

اسم الباحث:
ماجد سعد القرني





مادة/ دراسات نقدية

التكليف الثالث

مقدمة:

أصبحت حماية البيانات الشخصية من أهم القضايا القانونية في العصر الرقمي نتيجة التوسع الهائل في استخدام التطبيقات الذكية ومنصات التواصل الاجتماعي وتقنيات إنترنت الأشياء والذكاء الاصطناعي. وقد تبنت غالبية التشريعات الحديثة الخاصة بحماية البيانات الشخصية مبدأ "الموافقة الصريحة المسبقة" كأساس قانوني يضيف المشروعية على عمليات جمع البيانات ومعالجتها، ويقوم هذا المبدأ على افتراض أن الفرد يمتلك القدرة على اتخاذ قرار حر وواع بشأن بياناته الشخصية بعد اطلاعه على شروط وسياسات الخصوصية المقدمة إليه. غير أن التطور التقني المتسارع وظهور اقتصاد البيانات الضخمة أثارا تساؤلات جوهرية حول مدى واقعية هذا الافتراض ومدى كفاءة الموافقة كأداة قانونية لحماية الخصوصية فقد تحولت الموافقة في كثير من الحالات إلى إجراء شكلي يفتقر إلى المعنى الحقيقي، الأمر الذي يستوجب إعادة تقييم هذا الأساس القانوني والبحث عن نماذج أكثر فعالية لحماية الأفراد في البيئة الرقمية الحديثة.

أولاً: نقد مبدأ الموافقة الصريحة في عصر البيانات الضخمة وإنترنت الأشياء:

يقوم مبدأ الموافقة الصريحة على فكرة أن المستخدم يفهم طبيعة البيانات التي ستُجمع عنه، والأغراض التي ستُستخدم من أجلها، والجهات التي قد تشاركها لاحقاً. إلا أن هذا التصور يصطدم بواقع البيئة الرقمية المعاصرة التي تتسم بالتعقيد التقني والتغير المستمر في أساليب معالجة البيانات.

ففي ظل تقنيات البيانات الضخمة لا تقتصر المعالجة على الغرض الذي جُمعت البيانات من أجله ابتداءً، بل تمتد إلى عمليات تحليل واستنتاج وتنبؤ مستقبلية قد لا تكون معروفة حتى لمطوري النظام عند لحظة الحصول على الموافقة، وبالتالي تصبح الموافقة غير قادرة على الإحاطة بجميع أوجه المعالجة المحتملة، مما يفقدها شرط العلم الكافي الذي تقوم عليه الإرادة القانونية السليمة.

كما أن انتشار أجهزة إنترنت الأشياء أدى إلى جمع البيانات بصورة مستمرة وتلقائية من خلال الهواتف الذكية والساعات الذكية والكاميرات المنزلية وأجهزة الاستشعار المختلفة. وفي مثل هذه البيانات يصعب عملياً الحصول على موافقة حقيقية ومستنيرة لكل عملية معالجة تتم في الزمن الحقيقي.

وعليه فإن الاعتماد على الموافقة كوسيلة رئيسية للحماية أصبح غير متناسب مع حجم البيانات المتدفقة وسرعة تداولها.

ومن الناحية العملية، فإن المستخدم لا يمتلك القدرة التقنية أو القانونية الكافية لتقييم المخاطر المرتبطة بمعالجة بياناته، خاصة عندما تتعلق بخوارزميات معقدة أو تقنيات تعلم الآلة. ومن ثم فإن افتراض قدرة الفرد على اتخاذ قرار واعٍ في جميع الحالات يمثل افتراضاً نظرياً أكثر منه واقعاً عملياً.

ثانياً: تحوّل الموافقة إلى عقد إذعان رقمي شكلي:

من أبرز الانتقادات الموجهة لمبدأ الموافقة أنه تحول في الواقع العملي إلى ما يشبه عقد الإذعان الرقمي فعند استخدام التطبيقات أو المواقع الإلكترونية يُطلب من المستخدم الموافقة على سياسة الخصوصية وشروط الاستخدام كشرط أساسي للاستفادة من الخدمة، دون وجود إمكانية حقيقية للتفاوض أو تعديل الشروط.

وتتسم سياسات الخصوصية غالباً بالطول والتعقيد وكثرة المصطلحات التقنية والقانونية، الأمر الذي يجعل قراءتها وفهمها أمراً شاقاً بالنسبة للمستخدم العادي وقد أظهرت العديد من الدراسات أن معظم المستخدمين يضغطون على زر "أوافق" دون قراءة الشروط أو فهم آثارها القانونية، وذلك رغبة في الوصول السريع إلى الخدمة المطلوبة.

وفي هذه الحالة تصبح الموافقة مجرد إجراء شكلي لا يعكس إرادة حرة ومستنيرة، بل تعبر عن حاجة المستخدم إلى الخدمة الرقمية أكثر مما تعبر عن قبوله الحقيقي لسياسات معالجة البيانات. كما أن رفض الموافقة يؤدي غالباً إلى حرمان المستخدم من الوصول إلى الخدمة بالكامل، مما يخلق اختلالاً واضحاً في مراكز القوة التعاقدية بين الشركات التقنية والأفراد.

وعليه فإن الموافقة الرقمية الحالية لا تختلف في جوهرها عن عقود الإذعان التقليدية، بل قد تكون أكثر خطورة نظراً لعدم وضوح آثارها المستقبلية المتعلقة بالبيانات الشخصية وإمكانية إعادة استخدامها وتحليلها بطرق متعددة وغير متوقعة.

ثالثاً: قصور النص القانوني المحلي في توفير الحماية التقنية الفعلية:

على الرغم من أن التشريعات الوطنية الحديثة تمنح الأفراد مجموعة من الحقوق المرتبطة ببياناتهم الشخصية، مثل الحق في العلم والحق في الوصول والحق في التصحيح والحذف، إلا أن هذه الحقوق تظل في كثير من الأحيان ذات طبيعة قانونية شكلية أكثر من كونها ضمانات تقنية فعالة.

فالنصوص القانونية تركز بصورة كبيرة على تنظيم إجراءات الحصول على الموافقة، لكنها لا تفرض دائماً التزامات تقنية صارمة على الجهات المعالجة للبيانات تضمن الحد الأدنى من الجمع أو تمنع التتبع المفرط أو تحد من إعادة استخدام البيانات في أغراض جديدة. كما أن الفرد غالباً لا يملك الوسائل التقنية اللازمة للتحقق من كيفية استخدام بياناته فعلياً بعد جمعها.

إضافة إلى ذلك فإن التطور التقني يسير بوتيرة أسرع من قدرة التشريعات على التحديث والمواكبة، مما يؤدي إلى ظهور فجوة بين الحماية القانونية النظرية والمخاطر التقنية الواقعية. لذلك فإن الاقتصار على الموافقة باعتبارها حجر الأساس للحماية يؤدي إلى نقل عبء المسؤولية بالكامل إلى المستخدم، رغم كونه الطرف الأضعف والأقل معرفة في العلاقة الرقمية. ومن ثم فإن فعالية الحماية لا ينبغي أن تقاس بوجود موافقة شكلية، وإنما بمدى قدرة النظام التقني ذاته على منع الانتهاكات وتقليل المخاطر قبل وقوعها.

رابعاً: نحو مبدأ بديل قائم على الخصوصية بالتشديد والافتراض:
في ضوء الانتقادات السابقة، يبرز مبدأ "الخصوصية بالتشديد والافتراض" (Privacy by Design and by Default) بوصفه بديلاً أكثر واقعية وفعالية من الاعتماد الحصري على الموافقة يقوم هذا المبدأ على دمج متطلبات حماية البيانات في تصميم الأنظمة والتطبيقات منذ المراحل الأولى للتطوير، بحيث تصبح الخصوصية جزءاً أصيلاً من البنية التقنية وليس مجرد التزام قانوني لاحق كما يقتضي أن تكون الإعدادات الافتراضية للنظام هي الأكثر حماية للخصوصية دون حاجة إلى تدخل المستخدم.

ويترتب على هذا المبدأ التزام الجهات المعالجة للبيانات بعدد من الضمانات، أهمها:

- تقليل جمع البيانات إلى الحد الأدنى اللازم لتحقيق الغرض المحدد.
 - تفعيل إعدادات الخصوصية القصوى بشكل افتراضي.
 - استخدام تقنيات التشفير وإخفاء الهوية وحماية البيانات.
 - إجراء تقييمات دورية لأثر المعالجة على الخصوصية.
 - تحميل الجهة المعالجة مسؤولية إثبات سلامة إجراءاتها التقنية بدلاً من تحميل المستخدم عبء الحماية.
- وبذلك تنتقل الحماية من نموذج قائم على موافقة الفرد إلى نموذج وقائي استباقي يجعل الخصوصية جزءاً من تصميم النظام ذاته، وهو ما يتلاءم بصورة أكبر مع واقع البيانات الضخمة وإنترنت الأشياء.

خاتمة:

يتضح أن مبدأ الموافقة الصريحة المسبقة رغم أهميته التاريخية في تشريعات حماية البيانات الشخصية، لم يعد كافياً لتحقيق حماية فعالة في البيئة الرقمية الحديثة. فقد أدى تعقيد التقنيات الرقمية وانتشار البيانات الضخمة وإنترنت الأشياء إلى إضعاف قدرة الأفراد على اتخاذ قرارات واعية بشأن بياناتهم، كما تحولت الموافقة في التطبيق العملي إلى شكل من أشكال الإذعان الرقمي الذي يفتقر إلى الإرادة الحقيقية والمعرفة الكافية.

كما أن التركيز التشريعي على الموافقة لا يوفر حماية تقنية فعلية للبيانات، بل ينقل عبء الحماية إلى المستخدم الذي يفتقر غالباً إلى المعرفة والقدرة اللازمة لمواجهة الشركات التقنية الكبرى. لذلك فإن الاتجاه نحو مبدأ الخصوصية بالتشديد والافتراض يمثل حلاً أكثر كفاءة وواقعية، لأنه يفرض الحماية داخل التصميم التقني نفسه ويجعل الخصوصية التزاماً أصيلاً على عاتق الجهات المعالجة للبيانات، الأمر الذي يحقق توازناً أفضل بين التطور التقني وحماية الحقوق الأساسية للأفراد.