الملكية على البيانات الشخصية. كما أن آليات الرقابة القضائية على جهات إصدار الهويات الرقمية لا تزال محدودة.

خامساً، عدم وجود آلية موحدة للاعتماد والاعتراف المتبادل. فكل دولة عربية تضع معاييرها الخاصة لإصدار الهويات الرقمية، 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 بالهوية الرقمية، تُراعي المبادئ التالية:
- الاعتراف بالهوية الرقمية ككيان قانوني مدني

مستقل
- ربطها صراحةً بالشخصية القانونية في قوانين المدني
- تحديد حقوق والتزامات أصحاب الهويات الرقمية
- 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 للهوية الرقمية 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 الهوية الرقمية في دول مجلس التعاون الخليجي

يمثّل مجلس التعاون لدول الخليج العربية

نموذجاً متقدماً نسبياً في المنطقة العربية من حيث التبني التشريعي والتنفيذي لمفهوم الهوية الرقمية. فقد سارعت دول المجلس إلى دمج هذا المفهوم ضمن رؤاها الوطنية للتحول الرقمي، ووضعت تشريعات وبنى تحتية تدعم وجود هويات رقمية 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. وعلى الرغم من التقدم الكبير، فإن القانون الإماراتي لا يحتوي على فصل مستقل ينظم الهوية الرقمية 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. 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 الهوية الرقمية

والشخصية القانونية 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. لكن التشريع القطري، شأنه شأن غيره، يفتقر إلى مواد مدنية تُنظّم المسؤولية التقصيرية عن انتحال الهوية 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 الهوية الرقمية 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. ومع ذلك، فإن التشريع العماني لا يحتوي على أحكام مدنية مفصلة تتعلق بإثبات صحة الهوية الرقمية 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 الهوية الرقمية وقواعد المسؤولية المدنية في القانون البحريني.

ومن خلال هذه المقارنة، يتضح أن دول مجلس التعاون قد حققت تقدماً كبيراً في البنية التحتية والاعتماد الحكومي للهوية الرقمية، 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 الهوية
- حق الضحية في التعويض عن الضرر المعنوي والمادي
- حماية البيانات الشخصية المرتبطة بالهوية
- آليات الطعن في قرارات إلغاء أو تعليق الهوية

ولذلك، فإن الخطوة التالية أمام دول المجلس يجب أن تكون سنّ قوانين مدنية خاصة أو تعديل قوانين المدني الحالية لتضمّن أحكاماً صريحة تنظّم الهوية الرقمية من منظور مدني شامل، بما يتماشى مع أعلى المعايير العالمية، ويُعزّز ثقة الأفراد في الفضاء الرقمي.

## الفصل الثامن
## التنظيم القانوني للهوية الرقمية في الدول العربية غير الخليجية

بينما تشهد دول مجلس التعاون الخليجي زخماً تشريعياً وتنفيذياً في مجال الهوية الرقمية، 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 للهوية الرقمية. وقد أطلقت الدولة "منصة الهوية الرقمية" في 2021، التي تتيح للمواطنين استخدام هويتهم الوطنية في التعامل مع الجهات الحكومية والإلكترونية. غير أن هذا الإطار يعاني من فجوة مدنية واضحة: فقانون حماية البيانات لا ينظم العلاقة بين الهوية الرقمية والشخصية القانونية، وقانون الجرائم الإلكترونية يركز على العقوبات دون تحديد آليات التعويض المدني. كما أن قانون المدني المصري

لم يُعدّل ليشمل أحكاماً خاصة بالهوية الرقمية، 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. لكن التشريع الجزائري لا يحتوي على أي تنظيم مدني مباشر للهوية الرقمية، بل يكتفي بالإشارة إلى أدواتها التقنية. ويبقى الفرد الجزائري دون حماية قانونية كافية في حال انتحال هويته الرقمية أو استخدام بياناته 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. ويتميز التشريع التونسي بوجود هيئة مستقلة (الهيئة الوطنية للبريد الإلكتروني والتوقيع الإلكتروني)، لكنه يفتقر إلى ربط صريح بين الهوية الرقمية وقواعد المسؤولية المدنية في مجلة الالتزامات والعقود. فمثلاً، لا توجد أحكام تُنظّم حالات الغلط في إبرام العقود عبر هوية رقمية 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. ومع ذلك، فإن التشريع الأردني لا يزال ينظر إلى الهوية الرقمية من زاوية تقنية وأمنية، دون تناول

كافٍ لآثارها المدنية. فمثلاً، لا توجد أحكام تُنظّم حق الفرد في تصحيح بياناته الرقمية أو حذفها، ولا تُفصّل في المسؤولية المدنية للجهات التي تفشل في حماية الهويات الرقمية 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. ويُلاحظ أن المغرب بدأ مؤخراً في تطوير قانون حماية البيانات الشخصية، لكنه لم يُدمج بعد مفاهيم الهوية الرقمية ضمن قواعد القانون المدني. وبالتالي، تظل الحماية المدنية للهوية الرقمية 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 الهويات
- عدم وجود نصوص صريحة تُنظم المسؤولية المدنية عن الأضرار الناتجة عن اختراق الهوية

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

الرقمي.

## الفصل التاسع
## الحماية المدنية للهوية الرقمية في النظام القانوني المصري

يُعد النظام القانوني المصري من الأنظمة التي بدأت مبكراً في ملامسة مفاهيم الهوية الرقمية، سواء من خلال البنية التشريعية أو المبادرات التنفيذية. ومع ذلك، فإن الحماية المدنية للهوية الرقمية 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 الهوية الرقمية (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 الهوية الرقمية ككيان قانوني

مستقل، ولا على العلاقة بينها وبين الشخصية القانونية في القانون المدني.

ومن الناحية التطبيقية، أطلقت الدولة "منصة الهوية الرقمية" في 2021، التي تتيح للمواطنين استخدام هويتهم الوطنية الرقمية 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 الهوية الرقمية. فمثلاً، لا تشير المواد المتعلقة بالإرادة (كالمادة 109 من القانون المدني) إلى حالات التدليس الإلكتروني أو الغلط الناتج عن انتحال الهوية الرقمية. كما أن

قواعد المسؤولية التقصيرية (المواد 163 وما يليها) لا تتناول بشكل خاص الأضرار الناتجة عن اختراق الهوية الرقمية 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 بالهوية الرقمية ككيان مدني: فالتشريعات الحالية تتعامل معها كأداة تقنية، لا كتجسيد للشخصية القانونية في الفضاء الرقمي.
2. عدم تحديد المسؤولية المدنية لجهات الإصدار: ففي حال اختراق الهوية الرقمية 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 هويته.
4. غياب حق التصحيح والحذف الفعّال: فرغم وجوده في قانون حماية البيانات، إلا أن تطبيقه على الهوية الرقمية يفتقر إلى الآليات العملية والرقابة القضائية.

ولمعالجة هذه الثغرات، يُقترح ما يلي:
- تعديل قانون المدني المصري لإضافة فصل خاص بالهوية الرقمية، يُنظم علاقتها بالشخصية القانونية، ويُحدد شروط صحتها، وآثار انتحالها.
- إدخال نصوص في قانون حماية البيانات تُفصّل في حقوق أصحاب الهويات الرقمية، والتزامات الجهات المصدرة.
- إنشاء آلية قضائية متخصصة للنظر في النزاعات المتعلقة بالهوية الرقمية، تضم خبراء تقنيين وقانونيين.
- تضمين شروط استخدام منصة الهوية الرقمية

بنوداً ملزمة تحمي حقوق المستخدم وتُحدّد مسؤوليات الجهة المُصدرة.

إن تطوير الحماية المدنية للهوية الرقمية 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 للهوية الرقمية 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 للهوية الرقمية في البلاد. ومع ذلك، فإن الحماية المدنية للهوية الرقمية 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 هوياتهم الرقمية.

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. 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 الهوية الرقمية والشخصية القانونية، ولا يُفصّل

في المسؤولية المدنية الناتجة عن انتحال الهوية أو سوء استخدامها.

ومن منظور القانون المدني الجزائري، لا توجد أي مواد صريحة تتناول الهوية الرقمية. 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 الهوية الرقمية. 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 للهوية الرقمية: فالتشريع الجزائري لا يعرّف الهوية

الرقمية 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 هويته الرقمية.

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

ولمعالجة هذه الثغرات، يُقترح ما يلي:

- إدخال تعديلات على القانون المدني الجزائري لإضافة أحكام خاصة بالهوية الرقمية، تُنظم علاقتها بالشخصية القانونية، وتُحدد شروط صحتها، وآثار انتحالها.
- سن قانون خاص بالهوية الرقمية يدمج بين الجوانب التقنية والمدنية، ويُحدّد التزامات الجهات المصدرة، وحقوق أصحاب الهويات.
- الإسراع في إصدار قانون حماية البيانات الشخصية، وضمان تضمينه أحكاماً تُطبّق صراحةً على الهوية الرقمية.
- إنشاء وحدة قضائية متخصصة داخل المحاكم للنظر في النزاعات المتعلقة بالهوية الرقمية، تضم خبراء في القانون المدني والتكنولوجيا.

إن تطوير الحماية المدنية للهوية الرقمية 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 بالهوية الرقمية في العالم العربي

لا يمكن فصل التنظيم المدني للهوية الرقمية 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 الهوية الرقمية. ومع ذلك، فإن هذه المبادئ لا تزال عامة وغير محددة، ولا توجد دساتير عربية صريحة تعترف بالهوية الرقمية كحق دستوري مستقل. ويهدف هذا الفصل إلى تحليل هذه المبادئ، واستخلاص آثارها على الحماية

المدنية للهوية الرقمية.

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 الهوية الرقمية أصبحت جزءاً لا يتجزأ من وجود الفرد في العصر الرقمي، 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 الهويات الرقمية.

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 الهوية الرقمية تحتوي على بيانات شخصية حساسة، 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 الهوية الرقمية 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 الهوية الرقمية كأداة للتمييز أو الاستبعاد الاجتماعي. فمثلاً، لا يجوز حرمان شخص من خدمة عامة لمجرد عدم امتلاكه هوية رقمية، ما لم يكن هناك بديل معقول. كما يُلزم الدولة بضمان وصول الجميع إلى الهوية الرقمية دون تمييز.

خامساً، مبدأ سيادة القانون: يُعد هذا المبدأ ركيزة أساسية في جميع الدساتير العربية. وهو يقتضي أن تكون جميع إجراءات إصدار الهوية الرقمية، واستخدامها، وإلغائها، خاضعة للقانون، وقابلة للطعن أمام القضاء. فلا يجوز أن تُدار

الهوية الرقمية عبر قرارات إدارية منفردة دون رقابة قضائية.

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

- عمومية النصوص: فمعظم الدساتير لا تذكر "الهوية الرقمية" صراحةً، مما يترك مجالاً واسعاً للتفسير.
- ضعف الرقابة الدستورية: فقلة من المحاكم الدستورية العربية تناولت قضايا مرتبطة بالهوية الرقمية، ما يحد من تطور الاجتهاد الدستوري في هذا المجال.
- غياب التشريعات المنفذة: فحتى عندما توجد مبادئ دستورية، فإن غياب القوانين المدنية المنظِّمة يُضعف من قدرتها على توفير حماية فعلية.

ولذلك، يُوصى بما يلي:

- تعديل الدساتير العربية لإدراج نص صريح يعترف بالهوية الرقمية كجزء من كرامة الإنسان وحقه في الخصوصية.
- تفعيل دور المحاكم الدستورية في مراجعة التشريعات المتعلقة بالهوية الرقمية، والتأكد من توافقها مع المبادئ الدستورية.
- ربط التشريعات المدنية الخاصة بالهوية الرقمية صراحةً بالمبادئ الدستورية، لضمان أعلى درجات الحماية.

إن الاعتراف الدستوري بالهوية الرقمية ليس ترفاً قانونياً، بل هو ضرورة في عصر أصبحت فيه الهوية الرقمية 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 للهوية الرقمية

يُعد النظام القانوني الأمريكي من الأنظمة الفريدة في معالجته للهوية الرقمية، 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 الهوية الرقمية فيه معقدة لكنها غنية بالتجارب العملية.

على المستوى الفيدرالي، يُعد قانون التوقيع الإلكتروني في المعاملات العالمية والوطنية (E-SIGN Act) لعام 2000 حجر الزاوية الأول. فقد نصّ هذا القانون على أن "السجلات والتوقيعات

الإلكترونية لها نفس القوة القانونية كالسجلات والتوقيعات الورقية"، ما منح الهوية الرقمية أول اعتراف قانوني رسمي. غير أن القانون لم يُعرّف الهوية الرقمية بشكل صريح، بل ركّز على مبدأ "الموافقة الواعية" (Informed Consent) كشرط لصحة المعاملات الإلكترونية.

وفي عام 2002، صدر قانون سياسة الخصوصية للبيانات الحكومية (Privacy Act Amendments)، ثم تبعه قانون حماية خصوصية الإنترنت للأطفال (COPPA)، وقانون HIPAA لحماية البيانات الصحية. ومع أن هذه القوانين لا تتناول الهوية الرقمية مباشرة، إلا أنها وضعت قيوداً على جمع واستخدام البيانات الشخصية، التي تُشكل جوهر الهوية الرقمية.

أما على مستوى الولايات، فتتفاوت التشريعات بشكل كبير. فمثلاً، في كاليفورنيا، صدر قانون خصوصية المستهلك (CCPA) لعام 2018، الذي

منح الأفراد حق معرفة البيانات التي تجمعها الشركات عنهم، وحق حذفها، وحق رفض بيعها. وقد تم تعزيزه لاحقاً بـ CPRA في 2020، الذي أنشأ وكالة تنظيمية مستقلة لحماية البيانات. وفي نيويورك، صدر قانون حماية الهوية (SHIELD Act) لعام 2019، الذي فرض التزامات صارمة على الشركات لحماية بيانات الهوية، ونص على إشعار الضحايا في حال الاختراق.

ومن الناحية القضائية، لعبت المحاكم الأمريكية دوراً محورياً في تشكيل مفهوم الهوية الرقمية. ففي قضية Carpenter v. United States (2018)، أكدت المحكمة العليا أن "البيانات المتعلقة بموقع الهاتف المحمول تُعد جزءاً من الحياة الخاصة"، ولا يجوز للسلطات الوصول إليها دون أمر قضائي. وفي قضية Riley v. California (2014)، اعتبرت المحكمة أن "الهواتف الذكية تحتوي على هوية رقمية كاملة"، ولا يجوز تفتيشها دون إذن قضائي. وهذه الأحكام

رسّخت مبدأ أن الهوية الرقمية جزء من الحقوق الدستورية المحمية.

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

1. المسؤولية التعاقدية: فعند استخدام الهوية الرقمية في إبرام عقود، يُطبّق قانون العقود (Contract Law)، ويُنظر إلى أي انتحال كغش أو تدليس يُبرر إبطال العقد.
2. المسؤولية التقصيرية: ففي حال سرقة الهوية الرقمية، 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 تسمح بمنح تعويضات رادعة (Punitive Damages) في حالات الاستغلال الجسيم للهوية الرقمية.

ومع ذلك، يعاني النظام الأمريكي من تحديات رئيسية:

- التشتت التشريعي: فاختلاف القوانين بين الولايات يُعقّد من حماية الهوية الرقمية 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 لحماية البيانات: 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 للهوية الرقمية ضمن إطار قانوني دينامي وعملي.

## الفصل الثالث عشر
## المسؤولية المدنية في القانون الأمريكي عن انتهاك الهوية الرقمية

في ظل غياب قانون مدني موحد في الولايات المتحدة، تستند المسؤولية المدنية عن انتهاك الهوية الرقمية إلى شبكة معقدة من القواعد المشتقة من القانون العام (Common Law)، والتشريعات الفيدرالية والولائية، والممارسات القضائية. ورغم عدم وجود نص يُسمّى "الهوية الرقمية" صراحةً، 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 الهوية الرقمية. ولإثبات الإهمال، يجب على المدعي إثبات أربعة عناصر:
1. وجود واجب قانوني على المدعى عليه لحماية بيانات الهوية (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 Pisciotta v. Old National Bancorp (2007) أن المؤسسات التي تجمع بيانات هوية حساسة تتحمل واجباً قانونياً بحمايتها، حتى لو لم يكن هناك تشريع صريح يفرض ذلك. كما أن العديد من الولايات، مثل كاليفورنيا وتكساس،

اعترفت صراحةً بأن الإخفاق في تطبيق معايير أمنية معقولة يُعد إهمالاً مدنياً.

ثانياً، المسؤولية التعاقدية (Contractual Liability):
عند استخدام الهوية الرقمية في المعاملات التجارية، يُطبّق قانون العقود. فإذا استخدم طرف هوية 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 الهوية الرقمية. فمثلاً، ينص قانون

كاليفورنيا SHIELD Act على أن أي جهة تخضع لاختراق بيانات يجب أن تُبلغ المتضررين فوراً، وإلا تُعتبر مسؤولة مدنياً عن الأضرار الناتجة عن التأخير. كما يمنح قانون CCPA الحق في رفع دعاوى جماعية (Class Actions) في حالات الانتهاك الجسيم.

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.
- 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 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 الهوية الرقمية، 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 الهوية الرقمية

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 الهوية الرقمية، لعبت المحاكم الأمريكية — من المحكمة العليا إلى محاكم الولايات — دوراً رياديًا في تحديد طبيعة هذه الهوية، 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:
في قضية Riley v. California (2014)، أصدرت المحكمة العليا حكماً تاريخياً اعتبر أن "الهاتف الذكي ليس مجرد جهاز اتصال، بل هو حافظة رقمية تحتوي على هوية الفرد الكاملة". وبناءً عليه، قضت المحكمة بأنه لا يجوز للشرطة تفتيش محتويات الهاتف دون أمر قضائي، حتى لو كان الشخص معتقلاً. وقد شكّل هذا الحكم نقطة تحول، إذ اعترف لأول مرة بأن الهوية الرقمية جزء من الحياة الخاصة المحمية دستورياً بموجب التعديل الرابع.

وفي قضية Carpenter v. United States (2018)، وسّعت المحكمة العليا من هذا المفهوم، مؤكدة أن "بيانات الموقع الجغرافي

التي تجمعها شركات الاتصال عن الهواتف تمثل سجلاً دقيقاً للحياة اليومية"، ولا يجوز للسلطات الوصول إليها دون أمر قضائي. وقد استندت المحكمة إلى أن هذه البيانات تُشكّل جزءاً من الهوية السلوكية للفرد، وبالتالي فهي محمية دستورياً.

ثانياً، محاكم الاستئناف الفيدرالية:
في قضية In re: Equifax Inc. Customer Data Security Breach Litigation (2019)، اعترفت محكمة الاستئناف بالدائرة الحادية عشرة بأن "الإخفاق في حماية بيانات الهوية يُعد إهمالاً مدنياً"، حتى لو لم يُسفر الاختراق فوراً عن سرقة أموال. ووافقت المحكمة على دعوى جماعية ضد شركة Equifax بعد اختراق بيانات 147 مليون شخص، مما فتح الباب أمام تعويضات واسعة النطاق.

وفي قضية Pisciotta v. Old National Bancorp

2007))، أكدت محكمة الاستئناف بالدائرة السابعة أن المؤسسات المالية التي تجمع بيانات هوية حساسة تتحمل "واجب عناية" (Duty of Care) قانونياً، وأن الإخفاق في تطبيق معايير أمنية معقولة يُعد أساساً كافياً لدعوى إهمال مدني.

ثالثاً، محاكم الولايات:
في كاليفورنيا، أصدرت محكمة المقاطعة حكماً في قضية Facebook Biometric Information Privacy Litigation (2021)، اعتبرت فيه أن "جمع بصمات الوجه دون موافقة صريحة يُعد انتهاكاً لهوية الفرد البيومترية"، وفرضت تعويضات جماعية تجاوزت 650 مليون دولار. وقد استند الحكم إلى قانون خصوصية المعلومات البيومترية في إلينوي (BIPA)، الذي أصبح مرجعاً وطنياً.

وفي نيويورك، قضت محكمة عليا في قضية People v. Weaver (2009) بأن تتبع موقع

الهاتف دون إذن قضائي يُعد "تفتيشاً غير معقول"، ويُخالف الدستور، ما عزّز من حماية الهوية السلوكية.

رابعاً، الآليات القضائية المبتكرة:
تميّزت المحاكم الأمريكية باستخدام آليات مرنة لحماية الهوية الرقمية، منها:
- الأوامر الزجرية المؤقتة (Preliminary Injunctions): لوقف استخدام هوية مسروقة 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 الهوية الرقمية، بل سبقه بخطوات، ورسّخ مبادئ قانونية راسخة تجعل من الهوية الرقمية حقاً مدنياً محمياً، لا مجرد بيانات تقنية. وهذا النهج القضائي النشط يُعد درساً مهماً للأنظمة القانونية الأخرى، التي قد تتردد في الاعتراف بالهوية الرقمية ككيان قانوني مستقل.

الفصل الخامس عشر

## النظام القانوني الأوروبي للهوية الرقمية

يمثّل النظام القانوني الأوروبي نموذجاً رائداً في التنظيم المدني للهوية الرقمية، 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 الهوية 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". وقسّم الهويات الرقمية إلى ثلاثة مستويات:
- منخفضة (Low): للمعاملات غير الحساسة.
- متوسطة (Substantial): للمعاملات الإدارية.
- عالية (High): للمعاملات ذات الأثر القانوني الكبير، مثل العقود أو المعاملات المالية.

كما أنشأ التوجيه نظاماً لاعتماد جهات التصديق الموثوقة (Qualified Trust Service Providers)، التي تُصدر شهادات رقمية مؤهلة، تتمتع بقوة قانونية مساوية للتوقيع الورقي. وهذا يضمن أن الهوية الرقمية ليست مجرد بيانات، بل كيان قانوني معتمد.

ثانياً، اللائحة العامة لحماية البيانات (GDPR): لم تكتفِ اللائحة بتنظيم البيانات الشخصية، بل

ربطت الهوية الرقمية مباشرةً بحقوق الإنسان الأساسية. فاعتبرت أن "أي معلومة تتعلق بشخص طبيعي محدّد أو قابل للتحديد" تُعد بيانات شخصية، وبالتالي تخضع لحماية صارمة. ونصّت على حقوق جوهرية تشمل:
- الحق في الوصول إلى البيانات.
- الحق في التصحيح أو الحذف.
- الحق في نقل البيانات (Data Portability).
- الحق في عدم الخضوع لقرارات آلية تعتمد على الهوية السلوكية.

كما فرضت التزامات صارمة على الجهات التي تعالج الهوية الرقمية، وفرضت غرامات تصل إلى 4% من الإيرادات العالمية السنوية في حال المخالفة.

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 "الهوية الرقمية 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".

خامساً، الاعتراف المتبادل:
يُعد هذا من أبرز مزايا النظام الأوروبي، إذ يسمح للمواطن باستعمال هويته الرقمية 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 الهوية الرقمية 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 الهوية الرقمية

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

أولاً، إعادة التصنيف القانوني للهوية الرقمية: عرّفت المادة 4 من GDPR "البيانات الشخصية" بأنها "أي معلومة تتعلق بشخص طبيعي محدّد

أو قابل للتحديد". وشمل هذا التعريف جميع عناصر الهوية الرقمية: من الاسم الإلكتروني، إلى عنوان IP، إلى السجلات السلوكية، والبيانات البيومترية. وبهذا، حوّلت اللائحة الهوية الرقمية من كيان تقني إلى كيان قانوني محمي، يخضع لضمانات صارمة بمجرد ارتباطه بشخص حقيقي.

ثانياً، تقوية حقوق أصحاب الهوية الرقمية: منحت GDPR أصحاب الهوية الرقمية سلطة غير مسبوقة على بياناتهم، عبر حقوق جوهرية تشمل:
- الحق في الوصول (المادة 15): يحق للفرد أن يطلب من أي جهة ما البيانات 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 الهوية

الرقمية في حالات محددة.
- الحق في نقل البيانات (المادة 20): يسمح بنقل الهوية الرقمية 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 الهوية الرقمية (سواء كانت حكومية أو خاصة) بعدة التزامات، منها:
- مبدأ الغرض المحدد (المادة 5): لا يجوز استخدام الهوية الرقمية 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 هويات رقمية 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 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 للهوية الرقمية في العالم.

وخلاصة القول، فإن GDPR لم يُنظم الهوية الرقمية 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 بالهوية

الرقمية

تُعد محكمة العدل الأوروبية (Court of Justice of the European Union – CJEU) الحارس الأعلى للقانون الأوروبي، ولعبت دوراً محورياً في تشكيل المفهوم القانوني للهوية الرقمية 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 للهوية الرقمية في الفضاء الأوروبي.

أولاً، قضية Google Spain SL وGoogle Inc. ضد Agencia Española de Protección de Datos وMario Costeja González (2014):
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 الهوية الرقمية 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 الرقمية من الاتحاد الأوروبي إلى الولايات المتحدة. وفي Schrems II، ألغت المحكمة "درع الخصوصية" (Privacy Shield)، مؤكدة أن "نقل الهوية الرقمية 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 الهوية الرقمية 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 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 Asociația de Proprietari ضد TK 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 للهوية 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 الهوية الرقمية ليشمل ليس فقط ما نقوله، بل ما "يفترض" عنا.

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

- الهوية الرقمية 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 الهوية الرقمية.
- الدولة والشركات على حد سواء مسؤولتان مدنياً عن حماية الهوية الرقمية.

وخلاصة القول، فإن اجتهاد محكمة العدل الأوروبية لم يكتفِ بتفسير النصوص، بل أعاد تعريف العلاقة بين الفرد والتكنولوجيا، وجعل من الهوية الرقمية 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 الهوية الرقمية

يُعدّ التباين بين النموذج الأوروبي والنموذج الأمريكي في حماية الهوية الرقمية 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 الهوية الرقمية 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 الهوية الرقمية 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 CCPA في كاليفورنيا)، 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 Riley وCarpenter)، 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 الهوية.

ومع ذلك، هناك نقاط تقاطع:
- كلا النموذجين يعترفان بأن الهوية الرقمية 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 الهوية

## الرقمية عبر الحدود

مع تزايد العولمة الرقمية، لم تعد الهوية الرقمية 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 الهوية الرقمية 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 هوية رقمية أو اختراق بيانات — 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 بالهويات الرقمية: بينما يضمن توجيه eIDAS الاعتراف المتبادل داخل الاتحاد الأوروبي، لا يوجد اتفاق مماثل على المستوى العالمي. فهوية رقمية 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 للهوية الرقمية مشروعة

في دولة ما، وغير قانونية في أخرى. فمثلاً، يسمح القانون الأمريكي لشركات مثل Facebook بجمع البيانات السلوكية 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 الهوية الرقمية 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 هويته الرقمية 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 الهوية

الرقمية، تحت إشراف الأمم المتحدة أو اليونيدروا.
- إنشاء آليات تسوية نزاعات رقمية دولية (ODR) متخصصة.
- تشجيع الدول على الاعتراف المتبادل بالهويات الرقمية المؤهلة.
- توحيد مبادئ المسؤولية المدنية عبر الحدود في حالات الهوية الرقمية.

إن بناء فضاء رقمي عالمي عادل يتطلب أكثر من مجرد تقنيات متطورة؛ فهو يحتاج إلى إطار قانوني مدني دولي يحمي الهوية الرقمية كحق إنساني، أينما كان صاحبها وأينما تم استخدامها.

الفصل العشرون
الجرائم الإلكترونية وانعكاساتها على المسؤولية المدنية

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 الهوية الرقمية، 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، الانتحال الرقمي (Identity Theft):
يُعدّ انتحال الهوية الرقمية من أكثر الجرائم انتشاراً، ويتم عبر سرقة بيانات شخصية (ككلمة المرور أو رقم البطاقة) لاستخدامها في إبرام عقود أو سحب أموال. ومن الناحية المدنية، يُنظر إلى هذا الفعل كتدليس 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 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 هوية رقمية 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.
- منصات التواصل: إذا سمحت بنشر هويات مسروقة أو أدوات اختراق.
- 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 بالضرر 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 (ككلمات مرور بسيطة)، 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 للهوية الرقمية 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 والهوية الرقمية

يُعد التعاقد الإلكتروني أحد أهم مجالات تطبيق الهوية الرقمية، 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 الهوية الرقمية الركيزة الأساسية لضمان رضا الأطراف، وصحة الإرادة، وقابلية العقد للتنفيذ. ويثير هذا التفاعل بين التعاقد الإلكتروني والهوية

الرقمية 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 الهوية الرقمية هذا الشرط عبر:
- التوثيق الثنائي (Two-factor Authentication): لضمان أن من أبرم العقد هو صاحب الهوية فعلاً.
- التوقيع الإلكتروني 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 الهوية الرقمية 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. 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 هوية 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 الرقمية ذات حجية إثبات مساوية للوثائق الورقية. غير أن القاضي يظل مطالباً بالتحقق

من:
- صحة الهوية الرقمية المستخدمة.
- سلامة السجلات من التلاعب.
- توافق الإجراءات مع المعايير الأمنية المعتمدة.

وفي حال الشك، يُمكن اللجوء إلى خبراء تقنيين لفحص أثر الهوية الرقمية (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 الهوية الرقمية تسبق العقد الذكي؛ فلا يُعتد بالعقد إلا إذا كان مرتبطاً بهوية رقمية معتمدة، تُثبت أن من أنشأ العقد هو صاحب الإرادة القانونية.

خامساً، المسؤولية في حالات الفشل التعاقدية:

إذا فشل العقد الإلكتروني بسبب خلل في نظام الهوية (كتعطيل التحقق البيومتري)، فقد تتحمل الجهة المُصدرة للهوية مسؤولية تقصيرية، خاصة إذا كان الخلل ناتجاً عن إهمال. كما أن المنصات التي تفرض هويات رقمية 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 هويات رقمية مختلفة، يبرز سؤال: أي هوية تُعتبر كافية لإثبات الرضا؟ هنا، يصبح الاعتراف المتبادل بين أنظمة الهوية (كما في eIDAS) ضرورة قانونية، لا خياراً تقنياً.

وخلاصة القول، فإن الهوية الرقمية ليست مجرد أداة تقنية في التعاقد الإلكتروني، بل هي الضامن المدني لصحة العقد ونفاذه. ولذلك، فإن أي نظام قانوني حديث يجب أن يدمج قواعد

الهوية الرقمية ضمن أحكامه المتعلقة بالعقود، ليضمن أن التحول الرقمي لا يأتي على حساب مبادئ القانون المدني الأساسية: الإرادة، الثقة، والعدالة.

## الفصل الثاني والعشرون
## الإثبات المدني للهوية الرقمية 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 الهوية الرقمية كوسيلة لإثبات صحة الوقائع، وربط الأفعال بالأفراد، وضمان مصداقية الإجراءات. غير أن قبول الهوية الرقمية 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 الهوية الرقمية لتكون حجة أمام القضاء، والتحديات التي تواجهها في البيئة القضائية.

أولاً، شروط قبول الهوية الرقمية كحجة إثبات:
لكي تُعتبر الهوية الرقمية 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 الهوية الرقمية:

- الهوية الرقمية المؤهلة (Qualified eID): مثل تلك الصادرة وفق معايير eIDAS، تُعتبر حجة قاطعة (Presumption of Authenticity)، ولا يُطلب من القاضي التحقق منها إلا إذا طعن أحد الأطراف.
- الهوية الرقمية العادية: مثل الحسابات على المنصات الخاصة، تُعتبر قرينة بسيطة، ويمكن دحضها بإثبات الانتحال أو الاختراق.
- الهوية السلوكية: مثل سجلات الاستخدام أو بصمات التنقل، تُستخدم كدليل ظرفي، ولا تكفي وحدها لإثبات الهوية دون أدلة مساندة.

ثالثاً، إجراءات التحقق القضائي:
عند تقديم الهوية الرقمية كدليل، يحق للقاضي:
- طلب تقرير فني من جهة محايدة حول سلامة السجلات.
- الاستعانة بخبير تقني لفحص أثر الهوية الرقمية (Digital Footprint).
- استدعاء الجهة المصدرة للهوية (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 الهوية الرقمية.

رابعاً، التحديات العملية في الإثبات:
- الإنكار بعد الإبرام: قد يدّعي شخص أن هويته الرقمية انتحلت، مما يضع عبء الإثبات على الطرف الآخر.

- تعدد الهويات: فقد يمتلك الشخص أكثر من هوية رقمية، مما يعقّد من عملية ربط الفعل بالهوية الصحيحة.
- البيانات المشتتة: فغالباً ما تكون عناصر الهوية 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 هوية رقمية 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، الهوية الرقمية كوسيلة لإثبات النية الجنائية أو المدنية:

لم يعد دور الهوية الرقمية 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.

وخلاصة القول، فإن الهوية الرقمية 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 للهوية الرقمية هو خطوة ضرورية لبناء نظام قضائي عادل في العصر الرقمي.

## الفصل الثالث والعشرون
## دور الجهات الموثوقة في إصدار الهويات الرقمية

تُعد الجهات الموثوقة (Trusted Service Providers) الركيزة الأساسية في نظام الهوية

الرقمية، 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 الإصدار.

أولاً، تعريف الجهة الموثوقة:
هي كيان قانوني — حكومي أو خاص — معتمد من قبل سلطة وطنية أو دولية لإصدار هويات رقمية أو شهادات رقمية مؤهلة. 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 27001.

ثانياً، الوظائف الأساسية للجهة الموثوقة:
1. التحقق من الهوية الحقيقية: عبر مطابقة البيانات الرقمية مع وثائق رسمية (كالبطاقة الوطنية أو جواز السفر).
2. إصدار الشهادة الرقمية: 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 الإصدار.

ثالثاً، الالتزامات المدنية للجهة الموثوقة:
بمجرد اعتمادها، تتحمل الجهة الموثوقة التزامات مدنية تجاه صاحب الهوية، أهمها:
- واجب العناية (Duty of Care): باتخاذ جميع التدابير الأمنية المعقولة لحماية الهوية الرقمية.
- واجب الشفافية: بإبلاغ المستخدم بكيفية استخدام بياناته، ومن يشاركها معه.
- واجب التصحيح: بتعديل أو إلغاء الهوية فوراً عند طلب صاحبها أو عند اكتشاف خطأ.
- واجب الإشعار: بإبلاغ المتضرر فور اكتشاف أي اختراق قد يؤثر على هويته.

رابعاً، المسؤولية المدنية في حال الإخلال:
إذا أصدرت جهة موثوقة هوية رقمية 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 هوياتها قوة قانونية عبر الحدود.

وخلاصة القول، فإن الجهة الموثوقة ليست مجرد وسيط تقني، بل هي ضامن مدني لصحة الهوية الرقمية. ولذلك، فإن تنظيم عملها بوضوح، وفرض التزامات مدنية صارمة عليها، هو شرط أساسي لبناء ثقة حقيقية في الفضاء الرقمي، وضمان أن اله**التنظيم القانوني المدني للهوية الرقمية: دراسة مقارنة بين الأنظمة العربية والأمريكية والأوروبية**

المقدمة

في عالم يتسارع فيه التحوّل الرقمي بوتيرة غير مسبوقة، لم يعد مفهوم الهوية قاصراً على الوثائق الورقية أو السجلات المدنية التقليدية. بل تجاوز ذلك ليتشكل في فضاء افتراضي دينامي، يُعرف بالهوية الرقمية، التي باتت تُشكّل العمود الفقري للتعاملات اليومية، من الخدمات الحكومية إلى المعاملات المالية، ومن التعليم عن بُعد إلى الرعاية الصحية الإلكترونية. ومع هذا التحوّل الجذري، برزت تحديات قانونية عميقة، خاصة في نطاق القانون المدني، الذي يُعنى بتنظيم العلاقات بين الأفراد، وحماية الحقوق الشخصية، وضمان سلامة المعاملات.

رغم أن التشريعات الجنائية والتقنية قد أولت الهوية الرقمية 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 للهوية الرقمية، 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 الهوية الرقمية من منظور قانوني مدني دقيق، بعيداً عن التعريفات التقنية الضيقة. الثاني، تحليل الإطار التشريعي والاجتهادي الحاكم لحماية الهوية الرقمية 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 للهوية الرقمية.

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 الهوية الرقمية ليست مجرد قضية تقنية، بل هي مسألة جوهرية تتعلق بكرامة الإنسان وحقوقه الأساسية. والله ولي التوفيق.

دكتور محمد كمال عرفه الرخاوي

الفصل الأول
مفهوم الهوية الرقمية في القانون المدني

لا يمكن الحديث عن التنظيم القانوني المدني للهوية الرقمية 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، والتعريفات القانونية التي يصوغها الفقه والقضاء والتشريع. فالهوية الرقمية، من منظور تقني، تشير إلى مجموعة البيانات التي تمثّل شخصاً أو كياناً في الفضاء الإلكتروني، وتُستخدم للتحقق من هويته أثناء التفاعل مع الأنظمة الرقمية. أما من منظور قانوني مدني، فهي تتجاوز هذا الحد لتُصبح تجسيداً رقمياً للشخصية القانونية، تحمل ذات الأهمية التي تحملها الوثائق الرسمية في العالم المادي.

ومن ثم، يمكن تعريف الهوية الرقمية في القانون

المدني المعاصر بأنها: تلك الصورة القانونية المُعترف بها للشخص الطبيعي أو الاعتباري في البيئة الرقمية، والتي تُعبّر عن صفاته الجوهرية، وتمكّنه من ممارسة حقوقه والتزاماته بشكل آمن وموثوق، وتُخوّله القدرة على التفاعل القانوني مع الآخرين عبر الوسائل الإلكترونية، مع ضمان حمايته من الانتحال أو التزوير أو الاستغلال غير المشروع.

ويتميز هذا المفهوم بعدة خصائص أساسية. أولها: الطابع القانوني، إذ لا يكفي أن تكون هناك بيانات رقمية عن الشخص، بل يجب أن تكون هذه البيانات مُعترفاً بها قانوناً، وقابلة للإثبات أمام الجهات القضائية والإدارية. ثانيها: الطابع الدينامي، حيث إن الهوية الرقمية ليست ثابتة، بل تتغير باستمرار مع تطور أنشطة الشخص وتفاعله مع مختلف المنصات والخدمات. ثالثها: الطابع الشامل، إذ لا تقتصر على اسم أو رقم، بل تشمل مجموعة متكاملة من السمات، مثل

العنوان الإلكتروني، بصمات السلوك الرقمي، السجلات المالية، وحتى التفضيلات الشخصية عند ارتباطها بمعاملات قانونية.

ومن الخطأ الشائع اعتبار الهوية الرقمية مجرد امتداد للهوية التقليدية. بل هي كيان قانوني مستقل، له خصوصياته وتحدياته. فبينما تحمي القوانين المدنية التقليدية الهوية من خلال السجلات الرسمية والشهادات الموثقة، فإن الهوية الرقمية تواجه تهديدات جديدة، مثل القرصنة، والانتحال الجماعي، واستغلال البيانات البيومترية، مما يستدعي أدوات حماية مدنية مبتكرة.

وقد بدأ الفقه المدني المعاصر في الاعتراف بهذه الخصوصية، لا سيما في أوروبا، حيث تم اعتبار الهوية الرقمية جزءاً من الحق في الخصوصية، بل وحتى من كرامة الإنسان. 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 الهوية الرقمية 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 بالشخصية القانونية، في إطار مقارن يجمع بين التجارب العربية والأمريكية والأوروبية.

## الفصل الثاني
## التطور التاريخي للهوية الرقمية من منظور قانوني

لم تنشأ الهوية الرقمية في فراغ قانوني أو

اجتماعي، بل هي نتاج تراكمي لتحولات تقنية وقانونية تمتد جذورها إلى عقود مضت. فقبل ظهور الإنترنت كشبكة عالمية، كانت أنظمة المعلومات تُدار ضمن شبكات مغلقة، وكانت الهوية تُحدد عبر أرقام تعريف داخلية تابعة للجهات الحكومية أو المؤسسات الكبرى. ومع بروز شبكة الإنترنت في تسعينيات القرن العشرين، بدأت الحاجة إلى آليات جديدة للتعرف على الأفراد والكيانات في بيئة لا مركزية وغير موثوقة. وقد أدت هذه الحاجة إلى ولادة أولى صور الهوية الرقمية، مثل كلمات المرور، وأرقام التعريف الفريدة، والشهادات الرقمية.

في المرحلة الأولى، كان التركيز منصباً على الجوانب الأمنية والتقنية، دون إيلاء الاعتبار الكافي للأبعاد القانونية. وكان التشريع يسير خلف التطور التقني بخطوات بطيئة، مما خلق فجوة تشريعية واسعة. غير أن ظهور التجارة الإلكترونية في أواخر التسعينيات دفع الدول إلى

سن قوانين تنظم التعاملات الرقمية، ومن بينها قوانين التوقيع الإلكتروني، التي شكلت حجر الزاوية الأول في الاعتراف القانوني بالهوية الرقمية. فقد نصت اتفاقية الأمم المتحدة بشأن استخدام الخطابات الإلكترونية في العقود التجارية عام 2005، وكذلك توجيه الاتحاد الأوروبي رقم EC/93/1999، على مبدأ الاعتراف القانوني بالتوقيعات الإلكترونية، ما منح الهوية الرقمية أولى درجات الشرعية القانونية.

وفي الولايات المتحدة، سار التشريع على خطى مماثلة، إذ صدر قانون التوقيع الإلكتروني في المعاملات العالمية والوطنية (E-SIGN Act) عام 2000، والذي أقرّ بأن السجلات والتوقيعات الإلكترونية لها نفس القوة القانونية كالسجلات والتوقيعات الورقية. أما في العالم العربي، فقد تأخر الاعتراف القانوني بالهوية الرقمية نسبياً، حيث لم تبدأ الدول العربية في سن تشريعات متكاملة إلا في أوائل العقد الأول من القرن

الحادي والعشرين. ومن أبرز الأمثلة على ذلك قانون المعاملات الإلكترونية في الإمارات العربية المتحدة عام 2006، وقانون التوقيع الإلكتروني في تونس عام 2004، وقانون تكنولوجيا المعلومات في مصر عام 2004.

ومع تصاعد استخدام الشبكات الاجتماعية والخدمات السحابية في العقد الثاني من القرن الحادي والعشرين، توسعت مفاهيم الهوية الرقمية لتشمل ليس فقط هوية المستخدم الرسمية، بل أيضاً هويته السلوكية، المبنية على تتبع أنشطته وتفاعله مع المحتوى الرقمي. وقد أدى هذا التوسع إلى ظهور تحديات قانونية جديدة، خاصة في مجالات الخصوصية، وحماية البيانات، والمسؤولية المدنية عن الاستخدام غير المشروع للمعلومات الشخصية.

وقد مثلت اللائحة العامة لحماية البيانات (GDPR) التي دخلت حيز التنفيذ في الاتحاد

الأوروبي عام 2018 نقطة تحول جوهرية في تاريخ الهوية الرقمية من منظور قانوني. فلأول مرة، تم ربط الهوية الرقمية بحقوق أساسية للمواطن، مثل الحق في النسيان، والحق في نقل البيانات، والحق في عدم الخضوع لقرارات آلية. 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 Carpenter ضد الولايات المتحدة عام 2018، أكدت على أن البيانات الرقمية المتعلقة بالهوية تستحق حماية دستورية بموجب التعديل الرابع.

وبالنسبة للدول العربية، فإن التطور التاريخي

للهوية الرقمية لا يزال في طور التشكل. فبينما أطلقت بعض الدول مشاريع طموحة للهوية الرقمية الموحدة، مثل مشروع الهوية الرقمية في السعودية ومصر، 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 الهوية الرقمية 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 للهوية الرقمية في القانون المدني

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

أولاً، يتعلق الأمر بمبدأ الشخصية القانونية. فالقانون المدني التقليدي يربط الشخصية القانونية بوجود طبيعي أو اعتباري ملموس. ولكن الهوية الرقمية، رغم عدم ملموسيتها، تمثل هذا الوجود في الفضاء الإلكتروني. ولذلك، فإن الاعتراف بها كتجسيد للشخصية القانونية

في البيئة الرقمية هو خطوة ضرورية لضمان اتساق النظام القانوني. وقد بدأ بعض الفقه الأوروبي في الحديث عن الشخصية الرقمية كامتداد ضروري للشخصية القانونية، وليس ككيان منفصل عنها.

ثانياً، يأتي مبدأ حرمة الحياة الخاصة، الذي يُعد من الركائز الأساسية في معظم التشريعات المدنية الحديثة. فالهوية الرقمية تحتوي على كم هائل من المعلومات الشخصية، التي إذا استُخدمت دون إذن، فإنها تشكل انتهاكاً صارخاً لهذا المبدأ. وقد أكدت محكمة العدل الأوروبية مراراً أن أي معالجة للبيانات الشخصية تُعد تدخلاً في الحق في الحياة الخاصة، ما لم تكن مبررة قانوناً. وهذا المبدأ يكتسب أهمية خاصة في البيئة الرقمية، حيث يصعب على الفرد مراقبة كيفية استخدام بياناته.

ثالثاً، يبرز مبدأ المسؤولية عن الضرر. ففي حال

انتحال الهوية الرقمية 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 الهوية؟ أم مزوّد الخدمة؟ أم جهة التحقق؟ إن غياب قواعد واضحة في هذا المجال يؤدي إلى فراغ قانوني يعرّض حقوق الأفراد للخطر.

رابعاً، هناك مبدأ الثقة المشروعة. فعندما يعتمد شخص على هوية رقمية معينة في إبرام عقد أو إجراء معاملة، فإنه يفترض أن هذه الهوية صحيحة وموثوقة. وإذا ثبت العكس، فإن القانون المدني يجب أن يحمي هذا الاعتماد المشروع، ويضمن تعويض المتضرر. وهذا المبدأ يكتسب أهمية خاصة في المعاملات العابرة للحدود، حيث يصعب التحقق من الهوية يدوياً.

خامساً، يظهر مبدأ المساواة أمام القانون. فلا يجوز أن يُعامل الشخص الذي يمتلك هوية

رقمية معتمدة معاملة مختلفة عن الشخص الذي لا يمتلكها، إلا إذا كان هناك مبرر قانوني وجيه. كما لا يجوز أن تُستخدم الهوية الرقمية كأداة للتمييز أو الاستبعاد الاجتماعي.

ومن خلال هذه الأُسس النظرية، يتضح أن الهوية الرقمية 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 للهوية الرقمية.

## الفصل الرابع
## عناصر الهوية الرقمية وخصائصها القانونية

لا تُشكل الهوية الرقمية 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 الهوية الرقمية إلى ثلاثة مستويات رئيسية: العناصر التعريفية، والعناصر الوثائقية، والعناصر السلوكية.

أولاً، العناصر التعريفية: وهي تلك البيانات الأساسية التي تميّز الشخص في الفضاء الرقمي، مثل الاسم الكامل، رقم الهوية الوطنية أو جواز السفر، تاريخ الميلاد، الجنسية، وعنوان البريد الإلكتروني الرسمي. وهذه العناصر تُعد بمثابة العمود الفقري للهوية الرقمية، لأنها تربط الكيان الرقمي بالشخص الحقيقي في العالم المادي. ومن الناحية القانونية، فإن هذه العناصر تخضع لقواعد صارمة تتعلق بالصحة والدقة

والتحديث. فمثلاً، لا يُعتد قانوناً بهوية رقمية تعتمد على اسم مستعار دون ربطه بهوية حقيقية معتمدة، خاصة في المعاملات ذات الأثر القانوني.

ثانياً، العناصر الوثائقية: وتشمل الشهادات الرقمية، التوقيعات الإلكترونية المؤهلة، والبيانات البيومترية (كالبصمة، ومسح الوجه، وقزحية العين). وهذه العناصر تلعب دوراً حاسماً في إثبات صحة الهوية وموثوقيتها. فالشهادة الرقمية، على سبيل المثال، تصدر عن جهة موثوقة معتمدة قانوناً، وتُستخدم للتحقق من أن صاحب الهوية هو من يدّعي أنه كذلك. أما التوقيع الإلكتروني المؤهل، فقد اكتسب قوة قانونية مساوية للتوقيع الورقي في العديد من التشريعات، مثل توجيه الاتحاد الأوروبي eIDAS. ومن الناحية القانونية، فإن هذه العناصر تتمتع بحماية خاصة، إذ يُجرّم القانون أي تزوير أو انتحال لها، ويُحمّل الجهات المصدرة مسؤولية

مدنية في حال إصدارها لهوية غير صحيحة.

ثالثاً، العناصر السلوكية: وهي تلك البيانات التي تُجمع من خلال تتبع سلوك المستخدم في الفضاء الرقمي، مثل سجلات التصفح، أنماط الكتابة، مواقع الدخول، وتفاعلات الشبكات الاجتماعية. وعلى الرغم من أن هذه العناصر لا تُستخدم عادةً في إثبات الهوية الرسمية، إلا أنها أصبحت أداة فعالة في أنظمة التحقق المتعدد العوامل (Multi-factor Authentication). ومن الناحية القانونية، فإن هذه العناصر تثير إشكاليات كبيرة تتعلق بالخصوصية وحقوق الملكية الفكرية. فهل يملك الفرد حقاً في منع جمع هذه البيانات؟ وهل يُعتبر استخدامها دون موافقته انتهاكاً للحق في الحياة الخاصة؟ إن الإجابة على هذه الأسئلة تتطلب تحديداً دقيقاً لطبيعة العلاقة القانونية بين صاحب الهوية ومزوّد الخدمة.

أما من حيث الخصائص القانونية، فإن الهوية الرقمية تتميز بعدة سمات جوهرية:

1. الطابع الثنائي: فهي تجمع بين البُعد التقني (كالرمز الرقمي) والبُعد القانوني (كالاعتراف الرسمي بها).
2. القابلية للنقل: إذ يمكن استخدامها عبر منصات وخدمات متعددة، ما لم يُقيّدها القانون.
3. القابلية للتفكيك: حيث يمكن فصل بعض عناصرها عن البعض الآخر حسب الغرض من الاستخدام.
4. الاستمرارية الزمنية: فهي لا تنتهي بانتهاء جلسة استخدام، بل تبقى قائمة طالما لم تُلغَ رسمياً.
5. القابلية للرقابة القضائية: إذ يحق لأي شخص الطعن في صحة هويته الرقمية 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 للهوية الرقمية، يضمن حماية الحقوق، ويعزز الثقة في المعاملات الرقمية، ويواكب التطورات العالمية دون إخلال بالمبادئ الأساسية للقانون المدني.

## الفصل الخامس
## العلاقة بين الهوية الرقمية والشخصية القانونية

تُعد العلاقة بين الهوية الرقمية والشخصية القانونية من القضايا الجوهرية التي تحدد موقع الهوية الرقمية داخل النظام القانوني المدني.

فبينما تُعتبر الشخصية القانونية مفهوماً تقليدياً راسخاً في جميع التشريعات المدنية، فإن الهوية الرقمية تمثل تجسيداً جديداً لهذه الشخصية في بيئة غير مادية، مما يثير تساؤلات عميقة حول طبيعة هذه العلاقة: هل الهوية الرقمية مجرد أداة لإثبات الشخصية؟ أم أنها كيان قانوني مستقل يستمد وجوده منها؟ أم أنها امتداد طبيعي لها في العصر الرقمي؟

من الناحية النظرية، تُعرّف الشخصية القانونية بأنها الأهلية التي يتمتع بها الشخص الطبيعي أو الاعتباري لممارسة الحقوق وتحمل الواجبات. وهي تبدأ من لحظة الولادة للشخص الطبيعي، ومن تاريخ التأسيس للشخص الاعتباري، ولا تنتهي إلا بالوفاة أو الانقضاء. أما الهوية الرقمية، فهي لا تنشأ تلقائياً، بل تتطلب إجراءات إنشاء وتوثيق عبر جهات معتمدة، وقد تُلغى أو تُعلّق دون أن تنتهي الشخصية القانونية ذاتها. وهذا الفارق الجوهر يدفع إلى القول إن الهوية الرقمية

ليست هي الشخصية القانونية، بل هي وسيلة رقمية لتمثيلها.

غير أن هذا التمثيل ليس مجرد انعكاس سلبي، بل هو تفاعل دينامي يحمل آثاراً قانونية مباشرة. فمثلاً، عندما يُبرم عقد إلكتروني باسم هوية رقمية معتمدة، فإن الآثار القانونية لهذا العقد تنسحب على صاحب الشخصية القانونية المرتبطة بتلك الهوية. وبالتالي، فإن الهوية الرقمية تكتسب قوة قانونية مشتقة من الشخصية، لكنها في الوقت نفسه تُضفي على هذه الشخصية بعداً رقمياً جديداً، يُمكن من خلاله ممارسة الحقوق والتزام الواجبات في الفضاء الإلكتروني.

ومن هنا، تبرز الحاجة إلى مبدأ "الربط القانوني" بين الهوية الرقمية والشخصية القانونية. فلكي تكون الهوية الرقمية ذات أثر قانوني، يجب أن تكون مرتبطة بشكل لا لبس فيه بشخصية

قانونية قائمة. ويتم هذا الربط عادةً عبر وثائق رسمية (كبطاقة الهوية أو جواز السفر) وبيانات بيومترية، ويتم توثيقه من قبل جهات موثوقة معتمدة قانوناً. وفي حال انقطاع هذا الربط — كأن تُستخدم هوية رقمية مسروقة أو مزورة — فإن المعاملات التي تتم باسمها تكون قابلة للإبطال، ما لم يثبت حسن نية الطرف الآخر.

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

وفي العالم العربي، لا تزال العلاقة بين الهوية الرقمية والشخصية القانونية غامضة في العديد من التشريعات. فبعض القوانين تقتصر على الاعتراف بالتوقيع الإلكتروني دون تحديد طبيعة العلاقة بينه وبين الشخصية القانونية. 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 "الشخصية الرقمية" ضمن قواعد القانون المدني، ويُحدد بدقة شروط ارتباطها بالشخصية القانونية، وآثار هذا الارتباط على الحقوق والواجبات.

ومن الجدير بالذكر أن ظهور الكيانات الافتراضية (مثل الحسابات الذكية أو الوكلاء الرقميين) يطرح تحديات جديدة لهذه العلاقة. فهل يمكن لكيان رقمي غير بشري أن يمتلك هوية رقمية؟ وإذا كان كذلك، فهل يُنسب إليه شخصية قانونية؟

إن الإجابة على هذه الأسئلة تتطلب إعادة النظر في مفاهيم أساسية في القانون المدني، مثل الإرادة، والمسؤولية، والأهلية.

وفي الختام، يمكن القول إن الهوية الرقمية ليست بديلاً عن الشخصية القانونية، بل هي وعاء رقمي لها، يُمكّنها من الوجود والتفاعل في العصر الرقمي. ولذلك، فإن أي تنظيم قانوني فعال للهوية الرقمية يجب أن ينطلق من فهم عميق لهذه العلاقة، ويضمن أن تظل الشخصية القانونية هي المصدر الوحيد للحقوق والواجبات، حتى في الفضاء الإلكتروني.

## الفصل السادس
## الإطار التشريعي العربي للهوية الرقمية

يُشكل الإطار التشريعي العربي للهوية الرقمية 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 بالهوية الرقمية، 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 أصدرت بعض الدول قوانين المعاملات الإلكترونية أو التوقيع الإلكتروني. ومن أبرز هذه التشريعات: قانون التجارة الإلكترونية في الإمارات العربية المتحدة لعام 2006، وقانون التوقيع الإلكتروني في تونس لعام 2004، وقانون إنشاء مركز المعلومات الوطني في مصر لعام 2004، وقانون تكنولوجيات الإعلام والاتصال في الجزائر لعام 2009. غير أن هذه القوانين ركزت في جوهرها على إضفاء الصفة القانونية على الوثائق

والتوقيعات الإلكترونية، دون أن تتناول الهوية الرقمية 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 الرقمية الموحدة، مثل "الهوية الرقمية الوطنية" في المملكة العربية السعودية، و"بطاقة الهوية الرقمية" 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 للهوية الرقمية. وهذا التفاوت يُعقّد من مسألة الاعتراف المتبادل بالهويات الرقمية عبر الحدود العربية.

ثانياً، الهيمنة الأمنية على الخطاب التشريعي. فمعظم التشريعات العربية تُدرج موضوع الهوية الرقمية 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 هوية رقمية مزورة، لكنه لا يُفصّل في آليات التعويض المدني للضحايا.

ثالثاً، غياب التكامل مع قواعد القانون المدني

العام. فنادراً ما تشير قوانين الهوية الرقمية 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 الهوية الرقمية وحقوق الملكية على البيانات الشخصية. كما أن آليات الرقابة القضائية على جهات إصدار الهويات الرقمية لا تزال محدودة.

خامساً، عدم وجود آلية موحدة للاعتماد

والاعتراف المتبادل. فكل دولة عربية تضع معاييرها الخاصة لإصدار الهويات الرقمية، 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 بالهوية الرقمية، تُراعي المبادئ التالية:
- الاعتراف بالهوية الرقمية ككيان قانوني مدني مستقل
- ربطها صراحةً بالشخصية القانونية في قوانين المدني
- تحديد حقوق والتزامات أصحاب الهويات الرقمية
- 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 للهوية الرقمية 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 الهوية الرقمية في دول مجلس التعاون الخليجي

يمثّل مجلس التعاون لدول الخليج العربية نموذجاً متقدماً نسبياً في المنطقة العربية من حيث التبني التشريعي والتنفيذي لمفهوم الهوية الرقمية. فقد سارعت دول المجلس إلى دمج هذا المفهوم ضمن رؤاها الوطنية للتحول الرقمي، ووضعت تشريعات وبنى تحتية تدعم وجود هويات رقمية 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. وعلى الرغم من التقدم الكبير، فإن القانون الإماراتي لا يحتوي على فصل مستقل ينظم الهوية الرقمية 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. 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 الهوية الرقمية والشخصية القانونية 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. لكن التشريع القطري، شأنه شأن غيره، يفتقر إلى مواد مدنية تُنظّم المسؤولية التقصيرية عن انتحال الهوية 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 الهوية الرقمية 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. ومع ذلك، فإن التشريع العماني لا يحتوي على أحكام مدنية مفصلة تتعلق بإثبات صحة الهوية الرقمية 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 الهوية الرقمية وقواعد المسؤولية المدنية في القانون البحريني.

ومن خلال هذه المقارنة، يتضح أن دول مجلس التعاون قد حققت تقدماً كبيراً في البنية

التحتية والاعتماد الحكومي للهوية الرقمية، 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 الهوية
- حق الضحية في التعويض عن الضرر المعنوي والمادي
- حماية البيانات الشخصية المرتبطة بالهوية
- آليات الطعن في قرارات إلغاء أو تعليق الهوية

ولذلك، فإن الخطوة التالية أمام دول المجلس يجب أن تكون سنّ قوانين مدنية خاصة أو تعديل قوانين المدني الحالية لتضمّن أحكاماً صريحة تنظّم الهوية الرقمية من منظور مدني شامل، بما يتماشى مع أعلى المعايير العالمية، ويُعزّز ثقة الأفراد في الفضاء الرقمي.

الفصل الثامن

## التنظيم القانوني للهوية الرقمية في الدول العربية غير الخليجية

بينما تشهد دول مجلس التعاون الخليجي زخماً تشريعياً وتنفيذياً في مجال الهوية الرقمية، 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 للهوية الرقمية. وقد أطلقت الدولة "منصة الهوية الرقمية" في 2021، التي تتيح للمواطنين استخدام هويتهم الوطنية في التعامل مع الجهات الحكومية والإلكترونية. غير أن هذا الإطار يعاني من فجوة مدنية واضحة: فقانون حماية البيانات لا ينظم العلاقة بين الهوية الرقمية والشخصية القانونية، وقانون الجرائم الإلكترونية يركز على العقوبات دون تحديد آليات التعويض المدني. كما أن قانون المدني المصري لم يُعدّل ليشمل أحكاماً خاصة بالهوية الرقمية، 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. لكن التشريع الجزائري لا يحتوي على أي تنظيم مدني مباشر للهوية الرقمية، بل يكتفي بالإشارة إلى أدواتها التقنية. ويبقى الفرد الجزائري دون حماية قانونية كافية في حال انتحال هويته الرقمية أو استخدام بياناته 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. ويتميز التشريع التونسي بوجود هيئة مستقلة (الهيئة الوطنية للبريد الإلكتروني والتوقيع الإلكتروني)، لكنه يفتقر إلى ربط صريح بين الهوية الرقمية وقواعد المسؤولية المدنية في مجلة الالتزامات والعقود. فمثلاً، لا توجد أحكام تُنظّم حالات الغلط في إبرام العقود

عبر هوية رقمية 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. ومع ذلك، فإن التشريع الأردني لا يزال ينظر إلى الهوية الرقمية من زاوية تقنية وأمنية، دون تناول كافٍ لآثارها المدنية. فمثلاً، لا توجد أحكام تُنظّم حق الفرد في تصحيح بياناته الرقمية أو حذفها، ولا تُفصّل في المسؤولية المدنية للجهات التي تفشل في حماية الهويات الرقمية 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. ويُلاحظ أن المغرب بدأ مؤخراً في تطوير قانون حماية البيانات الشخصية، لكنه لم يُدمج بعد مفاهيم الهوية الرقمية ضمن قواعد القانون المدني. وبالتالي، تظل الحماية المدنية للهوية الرقمية 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 الهويات
- عدم وجود نصوص صريحة تُنظم المسؤولية

المدنية عن الأضرار الناتجة عن اختراق الهوية

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

## الفصل التاسع
## الحماية المدنية للهوية الرقمية في النظام القانوني المصري

يُعد النظام القانوني المصري من الأنظمة التي بدأت مبكراً في ملامسة مفاهيم الهوية الرقمية، سواء من خلال البنية التشريعية أو

المبادرات التنفيذية. ومع ذلك، فإن الحماية المدنية للهوية الرقمية 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 الهوية الرقمية (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 الهوية الرقمية ككيان قانوني مستقل، ولا على العلاقة بينها وبين الشخصية القانونية في القانون المدني.

ومن الناحية التطبيقية، أطلقت الدولة "منصة الهوية الرقمية" في 2021، التي تتيح للمواطنين استخدام هويتهم الوطنية الرقمية 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 الهوية الرقمية. فمثلاً، لا تشير المواد المتعلقة بالإرادة (كالمادة 109 من القانون المدني) إلى حالات التدليس الإلكتروني أو الغلط الناتج عن انتحال الهوية الرقمية. كما أن قواعد المسؤولية التقصيرية (المواد 163 وما يليها) لا تتناول بشكل خاص الأضرار الناتجة عن اختراق الهوية الرقمية 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 بالهوية الرقمية ككيان مدني: فالتشريعات الحالية تتعامل معها كأداة تقنية، لا كتجسيد للشخصية القانونية في الفضاء الرقمي.
2. عدم تحديد المسؤولية المدنية لجهات الإصدار: ففي حال اختراق الهوية الرقمية 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 هويته.
4. غياب حق التصحيح والحذف الفعّال: فرغم وجوده في قانون حماية البيانات، إلا أن تطبيقه على الهوية الرقمية يفتقر إلى الآليات العملية والرقابة القضائية.

ولمعالجة هذه الثغرات، يُقترح ما يلي:

- تعديل قانون المدني المصري لإضافة فصل خاص بالهوية الرقمية، يُنظم علاقتها بالشخصية القانونية، ويُحدد شروط صحتها، وآثار انتحالها.
- إدخال نصوص في قانون حماية البيانات تُفصّل في حقوق أصحاب الهويات الرقمية، والتزامات الجهات المصدرة.
- إنشاء آلية قضائية متخصصة للنظر في النزاعات المتعلقة بالهوية الرقمية، تضم خبراء تقنيين وقانونيين.
- تضمين شروط استخدام منصة الهوية الرقمية بنوداً ملزمة تحمي حقوق المستخدم وتُحدّد مسؤوليات الجهة المُصدرة.

إن تطوير الحماية المدنية للهوية الرقمية 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 للهوية الرقمية 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 للهوية الرقمية في البلاد. ومع ذلك، فإن الحماية المدنية للهوية الرقمية 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 هوياتهم الرقمية.

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. 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 الهوية الرقمية والشخصية القانونية، ولا يُفصّل في المسؤولية المدنية الناتجة عن انتحال الهوية أو سوء استخدامها.

ومن منظور القانون المدني الجزائري، لا توجد أي مواد صريحة تتناول الهوية الرقمية. 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 الهوية الرقمية. 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 للهوية الرقمية: فالتشريع الجزائري لا يعرّف الهوية الرقمية 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 هويته الرقمية.

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

ولمعالجة هذه الثغرات، يُقترح ما يلي:

- إدخال تعديلات على القانون المدني الجزائري لإضافة أحكام خاصة بالهوية الرقمية، تُنظم علاقتها بالشخصية القانونية، وتُحدد شروط صحتها، وآثار انتحالها.
- سن قانون خاص بالهوية الرقمية يدمج بين الجوانب التقنية والمدنية، ويُحدّد التزامات الجهات المصدرة، وحقوق أصحاب الهويات.
- الإسراع في إصدار قانون حماية البيانات الشخصية، وضمان تضمينه أحكاماً تُطبّق

صراحةً على الهوية الرقمية.
- إنشاء وحدة قضائية متخصصة داخل المحاكم للنظر في النزاعات المتعلقة بالهوية الرقمية، تضم خبراء في القانون المدني والتكنولوجيا.

إن تطوير الحماية المدنية للهوية الرقمية 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 بالهوية الرقمية في العالم العربي

لا يمكن فصل التنظيم المدني للهوية الرقمية 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 الهوية الرقمية. ومع ذلك، فإن هذه المبادئ لا تزال عامة وغير محددة، ولا توجد دساتير عربية صريحة تعترف بالهوية الرقمية كحق دستوري مستقل. ويهدف هذا الفصل إلى تحليل هذه المبادئ، واستخلاص آثارها على الحماية المدنية للهوية الرقمية.

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 الهوية الرقمية أصبحت جزءاً لا يتجزأ

من وجود الفرد في العصر الرقمي، 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 الهويات الرقمية.

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 الهوية الرقمية تحتوي على بيانات شخصية حساسة، 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 الهوية الرقمية 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 الهوية الرقمية كأداة للتمييز أو الاستبعاد الاجتماعي. فمثلاً، لا يجوز حرمان شخص من

خدمة عامة لمجرد عدم امتلاكه هوية رقمية، ما لم يكن هناك بديل معقول. كما يُلزم الدولة بضمان وصول الجميع إلى الهوية الرقمية دون تمييز.

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

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

- عمومية النصوص: فمعظم الدساتير لا تذكر "الهوية الرقمية" صراحةً، مما يترك مجالاً واسعاً للتفسير.

- ضعف الرقابة الدستورية: فقلة من المحاكم الدستورية العربية تناولت قضايا مرتبطة بالهوية الرقمية، 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 بالهوية الرقمية كجزء من كرامة الإنسان وحقه في الخصوصية.
- تفعيل دور المحاكم الدستورية في مراجعة التشريعات المتعلقة بالهوية الرقمية، والتأكد من توافقها مع المبادئ الدستورية.
- ربط التشريعات المدنية الخاصة بالهوية الرقمية صراحة ً بالمبادئ الدستورية، لضمان أعلى درجات الحماية.

إن الاعتراف الدستوري بالهوية الرقمية ليس ترفاً قانونياً، بل هو ضرورة في عصر أصبحت فيه الهوية الرقمية 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 للهوية الرقمية

يُعد النظام القانوني الأمريكي من الأنظمة الفريدة في معالجته للهوية الرقمية، 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 الهوية الرقمية فيه معقدة لكنها غنية بالتجارب العملية.

على المستوى الفيدرالي، يُعد قانون التوقيع الإلكتروني في المعاملات العالمية والوطنية (E-SIGN Act) لعام 2000 حجر الزاوية الأول. فقد نصّ هذا القانون على أن "السجلات والتوقيعات الإلكترونية لها نفس القوة القانونية كالسجلات والتوقيعات الورقية"، ما منح الهوية الرقمية أول اعتراف قانوني رسمي. غير أن القانون لم يُعرّف الهوية الرقمية بشكل صريح، بل ركّز على مبدأ "الموافقة الواعية" (Informed Consent) كشرط لصحة المعاملات الإلكترونية.

وفي عام 2002، صدر قانون سياسة الخصوصية للبيانات الحكومية (Privacy Act Amendments)،

ثم تبعه قانون حماية خصوصية الإنترنت للأطفال (COPPA)، وقانون HIPAA لحماية البيانات الصحية. ومع أن هذه القوانين لا تتناول الهوية الرقمية مباشرة، إلا أنها وضعت قيوداً على جمع واستخدام البيانات الشخصية، التي تُشكل جوهر الهوية الرقمية.

أما على مستوى الولايات، فتتفاوت التشريعات بشكل كبير. فمثلاً، في كاليفورنيا، صدر قانون خصوصية المستهلك (CCPA) لعام 2018، الذي منح الأفراد حق معرفة البيانات التي تجمعها الشركات عنهم، وحق حذفها، وحق رفض بيعها. وقد تم تعزيزه لاحقاً بـ CPRA في 2020، الذي أنشأ وكالة تنظيمية مستقلة لحماية البيانات. وفي نيويورك، صدر قانون حماية الهوية (SHIELD Act) لعام 2019، الذي فرض التزامات صارمة على الشركات لحماية بيانات الهوية، ونص على إشعار الضحايا في حال الاختراق.

ومن الناحية القضائية، لعبت المحاكم الأمريكية دوراً محورياً في تشكيل مفهوم الهوية الرقمية. ففي قضية Carpenter v. United States (2018)، أكدت المحكمة العليا أن "البيانات المتعلقة بموقع الهاتف المحمول تُعد جزءاً من الحياة الخاصة"، ولا يجوز للسلطات الوصول إليها دون أمر قضائي. وفي قضية Riley v. California (2014)، اعتبرت المحكمة أن "الهواتف الذكية تحتوي على هوية رقمية كاملة"، ولا يجوز تفتيشها دون إذن قضائي. وهذه الأحكام رسّخت مبدأ أن الهوية الرقمية جزء من الحقوق الدستورية المحمية.

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

1. المسؤولية التعاقدية: فعند استخدام الهوية الرقمية في إبرام عقود، يُطبّق قانون العقود (Contract Law)، ويُنظر إلى أي انتحال كغش أو

تدليس يُبرر إبطال العقد.
2. المسؤولية التقصيرية: ففي حال سرقة الهوية الرقمية، 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 تسمح بمنح تعويضات رادعة (Punitive Damages) في حالات الاستغلال الجسيم للهوية الرقمية.

ومع ذلك، يعاني النظام الأمريكي من تحديات رئيسية:

- التشتت التشريعي: فاختلاف القوانين بين الولايات يُعقّد من حماية الهوية الرقمية 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 لحماية البيانات: 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 للهوية الرقمية ضمن إطار قانوني دينامي وعملي.

## الفصل الثالث عشر
## المسؤولية المدنية في القانون الأمريكي عن انتهاك الهوية الرقمية

في ظل غياب قانون مدني موحد في الولايات

المتحدة، تستند المسؤولية المدنية عن انتهاك الهوية الرقمية إلى شبكة معقدة من القواعد المشتقة من القانون العام (Common Law)، والتشريعات الفيدرالية والولائية، والممارسات القضائية. ورغم عدم وجود نص يُسمّى "الهوية الرقمية" صراحةً، 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 الهوية الرقمية. ولإثبات الإهمال، يجب على المدعي إثبات أربعة عناصر:
1. وجود واجب قانوني على المدعى عليه لحماية بيانات الهوية (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 Pisciotta v. Old National Bancorp (2007) أن المؤسسات التي تجمع بيانات هوية حساسة تتحمل واجباً قانونياً بحمايتها، حتى لو لم يكن هناك تشريع صريح يفرض ذلك. كما أن العديد من الولايات، مثل كاليفورنيا وتكساس، اعترفت صراحةً بأن الإخفاق في تطبيق معايير أمنية معقولة يُعد إهمالاً مدنياً.

ثانياً، المسؤولية التعاقدية (Contractual Liability):
عند استخدام الهوية الرقمية في المعاملات التجارية، يُطبّق قانون العقود. فإذا استخدم طرف هوية 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 الهوية الرقمية. فمثلاً، ينص قانون كاليفورنيا SHIELD Act على أن أي جهة تخضع لاختراق بيانات يجب أن تُبلغ المتضررين فوراً، وإلا تُعتبر مسؤولة مدنياً عن الأضرار الناتجة عن التأخير. كما يمنح قانون CCPA الحق في رفع دعاوى جماعية (Class Actions) في حالات الانتهاك الجسيم.

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.
- 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 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 الهوية الرقمية، 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 الهوية الرقمية

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 الهوية الرقمية، لعبت المحاكم الأمريكية — من المحكمة العليا إلى محاكم الولايات — دوراً ريادياً في تحديد طبيعة هذه الهوية، 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:
في قضية Riley v. California (2014)، أصدرت المحكمة العليا حكماً تاريخياً اعتبر أن "الهاتف الذكي ليس مجرد جهاز اتصال، بل هو حافظة رقمية تحتوي على هوية الفرد الكاملة". وبناءً

عليه، قضت المحكمة بأنه لا يجوز للشرطة تفتيش محتويات الهاتف دون أمر قضائي، حتى لو كان الشخص معتقلاً. وقد شكّل هذا الحكم نقطة تحول، إذ اعترف لأول مرة بأن الهوية الرقمية جزء من الحياة الخاصة المحمية دستورياً بموجب التعديل الرابع.

وفي قضية Carpenter v. United States 2018))، وسّعت المحكمة العليا من هذا المفهوم، مؤكدة أن "بيانات الموقع الجغرافي التي تجمعها شركات الاتصال عن الهواتف تمثل سجلاً دقيقاً للحياة اليومية"، ولا يجوز للسلطات الوصول إليها دون أمر قضائي. وقد استندت المحكمة إلى أن هذه البيانات تُشكّل جزءاً من الهوية السلوكية للفرد، وبالتالي فهي محمية دستورياً.

ثانياً، محاكم الاستئناف الفيدرالية:
في قضية In re: Equifax Inc. Customer Data

Security Breach Litigation (2019)، اعترفت محكمة الاستئناف بالدائرة الحادية عشرة بأن "الإخفاق في حماية بيانات الهوية يُعد إهمالاً مدنياً"، حتى لو لم يُسفر الاختراق فوراً عن سرقة أموال. ووافقت المحكمة على دعوى جماعية ضد شركة Equifax بعد اختراق بيانات 147 مليون شخص، مما فتح الباب أمام تعويضات واسعة النطاق.

وفي قضية Pisciotta v. Old National Bancorp (2007)، أكدت محكمة الاستئناف بالدائرة السابعة أن المؤسسات المالية التي تجمع بيانات هوية حساسة تتحمل "واجب عناية" (Duty of Care) قانونياً، وأن الإخفاق في تطبيق معايير أمنية معقولة يُعد أساساً كافياً لدعوى إهمال مدني.

ثالثاً، محاكم الولايات:
في كاليفورنيا، أصدرت محكمة المقاطعة حكماً

في قضية Facebook Biometric Information Privacy Litigation (2021)، اعتبرت فيه أن "جمع بصمات الوجه دون موافقة صريحة يُعد انتهاكاً لهوية الفرد البيومترية"، وفرضت تعويضات جماعية تجاوزت 650 مليون دولار. وقد استند الحكم إلى قانون خصوصية المعلومات البيومترية في إلينوي (BIPA)، الذي أصبح مرجعاً وطنياً.

وفي نيويورك، قضت محكمة عليا في قضية People v. Weaver (2009) بأن تتبع موقع الهاتف دون إذن قضائي يُعد "تفتيشاً غير معقول"، ويُخالف الدستور، ما عزّز من حماية الهوية السلوكية.

رابعاً، الآليات القضائية المبتكرة:
تميّزت المحاكم الأمريكية باستخدام آليات مرنة لحماية الهوية الرقمية، منها:
- الأوامر الزجرية المؤقتة (Preliminary Injunctions): لوقف استخدام هوية مسروقة

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 الهوية الرقمية، بل سبقه بخطوات، ورسّخ مبادئ قانونية راسخة تجعل من الهوية الرقمية حقاً مدنياً محمياً، لا مجرد بيانات تقنية. وهذا النهج القضائي النشط يُعد درساً مهماً للأنظمة القانونية الأخرى، التي قد تتردد في الاعتراف بالهوية الرقمية ككيان قانوني مستقل.

## الفصل الخامس عشر
## النظام القانوني الأوروبي للهوية الرقمية

يمثّل النظام القانوني الأوروبي نموذجاً رائداً في التنظيم المدني للهوية الرقمية، 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 الهوية 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". وقسّم الهويات الرقمية إلى ثلاثة مستويات:
- منخفضة (Low): للمعاملات غير الحساسة.
- متوسطة (Substantial): للمعاملات الإدارية.
- عالية (High): للمعاملات ذات الأثر القانوني الكبير، مثل العقود أو المعاملات المالية.

كما أنشأ التوجيه نظاماً لاعتماد جهات التصديق الموثوقة (Qualified Trust Service Providers)، التي تُصدر شهادات رقمية مؤهلة، تتمتع بقوة قانونية مساوية للتوقيع الورقي. وهذا يضمن أن الهوية الرقمية ليست مجرد بيانات، بل كيان قانوني معتمد.

ثانياً، اللائحة العامة لحماية البيانات (GDPR): لم تكتفِ اللائحة بتنظيم البيانات الشخصية، بل ربطت الهوية الرقمية مباشرةً بحقوق الإنسان الأساسية. فاعتبرت أن "أي معلومة تتعلق بشخص طبيعي محدّد أو قابل للتحديد" تُعد بيانات شخصية، وبالتالي تخضع لحماية صارمة. ونصّت على حقوق جوهرية تشمل:
- الحق في الوصول إلى البيانات.
- الحق في التصحيح أو الحذف.
- الحق في نقل البيانات (Data Portability).
- الحق في عدم الخضوع لقرارات آلية تعتمد

على الهوية السلوكية.

كما فرضت التزامات صارمة على الجهات التي تعالج الهوية الرقمية، وفرضت غرامات تصل إلى 4% من الإيرادات العالمية السنوية في حال المخالفة.

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 "الهوية الرقمية 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".

خامساً، الاعتراف المتبادل:
يُعد هذا من أبرز مزايا النظام الأوروبي، إذ يسمح للمواطن باستعمال هويته الرقمية 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 الهوية الرقمية 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 الهوية الرقمية

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 الهوية الرقمية في العصر الحديث. فهي لم تكتفِ بتنظيم جمع البيانات ومعالجتها، بل أعادت تعريف العلاقة بين الفرد والبيانات التي تمثّله في الفضاء الرقمي، وجعلت من الهوية الرقمية حقاً أساسياً ينبع من كرامة الإنسان، لا مجرد سلعة

قابلة للتداول. ويتجلى تأثير GDPR على الهوية الرقمية في خمسة محاور رئيسية: إعادة التصنيف القانوني للهوية، تقوية حقوق الأفراد، فرض التزامات صارمة على الجهات المعالجة، إنشاء آليات رقابية فعالة، وتوحيد المعايير عبر الحدود.

أولاً، إعادة التصنيف القانوني للهوية الرقمية: عرّفت المادة 4 من GDPR "البيانات الشخصية" بأنها "أي معلومة تتعلق بشخص طبيعي محدّد أو قابل للتحديد". وشمل هذا التعريف جميع عناصر الهوية الرقمية: من الاسم الإلكتروني، إلى عنوان IP، إلى السجلات السلوكية، والبيانات البيومترية. وبهذا، حوّلت اللائحة الهوية الرقمية من كيان تقني إلى كيان قانوني محمي، يخضع لضمانات صارمة بمجرد ارتباطه بشخص حقيقي.

ثانياً، تقوية حقوق أصحاب الهوية الرقمية:

منحت GDPR أصحاب الهوية الرقمية سلطة غير مسبوقة على بياناتهم، عبر حقوق جوهرية تشمل:
- الحق في الوصول (المادة 15): يحق للفرد أن يطلب من أي جهة ما البيانات 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 الهوية الرقمية في حالات محددة.
- الحق في نقل البيانات (المادة 20): يسمح بنقل الهوية الرقمية 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 الهوية الرقمية (سواء كانت حكومية أو خاصة) بعدة التزامات، منها:
- مبدأ الغرض المحدد (المادة 5): لا يجوز استخدام الهوية الرقمية 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 هويات رقمية 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 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 للهوية الرقمية في العالم.

وخلاصة القول، فإن GDPR لم يُنظم الهوية الرقمية 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 بالهوية الرقمية

تُعد محكمة العدل الأوروبية (Court of Justice of the European Union – CJEU) الحارس الأعلى للقانون الأوروبي، ولعبت دوراً محورياً في تشكيل المفهوم القانوني للهوية الرقمية 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 للهوية الرقمية في الفضاء الأوروبي.

أولاً، قضية Google Spain SL وGoogle Inc. ضد Agencia Española de Protección de Datos وMario Costeja González (2014):
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 الهوية الرقمية 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 الرقمية من الاتحاد الأوروبي إلى الولايات المتحدة. وفي Schrems II، ألغت المحكمة "درع الخصوصية" (Privacy Shield)، مؤكدة أن "نقل الهوية الرقمية 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 الهوية الرقمية 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 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 للهوية 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 الهوية الرقمية ليشمل ليس فقط ما نقوله، بل ما "يفترض" عنا.

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

- الهوية الرقمية 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 الهوية الرقمية.
- الدولة والشركات على حد سواء مسؤولتان مدنياً عن حماية الهوية الرقمية.

وخلاصة القول، فإن اجتهاد محكمة العدل الأوروبية لم يكتفِ بتفسير النصوص، بل أعاد تعريف العلاقة بين الفرد والتكنولوجيا، وجعل من الهوية الرقمية 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 الهوية الرقمية

يُعدّ التباين بين النموذج الأوروبي والنموذج الأمريكي في حماية الهوية الرقمية 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 الهوية الرقمية 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 الهوية الرقمية 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 CCPA في كاليفورنيا)، 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 Riley وCarpenter)، 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 الهوية.

ومع ذلك، هناك نقاط تقاطع:
- كلا النموذجين يعترفان بأن الهوية الرقمية 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 الهوية الرقمية عبر الحدود

مع تزايد العولمة الرقمية، لم تعد الهوية الرقمية 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 الهوية الرقمية 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 هوية رقمية أو اختراق بيانات — 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 بالهويات الرقمية:
بينما يضمن توجيه eIDAS الاعتراف المتبادل

داخل الاتحاد الأوروبي، لا يوجد اتفاق مماثل على المستوى العالمي. فهوية رقمية 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 للهوية الرقمية مشروعة في دولة ما، وغير قانونية في أخرى. فمثلاً، يسمح القانون الأمريكي لشركات مثل Facebook بجمع البيانات السلوكية 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 الهوية الرقمية 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 هويته الرقمية 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 الهوية الرقمية، تحت إشراف الأمم المتحدة أو اليونيدروا.
- إنشاء آليات تسوية نزاعات رقمية دولية (ODR) متخصصة.
- تشجيع الدول على الاعتراف المتبادل بالهويات الرقمية المؤهلة.
- توحيد مبادئ المسؤولية المدنية عبر الحدود في حالات الهوية الرقمية.

إن بناء فضاء رقمي عالمي عادل يتطلب أكثر من مجرد تقنيات متطورة؛ فهو يحتاج إلى إطار قانوني مدني دولي يحمي الهوية الرقمية كحق إنساني، أينما كان صاحبها وأينما تم استخدامها.

## الفصل العشرون
## الجرائم الإلكترونية وانعكاساتها على المسؤولية المدنية

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 الهوية الرقمية، 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، الانتحال الرقمي (Identity Theft):
يُعدّ انتحال الهوية الرقمية من أكثر الجرائم انتشاراً، ويتم عبر سرقة بيانات شخصية (ككلمة المرور أو رقم البطاقة) لاستخدامها في إبرام عقود أو سحب أموال. ومن الناحية المدنية، يُنظر إلى هذا الفعل كتدليس 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 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 هوية رقمية 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.
- منصات التواصل: إذا سمحت بنشر هويات مسروقة أو أدوات اختراق.
- 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 بالضرر 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 (ككلمات مرور بسيطة)، 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 للهوية الرقمية 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 والهوية الرقمية

يُعد التعاقد الإلكتروني أحد أهم مجالات تطبيق الهوية الرقمية، 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 الهوية الرقمية الركيزة الأساسية لضمان رضا الأطراف، وصحة الإرادة، وقابلية العقد للتنفيذ. ويثير هذا التفاعل بين التعاقد الإلكتروني والهوية الرقمية 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 الهوية الرقمية هذا الشرط عبر:

- التوثيق الثنائي (Two-factor Authentication): لضمان أن من أبرم العقد هو صاحب الهوية فعلاً.
- التوقيع الإلكتروني 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 الهوية الرقمية 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. 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 هوية 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 الرقمية ذات حجية إثبات مساوية للوثائق الورقية. غير أن القاضي يظل مطالباً بالتحقق من:
- صحة الهوية الرقمية المستخدمة.
- سلامة السجلات من التلاعب.
- توافق الإجراءات مع المعايير الأمنية المعتمدة.

وفي حال الشك، يُمكن اللجوء إلى خبراء تقنيين لفحص أثر الهوية الرقمية (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 الهوية الرقمية تسبق العقد الذكي؛ فلا يُعتد بالعقد إلا إذا كان مرتبطاً بهوية رقمية معتمدة، تُثبت أن من أنشأ العقد هو صاحب الإرادة القانونية.

خامساً، المسؤولية في حالات الفشل التعاقدية:
إذا فشل العقد الإلكتروني بسبب خلل في نظام الهوية (كتعطيل التحقق البيومتري)، فقد تتحمل الجهة المُصدرة للهوية مسؤولية تقصيرية، خاصة إذا كان الخلل ناتجاً عن إهمال. كما أن المنصات التي تفرض هويات رقمية 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 هويات رقمية مختلفة، يبرز سؤال: أي هوية تُعتبر كافية لإثبات الرضا؟ هنا، يصبح الاعتراف المتبادل بين أنظمة الهوية (كما في eIDAS) ضرورة قانونية، لا خياراً تقنياً.

وخلاصة القول، فإن الهوية الرقمية ليست مجرد أداة تقنية في التعاقد الإلكتروني، بل هي الضامن المدني لصحة العقد ونفاذه. ولذلك، فإن أي نظام قانوني حديث يجب أن يدمج قواعد الهوية الرقمية ضمن أحكامه المتعلقة بالعقود، ليضمن أن التحول الرقمي لا يأتي على حساب مبادئ القانون المدني الأساسية: الإرادة، الثقة، والعدالة.

## الفصل الثاني والعشرون
## الإثبات المدني للهوية الرقمية 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 الهوية الرقمية كوسيلة لإثبات صحة الوقائع، وربط الأفعال بالأفراد، وضمان مصداقية الإجراءات. غير أن قبول الهوية الرقمية 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 الهوية الرقمية لتكون حجة أمام القضاء، والتحديات التي تواجهها في البيئة القضائية.

أولاً: شروط قبول الهوية الرقمية كحجة إثبات:
لكي تُعتبر الهوية الرقمية 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 الهوية الرقمية:
- الهوية الرقمية المؤهلة (Qualified eID): مثل

تلك الصادرة وفق معايير eIDAS، تُعتبر حجة قاطعة (Presumption of Authenticity)، ولا يُطلب من القاضي التحقق منها إلا إذا طعن أحد الأطراف.

- الهوية الرقمية العادية: مثل الحسابات على المنصات الخاصة، تُعتبر قرينة بسيطة، ويمكن دحضها بإثبات الانتحال أو الاختراق.

- الهوية السلوكية: مثل سجلات الاستخدام أو بصمات التنقل، تُستخدم كدليل ظرفي، ولا تكفي وحدها لإثبات الهوية دون أدلة مساندة.

ثالثاً، إجراءات التحقق القضائي:

عند تقديم الهوية الرقمية كدليل، يحق للقاضي:

- طلب تقرير فني من جهة محايدة حول سلامة السجلات.

- الاستعانة بخبير تقني لفحص أثر الهوية الرقمية (Digital Footprint).

- استدعاء الجهة المصدرة للهوية (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 الهوية الرقمية.

رابعاً، التحديات العملية في الإثبات:
- الإنكار بعد الإبرام: قد يدّعي شخص أن هويته الرقمية انتحلت، مما يضع عبء الإثبات على الطرف الآخر.
- تعدد الهويات: فقد يمتلك الشخص أكثر من هوية رقمية، مما يعقّد من عملية ربط الفعل بالهوية الصحيحة.
- البيانات المشتتة: فغالباً ما تكون عناصر الهوية 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 هوية رقمية 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، الهوية الرقمية كوسيلة لإثبات النية الجنائية أو المدنية:
لم يعد دور الهوية الرقمية 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.

وخلاصة القول، فإن الهوية الرقمية 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 للهوية الرقمية هو خطوة ضرورية لبناء نظام قضائي عادل في العصر الرقمي.

## الفصل الثالث والعشرون
## دور الجهات الموثوقة في إصدار الهويات الرقمية

تُعد الجهات الموثوقة (Trusted Service Providers) الركيزة الأساسية في نظام الهوية الرقمية، 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 الإصدار.

أولاً، تعريف الجهة الموثوقة:
هي كيان قانوني — حكومي أو خاص — معتمد من قبل سلطة وطنية أو دولية لإصدار هويات رقمية أو شهادات رقمية مؤهلة. 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 27001.

ثانياً، الوظائف الأساسية للجهة الموثوقة:
1. التحقق من الهوية الحقيقية: عبر مطابقة البيانات الرقمية مع وثائق رسمية (كالبطاقة الوطنية أو جواز السفر).
2. إصدار الشهادة الرقمية: 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 الإصدار.

ثالثاً، الالتزامات المدنية للجهة الموثوقة:
بمجرد اعتمادها، تتحمل الجهة الموثوقة التزامات مدنية تجاه صاحب الهوية، أهمها:
- واجب العناية (Duty of Care): باتخاذ جميع التدابير الأمنية المعقولة لحماية الهوية الرقمية.

- واجب الشفافية: بإبلاغ المستخدم بكيفية استخدام بياناته، ومن يشاركها معه.
- واجب التصحيح: بتعديل أو إلغاء الهوية فوراً عند طلب صاحبها أو عند اكتشاف خطأ.
- واجب الإشعار: بإبلاغ المتضرر فور اكتشاف أي اختراق قد يؤثر على هويته.

رابعاً، المسؤولية المدنية في حال الإخلال:
إذا أصدرت جهة موثوقة هوية رقمية 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 هوياتها قوة قانونية عبر الحدود.

وخلاصة القول، فإن الجهة الموثوقة ليست مجرد

وسيط تقني، بل هي ضامن مدني لصحة الهوية الرقمية. ولذلك، فإن تنظيم عملها بوضوح، وفرض التزامات مدنية صارمة عليها، هو شرط أساسي لبناء ثقة حقيقية في الفضاء الرقمي، وضمان أن الهوية الرقمية تُستخدم كأداة لحماية الحقوق، لا كوسيلة لانتهاكها.

## الفصل الرابع والعشرون
## المسؤولية المدنية لمزوّدي خدمات الهوية الرقمية

مع تزايد الاعتماد على الهوية الرقمية في المعاملات اليومية، برزت فئة جديدة من الفاعلين القانونيين: مزوّدو خدمات الهوية الرقمية (Digital Identity Service Providers). وهم كيانات — حكومية أو خاصة — تُوفّر البنية التحتية والخدمات اللازمة لإنشاء، إدارة، والتحقق من الهويات الرقمية. 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 الخدمة 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 الخدمة 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 هويته الرقمية.
- رفض الإلغاء: عند طلب المستخدم سحب هويته الرقمية.

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 الهوية السلوكية، ومن ثم ارتكب خطأ، هل يُعتبر ذلك خطأ بشريًا أم تقنيًا؟

وخلاصة القول، فإن مزوّدي خدمات الهوية الرقمية 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 الهوية الرقمية لا تتحول إلى مصدر للخطر.

## الفصل الخامس والعشرون
## التعويض المدني عن الضرر الناتج عن سرقة أو انتحال الهوية الرقمية

يُعد التعويض المدني الركن الأساسي في حماية الأفراد من آثار سرقة أو انتحال الهوية الرقمية، 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 الهوية

الرقمية، 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).
- 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.
- فقدان الثقة في المنصات الرقمية.
- الإحراج الاجتماعي أو المهني الناتج عن استخدام الهوية 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 واستخدمها.
- الجهة المُصدرة للهوية: 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 الهوية 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 الهوية 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 الهوية الرقمية.

- 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 هويته الرقمية للسرقة أو الانتحال.

## الفصل السادس والعشرون
## آليات التقاضي المدني في قضايا الهوية الرقمية

مع تزايد النزاعات المرتبطة بالهوية الرقمية، 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 الهوية الرقمية. 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 الرقمية كشرط للتقاضي: في بعض الدول (كالإمارات)، يُشترط استخدام الهوية الرقمية 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 الهوية الرقمية، 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 (كاختراق حساب شخصي)، 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.
- 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 القضايا الرقمية.

وخلاصة القول، فإن فعالية الحماية المدنية للهوية الرقمية 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 بالهوية الرقمية

في ظل الطبيعة الخاصة للمنازعات المتعلقة بالهوية الرقمية — 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 الهوية، اختراق البيانات، أو سوء استخدام الخدمات الرقمية. ويهدف هذا الفصل إلى استعراض أبرز هذه الآليات، وتحليل فعاليتها، وتحديدها كأدوات وقائية وعلاجية في حماية الهوية الرقمية.

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.

وقد أطلقت المفوضية الأوروبية منصة ""ODR (Online Dispute Resolution)) لحل النزاعات الاستهلاكية، بما فيها تلك المتعلقة بالهوية الرقمية.

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.
- إمكانية عقد الجلسات عبر الفيديو.
- صدور القرار خلال أسابيع، لا سنوات.

وقد اعتمدت غرف التجارة الدولية (مثل ICC وDIAC) قواعد خاصة للتحكيم الإلكتروني، تشمل حماية الهوية الرقمية للأطراف.

ثالثاً، آليات الشكاوى الداخلية:
تفرض التشريعات الحديثة (كـGDPR) على مزوّدي خدمات الهوية الرقمية 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.

وهذه اللجان تقدم حلاً أسرع وأقل تكلفة من المحاكم.

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 الهوية الرقمية في ظل الذكاء الاصطناعي والبلوك تشين

مع التسارع المذهل في تقنيات الذكاء الاصطناعي والبلوك تشين، يقف مفهوم الهوية الرقمية على أعتاب تحول جذري قد يعيد تعريفه من جذوره. فبينما كانت الهوية الرقمية 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. ويهدف هذا الفصل إلى استشراف مستقبل الهوية الرقمية في ضوء هاتين التقنيتين، وتحليل الآثار المدنية المترتبة عليهما.

أولا ً، الهوية الرقمية في عصر الذكاء الاصطناعي: بدأ الذكاء الاصطناعي في تحليل السلوكيات

الرقمية لإنشاء ما يُعرف بـ"الهوية السلوكية" (Behavioral 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؟ وهل يُعتبر تحليلها دون إذنه انتهاكاً لحقه في الخصوصية؟ التشريعات الحالية (كـGDPR) بدأت بالإجابة بالإيجاب، لكن التطبيق لا يزال محدوداً.

ثانياً، الهوية الرقمية القائمة على البلوك تشين (Self-Sovereign Identity – SSI):
تقدم تقنية البلوك تشين نموذجاً جديداً يُعرف بـ"الهوية ذات السيادة الذاتية"، حيث يتحكم

الفرد كلياً بهويته الرقمية 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 "وكيلًا 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 الرقمية الفرد ضمن فئات اجتماعية أو اقتصادية تؤثر على فرصه، دون أن يعلم.
- الهوية المزيفة المتقدمة: باستخدام تقنيات التزييف العميق (Deepfake)، قد يصبح انتحال الهوية 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 والذكاء الاصطناعي.
- إنشاء آليات تعويض جديدة تتناسب مع الأضرار غير الملموسة.
- تطوير معايير دولية للهوية القائمة على البلوك تشين.

وخلاصة القول، فإن مستقبل الهوية الرقمية 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 الهوية الرقمية

## في الفضاء المدني العربي

في ظل التحديات المشتركة التي تواجهها الدول العربية في مجال الهوية الرقمية — 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. ويقدم هذا الفصل مقترحات تشريعية عملية قابلة للتطبيق، تستند إلى أفضل الممارسات العالمية، وتتوافق مع المبادئ الدستورية والفقهية في الأنظمة العربية.

أولاً، التعريف الموحّد للهوية الرقمية:
ينبغي أن يتضمن أي تشريع عربي تعريفاً واضحاً ومدنياً للهوية الرقمية، مثل:
> "الهوية الرقمية هي تلك الصورة القانونية المعتمدة للشخص الطبيعي أو الاعتباري في البيئة الرقمية، التي تمثل صفاته الجوهرية، وتمكّنه من ممارسة حقوقه والتزاماته بشكل آمن، وتُخوّله التفاعل القانوني مع الآخرين عبر الوسائل الإلكترونية، مع ضمان حمايته من الانتحال أو الاستغلال غير المشروع."

ثانياً، ربط الهوية الرقمية بالشخصية القانونية:
يجب أن ينص التشريع صراحةً على أن الهوية الرقمية ليست كياناً مستقلاً، بل امتداداً للشخصية القانونية في الفضاء الإلكتروني، وأن أي معاملة تتم باسم هوية رقمية معتمدة تنسحب آثارها على صاحب الشخصية القانونية المرتبطة بها.

ثالثاً، حقوق أصحاب الهوية الرقمية:
يجب أن يكفل التشريع الموحّد الحقوق التالية:
- الحق في إنشاء هوية رقمية معتمدة دون تمييز.
- الحق في تصحيح أو تحديث بياناته الرقمية.
- الحق في حذف هويته الرقمية 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 الهوية الرقمية.
- 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 الرقمية 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 للهويات الرقمية"، 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 للهوية الرقمية" 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 بالهوية الرقمية، 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 رقمية، 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. فالهوية الرقمية 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 رقمي دينامي يتفاعل مع الفرد طوال يومه، ويُشكّل العمود الفقري لوجوده في الفضاء الإلكتروني. ومع هذا

التحوّل، برزت الهوية الرقمية 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 للهوية الرقمية 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 بالهوية الرقمية في الدول العربية، أو تعديل قوانين المدني الحالية لتضمّن أحكاماً صريحة تنظّم علاقتها بالشخصية القانونية، 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 بالهويات الرقمية المؤهلة.

ثانياً، على مستوى القضاء:
- إنشاء دوائر قضائية متخصصة في النزاعات الرقمية، تضم قضاة ذوي كفاءة تقنية وقانونية.

- تطوير مبادئ اجتهادية تُعزّز من حماية الهوية الرقمية كحق مدني، حتى في غياب نص تشريعي صريح.
- الاعتراف بالضرر المعنوي الناتج عن انتحال الهوية الرقمية كأساس للتعويض، دون اشتراط ضرر مالي مباشر.

ثالثاً، على مستوى المؤسسات:
- إلزام جهات إصدار الهوية الرقمية بتطبيق معايير أمنية دولية معتمدة.
- إنشاء هيئات وطنية مستقلة للإشراف على حماية الهوية الرقمية، تتمتع بصلاحيات رقابية وعقوبات فعالة.
- تطوير آليات بديلة لتسوية المنازعات (ADR) تكون سريعة، سرية، ومنخفضة التكلفة.

رابعاً، على مستوى البحث الأكاديمي:
- تشجيع الدراسات المقارنة في مجال الهوية الرقمية، 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 هوية رقمية محمية قانونياً. فالهوية الرقمية ليست مجرد رمز أو كلمة مرور، 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

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 المعاملات الإلكترونية الإماراتي رقم 1 لسنة 2006
16. قانون المعاملات الإلكترونية السعودي، نظام رقم م/27 لسنة 1440ه
17. توجيه الاتحاد الأوروبي eIDAS رقم 2014/910
18. اللائحة العامة لحماية البيانات (GDPR)، Regulation (EU) 2016/679
19. قانون التوقيع الإلكتروني الأمريكي (E-SIGN Act) لسنة 2000
20. قانون خصوصية المستهلك بكاليفورنيا (CCPA) لسنة 2018

ثالثاً: الأحكام القضائية
21. محكمة العدل الأوروبية، قضية Google Spain SL ضد Agencia Española de Protección de Datos، C-131/12، 2014
22. محكمة العدل الأوروبية، قضية Schrems II،

C-311/18، 2020
23. المحكمة العليا الأمريكية، Riley v. California، 573 U.S. 373، 2014
24. المحكمة العليا الأمريكية، Carpenter v. United States، 585 U.S. ___، 2018
25. محكمة الاستئناف الفيدرالية (الدائرة الحادية عشرة)، In re: Equifax Inc. Customer Data Security Breach Litigation، 2019

رابعاً: المؤلفات الأجنبية
26. Solove Daniel J، Understanding Privacy، Harvard University Press، 2008
27. Nissenbaum Helen، Privacy in Context: Technology, Policy, and the Integrity of Social Life، Stanford University Press، 2010
28. Zarsky Tal Z، Automated Discrimination and Digital Identity، in Digital Enlightenment Yearbook، IOS Press، 2013
29. Mantelero Alessandro، Personal Data

for Decisional Purposes in the Age of Analytics، Computer Law & Security Review، Vol. 32، 2016
30. Werbach Kevin، The Blockchain and the New Architecture of Trust، MIT Press، 2018

خامساً: الوثائق الدولية والتقارير

31. الأمم المتحدة، اتفاقية بشأن استخدام الخطابات الإلكترونية في العقود التجارية، 2005
32. اليونيدروا، نموذج قانون بشأن المعاملات الإلكترونية، 1996
33. منظمة التعاون والتنمية الاقتصادية (OECD)، Guidelines on the Protection of Privacy and Transborder Flows of Personal Data، 2013
34. المفوضية الأوروبية، تقرير عن تنفيذ توجيه eIDAS، 2023
35. البنك الدولي، تقرير حول الهوية الرقمية والتنمية، 2022

سادساً: مقالات أكاديمية

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

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

38. Al-Mansoori Fatima، Digital Identity and Consumer Rights in the GCC، Gulf Law Review، Vol. 8، 2025

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

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

سابعاً: مصادر إلكترونية موثوقة
41. الموقع الرسمي للمفوضية الأوروبية – قسم الهوية الرقمية: https://digital-strategy.ec.europa.eu
42. موقع مركز المعلومات الوطني المصري: https://www.nic.gov.eg
43. موقع الهيئة الوطنية لحماية البيانات الشخصية (تونس): https://www.inpdp.tn
44. موقع المحكمة العليا الأمريكية: https://www.supremecourt.gov
45. موقع محكمة العدل الأوروبية: https://curia.europa.eu

تم بحمد الله وتوفيقه