# الموافقة على المعالجة الرقمية للبيانات الشخصية

# "دراسة مقارنة"


**د. الصغير محمد مهدى**

**أستاذ القانون المدنى المساعد- كلية الحقوق- جامعة أسوان**

**أستاذ القانون المدنى المساعد- كلية القانون- جامعة أبوظبى**

(ISSN: 2537- 0758)

# الموافقة على المعالجة الرقمية للبيانات الشخصية
# "دراسة مقارنة"

د. الصغير محمد مهدى

**الملخص**:

أضحى مفهوم الموافقة بشأن معالجة البيانات الشخصية محط اهتمام كبير في النظم القانونية الحديثة، سواء على المستوى الأوروبي أو المصري، أو الاماراتى، ونظرًا لأهميته في تمكين الأفراد من ممارسة رقابة فعّالة على بياناتهم الشخصية والتحكم في استخدامها، خاصة في ظل الانتشار الواسع للفضاء الإلكتروني الذي يتضمن المواقع والتطبيقات الإلكترونية عبر شبكة الإنترنت، وما يصاحب ذلك من انتقال البيانات بين الأجهزة المختلفة، بدءًا من الحواسيب وصولًا إلى الهواتف الذكية والأجهزة اللوحية المحمولة.

ولقد ركزت الدراسة على استجلاء خصوصية هذه الموافقة في ضوء أحكام اللائحة العامة لحماية البيانات الشخصية في الاتحاد الأوروبي (GDPR) والقوانين الوطنية ذات الصلة، لا سيما القانونين الفرنسي والمصري، والاماراتى. وتهدف الدراسة إلى تحليل هذه الموافقة بوصفها مفهومًا ناشئًا في مرحلة التطور، وذلك من خلال الوقوف على تعريفها، وتحديد طبيعتها القانونية، واستعراض شروط التعبير عنها وشكله، باعتبار هذه المسائل متطلبات أساسية لضمان صحة هذا الموافقة وفعاليتها.

كما تناولت الدراسة أهلية الأفراد للتعبير عن الموافقة، مع التركيز على الطبيعة القانونية للنيابة عن القاصر في سياق معالجة البيانات الشخصية، وتحديد نطاق سلطات النائب وحدودها، وآليات التحقق من صحة الموافقة المعبر عنه من قبل النائب. وعلاوة على ذلك، سلطت الدراسة الضوء على الأحكام المرتبطة بهذه الموافقة، بما في ذلك دورها في عملية معالجة البيانات، وإثباتها، وحق الأفراد في العدول عنها.

واختتمت الدراسة بمجموعة من النتائج والتوصيات العلمية والعملية الموجهة إلى المشرّع المصري، والمشرع الاماراتى والتي تهدف إلى المساهمة في تحسين الإطار القانوني لحماية البيانات الشخصية، سواء من خلال تعديل القانون الحالي أو وضع قانون اخر جديد يتماشى والتطور الحادث للحياة الرقمية فى ظل سيطرة الذكاء الاصطناعى عليها، وعلى أمل أن توفر هذه التوصيات رؤى جديدة تدعم تطوير المنظومة التشريعية في هذا المجال.

## المقدمة

### التعريف بموضوع البحث:

شهد العالم في العقود الأخيرة تطورًا تقنيًا هائلًا في مجال تكنولوجيا المعلومات والاتصالات، مدفوعًا بالابتكارات المرتبطة بشبكة الإنترنت، الهواتف الذكية، الأجهزة المحمولة، وتقنيات الذكاء الاصطناعي وغيرها من التطورات التكنولوجية. وقد أدى هذا التطور إلى انتشار استخدام هذه التقنيات بشكل واسع، حتى أصبحت جزءًا لا يتجزأ من مختلف جوانب الحياة المعاصرة. كما كان له أثر عميق على تعزيز نمو الاقتصاد العالمي، حيث أسهم في تحسين الوصول إلى المعلومات وتسهيل التواصل الفوري بين الأفراد في مختلف أنحاء العالم، مما جعلها عنصرًا أساسيًا في الحياة اليومية لا يمكن الاستغناء عنه.

رغم الفوائد الجمة التي جلبتها التطورات التقنية للبشرية ونموها السريع، إلا أنها كشفت عن جانبها السلبي الذي أفرز تهديدات غير مسبوقة للحق في حماية البيانات الشخصية. فقد أصبحت هذه البيانات، في ظل البيئة الرقمية الحديثة، محورًا رئيسيًا لاستهداف خصوصية الأفراد[1]، نتيجة التوسع الكبير في حجم ونطاق تداولها

[1]– انظر: د. محمد عرفات الخطيب، ضمانات الحق في العصر الرقمي: "من تبدل المفهوم. . لتبدل الحماية" قراءة في الموقف التشريعي الأوروبي والفرنسي وإسقاط على الموقف التشريعي الكويت، مجلة كلية القانون الكويتية العالمية، المجلد ٦، ملحق خاصة أبحاث المؤتمر السنوي الدولي الخامس ٩–١٠ مايو ٢٠١٨، العدد ٣، الجزء الاول، مايو ٢٠١٨، ص ٢٥٩. وفي

(ISSN: 2537- 0758)

إلكترونيًا، وجمعها ومعالجتها بطرق غير مسبوقة. وقد أدى ذلك إلى بروز قيمتها الاقتصادية والتجارية، لا سيما مع ازدهار المعاملات الإلكترونية واتساع نطاقها، حتى غدت البيانات الشخصية أشبه بـ"العملة الجديدة" في البيئة الرقمية[٢]، ووصفت بأنها "نفط" أو "ذهب القرن الحادي والعشرين"[٣].

هذا الوضع شجع الشركات والمؤسسات، سواء العامة أو الخاصة، والتي تمتلك إمكانات تقنية هائلة، على جمع كميات ضخمة من البيانات الرقمية المتعلقة بالأفراد. ويتم استغلال هذه البيانات في أغراض دعائية وتسويقية من خلال أنظمة تقنية متقدمة تعمل على جمعها، معالجتها، تحليلها، استنباطها، تخزينها، ونقلها، مما يفتح المجال لمزيد من الانتهاكات لخصوصية الأفراد وحقوقهم في هذا المجال[٤].

---

هذا الصدد يؤكد جانب من الفقه على أن حماية الحق في البيانات الشخصية أصبحت أمرًا ضروريًا أكثر من أي وقت مضى؛ لأن التطورات التكنولوجية زادت من خطر إلحاق الضرر بالأفراد، انظر:

Astrid MARAIS, Droits des personnes, 3e éd., Dalloz, 2018, no. 234, p. 159; Laure MARINO, Les nouveaux territoires des droits de la personnalité, Gazette du Palais, no. 139, 18-19 mai 2007, p. 22.

[٢]– تعد "تجارة المعلومات" من أهم مصادر الثروة في الحياة الرقمية، ويدخل في هذه التجارة– على وجه الخصوص– التجارة المتعلقة بالبيانات الشخصية، ليس هذا فحسب، فالبيانات الشخصية تستعمل كذلك لأغراض سياسية وعسكرية وأمنية، ومن هنا يصف البعض– بحق– استغلال البيانات الشخصية بأنها "ظاهرة" بالمعنى الحقيقي لهذا المصطلح الوارد في علم الاجتماع القانوني، وارتبط بها العديد من الأنشطة الإنسانية، لهذا كان لزامًا على القانون التدخل لضبط هذه الظاهرة من خلال التشريع. انظر: دراسة نقدية لقانون حماية البيانات الشخصية رقم ١٥١ لسنة ٢٠٢٠، إعداد مركز بحوث القانون والتكنولوجيا بكلية القانون بالجامعة البريطانية، ٢٠٢٠، وخاصة تقديم الدراسة للدكتور حسن عبد الحميد، ص ٨.

[٣]– في هذا الصدد. انظر: د. عادل عبد الصادق، البيانات الشخصية الصراع على نفط القرن الحادي والعشرين، المركز العربي لأبحاث الفضاء الإلكتروني، ٢٠١٨، ص ٢١.

[٤]– راجع: د. سامح عبد الواحد التهامي، الحماية القانونية للبيانات الشخصية: دراسة في القانون الفرنسي (القسم الأول)، مجلة الحقوق، جامعة الكويت، المجلد ٣٥، العدد ٣، سبتمبر ٢٠١١،

ونظرًا لحجم المخاطر التي تهدد البيانات الشخصية، أصبح من الضروري أن توجه أنظار المشرعين في العديد من الدول نحو وضع أطر قانونية تهدف إلى توفير مستوى مناسب من الحماية لهذه البيانات، بما يحد من الانتهاكات المحتملة لخصوصية أصحابها[٥]. وتهدف هذه الأطر إلى تنظيم مختلف العمليات المتعلقة بالبيانات الشخصية، بما يشمل جمعها، معالجتها، استخدامها، الإفصاح عنها، نقلها، أو حتى إفشائها، وذلك من خلال وضع ضوابط قانونية واضحة وصارمة تكفل الحماية اللازمة لها، مع ضمان احترام حقوق الأفراد وحرياتهم في هذا السياق.

وفي الحقيقة، تعد موافقة صاحب البيانات (Consentement de la personne concernée)، أو ما يمكن تسميتها بالرضاء الرقمي كما يطلق عليها البعض[٦] (Consentement numérique)، الأساس المحوري لحماية البيانات

---

ص ٣٧٧؛ د. محمد سامي عبد الصادق، شبكات التواصل الاجتماعي ومخاطر انتهاك الحق في الخصوصية، دار النهضة العربية، القاهرة، ٢٠١٦، ص ٥٩. وراجع أيضًا: تقرير اللجنة المشتركة من لجنة الاتصالات وتكنولوجيا المعلومات ومكاتب لجان الشئون الدستورية والتشريعية والخطة والموازنة والدفاع والأمن القومي، حول مشروع قانون بشأن إصدار قانون حماية البيانات الشخصية، بتاريخ ٩ يوليو ٢٠١٩، ص ٨ وما بعدها. متاح على الموقع التالي:http: //www. elwatannews. com/data/pdf/iframe/pdf/25021748. pdf.

(٥)– في هذا المعنى، انظر: د. محمود عبد الرحمن، التطورات الحديثة لمفهوم الحق في الخصوصية (الحق في الخصوصية المعلوماتية)، مجلة كلية القانون الكويتية العالمية، العدد التاسع، السنة الثالثة، مارس ٢٠١٥، ص ١٠٦.

(٦)– حيث يفضل البعض من الفقة استخدام لفظ "الرضاء" ولم يجرى على استخدام لفظ "الرضا" رغم استخدامه أحيانًا من قبل البعض الاخر من الفقه، ويأتي ذلك اتساقًا حسب الراى الاول مع نهج القانون المدني المصري، حين أشار إليه عند تناوله لأركان العقد (في الفصل الأول من الباب الأول من الكتاب الأول منه)، وما ورد بالأعمال التحضيرية لهذا القانون، وشيوع استخدامه من قبل غالبية الفقه المصري. انظر: تامر محمد الدمياطى، الرضاء الرقمى بمعالجة البيانات الشخصية، دراسة مقارنة، مجلة القانون والتكنولوجيا، المجلد ٢، العدد ١، ابريل ٢٠٢٢، من ص ١٥ وما بعدها.

(ISSN: 2537- 0758)

الشخصية. فهى تمثل إحدى أهم الأدوات التشريعية التي اعتمدها المشرّع لضمان صحة ومشروعية عمليات جمع ومعالجة البيانات.

ويتطلب هذا الرضاء أن يصدر عن إرادة حرة واعية، خالية من أي عيب يؤثر على صحته، مما يجعله شرطًا جوهريًا لبدء أي عملية تتعلق بمعالجة البيانات الشخصية. وعليه، لا يمكن إجراء أي معالجة للبيانات دون الحصول على رضاء صريح من الشخص المعني، باستثناء حالات محددة تم حصرها بموجب القوانين ذات الصلة، لضمان التوازن بين حق الأفراد في حماية بياناتهم ومتطلبات المعالجة المشروعة.

وفى هذا الاطار يُعد الرضاء (Le consentement) حجر الزاوية في القانون المدني، كونه الأساس الذي يقوم عليه العقد، حيث لا يمكن تصور وجود رابطة عقدية دون توفر رضاء صحيح وصريح[٧]، ولكن لم يكن لهذا المفهوم نفس القدر من الأهمية في مجال حماية البيانات الشخصية حتى وقت قريب.

وقد بدأ الاهتمام الحقيقي بالموافقة أو بمفهوم الرضاء الرقمي كوسيلة لحماية البيانات الشخصية مع إقرار البرلمان والمجلس الأوروبي للتوجيه رقم ٩٥/٤٦ المؤرخ في ٢٤ أكتوبر ١٩٩٥[٨]. وقد مثل هذا التوجيه نقلة نوعية، حيث اعترف بالموافقة أو بالرضاء كأساس لمشروعية معالجة البيانات الشخصية. في ذلك الوقت، و كان هذا التوجيه الإطار التشريعي الرئيسي للاتحاد الأوروبي في مجال حماية البيانات،

---

[٧]– انظر: د. عبد الفتاح عبد الباقي، موسوعة القانون المدني المصري، نظرية العقد والإرادة المنفردة، دراسة معمقة ومقارنة بالفقه الإسلامي، الكتاب الأول، دار نهضة مصر للطباعة والنشر، ١٩٨٤، ص ٨٨: د. محمد حسن قاسم، القانون المدنى، الالتزامات، المصادر، ١– العقد، المجلد الاول– دراسة فقهية قضائية مقارنة في ضوء التوجهات التشريعية والقضائية الحديثة وقانون العقود الفرنسي الجديدة ٢٠١٦، دار الجامعة الجديدة، ٢٠١٧، ص ١٠٢.

[8]- Directive 95/46/CE du parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitment des données à caractère personnel et à la libre circulation de ces données, JOCE, no. L. 281/31, 23 nov. 1995 .

وأرسى مبادئ أساسية تنظم جمع البيانات الشخصية ومعالجتها، مع التركيز على أهمية الحصول على موافقة أو رضاء واضح من الأفراد لضمان احترام حقوقهم وحرياتهم في البيئة الرقمية.

من جهة أخرى، تجدر الإشارة إلى أن المشرّع الفرنسي كان من أوائل المشرّعين الذين أولوا اهتمامًا بحماية البيانات الشخصية، حيث أصدر القانون رقم ١٧ لسنة ١٩٧٨ المؤرخ في ٦ يناير ١٩٧٨ والمعروف باسم قانون المعلوماتية والحريات (La loi) (Informatique et Liberté)[٩] وعلى الرغم من أهمية هذا القانون في توفير إطار تنظيمي لحماية البيانات، إلا أنه لم يركز بشكل كبير على عنصر الموافقة أو الرضاء في سياق حماية البيانات الشخصية.

ظل هذا الوضع قائمًا حتى صدور التوجيه الأوروبي رقم ٩٥/٤٦، الذي أرسى مبدأ الرضاء أو الموافقة كأساس لمعالجة البيانات الشخصية. وقد تبنى المشرّع الفرنسي هذا المبدأ من خلال القانون رقم ٨٠١ لسنة ٢٠٠٤ المؤرخ في ٦ أغسطس ٢٠٠٤، المتعلق بحماية الأشخاص الطبيعيين في سياق معالجة البيانات الشخصية[١٠]. وبموجب هذا القانون، أصبح الرضاء أو الموافقة عنصرًا أساسيًا يُعتد به لضمان مشروعية معالجة البيانات[١١]، مما عكس تطورًا هامًا في التشريعات الفرنسية تماشيًا مع المعايير الأوروبية في هذا المجال[١٢].

---

(9)- Directive 95/46/CE du parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitment des données à caractère personnel et à la libre circulation de ces données, JOCE, no. L. 281/31, 23 nov. 1995 .

(10)- Loi n° 78-17 du 6 janvier 1978 relative à l'informtaique, aux fichiers et aux libertés, JORF du 7 janvier 1978 .

(11)- Anne DEBET, Jean MASSOT et Nathalie METALLINOS, Informatique et libertés: La protectiob des données à caractère en droit français et européen, Lextenso, 2015, n° 624 s .

(12)- Loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitments de données à caractère personnel, JORF 7 aout .

(ISSN: 2537- 0758)

ومع ذلك، لم يحظَ الرضاء الرقمي أو الموافقة الرقمية بالدور القانوني المؤثر بشكل حقيقي إلا مع إصدار البرلمان والمجلس الأوروبي اللائحة العامة لحماية البيانات الشخصية (General Data Protection Regulation- GDPR) رقم ٢٠١٦/٦٧٩، الصادرة بتاريخ ٢٧ أبريل ٢٠١٦[١٣].

وتُعد هذه اللائحة خطوة محورية في مجال حماية البيانات الشخصية، حيث ركزت على حماية الأشخاص الطبيعيين في سياق معالجة بياناتهم الشخصية، مع تعزيز حرية نقل هذه البيانات بين الدول الأعضاء. كما ألغت اللائحة التوجيه الأوروبي رقم ٩٥/٤٦، الذي كان سابقًا الإطار التشريعي الرئيسي في هذا المجال.

وتمثل اللائحة الأوروبية، كما يُشار إليها، قانونًا نموذجيًا أصبح مرجعًا للعديد من التشريعات الوطنية داخل الاتحاد الأوروبي وخارجه. وقد عززت بشكل خاص دور الرضاء الرقمي أو الموافقة الرقمية كعنصر رئيسي لضمان مشروعية معالجة البيانات الشخصية، مما جعلها معيارًا عالميًا في مجال حماية البيانات الشخصية[١٤].

---

[١٣]– ويطلق عليها بالفرنسية (RGPD) Le règlement general dur la protection des données (RGPD)، ولكن نفضل في هذا الإطار استعمال ما درج عليه العمل من استخدام المصطلح باللغة الإنجليزية (GDPR).

Règlement (UE) 2016/679 du Parment européen du Conseil du 27 avril 2016, relative à la protection des personnes physiques à l'égard du traitment des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement general sur la protection des données). Journal official de l'Union européenne, L 119/1, 4 mai 2016 .

[١٤]– كما أكد ميثاق الحقوق الأساسية للاتحاد الأوربي Charte des droits fondamentaux de l'Union européne الصادر في يونيو ٢٠١٦، على أهمية الرضاء الرقمي، حيث نصت المادة الثامنة منه على أن: "١– لكل شخص الحق في حماية البيانات الشخصية المتعلقة به. ٢– ويجب معالجة هذه البيانات بشكل عادل، ولأغراض محددة وعلى أساس رضاء صاحب البيانات أو على أساس آخر مشروع ينص عليه القانون..".

Journal official de l'Union européne, 7 Juin 2016, C 202/02 .

فـي الواقـع، تمكـن المشرّع الأوروبـي مـن التعامـل بفعاليـة مـع انتشـار اسـتخدام التكنولوجيـا الحديثـة، مـن خـلال وضـع تنظيم دقيـق لحمايـة البيانـات الشخصـية فـي سـياق التعامـل الرقمـي. وقـد عـززت اللائحـة العامـة لحمايـة البيانـات الشخصـية (GDPR)، منذ دخولها حيز التنفيذ في ٢٥ مايو ٢٠١٨، دور الموافقة أو الرضاء في هذا المجال، حيث أبرزت أهميته كأداة محورية لضمان مشروعية معالجة البيانات الشخصية.

**علاوة على ذلك**، ساهمت الأحكام القضائية الصادرة عن محكمة العدل التابعة للاتحـاد الأوروبـي[١٥](CJUE) فـي توضـيح أهميـة الموافقـة أو الرضـاء وتعزيـز مكانتـه[١٦]. ومنـذ ذلـك الحـين، أصـبحت الموافقـة أو الرضـاء يشـكل بحـق "المركـز العصبي لهذه الحماية، والمحدد الأساسي لمشروعية عمليات معالجة البيانات"[١٧].

---

[١٥]– تم إنشاء محكمة العدل الأوروبية La Cour de Justice de l'Union Européenne (CJUE) عام ١٩٥٢. ومقرها في لوكسمبورغ، وتتمثل مهمتها في ضمان احترام القانون في تفسير وتطبيق المعاهدات، وعملاً على تنفيذ هذه المهمة، فإن المحكمة يكون لها أن تراقب مشروعية أعمال مؤسسات الاتحاد الأوروبي، والتأكد من أن الدول الأعضاء تمتثل للالتزامات الناشئة عن المعاهدات، وتفسير قانون الاتحاد الأوروبي بناءً على طلب القضاة الوطنيين، وبالتالي فهي تعد السلطة القضائية للاتحاد الأوروبي وتكفل– بالتعاون مع محاكم الدول الأعضاء– التطبيق والتفسير الموحد لقانون الاتحاد. لمزيد من التفصيل راجع موقع المحكمة التالي: https: //curia. europa. eu/jcms/jcms/j_6/fr

[١٦]– انظر على سبيل المثال. حكم محكمة العدل الأوروبية الصادر في ١١ نوفمبر ٢٠٢٠، القضية رقم (C–١٩/٦١):

Cour de justice de l'Union européenne (2ème chamber), Arrêt du 11 novembre 2020, Affaire C-61/19, Journal official de l'Union européenne, 18 janvier 2021/ C 19/4 .

وكذلك حكمها الصادر في الأول من أكتوبر ٢٠١٩، القضية رقم (C– ٦٧٣/ ١٧):

Cour de justice fr l'Union europénne (grande chamber), Arrêt du ler octobre 2019, Planet49 GmbH, Afaire C-673/17, Journal official de l'Union européenne, 9 décembre 2019/C 413/04 .

[17]- Céline CASTETS-RENARD, Brève analyse du règlement general de la protection des données, Dalloz IP/IT, Juillet-Août 2016, p. 331 .

(ISSN: 2537- 0758)

كما يُعد من بين أبرز التحولات التي أدخلتها اللائحة الأوروبية لتعزيز حقوق الأفراد في مواجهة التحديات الرقمية المتزايدة[١٨].

ومع ذلك، لم تنص اللائحة على قاعدة عامة وشاملة بشأن الموافقة أو الرضاء في إطار حماية البيانات الشخصية[١٩]، مما أدى إلى ظهور غموض نسبي بشأن دوره في بعض السياقات. ومع ذلك، يظل من المؤكد أن الموافقة أو الرضاء أصبح يؤدي دورًا متزايد الأهمية في تعزيز الحماية القانونية للبيانات الشخصية، مما يعكس تطورًا ملحوظًا في التشريعات الأوروبية الموجهة نحو ضمان حقوق الأفراد في البيئة الرقمية[٢٠].

---

[١٨]– في شأن تعزيز حقوق الأفراد في اللائحة العامة لحماية البيانات GDPR، انظر:

Bathalie MARTAL-BRAZ, Le renforecement des droit de la personne concernée, Dalloz IP/T 2017, p. 253 ets .

[١٩]– وفي هذا الخصوص، يتحرز بعض الفقه من خطورة المبالغة في منح عنصر الرضاء أهمية على حساب الهدف من حماية البيانات، فيقول: "إذا كانت الرغبة في وضع الشخص في بؤرة حماية البيانات تمثل بلا شك تطورًا هامًا ومفيدًا لحقه، فيجب على المرء مع ذلك ألا يبالغ في منح الرضاء على المعالجة دورًا بالغ الأهمية، يمكن أن يضحى بالهدف الأساسي للحماية؛ لذا يجب أن تجد إرادة الشخص نظامًا عامًا قويًا يحميها".

Fanny ROGUE, Capacité et consentement au traitement de données à caractère personnel et au contrat, AJ Contrat (Actualité Juridique Contrat), Dalloz, Août-Septembre 2019, p. 370 .

[٢٠]– ركز واضعو اللائحة العامة لحماية البيانات GDPR كثيرًا على الرضاء، إذ جرى استخدامه ٦٨ مرة في هذه اللائحة مقابل ١٢ مرة في التوجيه الأوروبي رقم ٤٦/ ٩٥. في حين كان التوجيه المشار إليه يورد تعريفًا دقيقًا للرضاء، فإن اللائحة العامة لحماية البيانات GDPR جاءت أكثر تفصيلاً في هذا الشأن، فتصدت للتساؤلات التي تركها هذا التوجيه مفتوحة. وخاصة مسألة رضاء الأطفال، وأخيرًا حظى الرضاء بدور في تقييد معالجة البيانات الشخصية الحساسة ونقل البيانات الشخصية. انظر:

Anne DEBET, LE consentement dans le Règlement Général sur la Protection des données, Rôle et definition, Revue Communication commerce électronique. 2018, Eude n° 9, pp. 37- 44, spec. no. 1 .

وتماشـيًا مـع أحكـام اللائحـة الأوروبيـة العامـة لحمايـة البيانـات الشخصـية (GDPR)، أصدر المشرّع الفرنسي القانون رقم ٤٩٣ لسنة ٢٠١٨ بتاريخ ٢٠ يونيو ٢٠١٨ بشأن حماية البيانات الشخصية[٢١]. ويهدف هذا القانون إلى تعديل قانون المعلوماتية والحريات رقم ١٧ لسنة ١٩٧٨بما يتوافق مع المعايير الجديدة التي أقرّتها اللائحة الأوروبية[٢٢].

**علاوة على ذلك**، تم إصدار الأمر رقم ١١٢٥ لسنة ٢٠١٨ لتطبيق أحكام هذا القانون، مما ساهم في تطويع القواعد القانونية الفرنسية بما ينسجم مع متطلبات اللائحة الأوروبية. وقد مثّلت هذه التعديلات خطوة مهمة لضمان اتساق التشريعات الفرنسية مع المعايير الأوروبية وتعزيز حماية البيانات الشخصية على المستويين الوطني والدولي[٢٣].

---

(21)- Loi n° 2018- 493 du 20 Juin 2018 relative à la protection des données personelle, et portant modification de la loi n° 78-17 6 janvier 1978 relative à l'informatique, aux fichers et aux libertés et diverses dispositions concernant la protection des données à carcatère personnel, JORF n° 0 141 du 21 juin 2018 .

[٢٢]– جدير بالذكر أن هذا القانون يتعلق بحسب الأصل بالمعلوماتية والملفات والحريات l'informatique aux fichiers et aux libertés، ولكن درج العمل على اختصار تسميته إلى "قانون المعلوماتية والحريات".

[٢٣]– الأمر رقم ١١٢٥– ٢٠١٨ المؤرخ ١٢ ديسمبر ٢٠١٨ الصادر تطبيقًا للمادة ٣٢ من القانون رقم ٤٩٣– ٢٠١٨ المؤرخ ٢٠ من يونيو ٢٠١٨ بشأن حماية البيانات الشخصية وتعديل القانون رقم ٧٨– ٧٨ الصادر في ٦ يناير ١٩٧٨ المتعلق بالمعلوماتية والملفات والحريات".

Ordonnance n° 2018- 1125 du 12 décembre 2018 prise en application de l'article 32 de la loi no 2018- 493 du 20 juin 2018 relative à la protection des données personnelles et portant modification de la loi no 78- 17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et diverses disposition concernant la poritection des données à caractère personnel, JORF no 0288 du 13 décembre 2018, Text 5 .

كذلك صدر المرسوم رقم ٥٣٦– ٢٠١٩ المؤرخ ٢٩ مايو ٢٠١٩ بشأن تطبيق القانون رقم ١٧–٧٨ الصادر في ٦ يناير ١٩٧٨ المتعلق بالمعلوماتية والملفات والحريات المعدل بموجب الأمر رقم

(ISSN: 2537- 0758)

ومؤخرًا، أدرك المشرّع المصري أن تنظيم وحماية البيانات الشخصية أصبح ضرورة ملحّة وحيوية في ظل التحولات الرقمية المتسارعة. وفي هذا السياق، أصدر قانون حماية البيانات الشخصية رقم ١٥١ لسنة ٢٠٢٠[٢٤]، في محاولة للحاق بركب التشريعات العالمية المنظمة لهذا المجال.

ومع ذلك، فقد تضمن القانون بعض الجوانب التي شابها الغموض، لا سيما فيما يتعلق بمفهوم موافقة أو رضاء صاحب البيانات، الذي يُشار إليه في النصوص المصرية بـ "الشخص المعني بالبيانات"[٢٥]. وقد فضّل المشرّع المصري استخدام مصطلح "الموافقة "بدلًا من المصطلح الأكثر شيوعًا في اللغة القانونية و لدى الكثير من الفقه وهو "الرضاء". ورغم أن "الرضاء" يُعتبر مصطلحًا قانونيًا راسخًا، خصوصًا في مجالي القانون المدني والقانون الجنائي، إلا أن استخدام مصطلح "الموافقة" قد

---

٢٠١٨– ١١٢٥ المؤرخ ١٢ ديسمبر ٢٠١٨ (JORF, 30 mai 2019 text 16) وهدفه الرئيسي هو مواءمة القانون الفرنسي مع اللائحة الأوروبية لحماية البيانات (GDPR). واعتماد بعض القواعد الإجرائية أمام اللجنة الوطنية للمعلوماتية والحريات (CNIL).

[٢٤]– الجريدة الرسمية– المصرية العدد ٢٨ مكرر (هـ) في ٢٥ يوليو ٢٠٢٠.

[٢٥]– تعرف المادة ١ من قانون حماية البيانات المصري "الشخص المعني بالبيانات" بأنه: "أي شخص طبيعي تُنسب إليه بيانات شحصية معالجة إلكترونيًا تدل عليه قانونًا أو فعلاً، وتُمكن من تمييزه عن غيره". كما عرفت المادة ٤ بند ١ من اللائحة التعرف عليه أو يمكن تحديده بشكل مباشر أو غير مباشر، وخاصة بالرجوع إلى رقم الهوية أو إلى عامل أو أكثر من العوامل المحددة لهويته البدنية أو الفسيولوجية أو العقلية أو الاقتصادية أو الاجتماعية". كذلك يُعرفه المشرع الفرنسي في قانون المعلوماتية والحريات المعدل بأنه "كل شخص طبيعي تكون بياناته الشخصية موضوعًا للمعالجة (م٢ من القانون). ويستفاد من ذلك أن المشرع المصري حصر الشخص المعنى بالبيانات في نطاق الشخص الطبيعي. منتهجًا طريق المشرع الأوروبي، ومن ثم يقتصر نطاق الحماية على الشخص الطبيعي فقط دون الشخص الاعتباري".

أثار لدى البعض من الفقه، بعض التساؤلات حول مدى وضوحه ودقته في التعبير عن جوهر المعنى القانوني المطلوب[٢٦].

ورغم ما قد يشوب قانون حماية البيانات الشخصية رقم ١٥١ لسنة ٢٠٢٠ من بعض الغموض، إلا أن صدوره يُعد خطوة تشريعية بالغة الأهمية في مسار تأمين البيانات الشخصية المعالجة إلكترونيًا[٢٧]. و يُمكن للقانون أن يلبي الحاجة الملحّة للنظام القانوني المصري إلى وجود إطار عام ينظم عمليات حماية البيانات الشخصية، سواء أثناء جمعها أو تخزينها أو معالجتها أو تداولها، مما يعكس إدراكًا متزايدًا بأهمية وضع ضوابط قانونية تواكب التطورات التقنية وتحمي خصوصية الأفراد في البيئة الرقمية.

وفى دولة الإمارات العربية المتحدة فان القانون المنظم لحماية البيانات الشخصية هو القانون الاتحادي رقم ٤٥ لسنة ٢٠٢١ بشأن حماية البيانات الشخصية. حيث يُعد هذا القانون خطوة متقدمة في إطار تعزيز الخصوصية وضمان حماية البيانات

---

[٢٦]– تامر محمد الدمياطى، الرضاء الرقمى بمعالجة البيانات الشخصية، مرجع سابق، ص ١٩ وما بعدها.

[٢٧]– يقصد بالبيانات الشخصية، وفقًا للمادة ١ من قانون البيانات الشخصية المصري ١٥١ لسنة ٢٠٢٠، "أي بيانات متعلقة بشخص طبيعي محدد، أو يمكن تحديده بشكل مباشر أو غير مباشر عن طريق الربط بين هذه البيانات وأي بيانات أخرى، كالاسم أو الصوت، أو الصورة، أو رقم تعريفي، أو محدد للهوية عبر الإنترنت، أو أي بيانات تحدد الهوية النفسية، أو الصحية، أو الاقتصادية، أو الثقافية، أو الاجتماعية، ويتشابه هذا التعريف– إلى حد ما– مع التعريف الوارد في اللائحة الأوروبية، في المادة ٤ بند ١، الذي يجري نصها على ما يلي: البيانات الشخصية "تعنى أي معلومات تتعلق بشخص طبيعي محدد أو قابل للتجديد (يطلق عليه "صاحب البيانات")؛ و"الشخص الطبيعي الذي يمكن تحديده" هو الشخص الذي يمكن تحديده بشكل مباشر أو غير مباشر، بوجه خاص بالرجوع إلى "وسيلة لتحديد الهوية مثل الاسم أو رقم الضمان الاجتماعي أو بيانات الموقع أو المعرّف عبر الإنترنت أو إلى واحد أو أكثر من العناصر المحددة للهوية البدنية أو الفسيولوجية أو الجينية أو النفسية أو الاقتصادية أو الثقافية أو الاجتماعية".

(ISSN: 2537- 0758)

الشخصية في ظل التطورات التكنولوجية المتسارعة. ويهدف القانون إلى تنظيم معالجة البيانات الشخصية بطرق تحترم الحقوق الفردية، مع وضع ضوابط صارمة لضمان أمان البيانات ومنع إساءة استخدامها. و يتضمن القانون مبادئ رئيسية مثل الشفافية والمساءلة، ويوفر حقوقاً متعددة للأفراد، منها الحق في الوصول إلى البيانات، وتصحيحها، وحذفها. كما يفرض التزامات على الجهات التي تقوم بمعالجة البيانات، بما في ذلك الحصول على الموافقة المسبقة من أصحاب البيانات واستخدامها فقط للأغراض المحددة. و يُعد القانون خطوة هامة نحو مواءمة تشريعات الإمارات مع أفضل الممارسات الدولية، مثل اللائحة العامة لحماية البيانات (GDPR) في الاتحاد الأوروبي، مما يعزز الثقة في البيئة الرقمية المحلية والدولية.

- **مشكلة البحث**:

يثير موضوع الموافقة أو الرضاء الرقمي بمعالجة البيانات الشخصية عدة مشكلات قانونية، **أهمها:**

**المشكلة الاولى** هى تحديد المقصود بالموافقة أو الرضاء الرقمي بمعالجة البيانات، وبيان طبيعته القانونية، حيث من الضروري الوقوف على مفهوم الموافقة، أو الرضاء الرقمي وتوضيح طبيعته القانونية، خاصة في ظل الاختلافات الفقهية المتعلقة بتصنيفه. هل يُعد الرضاء تصرفًا قانونيًا مستقلًا أم مجرد شرط من شروط صحة عمليات جمع ومعالجة البيانات؟ كذلك، يتعين مناقشة مدى ارتباطه بالمبادئ العامة للقانون المدني، باعتباره انعكاسًا لإرادة حرة واعية.

اما **المشكلة الثانية** هى تحديد شروط التعبير عن الموافقة أو عن الرضاء الرقمي وشكله، حيث ينبغي تحليل الشروط الواجب توافرها في التعبير عن الموافقة الرقمية، مثل الوضوح، الاختيار الحر، والمعرفة الكاملة. كما يجب تحديد ودراسة الأشكال الممكنة للتعبير عنه، سواء كان صريحًا أو ضمنيًا، ومدى توافق هذه الأشكال مع المتطلبات التشريعية الوطنية والدولية.

**والمشكلة الثالثة** هى بيان الأهلية المطلوبة للتعبير عن الموافقة أو عن الرضاء الرقمي، وذلك من خلال تحديد الأهلية، حيث دراسة الحد الأدنى من الأهلية القانونية المطلوب للتعبير عن الموافقة أو الرضاء الرقمي في القانون المصري والقوانين المقارنة.

وكذلك توضيح احكام النيابة عن القاصر فى الموافقة الرقمية، حيث تحديد الطبيعة القانونية للنيابة عن القاصر في التعبير عن الموافقة الرقمية بمعالجة البيانات، مع تحليل حدود سلطة النائب وأسس تحقق صحة الموافقة التى يعبر عنها النائب بالنيابة عن القاصر، خاصة في إطار المعالجة الإلكترونية للبيانات.

**والمشكلة الرابعة** هى تحديد أحكام الموافقة على المعالجة الرقمية، اثباتها، ورصد دورها في حماية البيانات الشخصية. ففى بيان دورها في الحماية، يلزم استعراض دور الموافقة الرقمية كضمانة قانونية أساسية في حماية البيانات الشخصية.

وعن إثبات الموافقة، فيلزم دراسة الآليات المعتمدة لإثبات الموافقة، سواء كانت إلكترونية أو تقليدية، ومدى كفايتها لضمان حقوق الأفراد.

**والمشكلة الخامسة** هى تحديد الاحكام المنظمة للعدول عن الموافق، حيث نعالج مشكلة تحديد احكام الحق في العدول عن الموافقة، وذلك من خلال، بيان الشروط والإجراءات التي تتيح للأفراد سحب موافقتهم بعد منحها، وتأثير ذلك على مشروعية معالجة البيانات.

**واخيـرا** لعل من اشكاليات البحث كذلك التحديات والصعوبات التى تعترض الموافقة على المعالجة الرقمية للبيانات أو الرضاء الرقمى بالمعالجة، حيث يلاحظ انه يلزم بيان كيفية إزالة الغموض التشريعي، وهو الغموض الذي يحيط بقواعد الرضاء الرقمي، خاصة في القانون المصري، والاماراتى، وهو الامر الذى يفتقر إلى إطار قانوني عام أو نظرية متكاملة لتنظيم هذا المفهوم. وبيان ما اذا كانت اللائحة الأوروبية مصدر إلهام في ظل هذا الغموض من عدمه، حيث يبدو اللجوء إلى أحكام اللائحة الأوروبية لحماية البيانات الشخصية (GDPR) ضرورة عملية لبناء تصور

(ISSN: 2537- 0758)

واضح للموافقة على معالجة البيانات. وما يعزز ذلك هو الحراك التشريعي والقضائي الذي أعقب صدور هذه اللائحة، خاصة من خلال الأحكام الصادرة عن محكمة العدل الأوروبية التي أسهمت في توضيح المعايير اللازمة لهذه الموافقة.

ومن خلال هذا النهج، يمكن صياغة إطار قانوني متماسك للموافقة على معالجة البيانات تسهم في تعزيز حماية البيانات الشخصية، مع مراعاة التحديات المحلية والدروس المستفادة من التجارب الدولية.

## نطاق البحث:

يركز هذا البحث بشكل أساسي على دراسة الموافقة على المعالجة الرقمية المتعلقة بمعالجة البيانات الشخصية التي تُجرى رقمياً أو إلكترونيًا. ويخرج عن نطاق الدراسة معالجة البيانات الشخصية بالوسائل التقليدية، حيث ينصب الاهتمام على الجوانب الإلكترونية نظرًا لطبيعتها المميزة والمتعلقة بالتطورات التكنولوجية الحديثة.

## أهمية البحث:

باتت الموافقة الرقمية على المعالجة أحد المفاهيم الراسخة في التشريعات الحديثة المنظمة لحماية البيانات الشخصية، خاصة في ظل أحكام اللائحة العامة لحماية البيانات(GDPR)، التي قدمت تعريفًا واضحًا لمفهوم الموافقة "تحت مسمى الرضاء"، وشروطها وقواعدها[٢٨]. وقد أثرت هذه اللائحة على التشريعات الوطنية، لا

[٢٨]– المعالجة هى "أي عملية إلكترونية أو تقنية لكتابة البيانات الشخصية، أو تجميعها، أو تسجيلها، أو حفظها، أو تخزينها، أو دمجها، أو عرضها، أو إرسالها، أو استقبالها، أو تداولها، أو نشرها، أو محوها، أو تغييرها، أو تعديلها، أو استرجاعها أو تحليلها وذلك باستخدام أي وسيط من الوسائط أو الأجهزة الإلكترونية أو التقنية سواء تم ذلك جزئيًا أو كليًا". راجع: "المادة ١ من قانون حماية البيانات الشخصية المصري ١٥١ لسنة ٢٠٢٠، قارب فى ذلك المرسوم بقانون اتحادي في شأن حماية البيانات الشخصية رقم لسنة مرسوم بقانون اتحادي في شأن حماية البيانات الشخصية. راجع نص المادة الاولى من قان ونحماية البيانات الشخصية بموجب الاحكام المنظمة.

سيما القانون الفرنسي، الذي تبناها بصورة مباشرة، بينما استلهم منها القانون المصري، والاماراتى بعض أحكامه بقدر محدود.

وتنبع أهمية الموافقة الرقمية من دورها المحوري في حماية البيانات الشخصية، حيث تمثل إحدى أهم الضمانات القانونية التي تكفل لصاحب البيانات السيطرة الكاملة على بياناته[٢٩]. حيث تمنح الموافقة صاحب البيانات القدرة على فهم عمليات المعالجة، واتخاذ قراراته بحرية مطلقة بشأن قبولها أو رفضها[٣٠]. كما تتيح له الحق في الاعتراض على معالجة بياناته أو سحب الموافقة في وقت لاحق.

وتظهر الموافقة بشكل واضح في سياقات تسجيل المستخدمين على المواقع الإلكترونية أو الاشتراك في التطبيقات والخدمات الرقمية. ولضمان شرعية جمع البيانات أو معالجتها، يجب أن تستوفي الموافقة العناصر والشروط التي تنص عليها القوانين. وأي عملية لجمع أو معالجة البيانات تتم دون موافقة صريحة من صاحبها، أو خارج الحالات المصرح بها قانونًا، تُعد غير قانونية وتشكل انتهاكًا لحقوقه، مما يخول له الحق في المطالبة بالتعويض عند توافر شروطه.

---

[٢٩]– المتحكم هو "أي شخص طبيعي أو اعتباري يكون له بحكم أو طبيعة عمله، الحق في الحصول على البيانات الشخصية وتحديد طريقة وأسلوب ومعايير الاحتفاظ بها، أو معالجتها والتحكم فيها طبقًا للغرض المحدد أو نشاطه". أما المعالج فهو "أي شخص طبيعي أو اعتباري مختص بطبيعة عمله، بمعالجة البيانات الشخصية لصالحه أو لصالح المتحكم بالاتفاق معه ووفقًا لتعليماته". راجع: المادة ١ من قانون البيانات الشخصية المصري ١٥١ لسنة ٢٠٢٠. و فى القانون الاماراتى المتحكم هو: المنشأة أو الشخص الطبيعي الذي لديه بيانات شخصية، وبحكم نشاطه يقوم بتحديد طريقة وأسلوب ومعايير معالجة هذه البيانات الشخصية والغاية من معالجتها، سواء بمفرده أو بالاشتراك مع أشخاص أو منشآت أخرى. انظر نص المادة الاولى من قانون حماية البيانات الاماراتى. من المرسوم الاتجادى بقانون رقم ٤٥ لسنة ٢٠٢١ بشأن قانون حماية البيانات الشخصية.

[٣٠]– يعد مبدأ احترام إرادة صاحب البيانات في قبول المعالجة أو رفضها الركيزة الأساسية التي تقوم عليها العلاقة التي تربط المتحكم بصاحب البيانات، فهو وسيلة هامة لدعم الثقة وتحقيق التوازن وتجسيد الشفافية في إطار هذه العلاقة.

(ISSN: 2537- 0758)

**منهج وتقسيم البحث**:

يعتمد البحث على المنهج التحليلي، حيث يتم استعراض المعلومات المتعلقة بالموضوع وتحليلها بهدف تكوين صورة متكاملة عن مفهوم الموافقة الرقمية وضوابطها ومجالاتها. بالإضافة إلى ذلك، يتبنى البحث المنهج المقارن، من خلال مقارنة التشريعات والنظم القانونية في مصر والامارات وفرنسا والاتحاد الأوروبي، مع تركيز خاص على اللائحة العامة لحماية البيانات (GDPR).

**في ضوء ما تقدم**، سيتم دراسة الموافقة على المعالجة الرقمية للبيانات الشخصية **من خلال التقسيم الاتى:**

**المبحث الأول:** ماهية الموافقة.

**المبحث الثانى:** مقومات قيام الموافقة.

**المبحث الثالث:** اثار الموافقة.

## المبحث الأول

## ماهية الموافقة

**تمهيد وتقسيم**:

ان موافقة صاحب البيانات الشخصية على معالجة بياناته تعد مسألة قانونية هامة، حيث أصبحت مفهومًا يحظى باهتمام متزايد في التشريعات المعاصرة، لما لها من دور محوري في حماية البيانات الشخصية. وقد حظيت هذا الموافقة بتنظيم خاص من قبل المشرّعين الأوروبي والمصري، والاماراتى حيث تركزت الجهود على تعريفها وتحديد كيفية التعبير عنها، مع مراعاة خصوصيتها وتمييزها عن أنواع الموافقات الأخرى، لا سيما الموافقات التقليدية في العقود وفق النظرية العامة للعقد.

ورغم هذا الاهتمام، لا تزال النصوص القانونية تفتقر إلى تحديد دقيق للطبيعة القانونية لهذا النوع من الموافقة، مما يثير العديد من التساؤلات الفقهية حول أسسها وموقعها في الإطار التقليدى للنظام القانونى.

ومن الملاحظ ان بيان ماهية الموافقة على معالجة البيانات تتطلب بداية ان نوضح المقصود بالبيانات الشخصية التى تكون محلاً للمعالجة الرقمية، ومن ثم نوضح مفهوم واساس الموافقة على المعالجة الرقمية للبيانات.

**وفي ضوء ذلك، يصبح من المفيد تناول بيان ماهية الموافقة في سياق معالجة البيانات الشخصية من خلال التقسيم الاتى:**

**المطلب الاول:** التعريف بالبيانات الشخصية موضوع المعالجة.

**المطلب الثانى:** التعريف بالموافقة على معالجة البيانات.

## المطلب الاول

## التعريف بالبيانات الشخصية موضوع المعالجة

### أولاً- المقصود بالبيانات الشخصية:

يُعَدُّ الفقيه الأمريكي آلان ويستون من الروّاد الأوائل في مجال حماية البيانات الشخصية، حيث تناول هذا الموضوع في مؤلفه الصادر عام ١٩٦٧ بعنوان الخصوصية والحرية. وقد قدّم ويستون تعريفاً دقيقاً لخصوصية البيانات بوصفها "حق الفرد في تقرير الكيفية والزمان والنطاق الذي يمكن للآخرين الوصول فيه إلى بياناته الشخصية"(٣١).

وقدّم الفقيه ميلر تعريفاً لخصوصية البيانات في مؤلفه الصادر عام ١٩٧١ بعنوان الاعتداء على الخصوصية. وعرّفها بأنها "قدرة الفرد على التحكم في دورة المعلومات الخاصة به"، مما يعني أنها تشمل حق الفرد في منع الآخرين من الاطلاع على أو التصرف في المعلومات المتعلقة بحياته الخاصة(٣٢).

---

(31)- Nayeri, N. and Aghajani, M. (2010). Patients' privacy and satisfaction in the emergency department: a descriptive analytical study. Nursing Ethics, 17(2), 167-177. https: //doi. org/10. 1177/0969733009355377 . Kwasny, M., Caine, K., Rogers, W., & Fisk, A. (2008). Privacy and technology. . https: //doi. org/10. 1145/1358628. 1358846 .

(32)- Nayeri, N. and Aghajani, M ،Ibid. op. cit.. Kwasny, M., Caine, K., Rogers, W., & Fisk Ibid. op. cit .،

(ISSN: 2537- 0758)

فيما عرف المشرع المصرى البيانات الشخصية في المادة (١) من الفصل الأول من القانون الخاص بحماية البيانات الشخصية رقم ١٥١ لسنة ٢٠٢٠، بأنها: أى بيانات متعلقة بشخص طبيعي محدد أو يمكن تحديده بشكل مباشر أو غير مباشر، عن طريق الربط بين هذه البيانات وأى بيانات أخرى، كالإسم أو الصوت أو الصورة، أو رقم تعريفي أو محدد للهوية عبر الإنترنت أو أى بيانات تحدد الهوية النفسية أو الصحية أو الاقتصادية أو الثقافية أو الاجتماعية".

وعرفها المشرع الاماراتى فى المادة الاولى من المرسوم بقانون اتحادى رقم٤٥ لسنة ٢٠٢١ بخصوص حماية البيانات، بانها "... أي بيانات تتعلق بشخص طبيعي محدد، أو تتعلق بشخص طبيعي يمكن التعرف عليه بشكل مباشر أو غير مباشر من خلال الربط بين البيانات، من خلال استخدام عناصر التعريف كإسمه، أو صوته، أو صورته، أو رقمه التعريفي، أو المعرف الإلكتروني الخاص به، أو موقعه الجغرافي، أو صفة أو أكثر من صفاته الشكلية أو الفسيولوجية، أو الاقتصادية، أو الثقافية. أو الاجتماعية، وتشمل البيانات الشخصية الحساسة والبيانات الحيوية البيومترية".

بينما عرفتها المادة (٤/١) من اللائحة الأوروبية بشأن حماية البيانات ذات الطابع الشخصي، بأنها: أي معلومات تتعلق بشخص طبيعي محدد أو يمكن تحديده بشكل مباشر أو غير مباشر، على وجه الخصوص عن طريق الرجوع إلى عنصر أو أكثر من العناصر المميزة له، مثل: الإسم أو الرقم التعريفي أو بيانات الموقع أو معرف الإتصال عبر الإنترنت أو الخصائص الفسيولوجية أو أو الوراثية أو النفسية أو الإقتصادية أو الثقافية أو الإجتماعية"[٣٣].

[٣٣]– قارب جمال، أ.، "الحق المشترك في البيانات في ظل تقنية الذكاء الاصطناعي: دراسة نقدية لتنظيم البيانات الشخصية"، مجلة القانون والتقنيات الناشئة، العدد الرابع، الجزء الثاني، ٢٠٢٤، متاح على الرابط: https: //doi. org/10. 54873/jolets. v4i2. 206.

وبناءً على التعريفات السابقة، يمكن استنتاج أن البيانات الشخصية، أو ما يُعرف بالبيانات ذات الطابع الشخصي، تشمل أي معلومات ترتبط بشخص طبيعي محدد أو يمكن تحديده، سواء كان ذلك بصورة مباشرة أو غير مباشرة. ويحدث ذلك من خلال الربط بين هذه المعلومات وأنماط بيانات شخصية محددة مسبقًا، بما يُمكّن من التعرف على الهوية أو استنتاجها.

وقد أظهر المشرع المصرى و المشرع الاماراتى رؤية موفقة عند تحديد أنواع البيانات الشخصية التي تخضع للحماية القانونية، من خلال تقديم أمثلة واضحة لهذه البيانات. هذا النهج ساهم في تعزيز دقة مفهوم البيانات الشخصية، ومنح التعريف طابعًا مرنًا يستوعب مختلف أشكال البيانات الشخصية التي قد تنشأ.

ويتضح من النصوص التشريعية أن كلًّا من المشرع المصري والمشرع الإماراتي قد قصر نطاق حماية البيانات الشخصية على الأشخاص الطبيعيين دون أن تشمل الأشخاص الاعتباريين. ومع ذلك، يُستثنى من هذا القيد البيانات المرتبطة بالأفراد الذين يمثلون الأشخاص الاعتباريين. ويُفهم من ذلك أن الحماية القانونية تقتصر على البيانات التي ترتبط بالأشخاص الطبيعيين بشكل مباشر، دون امتدادها إلى الكيانات الاعتبارية إلا في حدود ما يتعلق بممثليها الطبيعيين.

وإضافة إلى ذلك، يُلاحظ أن قانون حماية البيانات الشخصية في كل من النظامين المصري والإماراتي قد ركّز بشكل رئيسي على حماية ومعالجة البيانات الشخصية الرقمية، متجاهلًا البيانات الشخصية التقليدية. فلم يُبدِ المشرع اهتمامًا كافيًا بمعالجة البيانات الشخصية غير الرقمية، ولم يخضعها للحماية القانونية سواء ضمن القوانين العامة أو القوانين المتخصصة بحماية البيانات الشخصية. ويظهر هذا التوجه بوضوح في تعريف المشرع لعملية معالجة البيانات الشخصية، حيث أشار صراحةً إلى مصطلحات مثل "الإلكترونية" و"التقنية"، مما يعكس اقتصار الحماية على البيانات الرقمية دون التقليدية.

(ISSN: 2537- 0758)

**ثانياً- أنواع البيانات الشخصية: هناك نوعين من البيانات الشخصية نوضحهما فيما يلى:**

**النوع الأول**– البيانات الشخصية العادية، وهي البيانات التي تتعلق بالفرد، ولكنه لا يعتبر إطلاع الآخرين عليها انتهاكًا لخصوصيته، ولا تشكل معرفتها تعديًا على حقوقه الشخصية. تشمل هذه البيانات، على سبيل المثال، الاسم، رقم الهاتف، وتاريخ الميلاد[٣٤].

**النوع الثاني**– البيانات الشخصية الحساسة التي عرفها المشرع المصرى فى المادة (١) من الفصل الأول من قانون حماية البيانات الشخصية بأنها: تلك البيانات التي تفصح عن الصحة النفسية أو العقلية أو البدنية أو الجينية أو البيانات البيومترية أو البيانات المالية أو الآراء السياسية أو الحالة الأمنية أو المعتقدات الدينية للشخص، وحظر التعامل عليها إلا بترخيص من مركز حماية البيانات الشخصية، وبموافقة الشخص المعنى بالبيانات صراحة وبشكل كتابي. وعرفها المشرع الاماراتى فى نص المادة الاولى من قانون حماية البيانات، بان البيانات الشخصية الحساسة: أي بيانات تكشف بشكل مباشر أو غير مباشر عن عائلة الشخص الطبيعي أو أصله العرقي أو آرائه السياسية أو الفلسفية أو معتقداته الدينية، أو سجل السوابق الجنائية الخاص به، أو بيانات القياسات الحيوية البيومترية الخاصة به، أو أي بيانات تتعلق بصحة هذا الشخص وتشمل حالته الجسدية أو النفسية أو الذهنية أو العقلية أو البدنية أو الجينية أو الجنسية، بما في ذلك المعلومات المتعلقة بتوفير خدمات الرعاية الصحية له التي تكشف عن وضعه الصحي.

---

[٣٤]– سامح عبد الواحد التهامي، ضوابط معالجة البيانات الشخصية، دراسة مقارنة بين القانون الفرنسي والقانون الكويتي، مجلة القانون الكويتية العالمية، ع، ٩، س ٣ مارس ٢٠١٥، ص ٤٠١. محمد حماد مرهج الهيتي، البحث عن حماية جنائية للبيانات والمعلومات الشخصية (الأسمية المخزنة في الحاسب الآلي، مجلة كلية الشريعة والقانون الإمارات، ع ٢٧، يوليو ٢٠١٦، ص ٤٠١.

فى ضوء ما تقدم يرى البعض أن البيانات الحساسة تعتبر نوع من البيانات الشخصية ذات نطاق ضيق، ومرد حظر جمع تلك البيانات أو تداولها أو معالجتها هو ارتباطها المباشر والوثيق بحق الفرد في حرمة الحياة الخاصة به، ذلك الحق الذي أقرته الدساتير الوطنية والمعاهدات[٣٥].

وتُعد البيانات الشخصية من الركائز الأساسية للاقتصاد في العصر الحديث، حيث تُشكّل أساسًا لفهم سلوك الأفراد، ومعرفة رغباتهم، والتأثير على قراراتهم. تلجأ شركات تحليل البيانات إلى إنشاء ملفات سيكوجرافية(Psychographic Profiles) لدراسة توجهات الأفراد المستهدفين، وتحليل احتياجاتهم وتطلعاتهم، ومن ثم توجيه رسائل مخصصة تهدف إلى التأثير على قناعاتهم وسلوكياتهم.

علاوةً على ذلك، تُعتبر البيانات الشخصية الأساس الذي يعتمد عليه قطاع الدعاية والإعلان، حيث تستغل الشركات هذه البيانات للترويج لمنتجاتها وخدماتها بشكل أكثر فاعلية. ومن أبرز الأمثلة على ذلك، شركات الطيران والسياحة وشركات التأمين، التي تستخدم البيانات الشخصية لتقديم عروض مخصصة تستهدف احتياجات العملاء المحتملين بدقة.

هذا ونجد أن جميع مواقع التواصل الإجتماعي (Facebook-twitter-LinkedIn) تتطلب إدخال المستخدم لبعض بياناته الشخصية لإتمام عملية التسجيل، وعليه تحتفظ تلك المواقع بالبيانات الشخصية التي يلتزم المستخدم بإدخالها عند رغبته في الإنضمام لأى منها، كما تحتفظ بالبيانات الخاصة بالإتصال بالإنترنت أي ما يعرف بالعنوان الإلكتروني (IP)، كما تصل إلى بيانات التصفح الخاصة بالمستخدم، وكذلك كافة التطبيقات التي يستخدمها وتكشف عن هوياته وميوله واهتماماته، وهو ما يمثل خطورة كبرى على خصوصية البيانات الخاصة بذلك

---

[٣٥]– محمد حماد مرهج الهيتي، البحث عن حماية جنائية للبيانات والمعلومات الشخصية، مرجع سابق، ص ٤٠١. المادة (٩٢) من الدستور المصرى ٢٠١٤؛ المادة (١٢) من الإعلان العالمي لحقوق الإنسان، والمادة (١٧) من العهد الدولي الخاص بالحقوق المدنية والسياسية.

(ISSN: 2537- 0758)

المستخدم. حيث يرى البعض ان الإدلاء بالبيانات الشخصية يعد إجراء أولى ووجوبي، يتعين على كل من يرغب في الإنضمام إلى مواقع التواصل الإجتماعي أن يدلى بها كتدوين اسمه ولقبه وجنسه وتاريخ ميلاده وبريده الإلكتروني وغير ذلك من البيانات التي قد تتفاوت من موقع لآخر[٣٦].

وتجدر الإشارة في هذا السياق إلى أن البيانات الشخصية للأفراد تُعد جزءًا أساسيًا ومتكاملًا من البيانات التي تُستخدم لتغذية تطبيقات الذكاء الاصطناعي بمختلف أنواعها ومجالاتها. فالبيانات الشخصية المُعتمدة في عمليات المعالجة تُعتبر بمثابة الوقود الذي تعتمد عليه تلك التقنيات والتطبيقات لتحقيق أهدافها.

على سبيل المثال، اللجوء إلى جمع البيانات الشخصية ومعالجتها لأغراض مثل التنبؤ بوقوع جريمة ما، قد يُثير تساؤلات قانونية وأخلاقية. ذلك لأن مثل هذه الاستخدامات قد تنطوي على انتهاك للحماية القانونية المقررة بموجب قانون حماية البيانات الشخصية رقم ١٥١ لسنة ٢٠٢٠، الذي يهدف إلى صون حقوق الأفراد وضمان عدم استغلال بياناتهم بطرق تخالف إرادتهم أو تضر بخصوصيتهم[٣٧].

وبذلك، يتضح أن البيانات الشخصية ليست فقط هدفًا للحماية القانونية، بل هي أيضًا محلًا رئيسيًا لتطبيقات الذكاء الاصطناعي، مما يُبرز أهمية تحقيق التوازن بين

---

[٣٦]– علاء عيد طه الحماية القانونية للأشخاص الطبيعين فيما يتعلق بمعالجة البيانات الشخصية وتداولها، دراسة في ضوء اللائحة التنظيمية رقم ٦٧٩/ ٢٠١٦ الصادرة عن البرلمان والمجلس الأوروبي، مجلة كلية الحقوق للبحوث القانونية والإقتصادية، ع ٢، ٢٠١٩، ص ٢٤. محمد سامى عبد الصادق، شبكات التواصل الإجتماعي. . مرجع سابق، ص ٣٧ وما يليها. علاء الدين عبد الله فواز الخصاونة، الحماية القانونية للخصوصية والبيانات الشخصية في نطاق المعلوماتية مجلة جامعة الشارقة للعلوم الشرعية والقانونية، جامعة الشارقة، مج ٨، ع ٢، ٢٠١١، ص ٥ وما يليها. محمود سلامة عبد المنعم الشريف الطبيعة القانونية للتنبؤ بالجريمة بواسطة الذكاء الإصطناعي ومشروعيته المجلة العربية لعلوم الأدلة الجنائية والطب الشرعى، مج ٣، ٢٠٢١، ص ٣٥١.

[٣٧]–محمود سلامة عبد المنعم الشريف الطبيعة القانونية للتنبؤ بالجريمة مرجع سابق، ص ٣٥١.

استثمار البيانات في تطوير هذه التطبيقات وضمان الالتزام بالضوابط القانونية والأخلاقية التي تكفل حقوق الأفراد في حماية خصوصيتهم[٣٨].

وعليه، فقد أصبحت العديد من مواقع الشبكات الاجتماعية تستفيد بشكل كبير من تطبيقات الذكاء الاصطناعي، حيث تُستخدم هذه التقنيات لتحديد الخصائص الديموغرافية الجديدة للمستخدمين. وتعتمد هذه المواقع على خوارزميات الذكاء الاصطناعي التي تُتيح جمع وتحليل كميات هائلة من البيانات المتعلقة بنشاط المستخدمين داخل شبكة اجتماعية معينة.

وتهدف هذه الخوارزميات إلى تقييم أو تحديد أنماط النشاط المختلفة للمستخدمين، مما يساعد على تحسين تجربة المستخدم، تطوير استراتيجيات التسويق، أو حتى استهداف إعلانات مخصصة. ومع ذلك، فإن هذا الاستخدام يثير تساؤلات حول حماية خصوصية الأفراد وضرورة ضمان التزام تلك المنصات بالقوانين التي تنظم جمع البيانات الشخصية ومعالجتها[٣٩].

ومن خلال جمع تلك البيانات، تتم عملية التجهيز كمرحلة لازمة لإجراء عملية المعالجة، وتعرف تلك العملية وفقا للمادة (٤) من اللائحة الأوروبية بأنها عملية أو مجموعة من العمليات التي يقوم بها القائم بعملية المعالجة على مجموعة من البيانات الشخصية، بالقيام بالجمع والتنظيم والتسجيل والهيكلة والتخزين والتعديل والتكييف والإسترجاع، والكشف عن طريق النشر أو البث أو أى شكل آخر للإتاحة أو المحو أو التدمير"- هذا ولم يعرف المشرع المصرى في مواده عملية التجهيز رغم أهميتها في معالجة البيانات؛ ومن ثم يقوم المعالج- بعملية المعالجة.

فالقائم بعملية المعالجة هو الذي يحدد طريقة المعالجة، وتعرف عملية المعالجة وفقا للمادة (١) من الفصل الأول من قانون حماية البيانات الشخصية بأنها: " أى

---

[٣٨]- عمار ياسر محمد زهير البابلي توظيف تقنيات الذكاء الإصطناعي في العمل الأمنى دراسة تطبيقية، مجلة الأمن والقانون مج ٢٨ ع ١، ٢٠٢٠، ص ٥٥.

[٣٩]- عمار ياسر محمد زهير البابلي توظيف تقنيات الذكاء الإصطناعي..، مرجع سابق، ص٥٥.

(ISSN: 2537- 0758)

عملية إلكترونية أو تقنية، لكتابة البيانات الشخصية أو تجميعها أو تسجيلها أو حفظها أو تخزينها، وذلك باستخدام أى وسيط من الوسائط أو الأجهزة الإلكترونية أو التقنية، سواء تم ذلك جزئيا أو كليا. بينما عرفتها اللائحة الأوروبية في (٤/٢) منها بأنها: عملية أو مجموعة من العمليات التي تجرى على البيانات الشخصية أو مجموعة منها، بأي وسيلة كانت تقليدية أو إلكترونية، مثل الجمع أو أو التسجيل أو التنظيم. وعرف المشرع الاماراتى المعالجة فى المادة الاولى من قانون حماية البيانات بانها "أي عملية أو مجموعة عمليات يتم إجراؤها على البيانات الشخصية باستخدام أي وسيلة من الوسائل الإلكترونية بما فيها وسيلة المعالجة وغيرها من الوسائل الأخرى، وتشمل هذه العملية جمع البيانات الشخصية، أو تخزينها، أو تسجيلها أو تنظيمها أو تكييفها أو تعديلها، أو تداولها، أو تحويرها، أو استرجاعها، أو تبادلها، أو مشاركتها، أو استعمالها، أو توصيفها، أو الإفصاح عنها عن طريق بثها أو نقلها أو توزيعها أو إتاحتها أو تنسيقها أو دمجها أو تقييدها أو حجبها أو محوها أو إتلافها أو إنشاء نماذج لها".

ويلاحظ على ما تقدم أن المشرع المصرى قد قصر عملية معالجة البيانات الشخصية على المعالجة الإلكترونية فقط، بينما المشرع الأوروبي أورد نوعين من عمليات المعالجة، المعالجة التقليدية إلى جانب المعالجة الإلكترونية، وإن كانت البيانات الشخصية التقليدية لا تختلف عن البيانات الشخصية الإلكترونية إلا في أن الأخيرة لا تستخدم إلا عند التعامل مع الوسائط الإلكترونية، فكلتاهما تعبر عن البيانات الشخصية للإنسان كالاسم واللقب والسن ورقم الهاتف وغيرها، إلا أنه من الأحرى بالمشرع المصرى مسايرة المشرع الأوروبي في إدراجه للمعالجة التقليدية للبيانات إلى جانب معالجة البيانات الإلكترونية، إمعانا في حماية أكبر للبيانات الشخصية للأفراد.

ونذكر في هذا الصدد أن هناك عدة بيانات شخصية تخرج عن نطاق الحماية القانونية المنصوص عليها في قانون حماية البيانات الشخصية، فقد نص القانون المصرى على عدم سريان أحكامه على البيانات الآتية[٤٠]:

- البيانات التي يحتفظ بها الشخص الطبيعي للغير، ويقوم بمعالجتها للاستخدام الشخصي.
- البيانات التي يتم معالجتها تطبيقا لنص قانوني أو بغرض الحصول على البيانات الإحصائية الرسمية.
- البيانات المتعلقة بمحاضر الضبط القضائي، والتحقيقات والدعاوى القضائية.
- البيانات التي تتم معالجتها حصرا لأغراض إعلامية، يحيث تكون دقيقة وصحيحة، ولا يتم استخدامها لأى أغراض أخرى، ودون الإخلال بالتشريعات المنظمة للصحافة والإعلام.
- البيانات الشخصية لدى جهات الأمن القومى، وما تقدره لإعتبارات أخرى.

## ثالثاً- المخاطر التي تهدد خصوصية البيانات الشخصية للأشخاص:

فيما يتعلق بالمخاطر التي تهدد خصوصية البيانات الشخصية للأفراد، يُلاحظ تفاوت هذه المخاطر بحسب المراحل المختلفة التي تمر بها البيانات الشخصية، والتي تشمل التجميع، المعالجة، الإتاحة عبر الإنترنت، وأي إجراءات أخرى تنطوي على مساس بخصوصية البيانات الشخصية، مما قد يهدد حقوق وحريات الأفراد. **وفيما يلي أبرز هذه المخاطر:**

**١- المخاطر المتعلقة بتجميع البيانات الشخصية:**

تعرف عملية التجميع بأنها أى عمل من أعمال جمع وترتيب عناصر البيانات الشخصية لشخص ما، وإدراجها في بطاقة معلومات ورقية كانت أو إلكترونية، فعملية جمع البيانات أمر حتمى لاجراء عمليات المعالجة التي لا تخلو من مخاطر الإعتداء على خصوصية تلك البيانات المجمعة، فكثيرا ما تقوم الجهات الحكومية أو

(٤٠)-رجع نص المادة رقم ٣ من القانون المصرى و يقابلها نص المادة رقم ٢ من القانون الاماراتى.

(ISSN: 2537- 0758)

الهيئات الخاصة بتجميع بيانات مفصلة خاصة بالمتعاملين معها، وهو ما قد يؤدى لإساءة استخدام تلك البيانات المحفوظة، خاصة وأن تلك الجهات تقوم بربط الأجهزة المشتركة عبر شبكات عامة لتسهيل عملية تبادل البيانات الشخصية فيما بينها[٤١].

كما قد يتم تجميع البيانات الشخصية للأفراد بدون علمهم بفضل التقنيات التكنولوجية الحديثة المستخدمة عبر شبكة الإنترنت كرسائل الكوكيز[٤٢]، التي تستخدمها الشركات التجارية في أغراض الدعاية لخدماتها ومنتجاتها، ورغم فوائدها العديدة إلا أنها تعد من أنجح الوسائل المستخدمة لملاحقة خصوصية الأفراد وكشف بياناتهم الشخصية، وهو ما قد يساء استخدامه في أغراض غير مشروعة، أما الوسيلة الأخطر من ذلك فهي أنظمة جمع المعلومات أو ما يعرف ببرمجيات التتبع والإلتقاط، فهى وسيلة تتبع تمكن مستخدمها من تجميع أكبر قدر ممكن من المعلومات السرية ومعالجتها بسرعة فائقة.

ومن جهة أخرى تقوم أغلب وسائل التواصل الإجتماعي بتجميع بيانات المستخدمين، وتقوم باستخدامها في عمليات التسويق المباشر، فضلا عن تعرضها لعمليات القرصنة، وانتحال الأفراد بها لشخصيات أخرى مغايرة، وقيامهم بنشاطات غير مشروعة، وهو ما عبر عنه (جورج) راى المسئول عن الأمن المعلوماتي بشركة الأستثمارات الأمريكية (كوفمان- روسن (كو)[٤٣] خلال منتدى الأمن المعلوماتي

---

[٤١]- محمود عبدالرحمن، التطورات الحديثة لمفهوم الحق فى الخصوصية..، مرجع سابق، ص١٠.

[٤٢]- الكوكيز عبارة عن ملفات نصية تضعها معظم مواقع الويب عند زيارة موقعها، بغرض جمع معلومات عن المستخدمين، بحيث تمكن الموقع من الرجوع إليها عند الحاجه. للمزيد انظر: محمد أحمد المعداوى، حماية الخصوصية المعلوماتية للمستخدم عبر شبكات مواقع الواصل الإجتماعى، د ا رسة مقارنة، مجلة كلية. الشريعة والقانون، جامعة طنطا، مج ٣٣، ع ٤، ديسمبر ٢٠١٨، ص ١٩٥٠ ومايليها.

-Joan E. Rigdon, Internet Users Say They'd Rather Not Share Their Cookies, Wall Street Journal, 14. Feb,1996, p. 25.

[٤٣]- محمود عبدالرحمن، مرجع سابق، ١٠٩- ١١٠.

الذي نظمته غرفة التجارة في بنما بقوله: يتعرض يوميا نحو مليون ونصف مليون شخص لعمليات القرصنة المعلوماتية، التي يستهدف منها هؤلاء الحصول على معلومات شخصية أو الإضرار ببعض المؤسسات، حيث تم تسجيل نحو ٥٥٦ مليون هجوم معلوماتى خلال سنة واحدة على مواقع التواصل الإجتماعي والبريد الإلكتروني، واستطرد قائلا أنه من السهل الحصول على معلومات شخصية من مواقع التواصل الإجتماعي، فضلا عن قيام الأفراد بانتحال الشخصيات والقيام بالأنشطة غير المشروعة"(٤٤).

**٢- المخاطر المتعلقة باستخدام ومعالجة البيانات الشخصية:**

**تنطوى هذه المرحلة على مخاطر عديدة، منها:**

المخاطر المتعلقة باستخدام البيانات خلال عملية المعالجة ونتائجها: فهذه المرحلة اعتبرتها اللجنة الوطنية للمعلوماتية والحريات بفرنسا من البيانات الشخصية الحساسة، خصوصا ما يتعلق منها بالهوس والفصام الذهني، وبالتالي فإن معالجة البيانات الشخصية لأغراض البحث العلمي خصوصا تلك المتعلقة بالأبحاث الجينية أو للأغراض الإحصائية كإجراء البحوث على مجموعة من المراهقين ذوى الأصول الإجرامية، قد تعرض الأفراد لإنتهاك خصوصيتهم والكشف عن حالتهم الصحية أو التنبؤ بسلوكهم الإجرامي، الأمر الذي من شأنه انتهاك حرمة الحياة الخاصة بهم(٤٥).

المخاطر المتعلقة بالهدف من عملية المعالجة: قد يتم استخدام تلك البيانات المستخدمة في عملية المعالجة لتحقيق أهداف غير مشروعة، أضف إلى ذلك

---

- Payne, D. and Kennett-Hensel, P. (2017). Combatting identity theft: a proposed ethical policy statement and best practices. Business and Society Review, 122(3), 393-420. https: //doi. org/10. 1111/basr. 12121 .

(44)- Macnamara, J., Zerfaß, A., Adi, A., & Lwin, M. (2018). Capabilities of pr professionals for key activities lag: asia-pacific study shows theory and practice gaps. Public Relations Review, 44(5), 704-716. https: //doi. org/10. 1016/j. pubrev. 2018. 10. 010.

(٤٥)– الزرعوني، أ. (٢٠٢٤). خصوصية المعلومات الجينية والتحديات التي تواجه حمايتها. مجلة جامعة الشارقة للعلوم القانونية، ٢١(٢). https: //doi. org/10. 36394/jls. v21. i2. 13

(ISSN: 2537- 0758)

غموض الأهداف أو اتساعها أو تحديد أكثر من هدف من قبل المسئول، الأمر الذى يعطى مجالا كبيرا للإنتهاكات المتعددة لخصوصية تلك البيانات(٤٦).

وقد عبرت المحكمة الدستورية في كارلسروه (ألمانيا) الإتحادية) عن ذلك بقولها: أن التقنيات الحديثة لجمع البيانات الشخصية واستخدامها والإحتفاظ بها من المرجح أنها سوف تقوض الحق في الحياة الخاصة بالأفراد، من خلال التخزين غير المحدود للبيانات، واستخدامها فى أى وقت، وفى غير الأغراض التي جمعت من أجلها؛ وبدون أى سيطرة عليها، فعملية جمع البيانات الشخصية الرقمية لأغراض المعالجة يجب أن تتم في حدود الأهداف المحددة(٤٧).

**٣- المخاطر الناجمة عن حوسبة البيانات الشخصية:**

حوسبة البيانات الشخصية: تعرف بتقنية تكنولوجيا التعلم، فغالبا ما تتميز تطبيقاتها بخاصية تكييف عملياتها مع البيانات التي تم الحصول عليها، ففى حالة المتجر متعدد الأقسام سيأخذ النظام في الإعتبار المشتريات السابقة من أجل الدعايا لمنتجاتهم، وتعريفنا بالمنتجات الأخرى الأنسب لنا. فشيوع عملية النقل الرقمى للبيانات خلق مشكلات أمنية، إذ سهل عمليات التجسس الإلكتروني والقرصنة، وأصبحت شبكات الاتصال غير قادرة على توفير الأمان المطلق أو السرية الكاملة لما ينقل عبرها من بيانات(٤٨).

---

(46)- Wieczorkowski, J. and Polak, P. (2017). Big data and privacy: the study of privacy invasion acceptance in the world of big data. Online Journal of Applied Knowledge Management, 5(1), 57-71. https: //doi. org/10. 36965/ojakm. 2017. 5(1)57-71

(47)- Le, Q. (2023). The social contract model in the digital era: revisiting rousseau and locke. ISSLP, 2(3), 15-26. https: //doi. org/10. 61838/kman. isslp. 2. 3. 3 .AllahRakha, N. (2024). Constitutional safeguards for digital rights and privacy. Irshad J. Law and Policy, 2(4), 31-43. https: //doi. org/10. 59022/ijlp. 172 .

(٤٨)– العميري، م. (٢٠٢٤). استراتيجيات الإعلام الإلكتروني في الكويت تجاه الأمن السيبراني.. المجلة العربية للعلوم الإنسانية، ٤٢(١٦٥)، ١١-٤٢. https: //doi. org/10. 34120/ajh. v42i165. 359

**٤- المخاطر المتعلقة بتدفق البيانات عبر الإنترنت:**

صاحب تطور التكنولوجيا الرقمية تدفق البيانات الشخصية للأفراد عبر الحدود، فأتاحت لهم فرصة إعطاء بياناتهم ومعلوماتهم الشخصية لجهات داخلية أو خارجية، وهو ما يعرض تلك البيانات للعديد من الإنتهاكات؛ خصوصا في الدول التي لا تتوافر فيها درجات عالية من مستويات الحماية، الأمر الذي دعا المشرع المصرى إلى حظر تداول البيانات الشخصية عبر الحدود؛ ولكن الأمر قد لا يكون فعالا في ظل غياب التنسيق وضمان أن تكون عملية نقل البيانات في إطار محكوم بإتفاقات دولية تكفل مستوى مماثل أو أعلى من الحماية"[٤٩].

وفي هذا الصدد قضت المحكمة العليا للإتحاد الأوروبى بتاريخ ٦ أكتوبر ٢٠١٠، ببطلان اتفاق الملاذ الأمن، ذلك الإتفاق الذي سمح للفيسبوك وبعض الشركات الأخرى مثل أمازون وجوجل بنقل بيانات المستخدمين بأعداد كبيرة وضخمة إلى أجهزتها في الولايات المتحدة الأمريكية، وتبين فيما بعد أن أكثر من آلاف شركة، كانت قد استغلت هذا الإتفاق[٥٠].

**٥- المخاطر المتعلقة باستخدام البيانات في التسويق المباشر:**

أصبح للبيانات الشخصية قيمة مادية في وقتنا المعاصر، ففيما يبدو أن البيانات المسجلة لدى العديد من الجهات مثل المصارف وشركات الهواتف المحمولة أصبحت

---

[٤٩]- الحسن..، (٢٠٢٣). الطبيعة الخاصة لبعض الجهات كمتحكمين في البيانات الشخصية أثناء تحولهم الرقمي. Journal of Law and Emerging Technologies, 3(2), 469-524. https: //doi. org/10. 54873/jolets. v3i2. 135

عرابي، س. (٢٠٢٢). المسئولية الجنائية عن انتهاك الخصوصية المعلوماتية عبر مواقع التواصل الاجتماعي. Journal of Law and Emerging Technologies, 2(2), 213-267. https: //doi. org/10. 54873/jolets. v2i2. 115

[50]- ECLI, available at: http: //curia. europa. eu/juris/document/document. jsf?docid=169195&doclang=EN ..McCusker, S. (2016). The eu us privacy shield: the antidote to the transatlantic data transfer headache?. Business Law Review, 37(Issue 3), 84-85. https: //doi. org/10. 54648/bula2016017 .

(ISSN: 2537- 0758)

تجارة رائجة تتداولها شركات التسويق في السوق المصرى، ضاربة عرض الحائط بمبادئ حماية خصوصية البيانات التي تنص عليها القوانين ويحميها حق دستورى(٥١).

هذا و قد اشترط المشرع المصرى و الاماراتى و كذلك الأوروبي لقيام عملية المعالجة ضرورة موافقة الشخص المعنى بالبيانات الشخصية بشكل صريح وواضح على قيام المعالج بجمع بياناته أو معالجتها أو الإفصاح عنها بأي وسيلة من الوسائل؛ وكذلك في الأحوال المصرح بها قانونا، و هذه الموافقة نتناول دراستها فى الفقرات القادمة.

## المطلب الثانى

## التعريف بالموافقة على المعالجة الرقمية للبيانات

### الفرع الأول

### المقصود بالموافقة

وفقًا للقواعد العامة في القانون المدني، يُعد الرضاء الركن الجوهري لإبرام العقود. وتزداد أهمية هذا الرضاء في سياق جمع ومعالجة البيانات الشخصية، نظرًا لأن العمليات التي تُجرى على البيانات قد تشكل انتهاكًا لخصوصية الأفراد، وهي حق أساسي يحرص المشرّع على صونه. لذلك، يجب أن يكون هذا الرضاء أو هذه الموافقة تعبيرًا عن إرادة حرة واعية وسليمة من أي عيب قد يؤثر على صحته.

ورغم الأهمية المحورية للرضاء، فإنه هو في جوهره مفهوم نفسي يصعب تحديده بشكل دقيق وشامل(٥٢). ولهذا السبب، لم يسعَ الفقه أو المشرّع في القواعد العامة إلى

---

(٥١)– محمود عبد العظيم، بيزنس البيانات الشخصية يغزو السوق المصرية، جريدة الإتحاد الإمارتية، بتاريخ ٨ يناير ٢٠٠٦، متاح على:
http: //www. alittihad. ae/details. php?id=44592&y=2006 .

(٥٢)– د. محمد عيد الغريب، التجارب الطبية والعلمية وحرمة الكيان الجسدي للإنسان، دراسة مقارنة، مطبعة أبناء وهبة حسان، القاهرة، الطبعة الأولى، ١٩٨٩، ص ٨٨.

وضع تعريف جامع مانع للرضاء، بل ركّز على عناصره وأحكامه بوصفه ركنًا أساسيًا للعقد.

وفي مجال حماية البيانات الشخصية، أُثيرت العديد من التساؤلات حول تطبيق مفهوم الرضاء الرقمي، لا سيما في ظل الأحكام الناظمة لمعالجة البيانات الشخصية إلكترونيًا. ويرجع ذلك إلى الغموض الفلسفي والمعنوي الذي يحيط بهذا المصطلح، ما استدعى البحث في تطبيقاته المختلفة ومحاولة تحديد مفهومه بوضوح.

وعليه، فإن تناول تعريف الموافقة الرقمية يتطلب مقاربة شاملة تبدأ من تعريف الرضاء في القواعد العامة، وتنتقل إلى دراسة تعريف الموافقة الرقمية أو الرضاء الرقمي في التشريعات الخاصة، والمختلفة، وفى شأن تعريف الرضاء في القواعد العامة، يتم عرض نظرة عابرة على ماهيته وعناصره في القانون المدني. وفى تعريف الموافقة الرقمية أو الرضاء الرقمي في اللائحة الأوروبية، يتم دراسة التفسير الوارد في اللائحة العامة لحماية البيانات(GDPR)..، وفى تعريف الرضاء الرقمي في القانون الفرنسي، يتم تحليل التعديلات التي أدخلها المشرّع الفرنسي على قانون المعلوماتية والحريات، بما يتوافق مع اللائحة الأوروبية. وفى بيان موقف المشرّعين المصري والاماراتى من مشكلة التعريف، يتم دراسة النصوص القانونية المصرية والاماراتية المتعلقة بحماية البيانات الشخصية ومدى وضوح تعريف الموافقة الرقمية أو الرضاء الرقمي فيهما. ثم نعرض الرأي الشخصي، من خلال محاولة تقديم تعريف شامل ومتكامل للموافقة الرقمية أو للرضاء الرقمي، يأخذ في الاعتبار أبعاده القانونية والعملية.

ويهدف هذا التحليل إلى بناء فهم دقيق ومتكامل لمفهوم الموافقة أو الرضاء الرقمي لمعالجة البيانات، حيث كونه أحد العناصر الرئيسية التي تستند إليها حماية البيانات الشخصية في العصر الرقمي.

(ISSN: 2537- 0758)

## أولاً: المعنى القانونى العام للموافقة، أو للرضاء:

الرضاء (Le consentement)، وفقًا للغة القانونية، يُقصد به في معناه العام: "اتجاه الإرادة إلى إحداث الأثر القانوني المطلوب"(٥٣). ويعني ذلك أن الرضاء ينبع من الإرادة، التي تُعتبر الركن الجوهري في تكوين العقد والتصرف القانوني بوجه عام(٥٤).

والإرادة، في هذا السياق، تُفهم بوصفها قرارًا فرديًا يتجسد في عزم الشخص على اتخاذ موقف محدد بوعي كامل(٥٥). ويشمل ذلك إدراك الشخص لطبيعة التصرف الذي يعتزم القيام به، وما يترتب عليه من حقوق والتزامات(٥٦). ومن ثم، لا يُعتد قانونًا بالإرادة إذا كانت صادرة عن شخص فاقد للتمييز، مثل الصبى غير المميز أو من يعاني من الجنون أو العته، أو إذا كانت الإرادة معدومة تمامًا، كما في حالة فقدان الوعي نتيجة سكر أو مرض(٥٧).

---

(٥٣)- انظر: د. عبد الفتاح عبد الباقي، مرجع سابق، ص ٨٨.

(٥٤)- يعتمد مفهوم الرضاء بشدة على إرادة الأطراف، لذا يشبه الفقيه "كاربونييه" الرضاء بأنه "إرادة كل متعاقد la volonté de chaque contractant مع "تطابق إرادتهم l'accord de leur volonté". انظر:

Jean CARBONNIER, Droit civil, Les obligation, Tom 4, Théme droit privé, 2e edition, PUF, Paris, 2000, p. 81 et 83 .

(٥٥)- د. منصور مصطفى منصور، ج. جلال محمد إبراهيم: الوجيز في مصادر الالتزام، بدون بدون ناشر ٢٠٠٠/ ٢٠٠١، ص ٤٧.

(٥٦)- في هذا المعنى، انظر: حمدي عبد الرحمن، الوسيط في النظرية العامة للالتزامات، الكتاب الأول- المصادر الإرادية للالتزام، دار النهضة العربية، القاهرة، ١٩٩٩، ص ٨٨ وما بعدها.

(٥٧)- راجع: د. سليمان غانم، في النظرية العامة للالتزام، مصادر الالتزام، الجزء الاول، العقد والإرادة المنفردة، مكتبة عبد الله وهبه، القاهرة، ١٩٦٦، ص ٧٩.

هذا ويثير استخدام مصطلحي الرضاء والتراضي بعض اللبس، حيث ان الرضاء يشير، وفقًا للمعنى اللغوي[٥٨]، إلى إرادة فردية صادرة عن طرف واحد. بينما التراضي، يُستخدم للإشارة إلى توافق إرادتين أو أكثر.

ورغم ذلك نجد في الكتابات الفقهية، اختلافًا في تفسير العلاقة بين المصطلحين، فجانب يعتبر المصطلحين مترادفين، ويُشار إليهما مجتمعين بعبارة "الرضاء أو التراضي"، دون تفرقة واضحة بينهما[٥٩]. بينما جانب اخر يخصص معنى مستقلاً للتراضي، ويرى أنه عملية أوسع نطاقًا تشمل رضاء الطرفين. ويؤكد أن وجود التراضي يستلزم رضاء الطرفين، والذي بدوره يتطلب وجود إرادة. وعليه، فإن انعدام الإرادة يؤدي إلى انعدام الرضاء، وبالتالي استحالة تحقق التراضي[٦٠]. ولذا فان غالبية الفقه تحذر من استخدام المصطلحين معًا، وتُفضل استخدام لفظ التراضي، لما يتطلبه من توافر إرادتين متوافقتين[٦١].

---

[٥٨]– يقصد بكلمة: "رضاء" لغةً: هي مصدر راضي ورضِيَ، رضِيَ بـ، رضِيَ على، رضِيَ عن. يقال رضَّى فلان آخاه: أرضاه؛ جعله يرضى، أي يقبل أو يكتفي؛ وراضى فلانًا: وافقه أو أرضاه، ورِضا، مصدر رضِيَّ، رضِيّ بـ، رضِيّ على، رضِيّ عن، ويقال نظر بعين الرِّضا: أي قبل الشئ عن طيب نفس. راجع: د. أحمد مختار عمر وآخرون، معجم اللغة العربية المعاصرة، المجلد الثاني، عالم الكتب، الطبعة الأولى، ٢٠٠٨، فقرة ٢١٢٤، ص ٩٠٤، مادة "رضاء– رضَّى"؛ المعجم الوجيز، مجمع اللغة العربية، طبعة خاصة بوازرة التربية والتعليم ١٩٩٠، ص ٢٩٩.

[٥٩]– د. عبد الفتاح عبد الباقي، مرجع سابق، ص ٨٩، وأيضًا ص ٩٢.

[٦٠]– د. محمود جمال الدين زكي، الوجيز في نظرية الالتزام في القانون المدني المصري، الجزء الأول، في مصادر الالتزام، مطبعة لجنة التأليف والترجمة والنشر، ١٩٦٨، ص ٢٧.

[٦١]– انظر في استخدام هذا اللفظ على سبيل المثال: د. عبد الرزاق السنهوري، الوسيط في شرح القانون المدني، الجزء الأول: نظرية الالتزام بوجه عام، مصادر الالتزام، تنقيح المستشار/ أحمد مدحت المراغي، طبعة نادي قضاة مجلس الدولة، ٢٠٠٨، ف ٦٨ وما بعدها، ص ١٤٢ وما بعدها؛ د. سليمان غانم، مرجع سابق، ص ٧٧ وما بعدها؛ د. جلال محمد إبراهيم، مصادر الالتزام، دار النهضة العربية، القاهرة، ٢٠١١، الطبعة الثالثة، ص ٢٨؛ د. محمد حسام محمود

(ISSN: 2537- 0758)

وبمعنى اخر اكثر تبسيطاً فان الرضاء، في صورته الأساسية، هو تعبير عن إرادة فردية تهدف إلى إحداث أثر قانوني محدد. أما التراضي، فهو يتطلب التقاء إرادتين أو أكثر لتحقيق ذلك الأثر. ومن ثم، يُعد الرضاء أحد مكونات التراضي، ولكنه ليس مرادفًا له، مما يجعل التفرقة بين المصطلحين ضرورية عند مناقشة الإطار القانوني لأي تصرف أو عقد.

ووفقًا لنهج المذكرة الإيضاحية للقانون المدني المصري، يُعتبر ركن التراضي أول أركان العقد، ويشمل عنصر الرضاء الذي يرتبط بتعبير كل طرف عن إرادته. وقد أشارت المذكرة الإيضاحية إلى حالة تبادل الرضاء، مما يوحي– تقدير البعض من الفقه[٦٢]– بأن الرضاء يمثل تعبير كل طرف عن إرادته، ومن اجتماع هذه الإرادات يتكون التراضي في العقد.

ومع ذلك فقد زاد الخلط بين مصطلحي الرضاء والتراضي عند صدور القانون المدني المصري عام ١٩٤٨ ونشره في الوقائع المصرية[٦٣]. ففي الأعمال التحضيرية، استخدم المشرّع مصطلح التراضي، لكن عند صياغة النصوص القانونية (خاصة فى المواد من رقم ٨٩ إلى رقم م١٣٠)، استخدم مصطلح الرضاء لوصف الركن الأول للعقد، وألحقه بركني المحل والسبب.

هذا مع وجوب ملاحظة أن الفقه درج على استخدام المصطلحين بشكل مترادف للإشارة إلى توافق الإرادتين[٦٤]، إلا أن التراضي، وفقًا لهذا الاتجاه، يستغرق الرضاء

---

لطفي، النظرية العامة للالتزام، مصادر الالتزام، النسر الذهبي للطباعة، القاهرة، الطبعة الثانية، ٢٠٠٢، ص ٢٩.

[٦٢]– د. تامر الدمياطى، المرجع السابق، ص ٢٦.

[٦٣]– الوقائع المصرية في ١٩٤٨/٧/٢٩– العدد ١٠٨ مكرر.

[٦٤]– يقصد بالتراضي التعاقدي، توافق إرادات أطراف العقد وارتباطها على إحداث الأثر القانوني الذي يرنو إليه كل منهم من وراء إبرامه، راجع: د. جلال محمد إبراهيم، مصادر الالتزام، مرجع سابق، ص ٤٢٨؛ د. محمد حسن قاسم، مرجع سابق، ص ١٠٢.

ويتضمنه، بحيث يكون التراضي نتاج اجتماع إرادتين أو أكثر، كل منهما يعبر عن رضاء مستقل.

وبالرغم من أن الترادف بين المصطلحين يبدو منطقيًا في سياق إبرام العقد، حيث لا توجد حاجة عملية للتفرقة بينهما، إلا أن هذا الوضع لدى البعض من الفقه يختلف في سياق حماية البيانات الشخصية. ففي مجال حماية البيانات، يتمتع مصطلح الرضاء بذاتية خاصة، حيث يُعبر عن إرادة فردية صادرة عن شخص يباشر حقوقه على بياناته الشخصية. وبالتالي، لا يُقصد بالرضاء هنا مجرد توافق إرادتين، بل يُركز على تعبير شخص واحد عن إرادته الحرة والمستنيرة فيما يتعلق بجمع بياناته الشخصية أو معالجتها[٦٥].

وبمعنى اخر اكثر توضيحاً فإنه في إطار حماية البيانات الشخصية، يُعد الرضاء الرقمي مصطلحًا ذا دلالة محددة، حيث يعبر عن إرادة صاحب البيانات في منح أو رفض الإذن بمعالجة بياناته. هذا المفهوم يتجاوز مجرد التوافق المتبادل (التراضي) كما هو في العقود التقليدية، ليُركز على حماية الفرد واستقلالية إرادته في مواجهة معالجي البيانات والمسؤولين عنها. وعليه، فإن التفرقة بين الرضاء والتراضي تصبح ضرورية في هذا السياق لضمان وضوح المعنى ودقة التطبيق القانوني متى اختلفت الية الموافقة عقدية كانت أو غير عقدية.

## ثانيا- المعنى القانونى الخاص للموافقة او للرضاء الرقمى فى اللائحة الأوروبية لحماية البيانات والقانون الفرنسي:

عرّفت المادة الثانية فقرة (ح) من التوجيه الأوروبي رقم ٩٥/٤٦ بشأن "حماية الأفراد فيما يتعلق بمعالجة البيانات الشخصية وحرية تداول البيانات" رضاء صاحب البيانات بأنه: "كل تعبير عن الإرادة يكون حرًا ومحددًا ومستنيرًا (informée)، يقبل بموجبه صاحب البيانات معالجة البيانات الشخصية المتعلقة به"[٦٦].

---

[٦٥]– د. تامر الدمياطى، المرجع السابق، ص ٢٦ وما بعدها.

[٦٦]– يجري النص الفرنسي للمادة ٢ فقرة (ح) من التوجيه الأوروبي رقم ٩٥/٤٦ (الملغي)، كما يلي:

(ISSN: 2537- 0758)

ومـن اللافـت للنظـر أن قـانون المعلوماتيـة والحريـات الفرنسـي رقـم ١٧-٧٨، الصـادر فـي ٦ ينـاير ١٩٧٨، لـم يتبنَّ التعريـف الـوارد فـي التوجيـه الأوروبـي رقـم ٩٥/٤٦، رغم أنـه اعتبـر الموافقـة أو الرضـاء شرطًا مسبقًا لإجراء عمليـات معالجـة البيانات الشخصية. وهذا الاختلاف يعكس توجهًا مختلفًا للمشرع الفرنسي في التعامل مع مفهوم الرضاء في سياق حماية البيانات.

وعلى الصعيد الأوروبي، تولى فريق عمل "المادة ٢٩ "المختص بحماية البيانات الشخصية[٦٧] مهمة تفسير مفهوم الموافقة أو الرضاء وتقديم إرشادات عملية لتطبيق أحكام التوجيه الأوروبي[٦٨]. وقد لعب هذا الفريق دورًا بارزًا في توضيح الإطار العملي والقانوني للرضاء على المستوى الأوروبي. وعلى الصعيد الوطني الفرنسي، قامت اللجنة الوطنية للمعلوماتية والحريات (CNIL) بمهمة مماثلة، حيث عملت على تفسير الأحكام المرتبطة بالرضاء وتطبيقها في إطار التشريع الفرنسي[٦٩].

---

"Consentement de la personne concernée: toute manifestation de volonté libre, spécifique et informée par laquelle la personne concernée accepte que des données à caractère personne la concernant fassent l'objt d'un traitement" .

[٦٧]– فريق عمل "المادة ٢٩" بشأن حماية البيانات الشخصية

Groupe de travail "Article 29" sur la protection des données (GT. Art, 29) .

هو فريق استشاري أوروبي مستقل تعامل مع قضايا الخصوصية والبيانات الشخصية حتى ٢٥ مايو ٢٠١٨ (قبل دخول اللائحة الأوروبية لحماية حيز التنفيذ)، وجرى إنشاء هذا الفريق بموجب المادة ٢٩ من التوجيه الأوروبي رقم ٤٦/ ٩٥ (الملغي) لمزيد من التفصيل، راجع:

Marie LIFRANGE, Protection des données à caractère personnel: le concentement à l'épreuve de l'ère numérique, Master en droit, Faculté de Droit, LiÈGE Université, 2017- 2018, p. 21 .

[٦٨]– اعتمد فريق عمل "المادة ٢٩" الإرشادات بشأن الرضاء في ظل لائحة الاتحاد الأوروبي رقم ٦٧٩/ ٢٠١٦ في ١٠ أبريل ٢٠١٨.

[٦٩]– تتمثل مهمة اللجنة الوطنية للمعلوماتية والحريات Commission nationale de l'informatique et des libertés وفقًا لقانون المعلوماتية والحريات رقم ١٧-٧٨ الصادر في ٦ يناير ١٩٧٨ وتعديلاته. باعتبارها سلطة إدارية مستقلة، في التأكد من أن تكنولوجيا

ومع صدور اللائحة الأوروبية العامة لحماية البيانات (GDPR) عام ٢٠١٦، تم إعادة تعريف موافقة أو رضاء صاحب البيانات بشكل أكثر دقة وتفصيلاً[٧٠]. حيث استهدفت هذه الخطوة تحقيق الهدف الرئيسي للائحة، وهو تعزيز حقوق الأفراد في السيطرة على بياناتهم الشخصية، وضمان قدرتهم على مراقبة جمع هذه البيانات واستخدامها. وقد أضافت اللائحة أحكامًا تفصيلية لضمان أن يكون الرضاء الصادر عن صاحب البيانات متوافقًا مع المعايير الحديثة لحماية الخصوصية في العصر الرقمي.

وعرّفت المادة ٤ بند ١١ من اللائحة العامة لحماية البيانات (GDPR) موافقة أو رضاء صاحب البيانات بأنه: "أي تعبير عن الإرادة يكون حرًا، ومحددًا، ومستنيرًا، وقاطعًا (لا لبس فيه)، يقبل بموجبه صاحب البيانات، من خلال إعلان أو تصرف إيجابي واضح، معالجة البيانات الشخصية المتعلقة به"[٧١].

---

المعلومات موضوعة في خدمة المواطن وأنها لا تؤثر على هوية الإنسان وحقوقه وخصوصياته وحرياته العامة أو الفردية، راجع الموقع الإلكتروني للجنة، التالي: https: //www. cnil. fr

وقد حدد قانون المعلوماتية والحريات صلاحياتها فأشار إلى تمتع هذهض اللجنة بسلطة رقابية تمكنها من حصر ومتابعة المخالفات المتعلقة بالمعالجة الآلية للبيانات الشخصية: الأمر الذي يجعل منها سلطة عقابية متى توافرت شروط معينة. ومن ناحية أخرى حدد المجلس الدستوري الفرنسي شروط الاعتراف بالعقوبات التي توقعها هذه اللجنة، وهي: ١- احترام مبدأ شرعية الجرائم والعقوبات. ٢- احترام مبدأ العقوبة. ٣- احترام مبدأ عدم رجعية قوانين العقوبات. ٤- احترام حقوق الدفاع. انظر: د. محمد سامي عبد الصادق، مرجع سابق، ص ص ٤٧، ٤٨.

[٧٠]- يدلل البعض ع دقة تعريف الرضاء في اللائحة الأوروبية بأنه يحل مشكلات عديدة تتعلق بنطاق الرضاء والموافقة على معالجة البيانات. د. محمد جميل خلف الله، الإطار التشريعي لحماية البيانات الشخصية في القانون المصري، مجلة رؤى تكنولوجية، تصدر عن مركز المعلومات ودعم اتخاذ القرار التابع لمجلس الوزراء المصري، العدد الأول، مارس ٢٠٢١، ص٣٦.

[٧١]- يجري النص الفرنسي للمادة ٤ بند ١١ من اللائحة العامة لحماية البيانات، كما يلي:

(ISSN: 2537- 0758)

ولتوضيح مفهوم الموافقة الرقمية أوالرضاء الرقمي وتفسير أحكامه بشكل عملي، أصدر مجلس حماية البيانات الأوروبي (EDPB)، الذي حل محل فريق عمل المادة ٢٩[٧٢]، الإرشادات رقم ٥ لسنة ٢٠٢٠. تهدف هذه الإرشادات، الصادرة بتاريخ ١٤ مايو ٢٠٢٠[٧٣]، إلى تقديم تفسير واضح ومفصل لأحكام اللائحة الأوروبية رقم ٢٠١٦/٦٧٩ (GDPR) فيما يتعلق بالرضاء، مع التركيز على كيفية تطبيق هذه الأحكام لضمان حماية حقوق الأفراد على بياناتهم الشخصية.

---

"Consentement" de la personne concernée, toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractèe personnel la concernant fassent l'objet d'un traitment".

[٧٢]– اعتبارًا من ٢٥ مايو ٢٠١٨ تاريخ نفاذ وتطبيق اللائحة العامة لحماية البيانات (GDPR)، تم حل فريق العمل الخاص بالمادة ٢٩، وتم استبداله بموجب اللائحة، بمجلس حماية البيانات الأوروبي Le comité européen de la protection des données "CEPD (وبالإنجليزية The European Data Protection Board "EDPB)، ويعد هذا المجلس هيئة أوروبية مستقلة، ويقع مقره في بروكسل ببلجيكا، وتتمثل مهمته الرئيسية في ضمان التطبيق المتسق لقواعد حماية البيانات في جميع أنحاء الاتحاد الأوروبي، وتعزيز التعاون بين سلطات حماية البيانات في الاتحاد الأوروبي، ويتكون المجلس من ممثلين عن هيئات حماية البيانات الوطنية، والمشرف الأوروبي على حماية البيانات Contrôleur européen de la protection des données. راجع: المبحث الثالث من الفصل السابع من اللائحة العامة لحماية البيانات GDPR، المواد ٦٨ إلى ٧٦ منها. ولمزيد من التفصيل حول مجلس حماية البيانات الأوروبي، راجع موقعه على الإنترنت التالي: https: //edpb. europa. eu/edpb

[٧٣]– جدير بالذكر أن هذه الإرشادات بشأن الرضاء كان حصيلة جهود فريق عمل "المادة ٢٩"، وقد اعتمدها الفريق في ١٠ أبريل ٢٠١٨، وقد وافق مجلس حماية البيانات الأوروبي في جلسته العامة الأولي على هذه الإرشادات، وأصدر نسخة محدثة قليلاً منها تحمل رقم ٢٠٢٠/٥، انظر:

Lignes directrices 5/2020 sur le consentement au sens du règlement (UE) 2016/6/679, Le Comité Européen de la Protection des Données, Version 1. 1, Adoptées le 4 mai Disponible sur le site: https: //edpb. europa. eu/site/edpb/files/files/file 1/edpb_guidelines_202005_consent_fr. pdf .

مع ذلك لم يقدم المشرع الفرنسي تعريفًا صريحًا للموافقة أو للرضاء ضمن تعديل قانون المعلوماتية والحريات رقم ١٧-٧٨ الصادر في ٦ يناير ١٩٧٨، والمعدل بالقانون رقم ٤٩٣ لسنة ٢٠١٨ بشأن حماية البيانات الشخصية. وبدلًا من ذلك، اكتفى بالإشارة إلى انطباق التعريفات الواردة في المادة ٤ من اللائحة الأوروبية العامة لحماية البيانات(GDPR) على أحكام القانون الفرنسي، ما لم يرد نص يقضي بخلاف ذلك (المادة ٢، الفقرة الأخيرة من قانون المعلوماتية والحريات)[٧٤].

ويترتب على ذلك أن تعريف "موافقة أو رضاء صاحب البيانات" الوارد في اللائحة الأوروبية يُعتبر ساريًا ومطبقًا على جميع الأحكام المتعلقة بالرضاء في إطار قانون المعلوماتية والحريات الفرنسي، مما يضمن التوافق بين التشريع الوطني الفرنسي والإطار الأوروبي لحماية البيانات الشخصية[٧٥].

ورغم التشابه بين التعريف الجديد للموافقة أو للرضاء الوارد في اللائحة الأوروبية (GDPR) وتعريفه في التوجيه الأوروبي رقم ٩٥/٤٦ (الملغى)، إلا أن التعريف الجديد يتميز بمزيد من الدقة والتفصيل. ومن أبرز الجوانب التي تميزه، الطابع الصريح للرضاء، حيث يجب أن يكون الرضاء ناتجًا عن إعلان واضح أو تصرف إيجابي يعبر بجلاء عن إرادة الشخص المعني ببياناته. والقاطع (غير الملتبس)، حيث أضاف التعريف عنصرًا جديدًا يتمثل في ضرورة أن تكون الموافقة أو الرضاء قاطعًا، أي لا يحتمل أي شك أو لبس في دلالته، مما يضمن وضوح نية صاحب

---

[٧٤]- هذه الفقرة مضافة بموجب المادة ١ من الأمر رقم ١١٢٥-٢٠١٨ الصادر في ١٢ ديسمبر ٢٠١٨، سالف الإشارة إليه.

[٧٥]- راجع: التقرير المقدم إلى رئيس الجمهورية الفرنسية بشأن الأمر رقم ١١٢٥- ٢٠١٨ المؤرخ ١٢ ديسمبر ٢٠١٨، وخاصة التعليق على تعديل المادة من قانون المعلوماتية والحريات، الذي يحدد التعريفات المطبقة في إطار هذا القانون، ويحيل إلى المادة ٤ من اللائحة الأوروبية في شأن هذه التعريفات. راجع:

Rapport au Président de la Réublique relatif à l'ordonnance no 2018- 1125 du décembre 2018. JORF, 13 décembre 2018, Text 4 .

(ISSN: 2537- 0758)

البيانات ويقلل من احتمالات إساءة الفهم أو التفسير. وهذا التطور يعكس اهتمامًا أكبر بحماية حقوق الأفراد، ويضع معايير أكثر صرامة لضمان صحة الموافقة أو الرضاء في سياق معالجة البيانات الشخصية.

وبوجه عام، يُبرز هذا التعريف عددًا من المسائل الأساسية المتعلقة بمفهوم الموافقة أو الرضاء، والتي سوف نوضح جوانبها المختلفة بالتحليل والتفصيل لاحقًا. وفي هذا السياق، سنقتصر على تقديم عرض موجز لهذه المسائل، بالقدر الذي يساعد على توضيح مدلول الموافقة أو الرضاء وتحديد أبعاده القانونية بشكل أولي[٧٦].

ويتطلب هذا التعريف، من ناحية أولى، أن تكون موافقة أو رضاء صاحب البيانات متمثلًا في "أي" شكل من أشكال التعبير عن الإرادة، وهي عبارة تعكس مرونة في تطبيقه، حيث لا يفرض التوجيه الأوروبي شكلًا محددًا للتعبير عن الرضاء. كما أن التعريف لم يشترط الكتابة كوسيلة للتعبير عن الإرادة، مما يُفسر على أنه نهج يهدف إلى تحقيق مرونة أكبر في الأحكام، بما يتلاءم مع تنوع السياقات الرقمية التي قد يُعبر فيها الأفراد عن موافقتهم.

وتأكيدا لذلك فقد أوضح فريق عمل "المادة ٢٩"، في الرأي الاستشاري رقم ٢٠١١/١٥ بشأن تعريف الموافقة أو الرضاء[٧٧]، أن استخدام عبارة "أي تعبير عن

---

[٧٦]– في شأن أحكام التوجيه الأوروبى، انظر: على سبيل المثال:

A. DWBET, J. MASSOT et N. METALLIONS, Informatique et Libertés, op. cit., pp. 73 et s.; Cécile DE TERWANGNE et Karen ROSIER, Le Règlement général de protection des données (RGPD/ GDPR), coll. Du CRIDS, Larcier, 1re édition, 2018 .

[٧٧]– في الرأي الاستشاري رقم ٢٠١١/١٥ بشأن تعريف الرضاء، الصادر عن فريق عمل المادة ٢٩، في ١٣ يوليو ٢٠١١، يركز فريق العمل حصريًا على دور الرضاء في حماية البيانات الشخصية، ويتكون الهدف المنشود منه في شقين: من ناحية، يوضح الفريق معظم الأحكام الغامضة للتوجيه رقم ٩٥/٦٤، ومن ناحية أخرى، يهدف لمراجعة التوجيه، واقترح الفريق تغييرات على تعريف الرضاء في هذا التوجيه. راجع:

الإرادة (toute manifestation de volonté) "يُتيح تفسيرًا واسعًا لنطاق هذا التعبير. ويعني ذلك أن أي إشارة واضحة يمكن أن تُعتبر دلالة كافية على وجود إرادة صاحب البيانات، بشرط أن تكون مفهومة من قبل المسؤول عن المعالجة أو المتحكم[٧٨]. وهذا النهج يهدف إلى ضمان استيعاب مختلف الأشكال والوسائل التي قد يستخدمها الأفراد للتعبير عن رضاءهم في سياقات متنوعة، بما يتلاءم مع التطورات التكنولوجية والمرونة المطلوبة في البيئة الرقمية.

ومن ناحية أخرى، يحدد التعريف عددًا من الشروط العامة اللازمة لصحة الموافقة أو الرضاء الصادر عن صاحب البيانات، وهي: أن يكون حرًا، حيث يجب أن يصدر الرضاء بإرادة خالية من أي إكراه أو ضغط خارجي. وأن يكون محددًا، حيث يجب أن يتعلق بغرض معين وواضح، دون أن يكون عامًا أو غير محدد. وأن يكون واضحًا وقاطعًا (لا لبس فيه)، حيث يتعين أن يكون التعبير عن الإرادة جليًا، بما لا يدع مجالًا للشك أو التأويل، لضمان صدوره عن إرادة حقيقية لصاحب البيانات.

من ناحية ثالثة، يشترط لصحة الموافقة أو الرضاء أن يتخذ التعبير عن الإرادة صورة إعلان أو تصرف إيجابي واضح، بحيث يدل بشكل لا لبس فيه على موافقة صاحب البيانات على معالجة بياناته الشخصية. وكما تؤكد اللائحة الأوروبية (GDPR) على حق صاحب البيانات في سحب الموافقة أو الرضاء (المادة ٧، الفقرة ٣)، مما يعني أن الموافقة أو الرضاء ليس قرارًا نهائيًا، بل هو قابل للعدول عنه

---

Groupe de travail "article 29", Avis 15/2011 sur ka définition du consentement, adopté le 13 juillet 2011, wp 187. Disponible sur le site: https: //cnpd. public. lu/dam-assets/fr/publications/groupe-art29/wp187_fr, pdf .

(77)- Groupe de travail "article 29", Avis 15/2011 sur la définition dy consentement, op. cit., p. 12 .

(٧٨)– راجع في هذا الشأن:

Groupe de travail "article 29", Avis 15/2011 sur la définition dy consentement, op. cit., p. 12 .

(ISSN: 2537- 0758)

في أي وقت. ويُبرز هذا الحق الدور المحوري للرضاء في تمكين صاحب البيانات من الاحتفاظ بدرجة من الرقابة المستمرة على معالجة بياناته، ويعزز مبدأ الشفافية وحماية الحقوق الفردية في التعامل مع البيانات الشخصية[٧٩].

وإلى جانب تقديمها تعريف محدد للموافقة أو للرضاء، فإن اللائحة الأوروبية (GDPR) تعتبر رضاء صاحب البيانات أحد الأسس القانونية الجوهرية التي يجب أن تستند إليها أية معالجة للبيانات الشخصية، وذلك وفقًا لما نصت عليه المادة ٦ من اللائحة. كما تقدم اللائحة إرشادات إضافية لضمان الامتثال لشروط الموافقة أو الرضاء في المادة ٧، مع تخصيص المادة ٨ لبيان الشروط الخاصة برضاء أو موافقة الأطفال في سياق خدمات مجتمع المعلومات.

**علاوة على ذلك**، توفر اللائحة أحكامًا تتعلق بأمن البيانات الشخصية، تحدد كيفية التزام المتحكم بضمان تحقيق العناصر الرئيسية لشروط الموافقة. وتشمل هذه الأحكام المواد ٣٢، ٣٣، ٤٢، و٤٣، التي تركز على التدابير الواجب اتخاذها لضمان حماية البيانات وسلامة عمليات معالجتها، بما يعزز الشفافية والثقة بين صاحب البيانات والمسؤول عن معالجتها.

## ثالثاً: تحديد معنى الموافقة الرقمية أو الرضاء الرقمي في قانوني حماية البيانات الشخصية المصري و الاماراتي:

خصص قانون حماية البيانات الشخصية المصري فى الفصل الأول منه (المادة الأولى) لتعريف المصطلحات المستخدمة في القانون، مثل البيانات الشخصية، البيانات الشخصية الحساسة، الشخص المعني بالبيانات، الحائز، والمتحكم في البيانات، إلى جانب تعريفات أخرى. ويبدو أن المشرع المصري استلهم في صياغة

[٧٩]– راجع في هذا الشأن:

Lignes directrices 5/2020 sur le consentement au sens du réglement (UE) 2016/679, op. cit, m no. 8-10, p. 9 .

العديد من هذه التعريفات من اللائحة الأوروبية لحماية البيانات (GDPR)، مع وجود بعض الاختلافات في صياغة بعض التعريفات أو إغفال البعض الآخر[٨٠].

ومع ذلك، يلاحظ وبحق البعض من الفقه المصرى[٨١] أن القانون المصري قد أغفل تقديم تعريف للموافقة الرقمية أو ما يطلق عليه عملياً الرضاء الرقمى للشخص المعني بالبيانات. ويثير هذا الأمر تساؤلات، خاصة وأن القانون توسع في تقديم تعريفات تفصيلية للمفاهيم الأخرى ذات الصلة. خاصة وانه كان من الأجدر أن يتضمن القانون تعريفًا واضحًا للموافقة أو للرضاء، بالنظر إلى أهميته كركيزة أساسية لمشروعية معالجة البيانات الشخصية، لتيسير فهمه من قبل المخاطبين بأحكام القانون وتعزيز اتساقه التشريعي مع المعايير الدولية.

ولهذا يبدو أنه من المناسب، عند تعديل القانون، ان يرد تعريف موافقة أو رضاء صاحب البيانات، ضمن المادة المعنية بالتعريفات، على غرار اللائحة الأوروبية، والقانون الاماراتى، خاصة وانه لا يمكن ان تتصدي اللائحة التنفيذية لتعريف رضاء أو موافقة الشخص المعني بالبيانات، باعتبارها من المسائل التي يختص بها القانون بحسب الأصل، باعتبار هذا التعريف يمس أحكامه ويتصل ويؤثر على جوهرها، مما لا يمكن تركه لتنظيم اللائحة التنفيذية[٨٢]، وهي أدنى من التشريع في مراتب تدرج القواعد القانونية.

وفى النظام القانونى الاماراتى، ووفقًا لنص المادة الاولى من القانون الاتحادي رقم ٤٥ لسنة ٢٠٢١ بشأن حماية البيانات الشخصية في دولة الإمارات العربية المتحدة، يُعرّف المشرع الموافقة بانها هى "الموافقة التي يصرح فيها صاحب البيانات

---

[٨٠]– د. محمد جميل خلف الله، مرجع سابق، ص ٣٦.

[٨١]– د. تامر الدمياطى، المرجع السابق، ص ٣١.

[٨٢]– وفقًا للمادة الرابعة من القانون رقم ١٥١ لسنة ٢٠٢٠ بشأن إصدار قانون حماية البيانات الشخصية يصدر الوزير المعني بشئون الاتصالات وتكنولوجيا المعلومات اللائحة التنفيذية للقانون المرافق خلال ستة أشهر من تاريخ العمل بهذا القانون.

(ISSN: 2537- 0758)

للغير بمعالجة بياناته الشخصية، على أن تكون هذه الموافقة بشكل محدد وواضح لا لبس فيه على قبوله بمعالجة بياناته الشخصية من خلال بيان أو إجراء إيجابي واضح".

وفى ضوء ما تقدم يرى جانب من الفقه(٨٣)، انه وان كان المشرع الأوروبي قد استخدم لفظ الرضاء consentement، للدلالة على اتجاه إرادة صاحب البيانات لقبول معالجة البيانات، قغنه لم يحسن المشرع المصري ترجمته، وصاغه على أنه يعنى "الموافقة"، رغم وجود فارق بين لفظي "الرضاء" و"الموافقة"، فالأول (الرضاء) أوسع نطاقًا ويستوعب اللفظ الآخر (الموافقة أو القبول L'acceptation)، كما جاء استخدامه لهذا اللفظ مبتعدًا عن اصطلاحات القانون المدني، رغم أن المصطلح القانوني يجب أن يرد في جميع النصوص في أي نظام قانوني لفظًا واحدًا لا يتبدل ولا يتغير، حتى لا تضطرب الاصطلاحات أو تتعارض(٨٤).

ويدعم هذا الرأى موقفه بالعديد من الحجج منها حرص المشرع الفرنسي في قانون المعلوماتية والحريات وتعديلاته على استخدام مصطلح "الرضاء "في سياق حماية البيانات الشخصية، متسقًا بذلك مع أحكام القانون المدني الفرنسي. هذا النهج يعكس رغبة المشرع في تحقيق التناغم بين المفاهيم والاصطلاحات القانونية داخل النظام القانوني الفرنسي نفسه، مما يعزز من وضوح النصوص القانونية ويسهل تطبيقها من قبل المخاطبين بها(٨٥).

وبالرجوع إلى المعاجم اللغوية الفرنسية، وخاصة القانونية، للوقوف على معنى لفظ consentement، المستخدم في اللائحة الأوروبية والقانون الفرنسي، يشير

(٨٣)– د. تامر الدمياطى، المرجع السابق، نفس الموضع.

(٨٤)– د. عبد الرزاق السنهوري: مرجع سابق، ص ٣٥.

(٨٥)– تدليلاً على تناسق المصطلحات القانونية في النظام القانوني، نجد نص المادة ١١٠٩ الجديدة من القانون المدني الفرنسي تنص على أن: "يكون العقد رضائيًا عندما ينعقد بمجرد تبادل الرضاء échange des consentements بين أطرافه أيًا كانت طريقة التعبير عنه".

معجم "كورنو CORNU" للمصطلحات القانونية، أنه يقصد به "الرضاء" ويعنى "اتفاق إرادتين أو أكثر على على إحداث آثار قانونية؛ فالتقاء هذه الإرادات هو شرط لإبرام عقد (مثل رضاء طرفي العقد، ورضاء الزوجين بالزواج)، كما يقصد به إرادة كل من طرفي التعاقد في الاتفاق (يتعلق الأمر هنا بتبادل الرضاء)، وأن هذا اللفظ يعني بصورة خاصة أحيانًا "القبول L'acceptation (الذي يقابل الإيجاب أو الطلب)"[٨٦].

**وأخيرًا**، يتضح أن المشرع المصري قد توسع في تحديد محل الموافقة الرقمية أو الرضاء الرقمي، أي النطاق الذي يمكن أن ينصب عليه التعبير عن رضاء صاحب البيانات. فقد شمل هذا النطاق جمع البيانات، معالجتها، الإفصاح عنها، أو إفشائها[٨٧].

في المقابل، ركزت اللائحة الأوروبية (GDPR) محل الموافقة أو الرضاء على المسائل المتعلقة بمعالجة البيانات الشخصية بشكل رئيسي، لكنها توسعت في تعريف مفهوم المعالجة ليشمل مجموعة واسعة من العمليات المرتبطة بالبيانات، مثل جمع البيانات، حفظها، إتاحتها، تعديلها، أو محوها[٨٨].

وهذا التباين يعكس اختلافًا في النهج التشريعي بين القانون المصري واللائحة الأوروبية، حيث يمنح القانون المصري تعريفًا أكثر تفصيلًا لمحل الرضاء، في حين يتبع النهج الأوروبي إطارًا أكثر تركيزًا لكنه يغطي العمليات ذات الصلة من خلال توسيع تعريف المعالجة.

---

(86)- 1-l'accord de deux ou plusieurs volontés en vue de créer effets de droit; rencontre de ces volontés qui est la condition de la formation du contrat (ex. Consentement des parties au contrat, des éoux au mariage). Gérard CORNU, Vocabulaire juridique, Association Henri Capiyant, Paris, Quadrige/PUF, 2009, Vo consentement, p. 217 .

(٨٧)– راجع: المادة ٢ فقرة أولى من قانون حماية البيانات الشخصية المصري.

(٨٨)– راجع: المادة ٢ بند ٢ "تعريف المعالجة" من اللائحة العامة لحماية البيانات GDPR.

(ISSN: 2537- 0758)

## رابعاً- التعريف المقترح للموافقة الرقمية أو للرضاء الرقمى فى شأن حماية البيانات:

لضمان إقتراح تعريف جامع و مانع للموافقة الرقمية أو للرضاء الرقمي، فإنه يجب أن يتضمن التعريف كافة العناصر الضرورية لوجود وصحة الموافقة. ومن أهم هذه العناصر، عنصرإرادة صاحب البيانات، حيث يجب أن يكون الرضاء نابعًا عن إرادة حرة ذاتية تتمتع بالتمييز القانوني، أي صادرة عن شخص يُعتد بإرادته قانونًا، سواء كان ذلك صاحب البيانات نفسه أو نائبه القانوني. وعنصر سمات أو خصائص الإرادة، حيث يجب أن تكون الإرادة واضحة، محددة، مستنيرة، وقاطعة، بما يعكس وعي الشخص بكافة تفاصيل المعالجة التي يوافق عليها. وعنصر نطاق الرضاء، حيث ينبغي أن يكون الرضاء مرتبطًا بخدمات مجتمع المعلومات الرقمى، بما في ذلك العمليات المتعلقة بمعالجة البيانات الشخصية في البيئة الرقمية سواء للمتحكم فى البيانات أو للمعالج لها.

وبناء على ما تقدم فان التعريف المقترح للموافقة أو للرضاء الرقمي لصاحب البيانات، واتساقًا مع أحكام اللائحة الأوروبية (GDPR)، وقانونى حماية البيانات المصرى والاماراتى، هو: كل تعبير عن الإرادة في صورة إلكترونية أو رقمية[٨٩]،

[٨٩]– وذكرت فى التعريف الوسائل الرقمية والالكترونية من باب الاحتياط ان كانت الوسائل الرقمية تختلف عن الوسائل الالكترونية من حيث اثارها القانونية، مع ان قانون حماية البيانات المقارنة لم يؤكد ذلك، وعليه فان ان اى تعبير عن الإرادة في صورة رقمية يشير إلى اى إعلان أو إظهار رغبة أو نية قانونية للطرف أو الأطراف المعنية في إتمام تصرف قانوني أو الالتزام بعمل معين، وذلك باستخدام الوسائل الرقمية بدلاً من الوسائل التقليدية المكتوبة أو الشفهية يعد تعبير رقمى أو موافقة رقمية. ومن الأمثلة على التعبير عن الإرادة في صورة رقمية نذكركذلك، التوقيع الإلكتروني، وذلك عندما يُعبر الشخص عن قبوله أو موافقته على عقد أو مستند قانوني باستخدام توقيع رقمي معتمد. وإرسال الموافقة عبر البريد الإلكتروني، وذلك حينما يرسل أحد الأطراف موافقته على شروط معينة من خلال رسالة إلكترونية موثقة. والنقر على زر "أوافق"، وذلك أثناء التسجيل فى اى تطبيق رقمى أو في خدمة إلكترونية أو شراء منتج عبر الإنترنت،

يصدر عن صاحب البيانات أو نائبه القانوني[٩٠]، يكون حرًا، واضحًا، محددًا، مستنيرًا، وقاطعًا، ويدل على رضائه بصورة صريحة وإيجابية بقيام أو بإتمام عملية رقمية أو الكترونية تتناول بياناته الشخصية"[٩١]. وهذا التعريف يضع إطارًا شاملًا

---

يعتبر النقر على زر "أوافق على الشروط والأحكام" تعبيراً عن الإرادة. وإبرام العقود الإلكترونية مثل توقيع عقود البيع أو الإيجار عبر منصات إلكترونية دون الحاجة إلى وثائق ورقية. وكذلك العقود الذكية، والتصريحات الرقمية الرسمية مثل تقديم إقرار ضريبي أو طلب رسمي عبر منصة حكومية إلكترونية. واخيرا الوصايا الرقمية، حيث الانتشار المتزايد للوصايا الرقمية، والتي يمكن إنشاؤها باستخدام الهواتف الذكية أو الكاميرات أو أجهزة الكمبيوتر. **انظر:**

Andropova, T. (2018). Testamentary: untypical forms of the will and the use of new technologies. Ex Jure, (1), 30-44. https: //doi. org/10. 17072/2619-0648-2018-1-30-44

Bhattacharya, S., Singh, A., & Hossain, M. (2019). Strengthening public health surveillance through blockchain technology. Aims Public Health, 6(3), 326-333. https: //doi. org/10. 3934/publichealth. 2019. 3. 326

- Michels, J. and Millard, C. (2022). The new things: property rights in digital files?. The Cambridge Law Journal, 81(2), 323-355. https: //doi. org/10. 1017/s0008197322000228

-Novitsky, A., Bondarev, A., Dobritsky, A., Tyurin, I., & Komarov, Y. (2022). Legal support for the digital economy in the russian federation: legal policy priorities. Revista De Investigaciones Universidad Del Quindío, 34(S3), 244-255. https: //doi. org/10. 33975/riuq. vol34ns3. 1074

[٩٠]– وهذا يفيد فى ان هذا التعبير عن الارادة للموافقة قد يكون فى صورة رضاء فردى مسبق صادر من صاحب البيانات، وقد يكون فى صورة رضاء أو تراضى متبادل حيث يكون التعبير إما بالإيجاب وإما بالقبول فى التعاقد صادر من صاحب البيانات أو من المعالج أو المتحكم، وقد يصدر من الشخص صاحب البيانات نفسه، وقدر يصدر من نائبه خاصة النائب القانونى.

[٩١]– وهذا يدل على ان الرضاء أو الموافقة تنصب على كل تعامل رقمى يتناول اى بيان من البيانات الشخصية أو جميعها سواء من قبل المتحكم "ان كان هو المعالج أم متحكم فقط"، ومن المعالج للبيانات، أو من مسئول حماية البيانات وغيره. خاصة وان اشخاص منظومة حماية البيانات متعددة و متنوعة. راجع نص المادة رقم (١) من المرسوم الاماراتى بقانون اتحادي رقم (٤٥) لسنة ٢٠٢١ ومن القانون المصرى رقم ١٥١ لسنة ٢٠٢٠.

(ISSN: 2537- 0758)

يضمن وضوح المفهوم ودقته، بما يتلاءم مع المعايير الحديثة لحماية البيانات الشخصية في العصر الرقمي.

## الفرع الثاني

## الطبيعة القانونية للموافقة

تثير الموافقة الرقمية أو الرضاء الرقمي المتعلق بمعالجة البيانات الشخصية تساؤلات متعددة حول طبيعتها القانونية، حيث يتمحور النقاش حول ما إذا كان هذا الرضاء يتوافق مع القواعد العامة للعقد، باعتباره جزءًا من الإطار التعاقدي التقليدي، أم أنه ينتمي إلى نظام قانوني مستقل يتميز بخصوصيته وتفرده. وتشابه هذه المسألة إلى حد كبير ما يُثار بشأن الموافقة أو الرضاء في العمل الطبي، الذي اتجه الفقه والقضاء إلى تصنيفه بعيدًا عن إطار الرضاء التعاقدي، معتبرين إياه بمثابة إذن أو رخصة صادرة من طرف واحد، دون الحاجة إلى تقابلها مع إرادة طرف آخر[٩٢].

هذا التمييز يعكس الخصوصية التي قد يحملها الموافقة أو الرضاء الرقمي، مما يستدعي دراسة معمقة لطبيعته القانونية ومدى ارتباطه بمبادئ العقود التقليدية أو انتمائه لنظام قانوني مستقل. وذلك من خلال استعراض الاتجاهات المختلفة فى هذا الشأن فيما يلى:

**الاتجاه الاول: القائل بان الموافقة عمل قانونى بالارادة المنفردة:**

اتجه بعض الفقه[٩٣] في سبيل بيان طبيعة الموافقة الرقمية في إطار اللائحة الأوروبية (GDPR)، أي الموافقة المستخدمة كأساس قانوني لمعالجة البيانات، إلى التأكيد على اختلافها التام عن الموافقة في العقد، مشيرًا إلى أنه "لا ينبغي النظر إلى

---

[٩٢]– انظر فى تفاصيل الموافقة على العمل الطبى، القادري، ف. (٢٠٢٤). العمل الطبي ومشروعيته والخطأ الناتج عنه. مجلة جامعة صنعاء للعلوم الإنسانية، العدد ١، الجزء ١. متاح عبر: https: //doi. org/10. 59628/jhs. v1i1. 601.

[93]- Thierry LÉONARD, "Yves tit u exploitais tes données?", in Droit norms et libertés dans le cybermonde: Liber Amicorym Yves Poullet, Larcier, Bruxelles, 2018, p. 663 et s .

الموافقة الواردة في اللائحة على أنها تنشئ علاقة تعاقدية محددة مع المتحكم في البيانات، بل ينبغي اعتبارها واجبًا قانونيًا (devoir legal) يُفرض على المتحكم بقوة القانون، من أجل توفير حماية خاصة لصاحب البيانات(٩٤).

وسواء أكانت الموافقة تشكل أساسًا لمشروعية المعالجة أم تمثل شرطًا لرفع الحظر المفروض على معالجة البيانات، فإن هذه الموافقة تُفرض بحكم الأثر الملزم للقانون، وليس تأسيسًا على توافق إرادات المتعاقدين بشأن طرق المعالجة المزمع إجراؤها. وينتهي هذا الاتجاه الفقهي إلى أن "موافقة صاحب البيانات تبدو كعمل قانوني صادر بالإرادة المنفردة (acte juridique unilateral)(٩٥)، باعتبارها مصدرًا للالتزام، يخول المتحكم فقط اتخاذ سلسلة من الإجراءات المتعلقة بالمعالجة المعنية امتثالًا لأحكام اللائحة الأوروبية".

---

(94)- Th. LÉONARD, op. cit., p. 666 .

(٩٥)– يقصد بالإرادة المنفردة أو العمل القانوني الصادر من جانب واحد acte juridique unilateral "اتجاه الإرادة إلى إحداث نتائج قانونية معينة"، فهو يرجع لإرادة الشخص منفردًا. راجع: د. عبد الرزاق السنهوري، مرجع سابق، رقم ٩٠٦، ص ١٠٩٥؛ ويقصد بها أيضًا: "تلك التي تصدر من شخص واحد، من غير أن تتوافق مع إرادة شخص آخر غيره". والإرادة المنفردة تستطيع في مجالات كثيرة أن ترتب بعض الآثار القانونية. انظر: د. عبد الفتاح عبد الباقي، مرجع سابق، ص ٦٧٦. وفي هذا السياق، يعرف جانب من الفقه الفرنسي التصرف بالإرادة المنفردة (من جانب واحد) acte unilateral بأنه "تعبير عن الإرادة صادر عن شخص يقرر من خلاله ترتيب آثارًا قانونية معينة، دون الحاجة للحصول على رضاء شخص آخر. لتحقق هذا الغرض". انظر:

Partick WERY, Droit des obligations, Volume II, Les sources des obligations extracontractuelles, Le régime general des obligations Collection des Précis de la Faculté de droit de l'U. C. L., Bruxelles, Larcier, 2016, p. 23 .

كما يعرف البعض في إيجاز بأنه: "عمل إرادي يحدد بموجبه الشهص، بإرادته وحده، آثار قانونية معينة". انظر:

François TERRÉ, Philippe SIMLER, Yves LEQUETTE, et François CHÉNEDÉ, Droit civil, Les obligations, 12e éd., Dalloz, 2018, no. 509, p. 591 .

(ISSN: 2537- 0758)

وفي هذا الاتجاه، يذهب بعض الفقه إلى ضرورة التمييز بين الموافقة الرقمية والعقد، باعتبارهما مسألتين مستقلتين، ويرى أنه من المناسب عدم الخلط بين "الموافقة على العقد والموافقة على المعالجة، حيث تُعد الأخيرة تعبيرًا عن الإرادة يأذن به الشخص المعني بمعالجة بياناته. وتوصف هذه الموافقة كتصرف قانوني من جانب واحد"(٩٦).

غير أن وجهة النظر السابقة لا يمكن التسليم بها، إذ إن الموافقة الرقمية لا يمكن اعتبارها تصرفًا قانونيًا صادرًا بالإرادة المنفردة كمصدر لالتزام صاحب البيانات، كما هو الحال في الإيجاب الملزم أو الوعد بجائزة في القانون المدني(٩٧). ويعود هذا الاختلاف إلى طبيعة الإرادة المنفردة، باعتبارها عملًا قانونيًا من جانب واحد، يمكن أن تولد التزامات قانونية على عاتق الشخص المعني، حيث يكون مصدر هذه

(96)- Thibault DOUVILLE, La protection des données à caractére personnel des mineurs et des majeurs protégés, Revue Lamy Droit Civil (RLDS), septembre 2018, bo. 162, p. 42 .

(٩٧)– هناك حالات متفرقة ينص فيها القانون على نشوء الالتزام، ويكون مصدر الالتزام هو الإرادة المنفردة. ومن ذلك الإيجاب الملزم الوارد في المادة ٩٣ مدني مصرى، فمصدر الالتزام فيه هو إرادة الموجب المنفردة، حيث يجري نصها على مايلى: "١– إذا عين ميعاد للقبول التزم الموجب بالبقاء على إيجابه إلى أن ينقضي هذا الميعاد. ٢– وقد يستخلص الميعاد من ظروف الحال أو من طبيعة المعاملة". كما تنص المادة ١٠٦٦ مدنى مصرى في تطهير العقار المرهون رهنًا رسميًا على أنه: "يجب على الحائز أن يذكر في الإعلان أنه مستعد أن يوفي بالديون المقيدة إلى القدر الذي قوّم به العقار". ومفاد هذا النص أن الحائز يلتزم بمجرد الإعلان، فيكون مصدر التزامه هو إرادته المنفردة. وتنص المادة ١٦٢ مدنى على الوعد بجائزة. وهو النص الوحيد للإرادة المنفردة باعتبارها المصدر الثاني للالتزام بعد العقد. لمزيد من التفصيل، راجع: د. سليمان غانم، مرجع سابق، ص ٣٩٣ وما بعدها.

الالتزامات المباشر هو نص القانون، مما يمنع صاحب التصرف من حق العدول عنه[٩٨].

وهذا التفسير يتعارض مع الأحكام القانونية المنصوص عليها في اللائحة الأوروبية والقانون المصري، و القانون الاماراتى التي تجيز صراحةً لصاحب البيانات الحق في العدول عن الموافقة، مما يدل على أن الموافقة الرقمية لا تُنشئ التزامًا قانونيًا بنفس الخصائص المرتبطة بالإرادة المنفردة في إطار القانون المدني[٩٩].

**الاتجاه الثاني: القائل بان الموافقة الرقمية ذات طبيعة تعاقدية:**

يرى جانب من الفقه[١٠٠] أن موافقة صاحب البيانات تتسم بالطبيعة التعاقدية، وذهب إلى أنه، وإن كان من الممكن اعتبار الموافقة الرقمية تصرفًا صادرًا من جانب واحد، أي من جانب صاحب البيانات، فإن ذلك لا يعني تعارضها تمامًا مع أحكام العقد. فالتدقيق في طبيعتها يكشف أنها تمثل مرحلة من مراحل إبرام العقد[١٠١]، وهي مرحلة قبول الإيجاب أو عرض المعالجة الصادر عن المتحكم، وشروطه التي تتمثل

---

[٩٨]– جدير بالذكر أنه متى كان الواعد بجائزة قد حدد مدة اشتراط أن يتم العمل في خلالها، التزم نهائيًا بإرادته، ولم يكن له حق الرجوع في هذا الوعد. انظر: د. عبد الرزاق السنهوري: مرجع سابق، ف ٩١٤، ص ١١١١.

[99]- Yves POULLET, Concentement et RGPD: des zones d'ombre!, DCCR (Droit de la consomation consumentenrecht), 2019, no 122-123, p. 12.

[١٠٠]– في هذا الصدد انظر:

Y. POULLET, Concentement et RGPD: des zones d'ombre!, op. cit., p. 12 ets; Emmanuel NETTER, L'extinction du contrat et le sort des données personnelles, AJ Contrat (Actualité Juridique Contrat), Dalloz, no 10-Octobre 2019, p. 146; Suzanne VERGNOLLE, L'effectivité de la protection des personnes par le droit des données à caractère personne,, Thèse Université Paris II, 2020, p. 247 ets .

[١٠١]– يشير البعض إلى أن صاحب البيانات لا يتصرف "بمفرده" حال معالجة البيانات الشخصية، بل يعمل وفقًا لإطار يقترحه المتحكم ويوافق هذا الشخص على الالتزام به، ويحتل المتحكم مكانًا أساسيًا في تحديد شروط المعالجة التي قبلها الشخص. انظر:

S. VERGNOLLE, Thèse Précité, p. 249 .

(ISSN: 2537- 0758)

بشكل خاص في "سياسات الخصوصي (Politiques de confidentialité)"[١٠٢] التي يُعلَن الشخص المعني بها عبر الموقع[١٠٣].

وبمجرد تسجيل الشخص وقبوله لهذه الشروط، يحدث تلاقي الإرادتين، مما يجعل وجود العقد أمرًا لا شك فيه. وتنطوي الطبيعة التعاقدية للموافقة الرقمية على حق صاحب البيانات في مطالبة المتحكم بالامتثال لالتزاماته الواردة في سياسات الخصوصية للموقع، والتي تُعد جزءًا من نطاق التعاقد. كما يُمنح صاحب البيانات الحق، على وجه الخصوص، في الاعتراض على أي تعديل يُجريه المتحكم على هذه السياسات بصورة منفردة، دون الإخلال بحقه في التعويض، وإمكانية توقيع العقوبات الأخرى المنصوص عليها في اللائحة الأوروبية(GDPR)..

ويضيف بعض أنصار هذا الرأي[١٠٤] أن البحث في مدى توافر معايير الموافقة (الحرّة، والمحددة، والمستنيرة، والقاطعة) هو في جوهره بحث في سلوك الطرف المتعاقد. وفي الوقت نفسه، تنطبق نظرية عيوب الإرادة على هذا التصرف الانفرادي لصاحب البيانات (الموافقة) كما هو الحال في المسائل التعاقدية.

ويستند هذا الرأي إلى ما أشار إليه فريق عمل "المادة ٢٩" في الرأي رقم ٢٠١١/١٥ بشأن تعريف الموافقة (وفقًا لأحكام التوجيه الأوروبي ٩٥/٤٦ الملغي)،

---

[١٠٢]– تهدف سياسة الخصوصية (بالإنجليزية Privacy Policy) بمواقع وتطبيقات الإنترنت إلى إعلام المستخدم بكيفية استخدام ومشاركة بياناته الشخصية، بما يحافظ على خصوصيته، وغالبًا ما تعد زيارة المستخدم للموقع بمثابة رضاء أو موافقة على سياسة الخصوصية التي يحيل إليها الموقع من خلال رابط محدد، وتتضمن هذه السياسة نوعية المعلومات التي يتم جمعها وسبب جمعها، وكيفية استخدام تلك المعلومات.

[١٠٣]– في كثير من الأحيان يغلب على سياسات الخصوصية طابع الإذعان نظرًا لعدم قابليتها للتفاوض. فإما يتم قبولها برمتها من جانب صاحب البيانات أو يرفضها كلها، دون إمكانية التعديل بها؛ وهذا الأمر نجده واضحًا في عقود الإذعان بوجه عام والعقود مع المستهلكين. انظر:

Y. POULLET, op. cit., pp. 12- 13 .

[104]- Y. POULLET, op. cit., p. 12- 13 .

حيث أوضح أن الموافقة تُعد مفهومًا يُستخدم أيضًا في مجالات قانونية أخرى، وبخاصة قانون العقود. وأكد أنه لا يوجد تناقض بين نطاق القانون المدني ونطاق التوجيه الأوروبي، بل هناك تداخل بينهما.

فالتوجيه الأوروبي لا يتناول الشروط العامة لصحة الموافقة وفق القانون المدني، لكنه في الوقت ذاته لا يستبعدها. وهذا يعني، على سبيل المثال، أنه عند تقييم صحة عقد المعالجة بموجب أحكام هذا التوجيه (المادة ٧/ب)، ينبغي أيضًا مراعاة الشروط العامة لصحة الموافقة كما هو وارد في القانون المدني(١٠٥).

**وأخيرًا**، يشير هذا الرأي إلى تنوع الموافقة في إطار العقد نفسه، مما يستدعي ضرورة التمييز بين مختلف أنواع الموافقة داخل العقد، سواء كانت الموافقة العامة على العقد، أو الموافقة الخاصة التي تُمنح لكل غرض محدد لمعالجة البيانات. ويهدف هذا التمييز إلى تلبية المتطلبات القانونية للعقد أو المصالح المشروعة للمتحكم(١٠٦).

ويرى هذا الاتجاه أن هذا الفصل بين أنواع الموافقة داخل العقد يتسق مع أحكام اللائحة الأوروبية(GDPR)، دون أن يمس أو يتعارض مع قواعد القانون المدني. إذ يُراعى هذا التمييز توفير حماية أكبر لصاحب البيانات، وضمان امتثال المتحكم للالتزامات القانونية المتعلقة بمعالجة البيانات(١٠٧).

---

(105)- Groupe de travail "article 29", Avis 15/2011 sur la définition du consentement, op. cit., p. 7 .

(١٠٦)– هناك رأي في الفقه الفرنسي يقترح اعتبار الرضاء الرقمي بمثابة "عقد خاص لمعالجة البيانات الشخصية"، وذلك بحسب محل العقد؛ فإذا كان محله جمع البيانات وتحليلها واستخدامها، أي تمثل السمة الرئيسية في العقد في معالجة البيانات الشخصية، فيجب وصفه بأنه "عقد معالجة بيانات شخصية". أما إذا كان محل العقد جمع بيانات لأداء خدمة أخرى فيعتبر عقدًا عاديًا يخضع للقواعد العامة في العقود. في هذا الشأن. انظر:
S. VERGNOLLE, Thèse Précité, p. 255 et s

(107)- Y. POLLET, op. cit., p. 13 .

(ISSN: 2537- 0758)

وقد سار بعض الفقه في نفس الاتجاه المنادي بالطبيعة التعاقدية للموافقة الرقمية، حتى في حالة تعبير القاصر عن إرادته في التسجيل على مواقع التواصل الاجتماعي والموافقة على معالجة بياناته. حيث يشير إلى أن القاصر في هذه الحالة يعبر عن موافقته بالمعنى المقصود في قانون العقود(١٠٨).

ورغم وجاهة هذا الرأي، إلا أنه لا يمكن التسليم به على إطلاقه، لضعف حجته وخلطه بين مسائل قانونية متباينة. فالموافقة الرقمية في إطار معالجة البيانات، بحكم خصائصها، تختلف في العديد من الجوانب عن الموافقة التعاقدية. فهي، من جهة، تتميز بصدورها عن إرادة واحدة غالباً، ويتطلب توافر مجموعة من الخصائص أو العناصر المجتمعة فيها، ولا يغني وجود أحدها عن الآخر. ومن جهة أخرى، ترتبط بحق صاحب البيانات في تقرير مصير استخدام بياناته الشخصية والتحكم فيها(١٠٩)، سواء بالتعديل أو المحو، باعتبارها مسألة تدخل في نطاق حماية خصوصيته.

كما أن الموافقة الرقمية تتسم بعدم الاستقرار؛ إذ يمكن لصاحب البيانات العدول عن موافقته المبدئية على المعالجة في أي وقت(١١٠)، وبدون توقيع جزاء عليه، خلافًا للموافقة التعاقدية التي تتقلص فيها مساحة رخصة العدول. ولا يحد من ذلك ما تقضي به بعض النصوص القانونية من أنه يجوز أن ينص القانون أو العقد على مهلة للعدول، وهي المهلة التي يمكن لمن تقرر لمصلحته الرجوع عن موافقته قبل انقضائها (المادة ١١٢٢ من القانون المدني الفرنسي)، حيث لا يمكن ممارسة هذا

(108)- Benjamin CHARRIER, LE consentement exprimé pa les mineurs en ligne, Dalloz IP/IT, 6 juin 2018, p. 333; Célia SCAULTZ, La protection du mineur à l'aune des réseaux sociaux, Mémoire, Université de Grenoble Aples, 2020, p. 40. Disponible sur le site: https: //dumas. ccsd. cnrs. fr/dumas-02960116/ document .

(109)- N. MARTIAL_BRAZ, op. cit., p. 253 .

(١١٠)– انظر: م٢/٢ بند ٢ من قانون حماية البيانات الشخصية المصري: المادة ٧ من اللاحة الأوروبية لحماية البيانات GDPR.

الحق إلا بعد مهلة من التعبير عن موافقة أحد الطرفين، كما أن لهذه الرخصة طابعًا استثنائيًا(١١١).

وبهذا المعنى، فإن الموافقة على معالجة البيانات الشخصية تقترب بشكل كبير من الموافقة الصادرة في المسائل الطبية، حيث يزول في الغالب الطابع التعاقدي(١١٢).

كذلك يبدو واضحًا من خلال استقراء النصوص المنظمة للموافقة غياب الطابع التعاقدي للعلاقات في إطار البيانات الشخصية، إلا في حالة وجود عقد مُبرم بين المتحكم وصاحب البيانات، ينظم عملية معالجة البيانات ويحدد حقوق والتزامات الطرفين(١١٣).

---

(111)- F. ROGUE, Capacité et consentement au traitment de données à caractére personnel et au contrat, op. cit., p. 370 .

(112)- F. ROGUE, op. cit., p. 372 .

جدير بالذكر أن المشرع الفرنسي أشار إلأى أهمية الرضاء المسبق في العمل الطبي، في الفقرة الرابعة من المادة ١١١١-٤ من قانون الصحة العامة الفرنسي المعدلة بالمرسوم رقم ٢٣٢ لسنة ٢٠٢٠ المتعلق بنظام القرارات المتخذة في مسائل الصحة أو الرعاية أو الدعم الاجتماعي أو الطبي الاجتماعي فيما يتعلق بالبالغين محل الحماية القانونية، التي يجري نصها على أن: "لايمكن ممارسة أي عمل أو علاج طبي دون الرضاء الحر والمستنير من الشخص ويمكن العدول عن هذا الرضاء في أي وقت". ويجري النص الفرنسي لهذه المادة على النحو التالي:

"Aucun acte médical ni aucun traitment ne peut être pratiqué sans le consentement libre et éclairé de la personne et ce consentement peut être retire à tout moment ."

(١١٣)– لهذا يجب التفرقة بين الرضاء الذي ينعقد به عقد معالجة البيانات الشخصية، وبين اشتراط الحصول على رضاء صحيح لمعالجة البيانات، وفي هذه الحالة قد يقال أنه لا يوجد ما يحول دون توظيف رضاء صاحب البيانات من أجل الإقرار بوجود رابطة عقدية، ولو ضمنية بين صاحب البيانات والمتحكم، وهو ما قد يدعو إلى القول بترتيب الطابع العقدي للمسئولية في مجال البيانات الشخصية. انظر في شأن هذا الرأي في إطار الرضاء في العقد الطبي: د. عبد الكريم مأمون، حق الموافقة على الأعمال الطبية وجزاء الإخلال به، دار النهضة العربية، القاهرة، ٢٠٠٦، ص ٦٣.

(ISSN: 2537- 0758)

ويُستدل على ذلك من أن قوانين حماية البيانات تقرر أحكامًا خاصة للموافقة الرقمية تختلف، إلى حد كبير، عن أحكامها في القانون المدني. فتستلزم لهذه الموافقة شروطًا معينة، مثل أن تكون محددة، مستنيرة، وقاطعة، كما تجيز لصاحب البيانات سحبها أو العدول عنها بإرادته المنفردة. بالإضافة إلى ذلك، تحدد هذه القوانين سنًا أقل لبلوغ الأهلية اللازمة للموافقة على المعالجة (مثل ١٥ عامًا وفق القانون الفرنسي)، مما يبرز الطابع الخاص والمتميز للموافقة الرقمية.

وبناءً على ذلك، يجوز للشخص الذي بلغ السن المحددة قانونًا للموافقة على المعالجة أن يعبر عنها بمفرده، شريطة أن يكون لديه القدرة على التمييز والإدراك (أي بلغ السن المحددة متمتعًا بقواه العقلية). وعلى العكس من ذلك، فإن القاصر أو الشخص غير المؤهل قانونيًا لن يكون بإمكانه بمفرده التعبير عن الموافقة على إبرام عقد لمعالجة البيانات مع المتحكم، إلا إذا بلغ سن الرشد المقرر في القانون المدني، والذي يزيد في كافة الأحوال عن السن المقرر للموافقة على المعالجة في إطار قوانين حماية البيانات.

ولهذا، يشير جانب من الفقه إلى أن قانون العقود ليس له تأثير يُذكر على قانون حماية البيانات عندما يتعلق الأمر بالموافقة على المعالجة. وعلى العكس من ذلك، يهدف قانون حماية البيانات إلى التأثير على قانون العقود، لا سيما من خلال الشروط الإضافية التي يفرضها لضمان صحة التعبير عن الموافقة. ومن هذه الشروط أن تكون الموافقة حرة، مستنيرة، محددة، وقاطعة[١١٤]، وهي متطلبات تتجاوز ما قد يكون مطلوبًا في نطاق القانون المدني أو قانون العقود التقليدي. ويعكس هذا التوجه الرغبة في توفير حماية أكبر لصاحب البيانات، وضمان أن تتم المعالجة بطريقة تتماشى مع القواعد الصارمة المنصوص عليها في قوانين حماية البيانات، مثل اللائحة الأوروبية العامة لحماية البيانات(GDPR)..

(114)- Anne DEBET, La protection des données personnelles, point de vue du droit privé. Revue du droit public, no. 1, 2016, p. 17; F. ROGUE, op. cit., p. 373

ولا يفوتنا في هذا الإطار التنويه إلى محاولة بعض أنصار الاتجاه المنادي بالطبيعة التعاقدية للموافقة الرقمية التخفيف من حدة الانتقادات الموجهة إليه. إذ يشير هؤلاء إلى أن الطابع الانفرادي للعدول عن الموافقة الرقمية لا يتعارض مع الطبيعة التعاقدية لهذه الموافقة، وذلك تأسيسًا على أن هناك تشريعات أخرى تنص على الحق في العدول لأغراض حماية الطرف الضعيف، مثل أحكام حماية المستهلك.

ويُبرز هذا الاتجاه أن الحاجة إلى حماية الطرف الضعيف، أيًا كانت صفته– في هذه الحالة، صاحب البيانات– تعزز فكرة الحق في العدول عن العقد المتعلق بمعالجة البيانات باعتباره مسألة تتعلق بالنظام العام. وبالتالي، فإن هذا الحق يُقرّ دون الحاجة إلى اللجوء إلى فكرة التصرف الانفرادي، الذي يُجيز العدول عنه بالإرادة المنفردة. وبهذا المعنى، يصبح العدول عن الموافقة الرقمية جزءًا من الإطار التعاقدي الذي يتسم بمرونة خاصة تهدف إلى تحقيق التوازن بين حقوق الأطراف والتزاماتهم[١١٥].

ويرى البعض من الفقه[١١٦] إن هذا الرأي غير سليم، حيث يستند بصفة أساسية إلى التسليم بالطبيعة التعاقدية للموافقة الرقمية، والتي تُعبّر في الفضاء الإلكتروني وعن بعد، متجاهلًا وجود اختلافات جوهرية بين العدول عن الموافقة والرجوع في العقد، وهي اختلافات تنطق بها الأحكام القانونية المنظمة لكل منهما.

فالرجوع في العقد يجب أن يتم خلال مهلة معينة تلي إبرامه، وفق ضوابط محددة تهدف إلى تحقيق توازن بين عدم الإضرار بمصالح الطرف الآخر من جهة، وضمان استقرار العلاقات التعاقدية من جهة أخرى. كما أن هذا الرجوع ينصب على حالات خاصة فقط، ولا يشمل كافة العقود المبرمة بين المهنيين والمستهلكين، بل يقتصر على بعض صور التعاقد التي قدّر المشرّع فيها أهمية منح المستهلك هذا الحق[١١٧].

---

(115)- Y. POULLET, op. cit., pp. 13-14 .

(١١٦)– د. تامر الدمياطى، المرجع السابق، ص ٣٦ وما بعدها.

(١١٧)– لمزيد من التفصيل في شأن الحق في الرجوع في إطار العقد. انظر: د. منى أبو بكر الصديق محمد حسان، الحق في الرجوع في العقد كإحدى الآليات القانونية لحماية المستهلك في

(ISSN: 2537- 0758)

أما العدول عن الموافقة، فإنه يتم في أي وقت، ودون حاجة إلى إبداء أسباب، مما يُبرز خصوصيته ويميزه بوضوح عن الرجوع في العقد. بالإضافة إلى ذلك، كان المشرع، سواء الأوروبي أو المصري، او الاماراتى صريحًا في النص على العدول عن الموافقة، وليس العدول عن العقد. ولو كان الأمر يتعلق بتلاقي الإرادتين، حيث تُعتبر موافقة صاحب البيانات قبولًا لعرض أو إيجاب المتحكم لمعالجة البيانات (كما يرى الرأي السابق)، لكان من الأنسب للمشرّع أن يشير إلى ذلك. ولكن المشرّع لم يفعل، مما يدل على أن العدول يتعلق بتعبير فردي سبق أن أذن به الشخص بمعالجة بياناته، وليس بعلاقة تعاقدية– فى الغلب– تستلزم حماية توازن المصالح بين الطرفين.

**الاتجاه الثالث**: **القائل بان الموافقة هى مجرد إذن أو رخصة بمعالجة البيانات**:

يتجه جانب من الفقه إلى القول بان الموافقة على المعالجة الرقمية للبيانات الشخصية هى مجرد إذن أو رخصة، حيث أن التعامل على الحقوق اللصيقة بالشخصية، ومن بينها البيانات الشخصية، لا يُعد تصرفًا بالمعنى القانوني لنظرية الالتزام، وإنما يتم عن طريق الموافقة، وهي عمل انفرادي يصدر عن الشخص، يجعل التعامل على البيانات مشروعًا. ويُستدل على ذلك بغياب وجود أي اتفاق أو عقد، أو حتى تصرف قانوني بالإرادة المنفردة، يترتب عليه التزام قانوني على من صدر منه، مما يُفسح المجال للشخص للعدول عن موافقته بمحض إرادته[١١٨].

---

مجال التعاقد عن بعد، دراسة تحليلية في ضوء القانون الفرنسي والتوجيهات الأوروبية، مجلة البحوث القانونية والاقتصادية، كلية الحقوق، جامعة المنصورة، العدد ٦٥، أبريل ٢٠١٨، ص ٧٩٨ وما بعدها.

[١١٨]– في هذا المعنى، انظر: حسام الدين كامل، الأهواني، المدخل للعلوم القانونية، الجزء الثاني نظرية الحق، بدون دار نشر، الطبعة الثالثة، ١٩٩٧، ص ٥٧.

وبناءً على ذلك، لا تُعتبر موافقة صاحب البيانات على المعالجة من قبيل الموافقة التعاقدية أو التصرف بالإرادة المنفردة؛ إذ لا يتضمن هذا الإجراء تصرفًا مُلزمًا يخضع لأحكام الالتزام في القانون المدني. فالموافقة، في هذا السياق، لا تتعلق بحق مالي قابل للتعامل، وإنما هي تعبير عن إرادة الشخص، يَصدر منه ليُجيز معالجة بياناته الشخصية. وبهذا الشكل، تُعد الموافقة من قبيل الإذن أو الإجازة المرتبطة بحق من الحقوق اللصيقة بالشخصية[١١٩].

ومن هنا، يمكن القول إن الموافقة في حالة البيانات الشخصية تتشابه مع الموافقة في حالة التجارب الطبية والعلمية[١٢٠]، إذ إنها لا تُعد تصرفًا قانونيًا مُلزمًا، بل هي مسلك إرادي له آثاره القانونية. وتُعد هذه الموافقة مظهرًا للحق في الحرية، ومباشرة لنشاط مشروع يكتفي فيه الشخص بتعبير إرادته بوضوح، شريطة أن يكون مدركًا ومميزًا[١٢١].

---

[١١٩]– قريب من ذلك، انظر: فتوى الجمعية العمومية لقسمي الفتوى والتشريع بمجلس الدولة رقم ٦٥٨، بتاريخ ١٩٩٥/٩/٦ في شأن شروعية نقل وزراعة الأعضاء البشرية، أشار إليه: د. حسام الدين كامل الأهواني، المرجع السابق، ص ٥٧. و قارب فى ذلك التهامي، سامح. (٢٠١١). الحماية القانونية للبيانات الشخصية– دراسة في القانون الفرنسي، مرجع سابق، ص٢٤٧ وما بعدها.

[١٢٠]–حيث ينحصر مفهوم الإذن أو التفويض أو الموافقة على التدخل الطبي في مبدأ الموافقة المستنيرة، وهو متطلب قانوني وضرورة أخلاقية. إنه يعمل على حماية المرضى وتعزيز الاستقلالية وإقامة علاقة الثقة بين المرضى ومقدمي الرعاية الصحية. وتؤكد التبعات القانونية للموافقة المستنيرة على أهميتها في الممارسة الطبية، وتسلط الضوء على ضرورة التواصل الواضح والتوثيق الشامل للتخفيف من المخاطر القانونية المحتملة. انظر:

Paterick, T., Carson, G., Allen, M., & Paterick, T. (2008). Medical informed consent: general considerations for physicians. Mayo Clinic Proceedings, 83(3), 313-319. https: //doi. org/10. 4065/83. 3. 313

Fitriana, D. (2023). The role of informed consent as legal protection for doctors in conducting medical procedures. law, 1(3), 235-245. https: //doi. org/10. 61194/law. v1i3. 101

[١٢١]– انظر: د. محمد عيد الغريب، مرجع سابق، ص ٨٧.

(ISSN: 2537- 0758)

## رابعاً- الرأى الراجح لدينا فى بيان الطبيعة القانونية للموافقة على المعالجة الرقمية للبيانات:

الواقع أن الموافقة الرقمية هي نوع خاص من الموافقة، تختلف عن الموافقة التعاقدية وكذلك عن التصرف بالإرادة المنفردة كمصدر للالتزام. ويتضح هذا الأمر جليًا من النصوص القانونية المنظمة لحماية البيانات، التي تضفي على الموافقة الرقمية طابعًا غير ملزم. حيث تجيز هذه النصوص إجراء المعالجة دون الحصول على الموافقة في الأحوال المصرح بها قانونًا. مع انها تخضع لاحكام القواعد العامة فى نظرية الالتزام من احكام العقد و الارادة المنفردة فيما ما لا يوجد بشانه حكم خاص.

كما تشير هذه النصوص إلى أن الموافقة تُعد أساسًا مستقلًا لشرعية عمليات المعالجة، وتضع العقد أساسًا آخر يليه في الترتيب[١٢٢]. ولتوضيح هذا الفارق، يُميز مجلس حماية البيانات الأوروبي بين الموافقة والعقد باعتبارهما أساسين متميزين لمعالجة البيانات الشخصية، ويُشير بوضوح إلى أنه لا يجوز اتحادهما أو دمجهما (fusionnées et amalgamées) عند تبرير المعالجة[١٢٣].

---

Baldemir, R. (2023). An overview of the concept of medical intervention and informed consent according to turkish law. Journal of Pulmonology and Intensive Care, 1(2), 42-45. https: //doi. org/10. 51271/jopic-0010

[١٢٢]– راجع المادة (١/٦) من اللائحة الأوروبية لحماية البيانات (GDPR)، البندين ١، ٢: المادة (٦) من قانون حماية البيانات الشخصية المصري، البندين ١، ٢، وكذلك فى القانون الاماراتى.

[123]- CEPD, Lignes directrices 5/2020, sur le consentement, op. cit., no 26, p. 11 .

وفي هذا الصدد، رفضت اللجنة الوطنية للمعلوماتية والحريات الفرنسية استناد متجر FNAC في معالجة بيانات العملاء إلى أساس الضرورة التعاقدية والمصلحة المشروعة بدلاً من الحصول على رضاء محدد من المستخدم بيام الشركة بالتسجيل بشكل افتراضي لبيانات البطاقات المصرفية لعملائها الخاصة بالمعاملات الآجلة.

إضافة إلى ذلك، تُحدد التشريعات المعنية سنًا معينة للموافقة الرقمية، تُعرف بسن الرشد الرقمي، وهو أقل من سن الرشد المقرر في القانون المدني. كما يرتب المشرع جزاءات جنائية على إجراء المعالجة في غير الأحوال المصرح بها قانونًا أو دون الحصول على موافقة صاحب البيانات (متى كانت الموافقة لازمة)، وقد تصل العقوبة في بعض الحالات إلى الحبس، فضلًا عن فرض غرامات مالية[١٢٤].

والملاحظ أن المشرع لا يكتفي بترتيب الجزاء المدني، مثل البطلان، مما يشير إلى رغبة واضحة في استقلالية الموافقة الرقمية عن الموافقة العقدية. هذا التوجه يعكس الأهمية البالغة التي يوليها المشرع لحماية البيانات الشخصية بوصفها حقًا لصيقًا بالشخصية، ويتطلب نظامًا قانونيًا خاصًا يتماشى مع طبيعة هذه الحقوق.

ولهذا يمكن وصف الموافقة الرقمية بأنها تصرف صادر عن إرادة منفردة، أي من جانب واحد، لكنها تنتمي إلى نوع التصرفات الانفرادية التي لا تُنشئ التزامًا قانونيًا

---

CNIL, Délibération no 20/2-214 du 19 juillet 2012 portant avertissement à l'econtre de la société FNAC. Disponible sur le site: https: //www. legifrance. gouv. /cnil/id/CNIL TEXT000026224040/

[١٢٤]– تحدد المادة (٣٦) فقرة أولى من قانون حماية البيانات الشخصية المصري، هذه الغرامة بألا تقل عن مائة ألف جنيه ولا تجاوز مليون جنيه، وتضيف الفقرة الثانية منها أن تكون العقوبة الحبس مدة لا تقل عن ستة شهور وغرامة لا تقل عن مائتي ألف جنيه ولا تجاوز مليوني جنيه، أو بإحدى هاتين العقوبتين، إذا ارتكب ذلك مقابل الحصول على منفعة مادة أو أدبية، أو بقصد تعريض الشخص المعني بالبيانات للخطر أو الضرر، وتعاقب المادة ٣٧ من القانون بغرامة لا تقل عن مائة ألف جنيه ولا تجاوز مليون جنيه كل من امتنع دون مقتض من القانون عن تمكين الشخص المعني بالبيانات من ممارسة حقوقه المنصوص عليها في المادة (٢) من هذا القانون كذلك تقرر المادة (٨٣) من اللائحة الأوروبية عقوبات مالية شديدة تصل إلى ٢٠ مليون جنيه أو ٤% من حجم أعمال الشركة على مستوى العالم (ف٥). وانظر أيضًا المادة (٢٠) من قانون المعلوماتية والحريات الفرنسي المعدل.

(ISSN: 2537- 0758)

بالمعنى التقليدي[١٢٥]. فهي تصدر عن الشخص المعني وحده حسب الغالب، مع احتفاظه بالحق في العدول عنها في أي وقت. كما انها ليست بالعقد غير اللازم فى الفقه الاسلامى وقانون المعاملات المدنية الاماراتى[١٢٦]، وهذا يجعلها أقرب إلى الإذن أو الرخصة التي تُخوّل للمتحكم إجراء المعالجة. وتترتب على هذه الموافقة آثار قانونية متنوعة، باعتبارها تصرفًا بالإرادة المنفردة لصاحب البيانات. و من بين هذه الآثار، ترتيب مشروعية المعالجة، و ذلك عندما تكون الموافقة شرطًا ضروريًا لإجراء المعالجة. ورفع الحظر عن المعالجة، كما هو في حالات معالجة البيانات الحساسة، مثل البيانات المالية أو الجينية أو بيانات الأطفال، والتي تتطلب موافقة واضحة وصريحة[١٢٧].

ولا شك أن هذه الآثار القانونية تُنظم من خلال التشريعات المعنية بحماية البيانات، التي تُحدد الأحكام الخاصة بالموافقة ومعاييرها وشروطها. وبتعبير صاحب البيانات عن موافقته، يسعى إلى تحقيق هذه الآثار القانونية التي تُصبح نافذة من لحظة صدور التعبير عن الإرادة، بشرط أن تتوافر فيه كافة المعايير والشروط

---

[١٢٥]– راجع المادة (١) من قانونى حماية البيانات الشخصية المصري، و الاماراتى الفقرة الخاصة بتعريف البيانات الشخصية الحساسة. وراجع أيضًا المادة (٤) من اللائحة الأوروبية (البنود من ١٣– ١٥). د. تامر الدمياطى، المرجع السابق، ص ٣٧ وما بعدها.

[١٢٦]–انظر فى العقد غير الازم و تطبيقاته حديثا، الدهماني، م. (٢٠٢٤). آثار العقد الفاسد وَفْقًا لقانون المعاملات المدنية الإماراتي "دراسة على ضوءٍ من أحكام الفقه الإسلامي". مجلة جامعة الشارقة للعلوم القانونية،٢١(١). https: //doi. org/10. 36394/jls. v21. i1. 4، ناظم، ص. (٢٠٢٤). الغاء العقد بالإرادة المنفرد. مندق، ١.https: //doi. org/10. 69513/jnfls v1. i2. a9

[١٢٧]– راجع في شأن التصرف بالإرادة المنفردة بوجه عام د. عبد الفتاح عبد الباقي، مرجع سابق، ص ٢٩١ وما بعدها؛ د. عبد الرزاق السنهوري، مرجع سابق، ف ٩٠٦، ص ١٠٩٥ وما بعدها.

اللازمة لصحته وسلامته وفق القواعد الخاصة وإلا طبقت القواعد العامة متى انتفى النص الخاص.

وبهذا المعنى، تحتل الموافقة الرقمية موقعًا فريدًا بين التصرفات القانونية، حيث تجمع بين خصائص التصرفات الانفرادية والإذن القانوني، مع خضوعها لنظام قانوني مستقل يعكس خصوصية التعامل مع البيانات الشخصية، وتخضع استثناءً للقواعد العامة وبما يتماشى وطبيبعتها متى انتفلا الحكم الخاص.

وبمناسبة ما تقدم يرى البعض من الفقه[١٢٨]، انه تأسيسًا على ما تقدم، يبدو في تقديره أن المشرع المصري قد جانبه الصواب عند استخدامه لفظ "الموافقة "للإشارة إلى تعبير صاحب البيانات عن إرادته في التعامل مع بياناته الشخصية.

ويدلل على صحة رأيه بأن دلالة كلمة "الموافقة" توحي بوجود إيجاب صادر عن القائمين على عمليات جمع البيانات أو معالجتها أو الإفصاح عنها، يتطلب اقترانه بقبول من صاحب البيانات. وهذا الفهم يجعل الموافقة تبدو مشابهة للقبول كأحد عناصر التعبير عن الإرادة في إطار العقد، وهو تصور يتعارض مع رفضه للطبيعة التعاقدية لهذا النوع من الموافقة.

كما يدعم رايه بالقول كذلك بان الطبيعة الخاصة للموافقة الرقمية، كما أوضحنا سابقاً، تنأى بها عن المفاهيم التقليدية للعقد، حيث إنها تصرف انفرادي صادر عن صاحب البيانات، يُرتب آثارًا قانونية دون الحاجة إلى تلاقي الإرادتين. ولذلك، فإن استخدام مصطلح أدق وأكثر تعبيرًا عن هذه الطبيعة، مثل "الإذن "أو "الإجازة"، كان سيُعبر بشكل أكثر دقة عن حقيقة هذا التصرف، ويُجنب أي لبس أو خلط مع المفاهيم التعاقدية التقليدية.

وبالتالي، فإن إعادة النظر في صياغة التشريعات بما يعكس الطبيعة الانفرادية والفريدة لهذه الموافقة بات أمرًا ضروريًا لضمان الوضوح التشريعي والتماسك بين القواعد القانونية المنظمة لحماية البيانات.

---

[١٢٨]– د. تامر الدمياطى، المرجع السابق، ص ٤١.

(ISSN: 2537- 0758)

في تقديري، لا يتمتع الرأي المذكور سابقًا بتأثير فقهي أو قضائي يُعتد به، كما أنه لا يرقى إلى التأثير على جوهر الفكرة أو الواقع العملي. فمصطلح "الموافقة" يُعد معادلًا لمصطلح "الرضا" طالما أن كليهما يؤدي ذات الوظيفة، وهي إجازة أو إباحة عملية المعالجة في سياق نظام قانوني خاص يضع لهما دلالة تختلف عن تلك المعتمدة في النظرية العامة. ويتجلى هذا بوضوح في قانون حماية البيانات الشخصية، حيث يُعد مصطلح "الموافقة" هو الأكثر تداولًا واعتمادًا في مختلف قوانين حماية البيانات حول العالم.

ومن هذا المنطلق، اختار المشرع في كل من مصر والإمارات العربية المتحدة استخدام مصطلح "الموافقة" ليتسق مع الاتجاه التشريعي العالمي. ويُفهم هذا المصطلح ضمن إطار قانون حماية البيانات بأنه يشمل كافة صور الرضاء بالمعالجة، سواء أكانت بناءً على إرادة منفردة من صاحب البيانات، كما هو الحال في التصرفات الفردية وفقًا لمفهوم قانون حماية البيانات، أو بناءً على إرادة مشتركة بين صاحب البيانات والمتحكم أو المعالج، وهو ما يُعد عقدًا ذا طبيعة خاصة تتناسب مع قانون حماية البيانات الشخصية، بعيدًا عن المفهوم التقليدي للعقد في النظرية العامة وان كان من المتصور ان تعبر الموافقة على معالجة البيانات فى بعض الاحيان عن عقداً وفق المعنى التقليدى فى نظرية العقد. ولهذه الأسباب، تم اعتماد مصطلح "الموافقة" بدلاً من "الرضا"، وهو ما انعكس جليًا في عنوان هذا البحث.

## المبحث الثانى
## مقومات الموافقة

**تمهيد وتقسيم**:

في ظل التطورات التكنولوجية المتسارعة التي يشهدها العالم الرقمي، باتت مسألة حماية البيانات الشخصية تحتل مكانة بارزة في الأنظمة القانونية. وتعد الموافقة على المعالجة الرقمية للبيانات الشخصية إحدى الركائز الأساسية لتحقيق التوازن بين استخدام التكنولوجيا الحديثة واحترام حقوق الأفراد، مما يفرض على القطاع القانونى فرض الأحكام القانونية المنظمة لهذه الموافقة من حيث اليات التعبير عنها، وشروطها، والضوابط اللازمة لصحتها بما يوفر حد ادنى من المقومات اللازمة لتوافر موافقة صحيحة لمعالجة البيانات الشخصية باعتبارها أداة قانونية تهدف إلى حماية الحقوق الفردية في مواجهة التحديات التقنية المتزايدة.

وعلى ذلك فإنه يلزم قانوناً حتى تتحقق الموافقة على أي جمع أو معالجة أو استخدام للبيانات الشخصية، أن يقوم صاحب البيانات بالتعبير عن إرادته، أي إخراجها من الحيز النفسي الداخلي إلى النطاق القانوني الخارجي. كما يجب أن يكون هذا التعبير سليمًا من الناحية القانونية، بحيث تتوافر فيه شروط وخصائص محددة، وأن يصدر عن صاحب البيانات نفسه أو من يمثله قانونًا. ومن جهة أخرى، يشترط أن يتم هذا التعبير وفق الشكل الذي تقرره القواعد القانونية المنظمة لحماية البيانات. ويترتب على عدم توافر الشروط اللازمة للموافقة اعتبارها غير موجودة، مما يؤدي إلى بطلان عملية المعالجة ذاتها، ويجعلها وكأنها صادرة دون موافقة من صاحب البيانات.

وعلى ذلك ندرس فى هذا المبحث القواعد الحاكمة للمقومات اللازمة لمنح أو توافر موافقة قانونية صحيحة لمعالجة البيانات الشخصية **من خلال التقسيم الاتى:**

**المطلب الاول:** شروط التعبير عن الارادة بالموافقة.

**المطلب الثانى:** شكل التعبير عن الارادة بالموافقة.

**المطلب الثالث:** اهلية التعبير للارادة بالموافقة.

(ISSN: 2537- 0758)

## المطلب الاول

## شروط التعبير عن الارادة بالموافقة

**تمهيد وتقسيم**:

تُعد موافقة صاحب البيانات شرطًا أساسيًا لمشروعية كافة العمليات التي تُجرى على البيانات الشخصية، سواء جمعها أو معالجتها أو الإفصاح عنها أو إفشائها، وذلك ما لم يصرح القانون بخلاف ذلك. وفي هذا السياق، يتعين أن تتوافر في هذه الموافقة مجموعة من الشروط اللازمة لوجودها وصحتها من الناحية القانونية. وتتمثل هذه الشروط، وفقًا لما نصت عليه المادة (١١/٤) من اللائحة الأوروبية العامة لحماية البيانات(GDPR)، في أن يكون التعبير عن الإرادة الصادر من صاحب البيانات: حرًا، أي أن يصدر عن إرادة حرة دون ضغط أو إكراه. ومستنيرًا، بمعنى أن يكون صاحب البيانات على دراية كاملة بأغراض المعالجة وطبيعتها. ومحددًا، بحيث يتصل بنطاق معين ومعروف بوضوح، ولا يكون عامًا أو غير محدد. وقاطعًا، أي أن يكون التعبير عن الإرادة واضحًا وصريحًا وغير قابل للتأويل. وكذلك يتطلب توافر هذه الشروط فى الموافقة وفق القانونين المصرى والاماراتى. ويُشترط أن تتوافر هذه الشروط مجتمعة، وإلا عُدت الموافقة باطلة وغير ذات أثر قانوني. ويقع المتحكم أو المعالج– اذا ما خالف احكام الشروط المطلوبة– تحت طائلة العقوبات الجنائية المنصوص عليها في التشريعات الخاصة بحماية البيانات. وغالبًا ما تكون هذه العقوبات مالية وقاسية، وتهدف إلى ردع المخالفين وضمان الامتثال لأحكام القانون[١٢٩]. وعلى ذلك نبحث احكام شروط التعبير عن الارادة بالموافقة من خلال الفروع الاتية:

**الفرع الاول:** التعبير عن الارادة الحرة بالموافقة.

---

[١٢٩]– المادتان (٣٦، ٣٧) من قانون حماية البيانات المصري، والمادة رقم ٢٦ من القانون الاماراتى، والمادة (٨٣) من اللائحة الأوروبية وخاصة الفقرتين (٤، ٥) والمادة (٢٠) من قانون المعلوماتية والحريات الفرنسي المعدل سالف الإشارة إليه.

**الفرع الثانى:** التعبير عن الارادة المستنيرة بالموافقة.

**الفرع الثالث:** التعبير عن الارادة المحددة بالموافقة.

**الفرع الرابع:** التعبير عن الارادة القاطعة بالموافقة.

## الفرع الاول

## التعبير عن الارادة الحرة بالموافقة

يتطلب لصحة موافقة الشخص– بوجه عام– أن تكون هذه الموافقة حرّة (libre)، أي أن تصدر عن إرادة سليمة وخالية من أي عيب من عيوب الإرادة. فلا يُعتد بالموافقة الصادرة إذا كانت إرادة الشخص معيبة بسبب الغلط، أو الإكراه، أو أي سبب آخر يؤدي إلى انتقاص حرية الاختيار أو انعدامها تمامًا.

وبالتالي، تُعد الارادة الحرة ركنًا أساسيًا لصحة الموافقة، حيث يجب أن تُعبر عن إرادة مستقلة وغير متأثرة بضغوط خارجية أو ظروف تجعل الشخص مضطرًا لقبول ما لا يريده فعليًا. فإذا ثبت وجود أي من هذه العيوب، فإن الموافقة تُعتبر باطلة ولا تنتج أي أثر قانوني.

وهذا المفهوم يُطبق بوجه خاص في إطار حماية البيانات الشخصية، لضمان أن تكون موافقة صاحب البيانات معبرة عن إرادته الحقيقية وغير متأثرة بأي عوامل تجعلها غير سليمة.

وتأخذ هذه المسألة أهمية بالغة في إطار حماية البيانات الشخصية، حيث تشترط اللائحة الأوروبية العامة لحماية البيانات (GDPR) لصحة موافقة صاحب البيانات أن يكون التعبير عن إرادته حرًا[١٣٠]. ويُقصد بذلك أن تكون الموافقة نابعة عن تفكير وتروٍ، مع توفير حرية حقيقية للشخص للاختيار بين الموافقة على المعالجة أو رفضها، أو حتى سحبها بعد صدورها، دون أن يتعرض لأي ضرر نتيجة رفضه أو سحبه للموافقة.

(130)- Groupe de travail "article 29", Avis 15/2011 sur la définition du consentement, op. cit., p. 14 .

(ISSN: 2537- 0758)

على سبيل المثال، يجب ألا يتعرض صاحب البيانات لأي ضرر مادي أو معنوي في حال رفضه أو سحب موافقته، كأن يتم تحميله بأعباء مالية أو تكلفة لا تتناسب مع الخدمة المقدمة، أو تقليل جودة الخدمة كوسيلة ضغط عليه للقبول بالمعالجة(١٣١).

علاوة على ذلك، تشدد اللائحة على ضرورة حماية صاحب البيانات من أي مخاطر قد تؤثر على حريته في التعبير عن الموافقة، مثل الخداع، أو الترهيب، أو الإكراه، أو الآثار السلبية الكبيرة في الممارسة العملية. لذا، يجب أن يتم الحصول على الموافقة في ظروف تضمن استقلالية الإرادة بشكل كامل، لضمان أن تكون المعالجة مشروعة ومستندة إلى موافقة صادقة وغير معيبة(١٣٢).

وتفسيرًا لذلك، أوضحت مجموعة عمل المادة "٢٩" أن "الموافقة الحرة" تعني قرارًا إراديًا (decision volontaire) يصدر عن شخص يتمتع بكامل قواه العقلية، دون أي تأثير أو ضغط خارجي. وتشمل هذه الضغوط أشكالًا متعددة مثل الإكراه الاجتماعي، أو المادي، أو النفسي، أو غيرها.

وأضافت المجموعة أن الموافقة لا يمكن اعتبارها حرّة إذا صدرت تحت تهديد صريح أو ضمني، مثل الحرمان من الخدمة، أو تقديم المعالجة بجودة أقل كوسيلة لإجبار الشخص على القبول(١٣٣).

هذا التفسير يعزز مفهوم أن الحرية في التعبير عن الإرادة يجب أن تكون مطلقة وغير مشروطة بأي ظروف أو ممارسات قد تؤثر على استقلالية القرار. ويُعد ذلك

(131)- Y. POULLET, Consentement et RGPD: des zones d' ombre!, op. cit., p.6 .

(132)- Groupe de travail "article 29",. Avis 15/2011 sur la définition du consentement, op. cit., p. 14 et s .

(133)- Groupe de travail "article 29", Document de travail du le trautement des données à caractére personnel relatives à la santé continues dans les dossiers médicaux électronique (DME), WP 131, Adopté le 15 février 2007, p. 9. Sur le site: https: //www. apda. ad/site/frfault/files/2018-10/wp131_fr. pdf

من المبادئ الأساسية التي تستند إليها التشريعات المعنية بحماية البيانات لضمان أن تكون المعالجة قائمة على موافقة حقيقية وصادقة من صاحب البيانات.

ومن ثم، لا يُعتبر الموافقة الحرة متوافرة إذا مارس المتحكم أي نوع من الضغط، أو الترهيب، أو التأثير على صاحب البيانات دون وجود مبرر مشروع. إذ يُعد ذلك تصرفًا يحدّ من قدرة صاحب البيانات أو يمنعه من التعبير عن إرادته بشكل مستقل (وفقًا للحيثيتين ٤٢ و٤٣ من اللائحة الأوروبية العامة لحماية البيانات). كما أن الموافقة لا تكون حرة إذا كان صاحب البيانات غير قادر على رفضها أو العدول عنها دون أن يترتب على ذلك ضرر مادي أو معنوي[١٣٤].

ووفقًا للمادة (٧) الفقرة (٤) من اللائحة الأوروبية[١٣٥]، لا يُعد التعبير عن الموافقة حرًا إذا تم تعليق تنفيذ العقد أو تقديم الخدمة على شرط الموافقة على معالجة

---

[١٣٤]– على سبيل المثال، قد يشترط تطبيق تحرير الصور على الهاتف المحمول لاستخدام خدماته ضرورة قيام مستخدميه بتنشيط موقعه الجغرافي على النظام العالمي لتحديد المواقع GPS ويخبر التطبيق مستخدميه أيضًا أنه سيستخدم البيانات التي تم جمعها لأغراض الدعاية، بيد أن تحديد الموقع الجغرافي أو الإعلان عبر الإنترنت لا يعد ضروريًا لتوفير خدمات تحرير الصور، وبالتالي يتجاوز كلاهما توفير الخدمة الأساسية المقترحة. ونظرًا لأن المستخدمين لا يمكنهم استخدام التطبيق دون الموافقة على هذه الأغراض، فلا يمكن اعتبار الرضاء حرًا في هذه الحالة. راجع:

Lignes directrices 5/2020 sur le consentement au sens du règlement (UE) 2016/679, op. cit., no 15, pp. 8-9 .

[١٣٥]– تتعلق المادة (٧) من اللائحة الأوروبية بشروط تطبيق الرضاء، وتنص فقرتها الرابعة على أن "عند تحديد ما إذا كان الرضاء الصادر من صاحب البيانات حرًا، ينبغي إيلاء أقصى قدر من الاعتبار لعدة أمور منها على وجه الخصوص حالة تعليق تنفيذ العقد أو تقديم الخدمة على طلب الحصول على الرضاء بمعالجة البيانات الشخصية غير الضرورية لتنفيذ العقد أو الخدمة المعنية. وتتناول هذه الفقرة حالة إدماج الرضاء في عقد أو ارتباطه بتقديم خدمة، وقد صيغت عبارات هذه الفقرة بطريقة واسعة ومرنة، حيث استخدمت عبارة ينبغى إيلاء أقصى قدر من الاعتبار لـ "عدة أمور entreautres". مما يعنى أن الحالة الواردة فيها (تنفيذ عقد أو تقديم خدمة) جاءت على سبيل المثال، ومن ثم يمكن أن يسرى حكمها على حالات أخرى، راجع:

(ISSN: 2537- 0758)

البيانات الشخصية غير الضرورية لتنفيذ هذا العقد[١٣٦] أو تقديم الخدمة المعنية. هذا النص يعكس حرص المشرع الأوروبي على منع أي استغلال للموافقة كوسيلة ضغط للحصول على مزايا إضافية للمتحكم، وضمان أن تكون المعالجة مقصورة فقط على البيانات اللازمة لتحقيق الغرض المشروع المتفق عليه.

كما يشترط مجلس حماية البيانات الأوروبي[١٣٧] للحصول على الموافقة الحرة من مستخدم الإنترنت، أن يكون استخدام الخدمات أو الميزات التي يوفرها الموقع غير مشروط بموافقة المستخدم على تخزين المعلومات أو الوصول إلى المعلومات المخزنة على جهازه.

---

Lignes directrices 5/2020 sur le consentement au sens du réglement (UE) 2016/679, op. cit., no 14, p. 8 .

[١٣٦]– وفقًا للرأي رقم ٢٠١٤/٦ الصادر عن فريق عمل المادة (٢٩)، ينبغي تفسير عبارة "ضرورى لتنفيذ العقد" نفسيرًا ضيقًا.

Groupe de travail "article 29", Avis 06/2014 sur le notion d'intérêt légitime poursuivi par le responsible du traitement des données au sens de l'article 7 de la directive 95/46/CE, 9 avril 2014, pp. 18-19 .

كما يلزم أن تكون المعالجة ضرورية لتنفيذ العقد المبرم مع صاحب البيانات، وقد يشمل ذلك، على سبيل المثال، معالجة عنوان صاحب البيانات بحيث يمكن معالجة بيانات بطاقة الائتمان الخاصة به لتمكين الوفاء عبر الإنترنت، وفي نطاق علاقات العمل قد يسمح هذا المبدأ على سبيل المثال بمعالجة البيانات المتعلقة بالأجور والحساب المصرفي من أجل دفع الاجور، ومن ثم يجب أن يكون هناك ارتباط مباشر وموضوعي بين معالجة البيانات والغرض من تنفيذ العقد، أما إذا كان المتحكم يسعى إلى معالجة البيانات الضرورية بالفعل لتنفيذ العقد، فإن الرضاء لا يعتبر هو الساس القانوني المناسب للمعالجة (حيث تستند المعالجة في هذه الحالة للمادة ٦/١ب من اللائحة الأوروبية.

Lignes directrices 5/2020 sur le consentement au sens du règlement (UE) 2016/679, op. cit., no 30-31, p. 12 .

[137]- Lignes directrices 5/2020, op. cit., p. 13.

وينطبق هذا بشكل خاص على ملفات تعريف الارتباط (cookies)[١٣٨]، التي تُعد أدوات تقنية تُستخدم لتتبع نشاط المستخدمين، خاصةً للأغراض الإعلانية. وبالتالي، لا يجوز للمواقع الإلكترونية إلزام المستخدمين بالموافقة على تفعيل هذه الأدوات كشرط للوصول إلى خدماتها، ما لم تكن هذه الأدوات ضرورية وظيفيًا لتقديم الخدمة المطلوبة من المستخدم.

هذا الاشتراط يهدف إلى تعزيز حرية الاختيار لدى المستخدمين، وضمان عدم ممارسة أي ضغوط خفية أو استغلال حاجتهم للوصول إلى الخدمات، بما يتماشى مع مبادئ حماية البيانات التي تنص على وجوب أن تكون الموافقة حرة، صريحة، ومبنية على إدراك كامل من قبل المستخدم.

---

[١٣٨]– ملفات تعريف (الارتباط) (كوكيز)، تُعرف أيضًا بسجل التتبع أو سجل المتصفح، وهي عبارة عن ملفات نصية صغيرة يت إرسالها من الموقع الإلكتروني الذي يتم زيارته، ويتم تخزينها على حاسوب المتصفح، ويستخدم الموقع هذه الملفات لجمع المعلومات وتخزينها حول كيفية تفاعل المستخدمين مع الموقع على نحو يسمح بحفظ معلومات عن التصفح (وهذا يشمل بروتوكول الإنترنت وعناوين الأخبار التي تمت زيارتها، نوع المتصفح المستخدم، مزود خدمة الإنترنت، تاريخ ووقت التصفح، وعدد النقرات)، مما يسهل زيارة الموقع مرة أخرى، ومن جهة أخرى تكمن أهمية هذه الملفات في تقديم إعلانات محددة الهدف وتحسين وتخصيص تجربة التصفح الخاصة بالمستخدم ولإجراء إحصاءات حول زوار الموقع والوسائط الأخرى، وغالبًا ما تحيل المواقع لمعرفة المزيد حول ملفات تعريف الارتباط إلى مراجعة سياسية الخصوصية الخاصة به، وهذه الملفات لا تعد من الفيروسات أو البرامج الضارة، حيث لا تندمج مع نظام التشغيل الخاص بالمستخدم ولا تؤذى ملفاته. انظر على سبيل المثال، استخدام شركة جوجل Google لهذه الملفات، على الموقع التالي (بتاريخ ٢٠٢١/٧/٨:
https: //policies. google. com/technologies/cookies?hl=ar
وفي شأن أنواع ملفات الارتباط، راجع: سارة الشريف، خصوصية البيانات الرقمية، سلسلة أوراق الحق في المعرفة تصدر عن مركز دعم لتقنية المعلومات، القاهرة، ١٣ مارس ٢٠١٤، ص٣.
**Zainab Sattar Jabbar Kazem. (2022).** الحماية المدنية للبيانات الشخصية عبر الإنترنت (دراسة مقارنة). Misan Journal of Comparative Legal Studies, 1(5), 132-169. https: //doi. org/10. 61266/mjcls. v1i5. 86

(ISSN: 2537- 0758)

وترتيبًا على ذلك، فرضت لجنة المعلوماتية والحريات (CNIL) في فرنسا، بتاريخ ٧ ديسمبر ٢٠٢٠، غرامة مالية قدرها ١٠٠ مليون يورو على شركة جوجل، مقسمة إلى ٦٠ مليون يورو على شركة جوجل الأمريكية(Google LLC).، و٤٠ مليون يورو على شركة جوجل إيرلندا (Google Ireland).، وذلك لعدم وفائها بشروط صحة الموافقة، حيث انتهكت القواعد القانونية المتعلقة بضرورة وجود خيار واضح للمستخدمين بقبول أو رفض ملفات تعريف الارتباط (cookies)[١٣٩]، وكانت هذه الغرامة أعلى غرامة تفرضها اللجنة حتى ذلك الوقت. وفي اليوم نفسه، فرضت اللجنة أيضًا غرامة مالية قدرها ٣٥ مليون يورو على شركة التجارة الإلكترونية "أمازون أوروبا" (Amazon Europe) لانتهاك القواعد ذاتها[١٤٠].

وأشارت اللجنة إلى أنه عند تصفح المستخدم لموقعي جوجل (فرنسا) وأمازون (فرنسا)، كانت العديد من ملفات تعريف الارتباط الخاصة بالأغراض الإعلانية تُثبت تلقائيًا على حواسيب المستخدمين دون تقديم معلومات واضحة عن كيفية استخدام هذه الملفات أو عن كيفية رفضها. وهذا السلوك يُعد انتهاكًا واضحًا للقواعد المتعلقة بالحصول على موافقة صحيحة وصريحة من مستخدمي هذه المواقع، حيث بذلك يكون قد اخلا كلا الموقعين بالالتزام بمعايير الشفافية وحرية الاختيار التي تفرضها القوانين الأوروبية، وعلى رأسها اللائحة العامة لحماية البيانات(GDPR)[١٤١].

(139)- CNIL Délibération no SAN-2020-012 du 7 décembre 2020 concernant la société AMAZON EUROPE CORE, J. O., 10 décembre 2020. Disponible sur le site: https: //www. legifrance. gouv. fr/cnil/id/CNIL-TEXT000042635729

(140)- CNIL, Délibération no SAN-2020-013 du 7 décembre 2020 concernant la société AMAZON EUROPE CORE J. O., décembre 2020, Disponible su le site: https: //www. legifrance. gouv. fr/cnil/id/CNIL-TEXT000042635729

(141)- https: //www. cnil. fr/fr/cloture-de-linjonction-prononcee-lencontre-de-google-0?utm_source=chatgpt. com

وفي ١٦ يوليو ٢٠٢١، فرضت اللجنة الوطنية لحماية البيانات الشخصية في لوكسمبورغ(CNPD)[١٤٢] غرامة قياسية بلغت ٧٤٦ مليون يورو على شركة أمازون أوروبا (Amazon Europe)، حيث يقع المقر الرئيسي للشركة في أوروبا. وتُعد هذه الغرامة أكبر غرامة تم توقيعها حتى الآن بشأن انتهاك أحكام اللائحة الأوروبية العامة لحماية البيانات(GDPR)[١٤٣].

واستندت اللجنة في قرارها إلى أن معالجة شركة أمازون للبيانات الشخصية تنتهك أحكام اللائحة الأوروبية، نظرًا لأن نظام الاستهداف الإعلاني (Le système de ciblage publicitaire) الذي تفرضه الشركة على مستخدمي خدماتها يتم تنفيذه دون الحصول على موافقة حرة وصريحة من المستخدمين.

ويُعد هذا التصرف مخالفًا لمبدأ المشروعية الذي تُبنى عليه معالجة البيانات الشخصية بموجب اللائحة الأوروبية، مما يجعل عمليات جمع ومعالجة البيانات التي تنفذها أمازون غير مشروعة[١٤٤].

---

(142)- Commission Nationale pour la Protection des Données, Luxembourg .

(١٤٣)– يأتي هذا القرار نتيجة شكوى جماعية مقدمة إلى اللجنة الوطنية للمعلوماتية والحريات الفرنسية (CNIL) عام ٢٠١٨ من قبل الرابطة الفرنسية La Quadrature (LQDN)، والتي ادعت بأن الاستهداف الإعلاني لأمازون لا يلبي اشتراط الحصول على الرضائ الحر للمستخدم، ووفقًا لإجراءات التعاون بين سلطات حماية البيانات التي أنشأتها اللائحة الأوروبية لحماية البيانات، كان الاختصاص بنظر هذه الشكوى ينعقد للجنة الوطنية لحماية البيانات بلوكسمبورج (CNPD)، حيث تم إنشاء شركة أمازون أوروبا كور Amazon Europe Core على أراضيها، وقد تعاونت اللجنة الوطنية للمعلومات والحريات الفرنسية بشكل وثيق مع نظيراتها في لوكسمبورج CNPD طوال الإجراءات، في سياق عمليات التحقق من الأدلة التي تم الحصول عليها وتحليلها، ثم أثناء فحس مسودة القرار. راجع: موقع اللجنة الوطنية للمعلوماتية والحريات (CNIL).

https: //www. cnil. fr/lautorite-luxembourgoise-de-protection-des=donnees-prononce-lencontre-damazon-europe-core-une .

(١٤٤)– يشار إلى أنه وفقًا لقانون حماية البيانات بلوكسمبورج Luxembourg يجب الالتزام بالسرية المهنية، ويحظر نشر قرار الغرامة إلا عقب استنفاد مواعيد الطعن على القرار التي تبلغ ثلاثة

(ISSN: 2537- 0758)

هذا القرار يعكس التطبيق الصارم لأحكام اللائحة الأوروبية لحماية البيانات، ويُبرز التزام الجهات الرقابية بضمان احترام حقوق الأفراد المتعلقة ببياناتهم الشخصية، لا سيما في مواجهة الممارسات التجارية التي تنتهك قواعد الشفافية والموافقة الحرة.

- **تعدد الموافقة، الموافقة القائمة على الرضاء الحر عند تعدد أغراض معالجة البيانات:**

تشير الحيثية ٤٣ من اللائحة الأوروبية إلى أن التعبير عن الرضاء يُفترض أنه لم يصدر بحرية إذا تعذر الحصول على رضاء منفصل لكل عملية من عمليات معالجة البيانات الشخصية، بحيث تُعالج كل عملية على حدة.

ويترتب على ذلك أنه في حال كانت الخدمة تتضمن عمليات معالجة متعددة ذات أغراض متنوعة، فإنه يجب إتاحة الفرصة لصاحب البيانات لاختيار الأغراض التي يرغب في الموافقة عليها بصورة منفصلة، دون أن يكون مضطرًا لقبول جميع أغراض المعالجة جملة واحدة. فالرضاء الحر يتطلب السماح لصاحب البيانات بالتعبير عن رضاء مستقل لكل غرض من أغراض المعالجة المحددة. وبذلك، يجوز لصاحب البيانات أن يوافق على بعض عمليات المعالجة ويرفض الأخرى، مما يعزز حرية الاختيار ويدعم مبدأ الموافقة المستنيرة.

وفي السياق ذاته، توضّح الحيثية ٣٢ من اللائحة الأوروبية أن الرضاء الصادر من صاحب البيانات يجب أن يكون محددًا وينطبق على جميع أنشطة المعالجة

---

أشهر، باعتبار أن هذا النشر يعد بمثابة عقوبة إضافية، ولكن ما حدث هو قيام شركة أمازون بالإشارة لهذا القرار في تقرير أعمالها ربع السنوي، في ٢٩ يوليو ٢٠٢١. في هذا الشأن، راجع موقع اللجنة الوطنية لحماية البيانات الشخصية بلوكسمبورج التالي:
https: //cnpd. public. lu/fr/actualitesinternational/2021/08/decision-amazon-2. html .

المرتبطة بنفس الغرض. أما إذا كانت المعالجة تهدف إلى تحقيق أغراض متعددة، فإنه يجب الحصول على رضاء مستقل لكل غرض من هذه الأغراض[١٤٥].

وينبني على ذلك أنه إذا قام المتحكم بتجميع العديد من أغراض المعالجة في طلب واحد ولم يحرص على الحصول على رضاء منفصل لكل غرض، فإن ذلك يُعد مساسًا بحرية الرضاء، مما يجعله غير صالح قانونيًا.

وترتبط هذه المسألة ارتباطًا وثيقًا بمبدأ أن يكون الرضاء محددًا، وهو أحد شروط صحة الرضاء وفقًا لأحكام اللائحة الأوروبية، وسيتم تناول هذا الشرط بالتفصيل لاحقًا.

-تأثير تبعية صاحب البيانات للمتحكم على وجود الموافقة أو الرضاء الحر: إحدى المشكلات البارزة المتعلقة باشتراط أن يكون الرضاء حرًا تكمن في مدى احترام الطابع الإرادي للموافقة في الحالات التي تنطوي على علاقة تبعية، حيث يخضع بمقتضاها صاحب البيانات لسلطة أو نفوذ المتحكم. وتظهر هذه الإشكالية بشكل واضح في علاقات العمل أو سياق خدمات الصحة العامة.

وتُعد علاقات العمل نموذجًا خصبًا لهذه العلاقة غير المتوازنة، حيث يكون هناك قدر كبير من عدم التوازن بين صاحب العمل (المتحكم) والعامل أو المرشح للعمل (صاحب البيانات). ففي هذا السياق، تفرض طلبات الإفصاح عن البيانات الشخصية، حيث قد يطلب رب العمل من المرشح للعمل الإفصاح عن بيانات شخصية، قد تتعلق بصميم أموره الخاصة أو الحساسة[١٤٦]، بحجة متطلبات الوظيفة أو تقييم الكفاءة. ويظهر الضغط أو الإكراه، حيث قد يتعرض العامل أو المرشح لضغط نفسي أو إكراه، سواء كان مباشرًا أو غير مباشر، لقبول معالجة بياناته

---

[١٤٥]- من أجل الامتثال لشروط الحصول على رضاء صحيح عند إجراء معالجة البيانات لأغراض مختلفة، يجب فصل الرضاء detailer le consentement، أي التفريق بين أغراض المعالجة، والحصول على الرضاء لكل غرض منها على حدة. انظر:
Lignes directrices 5/2020, op. cit., no. 44, p. 14 .

[146]- M. LIFRANGE, op. cit., p. 23 .

(ISSN: 2537- 0758)

الشخصية، خوفًا من أن يؤثر رفضه على فرص حصوله على الوظيفة أو يتسبب في تمييز سلبي أو سوء معاملة(١٤٧).

وفي هذه الحالات، تتأثر إرادة صاحب البيانات بشكل كبير بسبب طبيعة العلاقة التبعية وظروفها الخاصة. ومن ثم، يصبح من الصعب اعتبار أن الموافقة أو الرضاء قد صدر بحرية كاملة. بل إن الرضاء قد يُوصف في مثل هذه الحالات بالرضاء القسري، مما ينزع عنه الطابع الحر المطلوب قانونيًا.

ونتيجة لذلك، قد يُعتبر رضاء المرشح للعمل مصطنعًا أو غير حقيقي في بعض الأحيان، خاصة إذا كان صادرًا تحت تأثير ظروف تجعل العامل يشعر بأنه مجبر على القبول(١٤٨). لذا، من المناسب إعادة النظر في مثل هذه الحالات وتقييمها بعناية لضمان عدم انتهاك مبدأ حرية الرضاء.

ولذلك، يرى البعض أن الرضاء لا يبدو في هذه الصورة هو الأساس القانوني الأنسب للقول بمشروعية معالجة البيانات الشخصية، إذ يتعين التيقن بداية من أن يكون التعبير عن الرضاء حرًا في هذه الحالة(١٤٩)، فنظرًا لتأثير التبعية الناجمة عن علاقة صاحب العمل بالعامل، يبدو من الصعب قيام صاحب البيانات برفض إعطاء الموافقة على معالجة بياناته دون خوف من تحمل الآثار السلبية لهذا الرفض، ولذلك من غير المحتمل مثلاً أن يتمكن العمل من الاستجابة بحرية لطلب صاحب العمل الحصول على رضائه لتفعيل نظم كاميرات المراقبة في مكان العمل، دون الشعور بأنه ملزم بالرضاء.

---

(147)- Groupe de travail "article 29", Avis 15/2011 sur la définition du consentement, op. cit., p. 14 .

(١٤٨)– د. بطيحي نسمة، الجرائم المتعلقة بانتهاك الأحكام الإجرائية المقررة لحماية الحق في الخصوصية الرقمية في التشريع الجزائري، بحث منشور بمؤتمر الخصوصية في مجتمع المعلوماتية، طرابلس– لبنان، ١٩–٢٠ يولي ٢٠١٩، مركز جيل البحث العلمي، سلسلة كتاب أعمال المؤتمرات، العام السابع، العدد ٢٦، يوليو ٢٠١٩، ص ٧٣.

(149)- M. LIFRANGE, op. cit., p. 23 .

لهذا، يعتبر مجلس حماية البيانات الأوروبي EDPB أنه من الصعب استناد رب العمل على الرضاء لمعالجة البيانات الشخصية لعمالة الحاليين أو المحتملين؛ لأنه قد يتعذر تعبير العامل عن الرضاء بصورة حرة. ومن ثَّم، بالنسبة لمعظم عمليات معالجة البيانات التي تجرى في أماكن العمل، لا يمكن اعتبار رضاء العامل هو الأساس القانوني لها، نظرًا لطبيعة علاقة رب العمل بالعامل التي تتسم بعدم التوازن في القوى(١٥٠).

ومع ذلك، لا يعني ذلك استحالة لجوء صاحب العمل إلى الحصول على موافقة العامل كأساس قانوني لمعالجة البيانات، حيث توجد حالات يمكن فيها لصاحب العمل إثبات أن الموافقة قد صدرت بحرية تامة من العامل. بالإضافة إلى ذلك، وعلى الرغم من اختلال توازن القوى بين صاحب العمل والعامل، يمكن للعامل في بعض الحالات الاستثنائية التعبير عن موافقته بحرية، شريطة ألا تترتب على رفضه للموافقة أي آثار سلبية(١٥١).

ويشير فريق عمل المادة (٢٩) إلى بعض الافتراضات التي يكون فيها رضاء صاحب البيانات حرًا في الإطار المعني، فعلى سبيل المثال، قد تطلب الشركة من موظفيها الموافقة على وضع صورة شخصية لهم بجوار أسمائهم على شبكتها

(150)- Lignes directrices 5/2020 sur le consentement au sens du règlement (UE) 2016/679, op. cit., no 21, p. 10; L'avis 2/2017 sur le traitment des données au travail (WP 249), pp. 6-7 .

(151)- Lignes directrices 5/2020, op. cit., no. 22, p. 10; L'avis 2/2017 sur le traitment des données au travailm pragraphe 6. 2 .

ومن المثير للاهتمام في هذا الصدد أن إرشادات فريق عمل المادة (٢٩) بشأن الرضاء، والتي اعتمدها مجلس حماية البيانات الأوروبي، تقتصر على دراسة حالة تبعية صاحب العمل والعامل فقط دون ذكر الحالات الأخرى من "اختلال توازن القوى"، والتي غالبًا ما تكون قائمة في الخدمات التي تقدمها الشبكات الاجتماعية ومحركات البحث، وبشكل عام، من خلال المنصات على الإنترنت. راجع:

Y. POULLET, Consentement et RGPD: des zones d' ombre!, op. cit., p. 6, marge 20 .

(ISSN: 2537- 0758)

الإلكترونية الداخلية، وتجيز لهم رفض ذلك، فإذا أرسل الموظف صورة له، فيمكن اعتبار ذلك رضاءً صحيحًا صادرًا منه(١٥٢).

- **أثر دفع مقابل مالي لصاحب البيانات على وجود الموافقة أو الرضاء الحر:**

يثار التساؤل في هذا السياق حول مدى تأثير تقديم مقابل مالي مسبق أو منح حوافز ومنافع مادية على صحة الموافقة الصادرة عن صاحب البيانات؟ وتدخل ضمن هذا الإطار جميع أشكال الحوافز التي تحث الشخص أو تدفعه إلى الموافقة على معالجة بياناته. وفي الواقع، لا تقدم النصوص القانونية المتعلقة بحماية البيانات حلاً واضحاً لهذه الإشكالية. ومع ذلك، يُمكن بالتحليل المنطقي استنتاج أن الحصول على الموافقة مقابل منفعة مالية أو حتى أدبية قد يتعارض مع مفهوم الإرادة الحرة، التي يجب أن تكون نابعة من قناعة شخصية واختيار واعٍ مستقل. فطريقة الحصول على هذه الموافقة قد تنطوي على نوع من الإكراه، حيث يُعتبر المقابل المالي أو المنفعة الأدبية شكلاً من أشكال الضغط غير المباشر، لا سيما إذا كان الشخص في حالة ضرورة أو بحاجة ماسة إلى المال أو المنفعة. وفي مثل هذه الظروف، تكون الموافقة عرضة للعيب أو الانعدام بسبب التأثير على حرية الاختيار(١٥٣).

## الفرع الثانى

## التعبير عن الارادة المستنيرة بالموافقة

لا يكفي أن تكون موافقة الشخص المعني بالبيانات حرّة، بل يجب أن تكون كذلك مستنيرة éclairée، وفقًا لما تنص عليه المادة ٤، بند ١١ من اللائحة الأوروبية لحماية البيانات. ويترتب على هذا الشرط التزام على عاتق المسؤول عن المعالجة يتمثل في إبلاغ الشخص المعني بطبيعة وأغراض معالجة البيانات، وكافة التفاصيل المتعلقة بها، بما في ذلك النتائج المحتملة المترتبة على هذه المعالجة.

(152)- Groupe de Travail "article 29", Avis 15/2011 sur la définition du‹... op. cit., p. 15 .

(١٥٣)– في هذا المعنى في إطار التجربة الطبية، انظر: د. محمد عيد الغريب، مرجع سابق، ص٧٦.

ويرتبط هذا الالتزام ارتباطًا وثيقًا بمبدأ الشفافية، الذي يُعد أحد المبادئ الأساسية لمعالجة البيانات الشخصية، إلى جانب النزاهة والمشروعية، كما نصت عليه المادة الخامسة من اللائحة العامة لحماية البيانات.(GDPR) ويكتسب هذا الالتزام أهمية خاصة نظرًا للحاجة إلى مواجهة التحديات الناتجة عن الضعف المعرفي لدى مستخدمي المواقع أو التطبيقات الإلكترونية تجاه التقنيات المستخدمة، حتى عندما تكون هذه التقنيات مألوفة لهم. وتزداد التحديات تعقيدًا في حالة الأمية الرقمية، وهي ظاهرة شائعة لا تبعث على التفاؤل في كثير من الأحيان.

من هذا المنطلق، يمكن القول إن الخصائص الجوهرية للتكنولوجيا تستوجب وجود آليات فعّالة لضمان الحصول على موافقة حقيقية ومستنيرة، تُمكّن الشخص المعني من اتخاذ قرار واعٍ ومبني على فهم واضح لما ينطوي عليه استخدام بياناته الشخصية.

ووفقًا لإرشادات مجلس حماية البيانات الأوروبي (EDPB) بشأن الموافقة، يلتزم المتحكم في البيانات بتوفير جميع المعلومات الضرورية المتعلقة بعملية المعالجة قبل الحصول على موافقة صاحب البيانات. ويهدف ذلك إلى تمكين الشخص المعني من اتخاذ قرارات مستنيرة وفهم ماهية المعالجة التي يوافق عليها، بالإضافة إلى تيسير ممارسة حقه في سحب الموافقة عند رغبته.

ويشمل هذا الالتزام تقديم معلومات شاملة تغطي جميع الجوانب الموضوعية للمعالجة التي تستند إلى الموافقة كأساس قانوني للشرعية[١٥٤]. وفي حال إخلال

(154)- Lignes directrices 5/2020 sur le consentement au sens du réglement (UE) 2016/679, op. cit., no 62, p. 17 .

وفي هذا الإطار اعتبرت اللجنة الوطنية للمعلوماتية والحريات في فرنساCNIL أن مجرد الإشارة إلى استخدام محتوى الموقع أو التطبيق الإلكتروني على الهاتف لإجراء "مسح" حول اهتمامات الشخص المعني، للاستفادة منها في الإعلانات اللاحقة. هو أمر يصعب فهمه من قبل الأفراد، ولا يمكن أن يسمح بالتعبير عن الرضاء المستنير، إذ في الواقع يعتبر غير دقيق لأنه يغطي

(ISSN: 2537- 0758)

المسؤول عن المعالجة بهذا الالتزام، تُعتبر الموافقة الصادرة غير صحيحة. ويترتب على ذلك فقدان المعالجة لأساسها القانوني والمشروع، مما يعرض المسؤول عن المعالجة للمساءلة القانونية عن مخالفة أحكام القانون ذات الصلة(١٥٥).

- **مضمون الالتزام بإعلام صاحب البيانات بالمعلومات اللازمة لتكوين الموافقة المستنيرة:**

لضمان مشروعية جمع ومعالجة البيانات الشخصية، يلتزم المتحكم بإبلاغ الشخص المعني مسبقًا بوجود معالجة لبياناته، وبيان أساليب هذه المعالجة والغرض منها. كما يجب أن يُحاط الشخص علمًا بمعلومات دقيقة وواضحة تمكّنه من اتخاذ قرار مستنير بشأن الموافقة على جمع ومعالجة بياناته(١٥٦).

يمثل هذا الالتزام عنصرًا جوهريًا في إطار حماية البيانات الشخصية، حيث يهدف إلى جذب انتباه الشخص المعني وتنبيهه إلى المعلومات المقدمة من المتحكم، بما يضمن له فرصة حقيقية لاتخاذ قراره بحرية كاملة وبناءً على فهم واضح لكافة أبعاد العملية. وبهذا، تُرسخ هذه الخطوة مبدأ الشفافية وتعزز من قدرة الشخص المعني على ممارسة حقوقه بوعي ومسؤولية.

---

عددًا كبيرًا من المواقف، كما أن صياغته ليست مناسبة لعامة الأفراد الخاضعين للمعالجة، نظرًا لتعقيد المصطلحات المستخدمة.

(١٥٥)– تشترط المادة الثانية من قانون حماية البيانات المصري ضرورة الحصول على موافقة الشخص المعني للقيام بأية عمالة على البيانات، وترتب المادة (٣٦) من القانون جزاء جنائى حال عدم الحصول على هذه الموافقة. كذلك وفقًا للمادة (٦) من اللائحة العامة لحماية البيانات GDPR يعد رضاء صاحب البيانات أحد الشروط اللازمة لقانونية المعالجة.

Commission Nationale de l'informatique et des Libertés, Décision no MED 2018-042 du 30 octobre 2018 mettant en demeure la société X, 09 novembre 2018, disponible sur le site: https: //www. legifrance. gouv. fr/cnil/id/CNIL_TEXT000037594451/

(١٥٦)– د. سامح عبد الواحد التهامي، ضوابط معالجة البيانات الشخصية، مرجع سابق، ص ٤١٠.

وتحقيقا لتنفيذ الموافقة المستنيرة، فقد أكد مجلس حماية البيانات الأوروبي على ضرورة التزام المتحكم بإبلاغ الشخص المعني بمجموعة من المعلومات الأساسية كحد أدنى عند طلب الحصول على موافقته، وذلك لتحقيق الموافقة المستنيرة. وتشمل هذه المعلومات(١٥٧): هوية المتحكم، وذلك لضمان معرفة الشخص بالجهة المسؤولة عن معالجة بياناته(١٥٨). والغرض من كل عملية معالجة، حيث توضيح الهدف المحدد لكل عملية معالجة مشمولة بالموافقة المطلوبة. وأنواع البيانات المطلوبة، حيث تحديد البيانات الشخصية التي سيتم جمعها واستخدامها. وحق سحب الموافقة، حيث وجوب إعلام الشخص بحقه في سحب موافقته في أي وقت دون التأثير على قانونية المعالجة التي تمت بناءً على الموافقة قبل سحبها، وفقًا للمادة ٧، الفقرة ٣ من اللائحة العامة لحماية البيانات. واستخدام البيانات في اتخاذ القرار الآلي(١٥٩)، حيث ذا كانت المعالجة تتضمن قرارات مؤتمتة بالكامل تؤثر على الشخص بشكل جوهري، يجب توفير معلومات واضحة عن ذلك، وفقًا للمادة ٢٢، الفقرة ٢، بند ٦ من اللائحة(١٦٠). والمخاطر المرتبطة بنقل البيانات، حيث وجوب تقديم معلومات عن

---

(157)- Ligens directrices 5/2020 sur le consentement au sens du réglement (UE) 2016/679, op. cit., no 64, pp. 17-18 .

(١٥٨)– وفي هذا الصدد تشير الحيثية le considérant رقم ٤٢ من اللائحة العامة لحماية البيانات GDPR إلى أنه: "... حتى تكون الرضاء مستنيرًا، ينبغي أن يعرف صاحب البيانات على الأقل هوية المتحكم وأغراض معالجة البيانات الشخصية".

(١٥٩)– راجع أيضًا إرشادات فريق عمل "المادة ٢٩" بشأن القرارات الفردية الآلية والتنميط في ظل اللائحة رقم ٦٧٩/ ٢٠١٦، ص ٢٠ وما بعدها.

Lignes directrices du Groupe de travail "article 29" sur le decisions individuelles automatisées et le profilage au titre du règlement 2016/679 (WP 251), Paragraphe IV. B. p. 20 et suivantes .

(١٦٠)– وفقًا للمادة (١/٢٢) من اللائحة العامة لحماية البيانات GDPR "يكون لصاحب البيانات الحق في عدم الخضوع لقرار يستند فقط إلى المعالجة الآلية، بما في ذلك التنميط le profilage (تحديد ملامح البيانات)، وما يترتب عليه من آثار قانونية، تتعلق به أو تؤثر عليه بشكل ملحوظ". وتشير المادة (٢/٢٢) إلى أنه: "لا تنطبق الفقرة ١ عندما يكون القرار:... ج) يستند إلى الموافقة الصريحة لصاحب البيانات".

(ISSN: 2537- 0758)

المخاطر المحتملة المرتبطة بنقل البيانات إلى دول أو جهات لا توجد فيها قرارات بشأن مدى الكفاية أو ضمانات مناسبة لحماية البيانات[١٦١]. ويهدف توفير هذه المعلومات إلى تعزيز مبدأ الشفافية وضمان اتخاذ الشخص المعني لقراره بالموافقة أو الرفض بناءً على معرفة واعية وشاملة بجميع الجوانب المرتبطة بمعالجة بياناته الشخصية.

ولا شك أن هذه المعلومات تمثل الحد الأدنى من الاشتراطات المتعلقة بمضمون الالتزام بالإعلام اللازم لتكوين موافقة مستنيرة، وفقًا لما يؤكد عليه مجلس حماية البيانات الأوروبي. ومع ذلك، يفرض هذا الالتزام على المتحكم أن يقدم لصاحب البيانات أي معلومات إضافية من شأنها تمكينه من اتخاذ قرار مستنير قبل التعبير عن موافقته، وذلك استنادًا إلى ظروف كل حالة وسياقها الخاص.

ومن بين هذه المعلومات الإضافية التي قد تكون ذات أهمية، مدة الاحتفاظ بالبيانات، حيث وجوب تحديد الفترة الزمنية التي سيتم خلالها تخزين البيانات الشخصية. وحق الاعتراض على المعالجة، حيث وجوب إعلام الشخص بحقه في الاعتراض على معالجة بياناته في ظروف معينة، بما يتماشى مع أحكام القانون. والتقنيات المستخدمة في المعالجة، حيث لزوم توضيح الوسائل التقنية والأساليب التي سيتم استخدامها لمعالجة البيانات[١٦٢]. ويوفر هذا النهج الشامل لصاحب البيانات فهمًا أعمق لعمليات المعالجة المقترحة، بما يتيح له تقييم العواقب المحتملة بشكل أفضل واتخاذ قراره بالموافقة أو الرفض بناءً على إدراك واعٍ وشامل.

وفي هذا الإطار، تلزم المادة (١١٦/ ١) من قانون المعلوماتية والحريات الفرنسي (المعدل عام ٢٠١٨) المتحكم في البيانات أو من ينوب عنه، بإعلام الشخص الذي يتم جمع بياناته الشخصية، ما لم يكن قد أعلمه مسبقًا بما يأتي، هوية المتحكم وهوية

---

[١٦١]– وفقًا للمادة ١/٤٩ (أ) من اللائحة العامة لحماية البيانات، في حالة طلب الرضاء الصريح، يلزم الحصول على معلومات محددة تتعلق بغياب الضمانات الواردة في المادة (٤٦) من اللائحة.

[162]- Lignes drectrices 5/2020, op. cit., no 65, p. 18 .

ممثله عند الاقتضاء، والغرض من المعالجة التي تنصب على البيانات الطبيعية الإلزامية أو الاختيارية للرد، والعواقب المحتملة لعدم الرد، وفئات المستفيدين من البيانات، وحقوقه وفقًا لأحكام القانون(١٦٣).

ويتعين أن يتم هذا الإعلان قبل شروع المتحكم في جمع البيانات، أي مسبقًا، لضمان تزويد الشخص المعني بالمعلومات اللازمة قبل بدء عملية المعالجة. ويُستثنى من هذا الالتزام بعض الحالات المحددة قانونًا، مثل معالجة البيانات لأغراض إحصائية أو إعلامية، أو إذا كانت المعالجة تتم لاعتبارات تتعلق بالأمن القومي. وتستند هذه الاستثناءات إلى أهمية تحقيق التوازن بين حماية البيانات الشخصية وتحقيق المصالح العامة أو السيادية، مع مراعاة أن تكون هذه المعالجات متوافقة مع القوانين واللوائح المعمول بها لضمان عدم إساءة استخدامها(١٦٤).

- **كيفية تقديم المعلومات لتكوين الموافقة المستنيرة:**

لم تفرض اللائحة الأوروبية (GDPR) شكلًا محددًا لتقديم المعلومات اللازمة لتكوين الموافقة المستنيرة، وذلك يوحى بانه يتيح مرونة في اختيار وسائل تقديم هذه المعلومات. بمعنى اخر انه يمكن أن يتم ذلك عبر وسائل متنوعة، مثل الإعلانات

(١٦٣)– كما توجب المادة (٨٢) من قانون المعلوماتية والحريات المعدل عام ٢٠١٨ على المتحكم أو من ينوب عنه بأن يقوم بإعلام أي مشترك أو مستخدم لخدمة الاتصالات الإلكترونية بطريقة واضحة وشاملة. بالغرض من أي إجراء يهدف إلى الوصول. عن طريق الإرسال الإلكتروني، إلى المعلومات المخزنة بالفعل في أجهزة الاتصالات الإلكترونية الطرفية، أو إدخال المعلومات في هذه الأجهزة، وكذلك الوسائل المتاحة للاعتراض على ذلك.

(١٦٤)– في شأن الأحوال المستثناة قانونًا. راجع: المادة الثالثة من مواد إصدار قانون رقم ١٥١ لسنة ٢٠٢٠ بشأن قانون حماية البيانات الشخصية المصري، المعنية بالبيانات الشخصية التي تخرج من نطاق سريان أحكام هذا القانون والتي لا يشملها بالحماية. راجع أيضًا المادة (٦) من هذا القانون، التي تشير إلى أحوال مشروعية وقانونية المعالجة الإلكترونية للبيانات، والتي تشمل إلى جانب الرضا صورًا أخرى، كأن تكون المعالجة لازمة لتنفيذ التزام تعاقدي (م٦ بند٢) أو التزام ينظمه القانون (م٦ بند ٣).

(ISSN: 2537- 0758)

المكتوبة أو الشفهية أو باستخدام الرسائل الصوتية أو المرئية.، ومع ذلك حددت اللائحة متطلبات دقيقة لضمان وضوح وكفاية المعلومات المقدمة، وخاصة في المادة (٢/٧)، التي تنص على ما يلي "إذا وردت موافقة صاحب البيانات في سياق تصريح كتابي يتناول أيضًا مسائل أخرى، فيجب أن يُعرض طلب الحصول على الموافقة بطريقة تميزه بوضوح عن المسائل الأخرى، وأن يكون في شكل واضح ويسهل الوصول إليه، باستخدام عبارات مفهومة ولغة بسيطة. وأي جزء من هذا التصريح يشكل انتهاكًا لأحكام اللائحة لا يُعتبر ملزمًا". وبذلك تتلخص المتطلبات الأساسية لتقديم المعلومات فى وجوب التمييز الواضح، بمعنى إنه إذا كان طلب الموافقة جزءًا من وثيقة تشمل مواضيع أخرى، يجب فصل طلب الموافقة بوضوح عن باقي الموضوعات. وسهولة الوصول، حيث يجب أن تكون المعلومات المقدمة في متناول الشخص المعني بطريقة واضحة ومباشرة. واستخدام لغة بسيطة، حيث يلزم استخدام عبارات غير معقدة يسهل على الأشخاص العاديين فهمها دون لبس. وجوب الالتزام القانوني، حيث اذا تبين ان أي جزء من طلب الموافقة لا يتماشى مع أحكام اللائحة يُعتبر غير ملزم قانونًا[١٦٥].

ويتبين من ذلك وجود مرونة في وسيلة الحصول على الرضاء الكتابي لصاحب البيانات على نحو يؤدي إلى تحسين مستوى وضوح المعلومات، وتؤكد على ذلك الحيثية ٣٢ من اللائحة التي تشير إلى تنوع وسيلة الحصول على الرضاء الكتابي من خلال أي تصريح أو سلوك يشير بوضوح في هذا السياق إلى رضاء صاحب البيانات بالمعالجة المقترحة لبياناته.

(165)- Ribeiro, A., Dias, V., Ribeiro, S., Silva, J., & Barros, H. (2022). Geoprivacy in neighbourhoods and health research: a mini-review of the challenges and best practices in epidemiological studies. Public Health Reviews, 43. https: //doi. org/10. 3389/phrs. 2022. 1605105

ويشير فريق عمل المادة ٢٩ إلى نوعين من الاشتراطات التي تكفل توفير المعلومات الأساسية للحصول على رضاء مستنير بما فيه الكفاية، يتعلق الأول بطريقة توصيل المعلومات، ويتعلق الثاني بالوصول إلى المعلومات ووضوحها[١٦٦].

فيما يتعلق بأسلوب تقديم المعلومات، يتعين إعلانها بلغة بسيطة وواضحة ومفهومة بالنسبة لأي مستخدم عادي. وبالتالي، يجب الامتناع عن استخدام المصطلحات المعقدة أو الكلمات متعددة المعاني، كما يجب ألا تتضمن شروطًا تعسفية[١٦٧]. علاوة على ذلك، ينبغي أن تكون المعلومات واضحة ومرئية بشكل مباشر، بما يضمن سهولة وصول الشخص المعني إليها.

ولقد تم التركيز بشكل خاص على هذه المسألة في سياق معالجة البيانات باستخدام تقنيات الذكاء الاصطناعي، وذلك من خلال "الإرشادات الأخلاقية للذكاء الاصطناعي الجدير بالثقة Lignes Directrices en Matière d'Éthique)

---

(166)- Groupe de travail "article 29", Avis 15/2011 sur la définition du consentement, op. cit., p. 21 .

وانظر فى تفاصيل اكثر

Tikkinen-Piri, C., Rohunen, A., & Markkula, J. (2018). Eu general data protection regulation: changes and implications for personal data collecting companies. Computer Law & Security Review, 34(1), 134-153. https: //doi. org/10. 1016/j. clsr. 2017. 05. 015

(١٦٧)– تشير الحيثية رقم ٤٢ من اللائحة العامة لحماية البيانات GDPR إلى أن هذا الحكم يأتي استنادًا لأحكام التوجيه الأوروبي رقم ٩٣/١٣ بشأن الشروط التعسفية في العقود المبرمة مع المستلهكين.

Directie 93/13/CEE du Conseil, du 5 avril 1993, concernant les clauses abusives dans les contrats concluus avec les consommateurs, JOL 95 du 21. 4. 1993, p. 29. Drozd, O. (2023). A conceptual consent request framework for mobile devices. Information, 14(9), 515. https: //doi. org/10. 3390/info14090515

Kurteva, A., Chhetri, T., Pandit, H., & Fensel, A. (2024). Consent through the lens of semantics: state of the art survey and best practices. Semantic Web, 15(3), 647-673. https: //doi. org/10. 3233/sw-210438 .

(ISSN: 2537- 0758)

"pour une IA Digne de Confiance- GEHN IA)[١٦٨]، التي أصدرتها المفوضية الأوروبية في يونيو ٢٠١٨[١٦٩].

تشير هذه الإرشادات إلى أنه في ظل الآليات الحالية للتعبير عن الموافقة المستنيرة عبر الإنترنت، يقوم الأفراد بمنح موافقتهم دون إيلاء اهتمام كافٍ لمخاطر الخصوصية. وهذا يستلزم وجود التزام أخلاقي بتطوير وسائل جديدة وعملية للتعبير عن الموافقة المستنيرة والتحقق منها تلقائيًا باستخدام تقنيات الذكاء الاصطناعي أو غيرها من التقنيات المماثلة. وينطبق ذلك أيضًا على استخدام البيانات الشخصية "المجهولة"، التي قد تكون قابلة لإعادة نسبتها إلى أصحابها[١٧٠].

في هذا السياق، أصدرت اللجنة الوطنية للمعلومات والحريات (CNIL) قرارًا بفرض غرامة قدرها ٥ ملايين يورو على شركة "جوجل(Google)"[١٧١]، بسبب

---

[١٦٨]–في ٨ أبريل ٢٠١٩، قدم فريق الخبراء رفيعي المستوى المعنى بالذكاء الاصطناعي إرشادات أخلاقية للذكاء الاصطناعي الجدير بالثقة، جاء ذلك بعد نشر المسودة الأولى لهذه الإرشادات في ديسمبر ٢٠١٨، وقد تم تلقى أكثر من ٥٠٠ تعليق عليها من خلال استشارة مفتوحة، وتهدف هذه الإرشادات إلى تعزيز الذكاء الاصطناعي الجدير بالثقة، وتشير إلى أنه يجبأن يكون الذكاء الاصطناعي الجدير بالثقة: أ–قانوني: احترام جميع القوانين واللوائح المعمول بها. ب– أخلاقي: الالتزام بالمبادئ والقيم الأخلاقية. د– قوى: سواء من الناحيتين التقنية والاجتماعية، لأن أنظمة الذكاء الاصطناعي حتى مع وجود نوايا حسنة، يمكن أن تسبب ضررًا غير مقصود. راجع:

Lignes drectrices en matière d'éthique pour une IAdigne de confiance, Groupe d'experts de haut niveau sur l'intelligence artificielle, Disponible sur le site: https: //digitsl-strategy. ec. europa. eu/en/library/ethics-guidelines-trustworthy-ai

[169]- Groupe d'experts indépendants de haut niveau sur l'intelligence artificielle (GEHN IA), Constitute par la commission européenne en juin 2018.

[170]- Lignes directrices en matière d'éthique pour une IA digne de confiance, op. cit., no 130, p. 44 et Marge 72 .

[171]- CNIL, Délibération no SAN-2019-001, 21 janvier 2019, Disponible sur le site: https: //www. cnil. fr/sites/default/files/atoms/files/san-2019-001_21_01-2019 pdf .

اتهامها بانتهاك قواعد حماية البيانات في الاتحاد الأوروبي. وجاء ذلك نتيجة قيام الشركة بإلزام مستخدمي الأجهزة المحمولة التي تعمل بنظام "أندرويد (Android)" بقبول سياسة الخصوصية وشروط وأحكام خدماتها(١٧٢)، حيث ترتب على رفضهم لهذه الشروط عدم إمكانية استخدام الأجهزة.

واتهمت اللجنة شركة جوجل بالافتقار إلى الشفافية، نتيجة عدم تقديمها معلومات واضحة للمستهلكين حول كيفية جمع بياناتهم وتخزينها، مما يُعد مخالفة لالتزامات اللائحة العامة لحماية البيانات الأوروبية (GDPR) التي تتطلب توفير معلومات واضحة ومفهومة. وانتهت اللجنة إلى أن الشركة أخفقت في الحصول على الموافقة الصحيحة من المستخدمين عند معالجة بياناتهم الشخصية، باعتبار الموافقة أساسًا لمشروعية المعالجة. وأشارت اللجنة إلى أن المعلومات المقدمة للمستخدمين لم تكن واضحة أو مفهومة بما يكفي، وأنه كان يجب الحصول على موافقة محددة لكل غرض من أغراض معالجة البيانات بشكل مستقل(١٧٣).

---

(١٧٢)– حيث تشير سياسة خصوصية موقع "جوجل Google" إلى ما يلي: "نجمع هذه المعلومات عندما تتصل خدمة Google على جهازك بخوادمنا، على سبيل المثال، عندما تثبت تطبيقًا من "متجر جوجل بلاى Google Play أو عندما تتحقق إحدى الخدمات من وجود تحديثات تلقائية، إذا كنت تستخدم جهاز أندرويد Android مع تطبيقات جوجل Google، يتصل جهازك بصفة دورية بخوادم Google لتوفير معلومات حول جهازك والاتصال بخدماتنا. وهذه المعلومات تشمل أمورًا، مثل نوع جهازك واسم مشغل شبكة الجوّال وتقارير الأعطال والتطبيقات التى ثبتها". انظر الموقع التالي: https: //policies. google. com/privacy?hl=ar

(١٧٣)– حيث لم توضح شركة جوجل مدى وحدود جمع البيانات على التطبيقات المدمجة بالهواتف التي تستخدم نظام أندرويد (مثل يوتيوب وبلاى ستور وغيرها. حال اتخاذ الخطوات الأولى لضبط هذه الهواتف بما في ذلك الخيارات المختلفة المتوافرة. انظر: دان شيفت، الرضا والخصوصية، مجلة رؤى تكنولوجية، تصدر عن مركز المعلومات ودعم اتخاذ القرار التابع لمجلس الوزراء المصري، العدد الأول، مارس ٢٠٢١، ص ١٨.

(ISSN: 2537- 0758)

وأيّد مجلس الدولة الفرنسي، في حكمه الصادر بتاريخ ١٩ يونيو ٢٠٢١، قرار اللجنة الوطنية للمعلوماتية والحريات (CNIL) المشار إليه، ورفض طلب شركة "جوجل (Google)" بإلغاء الغرامة المفروضة عليها. وجاء هذا التأييد دون الحاجة إلى إحالة القضية إلى محكمة العدل الأوروبية، مستندًا إلى خطورة الانتهاكات المرتكبة، المتمثلة في تجاهل متطلبات الموافقة والإخلال بالالتزام بالإعلام والشفافية، وتأثير ذلك على حقوق المستخدمين المقررة بموجب اللائحة العامة لحماية البيانات الأوروبية(GDPR)..[١٧٤].

كما أخذ مجلس الدولة في الاعتبار الطبيعة المستمرة لهذه الانتهاكات والفترة الزمنية الطويلة التي استمرت خلالها. وأكد الحكم أن الغرامة المفروضة تتناسب مع الحدود القصوى المنصوص عليها في المادة (٨٣) من اللائحة الأوروبية، ومع الوضع المالي لشركة جوجل، حيث تتيح الفقرة الخامسة من هذه المادة فرض غرامات تصل إلى ٤% من إجمالي حجم الأعمال السنوية للشركة على مستوى العالم[١٧٥].

وفيما يتعلق بسهولة الوصول إلى المعلومات ووضوحها، يتعين تقديم المعلومات مباشرة إلى الشخص المعني، حيث لا يُعد مجرد "إتاحة" المعلومات على الموقع أو التطبيق الإلكتروني كافيًا. بل يجب أن تكون المعلومات واضحة من حيث نوع الخط وحجمه، بارزة، وكاملة. ولتسهيل ذلك، يمكن استخدام مربعات الحوار (boîtes de

(174)- Breuer, J., Zeeland, I., & Pierson, J. (2023). Walkshops– testing a low threshold methodology for participatory city making. Aoir Selected Papers of Internet Research. https: //doi. org/10. 5210/spir. v2022i0. 12978

(175)- Conseil d'État, 10ème chambres reunites, 19/06/2020, N° 430810,- Sté Google LLC, Publié au recueil Lebon Disponible sur le site: https: //www. conseil-etat. fr/fr/arianeweb/CRP/conclusion/2020-06-19/430810?download_pdf .Jang, W. and Newman, A. (2021). Enforcing european privacy regulations from below: transnational fire alarms and the general data protection regulation*. JCMS Journal of Common Market Studies, 60(2), 283-300. https: //doi. org/10. 1111/jcms. 13215

(dialogue التي تطلب من المستخدم الإجابة بـ"نعم" أو "لا"، بهدف تقديم معلومات محددة في وقت طلب الحصول على الموافقة(١٧٦).

وفي حالة حصول المتحكم على "الموافقة المستنيرة" من الطفل، يجب عليه شرح كيفية استخدام البيانات التي يتم جمعها بعبارات واضحة وبسيطة تتناسب مع مستوى فهم الطفل. ولكن إذا كان التعبير عن الموافقة متروكًا لصاحب السلطة الأبوية، فيتعين على المتحكم تقديم قدر كافٍ من المعلومات لتمكينه من اتخاذ قرار مستنير بشأن بيانات طفله(١٧٧).

ونخلص مما تقدم إلى القول بانه قدعززت اللائحة الأوروبية شروط الموافقة، بحيث لا يجوز للمتحكم الاعتماد على سياسات خصوصية عامة ومعقدة يصعب فهمها أو تضمين مصطلحات قانونية غامضة. حيث يتعين تقديم طلب الحصول على الموافقة بشكل واضح وسهل الوصول إليه، وبطريقة يمكن تمييزها عن الأمور الأخرى(١٧٨)، مع استخدام لغة بسيطة ومباشرة يفهمها الشخص العادي. ويجب أن

(176)- Lignes directrices 5/2020 sur le consentement au sens du règlement (UE) 2016/679, op. cit., no 67, pp. 18 et 19 .Groupe de travail "article 29", Avis 15/2011 sur la definition du consentement, op. cit., p. 22 . Kurteva, A., Chhetri, T., Pandit, H., & Fensel, A. (2024). Consent through the lens of semantics: state of the art survey and best practices. Semantic Web, 15(3), 647-673. https: //doi. org/10. 3233/sw-210438

(177)- Georgopoulou, A. (2024). Social media platforms and general data protection regulation violation for minor users. BMMCONF, 1(1), 1-12. https: //doi. org/10. 33422/bmmconf. v1i1. 258. Dempsey, J., Sim, G., & Cassidy, B. (2018). Designing for gdpr- investigating children's understanding of privacy: a survey approach. . https: //doi. org/10. 14236/ewic/hci2018. 26. Lignes directrices 5/2020, sur le consentement au sens du réglement (UE) 2016/679, op. cit., no 126, p. 30.

(١٧٨)– حينما يكون الرضاء مطلوبًا مثلاً في إطار عقد، يجب أن يكون طلب الحصول على الرضاء في شكل يميزه بوضوح عن الأمور الأخرى، وإذا كان العقد يتضمن العديد من الجوانب التي لا علاقة لها بمسألة الرضاء بالمعالجة، فيجب التعامل مع مسألة الرضاء بشكل يمكن تمييزه بوضوح لصاحب البيانات، أو في مستند منفصل (المادة ٢/٧ من اللائحة الأوروبية).

(ISSN: 2537- 0758)

يتضمن طلب الموافقة بيانًا صريحًا يوضح الغرض من معالجة البيانات المرتبطة بهذه الموافقة. ويترتب على ذلك ضرورة تجنب إخفاء المعلومات الضرورية لصدور الموافقة المستنيرة ضمن الشروط والأحكام العامة للموقع أو الصفحة الإلكترونية. كما يتعين على المتحكم توضيح أغراض معالجة البيانات الشخصية أو تخزينها، بما يمكن الشخص المعني من فهم الغايات المستهدفة من هذه المعالجة بشكل كامل[١٧٩].

وقياساً على ما تقدم فانه يجب أن يكون طلب الحصول على الموافقة المقدَّم بوسيلة إلكترونية منفصلاً ومميزًا، بحيث لا يجوز إدراجه كأحد البنود أو الفقرات ضمن الشروط والأحكام العامة. وينبغي أن يكون هذا الطلب واضحًا وموجزًا، وألا يؤدي إلى تعطيل استخدام الخدمة دون داعٍ، وذلك وفقًا لما ورد في الحيثية (٣٢) من اللائحة الأوروبية. ولمراعاة طبيعة الشاشات الصغيرة للهواتف المحمولة أو الأجهزة اللوحية مثل "التابلت"، التي قد لا تتيح عرض المعلومات بشكل كافٍ، يمكن عند الاقتضاء تصميم العرض بحيث تُعرض المعلومات بشكل تتابعي (Layered Approach)، مما يسهم في ضمان الاطلاع عليها وفهم مضمونها دون الإخلال بجودة التجربة أو الشفافية المطلوبة[١٨٠].

---

محمود فياض، "قواعد مساعدات الدولة للاتحاد الأوروبي لقطاع النقل الجوي في ضوء المادة ١٠٧ من معاهدة الاتحاد الأوروبي"، مجلة JOL، المجلد ٤٨، العدد ١، ٢٠٢٤، ص ٣٥٩-٤٠٤، متاح على الرابط: https: //doi. org/10. 34120/jol. v48i1. 183.

[١٧٩]- مربعات الحوار أو صناديق الحوار boîtes de dialogue هى "مربعات حوارية تظهر (على الموقع أو التطبيق) وتطلب من المستخدم الإجابة بنعم أو لا". راجع: د. شريف فهمي بدوى، معجم مصطلحات الكمبيوتر والإنترنت والمعلوماتية، إنجليزي- فرنسي-عربي، دار الكتاب المصري- القاهرة، دار الكتاب اللبناني- بيروت، الطبعة الأولى، ٢٠٠٧، رقم ١٠٣٤، ص ١٠٨.

Lignes directrices 5/2020 sur le consentement au sens du réglement (UE) 2016/679, op. cit., no 67, pp. 18 et 19 .

[١٨٠]- وفي هذا السياق تضرب إرشادات مجلس حماية البيانات الأوروبي- المشار إليها- مثالاً لكيفية تحقق المتحكم (الشركة) من توافر الرضاء المستنير لدى صاحب البيانات، متى تلقى

## الفرع الثالث

## التعبير عن الارادة المحددة بالموافقة

تتطلب احكام اللائحة الأوروبية لحماية البيانات حتى يكون التعبير عن الموافقة صحيحًا، توافر شروط عده منها ان يكون التعبير محددًا (spécifique)، وفقًا لما نصت عليه المادة (٤) بند (١١) من اللائحة. كما تؤكد المادة (٦/١/أ) المتعلقة بقانونية المعالجة على ضرورة أن تُعبِّر موافقة صاحب البيانات عن قبول معالجة بياناته الشخصية "لغرض واحد أو أكثر من الأغراض المحددة (pour une ou plusieurs finalités spécifiques)"، ولذا، يجب أن يكون لصاحب البيانات الحرية الكاملة في الموافقة أو الرفض لكل غرض من هذه الأغراض على حدة، مما يضمن أن تكون الموافقة طوعية ومبنية على اختيار واضح ومحدد لكل عملية معالجة[١٨١].

---

شكاوى حول عدم وضوح أغراض معالجة البيانات الواردة في طلب الحصول على الرضاء الخاص بأصحاب البيانات؛ إذ يتجه المتحكم نحو فحص مضمون المعلومات التي يوفرها في طلب الرضاء للتحقق مما إذا كانت مفهومة لصاحب البيانات، وتحقيقًا لهذا الغرض قد يلجأ المتحكم إلى إجراء اختبارات اختيارية لفئات محددة من عملائه، يُراعى في اختيارهم الحيادية والاستقلال وتنوع فئاتهم وعدم انحيازهم. وفي الوقت نفسه يقدم تحديثات جديدة لمعلومات الرضاء ويطرحها لعينة الاختبار قبل إصدارها للعامة، ومن خلال استبيان يعد لهذا الغرض يعبر أفراد عينة الاختبار عن مدى فهم المعلومات ووضوحها، ويستمر المتحكم في إجراء هذا الاختبار حتى تخلص النتائج إلى أن المعلومات أصبحت مفهومة لتكوين رضاء مستنير، ويعد المتحكم تقريرًا عن ذلك للرجوع إليه في المستقبل، وهو ما يفيده أيضًا في إثبات تلقي أصحاب البيانات لمعلومات واضحة قبل إصدار الرضاء على معالجة بياناتهم الشخصية من قبل المتحكم.

Lignes directrices 5/2020 sur le consentement au sens du réglement (UE) 2016/679, op. cit. et, no 71m p. 19, Exemple 12, no 73, p. 20 .

(181)- Lutomski, J., Rainey, L., Jong, M., Manders, P., & Broeders, M. (2023). Expanding the boundaries of previously obtained informed consent in research: views from participants in the personalised

(ISSN: 2537- 0758)

ووفقًا للمادة (٥/١/ب) من اللائحة الأوروبية لحماية البيانات، التي تتعلق بمبادئ معالجة البيانات الشخصية، فإن الحصول على موافقة صحيحة يتطلب بالضرورة أن يسبق ذلك تحديد أغراض محددة وصريحة ومشروعة ("finalités déterminées, explicites et légitimes") لجمع البيانات أو معالجتها.، هذا يعني أن المتحكم في البيانات ملزم بتحديد الغاية من المعالجة بشكل واضح قبل البدء في جمع البيانات أو معالجتها، وذلك لضمان الشفافية واحترام حقوق الأفراد، بما يتوافق مع مبادئ الحماية المقررة في اللائحة.

وقد عكس قانون حماية البيانات المصري هذا المبدأ، حيث اشترط في المادة (٦) بند (١) لمشروعية وقانونية معالجة البيانات، أن تكون موافقة الشخص المعني منصبة على "إجراء المعالجة من أجل تحقيق غرض محدد أو أكثر". كما منح القانون في المادة (٢) فقرة ثانية بند (٤) حقًا لصاحب البيانات في تخصيص نطاق المعالجة، بحيث يمكنه تحديد حدود استخدام بياناته وفقًا لما يراه مناسبًا، كذلك يشترط قانون حماية البيانات المصري، لجمع البيانات الشخصية ومعالجتها والاحتفاظ بها، "أن تجمع البيانات الشخصية لأغراض مشروعة (ومحددة) ومعلنة للشخص المعني" (م٣ بند ١ من القانون). ويتطابق موقف المشرع الإماراتي إلى حد كبير مع موقف المشرع المصري في هذا الشأن، حيث يتضح ذلك من مضمون نص الفقرة الثانية من المادة (٥) من قانون حماية البيانات الإماراتي.

### اولاً- مضمون الموافقة المحددة:

سبق أن أوضحنا أن الموافقة المحددة تُعد شرطًا جوهريًا لصحة الموافقة. ويعني ذلك أن الموافقة الصادرة عن صاحب البيانات لا يجوز أن تكون عامة أو غير محددة. بل يتعين على المتحكم تحديد محل الموافقة بدقة، من خلال بيان أغراض المعالجة ونطاقها، إضافة إلى توضيح النتائج المترتبة على هذه المعالجة.

risk-based mammascreening study. Health Expectations, 26(3), 1308-1317. https: //doi. org/10. 1111/hex. 13746 .Lignes directrices 5/2020, op. cit., no 65, p. 18.

ويستلزم توفر الموافقة المحددة أن يكون طلب الحصول عليها واضحًا ومفهومًا للشخص المعني، وأن ينصب على الجوانب المحددة لأنشطة المعالجة. هذا يضمن أن يكون الفرد على دراية كاملة بماهية البيانات التي ستتم معالجتها، ولأي غرض، وما هي العواقب المحتملة، مما يُعزز الشفافية ويضمن احترام حقوق الأفراد في التحكم ببياناتهم(١٨٢).

وفي هذا السياق، يرى جانب من الفقه الفرنسي(١٨٣) أن مبدأ تحديد الأغراض (principe de limitation des finalités) يُعد بمثابة "حجر الزاوية" لقانون حماية البيانات الشخصية. والسبب في ذلك أن العديد من مبادئ حماية البيانات تستمد وجودها من هذا المبدأ الأساسي، إذ يؤدي عدم الامتثال لمتطلباته إلى الإخلال تلقائي بالمبادئ الأخرى. ووفقًا لهذا الرأي، فإن تحديد الأغراض يشكل "النقطة المرجعية (point de référence) "التي يمكن من خلالها التحقق من قانونية المعالجة، وكفاية ودقة وملاءمة البيانات للأغراض المحددة، واحترام مبدأ الشفافية، ومدة الاحتفاظ بالبيانات ومدى تناسبها مع الغرض المعلن(١٨٤).

وبناءً على ذلك، يُنظر إلى مبدأ احترام الغرض المحدد للمعالجة على أنه المهيمن على دورة حياة البيانات الشخصية بأكملها، بدءًا من عملية جمع البيانات، ومرورًا بجميع مراحل معالجتها، وانتهاءً بمحوها المحتمل(١٨٥) عند انقضاء الغرض المحدد منها(١٨٦).

---

(182)- Drozd, O. op. cit, 14(9) .

(183)- Florence GAULLIER, Le principe de finalité dans le RGPD: beaucoup d'ancien et un peu de nouveau, communication commerce électronique, no 4, 2018, p. 1 .

(184)- A. DEBET, J. MASSOT et N. METALLINOS, op. cit., no 697 .

(١٨٥)– تأكيدًا على أهمية بيان الغرض من المعالجة، استخدمت اللائحة العامة لحماية البيانات (GDPR) مصطلح "الغرض "finalité مرة في أحكامها. راجع:
F. GAULLIER, Le principe de finalité dans le RGPD, op. cit., note 76, p. 2 .

(١٨٦)– وفقًا للمادة (٤) بند ٧ من قانون حماية البيانات المصري يلتزم المتحكم بـ "محو البيانات الشخصية لديه فور انقضاء الغرض المحدد منها، أما في حال الاحتفاظ بها لأي سبب من الأسباب المشروعة بعد انتهاء الغرض، فيجب ألا تبقى في صورة تسمح بتحديد الشخص المعني بالبيانات".

(ISSN: 2537- 0758)

علاوة على ذلك، يتطلب هذا الالتزام أن يكون الغرض من المعالجة محددًا بشكل واضح، بحيث لا يجوز أن يكون واسع النطاق أو مفصلاً بصورة مفرطة، كما لا ينبغي صياغته بطريقة غامضة أو مبهمة. الهدف الأساسي هو تمكين أصحاب البيانات من تحديد الأهداف الحقيقية للمعالجة وفهم العواقب المحتملة الناجمة عنها(١٨٧).

إن اشتراط أن تكون الموافقة "محددة" يهدف إلى ضمان درجة معينة من التحكم في استخدام البيانات الشخصية وتعزيز الشفافية لصاحب البيانات. لذلك، يجب على المتحكم إيلاء اهتمام خاص لتحديد الغرض أو الأغراض التي يتم جمع البيانات الشخصية من أجلها.

وبناءً على رأي فريق عمل "المادة ٢٩" في تقريره رقم ٢٠١٣/١٣ بشأن تحديد الغرض، فإنه لا يجوز للمتحكم جمع بيانات شخصية ليست ضرورية أو ذات صلة أو مناسبة للأغراض المحددة من المعالجة(١٨٨).

وفي الواقع، فإن التعبير عن غرض المعالجة بطريقة غامضة أو مبهمة يتعارض مع حق صاحب البيانات في الاعتراض الفعّال على معالجة بياناته لأغراض لم يكن على علم بها أو لم يقصدها منذ البداية(١٨٩). وبناءً على ذلك، أشار فريق عمل "المادة ٢٩" في رأيه المشار إليه إلى أن "الأغراض الغامضة أو العامة للمعالجة"، مثل، تحسين تجربة المستخدم، والأغراض التسويقية، و أغراض البحث المستقبلي، وأغراض الأمن المعلوماتي، دون تقديم تفاصيل إضافية واضحة، لا يمكنها عمومًا تلبية اشتراط أن تكون الموافقة محددة(١٩٠).

(187)- Benjamin BÉNÉZETH et all, Protection des données personnelles, Éditions Francis Lefebvre, Paris, 2018, p. 33.
(188)- Avis 3/2013 du groupe de travail "article 29" sur la limitation de la finalité, op. cit., p. 15.
(189)- B. BÉNÉZETH, Protection des données personnelles, op. cit., p. 33 .
(190)- Avis 3/2013 du groupe de travail "article" sur la limitation de la finalité, adopté le 2 avril 2013 (WP203), p. 16 .

**ثانياً- كيفية استيفاء اشتراط الموافقة المحددة**:

لا شك أن الحصول على موافقة "محددة "يتطلب إبلاغ أصحاب البيانات بشكل دقيق وواضح عن الأغراض المحددة لمعالجة بياناتهم. ويترتب على ذلك أن يكون لصاحب البيانات الحق في إبداء موافقته لكل غرض من الأغراض المحددة لمعالجة بياناته، بشكل منفصل ومستقل(١٩١). وهذا يعني أن الموافقة الصادرة عن صاحب البيانات ليست عامة أو مطلقة، وإنما هي موافقة خاصة ومحددة تنحصر في الغرض أو الأغراض التي تم تحديدها مسبقًا للمعالجة. وبناءً على ذلك، إذا رغب المتحكم في معالجة البيانات الشخصية لأغراض أخرى غير تلك التي تم الحصول على الموافقة بشأنها، يصبح من الضروري عليه أن يحصل على موافقة جديدة من صاحب البيانات لكل غرض من الأغراض الجديدة(١٩٢).

ويلتزم المتحكم في هذه الحالة بأن يتضمن كل طلب من طلباته الموافقة– الذي ينصب عليه كل غرض من أغراض المعالجة– معلومات محددة واضحة تتعلق بالبيانات التي تتم معالجتها بالنسبة لكل غرض على حدة. وذلك حتى يكون صاحب البيانات على دراية بالآثار المترتبة على اختياره(١٩٣).

وتأكيدًا لذلك، تنوه إرشادات مجلس حماية البيانات الأوروبي إلى الالتزامات التي تقع على عاتق المتحكم لكي تكون الموافقة محددة، فأشارت إلى أنه يجب عليه أن يضمن تحديد دقيق لأغراض المعالجة كضمانة تحول دون إساءة استخدامها، وبيان الطبيعة التفصيلية لطلب الحصول على الموافقة أو الرضاء، والفصل الواضح

(191)- POULLET, Consentement et RGPD: des zones d'ombre, op. cit., p. 7 .

(١٩٢)– د. بطيحي نسمة: المرجع السابق، ص ٧٤، وانظر أيضًا:

Cythia CHASSIGNEUX, L'encadrement juridique du traitment des données personnelles sur les sites de commerce en ligne, Thèse de doctorat, Université de Montréal, Paris, 2003, p. 150 .

(193)- Lignes directrices 5/2020 sur le consentement au sens du réglement (UE) 2016/79, op. cit., no 65, p. 17 .

(ISSN: 2537- 0758)

للمعلومات المتعلقة بالحصول على الموافقة بأنشطة معالجة البيانات عن المعلومات المتعلقة بأي مسائل أخرى(١٩٤).

على سبيل المثال، قد تقوم بعض مواقع الإنترنت بتجميع البيانات الشخصية لمستخدميها ومعالجتها ثم إرسالها إلى مواقع أخرى لأغراض الدعاية والتسويق. في هذه الحالة، يصبح من الضروري إبلاغ مستخدم الموقع بشكل شفاف ومحدد عن جميع العمليات التي تُجرى على بياناته داخل هذا الموقع. كما يتعين الحصول على موافقته الصريحة قبل الشروع في أي من هذه العمليات.

يمكن تحقيق ذلك من خلال وضع بيان خاص بحماية البيانات على الموقع، يوضح بوضوح الإجراءات التي يعتمدها الموقع لمعالجة بيانات المستخدمين، مع ذكر الغايات المحددة لهذه المعالجة.

وفي حال قام المستخدم بإدخال بياناته الشخصية على الموقع بعد اطلاعه على هذا البيان، وإبداء موافقته على الشروط والأحكام التي وضعها الموقع كشرط للاستفادة من خدماته أو تصفحه، فإن هذا يُعد موافقة صريحة ومستنيرة على معالجة بياناته الشخصية(١٩٥).

---

(194)- Lignes directrices 5/2020, op. cit., no 55, p. 16 .

(١٩٥)– في هذا الشأن، انظر: سامح عبد الواحد التهامي، ضوابط معالجة البيانات الشخصية، مرجع سابق، ص ٤١٢. كذلك تقوم بعض القنوات التليفزيونية الفضائية بالحصول على رضاء مشتركيها على جمع بياناتهم الشخصية، لتزويدهم باقتراحات شخصية لأفلام جديدة قد يرغبون في مشاهدتها، بناء على عادات المشاهدات لديهم، وبعد فترة قد ترغب القناة في تمكين أطراف أو شركات أخرى من إرسال (أو عرض) إعلانات مستهدفة للمشتركين استنادًا إلى عادات المشاهدة لديهم. ونظرً لوجود عرض جديد لجمع البيانات سيلزم الحصول على رضاء صاحب البيانات في هذه الحالة. انظر:

Lignes directrices 5/2020, op. cit., no 59, p. 17 .

## الفرع الرابع

## التعبير عن الارادة القاطعة بالموافقة

تتطلب اللائحة العامة لحماية البيانات (المادة ٤ بند ١١) لصحة الموافقة أن تكون قاطعة، أي واضحة ولا لبس فيها (univoque) وخالية من الغموض. وقد أكدت اللائحة أن الموافقة تتطلب صدور إعلان أو تصرف إيجابي واضح من صاحب البيانات، مما يعني أن الموافقة يجب أن تُمنح من خلال تصريح أو سلوك نشط (geste actif)، بحيث تدل بشكل لا يحتمل التأويل على موافقة صاحب البيانات على المعالجة المعنية[١٩٦].

وفي هذا السياق، يجدر الإشارة إلى أن المادة (٢/ح) من التوجيه الأوروبي رقم ٩٥/٤٦ (الملغي) لم تتضمن اشتراطًا بأن تكون الموافقة قاطعة، حيث كانت تُعرّف الموافقة على أنها تعبير عن الإرادة يقبل بموجبه صاحب البيانات معالجة بياناته الشخصية المتعلقة به. وقد حرصت اللائحة الأوروبية في المادة (٤) بند ١١ على تطوير هذا التعريف ومعالجة القصور في التعريف السابق، من خلال اشتراط أن يكون التعبير عن الإرادة قاطعًا (manifestation de volonté univoque)، وأن يتم عبر إعلان واضح أو تصرف إيجابي صريح.

وتعليقًا على موقف اللائحة الأوروبية، يشير البعض[١٩٧] إلى أن المناقشات التي دارت أثناء صياغتها ركزت على اختيار لفظ "قاطع" (univoque) لوصف التعبير عن الإرادة، واعتباره أكثر دقة وملاءمة مقارنة بمصطلح "عدم الغموض" (non ambigu) المستخدم في التوجيه الأوروبي رقم ٩٥/٤٦، أو مصطلح

(196)- Lignes directrices 5/2020 sur le consentement au sens du réglement (UE) 2016/79, op. cit., no 75, p. 20 .

(197)- C. DE TERQANGNE, Les principes relatifs au traitment des données à caractère personnel et à sa licéité, in C. TERWANFNE et K. ROSIER, Le réglement general de la protection des données, Analyse approfondie, op. cit., pp. 125 et s. Disponible sur le site: https: //pure unamur. be/ws/portalfiles, portal/54869646/8341. pdf

(ISSN: 2537- 0758)

"الصريح" (explicite)، الذي اعتمده المشرع الأوروبي في سياق بعض أنواع البيانات أو العمليات التي تجرى عليها.

ويُفهم من ذلك أن اللائحة تتطلب أن يكون التعبير عن الموافقة صادرًا بإعلان أو تصرف إيجابي واضح. وهذا يعني أن صاحب البيانات يجب أن يتخذ تصرفًا إراديًا يعبر بوضوح عن رضاه بالمعالجة المحددة، مما يضمن وضوح التعبير عن الموافقة ويزيل أي شك أو غموض حول وجودها(١٩٨).

ومع ذلك يكون للمتحكم الحرية في اختيار الطريقة المناسبة له للحصول على موافقة صاحب البيانات طالما كانت تتوافق مع اشتراطات اللائحة الأوروبية لحماية البيانات(١٩٩)، وفي المقابل يقع على عاتق المتحكم وضع آليات للحصول على الموافقة تكون واضحة لأصحاب البيانات، وتجنب أي غموض في هذا الشأن، وأن يكفل تمييز التصرف الذي يتم من خلاله التعبير عن الموافقة عن أي تصرف آخر لا يعد كاشفًا عنه. ولذلك، فإن مجرد استمرار المستخدم في التصفح العادي لأي موقع على الإنترنت، لا يعد تصرفًا إيجابيًا يستدل منه على تعبير صاحب البيانات عن موافقته عن عملية المعالجة المقترحة بشكل قاطع، كذلك لا يجوز اعتبار الموافقة العامة (بصورة إجمالية) على الشروط والأحكام العامة للموقع، تصرفًا إيجابيًا واضحًا تقوم به الموافقة على استخدام البيانات الشخصية(٢٠٠)، بل يجب على المتحكم تقديم

---

(198)- Lignes directrices 5/2020, op. cit., p. 20 .

(١٩٩)– مثل استخدام صاحب البيانات حركات معينة (سحب شريط على الشاشة، أو التلويح باليد أمام كاميرا ذكية) وهي أفعال إيجابية واضحة تشير إلى رضاء صاحب البيانات. ويجب أن يكون المتحكم قادرًا على إثبات حصول الرضاء من خلال هذه الطريقة، ويجب أيضًا أن يكون صاحب البيانات قادرًا على سحب موافقته بسهولة، في هذا الخصوص انظر:

Lignes drectrices 5/2020 sur le sonsentement au sens du réglement (UE) 2016/679, op. cit., no 93, p. 22; Noémie WEINBAUM, La prevue du consentement à l'ère du RGPD et de la blockchain, La semaine juridique, Entreprises et affaires, no 10. 2018, p. 30; Y. POULLET, Consentement et RGPD: des zones d'ombre, op. cit, p. 8 .

(200)- Lignes directrices 5/2020, op. cit., no 81 et no 84, pp. 21-22 .

طلب الموافقة في شكل واضح ويمكن الوصول إليه بسهولة وباستخدام لغة واضحة مفهومة(٢٠١).

وفي السياق الرقمي تتطلب العديد من الخدمات ضرورة الحصول على بيانات شخصية من المستخدم لاستخدامها أو لتحميلها، وقد يتلقى المستخدمون يوميًا طلبات عديدة للحصول على الرضاء يتعين عليهم الرد عليها بنقرة واحدة على خانة الموافقة، ولاشك أن هذا التعبير عن الإرادة قد يؤدي إلى إرهاق المستخدم وعزوفه في كثير من الأحيان عن قراءة المعلومات والشروط الخاصة بالرضاء، مما يشكل خطرًا كبيرًا على خصوصية أصحاب البيانات، ويثير بعض التخوفات حول مدى استيفاء مثل هذا التعبير لعناصر صحة الرضاء(٢٠٢).

ومن الممارسات الشائعة على الإنترنت إنشاء صفحات تتضمن سياسات خصوصية وأحكام وشروط مليئة بالبُنود، حيث يحرص المتحكم عادةً على إدراج بنود تمنحه أكبر قدر ممكن من الاستثناءات والمزايا. ومع ذلك، فإن زيادة عدد هذه النصوص وتعقيدها يؤدي غالبًا إلى تجاوز قدرة المستخدم العادي على فهم مضمونها. ونتيجة لذلك، يصبح من الشائع أن يُسجل مستخدم الإنترنت في الموقع أو التطبيق دون قراءة سياسة الخصوصية وأحكام وشروط الاستخدام(٢٠٣). وفي كثير من الأحيان، يصعب على المستخدم فهم نوعية البيانات الشخصية التي يُطلب منه

(٢٠١)– راجع: المادة (٢/٧) من اللائحة الأوروبية لحماية البياناتGDPR.

(٢٠٢)– ويرجع ذلك إلى الإشكاليات التي تثيرها المعاملات الإلكترونية؛ إذ يتعامل مستخدم الإنترنت مع نظام إلكتروني أو مع شخص (طبيعي أو اعتباري)، مما يستلزم في ظل هذا النظام وجود دليل كاف على الرضاء.

(٢٠٣)– يذهب البعض بحق إلى أن "صياغة سياسات خصوصية لطيفة أو عقود جميلة تصبح عديمة الفائدة إذا لم يقرأها أحد...". انظر:

Emmanuel NETTER, Sanction à 50 millions d'euros: au-delà de Google, La CNIL, s'attaque aux politique de confidentialité obscures et aux consentement creux, Dalloz IP/IT 2019, p. 165.

(ISSN: 2537- 0758)

الموافقة على جمعها ومعالجتها. بالإضافة إلى ذلك، قد لا تتوفر لديه القدرة على استيعاب تفاصيل المعالجة وتأثيراتها المحتملة عليه[٢٠٤].

وفي هذا السياق، يُلاحظ أن المستخدم غالبًا ما يقوم بـ"النقر (cliquer) "على خانة الموافقة دون إدراك أن هذا التصرف البسيط يمنح المتحكم صلاحية جمع ومعالجة بياناته الشخصية. ومع أن الموافقة التي يُعبر عنها من خلال "النقر" على زر القبول تُعتبر تصرفًا إراديًا، إلا أنها تتطلب وعيًا كافيًا من المستخدم ووقتًا للتروي للاطلاع على الشروط وسياسة الاستخدام المرتبطة بالمعالجة[٢٠٥]. ومع ذلك، يبدو أن العديد من أصحاب المواقع لا يولون اهتمامًا كافيًا لضمان أن زر الموافقة أو خانة القبول تُقدم بطريقة تتيح للمستخدم فهمًا كافيًا للمعالجة وشروطها.

وفي مواجهة هذا الأمر، تتطلب اللائحة الأوروبية من المتحكمين في البيانات تطوير حلول لهذه المشكلة في بيئة الإنترنت، عملاً على التأكد من أن موافقة مستخدم الإنترنت تقع قاطعَة لا لبس فيها، ولكنها أيضًا حرَّه ومستنيرَه وواضحَة، وتضرب إرشادات مجلس حماية البيانات الأوروبي مثالاً لحل هذه المشكلة يتمثل في الحصول على موافقة مستخدم الإنترنت من خلال ضبط إعدادات متصفحات الإنترنت الخاصة بالمستخدم، واشتراط الموافقة على كل غرض من أغراض المعالجة بصورة منفصلة[٢٠٦].

---

[٢٠٤]– في هذا الخصوص، راجع: رائد محمد فليح النمر، حماية خصوصية مستخدمي مواقع التواصل الاجتماعي على على ضوء التشريعات في مملكة البحرين، بحث منشور بمؤتمر الخصوصية في مجتمع المعلوماتية، طرابلس– لبنان، ١٩–٢٠ يوليو ٢٠١٩، مركز جيل البحث العلمي، سلسلة كتاب أعمال المؤتمرات، العام السابق، العدد ٢٦، يوليو ٢٠١٩، ص١٠٣.

[٢٠٥]– ويدلل البعض على ذلك بقوله: "يميل المستخدم على شبكة الإنترنت، أكثر من أي مكان آخر، إلى الجري مثل الثور الهائج عندما يمكنه الاستفادة من الخدمة". انظر:

E. NETTER, Sanction à 50 milions d'euros: au-delà de Google, op. cit., p.165

[206]- Lignes directrices 5/2020 sur le consentement au sens du réglement (UE) 2016/679, op. cit., no. 87-89, p. 22 .

- **وقت الحصول على موافقة صاحب البيانات:**

تشير إرشادات مجلس البيانات الأوروبي إلى أنه يجب الحصول على الموافقة مسبقًا قبل أن يبدأ المتحكم في معالجة البيانات الشخصية متى كانت الموافقة مطلوبًة لمشروعية المعالجة[٢٠٧]، وأكدت مجموعة عمل المادة (٢٩) مرارًا وتكرارًا في آرائها على وجوب صدور الموافقة قبل إجراء نشاط المعالجة[٢٠٨].

وعلى الرغم من أن تعريف الرضاء الوارد في المادة (١١/٤) من اللائحة الأوروبية ينص حرفيًا على وجوب صدور الموافقة قبل نشاط المعالجة، إلا أن هذا الأمر يُستفاد ضمنًا– في اللائحة الأوروبية والقانونين المصري والاماراتى– من اعتبار رضاء صاحب البيانات بمعالجة بياناته أحد شروط مشروعية المعالجة [٢٠٩]، وهو ما يعني ضمنيًا ضرورة وجود أساس قانوني سليم قبل بدء القيام بعملية معالجة البيانات، فإذا كانت الموافقة تنصب على غرض أو أغراض محددة لمعالجة البيانات، وتغير أي من هذه الأغراض بعد الحصول على الموافقة، أو إذا وجد غرض إضافي للمعالجة، فيجب الحصول على موافقة جديدة قبل إجراء هذه المعالجة.

نخلص مما تقدم إلى وجود حقيقة واضحة مفادها أنه لا يجوز جمع أو معالجة البيانات الشخصية دون موافقة صريحة من صاحب البيانات. ويجب أن تتوافر في هذه الموافقة مجموعة من العناصر المتكاملة التي تضمن صحتها وشرعيتها وفقًا لأحكام اللائحة الأوروبية لحماية البيانات. وتشمل هذه العناصر: حرية الإرادة، حيث يجب أن تكون الموافقة صادرة عن إرادة سليمة وخالية من أي ضغط أو إكراه، بحيث يتمتع صاحب البيانات بالحرية الكاملة في القبول أو الرفض. والتحديد، حيث يجب أن تكون الموافقة منصبة على بيانات معينة بعينها وأغراض معالجة محددة، مما

---

(207)- Lignes directrices 5/2020, op. cit., no 90, p. 23 .

(208)- Groupe de travail "article 29", Avis 15/2011 sur la definition du consentement, op. cit., pp. 34-36 .

(٢٠٩)– راجع المادة ١/٦ (أ) من اللائحة الأوروبية لحماية البيانات، وأيضًا والحيثية ٤٠ من اللائحة نفسها. وكذلك المادتين (٢ و ٦) بند ١ من قانون حماية البيانات الشخصية المصري.

(ISSN: 2537- 0758)

يضمن وضوح نطاق الموافقة وعدم تعميمها. والاستنارة، حيث ينبغي أن تكون الموافقة مبنية على علم مسبق وكافٍ بالغرض من جمع البيانات أو معالجتها، وبنتائج هذا النشاط. والوضوح والقطعية، حيث يجب أن يكون التعبير عن الموافقة قاطع الدلالة وخالٍ من أي لبس أو غموض، مما يدل بوضوح على قبول صاحب البيانات للمعالجة.

وعليه فان غياب أحد هذه العناصر يؤدي إلى عدم صحة الموافقة، والموافقة غير الصحيحة تجعل أي نشاط جمع أو معالجة للبيانات غير قانوني ويُعرض المتحكم للمساءلة بموجب أحكام اللائحة الأوروبية، و القوانين المختلفة.

ولا شك أن تشدد اللائحة الأوروبية في اشتراط وجود أربعة عناصر مجتمعة للرضاء، قد يكون رائدها هو تحقيق حماية خاصة للبيانات الشخصية للأفراد وخاصة في ظل المخاطر التي تواجهها عبر الإنترنت، ومع هذا قد يشكل اجتماع هذه العناصر في الرضاء نوعًا من التشدد، وقد يترتب عليها مشكلات عملية عد تطبيقها في بيئة الإنترنت مما قد يحد من الحصول على الرضاء في الواقع العملي، وقد تجعله غير ذى جدوى(٢١٠).

## المطلب الثانى

## شكل التعبير عن الموافقة على معالجة البيانات

لقيام الموافقة (الرضاء)، يتطلب القانون وجود إرادة صادرة عن شخص محدد. هذه الإرادة، باعتبارها أمرًا نفسيًا داخليًا، لا يعتد بها القانون ما لم تتجه إلى إحداث

(٢١٠)– يرى بعض الفقه الفرنسي أن اشتراط اللائحة توافر العديد من عناصر صحة الرضاء مجتمعة هو أمر مثير للدهشة، بالنظر إلى بعض القوانين الأخرى، مثل حماية المستهلك، رغم أنها تشترط الرضاء أيضًا إلا أنها تفرض كثيرًا من الاشتراطات النوعية لتوافره، كما يشير إلى أن هذه الاشتراطات التي تفرضها اللائحة لصحة الرضاء من شأنها أن تحد من اللجوء إلى الرضاء، كما يجب الاعتراف بأن اشتراط توافر كل هذه العناصر في الرضاء تجعله غير ذى جدوى. انظر:
Y. POULLET, Concentement et RGPD: des zones d'ombre!, op. cit., p. 10 .

أثر قانوني معين، ويتم إخراجها إلى العالم الخارجي بالتعبير عنها[٢١١]. ووفقًا لمبدأ الرضائية، لا يُشترط شكل أو وسيلة محددة للتعبير عن الإرادة[٢١٢]، حيث يتمتع الشخص بحرية اختيار الطريقة أو الكيفية التي يعبر بها عن إرادته، سواء كان ذلك شفويًا، كتابيًا، أو حتى ضمنيًا. و يمكن أن يكون التعبير عن الإرادة صريحًا، من خلال وسائل واضحة كالتصريح الشفوي أو الكتابي. وضمنيًا مستخلصًا من سلوك الشخص أو موقفه، وحتى في بعض الحالات من السكوت (وفقًا للمادة ٩٠ من القانون المدني المصرى، والفقرة الثانية من المادة رقم ١٣٥ من قانون المعاملات المدنية الاماراتى)، بشرط عدم وجود نص قانوني أو اتفاق يشترط التعبير الصريح[٢١٣].

بيد أن هذه المسألة تأخذ بعدًا مختلفًا بعض الشئ في إطار الموافقة أو الرضاء بعمليات معالجة البيانات، إذ تضع التشريعات المنظمة لحماية البيانات حدودًا معينة لشكل التعبير عن موافقة صاحب البيانات، ويتمثل ذلك بوجه خاص في اشتراط التعبير الصريح عن الموافقة، وهو ما يثير التساؤل حول صحة التعبير الضمني أو حتى صلاحية التصرفات السلبية مثل السكوت ومدى دلالته في التعبير عن الموافقة أوالرضاء في البيئة الرقمية، ومن هنا يكون من المناسب تناول هذه المسائل الثلاث، ونوضح كل ذلك فى الفروع الاتية.

---

(٢١١)– انظر في هذا الموضوع بصفة عامة، د. سليمان غانم، في النظرية العامة للالتزام، مرجع سابق، ص ٨٠ وما بعدها: د. عبد الرزاق السنهوري، مرجع سابق، فقرة ٧٥، ص ١٤٥ وما بعدها؛ محمد حسن قاسم، مرجع سابق، ص ١٠٣ وما بعدها.

(٢١٢)– راجع: د. سليمان غانم، المرجع السابق، ص ٨٠.

(٢١٣)– راجع: د. جلال على العدوي، أصول الالتزامات، مصادر الالتزامات، مشأة المعارف، الإسكندرية، ١٩٩٧، ص ص ٨٩، ٩٠. و انظر: د. محمد حسن قاسم، مرجع سابق، ص١٠٥؛ د. محمد حسام محمود لطفي، مرجع سابق، ص ٣٢.

(ISSN: 2537- 0758)

## الفرع الاول

## التعبير الصريح عن الارادة بالموافقة

التعبير الصريح- بوجه عام- هو اتخاذ الإرادة مظهرًا يفصح بذاته وبطريقة مباشرة عن هذه الإرادة حسب المألوف عند الناس، أيًا ما كان السبيل الذي يتخذه هذا التعبير[٢١٤]، وللتعبير الصريح وسائل عدة، فقد يكون باللفظ أو الكتابة أو الإشارة المتداولة عرفًا أو باتخاذ موقف لا تدع ظروف الحال شكًا في دلالته على حقيقة المقصود (م ١/٩٠ مدني مصرى و المادة رقم ١٣٢ من قانون المعاملات المدنية الاماراتى).

وبذلك يُعد التعبير الصريح عن الإرادة وسيلة مباشرة وواضحة للكشف عن اتجاه إرادة صاحب التعبير دون الحاجة إلى تفسير إضافي أو دعم خارجي. ويُفترض أن يحمل هذا النوع من التعبير دلالة ذاتية قاطعة تكفي بذاتها لتوضيح ما تنطوي عليه النفس من موافقة وإرادة، دون الحاجة إلى استيضاح أو ترجيح لما قد يُفهم من ذلك التعبير[٢١٥].

ولا يخرج الأمر عن هذا الإطار في سياق حماية البيانات، إذ يشترط قانون حماية البيانات المصري، وجود موافقة صريحة من المستخدم قبل جمع بياناته أو معالجتها، وكذلك قبل استخدامها (مادة ٢ من القانون المصرى). وقد أكد المشرع على هذا الشرط بشكل خاص فيما يتعلق بالبيانات الشخصية الحساسة. ويُلاحظ أن المشرع المصري قد استلهم نهجه في هذا الصدد من اللائحة الأوروبية لحماية

---

[٢١٤]- انظر: د. جميل الشرقاوي، النظرية العامة للالتزام، مصادر الالتزام، دار النهضة العربية، القاهرة، ١٩٩٥، ص ٨٦؛ د. محمد حسن قاسم، مرجع سابق، ص ١٠٥؛ وانظر أيضًا: د. عبد الرزاق السنهوري، مرجع سابق، ص ٧٦، ص ١٤٦. حيث يشير البعض إلى أن التعبير عن الإرادة يكون صريحًا إذا كان المظهر الذي اتخذه مزهرًا موضوعيًا في ذاته للكشف عن هذه الإرادة حسب ما هو مألوف بين الأفراد.

[٢١٥]- د. جلال على العدوي، مرجع سابق، ص ٩٧.

البيانات، غير أنه لم يقدم تعريفًا واضحًا لماهية الموافقة الصريحة في هذا السياق. و يقترب الى حدا ما موقف القانون الاماراتى فى هذا الشأن من موقف المشرع المصرى حيث يستخلص لزوم التعبير الصريح من نصوص المواد ارقام ١، و ٢، و ٦، و من القانون الاماراتى.

وفى اطار ما تقدم نوضح القواعد الحاكمة للتعبير الصرح عن الموافقة للمعالجة الرقمية للبيانات فى اللائحة الاوربية و فى القانونين المصرى والاماراتى كما يلى:

## أولاً: القواعد الحاكمة للتعبير الصريح للموافقة على معالجة البيانات فى اللائحة الأوروبية لحماية البيانات:

**١- ضرورة التعبير عن الإرادة من خلال إعلان أو تصرف إيجابي واضح:**

نظرًا لأهمية حماية البيانات الشخصية، حرص المشرع الأوروبي في اللائحة العامة لحماية البيانات (GDPR) على فرض وسيلة محددة للتعبير عن الإرادة في المادة (٤)، البند ١١. وقد تبنى قانون المعلوماتية والحريات الفرنسي المعدل هذا النهج في المادة ٢ (الفقرة الأخيرة)، حيث اشترط أن تُفرغ الإرادة في صورة تصريح أو فعل إيجابي واضح (déclaration ou un acte positif clair) يُعبر من خلاله صاحب البيانات عن موافقته على معالجة بياناته الشخصية. ويُفهم من ذلك أن الموافقة يجب أن تكون دائمًا في شكل تعبير صريح، واضح الدلالة، بحيث لا يدع مجالًا للشك في موافقة صاحب البيانات على المعالجة المقصودة[٢١٦].

لا شك أن التعبير الإيجابي عن الإرادة يُشير إلى أي إعلان أو تصرف أو فعل إيجابي يحمل دلالة قاطعة على اتجاه الإرادة نحو إحداث أثر قانوني[٢١٧]. وتكمن أهمية هذا التعبير في قدرته على إظهار الإرادة بشكل ملموس للعالم الخارجي، بما

---

[216]- Drozd, O., op. cit, p .٥١٥ Kyi, L. (2024). “it doesn’t tell me anything about how my data is used”: user perceptions of data collection purposes., 1-12. https: //doi. org/10. 1145/3613904. 3642260 .

[٢١٧]- د. جلال على العدوي، مرجع سابق، ص ٩٠.

(ISSN: 2537- 0758)

يُمكن الغير من التعرف عليها. ويتم هذا الإظهار بأي وسيلة تملك المدى الكافي لتحقيق الغرض من التعبير عن الإرادة.

ويُقصد بالتصرف الإيجابي الواضح (acte positif clair) كما ورد في أحكام اللائحة الأوروبية لحماية البيانات، أن تصدر الموافقة على المعالجة المحددة بناءً على تصرف إرادي واعٍ (acte délibéré) من صاحب البيانات[٢١٨]. وقد أشارت الحيثية رقم (٣٢) من اللائحة إلى أن هذا التصرف الإيجابي يمكن أن يتخذ صورًا متعددة، منها التعبير كتابةً أو شفهيًا (مسجل)، بما في ذلك الوسائل الإلكترونية. وتُعد الوسيلة الأكثر دقة للوفاء بمعيار "التعبير الصحيح" أن يُفرغ صاحب البيانات إرادته في خطاب أو بريد إلكتروني يُوجه إلى المتحكم يُوضح فيه مضمون الموافقة بدقة.

ومع ذلك، يندر تطبيق هذا الأسلوب في الممارسة العملية، نظرًا لتنوع صور التعبير عن الموافقة الصريحة بما يتوافق مع أحكام اللائحة الأوروبية[٢١٩]. وتشمل هذه الصور، على سبيل المثال، التوقيع الإلكتروني، النقر على خانة الموافقة عند زيارة الموقع الإلكتروني، إرسال رسالة بريد إلكتروني لتأكيد الموافقة، أو أي تعبير أو سلوك آخر يُظهر بوضوح موافقة صاحب البيانات على المعالجة المقترحة لبياناته الشخصية[٢٢٠].

---

(218)- Lignes directrices 5/2020, op. cit., no 77 et 78, p. 21 .

(219)- Lignes directrices 5/2020, op. cit., no 77 et 78, p. 21 et s .

(٢٢٠)– كذلك اعترفت الحيثية رقم ١٧ من التوجيه الأوروبي بشأن: "الخصوصية والاتصالات الإلكترونية" صراحة بقبول الإجراءات التي تنطوي على فعل إيجابي من قبل الشخص المعني، بقولها: "يجوز التعبير عن الرضاء بأي طريقة مناسبة تتيح للمستخدم التعبير عن رغباته بحرية وبطريقة محددة ومستنيرة، من ضمنها وضع علامة على الخانة المخصصة لذلك بأحد مواقع الويب التي يتصفحها". ويتماشى هذا التفسير مع جوهر تشريعات الاتحاد الأوروبي بشأن التجارة الإلكترونية والاستخدام الواسع للتوقيعات الإلكترونية، والتي تطلبت من الدول الأعضاء تعديل قوانينها الوطنية لاستيعاب الكتابة والمحررات والتوقيعات الإلكترونية ومنحه الحجية في الإثبات مثل المحررات الورقية. في هذا الصدد، انظر:

وسندا لما سبق تقضى الحيثية رقم (٣٢) من اللائحة الأوروبية بأن التعبير عن الموافقة يجب أن يتم من خلال تصرف إيجابي واضح. ويمكن تحقيق ذلك، على وجه الخصوص، عبر وضع علامة في خانة الاختيار (case à cocher) عند زيارة موقع إلكتروني، أو من خلال اختيار معايير تقنية معينة تتعلق بخدمات مجتمع المعلومات، أو عن طريق أي سلوك آخر يُظهر بوضوح في هذا السياق قبول صاحب البيانات بالمعالجة المقترحة لبياناته الشخصية[٢٢١].

وذلك في حين اعتبرت اللائحة الأوروبية العامة لحماية البيانات(GDPR) وضع المستخدم علامة في خانة الاختيار على الموقع الإلكتروني إحدى الوسائل المعتمدة للحصول على الموافقة، فقد جاء حكمها مرنًا بما يسمح بتحقيق هذا الغرض عبر أي وسيلة تتيح للمستخدم التعبير عن إرادته بوضوح وبشكل لا لبس فيه. ومن الأمثلة على ذلك، قيام المستخدم بنشر تعليقات على مدونة إلكترونية، بما يُعد تعبيرًا صريحًا عن موافقته على معالجة بياناته الشخصية. ودون الإخلال بأحكام القواعد العامة للعقد الواردة في التشريعات الوطنية الحالية لدول الاتحاد الأوروبي، يمكن الحصول على الموافقة من خلال تعبير شفوي مسجل. ومع ذلك، يُشترط أن يكون صاحب البيانات قد تم اطلاعه على المعلومات المتاحة له بشكل كامل قبل أن يصدر موافقته، لضمان وعيه التام بطبيعة المعالجة المقترحة وآثارها[٢٢٢].

هذا وقد أشارت مجموعة العمل المعنية بالمادة ٢٩ التابعة للمجلس الأوروبي، في تفسيرها لنص المادة الثانية من التوجيه الأوروبي رقم ٩٥/٤٦ المتعلق بحماية البيانات الشخصية (الملغي)، إلى أن الكتابة ليست شرطًا لصحة موافقة صاحب

---

Groupe de travail "article 29", avis 15/2011, op. cit., p. 29 .

(221)- Roman-Martinez, I., Calvillo-Arbizu, J., Mayor-Gallego, V., Madinabeitia-Luque, G., Estepa, A., & Estepa, R. (2023). Blockchain-based service-oriented architecture for consent management, access control, and auditing. Ieee Access, 11, 12727-12741. https: //doi. org/10. 1109/access. 2023. 3242605 .

(222)- Lignes directrices 5/2020, op. cit., no 77 et 78, p. 21 .

(ISSN: 2537- 0758)

البيانات. ويُفهم من ذلك أن الموافقة يمكن أن تصدر بشكل شفهي، حيث أوضحت أن صياغة المادة الثانية (البند (ح) الخاص بتعريف الموافقة) من هذا التوجيه لا تتضمن أي نص يلزم بتوافر شكل محدد للتعبير عن الإرادة[٢٢٣].

**٢- وجوب أن تكون موافقة صاحب البيانات صريحة في حالات معينة:**

تُشترط اللائحة الأوروبية أن تكون الموافقة صريحة (Consentement Explicite) في بعض الحالات التي تنطوي على مخاطر جسيمة على حماية البيانات الشخصية، وتتطلب مستوى عالٍ من التحكم في هذه البيانات من قبل صاحبها. ويتضح من نصوص اللائحة أن الموافقة الصريحة تعد ضرورية على نحو خاص في معالجة البيانات الحساسة (المادة ٢/٩، بند أ)، وفي الأحكام المتعلقة بنقل البيانات إلى بلدان أو منظمات خارج الاتحاد الأوروبي (المادة ١/٤٩، بند أ). كما تُعتبر الموافقة الصريحة مطلوبة في حالة اتخاذ القرارات الفردية الآلية، بما في ذلك التمنيط (المادة ٢/٢٢، بند ج).

وفي سبيل توضيح المقصود بالموافقة الصريحة، أشارت إرشادات مجلس حماية البيانات الأوروبي إلى أن مصطلح "صريحة (explicite) "يتعلق بالطريقة التي يُعبّر بها صاحب البيانات عن موافقته. ويعني ذلك أن صاحب البيانات يجب أن يُقدّم تعبيرًا واضحًا ومحددًا عن الموافقة. ومن بين الوسائل الأكثر ملاءمة لضمان الحصول على هذه الموافقة الصريحة هو التعبير عنها بشكل كتابي. كما يمكن للمتحكم، عند الضرورة، أن يسعى للحصول على توقيع صاحب البيانات على وثيقة كتابية تُثبت الموافقة الصريحة، مما يُسهم في تقديم دليل قاطع على وجودها، ويُقلّل من احتمالية إثارة أي منازعات بشأن صحتها أو وجودها[٢٢٤].

(223)- Groupe de travail "article 29", avis 15/2011, op. cit., pp. 28-29 .

(224)- Lignes directrices 5/2020, op. cit., no 93, p. 24; Groupe de travail "article 29", avis 15/2011, sur la définition du consentement, op. cit., p.28 .

ومن المهم الإشارة إلى أن الوثيقة الموقعة ليست الوسيلة الوحيدة للحصول على الموافقة الصريحة، ولا يمكن الادعاء بأن اللائحة الأوروبية العامة لحماية البيانات (GDPR) تشترط أن يكون التعبير في جميع الحالات كتابيًا وموقعًا. فوفقًا لمتطلبات الموافقة الصريحة، يمكن تحقيق ذلك بوسائل أخرى تتلاءم مع السياق، خاصة في البيئة الرقمية أو عبر الإنترنت. على سبيل المثال، يمكن لصاحب البيانات تقديم التعبير اللازم من خلال ملء نموذج إلكتروني، أو إرسال بريد إلكتروني يتضمن إقرارًا صريحًا بقبوله معالجة فئات معينة من البيانات، أو عن طريق رفع مستند يحمل توقيعه الخطي باستخدام الماسح الضوئي (Scanner)، أو استخدام التوقيع الإلكتروني[٢٢٥].

**بالإضافة إلى ذلك**، يمكن توفير خانة اختيار مخصصة للموافقة على معالجة البيانات الحساسة، أو اشتراط تأكيد إضافي من صاحب البيانات من خلال النقر على رابط محدد يتم إرساله عبر البريد الإلكتروني، كوسيلة للتحقق من موافقته على المعالجة بعد تعبيره عنها للمرة الأولى. هذه الوسائل تُظهر تنوع الطرق التي يمكن اعتمادها لتلبية اشتراطات الموافقة الصريحة وفقًا للائحة[٢٢٦].

ومن الناحية النظرية، يمكن أن يكون التعبير الشفهي كافيًا لتحقيق الموافقة الصريحة، بشرط أن يُستوفي جميع شروط صحة الموافقة. ومع ذلك، قد يكون من الصعب على المتحكم إثبات توافر هذه الشروط في حالة استخدام التعبير الشفهي،

---

[٢٢٥]– انظر: شريف فهمى بدوي، معجم مصطلحات الكمبيوتر والإنترنت والمعلوماتية، مرجع سابق، ص ٣٤٥.

- Lignes directrices 5/2020, op. cit., no 94, p. 24 .Clifford, D., Graef, I., & Valcke, P. (2018). Pre-formulated declarations of data subject consent citizen-consumer empowerment and the alignment of data, consumer and competition law protections. SSRN Electronic Journal. https: //doi. org/10. 2139/ssrn. 3126706 .

(226)- CNIL, Conformité RGPD: comment recueillir le consentement des personnes?, 3 août 2018, disponible sur le site: https: /www. cnil. fr/fr/les-legalesconsentement .

(ISSN: 2537- 0758)

إلا إذا تم تسجيل التعبير عن الإرادة بوسيلة تضمن موثوقيته. على سبيل المثال، يجوز لمنظمة أو شركة أن تحصل على موافقة صريحة من خلال محادثة هاتفية مع صاحب البيانات، بشرط تمكينه من اختيار الموافقة أو الرفض بطريقة نزيهة وواضحة، مع الحصول على تأكيد محدد منه، مثل الضغط على زر أثناء المكالمة أو تقديم تأكيد شفهي(٢٢٧).

وتُشير إرشادات مجلس حماية البيانات الأوروبي إلى أنه يمكن للمتحكم الحصول على موافقة صريحة من زائر لموقعه الإلكتروني من خلال عرض شاشة مخصصة تحتوي على خانات اختيار مرفقة بكلمتي "نعم" للموافقة أو "لا" للرفض. ويُشترط أن تكون المعلومات المقدمة واضحة وتحدد بجلاء أن الموافقة تتعلق بمعالجة البيانات الشخصية. على سبيل المثال، يمكن استخدام عبارة مثل: "أوافق بموجب هذا على معالجة بياناتي"، في حين لا تُعد عبارة مثل، "أنا على علم بأنه ستتم معالجة بياناتي" كافية لأنها تفتقر إلى الدلالة القاطعة على الموافقة الصريحة(٢٢٨).

بالإضافة إلى ذلك، يجب أن تُستوفى جميع الشروط الأخرى اللازمة للحصول على موافقة صحيحة، مثل شرط الحصول على موافقة مستنيرة(٢٢٩). وفي المقابل، يحق لصاحب البيانات رفض الإجابة على الأسئلة المتعلقة ببياناته الشخصية أثناء عملية الجمع، إذا كانت هذه الأسئلة غير إلزامية. كما يحق له رفض تقديم الموافقة

(227)- Fox, G., Lynn, T., & Rosati, P. (2022). Enhancing consumer perceptions of privacy and trust: a gdpr label perspective. Information Technology and People, 35(8), 181-204. https: //doi. org/10. 1108/itp-09-2021-0706. Fukui, N. (2024). Mixed methods approach to examining the implementation experience of a phone-based survey for a sars-cov-2 test-negative case-control study in california. Plos One, 19(5), e0301070. https: //doi. org/10. 1371/journal. pone. 0301070. Lignes directrices 5/2020, op. cit., no 95, p. 24.

(228)- Groupe de travail "article 29", avis 15/2011, op. cit., pp. 24-25 .

(229)- Tona, O., Someh, I., Mohajeri, K., Shanks, G., Davern, M., Carlsson, S., … & Kajtazi, M. (2018). Towards ethical big data artifacts: a conceptual design. . https: //doi. org/10. 24251/hicss. 2018. 571. Lignes directrices 5/2020, op. cit., Exemple 17, no 96, p. 24 .

الكتابية الصريحة المطلوبة لمعالجة البيانات الحساسة. أما في السياق الرقمي، يمكن لصاحب البيانات ببساطة اختيار الرفض من خلال خانة الاختيار المخصصة لذلك ضمن نموذج جمع البيانات على الموقع الإلكتروني[٢٣٠].

**ثانياً: موقف القانونين المصري و الاماراتى:**

ميز المشرع المصري، فيما يتعلق بصور التعبير عن الموافقة، بين "البيانات الشخصية الحساسة" وغيرها من البيانات الشخصية التي يمكن وصفها– بمفهوم المخالفة– بأنها عادية أو غير حساسة. وتأتي هذه التفرقة استنادًا إلى الطبيعة الخاصة للبيانات الحساسة، التي تتطلب درجة أعلى من الحماية القانونية، مما ينعكس في اشتراطات أكثر صرامة عند الحصول على موافقة صاحب البيانات لمعالجتها. في حين قد تكون الإجراءات المطلوبة للتعبير عن الموافقة على معالجة البيانات العادية أقل تعقيدًا. وان كان المشرع الاماراتى قد ميز بين الانواع المختلفة للبيانات الا انه لم ينص صراحة على التمييز بينهم فى صور التعبير عن الموافقة بشأن معالجتهم. **ونوضح كل ذلك فيما:**

**١– صور التعبير عن الموافقة في حالة البيانات الشخصية غير الحساسة:**

رغم تعدد وسائل التعبير عن الإرادة، كما ورد في المادة (٩٠) من القانون المدني المصرى، فإن المشرع المصري في قانون حماية البيانات الشخصية اكتفى باشتراط الحصول على "الموافقة الصريحة" من الشخص المعني بالبيانات كشرط أساسي لجمع ومعالجة البيانات (المادة ١/٢ من القانون)، واعتبرها متطلبًا أوليًا لقانونية ومشروعية المعالجة (المادة ٦، بند ١ من القانون). مع ان المشرع الامارتى لم يميز فى احكام الموافقة على المعالجة بين الموافقة على معالجة البيانات الشخصية العادية والموافقة على معالجة البيانات الحساسة.

---

(٢٣٠)– رائد محمد فليح النمر، حماية خصوصية مستخدمي مواقع التواصل الاجتماعي...، مرجع سابق، ص ١٠٢.

(ISSN: 2537- 0758)

ولـم يـنص القـانون المـدنى المصـرى علـى صـورة محـددة تُفـرغ فيهـا الموافقـة الصريحة، مما يتيح للشخص حرية اختيار الوسيلة أو الشكل الذي يعبر من خلاله عن إرادته، بشرط أن يُقصد من هذا التعبير إحاطة الغير علمًا بإرادته. ويمكن أن يكون التعبير شفويًا أو كتابيًا، بصرف النظر عن العبارات أو الصورة المستخدمة، سواء كان ذلك من خلال وسيلة شخصية، مثل خطاب أو برقية، أو وسيلة غير شخصية، مثل إعلان أو نشرة، أو حتى بالإشارة التي تحمل دلالة مفهومة[٢٣١].

وعدم اشتراط قانونى حماية البيانات المصرى والاماراتى لشكل معين قد يُفسر بأن الموافقة الشفوية كافية من الناحية القانونية لتلبية متطلبات مشروعية المعالجة. ومع ذلك، يظل التوثيق الكتابي ذا أهمية كبيرة من ناحية الإثبات، إذ يتحمل القائم بالمعالجة عبء إثبات توافر الموافقة الصريحة إذا دعت الحاجة.، خاصة وان قانون حماية البيانات الاماراتى قد قرر فى الفقرة الاولى من المادة السادسة منه، ان من شروط صحة الموافقة أن يكون المتحكم قادراً على إثبات موافقة صاحب البيانات في حال كانت المعالجة مبنية على موافقة صاحب البيانات لمعالجة بياناته الشخصية. وهذا يفيد بانه رغم ان الموافقة ليس لها شكل محدد ولكن على المتحكم عبء اثباتها خاصة عندما يكون تكون الموافقة محل نزاع[٢٣٢].

---

[٢٣١]– محمود جمال الدين زكى، مرجع سابق، ص ٢٩.

[٢٣٢]– هذا وتلعب التطورات التكنولوجية و خاصة الرقمية دورا هاما فى توفير وسيلة الاثبات المناسبة لوجود الموافقة على معالجة البيانات، مثل تقنية ساسلة الكتل blockchain، وكذلك مايسمى بالموافقة الديناميكية أو المتحركة او النسبية consent mechanisms. انظر فى تفاصيل ذلك:

Roman-Martinez, I., Calvillo-Arbizu, J., Mayor-Gallego, V., Madinabeitia-Luque, G., Estepa, A., & Estepa, R. (2023). Blockchain-based service-oriented architecture for consent management, access control, and auditing. Ieee Access, 11, 12727-12741. https: //doi. org/10. 1109/access. 2023. 3242605 .

وقد كان من الأوفق اشتراط الكتابة للتعبير عن إرادة صاحب البيانات، باعتبارها من أهم سائل التعبير عن الإرادة لما يميزها من ثبات وتحديد يقلل كثيرًا من فرص المنازعة بشأن دلالتها والمقصود منها(٢٣٣).

ورغم أن المشرع المصري لم يشترط إفراغ الموافقة في شكل مكتوب بالنسبة للبيانات الشخصية، إلا أنه من المتوقع أن يحرص المسؤول عن البيانات،– سواء أكان المتحكم أو المعالج،–على الحصول على هذه الموافقة في صورة مكتوبة. ويعود هذا الحرص إلى أهمية ضمان نسبتها إلى صاحبها وتيسير عملية إثباتها. وعادةً ما تُعد نماذج محددة لإفراغ هذه الموافقة، بما يتوافق مع الضوابط التي يحددها القانون.

كما يُمكن إفراغ الموافقة بوسائل إلكترونية، بشرط أن تتيح هذه الوسائل القدرة على إظهار الإرادة بوضوح. ومن الأمثلة على ذلك، الموافقة المتاحة عبر صفحات المواقع الإلكترونية، ووسائل التواصل الاجتماعي، أو التطبيقات الإلكترونية على الهواتف المحمولة. وتعد هذه الوسائل كافية طالما توافر اليقين المطلوب لإثبات صدور الموافقة عن صاحب البيانات(٢٣٤).

**٢– صور التعبير عن الموافقة في حالة البيانات الشخصية الحساسة:**

كما سبق بيانه، فإن التعبير عن إرادة صاحب البيانات لا يتقيد، كقاعدة عامة، بطريقة معينة أو بشكل محدد. ومع ذلك، خرج المشرع المصري عن هذا الأصل في حالة البيانات الشخصية الحساسة(٢٣٥)، حيث اشترط صراحةً الحصول على موافقة

---

(٢٣٣)– انظر: د. محمد حسن قاسم، مرجع سابق، ص ١٠٤.

(234)- Roman-Martinez, I., Calvillo-Arbizu, J., Mayor-Gallego, V., Madinabeitia-Luque, G., Estepa, A., & Estepa, R, op. cit., pp, 12727-12741 .

(٢٣٥)– وفق نص المادة الاولى من قانون حماية البيانات الشخصية المصري رقم ١٥١ لسنة ٢٠٢٠، "البيانات الحساسة" هي البيانات المتعلقة بالأصل العرقي، أو الآراء السياسية، أو المعتقدات الدينية أو الفلسفية، أو الصحة، أو الحياة الجنسية، أو الجرائم، أو البيانات الأمنية، بالإضافة إلى أي بيانات أخرى يعتبرها القانون حساسة بطبيعتها أو تتعلق بحقوق وحريات الأفراد.

(ISSN: 2537- 0758)

كتابية صريحة من الشخص المعني لجمع هذه البيانات أو نقلها أو تخزينها أو حفظها أو معالجتها أو إتاحتها.

ويمكن تبرير هذا الاشتراط بخصوصية البيانات الحساسة وأهميتها البالغة، إذ ترتبط بأدق تفاصيل حياة الشخص، مما يجعل حمايتها من أي اعتداء أو إساءة استخدام ضرورة مُلحّة. ويُعد هذا التشدد في الإجراء ضمانة إضافية لصيانة حقوق الأفراد وحماية خصوصياتهم، بما يتماشى مع طبيعة هذه البيانات الحساسة التي قد يؤدي المساس بها إلى انتهاك خطير للحقوق الشخصية.

وإذا كان المشرّع قد ميّز بين البيانات الشخصية والبيانات الشخصية الحساسة، فقد زاد في حالة الأخيرة باشتراط– إلى جانب الموافقة الصريحة– أن تصدر هذه الموافقة في صورة "كتابية". وهذا الشرط يقطع بما لا يدع مجالاً للشك في ضرورة الكتابة عند إصدار الموافقة على معالجة وجمع هذه البيانات. وبمفهوم المخالفة، لا يجوز أن يكون التعبير عن الإرادة في هذا السياق باللفظ أو الإشارة.

ورغم تقدير أهمية التعبير عن إرادة صاحب البيانات من خلال الكتابة، إلا أن القانون لم يحدد بشكل دقيق مضمون الشكل الكتابي للموافقة الصريحة. فالكتابة قد تكون رسمية أو عرفية، وقد تأتي في صورة خطية أو تأخذ أي شكل إلكتروني. وبالتالي، فإن هذا المصطلح يشمل أي صياغة أو ألفاظ تعبّر بشكل واضح وصريح عن إرادة الشخص[٢٣٦].

وهنا ينبغي التوقف لتأمل موقف المشرّع المصرى، إذ إن القانون رقم ١٥١ لسنة ٢٠٢٠ بشأن إصدار قانون حماية البيانات الشخصية قد أشار في صدر أحكامه، وخاصة في المادة الأولى من مواد الإصدار، إلى تحديد نطاق تطبيق أحكامه فيما يتعلق بحماية البيانات الشخصية التي تُعالَج إلكترونيًا، سواء جزئيًا أو كليًا، لدى أي حائز أو متحكم أو معالج لها. وكان من المناسب، في تقديري، أن تكون الكتابة

[٢٣٦]– في هذا المعنى، انظر: د. جلال على العدوى، مرجع سابق، ص ٩٠.

المطلوبة لموافقة صاحب البيانات من طبيعة البيانات نفسها، أي أن تكون كتابة إلكترونية تتماشى مع المعالجة الإلكترونية للبيانات[٢٣٧].

ويُعزّز هذا التوجه أن الكتابة الإلكترونية تتمتع بنفس حجية الكتابة الورقية في الإثبات،- وفقًا لقانون التوقيع الإلكتروني المصرى رقم ١٥ لسنة ٢٠٠٤، والقانون الاتحادي الاماراتى رقم ١ لسنة ٢٠٠٦ بشأن المعاملات والتجارة الإلكترونية والقانون الاماراتى الاتحادي رقم ١٤ لسنة ٢٠٢٠ بشأن المعاملات الإلكترونية وخدمات الثقة-، شريطة استيفائها الشروط الفنية والقانونية المطلوبة. ومع ذلك، فإن إطلاق المشرّع لعبارة "كتابي" دون تحديد نوع معين للكتابة، يمكن أن يُفهم على أنه يشمل كلا النوعين: الكتابة الورقية والإلكترونية، وهو ما يستدعي تفسير النص تفسيرًا واسعًا يضمن التناسق مع تطورات العصر ومتطلبات التقنية.

ومن ناحية أخرى، وقع المشرّع المصرى فى تناقضًا قانونيًا ملحوظًا في نص المادة (١٢) من القانون، حيث اشترط في البداية لمعالجة البيانات الحساسة ضرورة الحصول على موافقة "كتابية وصريحة" من الشخص المعني، باستثناء الحالات التي يُصرح بها قانونًا (المادة ١٢/فقرة ٢). ويتفق هذا الشرط مع خطورة وأهمية هذه البيانات. ومع ذلك، اكتفى المشرّع في الفقرة التالية من المادة نفسها، بالنسبة للعمليات المتعلقة ببيانات الأطفال، باشتراط الحصول على موافقة ولي الأمر، دون الإشارة إلى شكل هذه الموافقة، ما يثير تساؤلات حول ما إذا كان يجب أن تكون موافقة ولي الأمر مكتوبة وصريحة، كما هو الحال بالنسبة لموافقة صاحب البيانات الحساسة.

---

[٢٣٧]- وهذا هو الواقع القائم فى المعالجة الرقمية للبيانات الشخصية، حيث شيوع الوسائل الرقمية كاليات لتحقيق الموافقة الرقمية مثل تطبيقات سلسلة الكتل، وهذا ما يظهر من نصوص قوانين حماية البيانات فى مصرو الامارات، خاصة نص المادة الاولى من القانونان. انظر:

Fukui, N. op. cit., pp, 1ets . . .Roman-Martinez, I., Calvillo-Arbizu, J., Mayor-Gallego, V., Madinabeitia-Luque, G., Estepa, A., & Estepa, R. op. cit., pp,, 12727-12741 .

(ISSN: 2537- 0758)

وفى ضوء ما تقدم نؤيد من الاتجاه الذى يرى أن قصد المشرّع المصري، عند اعتبار بيانات الأطفال ضمن البيانات الشخصية الحساسة في جميع الأحوال، وفقًا لتعريفه لهذا النوع من البيانات في (المادة ١/فقرة ٣ من القانون)، يدل بوضوح على أن شرط الموافقة الكتابية والصريحة ينطبق على معالجة البيانات الحساسة بوجه عام. ويشمل ذلك سواء كان هذا التعبير صادراً عن الشخص نفسه أو عن نائبه القانوني. وبناءً عليه، يجب أن يكون تعبير النائب القانوني (ولي الأمر) عن الموافقة على معالجة أو جمع بيانات القاصر في صورة كتابية وصريحة، بما يتماشى مع اشتراطات القانون الخاصة بهذا النوع من البيانات.

## الفرع الثانى

## مدى جواز الاعتداد بالتعبير الضمني عن الموافقة الرقمية

في إطار التعامل مع الموافقة الرقمية، يُثار تساؤل حول مدى اعتبار التعبير الضمني وسيلة مقبولة قانونًا للإفصاح عن هذه الموافقة. فالتعبير الضمني يُعرف على أنه الاستنتاج المستفاد من سلوك معين للشخص دون تصريح مباشر منه. وعلى الرغم من أن التشريعات الحديثة تميل نحو اعتماد التعبير الصريح لتجنب الغموض وضمان حماية الحقوق الرقمية، إلا أن بعض السياقات الرقمية قد تعتمد ضمنيًا على الموافقة بناءً على تصرفات المستخدم، مثل الاستمرار في استخدام خدمة معينة بعد الاطلاع على شروطها. غير أن هذه الطريقة قد تواجه إشكاليات تتعلق بمدى وضوح وقصد المستخدم في إعطاء موافقته، خاصة في ظل التفاوت الكبير في فهم المستخدمين للسياسات الرقمية[٢٣٨].

وفقًا للقواعد العامة، لا يشترط أن يكون التعبير عن الإرادة صريحًا، إذ يصح أن يأتي ضمنيًا[٢٣٩]، كما ورد في نص المادة (٢/٩٠) من القانون المدني المصرى–

[238]- Ellis, L. (2023). Digital consent in gynecology: an evaluation of patient experience. Archives of Gynecology and Obstetrics, 309(2), 611-619. https: //doi. org/10. 1007/s00404-023-07304-1.

[٢٣٩]– راجع: د. عبد الفتاح عبد الباقي، مرجع سابق، ص ٩٧.

ويقابلها نص المادة رقم ١٢٥ من قانون المعاملات المدنية الاماراتى–، والتي تنص على أنه: "يجوز أن يكون التعبير عن الإرادة ضمنيًا، إذا لم ينص القانون أو يتفق الطرفان على أن يكون صريحًا".

وبناءً على ذلك، فإن الأصل في القواعد العامة هو أن أي مظهر من مظاهر التعبير عن الإرادة، سواء أكان صريحًا أم ضمنيًا، يعد كافيًا للتعبير إرادة الشخص بوجه عام، ويُعتبر التعبيران متساويين من حيث القيمة القانونية في مجال الاعتداد بالإرادة. ولا يُستثنى من هذا الأصل إلا في حالتين، إذا ورد نص قانوني صريح يقتضي اشتراط التعبير الصريح للإرادة. وإذا اتفق الطرفان على اشتراط التعبير الصريح. وبذلك، فإن الاعتداد بالتعبير الضمني عن الإرادة يمثل قاعدة عامة، إلا في الأحوال التي يستلزم فيها القانون أو الاتفاق بين الأطراف شكلاً معينًا للتعبير "التعبير الصريح".

ويقصد بالتعبير الضمني الإفصاح عن الإرادة من خلال تصرف أو موقف لا يُقصد به في الأصل التعبير عنها صراحة، ولكن لا يمكن تفسيره أو فهمه إلا على نحو يشير إلى وجود هذه الإرادة. فهذا النوع من التعبير يُستدل على وجود الإرادة فيه بشكل غير مباشر، حيث إن الإرادة لم تُفصح عنها بوسيلة تقليدية صريحة تهدف للكشف عنها، وإنما يمكن استنباطها من موقف أو تصرف يتخذه الشخص، مما يرجح أن إرادته قد اتجهت إلى معنى معين[٢٤٠].

ووفقًا للقواعد العامة، يعتبر التعبير الضمني معادلًا للتعبير الصريح من حيث الآثار القانونية، طالما أنه يعبر عن إرادة حقيقية تتجه إلى تحقيق الأثر القانوني

---

[٢٤٠]– راجع: د. على حسن نجيده، دور الإرادة والتعبير عنها في الفقهين: الإسلامي والوضعي، مجلة معهد الإدارة العامة، الرياض– السعودية، ص ٢٥، العدد ٤٩، ١٩٨٦، ص ١٤٦. د. سليمان غانم، مرجع سابق، ص ٨١. وانظر أيضًا: د. عبد الرزاق السنهوري، مرجع سابق، ص ١٤٧. . سليمان مرقس، نظرية العقد، دار النشر للجامعات المصرية، القاهرة، ١٩٥٦، ص ٩٦.

(ISSN: 2537- 0758)

المطلوب. ومع ذلك، قد يُستبعد التعبير الضمني إذا اشترط القانون أو الاتفاق بين الأطراف أن يتم التعبير عن الإرادة بطريقة محددة، مثل أن يكون مكتوبًا أو مثبتًا في محرر رسمي. ويهدف المشرع من وراء هذا الشرط إلى تنبيه الأطراف إلى أهمية وخطورة التصرف القانوني الذي ينوون الإقدام عليه(٢٤١).

هذا وتبرز خصوصية التعبير عن الإرادة بشكل واضح في سياق حماية البيانات الشخصية، حيث يشترط لتوافر موافقة الشخص على المعالجة أن تكون هناك إرادة حقيقية يعبر عنها بصورة صريحة وحازمة، بما يدل على قبول صريح لإجراء العمليات المقترحة على بياناته. وبالتالي، لا يُعتد بالتعبير الضمني عن الإرادة أو بالتعبير المعلق على شرط. ويعود ذلك إلى أن موافقة الشخص تمثل الأساس القانوني للمعالجة، نظرًا لأن بياناته تتعلق بجوانب من خصوصيته، وقد تمتد لتشمل حياته العائلية التي يحرص على إبقائها بمنأى عن التدخل أو الاطلاع غير المصرح به.

وتقتضي حماية البيانات أن يكون التعبير عن الإرادة صريحًا، إذ لا يكفي الاعتماد على التعبير الضمني، وذلك للتأكيد على خطورة التصرف الذي يُقدم عليه صاحب البيانات. وغالبًا ما يستند هذا الشرط إلى نصوص قانونية صريحة، حيث اشترط القانون المصري– كما أشرنا سابقًا– أن يكون التعبير عن الإرادة واضحًا وصريحًا، مما يقطع بعدم صلاحية التعبير الضمني في مجال حماية البيانات الشخصية، خاصة البيانات الشخصية الحساسة.

وجدير بالذكر أنه قبل صدور اللائحة الأوروبية لحماية البيانات، كانت محكمة النقض الفرنسية تقر بصحة الموافقة الضمنية على نشر صور الشخص أو وقائع من حياته الخاصة. وقد اعتبرت المحكمة أن ذلك لا يمس حرمة الحياة الخاصة المنصوص عليها في المادة (٩) من القانون المدني الفرنسي، شريطة توافر الشروط

(٢٤١)– راجع: د. على حسن نجيدة، مرجع سابق، مرجع سابق، ص ١٤٦. ولمزيد من التفصيل، انظر: د. سليمان غانم، مرجع سابق، ص ٨١ وما بعدها.

القانونية اللازمة والالتزام بالتفسير الضيق لهذه الموافقة، بما يضمن عدم تجاوز نطاقها أو الإضرار بالحقوق المحمية[٢٤٢].

**وخلاصة القول**، إنه في الوقت الراهن، ومع صراحة نصوص اللائحة الأوروبية والقانون المصري في اشتراط التعبير الصريح عن الموافقة، لا يجوز الاعتداد بالموافقة الضمنية لصاحب البيانات فيما يتعلق بعمليات جمع ومعالجة بياناته الشخصية. بينما نصوص القانون الاماراتى قد تحتمل قبول التعبير الضمنى للموافقة على المعالجة الرقمية للبيانات وان كنا نرى ان التعبير الصريح شرط لصحة التعبير عن الموافقة بمعالجة البيانات ولا استثناء عليه، وذلك استناداً الى تعريف المشرع للموافقة فى نص المادة الاولى من القانون الاماراتى.

## الفرع الثالث

## مدى صلاحية السكوت للتعبير عن الموافقة الرقمية

السكوت Le silence ليس مجرد امتناع عن الكلام فحسب، بل هو موقف سلبي لا ينطوي بذاته على دلالة واضحة على وجود إرادة معينة[٢٤٣]. ويترتب على ذلك أن السكوت، في حالته المجردة دون اقترانه بأي ظرف أو سياق يدل عليه، لا يمكن اعتباره إفصاحًا أو تعبيرًا عن الإرادة، لأن الموافقة تُعد عملًا إيجابيًا، في حين

(242)- Breen, S., Ouazzane, K., & Patel, P. (2020). Gdpr: is your consent valid?. Business Information Review, 37(1), 19-24. https: //doi. org/10. 1177/0266382120903254. Keyes, M. (2019). Optional choice of court agreements in private international law: general report., 3-48. https: //doi. org/10. 1007/978-3-030-23914-5_1. Cass. Civ. Lére, 11 décembre 2008, no 07-19. 494 P: D., 2009, p. 100; JCP 2009. II. 10025, note Loiseau: RTD civ. 2009. 295, obs. Hauser; RTD com. 2009. 141, obs. Pollaud-Dulian; RDC 2009477, obs. Laithier. Cass. Civ. Lére, 4 novembre 2011: D., 2012, p. 765, obs. Dreyer; RTD civ., 2012, p. 90, obs. Huser; JCP, 2012, No. 71, note Loiseau .

(٢٤٣)– انظر في ذلك تفصيلاً: د. عبد الرزاق السنهوري، مرجع سابق، رقم ١١٢، ص ١٨٥ وما بعدها؛ د. عبد الفتاح عبد الباقي، مرجع سابق، ص ٨١ وما بعدها؛ د. محمود جمال الدين زكى، مرجع سابق، ص ٣٥ وما بعدها.

(ISSN: 2537- 0758)

أن السكوت هو موقف سلبي. وبالتالي، لا يمكن اعتبار السكوت المجرد إرادة ضمنية، إذ تستخلص الإرادة الضمنية من ظروف أو مواقف إيجابية تدل على وجودها، بينما يبقى السكوت، في حد ذاته، مكافئًا للعدم من حيث التعبير عن الإرادة(٢٤٤).

وقد استبعد القانونان المدني المصري و الاماراتى أي قيمة للسكوت البسيط، فلم يعتبره إفصاحًا أو تعبيرً عن الإرادة، ومع ذلك، وفى القواعد فقد أجاز هذان القانونان، في بعض فروض استثنائية أن يعتبر السكوت قبولاً في حالة السكوت الملابس Silenvr circonstancié، متى كان هناك تعامل سابق بين المتعاقدين واتصل الإيجاب بهذا التعامل أو إذا تمحض الإيجاب لمنفعة من وجه إليه، أو ان يجرى العرف التجاري أو طبيعة المعاملة على أن الموجب لم يكن لينتظر تعبيرا صريحًا بالقبول (م ٩٨ مدنى مصرى والمادة رقم ١٣٠ معاملات مدنية اماراتى).

- **عدم جواز التعبير عن الموافقة الرقمية من خلال تصرف سلبي(٢٤٥):**

إن التعبير عن الموافقة الرقمية يتطلب أن يكون واضحًا وصريحًا، مما يستبعد التصرفات السلبية كالسكوت أو الامتناع عن اتخاذ إجراء معين كوسيلة لإظهار الموافقة. ويرجع ذلك إلى عدة اعتبارات قانونية ومنطقية تتعلق بطبيعة الموافقة

(٢٤٤)– راجع: مجموعة الأعمال التحضيرية للقانون المدني، الجزء الثاني، مرجع سابق، ص ٥٧ وما بعدها.

(٢٤٥)– هذا على الرغم من ان هناك من يرى امكانية قبول السكوت كتعبير عن الموافقة فى المعاملات الرقمية عامة، كما هو فى سياق التنمر الرقمى، ولكن الاصل والغالب رفض السكوت ان يكون تعبيرا عن الموافقة على معالجة البيانات، **انظر تفاصيل ذلك:**

-Kassam, I., Ilkina, D., Kemp, J., Roble, H., Carter-Langford, A., & Shen, N. (2023). Patient perspectives and preferences for consent in the digital health context: state-of-the-art literature review. Journal of Medical Internet Research, 25, e42507. https: //doi. org/10. 2196/42507.. Rad, D., Dughi, T., Roman, A., & Ignat, S. (2019). Perspectives of consent silence in cyberbullying. Postmodern Openings, 10(2), 57-73. https: //doi. org/10. 18662/po/71. Groue de travail "article 9", Avis 15/2011 sur la définition du consetement, op. cit., p. 14 .

الرقمية وحماية حقوق الأفراد، لا سيما في بيئة التعاملات الرقمية التي تفتقر في الغالب إلى التفاعل الشخصي المباشر.

ووفقًا للحيثية (٣٢) من اللائحة الأوروبية العامة لحماية البيانات GDPR، لا يُعتبر السكوت، أو التعبير عن الموافقة من خلال مربع اختيار مفعّل مسبقًا بشكل افتراضي (cases cochés par défaut)، أو الامتناع عن اتخاذ إجراء (inactive)، موافقة صحيحة بموجب أحكام اللائحة. ويرجع ذلك إلى اعتبار هذه التصرفات تصرفات سلبية لا تستوفي شرط ضرورة التعبير عن الموافقة عبر تصرف إيجابي واضح وصريح، كما نصت عليه المادة (١١/٤) من اللائحة.

ولقد أشارت مجموعة عمل المادة (٢٩) إلى أن التعبير السلبي، في الممارسة العملية، ينطوي على قدر كبير من الغموض، مما يجعل من الصعب الوفاء بالمتطلبات التي يفرضها التوجيه الأوروبي بشأن صحة الموافقة. ويُعتبر هذا الغموض عائقًا أمام تحقيق الشفافية والوضوح اللازمين لضمان تعبير حقيقي وصريح عن إرادة الشخص المعني، وهو ما يشكل شرطًا أساسيًا لصحة الموافقة في إطار التشريعات الأوروبية[٢٤٦].

ومن هذا المنطلق، لا يمكن اعتبار السكوت وسيلة للتعبير عن الموافقة على معالجة البيانات الشخصية، إذ يشترط أن يصدر التعبير عن الإرادة من خلال تصرف إيجابي واضح. فالسكوت، بطبيعته، لا يتسم بالإيجابية أو الوضوح؛ بل هو تصرف سلبي يعادل العدم، والعدم لا يحمل أي دلالة واضحة. وعليه، يمكن القول إن القاعدة العامة في اللائحة الأوروبية GDPR تستبعد تمامًا فكرة السكوت كوسيلة للتعبير عن الموافقة في سياق جمع ومعالجة البيانات الشخصية. فلا يُعتبر السكوت قبولًا للمعالجة، ولا توجد استثناءات لهذه القاعدة في مجال حماية البيانات، على عكس قانون العقود الذي يعترف أحيانًا بالسكوت الملابس كدليل على القبول. ويعود

(246)- Groue de travail "article 9", Avis 15/2011 sur la définition du consetement, op. cit., p. 14 .

(ISSN: 2537- 0758)

هذا الاختلاف إلى صعوبة تيقن المتحكم من وجود موافقة حقيقية في حالة السكوت[٢٤٧]، وكذلك تعذر توفير دليل إثبات قاطع على حصول تلك الموافقة.

هذا ولا تُعد الموافقة قائمة في حالة التعبير عن الإرادة من خلال النقر على مربع اختيار مفعّل مسبقًا بشكل افتراضي من قبل الموقع[٢٤٨]، والمعروف بالخيارات الافتراضية Options par défaut.، ولتوضيح هذه المسألة التقنية، يُشار إلى أن المتحكم في موقع الإنترنت قد يقوم بإعداد مربع اختيار مرتبط ببنود الخصوصية التي تتعلق بجمع ومعالجة البيانات الشخصية، ويضع بداخله علامة محددة مسبقًا تشير إلى قبول المستخدم لهذه البنود بمجرد تصفحه للموقع. وفي هذه الحالة، يتعين على المستخدم صاحب البيانات اتخاذ إجراء لتعديل الإعداد الافتراضي (إزالة العلامة) إذا كان يرغب في رفض المعالجة.

ومع ذلك، فإن هذه الطريقة لا تُلبي شرط التعبير الإيجابي الواضح عن الموافقة الذي تفرضه التشريعات الحديثة، مثل اللائحة الأوروبية GDPR، التي تتطلب أن

---

(٢٤٧)– يضرب فريق عمل "المادة ٢٩" مثالاً على ذلك، بقوله: يمكن أن يتخليل أنه عقب إرسال الموقع خطاب إلى العملاء، لإبلاغهم بأنه يتم النظر في نقل بياناتهم ما لم يعترضوا في غضون أسبوعين يستجيب ١٠% فقط من العملاء، في هذه الحالة من المشكوك فيه أن ٩٠% من العملاء الذين لم يستجيبوا يوافقون بالفعل على نقل بياناتهم. راجع: فريق عمل "المادة ٢٩"، الرأي الاستشاري رقم ٢٠١١/١٥ بشأن تعريف الرضاء- المعتمد في ١٣ يوليو ٢٠١١، ص ص ١٣، ١٤.

Groupe de travail, "article 29", Avis 15/2011 sur la définition du consentement, op. cit., pp. 13/14 .

(٢٤٨)– وهو عبارة عن مربع اختيار يقوم الموقع مسبقًا بوضع علامة معينة بداخله مثل موافق أو نعم للدلالة على قبول صاحب البيانات بشروط الاستخدام أو شروط الخصوصية التي تنطوى على جمع ومعالجة بياناته. بما يشير لأى من موافقته المسبقة، طالما استمر في تصفح الموقع، أما في حالة عدم الرضاء، فيتعين عليه النقر على المربع لإزالة هذه العلامة للتعبير عن رفضه لجمع ومعالجة بياناته.

يكون قبول المستخدم ناتجًا عن إجراء إيجابي يعكس إرادته الحقيقية والصريحة، دون الاعتماد على الإعدادات الافتراضية التي قد تفتقر إلى الشفافية أو الوضوح.

ويرجع السبب في عدم الاعتداد بالموافقة الصادرة من خلال مربع اختيار مفعّل مسبقًا بشكل افتراضي، وفقًا لقضاء محكمة العدل الأوروبية[٢٤٩]، إلى أن هذه الوسيلة لا تعكس سلوكًا إيجابيًا من جانب مستخدم الموقع. ومن ثم، لا يمكن اعتبارها تعبيرًا عن موافقة "قاطعة"، حيث يصبح من المستحيل عمليًا إثبات صدور موافقة المستخدم على معالجة بياناته الشخصية استنادًا فقط إلى عدم قيامه بإلغاء التحديد المسبق الموجود بمربع الاختيار الذي أعده الموقع.

**علاوة على ذلك**، يصعب التأكد من أن هذه الموافقة قد صدرت بطريقة مستنيرة، إذ لا توجد وسيلة لإثبات أن المستخدم شاهد مربع الاختيار المفعّل افتراضيًا أو قرأ شروط الاستخدام ووافق عليها قبل مواصلة نشاطه على الموقع الإلكتروني. وأوضحت المحكمة ضرورة تزويد المستخدم بمعلومات واضحة وشاملة تتعلق بتثبيت ملفات تعريف الارتباط (الكوكيز) للوفاء باشتراط صحة الموافقة. وأكدت المحكمة أن المعلومات الواضحة والشاملة يجب أن تتضمن، مدة بقاء ملفات تعريف الارتباط قيد التشغيل. وما إذا كان بإمكان أطراف ثالثة الوصول إلى بيانات ملفات تعريف الارتباط. ويهدف ذلك إلى تمكين المستخدمين من فهم النتائج المترتبة على قبول الشروط الواردة في خانة الاختيار الافتراضية، بما يضمن صدور موافقة مستنيرة وصحيحة وفقًا للمتطلبات القانونية[٢٥٠].

وفي السياق نفسه، يشير رأي فريق عمل "المادة ٢٩" بشأن الرضاء إلى أن الحصول على رضاء صحيح يقتضي استخدام آليات لا تدع مجالاً للشك في اتجاه نية الشخص المعني نحو الرضاء على المعالجة، مع الوضع في الاعتبار أنه في

(249)- Cour de justice de l'Union européenne (grande chambre), Arrêt 2019, op. cit., points 55 et 57 .

(250)- Cour de justice de l'Union européenne (2éme chambre), Arrête du 11 novembre 2020, op. cit., point 53 .

(ISSN: 2537- 0758)

سياق البيئة الإلكترونية لا يعتبر من قبيل الرضاء الذي لا لبس فيه، الرضاء القائم على السكوت، وأيضًا استخدام مربع الاختيار المحدد مسبقًا (الخيارات الافتراضية) التي يجب على صاحب البيانات التدخل لتعديلها عند رغبته في رفض المعالجة، ومن شأن ذلك أن يمنح الأفراد قدرًا أكبر من السيطرة على بياناتهم الشخصية عندما تستند المعالجة على رضائهم[٢٥١].

وفى اطار ذلك تُظهر ضمنياً أحكام قانونى حماية البيانات الشخصية المصري والاماراتى عدم إمكانية الاعتداد بالسكوت أو "مربع الاختيار المحدد مسبقًا" كوسيلة للتعبير عن إرادة صاحب البيانات. ويعود ذلك إلى اشتراط القانونان ضرورة الحصول على "الموافقة الصريحة" لمعالجة البيانات الشخصية، وفقًا لما نصت عليه المادة (٢) من القانون المصرى، والمادة (١) من القانون الاماراتى. وهذا الاشتراط يعكس حرص المشرّعان على ضمان أن تكون الموافقة نابعة من إرادة حرة ومبنية على علم تام، وبتعبير صريح بما يعزز من حماية حقوق الأفراد في مواجهة أي معالجة غير مشروعة أو غير مستنيرة لبياناتهم الشخصية.

هذا ويشترط قانون حماية البيانات الشخصية المصري الحصول على "الموافقة الكتابية الصريحة" لمعالجة البيانات الشخصية الحساسة. وهذا الشرط يعكس أهمية التعبير الصريح، وأيضًا الكتابي، الذي يتطلب قيام الشخص المعني بتصرف إيجابي واضح، وليس سلبيًا، يُظهر بجلاء علمه بإمكانية جمع ومعالجة بياناته الشخصية، وإبداء موافقته بناءً على هذا العلم.

وتُشير أحكام قانونى حماية البيانات المصري والاماراتى واللائحة الأوروبية إلى أن الموافقة الصحيحة تفترض علم الشخص المعني مسبقًا بطبيعة عمليات المعالجة التي ستُجرى على بياناته، باستثناء الحالات التي يجيزها القانون صراحةً. وتهدف هذه الضوابط إلى ضمان قدرة الأفراد على التعبير عن إرادتهم بحرية من خلال

(251)- Groupe de travail "article 29", avis 15/2011, op. cit., p. 41 .

الموافقة الصريحة أو الرفض، استنادًا إلى فهم تام لجميع الجوانب ذات الصلة بمعالجة بياناتهم الشخصية.

ويمكن استنباط عدم دلالة السكوت كوسيلة للتعبير عن الإرادة في هذا السياق من النص القانوني الذي يمنح الشخص الحق في العدول عن الموافقة المسبقة على الاحتفاظ ببياناته الشخصية أو معالجتها (المادة ٢، الفقرة الثانية من قانون حماية البيانات الشخصية والمادة ١٧ من القانون الاماراتى). وهذا الحق في العدول يفترض، بشكل أساسي، وجود علم مسبق بعمليات المعالجة وموافقة صريحة عليها. وبالتالي، لا يمكن بأي حال استنباط هذه الموافقة من مجرد السكوت، إذ أن العدول ذاته يعتمد على موافقة واضحة وإيجابية سبقت أي إجراء يتعلق بالبيانات الشخصية.

كما انه ومن ناحية أخرى، يتبين أن السكوت المجرد لا يتوافق مع طبيعة عمل المواقع الإلكترونية أو شبكات التواصل الاجتماعي. فعندما يطلب المتحكم من المستخدم موافقته على جمع ومعالجة بياناته الشخصية، ويُحجم المستخدم عن الضغط على زر القبول، أي يلتزم السكوت، فلا يمكن اعتبار هذا السكوت بمثابة موافقة في هذه الحالة.

ويمكن الاستدلال على عدم صلاحية السكوت كوسيلة للتعبير عن الموافقة من اشتراط أن تشمل الموافقة جميع أنشطة المعالجة المتعلقة بنفس الغرض أو الأغراض المحددة. وفي حالة وجود أغراض متعددة للمعالجة، يجب الحصول على موافقة صريحة على كل غرض على حدة. هذا الاشتراط يجعل من الواضح أن السكوت، بطبيعته السلبية، لا يمكن أن يفي بمتطلبات الموافقة الصحيحة، حيث يعجز عن التعبير عن إرادة واضحة تشمل جميع أغراض المعالجة[٢٥٢].

فضلًا عن ذلك، يؤثر السكوت سلبًا على شفافية المعاملات التجارية عبر الإنترنت، مما يؤدي إلى تراجع ثقة مستخدمي الإنترنت في كيفية إدارة بياناتهم الشخصية. ويترتب على ذلك تأثير سلبي على حجم وانتشار هذه المعاملات، حيث

(252)- Lignes directrices 5/200, op. cit., no 79, p. 21 .

(ISSN: 2537- 0758)

يعتمد نجاح البيئة الرقمية على توفير مستويات عالية من الشفافية والثقة بين الأطراف المعنية.

وبشكل أكثر تحديدًا، يُعد اعتبار السكوت كوسيلة للتعبير عن الموافقة انتهاكًا للالتزام القانوني الواقع على عاتق المتحكم في موقع الإنترنت، الذي يتطلب إعلام الأشخاص المزمع جمع بياناتهم الشخصية بوضوح وشفافية حول طبيعة المعالجة وأغراضها. هذا الإخلال بالالتزام يضعف من حماية حقوق المستخدمين ويُعوق تعزيز بيئة آمنة ومضمونة للمعاملات الإلكترونية[٢٥٣].

أما بالنسبة للسكوت الذي تلازمه ملابسات تدل على الرضاء، والذي يُعتد به المشرع المدني كتعبير عن الإرادة في بعض الحالات، فإننا نرى عدم جواز الاعتداد به كتعبير عن قبول الشخص لمعالجة وجمع بياناته الشخصية. ونستند فى ذلك عدم وجود نص قانوني صريح يقر هذه الوسيلة للتعبير عن الإرادة في سياق حماية البيانات الشخصية.

كما أن السماح بالاعتداد بهذا النوع من السكوت قد يُصبح ذريعة تفتح الباب أمام المتحكمين في المواقع الإلكترونية وشبكات التواصل الاجتماعي لابتداع نماذج نمطية أو صياغات مبهمة تُستخلص منها دلالة على التعبير عن الإرادة بشكل غير صريح. ومثال ذلك اعتبار مجرد الاستمرار في تصفح الموقع بمثابة قبول ضمني لجمع ومعالجة بيانات المستخدم، أو اعتباره موافقة على تلقي الإشعارات والإعلانات من الموقع نفسه أو من مواقع أخرى مرتبطة به. وهذا النهج قد يؤدي إلى انتهاك حقوق المستخدمين وتقويض مبدأ الشفافية الذي يُعد حجر الأساس لحماية البيانات الشخصية، مما يوجب استبعاده تمامًا في هذا الإطار.

**وأخيرًا**، نشير إلى أن السبب في عدم الاعتداد بالسكوت كوسيلة للتعبير عن الإرادة في إطار البيانات الشخصية، يعود إلى خطورة عمليات المعالجة وما تنطوي

(253)- C. CHASSUGBEUXM L'encadrement jruidique du traitement des données personnelles sur les sites de commerce en ligne, Thése précité, p. 182 .

عليه من مساس بخصوصية الشخص المعني. وهذه العمليات تتطلب قدرًا عاليًا من التدبر والتفكير والتروي من قبل صاحب البيانات للموافقة عليها، مما يستوجب اتخاذ تصرف إيجابي يعبر بوضوح ودقة عن اتجاه إرادته لتحقيق الأثر القانوني المطلوب. وفى هذا النهج ما يعزز من حماية حقوق الأفراد في مواجهة أي معالجة قد تتم دون موافقة مستنيرة وصريحة، وهو ما يتماشى مع التشريعات الحديثة التي تؤكد على ضرورة احترام إرادة الأفراد في إدارة بياناتهم الشخصية.

## المطلب الثالث

## أهلية الموافقة على معالجة البيانات

**تمهيد**:

نفضل فى بداية الحديث عن احكام اهلية الموافقة على المعالجة الرقمية للبيانات الشخصية ان نبين مفهوم اهلية الموافقة على معالجة البيانات و نسميها الموافقة الرقيمة، حيث ان أحد الاعتبارات الأساسية لأهلية الموافقة الرقمية فى راينا هي قدرة المشارك رقمياً، أى قدرة صاحب البيانات رقمياً على تقديم موافقة رقمية مستنيرة خاصة من ناحية التقنية الفنية. وقد أظهرت الدراسات أن الأفراد يجب أن يمتلكوا فهمًا كافيًا للمعلومات المقدمة لهم رقميًا حتى تتحقق تلك الموافقة المستنيرة، بما يعنى ان التقنية الرقمية لها دورا جوهريا فى تحديد معنى و مضمون الاهلية اللازمة للموافقة الرقمية على معالجة البيانات الشخصية، على سبيل المثال، فأن جزءًا كبيرًا من اصحاب البيانات غير مؤهلين رقمياً و يفتقرون إلى الخبرة في الأدوات الرقمية، مثل تطبيقات الهواتف الذكية، و تطبيقات التواصل الاجتماعية والتي يمكن أن تعيق مشاركتهم في المعاملات الرقمية و منها الموافقة الرقمية على معالجة البيانات[٢٥٤].

---

[٢٥٤]– ولا سيما فى الموافقة الرقمية على معالجة البيانات الشخصية المتعلقة بالحالة الصحية والمرضية، انظر فى تفاصيل اكثر

- Avram, R., So, D., Iturriaga, E., Byrne, J., Lennon, R., Murthy, V., … & Pereira, N. (2022). Patient onboarding and engagement to build a digital study after enrollment in a clinical trial (tailor-pci digital study):

(ISSN: 2537- 0758)

وتتسم العمليات المتعلقة بالبيانات الشخصية، سواء كانت جمعًا أو معالجة أو إفشاءً أو تداولًا، بدرجة عالية من الخطورة نظرًا لما تنطوي عليه من تأثير مباشر على الحق في حماية البيانات الشخصية. وعليه، فإن الموافقة على إجراء هذه العمليات يجب أن تصدر عن صاحب البيانات بعد تفكر وتروٍ وتدبر، مع إدراك كامل للعواقب المترتبة عليها. ومن هذا المنطلق، يصبح من الضروري أن يكون لصاحب البيانات القدرة أو الصلاحية القانونية التي تتيح له مباشرة هذه التصرفات بمفرده، بما يعني ضرورة تمتعه بالأهلية القانونية الكاملة للتعبير عن الموافقة على معالجة بياناته دون الحاجة إلى موافقة من يمثله قانونًا. وتعني أهلية الموافقة الرقمية القدرة القانونية للشخص على التعبير عن إرادته بالادوات الرقمية والإلكترونية بطريقة صحيحة ومعتبرة قانونًا. وتتطلب هذه الأهلية أن يكون الشخص متمتعًا بقدرة رقمية كافية بعد ان يكون متمتعاً بالقدرة العقلية الكاملة، وأن يكون على علم وإدراك تام بطبيعة التصرف الرقمى والإلكتروني الذي يقدم عليه. **ونوضح ما تقدم فى الفروع التالية.**

## الفرع الاول

## مفهوم الاهلية فى سياق المعالجة الرقمية للبيانات

الأهلية، من الناحية القانونية، تُعرف بأنها قدرة الشخص على ممارسة حقوقه وإبرام التصرفات القانونية التي تنتج آثارًا قانونية ملزمة. وفي سياق الموافقة الرقمية، تُشير الأهلية إلى قدرة الفرد على منح موافقة صحيحة ومُلزمة قانونيًا على معالجة بياناته الشخصية في البيئة الرقمية. ويُشترط أن يكون الفرد مدركًا لأبعاد الموافقة وللآثار القانونية المترتبة عليها.

intervention study. Jmir Formative Research, 6(6), e34080. https: //doi. org/10. 2196/34080 .Doan, X., Florea, M., & Carter, S. (2023). Legal-ethical challenges and technological solutions to e-health data consent in the eu.. https: //doi. org/10. 3233/faia230088 .

ويجب أن يكون الشخص في حالة عقلية تمكنه من إدراك ماهية المعالجة الرقمية، وطبيعتها، وأغراضها. وهذا يشمل فهم المخاطر المترتبة على مشاركة البيانات الشخصية. وغالبًا ما تُشترط سن قانونية معينة ليُعتبر الشخص قادرًا على منح الموافقة. تختلف هذه السن من دولة لأخرى، ولكنها تتراوح عمومًا بين ١٦ إلى ١٨ عامًا، مع استثناءات تُجيز موافقة الأوصياء القانونيين على معالجة بيانات القُصَّر. ولا بد أن يكون الشخص متمتعًا بالأهلية القانونية الكاملة، مما يعني عدم وجود موانع قانونية مثل حالات الحجر أو وجود إعاقات ذهنية تؤثر على قدرته على اتخاذ قرارات واعية.

وعليه إذا ثبت أن الشخص الذي منح الموافقة لا يتمتع بالأهلية القانونية اللازمة، تُعتبر الموافقة باطلة وغير ملزمة قانونيًا. وهذا البطلان يؤدي إلى إبطال المعالجة الرقمية المرتبطة بها. و في حال غياب الأهلية، تقع على عاتق الجهة التي تتلقى الموافقة مسؤولية التحقق من توافرها. وعدم الالتزام بهذا الواجب قد يؤدي إلى مساءلة قانونية وغرامات مالية.

والغالب أنه ينشأ التزام قانوني خاص بحماية الفئات غير المؤهلة، مثل القُصَّر أو الأشخاص ذوي الإعاقة، لضمان عدم استغلال بياناتهم الشخصية في هذا السياق، حيث تُلزم بعض القوانين الشركات الرقمية باتخاذ تدابير إضافية للتحقق من أهلية الأطراف المانحة للموافقة.

## أولاً- لزوم توافر أهلية الموافقة على معالجة البيانات:

لا يُعتبر رضا صاحب البيانات شرطًا كافيًا لمشروعية معالجة بياناته الشخصية ما لم يستوفِ جميع شروطه وعناصره من جهة، ويصدر عن شخص يتمتع بالأهلية القانونية اللازمة من جهة أخرى. فحتى تكون الموافقة صحيحة ومرتبة لآثارها القانونية، يجب أن تصدر من شخص مكتمل المدارك وناضج بما يكفي ليدرك طبيعة العمليات التي يوافق على إجرائها بشأن بياناته الشخصية، وأن يكون قادرًا على تقدير الآثار الخطيرة المحتملة المترتبة عليها. وتبرز هذه الخطورة نظرًا لكون هذه العمليات

(ISSN: 2537- 0758)

تمس أحد الحقوق اللصيقة بشخصية الفرد، مما يستوجب التأكد من أن الموافقة تستوفي الشروط القانونية اللازمة لضمان حمايتها وصيانتها[٢٥٥].

عرفنا إن الموافقة الرقمية على معالجة البيانات الشخصية قد تتم بناء على اتفاق، وقد تتم بارادة صاحب البيانات وحده و هذا هو الغالب، حيث ان الموافقة الرقمية هنا من صاحب البيانات تعد تصرفًا انفراديًا وليست من قبيل الموافقة التعاقدية، حتى وإن وجد تشابه بينهما. وبالتالي، لا تُطبق عليها القواعد المتعلقة بأهلية الأداء في القانون المدني، التي تُقصد بها صلاحية الشخص لمباشرة التصرفات القانونية التي تُكسبه حقًا أو تُحمله التزامًا[٢٥٦]. إذ إن هذه الموافقة تكتفي بتوافر أهلية خاصة ينظمها القانون، وتعتمد على إدراك وإرادة الشخص. تُعرف هذه الأهلية بـ "الأهلية الرقمية[٢٥٧]Capacité numérique"، وترتبط ببلوغ صاحب البيانات سنًا محددة

---

[٢٥٥]– حيث تعد أهلية الموافقة على معالجة البيانات الشخصية شرطًا أساسيًا لضمان صدور الموافقة بشكل صحيح ومعتبرة قانونًا. إذ يتطلب الأمر أن يكون الشخص المانح للموافقة متمتعًا بالأهلية القانونية الكاملة، بحيث يكون قادرًا على فهم طبيعة العملية المتعلقة ببياناته الشخصية، وتقدير عواقبها المحتملة. وبذلك، لا يمكن اعتبار الموافقة على معالجة البيانات صالحة إذا صدرت عن شخص يفتقد الأهلية، سواء بسبب نقص في الإدراك أو قصور قانوني، مما يستدعي في هذه الحالات تدخل من يمثله قانونًا لضمان حماية مصالحه وحقوقه، خاصة حقوقه اللصيقة بالشخصية. انظر فى تفاصيل تلك الحقوق: د. عبد الحي حجازى، المدخل لدراسة العلوم القانونية، الجزء الثاني الحق وفقًا للقانون الكويتي "دراسة مقارنة"، مطبوعات جامعة الكويت، ١٩٧٠، ص ١٦٢.

[٢٥٦]– انظر: د. أحمد سلامة، المدخل لدراسة القانون، الكتاب الثاني، مقدمة القانون المدني أو نظرية الحق الطبعة الخامسة، مكتبة عين شمس، القاهرة، بدون سنة نشر، ص ٣٧.

[٢٥٧]– يذهب جانب من الفقه إلى التوسع في نطاق أهلية الأداء، مشيرًا إلى أنها لا تقف عند حد الأهلية الإجرائية (أهلية الأداء القضائية) أو الأهلية التصرفية (وهي صلاحية الشخص لإبرام تصرفات قانونية ولتلقي تعبيرات عن الإرادة تكون موجهة إليه)، بل "لايزال هناك مجال كبير قلما ترتاده أبحاث الشرح، وهي القيام بالأعمال التي لا هي من قبيل التصرفات القانونية، ولا من قبيل الأعمال غير المشروعة، كإنشاء موطن أو تغييره، وكالتعبير عن علم أي الأخبار

(سن الموافقة الرقمية)، الذي تختلف التشريعات في تحديده استنادًا إلى معيار العمر الذي يُعبر عن النضج العقلي وقدرة الفرد على التعبير عن إرادته بشكل مستقل فيما يتعلق بمعالجة بياناته الشخصية[٢٥٨]. وبناءً على ذلك، تصح موافقة القاصر في هذا السياق متى بلغ السن القانونية المقررة[٢٥٩].

---

declaration de science...". انظر: د. عبد الحي حجازى، مرجع سابق، ص ٤٠٩. ولعل ما يدعم ذلك الدراسات المختلفة التى تدور حول مدى صلاحية الشخص لاصدار الموافقة الرقمية، حيث تشير الدراسات إلى أن الأفراد الأصغر سنًا، وخاصة أولئك الذين تقل أعمارهم عن ١٨ عامًا، غالبًا ما يكونون أكثر مهارة فنية في استخدام التقنيات الرقمية. ويتضح ذلك من الدراسات التي تسلط الضوء على المشاركة النشطة للشباب في المنصات الرقمية للتغيير الاجتماعي والمشاركة المدنية. و تعد المهارات الرقمية المكتسبة خلال السنوات التكوينية أمرًا بالغ الأهمية لأنها تعد الأفراد لمتطلبات المجتمع الرقمي. وعلاوة على ذلك، يؤكد التكامل المتزايد للتكنولوجيات الرقمية في التعليم على أهمية محو الأمية الرقمية منذ سن مبكرة، مما يشير إلى أنه من الناحية المثالية يجب تطوير المهارات الأساسية اللازمة للمشاركة الرقمية قبل الوصول إلى مرحلة البلوغ. و كل ذلك يشكل مقوم من مقومات ومضمون الاهلية الرقمية ومن ثم اهلية الموافقة الرقمية على معالجة البيانات الشخصية. انظر:

- Chauke, T. (2024). Skills learnt in youth work practice necessary for the digital age: a qualitative study of neet youth. Research in Social Sciences and Technology, 9(1), 351-368. https: //doi. org/10. 46303/ressat. 2024. 20. Pawluczuk, A. (2020). Digital youth inclusion and the big data divide: examining the scottish perspective. Internet Policy Review, 9(2). https: //doi. org/10. 14763/2020. 2. 1480 .Sarva, E., Slišāne, A., Oļesika, A., Daniela, L., & Rubene, Z. (2023). Development of education field student digital competences—student and stakeholders' perspective. Sustainability, 15(13), 9895. https: //doi. org/10. 3390/su15139895 .

[٢٥٨]– في فنلندا، يُحدد سن الموافقة الرقمية عند ١٣ عامًا، حيث سيطرة معيار ظاهرة "الفجوة الرقمية". حديثاً، وقديما اختلاف دور سيطرة معيار العمر على تحدد الاهلية وتدرجها، انظر: د. عبد الرزاق السنهوري: مرجع سابق، ص ٢٢١؛ د. محمد حسام محمود لطفي، مرجع سابق، ٨٣؛ د. محمود جمال الدين زكي، مرجع سابق، ص ٥٤؛ د. عبد الحي حجازى، مرجع سابق، ص ٤٢٥. **وانظر كذلك:**

(ISSN: 2537- 0758)

من ثم، يصبح معيار توافر الأهلية الرقمية للموافقة على المعالجة للبيانات الشخصية هو قدرة الشخص على فهم طبيعة ما يوافق عليه من جمع أو معالجة للبيانات وتقدير آثارها. و يتحقق هذا المعيار عندما يكون الشخص كامل الأهلية الرقمية، أي قد بلغ سن الموافقة الرقمية المحدد، ويتمتع بقواه العقلية. في المقابل، فإن موافقة الشخص عديم التمييز لا تحمل أي قيمة قانونية، نظرًا لافتقاره إلى القدرة العقلية اللازمة لفهم وتمييز طبيعة المعالجة التي يوافق عليها، مما يجعل موافقته في هذه الحالة غير حرة وغير مستنيرة[٢٦٠].

أما فيما يتعلق بالقاصر ومن في حكمه، فتُثار مسألة الأهلية لتحديد مدى قدرته على الموافقة على معالجة بياناته، وكذلك أحوال النيابة القانونية التي تُمارس بالنيابة

---

Friemel, T. (2014). The digital divide has grown old: determinants of a digital divide among seniors. New Media & Society, 18(2), 313-331. https: //doi. org/10. 1177/1461444814538648 .Olphert, W. and Damodaran, L. (2013). Older people and digital disengagement: a fourth digital divide?. Gerontology, 59(6), 564-570. https: //doi. org/10. 1159/000353630. Palviainen, Å. and Räisä, T. (2021). The winding road to accessing the voices of one thousand schoolchildren: a nexus analysis of collecting data for a survey. Scandinavian Journal of Educational Research, 66(5), 793-807. https: //doi. org/10. 1080/00313831. 2021. 1939137 .Kassam, I., Ilkina, D., Kemp, J., Roble, H., Carter-Langford, A., & Shen, N. op. cit. Research, 25 .

[٢٥٩]– انظر: د. محمد عيد الغريب، مرجع سابق، ص ٨٧. عبدالله، هـ. (٢٠٢١). مضمون العقد في ضوء التعديلات الحديثة للقانون المدني الفرنسي (دراسة مقارنة بالفقه المالكي). مجلة جامعة الشارقة للعلوم القانونية، ١٧(٢)، ٦١٥– ٦٤١ .https: //doi. org/10. 36394/jls. v17. i2. 21

عبدالله، هـ. (٢٠٢٢). عقود الإطار دراسة مقارنة في ضوء مرسوم قانون رقم (١٣١–٢٠١٦) للقانون المدني الفرنسي. https: //doi. org/10. 34120/jol. v46i5. 2881 .jol, 46(5)

[٢٦٠]– قارب د. محمد عيد الغريب، المرجع السابق، ص ص ٨٦– ٨٧؛ وأيضًا: د. محمد حسين منصور، نظرية الحق، دار الجامعة الجديدة، الإسكندرية، ٢٠٠٤، ص ٦١. وانظر عبدالله، هـ. مضمون العقد في ضوء... مرجع سابق، ص ٦١٥ وما بعدها. عبدالله، هـ. عقود الإطار... مرجع سابق، ص ١٣١ و ما بعدها.

عن القاصر في هذا الشأن. وتجدر الإشارة إلى أنه لا يتطلب الحصول على موافقة الشخص، سواء كان رشيدًا أو قاصرًا، أو من يمثله قانونيًا، إذا كانت المعالجة مشروعة استنادًا إلى مسوغات أخرى، مثل كون المعالجة ضرورية لتنفيذ التزام تعاقدي[٢٦١].

## ثانياً- تحديد سن الموافقة الرقمية في قوانين حماية البيانات:

تختلف قوانين حماية البيانات حول العالم في تحديد السن الأدنى الذي يتمتع فيه الفرد بالأهلية الكاملة لتقديم الموافقة الرقمية على معالجة بياناته الشخصية. ويُعرف هذا المفهوم غالبًا بـ "سن الموافقة الرقمية"، وهو العمر الذي يُعتبر فيه الفرد قادرًا قانونيًا على فهم طبيعة المعالجة وآثارها، وبالتالي تقديم موافقة مستنيرة وحرة.

وفقًا للفقرة الأولى من المادة (٨) من اللائحة الأوروبية (المعنية بالشروط المطبقة على رضاء الأطفال فيما يتعلق بخدمات مجتمع المعلومات)، حينما يشترط لمشروعية المعالجة رضاء صاحب البيانات بمعالجة بياناته الشخصية لغرض أو أكثر من الأغراض المحددة (وفقًا للمادة ٦/١أ من اللائحة)، فيما يتعلق بتقديم خدمات مجتمع المعلومات مباشرة إلى الطفل[٢٦٢].، فإن معالجة البيانات الشخصية الخاصة بالطفل تكون مشروعة متى كان سن الطفل ستة عشر عامًا على الأقل، أما إذا لم يتجاوز الطفل هذه السن، فإن هذه المعالجة لا تكون مشروعة إلا إذا صدر الرضاء أو الإذن به من صاحب السلطة الأبوية على الطفل، ويجوز للدول الأعضاء

---

[٢٦١]– كما هو واضح فى احكام قوانين حماية البيانات المختلفة، انظر المادة ٦ (البنود من ٢–٤) من قانون حماية البيانات الشخصية المصري، و المادة ٤ من قانون حماية البيانات الاماراتى، والمادة ٦ (البنود من "ب" إلى "و") من اللائحة الأوروبية لحماية البيانات GDPR، والمادة ٥ من قانون المعلوماتية والحريات المعدل (البنود من ٢–٦).

[٢٦٢]– يشير بعض الفقه الفرنسي أن مفهوم خدمات مجتمع المعلومات Les services de la société de l'information واسع للغاية. ويتسم بعدم التحديد. راجع:

A. DEBET, Le consentement dans le Règlement Général sur la Protection des données, op. cit., no 6 .

(ISSN: 2537- 0758)

أن تقرر تخفيض هذه السن في قوانينها الوطنية بشرط ألا يقل بأى حال من الأحوال عن ١٣ سنة.

ومع ذلك تُتيح اللائحة للدول الأعضاء في الاتحاد الأوروبي تخفيض الحد الأدنى لسن الموافقة الرقمية في قوانينها الوطنية، بشرط ألا يقل هذا السن بأي حال من الأحوال عن ١٣ عامًا. وقد أخذ المشرع الفرنسي بهذه الرخصة في المادة (٤٥) من قانون المعلوماتية والحريات المعدل عام ٢٠١٨، وفضل خفض سن الرضاء الرقمي إلى ١٥ عامًا، باعتباره مناسبًا لنمو مدارك القاصر وإلمامه بمجريات التطور التقني وبراعته في ذلك.

ومن ثم، فإن القاصر الذي يبلغ السن المحددة قانونيًا وفقًا للتشريعات ذات الصلة، يصبح أهلاً لتقديم موافقته المستقلة على معالجة بياناته الشخصية فيما يتعلق بتقديم خدمات مجتمع المعلومات مباشرة له، دون الحاجة إلى الحصول على موافقة أو إذن من نائبه القانوني أو من يمثله. و هذا التحديد يعكس الاعتراف القانوني بقدرة القاصر الذي يبلغ هذا السن على فهم طبيعة المعالجة وآثارها، مما يعزز استقلاليته في اتخاذ القرارات المتعلقة ببياناته الشخصية في البيئة الرقمية.

واتجه المشرع المصري إلى تحديد سن الموافقة الرقمية بسن الطفل، أي ١٨ عامًا، وهو السن الذي يبلغ فيه الشخص الأهلية القانونية الكاملة للمسئولية الجنائية. ويتضح هذا التوجه من نص المادة (١٢) الفقرة الثالثة من قانون حماية البيانات الشخصية المصري، حيث تشترط هذه المادة حصول المتحكم أو المعالج على موافقة ولي الأمر عند القيام بأي عملية تتعلق ببيانات الأطفال، سواء كانت جمع البيانات، أو نقلها، أو تخزينها، أو حفظها، أو معالجتها، أو إتاحتها للغير. ويُبرز هذا التنظيم حرص المشرع المصري على تعزيز حماية خصوصية الأطفال في البيئة الرقمية، مع إعطاء الأولوية لدور أولياء الأمور في اتخاذ القرارات المتعلقة ببيانات أطفالهم لضمان حماية مصالحهم الفضلى.

وعن سن الموافقة الرقمية فى النظام القانونى الاماراتى نرى انه ذات السن المقرر فى القانون المصرى، حيث ينظم المرسوم بقانون اتحادي رقم (٤٥) لسنة ٢٠٢١، حماية البيانات الشخصية، وخاصة معالجة البيانات الشخصية بناء على الموافقة الرقمية– فى ضوء القواعد العامة–، ويشدد على أهمية الحصول على موافقة صاحب البيانات قبل معالجتها. إلا أن هذا القانون لا يحدد سنًا معينًا للموافقة الرقمية بما يفيد باعتماد سن ١٨ عاما وفق القواعد العامة و قانون حماية الطفل. ويدعم ذلك، انه في بعض المناطق الحرة مثل مركز دبي المالي العالمي، تم تحديد سن الموافقة الرقمية. وفقًا لقانون حماية البيانات رقم ٥ لعام ٢٠٢٠ في مركز دبي المالي العالمي، حيث يُعتبر الأفراد الذين تبلغ أعمارهم ١٨ عامًا فما فوق مؤهلين لتقديم الموافقة على معالجة بياناتهم الشخصية. وبالنسبة للأفراد الذين تقل أعمارهم عن ١٨ عامًا، يتطلب الحصول على موافقة ولي الأمر أو الوصي القانوني قبل معالجة بياناتهم الشخصية[٢٦٣].

## ثالثًا- النيابة القانونية عن القاصر في إطار حماية البيانات الشخصية:

النيابة القانونية عن القاصر في إطار حماية البيانات الشخصية تُعَدُّ من الضمانات الأساسية التي تهدف إلى حماية حقوق القُصَّر ومصالحهم عند معالجة بياناتهم الشخصية. وفي هذا السياق، يتم تنظيم النيابة القانونية وفقًا لقوانين حماية البيانات الشخصية، التي تُلزِم الجهات المعنية باتباع إجراءات صارمة لضمان احترام حقوق القُصَّر. خاصة وان القانون يفترض في القاصر عدم توافر الأهلية اللازمة للتصرف كقاعدة عامة، لضعفه وعدم نضجه وعدم قدرته الطبيعية، مما يقتضي خضوعه لنظام خاص للحماية يكفل وجود من يمثله قانونًا فيما يتعلق بالتصرفات

[٢٦٣]– الحسن،، الطبيعة الخاصة... مرجع سابق، ص ٤٦٩ و ما بعدها. اليحيائي، الآثار القانونية لجائحة كورونا..، مرجع سابق، نفس الموضع.

(ISSN: 2537- 0758)

الخاصة بشخصه أو بأمواله التي لا يجوز له إبرامها بمفرده إلا إذا توافرت له الأهلية اللازمة لمباشرتها[٢٦٤].

وتبرز هذه المسألة كواحدة من القضايا الجديرة بالاهتمام، خاصة في إطار حماية البيانات الشخصية، حيث أتى تنظيم الأحكام المتعلقة بالقاصر – وهو من لم يبلغ السن المحددة للتعبير عن الموافقة الرقمية– بصورة مقتضبة في التشريعات المقارنة.

ففي القانون المصري، والقانون الاماراتى، تم الإشارة إلى هذه الأحكام دون تفصيل وافٍ، مما يترك ثغرات في تحديد نطاق وآليات ممارسة النيابة القانونية عن القاصر بشكل يتناسب مع طبيعة البيانات الشخصية والبيئة الإلكترونية.

أما اللائحة العامة لحماية البيانات الأوروبية (GDPR) والقانون الفرنسي، فعلى الرغم من تقدمهما في تنظيم حماية البيانات، إلا أنهما لم يقدما نظامًا دقيقًا ومحددًا لهذه النيابة، يأخذ في الاعتبار الخصوصية المزدوجة المرتبطة بحماية بيانات القُصَّر من جهة، والطبيعة المعقدة للبيئة الإلكترونية من جهة أخرى.

وهذا النقص الواضح في الإطار القانوني القائم يجعل من الضروري وضع تشريعات خاصة أو لوائح مكملة تُعنى بتنظيم دور الوصي القانوني وآليات ممارسته للنيابة عن القاصر، بما يضمن تحقيق التوازن بين حماية البيانات الشخصية وحقوق القاصر في البيئة الرقمية. ومع ذلك يكون من المناسب هنا تحديد الطبيعة القانونية للنيابة عن القاصر، وتناول حدود سلطة النائب القانوني عن هذا القاصر، وبيان آليات التحقق من رضاء النائب عن القاصر، وهذا موضوع الفروع اللاحقة.

---

(264)- Philippe BONFILS et Adeline GOUTTENOIRE, Droit des mineurs, Précis Dalloz, 2008, no 35 ets .

صادقي، م.، "النيابة في التعاقد وآثارها على أطراف العقد"، مجلة كوفة للفنون، المجلد ١، العدد ٥٦، ٢٠٢٣، ص ٢٤٥-٢٦٣، متاح على الرابط: https: //doi. org/10. 36317/kaj/2023/v1. i56. 11619.

## الفرع الثانى

## الطبيعة القانونية للنيابة عن القاصر فى الموافقة الرقمية.

### اولاً- نوعى الولاية على القاصر:

يحتاج القاصر، ومن في حكمه، في جميع الأحوال إلى من يقوم على شئونه لحمايته ورعاية مصالحه[٢٦٥]، ولذلك وجب تعيين من يتولى أمره في نفسه أو ماله، والولاية عليه نوعان: ولاية على النفس، وولاية على المال، ويُقصد بالولاية على النفس: العناية بكل ما له علاقة بشخص القاصر ونفسه والإشراف عليه وحفظه وتربيته وتعليمه وتوجيه حياته وإعداده إعدادًا صالحًا، ويدخل في ذلك الموافقة على تزويجه[٢٦٦].، أما الولاية على المال: فيقصد بها العناية بكل ما له علاقة بمال القاصر وحفظه وإدارته واستثماره[٢٦٧].

والولاية على النفس ذات ارتباط شديد الصلة بالأسرة، هدفها حفظ الصغار ذكورًا أو إناثًا، وعمادها أن يكون الولي قادرًا على رعاية القاصر، حريصًا على صيانة حقوقه، ولذا كان الأصل في الولاية أن يتولاها أقرب الأشخاص نسبًا إلى القاصر،

---

[٢٦٥]- يذهب الفقيه كورنو CORNU إلى عدم أهلية القصر، والاعتراف القانوني بحالة ضعفهم الطبيعي، هو أثر لسياسية الحماية القانونية، فالشخص عديم الأهلية ليس ضحية، بل هو المستفيد من أحكام تعيد لصالحه توازنًا للقوى لم تحققه له الطبيعة بعد. انظر:
Gérard CORNU, L'âge civil, in, Mélanges en l'honneur de Paul ROUBIER, T. II. Librairie Dalloz et Sirey, 1961, p. 9 .

[٢٦٦]- انظر المادة ١/١٧٨- أ، من قانون الأحوال الشخصية لدولة الإمارات العربية المتحدة، القانون الاتحادي رقم ٢٨ لسنة ٢٠٠٥. راجع: د. وهبة الزحيلي، الفقه الإسلامي وأدلته، الجزء السابع: الأحوال الشخصية، دار الفكر للطباعة والنشر والتوزيع بدمشق، سوريا. ط٢، ١٩٨٥، ص ١٨٧.

[٢٦٧]- انظر المادة (١٧٨/ ١-ب) من قانون الأحوال الشخصية لدولة الإمارات العربية المتحدة، كما يعرف البعض الولاية على المال بأنها: "تدبير شئون القاصر المالية من استثمار وتصرف وحفظ وإنفاق". راجع: د. وهبة الزحيلي، الفقه الإسلامي وأدلته، الجزء السابع، مرجع سابق، ص ١٨٧.

(ISSN: 2537- 0758)

ومن ثم ثبت هذه الولاية كأصل عام للعصبة من الرجال[٢٦٨]، فتكون للأب أولاً، ثم الجد أو غيره من الأولياء[٢٦٩].

أما الولاية على مال القاصر فتثبت للأب بقوة القانون، إن كان حيًا، فإن لم يوجد فإنها تثبت للوصي الذي اختاره الأب قبل وفاته، فإن لم يكن قد اختار وصيً، فإن الولاية تثبت بقوة القانون للجد الصحيح ومن علاه، فإن لم يوجد الجد، فللوصي الذي تختاره المحكمة.

وقد تكون الولاية على النفس والمال معًا، فتشمل الشئون الشخصية والمالية للقاصر[٢٧٠]، كولاية الأب على أولاده فاقدي الأهلية أو ناقصيها[٢٧١].

وإذا كانت مهمة الولي– بوجه عام– تتمثل في العمل على تحقيق مصلحة القاصر في شؤونه الشخصية والمالية، فإنه يُشترط أن تتوافر فيه الأهلية القانونية اللازمة لذلك، بأن يكون بالغًا، عاقلاً، راشدًا، أمينًا على نفس القاصر، وقادرًا على إدارة شؤونه وحماية مصالحه. كما يشترط أن يكون متحدًا معه في الدين. وتنتهي الولاية على النفس عند بلوغ القاصر، سواء كان ذكرًا أو أنثى، سن الخامسة عشرة

---

[٢٦٨]– راجع: حكم المكمة الدستورية العليا، مصر، القضية رقم ٦٠ لسنة ٣١ق. دستورية، جلسة ٦ مارس ٢٠٢١. الجريدة الرسمية– العدد ١٠ (مكرر) في ١٥ مارس ٢٠٢١، القضية رقم ١٦٤ لسنة ١٩ ق دستورية، جلسة ٣ يوليو ١٩٩٩. الجريدة الرسمية، العدد–١٨ في ١٥ يوليو ١٩٩٩.

[٢٦٩]– د. عبد الرزاق السنهورى، مرجع سابق، ف ٦٦٧، ص ٨٥٧؛ د. جلال على العدوي، د. رمضان أبو السعود، د. محمد حسن قاسم، الحقوق والمراكز القانونية، منشأة المعارف، الإسكندرية، ١٩٩٦، ص ٨٥٦؛ د. وهبة الزحيلي، الفقه الإسلامي وأدلته، مرجع سابق، ص١٨٧.

[٢٧٠]– د. وهبة الزحيلي: مرجع سابق، ص ١٨٧.

[٢٧١]– وفي هذا تقول مكمة النقض المصرية: "إن ولاية الأب تعم النفس والمال، وهي مقيدة بالنظر والمصلحة وليس من النظر أن يمتنع عن الإنفاق على أولاده أو أن يسيء إليهم أو أن يهمل شئونهم ويتخلى عن تربيتهم فيكون للقاضي ٣٥ق، جلسة ١٩٦٦/٦/٢٢، مكتب فني ١٧، جزء ٣ قاعدة ٢٠٠، ص ١٤٣٧.

وهو متمتع بقواه العقلية. أما الولاية على المال، فتستمر حتى بلوغ القاصر سن الرشد المدني (٢١ عامًا)، بشرط أن يكون متمتعًا بقواه العقلية وألا يكون قد صدر حكم بالحجر عليه[٢٧٢].

## ثانياً- حماية البيانات الشخصية للقاصر بين الولاية على النفس والولاية على المال:

ذهب جانب من الفقه[٢٧٣] إلى اعتبار الحق في حماية البيانات الشخصية من الحقوق اللصيقة بالشخصية، والتي ترتبط بالمقومات المعنوية للإنسان. ونظرًا لاتصال هذه الحقوق بالشخصية، فإنها تكتسب ذات الصفات التي تتمتع بها الحقوق اللصيقة بالشخصية. لذلك، فهي لا تُعتبر من الحقوق المالية، إذ لا تقوَّم بمال، مما يخرجها عن نطاق التعامل القانوني. وبالتالي، تكون هذه الحقوق غير قابلة للتصرف

---

[٢٧٢]– انظر: المستشار/ محمد عزمي البكري، موسوعة الأحوال الشخصية، المجلد الأول، دار محمود للنشر، القاهرة، ٢٠١٧. ص ٢٥٣ وما بعدها؛ محمد غالي العنزي، الولاية على نفس الطفل بين الشريعة الإسلامية ومنظومة القوانين الكويتية، مجلة الشريعة والدراسات الإسلامية، مجلس النشر العلمي– جامعة الكويت، المجلد ٣٥، العدد ١٢٢، سبتمبر ٢٠٢٠، ص ٢٨٨ وما بعدها. وانظر أيضًا: المادة (١٨٠) من قانون الأحوال الشخصية الإماراتي: والمادة ٢١١ من قانون الأحوال الشخصية الكويتي. وانظر الطعن رقم ١٠٤ لسنة ٥٩ق، جلسة ٥ فبراير ١٩٩١، محكمة النقض المصرية، مكتب فني، س ٤٢، ق ٦٦، ص ٣٩٨. وانظر: د. محمد محمد أبو زيد، نظرية الحق "مقدمة القانون المدنى". بدون سنة نشر، الدار المحمدية للطباعة، القليوبية، ص ٥٧، وما بعدها.

[273]- Allah Rakha, N. (2024). Constitutional safeguards for digital rights and privacy. Irshad J. Law and Policy, 2(4), 31-43. https: //doi. org/10. 59022/ijlp. 172 .Agathe LEPAGE, Droit de la personnalitém Répertoire de droit civil Dalloz, 2009, no 31 ets: Murielle BENEJAT, Les droits sur les données personnelles, in Jean-Christophe SAINT-PAU et all, Droit de la personnalité, Lexis-Nexis, 2013, no 926, p. 561 .

– حسام الدين كامل الأهواني، الحق في احترام الحياة الخاصة "الحق في الخصوصية" دراسة مقارنة، دار النهضة العربية، القاهرة، بدون سنة نشر، ص ٢٣١.

(ISSN: 2537- 0758)

فيها أو الحجز عليها، كما أنها لا تسقط بمرور الزمن ولا تكتسب بالتقادم. وعليه، تتمتع هذه الحقوق بالحماية القانونية المقررة ضد أي اعتداء عليها، حفاظًا على كرامة الفرد وخصوصيته(٢٧٤).

وفي حين يستقيم هذا التصور في البيئة التقليدية، فإن البيئة الرقمية قد أفرزت أبعادًا جديدة للحق في البيانات الشخصية، بدت جلية في إمكانية الاستغلال التجاري لهذه البيانات على نطاق واسع(٢٧٥). وقد أدى ذلك إلى ظهور منظور جديد لمفهوم هذا الحق يحمل دلالات تجارية، مما أعاد إحياء الجدل القانوني حول طبيعته. ويتمحور النقاش حول ما إذا كان هذا الحق يُعد من الحقوق الملازمة أو اللصيقة بالشخصية، والتي تخرج بطبيعتها عن نطاق التعامل، أم أنه يُعتبر من الحقوق المدنية التي يمكن أن تخضع للتعامل التجاري(٢٧٦).

---

(٢٧٤)– راجع: د. حسن كيره، الموجز في المدخل للقانون، مقدمة عامة "النظرة العامة للقاعدة القانونية– النظرية العامة للحق". الطبعة الثانية، منشأة المعارف، الإسكندرية، ١٩٦٣، ص٢٢٧؛ د. عبد الحي حجازى، مرجع سابق، ص ٢١٤ وما بعدها.

(٢٧٥)– ومن ذلك على سبيل المثال، فضيحة استيلاء شركة كامبريدج أناليتيكا Cambridge Analytica البريطانية على البيانات الشخصية لملايين المستخدمين لشبكة فسبوك، وتوظيفها لأهداف غير قانونية، حيث أثير الاتهام حول دورها في دعم حملة مرشح الحزب الجمهوري "دونالد ترامب" في انتخابات رئاسة الولايات المتحدة الأمريكية عام ٢٠١٦، من خلال جمع وتحليل البيانات للتأثير على الناخبين، وما نجم عن ذلك من فوز ترامب وأصبح حينها الرئيس الخامس والأربعين للولايات المتحدة، قبل أن يخسر الانتخابات عام ٢٠٢٠. انظر: د. محمد عرفان الخطيب، ضمانات الحق في العصر الرقمي، مرجع سابق، ص ٢٥٩، حاشية ١٧.

(٢٧٦)– في هذا الخصوص، انظر: د. محمد عرفان الخطيب، المرجع السابق، ص ٢٦١ وما بعدها. ولمزيد من التفصيل، راجع:

Philippe MOURON, Pour ou contre la ptrimonialité des données personnelles, Revueve Européenne des Médias et du Numérique, no 46-47, Printemps-Été 2018, pp. 90-96. Disponible sur le site: https: //hal/amu. archives-ouvertes. Fr/hal-0182390/document .

ويثير هذا الأمر تساؤلات قانونية متعددة، أبرزها مدى مشروعية الاستغلال التجاري للبيانات الشخصية، والتكييف القانوني للاعتداء على هذه الحقوق، وإمكانية تصرف الشخص فيها أو التعامل عليها. ويتفرع عن ذلك تساؤل آخر حول ما إذا كان الاعتداء عليها يندرج ضمن نطاق الاعتداء على الحقوق المرتبطة بشخصية الإنسان أم بالقيم المالية. هذه التساؤلات تحمل نتائج قانونية هامة، لا سيما في حالة الاتفاق على الانتفاع التجاري بالبيانات الشخصية. ورغم الأهمية البالغة لهذه المسألة، فإنها لا تزال محل نقاش في الفقه القانوني ولم يصدر بشأنها حسم تشريعي حتى الآن[٢٧٧].

وقد دفع ذلك جانبًا من الفقه[٢٧٨] إلى اعتبار الحق في خصوصية البيانات في العالم الرقمي من الحقوق المدنية التي يجوز التعامل التجاري بها. وقد استند هذا الاتجاه إلى أن البيانات الشخصية أصبحت ذات قيمة اقتصادية واضحة، مما يبرر التعامل معها كسلعة قابلة للاستثمار، بما في ذلك إمكانية بيعها أو التنازل عنها. ويترتب على هذا التصور إحياء فكرة ملكية الشخص لبياناته، وتعزيز سيادته على ذمته المعلوماتية[٢٧٩]. كما يمنحه هذا النهج إمكانية الاستفادة من الفوائد الاقتصادية الناتجة عن استغلال بياناته.

---

[٢٧٧]– في هذا الخصوص، انظر: د. محمد عرفان الخطيب، المرجع السابق، ص ٢٦١ وما بعدها.

ولمزيد من التفصيل، راجع:

Philippe MOURON, Pour ou contre la ptrimonialité des données personnelles, Revueve Européenne des Médias et du Numérique, no 46-47, Printemps-Été 2018, pp. 90-96. Disponible sur le site: https: //hal/amu. archives-ouvertes. Fr/hal-0182390/document .

[٢٧٨]– انظر: د. محمد عرفان الخطيب، المرجع السابق، ص ٢٦١. وانظر أيضًا:

Pierre STORRER, Pour un droit commercial de l'exploitation des données à caractère personnel, Recueil Dalloz, no 27, 25 Juillet 2013, p. 1844; L. MARINO, op. cit., pp. 22-28 .

[279]- Alain BENSOUSSAN, Informatique et libertés, Editions Francis Lefebvre, Paris, 2e édition, 2010, p. 42 .

(ISSN: 2537- 0758)

وعلى النقيض، يتجه الرأي الغالب إلى اعتبار الحق في حماية البيانات الشخصية، بما يتضمنه من أهداف لحماية خصوصية الأفراد، جزءًا لا يتجزأ من الحقوق اللصيقة بالشخصية. ويندرج هذا الحق ضمن صور الحق في احترام الحياة الخاصة، أو ما يُعرف بالحق في الخصوصية(٢٨٠). وقد أيدت المحكمة الأوروبية لحقوق الإنسان هذا الاتجاه، معتبرةً أن حماية البيانات الشخصية تُعد إحدى المكونات الأساسية للحق في الخصوصية(٢٨١).

وقد أكدت اللجنة الاستشارية الوطنية لحقوق الإنسان في فرنسا هذا الاتجاه، مشددة على أن الحق في حماية البيانات الشخصية لا يجوز التنازل عنه، ولا يدخل ضمن دائرة المعاملات المالية. ورغم أنه قد تم العمل في بعض الحالات على صحة التنازل عن هذا الحق بمقابل مالي، فإن ذلك لا يغير من جوهره كأحد الحقوق اللصيقة بالشخصية. فقابلية هذا الحق للتعامل أو الاستغلال ضمن حدود معينة لا تنزع عنه خصائصه الأساسية، ولا تضفي عليه الطبيعة التجارية(٢٨٢).

---

(280)- Jean-Michel BRUGUIERE, Bérengère GLEIZE, Droits de la personnalité, Ellipses édition, 2015, p. 18; Ph. MOURON, op. cit., pp. 7 et 8; L. MARINO, Les nouveaux territoires des droits de la personnalité, p. 22 ets .

وعلى عكس ذلك، يذهب البعض إلى وجود استقلال للحق في حماية البيانات الشخصية عن الحق في الخصوصية. انظر:

J. -C. SAINT-PAU et all, Droit de la Personnalité, p. 545 et .

(٢٨١)– انظر في شأن الاتجاه المؤيد لاعتبار الحق في احترام الحياة الخاصة والحق في الخصوصية من الحقوق اللصيقة بالشخصية، ومن ثم تتمتع بنفس خصائصها. في هذا الخصوص، انظر: حسام الدين كامل الأهواني، الحق في احترام الحياة الخاصة "الحق في الخصوصية". مرجع سابق، ص ٢٢٣،

**وراجع ايضا:**

J. -M. BRUGUIÉRE, B. GLEIZE, op. cit., p. 12 .

(282)- Cour Europénne des droits de l'homme (CEDH), Grande chambre, S. et Marper c/Royaume-Uni, 4 décembre 2008, req. no 30562/04 et 30566/04 .

وبذلك يظل هذا الحق مرتبطًا بشخص صاحبه بشكل لا ينفصل عنه، مما يجعله خارج نطاق التعامل من حيث المبدأ، فلا يجوز التصرف فيه أو التنازل عنه، كما لا يخضع للتقادم[٢٨٣]. ويُعزز هذا الرأي الطابع غير المالي للبيانات الشخصية، حيث إن أحكام اللائحة الأوروبية لحماية البيانات، التي تضم ١٧٣ حيثية و٩٩ مادة، لم تتضمن أي نصوص صريحة تُجيز بيع أو استغلال البيانات الشخصية لصاحبها[٢٨٤]. ويؤكد هذا الاتجاه أيضًا أن أحكام أهلية الأداء تقتصر على الحقوق

---

فصلين متميزين لهذه الحقوق الأساسية للاتحاد الأوروبي La Charte des droit fondamentaux de l'Union européenne فصلين متميزين لهذه الحقوق؛ حيث تتناول المادة (٧) من الميثاق في الحق في الحياة الخاصة والعائلية، بينما تتناول المادة (٨) حماية البيانات الشخصية.

(٢٨٣)– جدير بالذكر أن اللجنة الاستشارية الوطنية لحقوق الإنسان في فرنسا قد حسمت هذه المسألة في الرأي المؤرخ ٢٢ مايو ٢٠١٨ بشأن حماية الخصوصية في العصر الرقمي، المنشور في الجريدة الرسمية الفرنسية في ٣ يونيو ٢٠١٨، وأكدت على أنه في سياق تداول البيانات وتسويقها، لا تعد البيانات الشخصية محلاً للتعامل التجاري، ولا تتعلق بالحرية التعاقدية الكاملة، فهي تخضع للمبادئ والحقوق الأساسية، للشخص بما في ذلك الحق في احترام الخصوصية، وتتبع حماية البيانات الشخصية من ارتباط قانوني قوى ينشأ بين الشخص وبياناته الشخصية، فحق الشخص على بياناته ليس حقًا على شيء (حق عيني) ولكنه حق ملازم للإنسان ويحمي شخصيته (من حقوق الشخصية)، وتستند ممارسته إلى الموافقة الحرة والمستنيرة والمحددة من صاحبها، ويضيف رأي اللجنة أن قانون المعلوماتية الحريات الفرنسي وضع البيانات الشخصية في إطار الحقوق غيرالمالية، حيث تندرج هذه البيانات في إطار حقوق الشخصية وبالتالي تتصف بكامل سماتها، انظر:

Commision nationale consultative des droits de l'homme (CNCDH), Avis du 22 mai 2018 sur la protection de la vie privée à l'ère du numérique, JORF no0126 du 3juin 2018, Texte no 63. Disponible sur le site: https: //www. legifrance. gov. fr/jorf/article_jo/JORFART000036977284

(284)- Th. LÉONARD, "Yves, si tu exploitais tes données?", op. cit., p. 659 à 683 .

(ISSN: 2537- 0758)

المالية، ولا تمتد تلقائيًا إلى الحقوق اللصيقة بالشخصية، حتى إذا كانت هذه الحقوق تحمل بعض الصفات أو الآثار المالية(٢٨٥).

والأصل في هذا السياق أن الأهلية المقررة هي "أهلية طبيعية capacité naturelle" أو واقعية، تتحقق متى توفرت لدى الشخص القدرة على فهم نطاق أفعاله وتصرفاته، إلى جانب النضج الكافي لاتخاذ قرارات تتعلق بشخصه ومصالحه(٢٨٦). ولهذا السبب، قد يكون القاصر أكثر قدرة على إدراك الأمور التي تمس شخصه مقارنةً بقدرته على فهم المسائل المالية(٢٨٧).

كما أكد مجلس الدولة الفرنسي على أن حماية البيانات الشخصية تُعد من الحقوق اللصيقة بالشخصية، مستبعدًا بشكل كامل أي صفة مالية لها. واعتبر أن حق الشخص في بياناته الشخصية لا يُصنف كحق ملكية، إذ قرر أن المشرع الفرنسي، سواء في قانون المعلوماتية والحريات لعام ١٩٧٨ أو التوجيه الأوروبي رقم ٩٥/٤٦، يخرج البيانات الشخصية من نطاق الحقوق ذات الطبيعة المالية، ويُدخلها ضمن فئة الحقوق اللصيقة بالشخصية. وبهذا، تُعتبر البيانات الشخصية وثيقة الصلة بصاحبها وتشكل امتدادًا لشخصيته ذاتها(٢٨٨).

وينبني على ذلك أن الموافقة على معالجة البيانات الشخصية، باعتبارها مرتبطة بشخص القاصر نفسه، لا تتعلق– في الأصل– بحق مالي يدخل ضمن دائرة القابلية

---

(٢٨٥)– راجع: د. حسام الدين كامل الأهواني، المرجع السابق، ص ٢٢٣، ص ٢٣١.

(286)- Françoise BETAILLOLE-GONTHIER, La capacité naturelle, Thèse Bordeaux 4, 1999, p. 16 .

(٢٨٧)– في هذا الخصوص انظر: د. حسام الدين كامل الأهواني، المرجع السابق، ص ٢٣١ وما بعدها.

(٢٨٨)– راجع الدراسة السنوية لمجلس الدولة الفرنسي الصادرة عام ٢٠١٤ بشأن التكنولوجيا الرقمية والحقوق الإنسانية، ص ٢٦٤ وما بعدها.

Etude annuelle du Conseil d'Etate, Le numèrique et les droits fondamentaux, 2014, pp. 264 ets. Disponible sur le site :https: //www. vie-publique. dr/sires/defaukt/files/rapport/pdf/144000541. pdf .

للتعامل. وإنما تتصل بحق من الحقوق اللصيقة بالشخص، مستمدة من إنسانيته وآدميته، وليس بموجب شخصيته القانونية فقط. وعليه، تخضع هذه الموافقة لنظام قانوني مستقل عن أحكام المعاملات المالية[٢٨٩]. وبذلك، يدخل هذا الحق ضمن نطاق سلطة الولي على النفس، الذي يتولى رعاية شؤون القاصر وشخصه بما يحقق مصالحه ويحمي حقوقه الشخصية.

ووفقًا لوجهة النظر السابقة، ينبغي النظر إلى الحق في حماية البيانات الشخصية من منظور مجرد، باعتباره أحد أشكال الحق في حماية الخصوصية الرقمية. ويرتبط هذا الحق أساسًا بشخصية الإنسان، حيث يعبر عن ذاتيته وكيانه المعنوي[٢٩٠]. وهذا التصور يظل قائمًا بصرف النظر عن إمكانية إدخال أي عنصر أو مكون من هذه الذاتية ضمن نطاق التعامل التجاري، مثل الاتفاق على استغلال صورته[٢٩١]، التي تُعد من البيانات الشخصية وفقًا للقانون المصري، سواء بمقابل مالي أو بالمجان.

---

[٢٨٩]– انظر: د. حسام الدين كامل الأهواني: نحو نظام قانوني لجسم الإنسان، مجلة العلوم القانونية والاقتصادية، كلية الحقوق، عين شمس، المجلد ٤٠، العدد الأول، يناير ١٩٩٨، ص٤١.

[٢٩٠]– لا شك أن الصفة الغالبة في الحق في احترام الحياة الخاصة هي حماية الشخص، ويأتي ارتباطها بالذمة المالية مسألة ثانوية، وأن الأمر متروك لصاحب السلطة الأبوية للتصرف في هذا السياق، في هذا المعنى، انظر:

CA. Paris, 9 nov. 1970, D. 1981, 109, note E. ABITBOL .

[٢٩١]– في هذا الصدد، قررت محكمة النقض الفرنسية أنه يجب على القاضي التأكد من أن الإذن الصادر من صاحب الحق في الصورة (باستغلالها) يراعى الطبيعة غير المالية nature extrapatrimoniale لهذا الحق، انظر:

Cass. 1re Civ., 20 mars 2007, pourvoi no 06-10-305, Bull, 2007, I, no 125 .

كما أكد المحامي العام sudre في رأيه الخاص بقضية تتعلق باستغلال صورة مطرب متوفي أن "الاعتراف بواقع تسويق الصورة لا يعني التخلي عن حماية حقوق الشخصية التي تنتمي إليها" انظر:

Cass. 1re Civ., 4 février 2015, pourvoi no 14-11. 458 .

(ISSN: 2537- 0758)

ويعتبر هذا التصرف جائزًا، دون أن يمس الطبيعة غير المالية لهذا الحق، حيث يظل في إطار حقوق الشخصية. ويؤيد هذا الرأي أيضًا إمكانية عدول الشخص عن نشر خصوصياته، مما يؤكد الطابع الشخصي للحق(٢٩٢). أما بالنسبة للبيانات الحساسة، ومن بينها البيانات الجينية التي تُستخلص من جسم الإنسان، فإنها تُعد مكونًا ماديًا من مكونات جسده، ولا تُعامل كسلعة ذات قيمة اقتصادية. وبدلاً من ذلك، يجوز استخدامها ضمن حدود معينة، مثل أغراض البحث الطبي، دون توقع أي عائد مالي، مما يرسخ الطبيعة غير المالية لهذه البيانات(٢٩٣).

ومن الجدير بالذكر ان البعض من الفقه يرى أن موافقة الشخص على استعمال بياناته لأغراض تجارية أو نشر صورته لا تُعد لديهم خروجًا على مبدأ عدم قابلية التصرف في الحق في الخصوصية. ذلك أن الشخص الذي يُجيز للغير تصويره أو استعمال بياناته لا يتنازل عن حقه في هذه البيانات، وإنما يتنازل بصورة مؤقتة عن

---

(٢٩٢)– انظر: د. عاقلي فضيلة، الحماية القانونية للحق في حرمة الحياة الخاصة، دراسة مقارنة، رسالة دكتوراه، كلية الحقوق جامعة الإخوة منتوري–قصنطينة، الجزائر، ٢٠١١– ٢٠٢١، ص ١٢١. وانظر أيضًا:

A. LEPAGE, Droits de la personnalité, o. cit., no 17 .

وفي هذا الصدد، قررت محكمة النقض الفرنسية عدم جواز نشر صورة الشخص أو استغلالها دون رضائه، على سبيل المثال، انظر:

Cass. 2e Civ., 30 juin 2004, pourvoi no 02-19-599, Bull, 2004, II, no 340: Cass. 1re Civ., 9 juillet 2009, pourvoi no 07-19-758, Bull. 2009. I, no 175 .

كما رتبت محكمة النقض الفرنسية على انتهاك الحق في الصورة بحق المضرور في المطالبة بالتعويض. انظر:

Cass. 1re Civ., 12 décembre 2000, pourvoi no 98-17. 521, Bull. 2000, I, no 321; Cass 1re Civ., 5 juillet 2006, pourvoi no 05-14. 738, Bull 2006, I, no 362 .

(٢٩٣)– لمزيد من التفصيل، راجع: د. طارق جمعة السيد راشد، الحماية القانونية للحق في خصوصية البيانات الجينية (دراسة تحليلية مقارنة)، المجلة القانونية، كلية الحقوق فرع الخرطوم، جامعة القاهرة، المجلد ٨، العدد ١٢، الخريف ٢٠٢٠، ص ٣٩٤٤ وما بعدها.

ممارسة السلطات التي يمنحها له هذا الحق. ويظل الحق في الخصوصية، بما يشمله من الحق في الصورة، محفوظًا لصاحبه، إذ إن هذه الموافقة لا تؤدي إلى فقدان الشخص لهذا الحق أو انتقاله إلى الغير، بل تُعتبر ترخيصًا مؤقتًا أو محدودًا بموجب إرادة صاحب الحق(٢٩٤).

علاوة على ذلك، فإن تخويل الشخص الحق في استغلال بياناته الشخصية من الناحية المالية(٢٩٥) يبرز الصلة بين الحق في خصوصية البيانات والولاية على المال. إذ تنطوي هذه المسألة على حقوق مالية للشخص تنشأ نتيجة استغلال بياناته الشخصية. كما يمكن أن تنشأ حقوق مالية إضافية، مثل الحق في التعويض عن الأضرار المادية أو المعنوية التي تلحق بصاحب البيانات نتيجة المساس بها.

ورغم أن الحق في خصوصية البيانات يُعتبر حقًا غير مالي في جوهره، إلا أن ما قد يترتب عليه من مسائل مالية يمكن أن يدخل ضمن نطاق سلطة الولي على المال، حيث يتولى الولي إدارة هذه الحقوق المالية وحمايتها بما يحقق مصلحة صاحب البيانات، خاصة إذا كان قاصرًا أو عديم الأهلية(٢٩٦).

---

(٢٩٤)– انظر: د. سعيد جبر، الحق في الصورة، دار النهضة العربية، القاهرة، ١٩٨٦، ص ١٣١؛ د. عاقلي فصيلة، مرجع سابق، ص ١٢٢.

(295)- Pierre KAYSER, Les droits de la personnalité: aspects théoriques et pratiques, RTD. Civ., 1971, p. 445 et s., spécialement, p. 495 .

جدير بالذكر أن التوجيه الأوروبي رقم ٧٧٠/ ٢٠١٩ المتعلق ببعض الجوانب المتعلقة بعقود توريد المحتوى الرقمي والخدمات الرقمية هو أول نص أوروبي يأخذ في الاعتبار بشكل مباشر حالة استغلال البيانات من قبل صاحب البيانات نفسه، والذي سيحصل بعد ذلك على خدمة مقابل الوصول والاستغلال اللاحق للبيانات من قبل مزود الخدمة.

Directive (UE) 2019/770 du Parlement européen et du Conseil du 20 mai 2019 relative à certainsaspects consernant les contrats de fourniture de contenus numériques et de services numériques, J. O. U. E., L 136, 22 mai 2019. Voir: T. LÉONARD, "Yves, si tu exploitais tes données?', op. ci., p. 677 .

(٢٩٦)– انظر: د. حسام كامل الأهواني، الحق في احترام الحياة الخاصة "الحق في الخصوصية"، مرجع سابق، ص ٢٣٢.

(ISSN: 2537- 0758)

وبشكل عام، إذا كان من الصعب في كثير من الأحيان وضع حد فاصل وواضح بين ما يدخل في سلطة النائب القانوني فيما يتعلق بحماية شخص القاصر ورعايته، وما يدخل في نطاق الولاية على المال كنتيجة للاستغلال المالي لحقوقه[٢٩٧]، فإن هذا الأمر لا يؤثر على طبيعة الحق في خصوصية البيانات. إذ يظل هذا الحق جزءًا أساسيًا من المقومات المعنوية للشخص، ويحتفظ بطبيعته غير المالية، ويبقى ملازمًا لشخصيته لا ينفصل عنها. ويكون لصاحب البيانات وحده– عند بلوغه السن المحددة– الحق في الموافقة على معالجة بياناته أو جمعها أو تداولها، أو رفض ذلك. كما يملك سلطة تعديل بياناته أو محوها أو سحبها. وفي المقابل، تقع سلطة مباشرة هذه التصرفات على عاتق من يتولى رعاية شخص القاصر حال عدم بلوغه سن الموافقة[٢٩٨].

## الفرع الثالث

## نطاق سلطة النائب فى شأن الموافقة على معالجة بيانات القاصر

وفقًا للنصوص التشريعية المتعلقة بحماية البيانات الشخصية للقاصر، يجب الحصول على موافقة الشخص الذي يتولى السلطة على القاصر لمعالجة أو جمع بياناته أو أي تصرف آخر يمس بياناته الشخصية، وذلك في حالة عدم بلوغ القاصر السن القانوني للموافقة المحددة. ويكون النائب القانوني هو الممثل للقاصر حتى بلوغه السن المحدد للموافقة الرقمية (أو ما يُعرف بسن الرشد الرقمي). وتتباين

---

[٢٩٧]– د. حسام الدين كامل الأهواني، المرجع السابق، ص ص ٢٣٢، ٢٣٣.

[٢٩٨]– يرى البعض أن الرضاء أو الإذن بالتنازل عن سرية المعلومات المتعلقة بالقاصر يدخل في إطار التصرفات الخاصة بشخص الإنسان، ولا ترتبط بالمسائل المتعلقة بإدارة ذمته المالية، وتخضع لسلطة النائب القانوني عن شخص القاصر، أي أصحاب السلطة الأبوية. انظر:

C. QUENNESSON, Mineur et secret, Thèse Précitée, p. 111 . Vanwymelbeke, J., Coninck, D., Matthijs, K., Leeuwen, K., Lierman, S., Boone, I., … & Toelen, J. (2022). Clinical adolescent decision-making: parental perspectives on confidentiality and consent in belgium and the netherlands. Ethics & Behavior, 33(5), 371-386. https: //doi. org/10. 1080/10508422. 2022. 2086873 .

الأنظمة القانونية بشأن هذه النيابة، حيث تكون في بعض الحالات منفردة دون مشاركة القاصر، كما هو الحال في اللائحة الأوروبية والقانون المصري، بينما تتطلب أن تصدر الموافقة من القاصر ونائبه معًا، كما هو الحال في القانون الفرنسي[٢٩٩].

## الغصن الأول

## انفراد النائب باصدار الموافقة الرقمية على معالجة بيانات القاصر

### أولاً- في اللائحة الأوروبية لحماية البيانات(GDPR)::

أشارت المادة (١/٨) من اللائحة الأوروبية لحماية البيانات إلى تحديد سن الموافقة الرقمية بستة عشر عامًا. ويترتب على ذلك أن صاحب البيانات بمجرد بلوغه هذه السن يصبح متمتعًا بالأهلية الرقمية الكاملة، مما يتيح له التعبير عن إرادته بمفرده فيما يتعلق بمعالجة بياناته الشخصية، دون الحاجة إلى الحصول على موافقة من يمثله قانونًا. وعلى النقيض، فإن معالجة بيانات القاصر الذي لم يبلغ ستة عشر عامًا تُعتبر غير قانونية، ما لم يتم الحصول على الموافقة المسبقة من صاحب السلطة الأبوية الذي ينوب عنه قانونًا.

---

[٢٩٩]–هذا مع العلم بان الموافقة عامة و الموافقة الرقمية خاصة بشأن معالجة أو التعامل مع البيانات الشخصية و الرقمية الخاصة بالقاصر اثارت و مازلت تثير الكثير من الخلافات على مستويات مختلفة منها القانونية و الاجتماعية و الصحية و غيرها انظر امثلة لذلك الدراسات الاتية:

- Weisleder, P. (2004). The right of minors to confidentiality and informed consent. Journal of Child Neurology, 19(2), 145-148. https: //doi. org/10. 1177/08830738040190021101. Talib, H., Silver, E., & Alderman, E. (2016). Challenges to adolescent confidentiality in a children's hospital. Hospital Pediatrics, 6(8), 490-495. https: //doi. org/10. 1542/hpeds. 2016-0011 .Stavleu, D., Winter, P., Veenstra, X., Stralen, K., Coninck, D., Matthijs, K., … & Toelen, J. (2021). Parental opinions on medical decision-making in adolescence: a case-based survey. Journal of Developmental & Behavioral Pediatrics, 43(1), 17-22. https: //doi. org/10. 1097/dbp. 0000000000000978 .

(ISSN: 2537- 0758)

ويتضح من ذلك أن نصوص اللائحة جاءت واضحة وحاسمة في إعطاء النائب القانوني الحق الحصري للتعبير عن الموافقة نيابة عن القاصر في معالجة بياناته، دون حاجة لمشاركة القاصر أو الرجوع إليه في هذا الشأن.

ومع ذلك، وعلى الرغم من وجود ميزة جزئية لأحكام اللائحة الأوروبية في وضع إطار خاص لحماية بيانات القصر، إلا أن هذا التنظيم بقي محدودًا للغاية ولا يغطي كافة القضايا المتعلقة بحماية بياناتهم. كما لم تقدم نصوص اللائحة الأوروبية حلولًا شاملة، خاصة فيما يتعلق بمفهوم "موافقة الوالدين(consentement parental)"، إذ تبدو النصوص غير كافية لتقديم إطار قانوني متكامل يحدد أحكام السلطة الأبوية في سياق حماية البيانات الشخصية للقصر[٣٠٠].

**ثانياً- في قانونى حماية البيانات الشخصية المصري و الاماراتى**:

وفقًا لقانونى حماية البيانات الشخصية المصري و الاماراتى، تحل موافقة النائب القانوني (الولي على النفس) محل موافقة القاصر، مما يعني أن النائب القانوني ينفرد بالتعبير عن الموافقة نيابة عن القاصر دون أي مشاركة منه، وذلك حتى بلوغ القاصر سن الثامنة عشرة، أي تجاوز سن الطفل (اى بلوغه سن الموافقة الرقمية). ويترتب على ذلك التزام النائب القانوني بضمان عدم تعرض القاصر لأي مخاطر، طالما أن الإجراء المتعلق بالبيانات لا يقدم للقاصر أي فائدة أو مساعدة تُبرر معالجته[٣٠١].

وتؤكد المادة (١٢) من قانون حماية البيانات الشخصية المصري هذا النهج، حيث تلزم المتحكم أو المعالج بالحصول على موافقة "ولي الأمر" عند جمع البيانات الشخصية للأطفال أو تخزينها أو معالجتها أو نقلها أو إتاحتها.

ومع ذلك، يُلاحظ أن استعمال المشرع المصرى لمصطلح "ولي الأمر" قد يثير بعض اللبس، نظرًا لعدم اتساقه مع المصطلحات القانونية المستقرة المتعلقة بالولاية على الصغير، التي يضطلع بها من ينوب عنه قانونًا (الولي على النفس). وكان من

(300)- F. ROGUE, Capacité et consentmenet au traitement de données à caractère personnel et au contract, op. cit., p. 372 .

(٣٠١)– قارب: د. محمد عيد الغريب، مرجع سابق، ص ٩٠.

الأنسب استعمال مصطلح "النائب القانوني" أو "من ينوب عنه قانونًا"، خاصة و أن المصطلح الأخير قد استخدمه المشرع ذاته في نص المادة (١٥) من القانون المصرى[٣٠٢] عند الحديث عن الموافقة لنقل البيانات عبر الحدود إلى دولة لا توفر مستوى الحماية المطلوب. وبالتالي، يتبين افتقار مصطلحات القانون للاتساق الداخلي مع أحكامه ومع القواعد العامة للولاية الواردة في القانون المدني. وبذلك تتوسع نصوص القانون المصري صراحة في عدم الاعتداد بموافقة الطفل فيما يتعلق بجمع بياناته الشخصية أو معالجتها، مما يخوّل للنائب القانوني وحده السلطة الكاملة في هذا الشأن، دون النظر إلى إشراك الطفل أو تقدير مدى نضجه العقلي.

وفي هذا السياق، يمكن قبول انفراد النائب القانوني بالموافقة نيابة عن القاصر إذا كان القاصر غير مميز أو فاقد الإدراك والتمييز، إلا أنه في حالة بلوغ القاصر سنًا تمكنه من الإدراك والتمييز– حتى لو لم يصل إلى سن الموافقة الرقمية (١٨ عامًا)– فإنه من المناسب أن يُشرك في التعبير عن الموافقة المتعلقة بمعالجة بياناته الشخصية، بما يتماشى مع مبدأ احترام كرامة الطفل وحقه في التعبير عن إرادته[٣٠٣].

## الغصن الثاني

## مشاركة القاصر للنائب فى اصدار الموافقة على معالجة بيانات القاصر

بالاستفادة من المادة (٤٥) من قانون المعلوماتية والحريات الفرنسي المعدل، يتبين أن الموافقة الصادرة عن القاصر مطلوبة في جميع الحالات المتعلقة بجمع

---

[٣٠٢]– تنص المادة (١٥) من قانون حماية البيانات المصرى على ما يلى: "استثناءً من حكم المادة (١٤) من هذا القانون، يجوز في حالة الموافقة الصريحة للشخص المعني بالبيانات أو من ينوب عنه نقل أو مشاركة أو تداول أو معالجة البيانات الشخصية إلى دولة لا يتوافر فيها مستوى الحماية المشار إليها في المادة السابقة وذلك فى الحالات التى حددها النص.

[٣٠٣]– في هذا المعنى، راجع: د. حسام الدين كامل الأهواني، الحق في احترام الحياة الخاصة "الحق في الخصوصية"، مرجع سابق، ص ٢٢٨.

(ISSN: 2537- 0758)

ومعالجة البيانات، حتى إذا لم يبلغ القاصر السن المحددة للموافقة الرقمية (١٥ عامًا). وفي هذه الحالة، يجب أن تصدر الموافقة بشكل مشترك من القاصر ونائبه القانوني، ولا يجوز للقاصر التصرف بمفرده في هذا الشأن.

ومن الواضح أن هذا النهج يراعي رأي القاصر، باعتباره المعني الأساسي بالأمر، خصوصًا عندما تتعلق الإجراءات بجوانب مرتبطة بشخصيته وكيانه. وفي الوقت ذاته، لا يُغفل دور النائب القانوني، حيث يشترط أن تكون الموافقة صادرة بالتوافق بين القاصر والنائب، دون أن ينفرد أي منهما باتخاذ القرار. وفي حال مخالفة ذلك، تُعد الموافقة غير مشروعة وغير معترف بها[٣٠٤].

وقد نص المشرع الفرنسي على تحديد الشخص المسؤول عن ممارسة السلطة على القاصر في سياق معالجة البيانات، وهو صاحب (أو أصحاب) السلطة الأبوية Le titulaire de l'autorité parentale، وذلك بما يتفق مع أحكام المادة (١/٨) من اللائحة الأوروبية. وقد اعتمد المشرع في هذا التحديد على المفهوم الراسخ للسلطة الأبوية في القانون المدني، الذي تم بيانه وتنظيمه بدقة[٣٠٥].

تحدد المادة (٣٧١-١) من القانون المدني الفرنسي معالم مفهوم "السلطة الأبوية المتعلقة بشخص الطفل"، بوصفها مجموعة من الحقوق والواجبات التي تهدف إلى تحقيق المصالح الفضلى للطفل. وتشمل هذه السلطة حماية الطفل في سلامته الجسدية والنفسية، والحفاظ على صحته وأخلاقه، وضمان تعليمه وتنشئته بما يكفل احترام شخصه.

---

(٣٠٤)- لا يخضع القاصر للنيابة القانونية الكاملة إلا فيما يتعلق بإدراة مصالحه المالية، وتستبعد أحكام النيابة القانونية حيث لا تسري إلا على المسائل المالية. راجع: د. حسام كامل الأهواني، المرجع السابق، ص ص ٢٢٦، ٢٢٧.

(٣٠٥)- أفرد القانون المدنى الفرنسي لفكرة "السلطة الأبوية" بابًا خاصًا هو الباب التاسع من الكتاب الأول من التقنين المدنى، تناول الفصل الأول منه "السلطة الأبوية المتعلقة بشخص الطفل (المواد من ٧١- ٣٨١". وتضمن الفصل الثانى "السلطة الأبوية المتعلقة بأموال الطفل (المواد من ٣٨٢ إلى ٣٨٧).

وتُمنح هذه السلطة للأب والأم معًا، وتمارس حتى بلوغ الطفل سن الرشد أو إجازة تصرفه القانوني. كما تشدد المادة على أن السلطة الأبوية تُمارَس بطريقة تضمن سلامة الطفل، دون استخدام العنف الجسدي أو النفسي، مع ضرورة إشراك الطفل في اتخاذ القرارات المتعلقة به بما يتناسب مع عمره ومستوى نضجه(٣٠٦).

وتتجلى الوظيفة الأساسية للسلطة الأبوية في حماية سلامة الطفل وصحته وأخلاقه(٣٠٧)، حيث يتحمل الوالدان مسؤولية مباشرة تتعلق بحراسة الطفل ومراقبته وتعليمه. وتشكل هذه المسؤوليات واجبات جوهرية ضمن إطار الرعاية الأبوية التي تُعنى بتلبية احتياجات الطفل، وضمان حمايته والاهتمام بشؤونه(٣٠٨).

وفي ضوء هذه الوظيفة، فإن تمثيل أصحاب السلطة الأبوية للقاصر يجب أن يتم وفقًا لمعايير حيادية تراعي تحقيق المصالح الفضلى للطفل، بعيدًا عن أي اعتبارات قد تتعارض مع هذه المصالح. ويُعد الالتزام بهذه الحيادية أساسًا لضمان تحقيق أهداف السلطة الأبوية في تأمين رفاهية الطفل ورعايته بشكل شامل(٣٠٩).

وفي هذا السياق، اشترط المشرع الفرنسي في المادة (٣٧٢-١) من القانون المدني أن يمارس الأب والأم معًا السلطة الأبوية فيما يتعلق بشخص الطفل. ولا يعني ذلك استئثارهما بهذه السلطة بمعزل عن إرادة الطفل، بل يتوجب عليهما احترام

---

(306)- Art. 371-1 Civil. "L'autorité parentale est un ensemble de droits et de devoirs ayant pour finalité l'intérêt de l'efant. Elle appartient aux parents jusqu' à la majorité ou l'émancipation de l'enfant pour le protéger dans sa sécurité, sa santé et sa moralité, pour assurer son éducation et permetrre son dévelopment. Dans le respect dû à sa personne, L'autorité parentale s'exerce sans violences physiques ou psychologiques .

Les parents associent l'enfant aux décisions qui le concernent, selon son âge et son degré de maturité" .

(٣٠٧)- بهذا الوصف يرى البعض أن السلطة الأبوية تعد بمثابة حق وظيفي un droit fonction غرضه الأساسي هو تحقيق المصالح الفضلى الطفل، وهي تستند إلى الفطرة الطبيعية لدى الوالدين لحماية أطفالهم.

Gérard CORNU, Droit civil, La famille, Montchrestien, Paris, 7éme édition 2001, no 71, et no 73 .

(308)- G. CORNU, Droit civil, La famillie, op. cit., no 77 .

(309)- Adeline & Patrimoine, No 300, Mars 2020, p. 39 ets .

(ISSN: 2537- 0758)

رأيه وإشراكه في اتخاذ جميع القرارات التي تؤثر على حياته، مع مراعاة سن الطفل ودرجة نضجه[٣١٠]. حيث يشدد هذا التنظيم على التوازن بين ممارسة السلطة الأبوية من قِبَل الوالدين وبين الاعتراف بحق الطفل في التعبير عن آرائه، بما يضمن تعزيز استقلاليته التدريجية بما يتناسب مع مراحل نموه.

ويُفهم من نص المادة سالف الذكر أن إشراك الوالدين للقاصر في القرارات المتعلقة بشخصه، بما في ذلك معالجة البيانات الشخصية، يُعتبر قاعدة أساسية في النظام القانوني الفرنسي. وقد رسّخ المشرع هذه القاعدة في القانون المدني، وحرص على تأكيدها بشكل واضح ضمن الأحكام المتعلقة بحماية البيانات الشخصية، ما يعكس توجهًا قانونيًا متكاملًا يراعي مصالح القاصر.

ومع ذلك، فإن إمكانية إشراك القاصر في مثل هذه القرارات تعتمد بشكل جوهري على سنّه ودرجة نضجه، أي على وصوله إلى مستوى معين من التمييز والإدراك. ففي حال كان القاصر غير مميز ولم يصل إدراكه إلى درجة كافية تمكنه من فهم مخاطر معالجة البيانات، يكون من المنطقي أن تُصدر الموافقة من النائب القانوني وحده.

---

(٣١٠)– تتضمن السلطة الأبوية القيام بتصرفات تتعلق بشخص الطفل من حيث أساوب حياته وصحته وسلامته، وتستند هذه التصرفات إلى ما تخوله السلطة الأبوية من النيابة القانونية عن القاصر، انظر:

Ph. BONFLS et A. GOUTTENOIRE, Droit des mineurs, op. cit., no 1077 ets; C. QUENNESSON, Mineur e secret, Thése précité, p. 19 .

يكون لأصحاب السلطة الأبوية، من أجل حماية القاصر، الرضاء بالكشف عن العناصر المتعلقة بسرية حياته الخاصة. انظر:

J. C. SAINT-PAU, Droits de la personnalité, op. cit., no 1245 .

ويؤكد القضاء الفرنسي على واجب الاحترام المتبادل بين الوالدين: مشيرًا إلى أنه من أجل بلوغ الأهداف المحددة في المادة (٣٧١-١) مدني يتعين على الوالدين أن يحترم أحدهما الآخر، وأن يقوم كل منهما بالجهود الضرورية لترجمة مسئوليتهما بصورة إيجابية في حياة ولدهما، وعلى الأخص في احترام مكانة الوالد الآخر والحفاظ على الحوار الضرورى بينهما، انظر:

CA Paris. II sep. 2002: D. IR 3241 .

ويتحقق ذلك إذا كان القاصر دون سن السابعة أو يعاني من عاهة عقلية جسيمة تُعدِم الإرادة، حيث يُفترض أن الطفل في هذه المرحلة العمرية أو تلك الحالة العقلية يكون غير قادر على فهم طبيعة وأبعاد العمليات المرتبطة بالبيانات الشخصية أو المواقع الإلكترونية. وهذا الافتراض بحسب المنطق و الغالب لا يقبل إثبات العكس، حتى إذا ثبت أن القاصر يتمتع بإدراك متقدم يفوق عمره، نظراً لأن الاعتداد بمثل هذه الحالات يُشكل استثناءً لا ينسجم مع القواعد العامة المقررة لحماية القاصرين.

كذلك تفترض بعض منصات التواصل الاجتماعي أو التطبيقات الإلكترونية أن الصبي الذي لم يبلغ الثالثة عشرة من عمره لا يتمتع بالتمييز والإدراك الكافي بسبب ضعف درجة نضجه في هذه المرحلة العمرية. وبناءً على ذلك، لا يُسمح للقاصر بالتسجيل في هذه التطبيقات قبل بلوغ هذا العمر، إلا بعد الحصول على الموافقة المسبقة من صاحب السلطة الأبوية منفردًا، دون الحاجة- منطقيًا- إلى إشراك القاصر في هذا القرار.

وفي حال وفاة أحد الوالدين أو حرمانه من ممارسة السلطة الأبوية، فإن الوالد الآخر يمارس هذه السلطة وحده، وفقًا للمادة (٣٧٣-١) من القانون المدني الفرنسي. كما يجوز للقاضي، استنادًا إلى المادة (٣٧٣-٢-١) من ذات القانون، أن يعهد بممارسة السلطة الأبوية إلى أحد الوالدين إذا اقتضت مصلحة الطفل الفضلى ذلك.

أما بشأن مشاركة القاصر لوالديه في إصدار الموافقة على معالجة البيانات، إذا كان القاصر قادرًا على التعبير عن إرادته والمشاركة في اتخاذ القرار، فإن هذه الحالة تطرح إشكالية عملية مهمة تتمثل في حالة رفض صاحب السلطة الأبوية لتسجيل القاصر على الموقع أو التطبيق، رغم رغبة القاصر وموافقته.

هذا وتفتقر نصوص قانون المعلوماتية والحريات الفرنسي إلى معالجة مباشرة لهذه الإشكالية. ومع ذلك، يمكن الاسترشاد بأحكام السلطة الأبوية المنصوص عليها في القانون المدني الفرنسي، والتي تؤكد على أن الهدف الأساسي من ممارسة السلطة الأبوية هو الحفاظ على المصالح الفضلى للقاصر (المادة ٣٧١ مدني فرنسي).

(ISSN: 2537- 0758)

وبالتالي، عند نشوء نزاع بين القاصر وصاحب السلطة الأبوية حول مثل هذه القرارات، يُفترض أن يتم النظر في القضية من منظور تحقيق مصالح القاصر الفضلى، مع الأخذ بعين الاعتبار مدى تأثير القرار على سلامة الطفل ونموه النفسي والاجتماعي، وقد يُرجع الأمر إلى السلطة القضائية للفصل فيه بما يضمن تحقيق هذه المصالح.

وفى الحقيقة، فإن رفض صاحب السلطة الأبوية لمعالجة بيانات القاصر يؤدي إلى اعتبار المعالجة غير مشروعة لعدم تحقق شرط الموافقة، وهو أحد الشروط الجوهرية لصحة المعالجة. وبناءً عليه، لا يجوز للمتحكم (المتحكم في البيانات) المضي في عملية المعالجة في هذه الحالة. ومع ذلك، ينبغي أن يكون هذا الرفض مبنيًا على مبرر جدي يستند إلى اعتبارات موضوعية تُظهر أن المعالجة قد تُلحق ضررًا بالقاصر أو تتعارض مع مصالحه. كما يجب أن يكون الرفض موجهًا لتحقيق المصالح الفضلى للقاصر، التي تُعد المعيار الأساسي لتقييم أي قرار يتعلق بالقاصر، وفقًا لما تقرره أحكام القانون المدني الفرنسي.

ويظهر من هذا التحليل أهمية الالتزام بالحيادية والتوازن عند ممارسة السلطة الأبوية، بحيث لا يكون الرفض تعسفيًا أو غير مبرر، بل يُستخدم كوسيلة لضمان حماية القاصر بما يتماشى مع تطلعات النظام القانوني نحو حماية حقوق الطفل وتعزيز رفاهيته.

ومن ناحية أخرى، قد ينشأ خلاف بين الأب والأم أثناء الممارسة المشتركة للسلطة الأبوية بشأن المسائل المتعلقة بشخص القاصر[٣١١]، بما في ذلك جمع بياناته الشخصية ومعالجتها. وفي مثل هذه الحالات، يسعى القاضي للتغلب على حالة عدم الاتفاق[٣١٢] من خلال محاولة مصالحة الطرفين. ويمكن للقاضي اقتراح

---

[٣١١]- في شأن حلول الخلاف بين الوالدين فيما يتعلق بممارسة السلطة الأبوية، انظر:
Claire QUENNESON, Mineur et secret, Université de Bordeaux, 2017, pp. 130 ets .

[٣١٢]- وفقًا للمادة (٣٧٣-٢-٦) يقصد بالقاضي هنا هو قاضي محكمة الأسرة، وهو قاضي المحكمة الابتدائية المنتدب لشئون الأسرة، ويسهر على حفظ مصالح القصر، وفي هذا الصدد،

تعيين وسيط عائلي (médiateur familial) لتسهيل التواصل بين الوالدين والوصول إلى ممارسة توافقية للسلطة الأبوية. علاوة على ذلك، يجوز للقاضي إلزام الطرفين بلقاء الوسيط العائلي وفقًا للمادة (٣٧٣-٢-١٠) من القانون المدني الفرنسي. ومع ذلك، إذا تفاقم الخلاف وتمسك كل طرف بوجهة نظره، وكان التوافق بين الوالدين مستحيلًا، يتدخل القاضي لحسم النزاع، حيث يحدد طرق ممارسة السلطة الأبوية بما يحقق مصالح القاصر الفضلى[٣١٣].

وعلى الرغم من هذا الإطار القانوني، فإن تدخل القاضي لتسوية النزاعات بين الوالدين حول القرارات المتعلقة بالقاصر يُعد من الأمور النادرة نسبيًا من الناحية العملية، حتى في الحالات التي يكون فيها الوالدان منفصلين. يُعزى ذلك إلى ميل الأطراف إلى حل الخلافات بالطرق الودية أو عبر الوساطة قبل اللجوء إلى القضاء، مما يُظهر أهمية الوساطة كأداة فعّالة لتقليل النزاعات وتجنب تصعيدها[٣١٤].

ويتضح من ذلك أنه في الحالات التي يرفض فيها أحد الوالدين الإذن بتصرف يتعلق بشخص القاصر، رغم موافقة الطرف الآخر، فإن القانون يتيح للطرف الموافق

---

تعترف محكمة النقض باختصاص قاضي محكمة الأسرة في حل النزاع المتعلق بشخص ونفس القاصر في إطار الممارسة المشتركة للسلطة الأبوية.

Cass. 1re civ. 8, novembre 2005, Dr. fam. 2006, comm. No 28, obs A. GOUTTENOIRE .

يتعلق هذا الحكم بقيام قاضي محكمة الأسرة بتسوية نزاع خاص بتعليم الطفل. وينصب حول تسجيل طفل في مدرسة تتحدث لغة الأب. وانظر أيضًا حكم آخر حول اختصاص قاضي محكمة الأسرة بتسوية نواع بين الأب والأم حول تعميد الطفل في الكنيسة:

Cass. 1re., 23 septembre 2015, no 14-23. 724, Bull. Civ., no 212, Juris Data: no 2015021007, D. 2015. 1952; RTD. Civ., 2015, p. 861. Obs. J. HAUSER

[٣١٣]- تحدد المادة (٣٧٣-٢-١٠) مدنى فرنسي الأمور التي يجب أن يأخذها القاضي في اعتباره عندما ينطق بالحكم حول طرق ممارسة السلطة الأبوية، ومنها على سبيل المثال: الممارسة التي يكون الوالدان قد اتبعاها سابقًا أو الاتفاقات التى كانا قد عقداها سابقًا، التي يُعبر عنها الولد القاصر ضمن الشروط الملحوظة في المادة (٣٨٨-١)، وقدرة كل من الوالدين على تحمل واجباته واحترام حقوق الآخر.

[314]- C. QUENNEDDON, Thèse Précité, p. 131 .

(ISSN: 2537- 0758)

اللجوء إلى قاضي محكمة الأسرة بطلب الإذن بتجاوز هذا الرفض[٣١٥]. حيث انه هذه الحالة، يملك القاضي سلطة تقديرية للنظر في الطلب وتقييمه بناءً على المصالح الفضلى للقاصر، وهو المعيار الأساسي الذي يحكم القرارات المتعلقة بممارسة السلطة الأبوية. إذا رأى القاضي أن التصرف المقترح يصب في مصلحة القاصر، فإنه يملك صلاحية الإذن بهذا التصرف، حتى في مواجهة اعتراض الطرف الآخر. وهذا الإجراء يعكس التوازن الذي يسعى المشرع لتحقيقه بين ضمان ممارسة السلطة الأبوية بشكل مشترك من جهة، وحماية حقوق ومصالح القاصر من جهة أخرى، لا سيما في الحالات التي يتعذر فيها الوصول إلى توافق بين الوالدين.

## الفرع الرابع

## آليات التحقق من موافقة النائب القانوني عن القاصر

تقضي اللائحة الأوروبية، في المادة (٢/٨)، على تنظيم آلية الحصول على موافقة أصحاب السلطة الأبوية بشأن معالجة بيانات القاصر في سياق خدمات مجتمع المعلومات. وتلزم اللائحة المتحكم ببذل جهود معقولة للتحقق من صحة صدور الموافقة عن صاحب السلطة الأبوية على الطفل أو الإذن بذلك، وذلك في حال عدم بلوغ الطفل السن القانوني للموافقة، مع مراعاة الوسائل التكنولوجية المتاحة. ويقابل ذلك المادة الجديدة (٧-١، بند ٢) من قانون حماية البيانات الفرنسي[٣١٦].

ومن ثمَّ يتعين على المتحكم في مواقع الإنترنت الحصول على رضاء واضح وصريح من النائب القانوني عن القاصر قبل جمع أو معالجة أو تداول بياناته الشخصية، ويتطلب هذا الأمر من المتحكم أن يبذل بعض الجهد في هذه الحالات، مستخدمًا في ذلك كافة الوسائل التكنولوجية المتاحة، للتيقن من استقبال النائب

---

(315)- C. QUENNESSON, Thèse prècité, p. 132 .

(٣١٦)- يُترك الأمر للمتحكم للحصول على إذن الوالدين على معالجة بيانات الطفل، والتحقق من أنه صادر ممن يملك السلطة الأبوية، مع احترام مبدأ الحصول على الحد الأدنى للبيانات، راجع:
B CHARRIER, op. cit., p. 336; Th. DOUVILLE, op. cit., p. 44 .
ويدعو الأخير إلى إنشاء نهج وطني لتحديد الهوية إلكترونيًا من شأنه أن ييسر تحديد هوية الوالدين على نحو موثوق.

القانوني إشعارًا كافيًا منه بشأن طريقة جمع ومعالجة البيانات والتأكد من حصول رضائه بها.

على الرغم من أن الهدف من نص المادة (٢/٨) من اللائحة الأوروبية يتمثل في توفير الحماية اللازمة للقصر ضد استغلال بياناتهم عبر الإنترنت، وذلك من خلال الاعتماد على موافقة الوالدين وتقييمهم لمدى خطورة المعالجة على خصوصية أطفالهم، إلا أنه يظل من الصعب تصور وجود آليات فعّالة ومتميزة لضمان الحصول على هذه الموافقة من صاحب السلطة الأبوية[٣١٧]، دون أن تكون عرضة لتحايل القاصر[٣١٨].

علاوة على ذلك، ينبغي التعامل بحذر عند تناول مفهوم "الوسائل التكنولوجية المتاحة" التي أشارت إليها اللائحة الأوروبية والقانون الفرنسي، حيث تُترك هذه الوسائل لتقدير المتحكم دون تقديم توضيح دقيق حول كيفية التحقق من هوية صاحب السلطة الأبوية. فعلى سبيل المثال، قد يتطلب الأمر تقديم الوالدين مستندات تثبت الهوية والنسب للقاصر الذي يقل عمره عن (١٥ عامًا في فرنسا)، إلا أن هذه المستندات، في الواقع، قد لا تُعد دليلاً قاطعًا على أحقية الشخص في ممارسة السلطة الأبوية[٣١٩].

---

(317)- Géraldine CRIQUI-B-BARTHALAIS, La protection des libtertés individuelles sur le réseau Internet, Thèse Paris II- Panthéon-Assas, 2018, p. 152 .

حيث ترى عدم فاعلية رضاء أصحاب السلطة الأبوية عن القاصر، وتعرب عن أسفها أن حماية القصر فيما يتعلق بخدمات الإنترنت تتم من خلال منظور حماية البيانات الشخصية والالتزام بالحصول على رضاء الشخص على معالجة بياناته.

[٣١٨]– ومن ذلك على سبيل المثال، قيام المتحكم بإدراج مربع اختيار بسيط à simple case cocher على الموقع للحصول على التعبير عن الرضاء، أو حتى إدراج متطلبات معقدة، مثل اشتراط إنشاء توقيع إلكتروني وإرفاق نسخة من أوراق الهوية، وما إلى ذلك. انظر:

Laurélenn BEGNY, Règlement général sur la protection des données personnelles: vers une remise en cause du modèle français? Mémoire pour le Master, Université de Poitiers, 2017, p. 68 .

(319)- G. CRIQUI-BARTHALAIS, Thèse précite, p. 153 .

(ISSN: 2537- 0758)

وبإمعان النظر في أحكام اللائحة الأوروبية نجد أنها لا توضح على نحو دقيق كيفية تنفيذ موافقة صاحب السلطة الأبوية وضوابطه؛ مما يؤدي إلى وجود صعوبات في إثبات هذه الموافقة عند تنفيذها في البيئة الرقمية، ويثير العديد من التساؤلات؛ إذ يُفترض قيام موقع الإنترنت بطلب الحصول على البريد الإلكتروني للوالدين من القاصر، أو حتى العنوان البريدي لمحل الإقامة إذا كان هو الحل الأكثر أمانًا(٣٢٠). فضلاً عن كيفية تحقق المواقع من صحة النيابة القانونية على القاصر، وهي مسألة ليست يسيرة وتتعارض مع السرعة التي هى من أبرز سمات العصر الرقمي.

هذا و الملاحظ انه لم تتضمن اللائحة الأوروبية، بالإضافة إلى القوانين المصرية والإماراتية والفرنسية، تحديدا للوسائل أو الآليات الكفيلة بضمان الحصول على موافقة النائب القانوني فيما يتعلق بمعالجة بيانات القاصر، أو التحقق من أن الشخص المعني يتمتع بالصفة القانونية التي تخوله التعبير عن هذه الموافقة نيابة عن القاصر (٣٢١).

وامام هذا الفراغ التشريعى تثور عدة تساؤلات حول الوسيلة المناسبة للحصول على هذه الموافقة، وما إذا كان من الضروري أن تتم بطريقة إلكترونية أو رقمية حصراً، أم أنه يمكن قبولها بوسائل أخرى.؟

في الواقع، قد تلجأ بعض مواقع التواصل الاجتماعي والتطبيقات الإلكترونية، والرقمية إلى استخدام طرق وأساليب معينة للحصول على موافقة النائب القانوني عن القاصر، مثل تضمين مصطلحات تقنية غامضة في سياسة الخصوصية. هذه المصطلحات تمنح المتحكم حرية واسعة في التصرف بالبيانات التي يتم جمعها عن القصر، مما يثير تساؤلات جدية حول مشروعية المعالجة المستندة إلى موافقة النائب القانوني، خاصة إذا لم يكن قد قرأ سياسة الخصوصية المحددة أو لم يتمكن من فهم طبيعة أساليب المعالجة وأهدافها(٣٢٢).

---

(320)- A. DEBET, op. cit., no 6 .

(321)- Lignes directrices 5/2020, op. cit., no 130, p. 31 .

(٣٢٢)– انظر، لقاط لبيب. ، د. هاشمي حسن، "حماية المعطيات ذات الطابع الشخصي للطفل: قراءة على ضوء أحكام القانون رقم ١٨–٧"، مجلة العلوم القانونية والسياسية، جامعة الشهيد حمة لخضر– الوادي، الجزائر، المجلد ١١، العدد ١، إبريل ٢٠٢٠. ، ص ١٠٥.

وفي هذا السياق، يقدم مجلس حماية البيانات الأوروبي توجيهات محددة بشأن تنظيم موافقة صاحب السلطة الأبوية، حيث يوصي بالحصول على معلومات محدودة عن الشخص الذي يمنح الإذن للقاصر، مثل بيانات الاتصال بأحد الوالدين أو الوصي. ويستند المجلس في توصياته إلى المادة (٢/٨) من اللائحة الأوروبية، التي تُلزم المتحكم ببذل جهود معقولة للتحقق من صحة صدور الموافقة من صاحب السلطة الأبوية، وإلى المادة (٥/١-ج) من اللائحة، التي تنص على ضرورة تقليل البيانات الشخصية إلى أدنى حد ممكن[٣٢٣].

وجدير بالذكر أن الإجراء الذي يعتمده المتحكم، سواء للتحقق من بلوغ المستخدم السن القانوني للموافقة أو للتأكد من توافر صفة النيابة القانونية للشخص الذي يعبر عن الموافقة نيابة عن القاصر، يرتبط بمستوى مخاطر المعالجة والتكنولوجيات المتاحة. ففي حالات جمع ومعالجة البيانات منخفضة المخاطر، كاستخدام المتحكم بيانات القاصر لأغراض داخلية بحتة دون الكشف عنها أو تداولها، يكون الإجراء المطلوب للحصول على موافقة النائب القانوني أقل صرامة، وقد يتم عبر وسائل بسيطة مثل البريد الإلكتروني.

وعلى النقيض، في حالات جمع ومعالجة البيانات التي قد تمثل انتهاكًا لخصوصية القاصر، كاستخدام المتحكم هذه البيانات أو تداولها مع أطراف ثالثة، ينبغي أن تكون الإجراءات المتبعة للحصول على موافقة النائب القانوني أكثر صرامة وحذرًا. في هذه الحالة، قد يتطلب الأمر تقديم أدلة إضافية من النائب القانوني، لتمكين المتحكم من التحقق من صحة المعلومات وتوثيقها. ويأتي هذا التطبيق اتساقًا

---

Harjono, D. (2022). Legal development of the validity of electronic mortgage certificates in the land registration system in indonesia. Yustisia Jurnal Hukum, 11(2), 110. https: //doi. org/10. 20961/yustisia. v11i2. 61111 .Iswari, D. (2023). Examining the legal standing of digital signatures under civil and ite laws. Policy Law Notary and Regulatory Issues (Polri), 2(2), 142-154. https: //doi. org/10. 55047/polri. v2i2. 603 .

(323)- Lignes drectrices 5/2020, op. cit., no 136, p. 32 .

(ISSN: 2537- 0758)

مع المادة (١/٧) من اللائحة الأوروبية، التي تشترط إثبات موافقة صاحب البيانات على المعالجة[٣٢٤].

وتشير إرشادات مجلس حماية البيانات الأوروبي إلى مثال عملي لكيفية تحقق المتحكم من صدور موافقة صاحب السلطة الأبوية. فعندما تسعى إحدى منصات الألعاب الإلكترونية إلى ضمان عدم اشتراك العملاء القاصرين في خدماتها إلا بموافقة الوالدين أو ولي الأمر، **توصي الإرشادات باتباع الخطوات التالية:**

**الخطوة الأولى:** يُطلب من المستخدم تحديد ما إذا كان عمره يتجاوز ١٦ عامًا أو أقل من ذلك (أو أي سن آخر محدد للموافقة الرقمية). وإذا أشار المستخدم إلى أنه لم يبلغ السن الأدنى للموافقة الرقمية، يتم الانتقال إلى الخطوات التالية.

**الخطوة الثانية:** يتم إخطار الطفل بأنه يلزم الحصول على موافقة الوالدين أو الوصي على معالجة البيانات قبل تقديم الخدمة. ويُطلب من المستخدم تقديم عنوان البريد الإلكتروني للوالدين أو الوصي.

**الخطوة الثالثة:** يتواصل المتحكم عبر البريد الإلكتروني مع الوالد أو الوصي للحصول على موافقته على المعالجة، مع بذل جهود معقولة للتحقق من أن الشخص البالغ المعني هو صاحب السلطة الأبوية.

---

[٣٢٤]– قريب من ذلك، انظر: د. عصام محمد رشيد منصور، قوانين حماية خصوصية الأطفال على الإنترنت، قراءة في القانون الأمريكي COPPA مع استعراض للموقف العربي من مثل هذه القوانين، مجلة دراسات المعلومات، جمعية المكتبات والمعلومات السعودية، العدد السادس، سبتمبر ٢٠٠٩. وانظر أيضًا:

Lignes drectries 5/2020, op. cit., no 137, pp. 31-32 .

وتشير هذه الإرشادات إلى أنه يمكن للمراقب في هذه الحالة، على سبيل المثال، أن يطلب من الوالدين أو الوصي دفع مبلغ رمزي قدره (٠,٠٠١ يورو) عن طريق التحويل المصرفي، على أن تتضمن الرسالة المرتبطة بالمعاملة تأكيد موجز بأن صاحب الحساب المصرفي هو صاحب السلطة الأبوية للمستخدم، وينبغي عند الاقتضاء توفير طريقة بديلة للتحقق من رضاء الوالدين، حرصًا على تجنب المعاملة التمييزية غير المبررة للأشخاص الذين ليس لديهم حساب مصرفي. راجع:

Lignes directrices/2020, op. cit., p. 33, marge 68 .

**الخطوة الرابعة:** في حال تقديم شكوى، يقوم المتحكم في المنصة باتخاذ إجراءات إضافية للتحقق من سن المستخدم وضمان امتثال الإجراءات للقواعد المنظمة[٣٢٥].

ويُستخلص من ذلك أن المتحكم يمكنه إثبات بذله لجهود معقولة للتحقق من صحة الموافقة المقدمة من الطفل عند تقديم الخدمات إليه، أو التأكد من صدور الموافقة عن صاحب السلطة الأبوية، وذلك بما يتماشى مع المادة (٢/٨) من اللائحة الأوروبية. ومع ذلك، ينبغي على المتحكم، كقاعدة عامة، تجنب استخدام وسائل تحقق تقتضي إفراطًا غير مبرر في جمع البيانات الشخصية.

ويُقر مجلس حماية البيانات الأوروبي بأن هناك حالات قد تجعل من عملية التحقق أمرًا بالغ الصعوبة. فعلى سبيل المثال، قد لا يقدم الأطفال الذين يعبرون عن موافقتهم ما يثبت أعمارهم، أو قد يكون من العسير التحقق بسهولة من توافر صفة النيابة القانونية لمن يدعي تمثيل القاصر[٣٢٦].

وفي الواقع، يتمتع صاحب البيانات باستقلالية كاملة فيما يتعلق بإبداء الموافقة على معالجة بياناته الشخصية والتحكم في عملية المعالجة. وبالتالي، يكون للقاصر، عند بلوغه سن الموافقة الرقمية، الحق في إقرار الموافقة الصادرة عن صاحب السلطة الأبوية أو الإذن الصادر منه لمعالجة بياناته الشخصية نيابة عنه. كما يحق له تعديل بياناته أو سحب موافقته بنفسه، وفقًا للمادة (٣/٧) من اللائحة الأوروبية.

ومن الناحية العملية، إذا لم يقم صاحب البيانات بأي إجراء، كالتعديل أو السحب، بعد بلوغه السن القانونية، فإن الموافقة على المعالجة أو الإذن بها من قبل صاحب السلطة الأبوية ستظل أساسًا قانونيًا صحيحًا لاستمرار المعالجة[٣٢٧].

من الجدير بالذكر أنه، وفقًا للحيثية رقم (٣٨) من اللائحة الأوروبية، لا يُشترط الحصول على موافقة أحد الوالدين أو الوصي في سياق خدمات الوقاية أو المشورة المقدمة مباشرة إلى الطفل. فعلى سبيل المثال، لا ينبغي أن يتطلب توفير خدمات حماية الطفل عبر الإنترنت، مثل خدمات الرسائل الفورية، الحصول على إذن مسبق من صاحب السلطة الأبوية[٣٢٨].

---

(325)- Lignes directrices 5/2020 Examples 23, op. cit., no 138- 143m p. 33 .
(326)- Lignes directrices 5/2020, op. cit., no 144- 146, p. 33 .
(327)- Lignes directrices 5/2020, op. cit., no 150, p. 34 .
(328)- Lignes directries 5/2020, op. cit., no 147-149, p. 34 .

(ISSN: 2537- 0758)

وعلى الرغم من ذلك، يكشف الواقع العملى الرقمي عن إمكانية تحايل القاصر على شروط وقواعد التسجيل في المواقع التي يرغب في استخدامها، من خلال الإقرار ببلوغه سن الموافقة الرقمية خلافًا للحقيقة، والتعبير عن الموافقة على معالجة بياناته الشخصية بمفرده بدلاً من نائبه القانوني. هذا السلوك يتعارض بوضوح مع متطلبات صدور التعبير عن الإرادة من أشخاص بلغوا السن المحددة للموافقة الرقمية وفقًا للقانون المطبق.

وتُسهم بعض منصات التواصل الاجتماعي في تعزيز هذا النمط من السلوك، حينما لا تولي اهتمامًا كافيًا للتحقق من بلوغ مستخدميها السن القانونية للتسجيل[٣٢٩]. ومن جهة أخرى، غالبًا ما يكون القاصر بمفرده خلف شاشة جهاز الحاسوب أو الهاتف المحمول، دون رقابة من النائب القانوني الممثل له. وبالتالي، يصبح الحصول على موافقة النائب القانوني، الذي قد يكون غائبًا عن العالم الرقمي، مهمة شديدة التعقيد بالنسبة للمواقع الإلكترونية[٣٣٠].

ولمواجهة هذه الإشكالية، قد يكون من المفيد إلزام المتحكم الذي يسعى إلى جمع ومعالجة البيانات الشخصية للقاصر أو تداولها، بالتحقق من الحصول على موافقة صريحة من النائب القانوني للقاصر أو أي شخص مسؤول عنه، مع التأكد من صحة هذه الموافقة. ويمكن تحقيق ذلك من خلال اعتماد بعض الإجراءات الضرورية، مثل: تقديم استمارة مخصصة تُوقع من ولي الأمر وإرسالها عبر البريد الإلكتروني أو الفاكس. أو إجراء اتصال هاتفي مرئي مع ولي الأمر للتحقق من موافقته. أو التحقق من رقم بطاقة الائتمان التي قد تُستخدم كوسيلة للتواصل أو التأكيد. أو استخدام البريد الإلكتروني مصحوبًا بتوقيع إلكتروني لضمان موثوقية الموافقة المقدمة[٣٣١].

---

[٣٢٩]– في هذا المعنى، انظر: لبيب لقاط، د. هاشمي حسن، مرجع سابق، ص ص ١٠٥– ١٠٦.

[330]- C. SCAULTZ, La protection du mineur à l'aune des réseaux sociaux, op. cit., p. 45 .

[٣٣١]– جدير بالذكر أنه يتم الاستعانة بهذه الحلول لتعزيز الحصول على رضاء النائب عن القاصر النائب عن القاصر (دون الثالثة عشرة) في القانون الأمريكي بشأن حماية خصوصية الأطفال عبر الإنترنت الصادر في ٢١ أكتوبر عام ١٩٩٨. راجع، د. عصام محمد رشيد منصور، مرجع سابق، ص ص ١٣٦، ١٣٧، وخاصة ص ١٤٢؛ د. خالد صلاح حنفي محمود، حماية الطفل العربي

## المبحث الثالث
## اثار الموافقة

**تمهيد وتقسيم**:

رسم المشرع الأوروبي إطارًا واضحًا لأحكام الموافقة الرقمية، مبينًا دورها في التحقق من مشروعية معالجة البيانات الشخصية، وأهميتها كاستثناء من الحظر المفروض على معالجة بعض أنواع البيانات. وسار على هذا النهج كل من المشرعين الفرنسي والمصري، والاماراتى. ومع ذلك، فإن هذه الموافقة، رغم الحرص على التأكد من استيفاء شروطها ونسبتها لصاحب البيانات، تُعد من الحقوق التي يمكن لصاحب البيانات العدول عنها في أي وقت. ويعتبر هذا العدول أحد الضمانات القانونية التي تسعى لحماية مصالح صاحب البيانات، باعتباره الطرف الأضعف في مواجهة المتحكم في البيانات الذي يمتلك القدرة التقنية. ورغم أن العدول عن الموافقة لا يسري على المعالجات السابقة، فإنه يقلل من القوة الإلزامية للموافقة، حفاظًا على حقوق صاحب البيانات.

ويُلاحظ أن الموافقة، في حال عدم إقامة الدليل على وجودها بشكل صحيح، تعد كأنها لم تكن. ومن ثم، يتعين على المتحكم إعطاء أولوية لإثبات صحة الموافقة، لضمان مواجهة أي ادعاءات أو نزاعات قد تُثار بشأنها.

وفى ضوء ما تقدم، ندرس الاحكام المنظمة لاثار الموافقة الرقمية على معالجة البيانات الشخصية، من خلال بيان دور الموافقة الرقمية في معالجة البيانات الشخصية فى المطلب الاول، واحكام إثباتها فى المطلب الثانى، واحكام الحق في العدول عنها فى المطلب الثالث.

---

على الإنترنت في ضوء الاتجاهات العالمية المعاصرة "دراسة تحليلية"، مجلة الطفولة والتربية، يصدرها المجلس العربي للطفولة والتنمية، القاهرة، ع ٣٤، ٢٠١٩، ص ١١٤ وما بعدها.

(٢٠٢٤). استغلال الأطفال في المواد الإباحية عبر الإنترنت. مجلة التراث الثقافي، ١(٢)، ٠-٠. https: //doi. org/10. 21608/jhc. 2024. 367489

(ISSN: 2537- 0758)

## المطلب الاول
## دور الموافقة الرقمية

وفقًا للقواعد العامة في العقد، يُعبَّر عن الإرادة من الناحية القانونية من خلال الموافقة، التي تُعد جوهر العقد وأساس وجوده. ولهذا، يمنح القانون للموافقة أهمية قصوى، بحيث لا يمكن أن يقوم العقد بدونها[٣٣٢]. ومع ذلك، إذا كانت الموافقة تُعد شرطًا لازمًا لقيام العقد ووجوده، فإن النظرة الفاحصة لنصوص اللائحة الأوروبية والقانونين المصري والفرنسي تُظهر أن الموافقة قد لا تكون دائمًا شرطًا لازمًا لقيام المعالجة[٣٣٣].

ففي بعض الحالات، لا ترتبط الموافقة بالمعالجة من حيث الوجود أو العدم بالدرجة نفسها التي ترتبط بها بالعقد، إذ تسمح النصوص القانونية بتجاوز شرط الموافقة في ظل وجود أسباب ومبررات منصوص عليها. وفي ظل هذا الواقع، أصبحت الصفة الآمرة للموافقة موضع تساؤل عميق، بالنظر إلى إمكانية الالتفاف عنها في العديد من الحالات لدواعٍ وذرائع متنوعة، مرتبطة بالأوضاع المصرح بها قانونًا، دون وجود ضوابط دقيقة أو تحديد واضح.

---

(332)- F. TRRÉ, P. SIMLER, Y. LEQUETTE et F. CHÈNEDè, op. cit., no 78, p. 88 .

(٣٣٣)– يثير هذا الموقف استغراب البعض، حيث تتساءل قائلة: طالما لم يكن الرضاء لازمًا لصحة المعالجة، فلماذا يصبح "شرط أساسي" منذ دخول اللائحة الأوروبية حيزالتنفيذ؟ وترى أن إقرار الرضاء يشهد على رغبة المشرع الأوروبي في تعزيز سيطرة صاحب البيانات على استخدام بياناته. وتجرى مقارنة مع مبدأ سلطان الإرادة المعروف في القانون المدني، وترى في اشترط الرضاء هنا شكل من أشكال "الرق الإرادي servitude volontaire تأسيسًا على أن الرضاء هو السند والمبرر لتقييد حريات صاحب البيانات، كما أن رضاء صاحب البيانات يتيح للمسئول عن المعالجة بالتنصل من الحظر الذي تقرضه بعض النصوص، فيدخله في نطاق الإباحة.

F. ROGUE, Capacité et consentement au traitment de données à caractére personnel et au contrat, op. cit.,. 371 .

**ومما يُفهم من ذلك**، أن دور الموافقة في سياق معالجة البيانات يظل محدودًا بحدود ما تمنحه النصوص القانونية من أهمية. فقد تُعلي هذه النصوص من شأن الموافقة في بعض الأحيان، وتجعلها شرطًا أساسيًا لقيام المعالجة، بينما قد تقلل من أهميتها أو تستبعدها تمامًا في أحيان أخرى، متى توافرت بدائل أو مبررات قانونية تغني عنها. ويعتمد ذلك على رؤية المشرع، التي غالبًا ما تتوارى خلف العبارة الفضفاضة "في الأحوال المصرح بها قانونًا[٣٣٤].

وفي إطار البحث عن الدور الحقيقي للموافقة في مجال معالجة البيانات الشخصية، ومن خلال تحليل نصوص اللائحة الأوروبية والقانونين الفرنسي والمصري، والاماراتى، يظهر أن الموافقة يمكن أن تؤدي دورًا وقائيًا متميزًا لصاحب البيانات، خاصة عندما تكون الأساس القانوني لإجراء عملية المعالجة.

ومن ناحية أخرى، قد تتخذ الموافقة دورًا مختلفًا، يتمثل في تمكين المسؤول عن المعالجة من تجاوز القيود التي تفرضها النصوص القانونية. وفي هذه الحالة، لا تسهم الموافقة في حماية الشخص صاحب البيانات، بل تمنح المتحكم أو المعالج فرصة للتحلل من الحظر المفروض على جمع البيانات أو معالجتها. **ونوضح كل ما تقدم فى الفروع التالية:-**

## الفرع الاول

## الدور الوقائى للموافقة في حماية البيانات الشخصية

اوضحنا سابقاً انه تشترط اللائحة الأوروبية والقانونين الفرنسى والمصري والاماراتى الحصول على موافقة صريحة من صاحب البيانات قبل الشروع في جمع أو معالجة بياناته، ما لم ينص القانون على خلاف ذلك أو توجد أسس قانونية أخرى يمكن الاستناد إليها لإجراء المعالجة. **وفيما يلي نتناول هذا الأمر بالتفصيل:**

---

[٣٣٤]- وهذا هو راى جانب من الفقة المصرى، ونؤيده بحق استنادا الى الاحكام الواردة فى قانونى حماية البيانات المصرى والاماراتى. انظر: د: تامر الدمياطى، المرجع السابق، ص ١٠٠.

(ISSN: 2537- 0758)

## أولاً- موافقة صاحب البيانات على معالجة بياناته كشرط قانوني لمشروعية المعالجة:

تُظهر النصوص المنظمة للموافقة أنها ليست الشرط الوحيد لمشروعية المعالجة، حيث توجد إلى جانبها عدة شروط أخرى. ويؤدي توافر أحد هذه الشروط إلى إمكانية استبعاد الموافقة كشرط ملزم. وبالتالي، تُعد الموافقة أحد الخيارات أو الأسس القانونية المتعددة التي يمكن للمتَحكِّم الاستناد إليها عند معالجة البيانات[٣٣٥].

**وفي هذا السياق،** تقدم المادة (٦) من اللائحة الأوروبية "الموافقة" كأحد الشروط الستة لمشروعية معالجة البيانات الشخصية .(Licéité du traitement) وتشير المادة إلى أن معالجة البيانات تكون مشروعة فقط عند استيفاء **أحد الشروط التالية:**

أ- موافقة صاحب البيانات على معالجة بياناته الشخصية لغرض أو أكثر من الأغراض المحددة[٣٣٦].

ب-أن تكون المعالجة ضرورية لتنفيذ عقد يكون صاحب البيانات طرفًا فيه، أو لتنفيذ إجراءات سابقة على التعاقد بناءً على طلبه.

ت-أن تكون المعالجة ضرورية للامتثال لالتزام قانوني يخضع له المتحكم.

ث-أن تكون المعالجة ضرورية لحماية المصالح الحيوية لصاحب البيانات أو لشخص طبيعي آخر.

ج- أن تكون المعالجة ضرورية لحماية المصلحة العامة أو تدخل ضمن نطاق ممارسة السلطة العامة المخولة للمتحكم.

---

[٣٣٥]- ومع ذلك فإن بعض الدول قد تعتبره شرطًا متميزًا في هذا المجال. قد يصل أحيانًا إلى مصاف المبدأ الدستوري، لارتباطه بالحق في حماية البيانات. راجع:

Groupe de travail "article 29". Avis 15/2011 sur la définition du consentement, op. cit., p. 7 .

[٣٣٦]- يجري النص الفرنسي للمادة (١/٦) بند (أ) من اللائحة الأوروبية لحماية البيانات الشخصية على ما يلى:

"1- Le traitement n'est licite que si, et dans la mesure oú, au moins une des conditions suivantes est remplie: a) la personne concernée a consenti au traitement de ses données à caractére personnel pour une ou plusieurs finalités spcifiques؛"

ح- أن تكون المعالجة ضرورية لأغراض المصالح المشروعة التي يسعى إليها المتحكم أو الغير، ما لم تعلو عليها مصالح أو حقوق وحريات صاحب البيانات التي تتطلب حماية بياناته الشخصية، وبخاصة عندما يكون صاحب البيانات طفلاً. وتجدر الإشارة إلى أن هذه الفقرة لا تنطبق على المعالجات التي تُجريها السلطات العامة أثناء أداء مهامها.

وهذا التوجه يتماشى مع ما نصت عليه الحيثية رقم (٤٠) من اللائحة الأوروبية، التي أكدت المبادئ ذاتها[٣٣٧].

وفي الاتجاه ذاته، أعادت المادة (١/٥) من قانون المعلوماتية والحريات الفرنسي المعدّل التأكيد على أن الحصول على موافقة صريحة من صاحب البيانات يُعد أحد شروط مشروعية معالجة البيانات الشخصية، وذلك بما يتماشى مع الشروط المنصوص عليها في المادة (٤) بند (١١) والمادة (٧) من اللائحة الأوروبية[٣٣٨]. وقد جاء نص هذه المادة متسقًا مع حكم المادة (٦) من اللائحة الأوروبية المشار إليها، مما يعكس تبنيًا واضحًا لمبادئها الأساسية.

ولتوضيح دور الموافقة في هذا السياق، يصبح من الضروري استكشاف العلاقة بين الموافقة وبين الشروط الأخرى لمشروعية المعالجة، خاصة تلك المتعلقة بتنفيذ العقود أو الامتثال للالتزامات القانونية أو أداء مهام تتعلق بالمصلحة العامة أو تحقيق المصالح المشروعة للمتَحكِّم.

ورغم أهمية ترتيب الأسس القانونية "الاختيارية" لمشروعية المعالجة الوارد في نص المادة (٦) من اللائحة الأوروبية، إلا أن ذلك لا يعني أن الموافقة هي دائمًا

---

[٣٣٧]- تنص الحيثية ٤٠ من اللائحة الأوروبية لحماية البيانات على أن: "لكي تكون معالجة البيانات الشخصية مشروعة، يجب أن تستند إلى رضاء صاحب البيانات أو أن تستند إلى أي أساس مشروع آخر ينص عليه القانون، إما في هذه اللائحة أو في قاعدة من قواعد القانون أو قانون الاتحاد، على النحو المنصوص عليه في هذه اللائحة...".

[٣٣٨]- تحدد المادة (٥) من قانون المعلوماتية والحريات، المعدلة بالمادة (١) من المرسوم رقم ١١٢٥- ٢٠١٨ الصادر في ١٢ ديسمبر ٢٠١٨، شروط مشروعية معالجة البيانات، وهي تتطابق تمامًا مع نص المادة (٦) من اللائحة الأوروبية.

(ISSN: 2537- 0758)

الأساس الأنسب لإضفاء المشروعية على معالجة البيانات الشخصية. فقد بدأ النص بالموافقة في مقدمة الأسس القانونية، ثم انتقل إلى استعراض الأسس الأخرى، مثل العقود والالتزامات القانونية، قبل التطرق إلى ميزان المصالح، سواء كانت عامة أو حيوية أو مشروعة.

ومع ذلك، لا يعني ترتيب الموافقة في الصدارة ضمن النص أن الالتزام بها أكثر مرونة من الأسس الأخرى لمشروعية المعالجة[٣٣٩]. علاوة على ذلك، فإن الحصول على الموافقة لا يعفي المتحكم من الالتزامات الأخرى المفروضة عليه بموجب النصوص القانونية ذات الصلة. وتشمل هذه الالتزامات الالتزام بمبادئ معالجة البيانات الشخصية، مثل الشفافية، المشروعية، الإنصاف، الدقة، والنزاهة، كما نصت عليه المادة (٥) من اللائحة. بالإضافة إلى ذلك، يجب الامتثال للشروط الخاصة بموافقة الأطفال على المعالجة، الواردة في المادة (٨) من اللائحة.

ومع ذلك، قد يتجه المتحكم في الواقع العملي إلى تفضيل عدم الاعتماد على الموافقة كأساس لمعالجة البيانات، والبحث عن أساس قانوني آخر. ويعود هذا التوجه غالبًا إلى التخوف من عدم استيفاء الموافقة للشروط المنصوص عليها في اللائحة أو من إمكانية سحبها من قبل صاحب البيانات، مما يؤدي إلى فقدان المشروعية القانونية للمعالجة. في هذا الإطار، يمكن النظر إلى الموافقة على أنها أساس قانوني "احتياطي"، يُلجأ إليه فقط في حال غياب الأسس الأخرى لمشروعية المعالجة[٣٤٠].

وبالرغم مما تقدم، تظل الموافقة أكثر اتساعًا مقارنة بالأسس الأخرى لمشروعية المعالجة. حيث يتم تفسير الأسس الأخرى، مثل الضرورة لتنفيذ عقد أو تحقيق المصالح المشروعة للمسؤول عن المعالجة، بصورة ضيقة من قبل اللجنة الوطنية للمعلوماتية والحريات (CNIL) ومجموعة "المادة ٢٩" (التي استبدلها مجلس حماية

---

[٣٣٩]– ويشير فريق عمل "المادة ٢٩" إلى أن الأسس الخمسة التي تلي الموافقة تفرض معيار "الضرورة"، مما يجد بشكل كبير من المجال الذي يمكن أن تنطبق فيه. انظر:

Groupe de travail "article 29". Avis 15/2011 sur la définition du consentement, op cit., p. 8 .

[340]- F. ROGUE, op. cit., p. 371 .

البيانات الأوروبي). وقد يؤدي هذا التفسير إلى الحد من إمكانية الاستناد إلى هذه الأسس في بعض الحالات. ولهذا السبب، يمكن للمسؤول عن المعالجة أن يرى في الموافقة خيارًا أكثر موثوقية وضمانًا لمشروعية المعالجة التي يقوم بها، خاصة عندما تُراعى الشروط القانونية المقررة بشأنها[٣٤١].

وفي السياق ذاته، نص قانون حماية البيانات المصري في المادة (٢) منه على أنه يشترط لجمع البيانات الشخصية أو معالجتها أو الإفصاح عنها أو إفشائها بأي وسيلة من الوسائل، الحصول على "موافقة" صريحة من الشخص المعني بالبيانات، "أو "أن تكون المعالجة ضمن الأحوال المصرح بها قانونًا[٣٤٢].

كما أوضح المشرع المصرى في المادة (٦) من القانون ذاته أن المعالجة الإلكترونية تُعد مشروعة وقانونية في حال توافر أي من الحالات الآتية:-

١. موافقة الشخص المعني بالبيانات لتحقيق غرض محدد أو أكثر.
٢. أن تكون المعالجة لازمة وضرورية لتنفيذ التزام تعاقدي، أو تصرف قانوني، أو لإبرام عقد لصالح الشخص المعني بالبيانات، أو لمباشرة أي من إجراءات المطالبة بحقوقه القانونية أو الدفاع عنها.
٣. تنفيذ التزام قانوني ينظمه القانون، أو أمر صادر عن جهات التحقيق المختصة، أو بناءً على حكم قضائي.
٤. تمكين المتحكم من القيام بالتزاماته أو ممارسة حقوقه المشروعة، شريطة ألا يتعارض ذلك مع الحقوق والحريات الأساسية للشخص المعني بالبيانات.

هذا ويُلاحظ أن صياغة نص القانون المصري تُعد ترديدًا لحكم اللائحة الأوروبية إلى حد كبير، حيث يُفهم منه إمكانية تجاوز شرط الموافقة في الأحوال المصرح بها قانونًا (وفق المادة ٢)، أو عند تحقق أحد شروط مشروعية المعالجة الأخرى الواردة في المادة (٦) من القانون، التي لا تشترط وجود الموافقة بشكل صريح.

---

[341]- F. ROGUE, op. cit., p. 371 .

[٣٤٢]- تنص المادة (٢) من قانون حماية البيانات الشخصية المصري على أن: "لا يجوز جمع البيانات الشخصية أو معالجتها أو الإفصاح عنها أو إفشائها بأي وسيلة من الوسائل إلا بموافقة صريحة من الشخص المعني بالبيانات، أو في الأحوال المصري بها قانونًا".

(ISSN: 2537- 0758)

كما يُلاحظ أن المشرع المصري قد اعتمد نهجًا موحدًا في التعامل مع الموافقة، وجعلها شرطًا عامًا يشمل جميع جوانب البيانات الشخصية، سواء جمعها أو معالجتها أو الإفصاح عنها أو إفشائها، دون تمييز بين الطبيعة الخاصة لكل حالة منها. في المقابل، اقتصر المشرع الأوروبي على تناول الموافقة ضمن نطاق معالجة البيانات الشخصية فقط، نظرًا لأنها تُعد من أكثر أنواع التعامل على البيانات خطورة.

ومن جهة أخرى، يثار تساؤل حول مصير البيانات التي جرى جمعها أو حفظها قبل صدور قانون حماية البيانات الشخصية المصري، ودون الحصول على الموافقة المسبقة من صاحبها. في هذا الصدد، لا تبدو هناك صعوبة تُذكر، حيث نصت المادة الرابعة من مواد إصدار قانون حماية البيانات على التزام المخاطبين بأحكامه بتوفيق أوضاعهم بما يتوافق مع القانون ولائحته التنفيذية خلال سنة من تاريخ صدور اللائحة.

وقد اهتم المشرع المصري بمواجهة مختلف صور الانتهاكات المتعلقة بالموافقة، واعتبر التعامل غير المشروع على البيانات، سواء تم ذلك دون موافقة صاحبها أو خارج الأحوال المصرح بها قانونًا، جريمة جنائية. وفرض عقوبات تتراوح بين الغرامة التي لا تقل عن مائة ألف جنيه ولا تجاوز مليون جنيه. وإذا كان الانتهاك مقابل منفعة مادية أو أدبية، أو بقصد الإضرار بصاحب البيانات، فقد تضاعفت العقوبات لتصل إلى الحبس لمدة لا تقل عن ستة أشهر وغرامة لا تزيد على مليوني جنيه، أو بإحدى هاتين العقوبتين (المادة ٣٦).

كما شدد المشرع العقوبات في حالة الانتهاكات التي تتعلق بالبيانات الشخصية الحساسة، حيث نص على عقوبة الحبس لمدة لا تقل عن ثلاثة أشهر، وغرامة لا تقل عن خمسمائة ألف جنيه ولا تجاوز خمسة ملايين جنيه، أو بإحدى هاتين العقوبتين (المادة ٤١).

وقد أقرت اللائحة الأوروبية مجموعة من الغرامات الإدارية المالية كجزاء على مخالفة الأحكام المتعلقة بالموافقة الواردة فيها، وفقًا لما نصت عليه المادة (٨٣). وقد قُسمت هذه الغرامات إلى فئتين: الفئة الأولى: غرامة مالية قدرها ١٠ ملايين يورو، أو في حالة الشركات، تصل إلى ٢% من إجمالي الدخل السنوي للسنة المالية

السابقة، أيهما أعلى. و تنطبق هذه الغرامة على مخالفات معينة محددة في المادة (83/4)[٣٤٣]. والفئة الثانية: غرامة مالية قدرها ٢٠ مليون يورو، أو في حالة الشركات، تصل إلى ٤% من إجمالي الدخل السنوي للسنة المالية السابقة، أيهما أعلى. تنطبق هذه الغرامة على مخالفات أشد خطورة، كما هو موضح في المادة(٨٣/٥)[٣٤٤]. وقد أشرنا سابقًا إلى أن اللجنة الوطنية للمعلوماتية والحريات في فرنسا (CNIL) قد استندت إلى هذا النص لتوقيع غرامة مالية كبيرة على شركة Google نتيجة عدم امتثالها للاشتراطات الخاصة بموافقة صاحب البيانات.

## ثانياً- حالات إجراء المعالجة دون الحاجة لصدور موافقة من صاحب البيانات:

الموافقة على المعالجة الرقمية للبيانات الشخصية امر واجب كاصل عام للقيام باى معالجة رقمية للبيانات الشخصية، ولكن يبدوا ان هذا الاصل عليه خروج نوضحه فى الفقرات الاتية:

---

[٣٤٣]- تشير المادة ٨٣ فقرة ٤ من اللائحة العامة لحماية البيانات إلى أن هذه الغرامات تنصب على مخالفة الأحكام الآتية: (أ) التزامات المتحكم والمعالج بموجب المواد (٨و١١و ٢٥) إلى (٣٩و ٤٢و ٤٣) من اللائحة؛ (ب) التزامات هيئة التصديق بموجب المادتين (٤٢ و ٤٣) (ج) التزامات الهيئة المسئولة عن رصد مدونات قواعد السلوك عملاً بالمادة (٤/٤١) من اللائحة.

[٣٤٤]- وفقًا للمادة (٨٣) فقرة (٥) من اللائحة العامة لحماية البيانات تنصب هذه الغرامات على مخالفة الأحكام الآتية: (أ) المبادئ الأساسية للمعالجة، بما في ذلك الشروط المطبقة على الرضاء بموجب المواد (٥ و ٦و ٧و ٩) من اللائحة (ب) الحقوق التي يتمتع بها أصحاب البيانات بموجب المواد من ١٢ إلى ٢٢ (ج) نقل البيانات الشخصية إلى متلقى موجود في بلد ثالث أو إلى منظمة دولية وفقًا للمواد من ٤٤ إلى ٤٩ (د) جميع الالتزامات الناشئة عن قانون الدول الأعضاء المعتمدة بموجب الفصل التاسع (هـ) عدم الامتثال لأمر قضائي أو تقييد مؤقت أو نهائي لمعالجة البيانات أو تعليق تدفقات البيانات التي أمرت بها السلطة الإشرافية وفقًا للمادة (٢/٥٨)، أو منع حق الوصول المقصود بالمخالفة للمادة (٥٨) فقرة (١) من اللائحة.

(ISSN: 2537- 0758)

- **الطبيعة غير الملزمة للموافقة الرقمية:**

الموافقة تُعدّ أحد الأسس القانونية التي تمنح المتحكم صلاحية معالجة البيانات الشخصية أو جمعها أو إفشاءها. ومع ذلك، يُلاحظ من تحليل النصوص القانونية المنظمة للموافقة في القانون المصري والاماراتى واللائحة الأوروبية أن هذه النصوص تمنحها طابعًا غير مُلزِم. إذ تتيح للمتحكم إمكانية التخلي عنها في حالات محددة، وتنفيذ المعالجة الإلكترونية للبيانات الشخصية استنادًا إلى أي أساس قانوني آخر منصوص عليه في التشريع الخاص بحماية البيانات، أو في الحالات التي يسمح بها القانون. وبالتالي، تُعتبر المعالجة في هذه الحالات مشروعة وقانونية، حتى في حال عدم الحصول على موافقة صاحب الشأن.

ويُستدل من ذلك أن وجود إحدى هذه الحالات يغني عن اشتراط الموافقة، مما يجعل الموافقة، في هذا السياق، بمثابة "أساس احتياطي"، كما أشرنا سابقًا. وهذا قد يفتح المجال للمسؤول عن المعالجة لتجاهل شرط الموافقة عند تحقق إحدى هذه الحالات. **وسوف نقوم بتوضيح هذه المسائل على النحو الآتي:**

١- **إمكانية الاستغناء عن الموافقة في الأحوال المصرح بها قانونًا:** أشارت المادة (٢) من قانون حماية البيانات الشخصية المصري إلى القاعدة العامة التي تحظر التعامل مع البيانات الشخصية دون الحصول على موافقة صريحة من صاحب البيانات، أو في الحالات المصرح بها قانونًا.

ويُفهم من ذلك أن النص يُجيز الاستغناء عن موافقة الشخص في بعض الحالات المصرح بها قانونًا، ومنها على سبيل المثال: إذا كانت معالجة البيانات تحقق مصلحة صاحبها وتعذّر الاتصال به، أو إذا كان الحصول على موافقته يتطلب جهدًا شاقًا، أو إذا كانت المعالجة مطلوبة بموجب القانون أو وفقًا لاتفاق يكون الشخص المعني طرفًا فيه، أو إذا كانت المعالجة تهدف إلى الحفاظ على المصالح الحيوية للشخص المعني في حال عدم قدرته، جسديًا أو قانونيًا، على التعبير عن موافقته. كما تشمل الحالات التي ترتبط بتحقيق مصلحة عامة أو مصلحة مشروعة يسعى

إليها المسؤول عن المعالجة، بشرط مراعاة حقوق الشخص المعني وحرياته الأساسية[٣٤٥].

وفي تقدير البعض من الفقه وبحق فإن إطلاق المشرّع لعبارة "في الأحوال المصرح بها قانونًا" بهذه الصيغة العامة قد يُفرغ شرط الموافقة من محتواه، ويهدمه من أساسه إذا لم يقم المشرّع بتحديد هذه الأحوال بوضوح، وحصرها في أضيق نطاق ممكن بما يتماشى مع أهداف حماية البيانات الشخصية[٣٤٦].

**٢- الاستغناء عن موافقة صاحب البيانات متى كانت المعالجة ضرورية لتنفيذ عقد:**

تشير المادة ١/٦ (ب) من اللائحة الأوروبية[٣٤٧] إلى شروط إضافية لمشروعية المعالجة بخلاف موافقة صاحب البيانات، ومن بين هذه الشروط أن تكون المعالجة ضرورية لتنفيذ عقد يكون صاحب البيانات طرفًا فيه، أو لتنفيذ الإجراءات التمهيدية اللازمة قبل التعاقد بناءً على طلب صاحب البيانات.

وبالمثل، نصت المادة ٦ من قانون حماية البيانات الشخصية المصري على شروط أخرى تُجيز مشروعية المعالجة دون الحاجة إلى الموافقة. ومن بين هذه الشروط أن تكون المعالجة ضرورية لتنفيذ التزام تعاقدي أو إجراء قانوني، أو لإبرام عقد لصالح الشخص المعني بالبيانات. كما تشمل الحالات التي تكون فيها المعالجة مطلوبة لمباشرة أي من إجراءات المطالبة بالحقوق القانونية للشخص المعني أو الدفاع عنها (المادة ٦، بند ٢).

---

[٣٤٥]- د. عمرو طه بدوى، التنظيم القانوني لمعالجة البيانات الشخصية- دراسة تطبيقية على معالجة تسجيلات المراقبة البصرية، أكاديمية أبو ظبي القضائية، ٢٠١٩، ص ص ١٠٩، ١١٠.

[٣٤٦]- د. تامر الدمياطى، المرجع السابق، ص ١٠٦.

[٣٤٧]- يقابلها المادة (٥) بند ٢ من قانون المعلوماتية والحريات الفرنسي المعدل بالقانون ٤٩٣ لسنة ٢٠١٨ بشأن حماية البيانات الشخصية.

(ISSN: 2537- 0758)

**٣- عدم اشتراط الحصول على الموافقة عند تنفيذ التزام قانوني أو عمل قضائي أو مراعاة المصلحة العامة:**

تُعدّ المعالجة مشروعة وفقًا للمادة ١/٦ (ج) من اللائحة الأوروبية[٣٤٨] إذا كانت ضرورية للامتثال لالتزام قانوني يخضع له المسؤول عن المعالجة، مثل الالتزامات المرتبطة بمجالات الضرائب أو الضمان الاجتماعي التي تُفرض على صاحب العمل. وقد تبنى القانون المصري و القانون الاماراتى هذا النهج في المادة (٦)، بند ٣، مصرى، والفقرة ١٠ من المادة ٤ غماراتى، حيث اعتبر المعالجة مشروعة وقانونية في حالات "تنفيذ التزام ينظمه القانون، أو استجابة لأمر صادر من جهات التحقيق المختصة، أو تنفيذًا لحكم قضائي".

وعلاوة على ذلك، تُعتبر المعالجة مشروعة إذا كانت ضرورية لأداء مهمة تُنفّذ للمصلحة العامة، أو في سياق ممارسة السلطة العامة التي تم تخويلها للمسؤول عن المعالجة، وذلك وفقًا للمادة ١/٦ (هـ) من اللائحة الأوروبية[٣٤٩].

مع ذلك، ينبغي التأكيد على أن الاستغناء عن الموافقة في هذه الحالات يرتبط ارتباطًا وثيقًا بالامتثال للالتزام القانوني المحدد. وفي حال تجاوز المسؤول عن المعالجة حدود هذا الالتزام، يحق للشخص المعني الاعتراض على أي إجراء يتعلق بالمعالجة إذا كان خارج نطاق هذا الالتزام القانوني[٣٥٠].

**٤- عدم اشتراط الموافقة في حالة مراعاة المصالح المشروعة للمسئول عن المعالجة أو الغير أو صاحب البيانات:**

تُعتبر المعالجة مشروعة، بغض النظر عن توفر موافقة الشخص، وفقًا للمادة (١/٦) (و) من اللائحة الأوروبية[٣٥١]، إذا كانت المعالجة ضرورية لتحقيق مصالح

---

[٣٤٨]- يقابلها المادة (٥) بند ٣ من قانون المعلوماتية والحريات الفرنسي المعدل، سبق ذكره.

[٣٤٩]- يقابلها المادة (٥) بند ٥ من قانون المعلوماتية والحريات الفرنسي المعدل، سبق ذكره.

[٣٥٠]- انظر: د. سامح عبد الواحد التهامي، الحماية القانونية للبيانات الشخصية: دراسة في القانون الفرنسي (القسم الثاني)، مجلة الحقوق، جامعة الكويت، المجلد ٣٥، العدد ٤ ديسمبر ٢٠١١، ص ٢٥٣.

[٣٥١]- يقابلها المادة (٥) بند ٦ من قانون المعلوماتية والحريات الفرنسي المعدل، سبق ذكره.

مشروعة للمسؤول عن المعالجة أو الغير، بشرط ألا تتعارض هذه المصالح مع الحقوق والحريات الأساسية لصاحب البيانات، والتي تستلزم حماية بياناته الشخصية، خاصة إذا كان صاحب البيانات طفلاً. ويُستثنى من هذا الحكم المعالجات التي تقوم بها السلطات العامة أثناء أداء واجباتها.

وقد استقى المشرّع المصري، والمشرع الاماراتى هذا المفهوم في المادة (٦)، بند ٣، من قانون حماية البيانات الشخصية المصرى، والفقرة ٨ من المادة الرابعة فى القانون الاماراتى، حيث نص على أن المعالجة تكون مشروعة إذا كانت تهدف إلى "تمكين المتحكم من القيام بالتزاماته أو أي ذي صفة من ممارسة حقوقه المشروعة، ما لم يتعارض ذلك مع الحقوق والحريات الأساسية للشخص المعني بالبيانات". وبذلك، تُقيَّد المصلحة المشروعة بعدم تجاوز حقوق وحريات صاحب البيانات الأساسية.

وتُضيف اللائحة الأوروبية إلى حالات مشروعية المعالجة– التي يمكن أن تتم دون موافقة الشخص– حالة أن تكون "المعالجة ضرورية لحماية المصالح الحيوية لصاحب البيانات أو لشخص طبيعي آخر" (المادة ٦/١ (د) من اللائحة)[٣٥٢]. ويُركز جوهر هذه الحالة على مصلحة صاحب البيانات ويهدف إلى تحقيق الأغراض ذاتها التي يُراد بها الموافقة التعاقدية، لا سيما إذا كان الشخص المعني غير قادر، من الناحية البدنية أو القانونية، على التعبير عن موافقته. ومع ذلك، لم يتناول القانونان المصري والاماراتى هذه الحالة ضمن الأحكام التي تنظّم مشروعية وقانونية المعالجة، رغم أهميتها العملية في بعض الظروف.

**وفي الختام**، يتضح من تحليل الأحكام المتعلقة بمشروعية وقانونية المعالجة في كل من اللائحة الأوروبية والقانونان المصري، والاماراتى، أن موافقة صاحب البيانات لا تُعطى الأولوية المطلقة ضمن شروط معالجة البيانات. كما أنها لا تُعتبر بالضرورة الأساس المفضل بالنسبة للمسؤولين عن المعالجة، إذ يتم الاعتماد بشكل متزايد على أسس قانونية أخرى تتيح المرونة في التعامل مع البيانات الشخصية.

---

[٣٥٢]– يقابلها المادة (٥) بند ٤ من قانون المعلوماتية والحريات الفرنسي المعدل، سبق ذكره..

(ISSN: 2537- 0758)

## الفرع الثاني
## دور الموافقة في الاستثناء من أحكام حماية البيانات الشخصية

بالإضافة إلى دور الموافقة في إضفاء المشروعية على المعالجة، قد تكون الموافقة ضرورية للسماح للمسؤول عن المعالجة بالتحلل من بعض القواعد أو الاشتراطات القانونية المرتبطة بعملية المعالجة. وأبرز مثال على ذلك هو الحظر المفروض على معالجة البيانات الحساسة أو نقل البيانات عبر الحدود. فالأصل في هذه الحالة هو الحظر، لكن يُسمح للمسؤول عن المعالجة، في بعض الحالات، بتجاوز هذا الحظر عن طريق الحصول على موافقة صريحة من صاحب البيانات. وبذلك، تُصبح الموافقة وسيلة استثنائية تُمنح للمسؤول عن المعالجة لتجاوز القيود القانونية المفروضة، شريطة أن تكون هذه الموافقة مستوفية للشروط القانونية المقررة، بما يضمن احترام حقوق وحريات صاحب البيانات.

وفي ظل هذا الوضع، يشكك البعض في دور الموافقة في مثل هذه الحالات، مشيرين إلى أنها قد تبتعد عن كونها أداة لحماية صاحب البيانات[٣٥٣]، بل على العكس قد تصبح وسيلة للإضرار به. إذ تُتيح الموافقة للمسؤول عن المعالجة تجاوز محظورات كان الأصل فيها المنع.

وعلى الرغم من أن هذا الرأي يعكس واقعًا مبررًا وحرصًا على تعزيز حماية صاحب البيانات، إلا أنه لا يتماشى مع منطق ونصوص اللائحة الأوروبية. فاللائحة تُجيز للمسؤول عن المعالجة تجاوز الحظر المفروض على المعالجة في بعض الحالات بناءً على أسس قانونية أخرى غير الموافقة. ومن بين هذه الحالات، كما نصت المادة ٢/٩ (ج) من اللائحة، أن تكون المعالجة ضرورية لحماية المصالح الحيوية لصاحب البيانات أو لشخص آخر. وهذا النهج يعكس توازناً بين حماية البيانات الشخصية وتمكين المعالجة في ظروف استثنائية تقتضيها المصلحة العامة أو المصالح الحيوية، مما يجعل الموافقة إحدى الوسائل الممكنة، لكنها ليست الوسيلة الحصرية لتجاوز الحظر. **ونوضح تفاصيل كل ما تقدم كما يلى:**

---

(353)- A. DEBET, op. cit., no 3 ets .

## أولاً- موافقة صاحب البيانات كمصدر للاستثناء من حظر معالجة البيانات الحساسة:

تنص المادة ١/٩ من اللائحة الأوروبية على حظر معالجة البيانات الحساسة التي تكشف عن الأصل العرقي أو الإثني، الآراء السياسية، المعتقدات الدينية أو الفلسفية، أو عضوية النقابات. ويشمل الحظر أيضًا معالجة البيانات الجينية، والبيومترية المستخدمة لتحديد هوية الشخص الطبيعي بشكل فريد، بالإضافة إلى البيانات المتعلقة بالصحة، أو الحياة الجنسية للشخص الطبيعي، أو ميوله الجنسية.

ورغم إقرار الفقرة الأولى من المادة ٩ بمبدأ الحظر المطلق لمعالجة هذه الفئات من البيانات، جاءت الفقرة الثانية (البند "أ") لتقيّد نطاق هذا الحظر. حيث أجازت معالجة البيانات الحساسة في حالة الحصول على موافقة صريحة من صاحب البيانات لمعالجة بياناته لأغراض محددة. ومع ذلك، يظل هذا الاستثناء محكومًا بقيود قانونية أخرى، حيث يجوز لقانون الاتحاد الأوروبي أو قوانين الدول الأعضاء أن تنص صراحة على عدم جواز رفع الحظر عن معالجة البيانات الحساسة، حتى بموافقة صاحب البيانات.

وفقًا للائحة الأوروبية لحماية البيانات، تم التوسع في تحديد الحالات المستثناة من الحظر المفروض على معالجة البيانات الحساسة، حيث وردت تسع حالات (المادة ٢/٩ من اللائحة، البنود من "ب" إلى "ي") تتيح معالجة البيانات الحساسة. ومن هذه الحالات، ما إذا كانت المعالجة ضرورية للوفاء بالالتزامات أو لممارسة الحقوق القانونية المتعلقة بالمتحكم أو صاحب البيانات، وفقًا لقوانين العمل أو الضمان الاجتماعي أو الحماية الاجتماعية (المادة ٢/٩-ب). كما تشمل الاستثناءات الحالات التي تكون فيها المعالجة ضرورية لحماية المصالح الحيوية لصاحب البيانات أو لشخص طبيعي آخر، في حالة وجود مانع جسدي أو قانوني يمنع صاحب البيانات من التعبير عن الموافقة (المادة ٢/٩-ج). وتشمل الاستثناءات أيضًا الضرورة لإقامة الدعاوى القضائية أو مباشرتها (المادة ٢/٩-و)، والأسباب المرتبطة بالمصلحة العامة (المادة ٢/٩-ز)، وكذلك الأغراض المتعلقة بالأرشفة

(ISSN: 2537- 0758)

للصالح العام أو البحث العلمي أو التاريخي أو الأغراض الإحصائية (المادة ٢/٩-ي).

أما قانون حماية البيانات الشخصية المصري، فقد نص في المادة (١٢) على أنه: "يُحظر على المتحكم أو المعالج، سواء كان شخصًا طبيعيًا أو اعتباريًا، جمع البيانات الشخصية الحساسة أو نقلها أو تخزينها أو حفظها أو معالجتها أو إتاحتها إلا بترخيص من المركز. وفي غير الحالات المصرح بها قانونًا، يجب الحصول على موافقة كتابية وصريحة من الشخص المعني. وفيما يتعلق بمعالجة بيانات الأطفال، يتطلب الأمر الحصول على موافقة ولي الأمر. ويتم ذلك كله وفقًا للمعايير والضوابط التي تحددها اللائحة التنفيذية لهذا القانون".

ويتضح من النص أن التعامل مع البيانات الحساسة من قِبَل أطراف عملية المعالجة (المتحكم أو المعالج) يرتبط، نظرًا لأهميتها وخطورتها على خصوصية الأفراد، بشروط محددة. فمن ناحية أولى، يتطلب ذلك الحصول على ترخيص من مركز حماية البيانات الشخصية[٣٥٤]. ومن ناحية ثانية، تشترط المادة المذكورة الحصول على موافقة كتابية وصريحة من الشخص المعني بالبيانات، وذلك باستثناء الحالات المصرح بها قانونًا. إلا أن العبارة الأخيرة تظل غامضة، إذ لم يحدد القانون تلك الحالات أو يصفها بصورة دقيقة، وهو ما يمثل قصورًا كان يمكن تلافيه. فقد كان بإمكان المشرع المصري أن يتبنى نهجًا مشابهًا للائحة الأوروبية، التي أوردت هذه الحالات بشكل واضح، بدلاً من ترك الأمر مفتوحًا ودون تحديد.

وبالنظر إلى الوضع في ظل القانون المصري، فإن شرط الحصول على ترخيص من مركز حماية البيانات الشخصية هو شرط لا يمكن الاستغناء عنه لرفع الحظر عن معالجة البيانات الحساسة. أما الشرط الآخر، وهو موافقة الشخص المعني،

---

[٣٥٤]- خصص قانون حماية البيانات الشخصية المصري الفصل التاسع منه لمركز حماية البيانات الشخصية (المواد ١٩-٢٥)، وهو هيئة عامة اقتصادية، تتبع الوزير المعني بشئون الاتصالات وتكنولوجيا المعلومات، وتكون لها الشخصية الاعتبارية وتهدف إلى حماية البيانات الشخصية وتنظيم معالجتها وإتاحتها، وقد حدد القانون اختصاصاته (م ١٩) وتسكيل مجلس إدارته (م ٢٠) واختصاصات مجلس الإدارة (م ٢١)، وكيفية انعقاد اجتماعاته (م ٢٢)، وتعيين رئيسه التنفيذي (م ٢٣).

فيبدو من حيث الظاهر شرطًا لازمًا وجوهريًا. ومع ذلك، فإن النص يجيز استبعاد شرط الموافقة "في الأحوال المصرح بها قانونًا"، مما يشير إلى إمكانية وجود حالات في القانون تُخول المتحكم أو المعالج التعامل مع البيانات الحساسة دون الحصول على موافقة صاحبها.

**ثانيا- الموافقة على نقل البيانات الشخصية عبر الحدود**:

تهدف قواعد حماية البيانات الشخصية إلى ضمان التدفق الحر للبيانات عبر الحدود من خلال وضع آليات ملائمة لنقل البيانات، بما يكفل توفير ضمانات فعالة لحماية حقوق أصحاب البيانات. وتخضع هذه الآليات لرقابة صارمة وشفافة، مع الاعتماد على وسائل فعالة تضمن حقوق الأفراد عند نقل البيانات عبر الحدود الجغرافية.

وفي إطار اللائحة الأوروبية لحماية البيانات، يُحظر نقل البيانات الشخصية خارج نطاق الاتحاد الأوروبي، إلا إذا تم النقل إلى بلد أو منظمة يتوافر فيها مستوى الحماية الذي تقره المفوضية الأوروبية (المادة ٤٥ من اللائحة). كما يجوز نقل البيانات في حال وجود ضمانات حماية مناسبة للنقل، وفقًا لما تنص عليه المادة ٤٦ من اللائحة[٣٥٥].

أما في الحالات التي لا يتوافر فيها مستوى الحماية المقرر في اللائحة أو ضمانات مناسبة لنقل البيانات، فلا يجوز نقل البيانات الشخصية إلى بلد ثالث أو منظمة دولية، إلا إذا تحقق أحد الشروط الواردة في المادة ١/٤٩ من اللائحة. وأبرز هذه الشروط هو الحصول على موافقة صريحة من صاحب البيانات على النقل المقترح، شريطة إعلامه بالمخاطر المحتملة المتعلقة بالنقل إلى جهة لا توفر مستوى الحماية أو الضمانات المناسبة (المادة ١/٤٩-أ)[٣٥٦].

---

[٣٥٥]- تنظم اللائحة العامة لحماية البيانات الشخصية GDPR أحكام نقل البيانات الشخصية إلى دول أخرى أو منظمات دولية. في الفصل الخامس (المواد من ٤٥ إلى ٥٠) من اللائحة. كما تناولها قانون المعلوماتية والحريات الفرنسي المعدل في المادتين "١٢٣ و ١٢٤ منه".

[٣٥٦]- تضيف المادة (١/٤٩) من اللائحة العامة لحماية البيانات GDPR (ويقابلها المادة ١٢٤ من قانون المعلوماتية والحريات الفرنسي) حالات أخرى يجوز فيها نقل البيانات خارج الحدود، عند عدم توافر مستوى حماية، وهى أن يكون.....".

(ISSN: 2537- 0758)

وعلى غرار الاستثناءات الخاصة بالبيانات الحساسة، تشير اللائحة الأوروبية (المادة ٤٩/١-و) إلى إمكانية نقل البيانات الشخصية دون اشتراط الحصول على موافقة صاحب البيانات، إذا كان النقل ضروريًا لحماية مصالحه الحيوية أو مصالح أشخاص آخرين، في حالة عدم قدرة صاحب البيانات على التعبير عن إرادته لأسباب جسدية أو قانونية. وقد تبنى قانون المعلوماتية والحريات الفرنسي المعدل أحكامًا مماثلة في المادتين ١٢٣ و١٢٤.

أما القانون المصري، فقد نصت المادة (١٥) على اشتراط الحصول على موافقة صريحة من صاحب البيانات أو من ينوب عنه عند نقل أو مشاركة أو تداول أو معالجة البيانات الشخصية إلى دولة لا يتوافر فيها مستوى الحماية المنصوص عليه في القانون. ويُستثنى من ذلك بعض الحالات التي يمكن فيها إجراء النقل[٣٥٧]، **وتشمل:**

١. الحفاظ على حياة الشخص المعني بالبيانات، وتوفير الرعاية الطبية أو العلاج أو إدارة الخدمات الصحية له.

---

ب- النقل ضروري لأداء عقد بين صاحب البيانات والمسئول عن المعالجة أو لتنفيذ التدابير التعاقدية المسبقة المتخذة بناءً على طلب صاحب البيانات؛

ج- النقل ضروري لإبرام أو تنفيذ عقد مبرم لمصلحة صاحب البيانات بين المسئول عن المعالجة وشخص طبيعي أو اعتباري آخر؛

د- النقل ضروري لأسباب مهمة تتعلق بالمصلحة العامة؛

هـ- النقل ضروري لمباشرة إجراءات المطالبة القضائية بالحقوق أو الدفاع عنها".

[٣٥٧]- تحظر المادة (١٤) من قانون حماية البيانات الشخصية المصري إجراء عمليات نقل للبيانات الشخصية التي تم جمعها أو تجهيزها للمعالجة إلى دولة أجنبية أو تخزينها أو مشاركتها إلا بتوافر مستوى من الحماية لا يقل عن المستوى المنصوص عليه في هذا القانون، وبترخيص أو تصريح من المركز (مركز حماية البيانات الشخصية)، وتحدد اللائحة التنفيذية لهذا القانون السياسات والمعايير والضوابط والقواعد اللازمة لنقل أو تخزين أو مشاركة أو معالجة أو إتاحة البيانات الشخصية عبر الحدود وحمايتها.

٢. تنفيذ التزامات بما يضمن إثبات حق أو ممارسته أمام جهات العدالة أو الدفاع عنه.
٣. إبرام عقد أو تنفيذ عقد قائم أو يتم إبرامه بين المسؤول عن المعالجة وأطراف أخرى، بما يحقق مصلحة الشخص المعني بالبيانات.
٤. تنفيذ إجراء متعلق بتعاون قضائي دولي.
٥. وجود ضرورة أو التزام قانوني يهدف إلى حماية المصلحة العامة.
٦. إجراء تحويلات مالية إلى دولة أخرى وفقًا لتشريعاتها السارية.
٧. تنفيذ اتفاق دولي ثنائي أو متعدد الأطراف تكون جمهورية مصر العربية طرفًا فيه.

## ثالثاً- اشتراط موافقة صاحب البيانات بالتسويق الإلكتروني المباشر له:

يلجأ العديد من المتحكمين في البيانات إلى استخدام نظم الاتصالات الإلكترونية بشكل يومي لأغراض التسويق المباشر (Direct Marketing)[٣٥٨]. بهدف جذب

[٣٥٨]– يقصد بالتسويق الإلكتروني: "إرسال أي رسالة أو بيان أو محتوى إعلاني أو تسويقي بأي وسيلة تقنية أيًا كانت طبيعتها أو صورتها تستهدف بشكل مباشر أو غير مباشر ترويج سلع أو خدمات أو التماسات أو طلبات تجارية أو سياسية أو اجتماعية أو خيرية موجهة إلى أشخاص بعينهم. راجع المادة (١) من قانون حماية البيانات الشخصية المصري. وجدير بالذكر أن اللائحة الأوروبية GDPR لم تبين المقصود بعبارة "التسويق المباشر"، ولا يوجد تعريف قانوني مقبول بشكل عام على المستوى الأوروبي لهذا المفهوم، وبناءً على اقتراح لائحة البرلمان والمجلس الأوروبي في ١٨ سبتمبر ٢٠١٩ بشأن احترام الحياة الخاصة وحماية البيانات الشخصية في الاتصالات الإلكترونية، تقترح هيئة حماية البيانات الشخصية Autorité protection des données) APD) تحديد المقصود بالتسويق المباشر بأنه: "أي اتصال يهدف إلى الترويج لمنظمة أو شخص أو خدمات أو منتجات، سواء كانت مدفوع أو مجاني، بالإضافة إلى العلامات التجارية أو الأفكار، يوجه بشكل مباشر من منظمة أو شخص بتصرف في سياق تجاري أو غير تجاري، لشخص طبيعي أو أكثر في سياقر خاص أو

(ISSN: 2537- 0758)

انتباه ملايين الأفراد المعنيين. وغالبًا ما تشتمل هذه الأنشطة على معالجة منتظمة للبيانات الشخصية، مما أدى إلى انتشارها بشكل كبير وتحولها إلى بيئة خصبة لاستغلال البيانات. هذا الاستخدام المكثف قد يُعرض البيانات الشخصية لانتهاكات محتملة لأحكام القوانين التي تنظم حماية البيانات الشخصية[٣٥٩].

ولضمان حماية حقوق أصحاب البيانات، توجهت التشريعات المختلفة إلى فرض قيود صارمة على عملية الاتصال الإلكتروني لأغراض التسويق المباشر. ومن أبرز هذه القيود اشتراط الحصول على موافقة مسبقة من صاحب البيانات. وفي هذا الإطار، تؤكد المادة (١٧) من قانون حماية البيانات الشخصية المصري على حظر إجراء أي اتصال إلكتروني بغرض التسويق المباشر **إلا إذا توافرت الشروط الآتية: الشرط الاول،** هو الحصول على موافقة صريحة من الشخص المعني. **والشرط الثانى،** هو أن يتضمن الاتصال هوية الجهة المنشئة والمرسلة. **والشرط الثالث،** هو توفير عنوان صحيح وكافٍ للمرسل يسهل الوصول إليه. **والشرط الرابع،** هو الإشارة إلى أن الاتصال الإلكتروني موجه لأغراض التسويق المباشر. **والشرط الخامس،** هو وضع آليات واضحة وسهلة تمكن الشخص المعني بالبيانات من رفض الاتصال الإلكتروني أو العدول عن موافقته على تلقي هذه الرسائل.

ويتضح من نص المادة المذكورة أن الموافقة تعد شرطًا أساسيًا لصحة الاتصال الإلكتروني في هذه الحالة، ولا يجوز للمتحكم الاستناد إلى أي أساس قانوني آخر

---

مهني، بأى وسيلة، بما في ذلك معالجة البيانات الشخصية". انظر: التوصية رقم ٢٠٢٠/١ الصادرة عن هيئة حماية البيانات الشخصية، ص ٨.

[٣٥٩]– راجع: التوضية رقم ٢٠٢٠/٠١ المؤرخة ١٧ يناير ٢٠٢٠ الصادرة عن هيئة حماية البيانات الشخصية المتعلقة بمعالجة البيانات الشخصية لأغراض التسويق المباشر، ص ٨.

RECOMMANDATION no 01/2020 du 17 janvier 2020, relative aux traitements de données à caractère personnel à des fins marketing drect, Autorité de protection des données (APD), disponible sur le site: https: //www. dpopro. be/fr/news/recommandation-relative-aux-traitement-de-donnees-a-caractere-personnel-a-des-fins-demarketing-direct-public-par-lapd/

للتخلي عن هذا الشرط. كما يتعين أن تتوافر جميع الشروط المذكورة مجتمعة لضمان صحة الاتصال الإلكتروني بغرض التسويق المباشر.

**ومن جهة أخرى**، يلتزم المرسل للاتصال الإلكتروني لأغراض التسويق المباشر بما يلي: الالتزام بالغرض التسويقي المحدد. والالتزام بعدم الإفصاح عن بيانات الاتصال الخاصة بالشخص المعني. والالتزام بالاحتفاظ بسجلات إلكترونية تثبت موافقة الشخص المعني وتعديلاتها أو عدم اعتراضه على استمرار تلقي الاتصالات التسويقية، وذلك لمدة ثلاث سنوات من تاريخ آخر إرسال. والالتزام بالقواعد والشروط التي تحددها اللائحة التنفيذية للقانون بشأن التسويق الإلكتروني (المادة ١٨ من القانون).

وفيما يتعلق بالاتحاد الأوروبي، تشترط اللائحة الأوروبية (المادة ١١/٤) توافر جميع عناصر وشروط صحة الموافقة عند إجراء التسويق المباشر. وينطبق ذلك أيضًا على حق الشخص في العدول عن هذه الموافقة أو الاعتراض على معالجة بياناته في هذا السياق. كما تفرض اللائحة حماية خاصة عند استخدام بيانات الأطفال لأغراض التسويق المباشر، لا سيما في خدمات مجتمع المعلومات المقدمة مباشرة إلى الطفل (الحيثية ٣٨ من اللائحة الأوروبية).

## المطلب الثاني
## إثبات الموافقة الرقمية

لا شك أن إثبات موافقة صاحب البيانات يُعد من المسائل ذات الأهمية البالغة في إطار حماية البيانات الشخصية. فإثبات هذه الموافقة يُمكّن من التأكد من صحتها وصدورها عن الشخص الذي يملك الحق القانوني في التعبير عنها، سواء كان ذلك الشخص هو صاحب البيانات نفسه أو نائبه القانوني.

ويحقق إثبات الموافقة فوائد جوهرية للمتحكم في البيانات، لا سيما عند الاستناد إلى هذه الموافقة كشرط لمشروعية المعالجة. كما يتعاظم دور هذا الإثبات في حال الحاجة إلى تقديم دليل على وجود الموافقة وصحتها عند حدوث نزاع بين المتحكم وصاحب البيانات.

(ISSN: 2537- 0758)

وفي الواقع العملي، قد يُطلب من المتحكم تقديم هذه الأدلة في سياق إجراءات إنفاذ قانون حماية البيانات المعمول به. لذلك، يتعين على المتحكمين إنشاء وحفظ الأدلة التي تثبت صدور التعبير عن الموافقة من الشخص المعني. بمعنى آخر، ينبغي أن تكون الموافقة موثقة وقابلة للتحقق منها بما يضمن تحقيق الشفافية والمصداقية(٣٦٠).

## أولاً- عبء إثبات حصول موافقة صاحب البيانات:

يقع عبء إثبات صدور الموافقة من صاحب البيانات على عاتق المتحكم(٣٦١). وقد نصت المادة (١/٧) من اللائحة الأوروبية لحماية البيانات على ذلك بوضوح، حيث جاء فيها: "في الحالات التي تعتمد فيها المعالجة على الموافقة، يجب أن يكون المتحكم قادرًا على إثبات أن صاحب البيانات قد أعطى موافقته على معالجة البيانات الشخصية المتعلقة به. " كما أكدت الحيثية رقم (٤٢) من اللائحة ذاتها على هذا المبدأ بقولها: "عندما تستند المعالجة إلى موافقة صاحب البيانات، يجب أن يكون المتحكم قادرًا على إثبات موافقة هذا الشخص على عملية المعالجة".

ويُعد هذا الالتزام تطبيقًا عمليًا لمبدأ المسؤولية (Accountability)، الذي أصبح من المبادئ الأساسية في معالجة البيانات الشخصية وفقًا للائحة الأوروبية. ويهدف هذا المبدأ إلى ضمان الشفافية وتعزيز الثقة في عمليات معالجة البيانات من خلال توفير آليات واضحة لإثبات الامتثال للقوانين المعنية بحماية البيانات(٣٦٢).

---

(360)- Groupe de travail "article", Avis 15/2011 sur la définition du consentement, op. cit., p. 24 .

(361)- Lignes directrices 5/2020 sur le consentement ay sens du règlement (UE) 2016/679, op. cit., p. 13 .

(٣٦٢)– يلاحظ أنه من حيث المبدأ، سيتعين على المتحكم التحقق من صحة الرضاء، الأمر الذي قد يكون صعبًا في بعض الأحيان، في شأن التساؤل والحلول التي يمكن أن تقدمها التقنيات الحديثة مثل البلوك تشين Blockchain. راجع:

N. WEINBAUM, Le consentement à l'ère du RGPD et de la Blockchain, op. cit., p. 31 .

ويتضح من ذلك أن المتحكم يجب أن يكون قادرًا في جميع الأوقات على تقديم الدليل الذي يثبت حصوله على موافقة صحيحة من المستخدم فيما يتعلق بمعالجة بياناته الشخصية. ويتمتع المتحكم بحرية اختيار الأساليب أو المنهجيات الملائمة التي تضمن الامتثال لالتزامه بإثبات الموافقة، بما يتماشى مع متطلبات اللائحة الأوروبية.

ومع ذلك، ينبغي التنبيه إلى أن التزام المتحكم بإثبات الحصول على الموافقة الصحيحة لا يعني جواز الإفراط في إجراء عمليات معالجة إضافية للبيانات. بل يتعين على المتحكم الاكتفاء بجمع ومعالجة البيانات الضرورية فقط لتحقيق غرض إثبات الموافقة. وبذلك، يلتزم المتحكم بمبدأ تقليل البيانات (Data Minimization) المنصوص عليه في أحكام اللائحة، والذي يتطلب أن تكون البيانات التي يتم جمعها ومعالجتها محدودة ومرتبطة بالغرض المشروع الذي يتم من أجله جمعها[٣٦٣].

وفى هذا السياق ترسخ المادة (٢/٥) من اللائحة الأوروبية لحماية البيانات مبدأ مسؤولية المتحكم (Accountability)، حيث تُلزم المتحكم بالامتثال لمبادئ معالجة البيانات الشخصية، وتؤكد على وجوب أن يكون المتحكم قادرًا على إثبات امتثاله لهذه المبادئ.

كما توضح المادة (١/٢٤) من اللائحة كيفية تحقيق هذا الالتزام، من خلال إلزام المتحكم باتخاذ التدابير الرقمية والتنظيمية المناسبة لضمان إثبات الامتثال لأحكام اللائحة[٣٦٤]. ويشمل ذلك مراجعة هذه التدابير وتحديثها عند الضرورة، مع مراعاة الجوانب التالية: طبيعة المعالجة. ونطاقها ومداها. والأغراض المرجوة منها. ونسبة المخاطر المحتملة الناجمة عن المعالجة. والتأثيرات المحتملة على حقوق وحريات

---

(363)- Lignes directrices 5/220 sur le consentement au sens du règlement (UE) 2016/679, op. cit., no 106, p. 26 .

(٣٦٤)– مثل مبادئ المشروعية والنزاهة والشفافية وتحديد الهدف والدقة والسلامة والسرية وغيرها من المبادئ الواردة في الفقرة الأولى من المادة (٥) من اللائحة الأوروبية، وفي شأن التزامات المتحكم، انظر: دراسة نقدية لقانون حماية البيانات الشخصية رقم ١٥١ لسنة ٢٠٢٠، مرجع سابق، ص ٦٠ وما بعدها.

(ISSN: 2537- 0758)

الأفراد المعنيين بالبيانات[٣٦٥]. ويتطلب هذا النهج من المتحكم أن يكون على دراية تامة بالطبيعة الديناميكية للبيئة التنظيمية والتقنية، وأن يتبنى سياسات وإجراءات مرنة تتيح التكيف مع التحديات الناشئة لضمان الامتثال المستمر للقواعد المنصوص عليها في اللائحة.

ويبقى الالتزام بإثبات الموافقة قائمًا طالما استمر نشاط المعالجة المحدد. ويترتب على ذلك أنه عند اكتمال نشاط المعالجة، لا يجوز للمتحكم الاحتفاظ بدليل إثبات الموافقة لفترة أطول من اللازم. ومع ذلك، يمكن للمتحكم الاحتفاظ بهذه الأدلة لفترة أطول إذا كان ذلك ضروريًا للامتثال لالتزام قانوني، أو لإقامة الدعاوى القضائية أو مباشرتها أو الدفاع فيها. وقد نصت المادة (٣/١٧) من اللائحة الأوروبية[٣٦٦]، في البندين (ب) و(هـ)، على هذه الاستثناءات، مما يضمن تحقيق التوازن بين حماية حقوق الأفراد واحترام متطلبات الامتثال القانوني.

---

[٣٦٥]– تعتمد التدابير التي يجب أن يلجأ إليها المتحكم، لإثبات الامتثال لأحكام اللائحة، ومن بينها الحصول على الرضاء متى كان مطلوبًا لصحة المعالجة، على طبيعة هذه التدابير وحجمها وبنيتها. وعملية معالجة البيانات التي يقوم بها. راجع: منى الأشقر جبور ومحمود جبور، البيانات الشخصية والقوانين العربية: الهمّ الأمني وحقوق الأفراد، المركز العربي للبحوث القانونية والقضائية، مجلس وزراء العدل جامعة الدول العربية، الطبعة الأولى، بيروت– لبنان، ٢٠١٨، ص ١٤٠. وتشير إلى أن هذه المسألة ترتبط بمبدأ المسئولية responsabilité الذي يتصل بآليات الحوكمة الرشيدة، وإمكانات محاسبة المسئول عن تنفيذ مهمة ما".

[٣٦٦]– تقرر المادة (٣/١٧) من اللائحة الأوروبية أن: "لا تنطبق الفقرات ١ و ٢ من هذه المادة (تعني الفقرة الأولى بإقرار الحق في محو البيانات "الحق في النسيان". وتتناول الثانية التزام المتحكم في هذا الشأن) بقدر ما تكون هذه المعالجة ضرورية....

(ب) الامتثال لالتزام قانوني يتطلب إجراء المعالجة المنصوص عليه في قانون الاتحاد أو بموجب قانون الدولة العضو التي يخضع لها المتحكم، أو لأداء مهمة تخدم المصلحة العامة أو تقع في نطاق ممارسة السلطة العامة المخولة للمتحكم؛..... (هـ) لإقامة الدعاوي القضائية أو مباشرتها أو الدفاع فيها. في هذا الصدد، انظر:

Lignes drectrices 5/2020 sur le consentement au sens du règlement (UE) 2016/679, op. cit., no 109, p. 26 .

وهذا التحديد الزمني يعكس مبدأ تقليل البيانات (Data Minimization)، الذي يتطلب من المتحكم معالجة البيانات والاحتفاظ بها فقط للفترة الزمنية التي تكون فيها ضرورية لتحقيق الأغراض المشروعة، مع مراعاة عدم تجاوز الحدود المطلوبة لتحقيق تلك الأغراض.

أما قانون حماية البيانات الشخصية المصري، فقد خلا من النص الصريح على عبء إثبات الموافقة، مكتفيًا بفرض التزام عام على المتحكم بتوفير الإمكانيات اللازمة لإثبات التزامه بتطبيق أحكام القانون. كما ألزم القانون المتحكم بتمكين مركز حماية البيانات من ممارسة التفتيش والرقابة للتأكد من الامتثال (المادة ٤ بند ١٢). وفي السياق ذاته، يلتزم المعالج بتوفير الإمكانيات اللازمة لإثبات التزامه بتطبيق أحكام القانون، وذلك عند طلب المتحكم، فضلًا عن تمكين مركز حماية البيانات من التفتيش والرقابة للتحقق من هذا الالتزام (المادة ٥ بند ١٠). وقد ترك القانون للائحة التنفيذية تحديد السياسات والإجراءات والضوابط والمعايير الفنية التي تحكم هذه الالتزامات، لضمان توحيد التطبيقات العملية وتعزيز الامتثال لأحكام القانون[٣٦٧].

وفى رأى البعض من الفقه فإن إثبات حصول الموافقة على معالجة البيانات يندرج بطبيعته ضمن إطار "إثبات الالتزام بتطبيق أحكام القانون "الواردة في النصوص التشريعية. فهذه العبارة العامة تشمل جميع أحكام قانون حماية البيانات الشخصية، دون استثناء. ولم يحدد القانون المصري طبيعة الإمكانيات المستخدمة لإثبات التزام المتحكم، إذ ترك ذلك للائحة التنفيذية التي تعالج هذه المسائل باعتبارها قضايا تقنية. ويُعد هذا التوجه متسقًا مع نهج القانون العام، الذي يترك التفاصيل التقنية للتنظيم اللائحي، بما يتيح مرونة تعديلها وفق التطورات التقنية المتسارعة، ومن ثم، يمكن القول إن الأحكام الواردة في قانون حماية البيانات الشخصية المصري تكاد تتطابق مع مضمون المادة (٢٤) من اللائحة الأوروبية، التي تُلزم المتحكم باتخاذ التدابير اللازمة لضمان إثبات امتثاله لأحكام اللائحة[٣٦٨].

---

[٣٦٧]– راجع الفقرة الأخيرة من المادة (٤) والمادة (٥) من قانون حماية البيانات الشخصية رقم ١٥١ لسنة ٢٠٢٠.

[٣٦٨]–د. تامر الدمياطى، المرجع السابف، ص ١١٦.

(ISSN: 2537- 0758)

ولا شك أن إلقاء عبء إثبات الموافقة على عاتق المتحكم يتماشى مع دوره باعتباره الجهة المهيمنة على عمليات جمع ومعالجة البيانات الشخصية، بما يمتلكه من إمكانات تقنية وفنية واسعة. وبحكم طبيعة عمله، يتمتع المتحكم بسلطة تحديد الأساليب والمعايير المناسبة للاحتفاظ بالبيانات ومعالجتها والتحكم فيها بما يتوافق مع الغرض أو النشاط المحدد.

ويترتب على ذلك اعتبار المتحكم المسؤول الأساسي عن ضمان مشروعية عمليات المعالجة، بما يتفق مع القواعد القانونية ذات الصلة، ويُحمّله عبء الامتثال الكامل للإطار التنظيمي، مما يعزز من حماية حقوق أصحاب البيانات وضمان الشفافية في جميع مراحل معالجة البيانات الشخصية.

## ثانياً- محل إثبات موافقة صاحب البيانات:

يتعين على المتحكم في البيانات ضمان صدور موافقة صاحب البيانات على عمليات جمع ومعالجة بياناته الشخصية. علاوة على ذلك، يجب أن يكون المتحكم قادرًا على إثبات استيفاء شروط صحة هذه الموافقة، بحيث تكون: حرة، أي صادرة دون إكراه أو ضغط. ومحددة، تتعلق بغرض معين واضح ومعروف مسبقًا. ومستنيرة، تُمنح بناءً على معرفة كاملة بجميع التفاصيل والمخاطر المحتملة. وقاطعة، تعبر عن رغبة واضحة لا لبس فيها. بما يفيد أن الموافقة قد صدرت بشكل قانوني من صاحب البيانات. وأن الموافقة استوفت جميع شروط الصحة المنصوص عليها. وأن عملية المعالجة تمت وفقًا لما هو مذكور في نص الموافقة ودون تجاوز أغراضها.

ولذا، يُلتزم المتحكم في البيانات بتوثيق شروط الحصول على الموافقة لضمان القدرة على إثبات ما الوقائع الاتية[٣٦٩]: تمتع صاحب البيانات بحرية حقيقية في اتخاذ قراره بشأن منح الموافقة أو رفضها، وكذلك حريته في العدول عن الموافقة دون التعرض لأي ضرر. كما يتعين على المتحكم إثبات إنشاء آليات فعالة لضمان عدم ربط منح الموافقة بإبرام عقد (الموافقة "الحرة"). علاوة على ذلك، ينبغي الفصل

(369)- Les guides pratiques du Club de la sécurité de l'information Français "CLUSIF", Le consentement au traitement des données personnelles, p. 6, disponsible sur le site: https: //clusif. fr/publications/faq-le-consentement-au-traitment-de-donnees-personnelles/

الواضح بين أغراض المعالجة المختلفة لضمان أن تكون الموافقة "محددة" أو دقيقة. ويجب تقديم المعلومات المناسبة لأصحاب البيانات عند طلب الحصول على الموافقة، بما يكفل أن تكون "مستنيرة". وأخيرًا، يجب أن يكون التعبير عن إرادة صاحب البيانات إيجابيًا وواضحًا لضمان أن تكون الموافقة "قاطعة".

وفي هذا السياق، أكدت محكمة العدل الأوروبية أن المتحكم في البيانات يتحمل عبء إثبات أن صاحب البيانات قد عبّر عن موافقته من خلال تصرف إيجابي يدل بوضوح على رغبته في معالجة بياناته الشخصية. كما شددت المحكمة على ضرورة أن يحصل صاحب البيانات على معلومات مسبقة مقدمة بطريقة مفهومة، ومتاحة بسهولة، ومصاغة بعبارات واضحة وبسيطة، بحيث تسمح له بتقدير آثار الموافقة وتحديدها بسهولة، بما يضمن صدور الموافقة بصورة مستنيرة وبما يتوافق مع ظروف المعالجة المعنية[٣٧٠].

## ثالثاً- كيفية إثبات موافقة صاحب البيانات:

رغم أن اللائحة الأوروبية تُحمّل المتحكم عبء إثبات الحصول على موافقة صحيحة من صاحب البيانات، إلا أنها لا تحدد بدقة الوسائل التي يجب أن يعتمدها المتحكم للقيام بهذا الإثبات. ومع ذلك، تشير اللائحة إلى ضرورة أن يكون المتحكم قادرًا على إثبات أن صاحب البيانات قد عبّر عن موافقته بشكل صريح، ولغرض محدد وفي سياق معين[٣٧١]. على سبيل المثال، يمكن للمتحكم الاحتفاظ بسجل يتضمن تفاصيل الموافقة التي تم الحصول عليها من الشخص المعني، بحيث يشمل طريقة الحصول على الموافقة، مثل نموذج إلكتروني أو وثيقة موقعة.، وقت الحصول على الموافقة، لتحديد الفترة الزمنية المرتبطة بالموافقة. والمعلومات المقدمة، وهي التفاصيل التي تم تقديمها لصاحب البيانات لتكوين قراره بالموافقة.

---

(370)- Cour de justice de l'Union européenne (2ème ch.), Arrêt du 11 november 2020, op. cit., point 53 ets .

(٣٧١)– راجع المادة (١/٧) من اللائحة الأوربية لحماية البيانات، والحيثية رقم ٤٢ من هذه اللائحة، وأيضًا انظر:

Lignes directrices 5/2020, op. cit., no 107, p. 26 .

(ISSN: 2537- 0758)

ويجب أن يكون المتحكم قادرًا على إثبات أنه قد استوفى التزامه بإبلاغ الشخص المعني بجميع المعلومات الضرورية التي تتيح له اتخاذ قرار مستنير. كما يتعين عليه التأكد من أن جميع الإجراءات التي اتخذها تتوافق مع المعايير القانونية للحصول على موافقة صحيحة، بما في ذلك: ضمان أن تكون الموافقة صادرة بحرية ودون إكراه. وتقديم المعلومات بطريقة واضحة وبسيطة وسهلة الفهم. وضمان أن تكون الموافقة مرتبطة بغرض محدد ومعلن مسبقًا[٣٧٢].

ولا شك أن الإمكانات التقنية التي يمتلكها المتحكم في مواقع الإنترنت تتيح له الاحتفاظ بمعلومات مفصلة حول تفاعل المستخدم على الموقع الإلكتروني خلال إطار زمني محدد. وتشمل هذه المعلومات سجلات مشاهدات المستخدم، وتفاعلاته، ومعاملاته، مما يتيح للمتحكم توثيق موافقة صاحب البيانات على معالجة بياناته، مع تحديد وقت منح هذه الموافقة بدقة[٣٧٣].

**علاوة على ذلك**، يمكن للمتحكم توثيق عملية الموافقة أثناء تصفح المستخدم للموقع، بما يشمل حفظ نسخة من المعلومات التي تم تقديمها للمستخدم في ذلك الوقت[٣٧٤]. ويشمل ذلك التوضيحات والشروط المتعلقة بالموافقة، والتي يمكن

---

(372)- Lignes directrices 5/2020, op. cit., no 108, p. 26 .

(٣٧٣)– تستخدم المواقع الإلكترونية ما يسمى بجلسة الويب Web Session، وهي عبارة عن تقنية للترابط بين المستخدم وموقع الويب، ويمكن اعتبار هذه الجلسة بمثابة حاولة للإجراءات التي يتخذها المستخدم على موقع الويب وتفاعلاته خلال إطار زمني معين، وتتيح تعرف خادم الموقع على المستخدم عند زيارته مرة أخرى، على سبيل المثال، يمكن أن تحتوي جلسة واحدة على مشاهدات صفحات وأحداث وتفاعلات اجتماعية ومعاملات تجارة إلكترونية متعددة، ويمكن أن يفتح مستخدم واحد جلسات متعددة، ويمكن أن تحدث هذه الجلسات في اليوم نفسه، أو على مدار عدة أيام أو أسابيع أو أشهر، انظر: كيفية تعريف جلسة الويب، مركز دعم جوجل، متاح بتاريخ ٢٠٢١/٧/٨ على الموقع التالي:
https: //support. googlw. com/analytics/answer/2731565?h1=en#zippy=%2Cin-this-aricle

(374)- Lgines directrices 5/2020, op. cit., no 108,p. 26 .

للمتحكم الرجوع إليها عند الحاجة، سواء لإثبات صحة الموافقة أو للتأكد من استيفاء جميع المتطلبات القانونية اللازمة للحصول عليها.

ويقدم التوجيه الأوروبي رقم ٦٨٠ لسنة ٢٠١٦ مجموعة من الضوابط المتعلقة بكيفية إثبات المتحكم لقانونية أنشطة المعالجة التي يشرف عليها[٣٧٥]. فقد نصت الحيثية رقم ٥٦ من التوجيه على أنه، لضمان الالتزام بأحكامه، يتعين على المتحكم أو المعالج الاحتفاظ بسجلات لجميع فئات أنشطة المعالجة الواقعة تحت مسئوليتهما. كما أشار التوجيه إلى ضرورة أن يتعاون كل من المتحكم والمعالج مع السلطة الإشرافية، من خلال إتاحة السجلات عند الطلب، لتمكين السلطة من مراقبة الامتثال القانوني للأنشطة المعنية.

**بالإضافة إلى ذلك**، يُلزم التوجيه المتحكم أو المعالج الذي يقوم بمعالجة البيانات الشخصية باستخدام أنظمة غير إلكترونية بأن يُزوّد نفسه بوسائل فعالة تُسهم في إثبات قانونية المعالجة. وتشمل هذه الوسائل أدوات تساعد في ممارسة المراقبة الذاتية وضمان سلامة البيانات وأمنها، مثل الاحتفاظ بدفاتر أو سجلات ورقية أو أي أشكال توثيق أخرى تفي بالغرض. ومن ثم قيام المتحكم بإثبات الرضاء يتطلب منه بداهةً حفظ وأرشفة التعبير عن الرضاء الصادر من صاحب البيانات في ملفات إلكترونية خاصة تدون فيها كافة المعلومات اللازمة لمتابعة عملية المعالجة، بحيث تشمل أغراضها المحددة، وطبيعة البيانات، وفئات الأشخاص الطبيعيين أصحاب البيانات، والجداول الزمنية لحفظها ومحوها، وتدابير الحماية، سواء الفنية أو التنظيمية، المطبقة على أنشطة المعالجة[٣٧٦]، كما يجب على المتحكم أن يثبت أيضًا أن النظام

---

[٣٧٥]– التوجيه الأوروبي رقم ٢٠١٦/٦٨٠ الصادر عن البرلمان والمجلس الأوروبي بتاريخ ٢٧ أبريل ٢٠١٦ بشأن حماية الأفراد فيما يتعلق بمعالجة البيانات الشخصية من قبل السلطة المختصة لأغراض منع وكشف الجرائم الجنائية والتحقيقات والملاحقات القضائية بشأن تنفيذ العقوبات الجنائية، وحرية نقل هذه البيانات.
Journal officiel de l'Union européenne, 4 Mau 2016, L 119/89 .

[٣٧٦]– انظر: منى الأشقر جبور ومحمود جبور، مرجع سابق، ص ص ١٤٠، ١٤١.

(ISSN: 2537- 0758)

الذي وضعه للحصول على الرضاء يستوفي كافة متطلبات صحة الرضاء التي تفرضها اللائحة الأوروبية (GDPR)[٣٧٧].

وفي الواقع، يمكن إثبات الحصول على الموافقة في البيئة الإلكترونية، على وجه الخصوص، من خلال استخدام وسائل تعبير صريحة عن الموافقة، مثل إصدار إعلان أو تقديم تصريح مكتوب وموقع من صاحب البيانات. ولا شك أن هذه الآليات تفي بمتطلبات صحة الموافقة كما تحددها القوانين ذات الصلة، إذ توفر دليلاً واضحًا على الحصول على الموافقة، مما يعزز موثوقية عملية الإثبات. في المقابل، فإن التعبير الشفوي أو مجرد السكوت عن الرد قد يؤدي إلى وجود شكوك بشأن توفر دليل إثبات على الموافقة، ويصعب إثباته عمليًا. لهذا السبب، يميل المتحكمون في البيانات غالبًا إلى اعتماد الموافقة الكتابية كوسيلة إثبات أساسية، خاصةً في السياقات التي تتطلب توثيقًا قويًا ودقيقًا[٣٧٨].

هذا مع العلم أن قيمة الدليل على الموافقة قد تختلف بناءً على الآلية أو الإجراء الذي يتبعه المتحكم للحصول على هذه الموافقة. فعلى سبيل المثال، يُعد النقر على خانة أو مربع في الموقع الإلكتروني ذو حجية أضعف في الإثبات مقارنةً بالإجراءات التي تتطلب خطوات أكثر تعقيدًا، مثل التسجيل في الموقع وعبور إجراءات متعددة تكفل دلالة واضحة على الموافقة.

---

(377)- Y. POULLET, Consentement et RGPD: des zones d' ombre!, op. cit., p. 9 .

(٣٧٨)– يضرب فريق عمل المادة (٢٩) مثالاً على ذلك، بحالة الرضاء بتلقى الشخص معلومات حول الإجراءات الترويجية لأحد الفنادق عن طريق البريد، ويتحقق ذلك حينما يطلب الفندق من عملائه الإشارة إلى عنوانهم البريدي في نموذج مكتوب. متى كانوا يرغبون في إبلاغهم بإجراءاته الترويجية عن طريق البريد، فإذا قام العميل، بعد تدوين عنوانه البريدي. بالتوقيع على النموذج الكتابي للتعبير عن رضائه، فإن هذا يعد رضاء لا يمكن دحضه، وفي هذه الحالة سيكون الرضاء صريحًا وكتابيًا، ويوفر هذا الإجراء للمتحكم دليلاً كافيًا على حصوله على رضاء جميع العملاء، طالما كان يحتفظ بجميع النماذج الممهورة بتوقيعاتهم.

Groupe de travail "article 29", Avis 15/2011 sur la définition du consentement, op. ckt., pp. 28- 29 .

علاوة على ذلك، فإن قوة الدليل على الموافقة تعتمد أيضًا على طبيعة البيانات التي تم جمعها والغرض المحدد من المعالجة. فكلما كانت البيانات حساسة أو كان الغرض من المعالجة دقيقًا، زادت أهمية توفير دليل قوي وواضح على الموافقة.

وأخيرًا، يجب أن تكون الموافقة الصريحة التي يقدمها صاحب البيانات عبر الإنترنت قابلة للحفظ بشكل يتيح الوصول إليها واستخدامها كدليل عند الحاجة. ويتطلب ذلك من المتحكم استخدام أنظمة موثوقة لتوثيق وحفظ الموافقة بطريقة تضمن سلامتها وقابليتها للاستخدام لاحقًا، سواء لأغراض قانونية أو رقابية[٣٧٩].

## المطلب الثالث

## العدول عن الموافقة الرقمية

### أولاً- المدى الزمنى لصحة الموافقة الرقمية:

لا تحدد قوانين حماية البيانات الشخصية فترة محددة لسريان الموافقة الرقمية، وإنما اكتفت بوضع أطر لفترات الاحتفاظ بالبيانات بما يتوافق مع أغراض جمعها ومعالجتها[٣٨٠].

ولهذا السبب، سعت إرشادات مجلس حماية البيانات الأوروبي (EDPB) إلى وضع معايير لتحديد مدة صلاحية الموافقة، مشيرة إلى أن هذه المدة تعتمد على مضمون الموافقة الأصلية أو سياقها، ونطاقها، وتوقعات الشخص المعني. بناءً على ذلك، تظل الموافقة صالحة طوال فترة المعالجة، بشرط عدم الرجوع عنها، وهو أمر منطقي يتماشى مع وجود الموافقة ذاتها. كما يشترط احترام الأغراض التي وافق عليها صاحب البيانات. وفي حال تغيرت أغراض المعالجة أو تطورت بشكل جوهري، تصبح الموافقة معيبة، مما يستلزم الحصول على موافقة جديدة. ولهذا يوصي مجلس حماية البيانات الأوروبي بأن يقوم المتحكم بتجديد الموافقة على فترات

(379)- Groupe de travail "article 29", Avis 15/2011 sur la définition du consentement, op. cit., pp. 28- 29 .

(٣٨٠)– راجع: المادة (٥) بند ٥ من اللائحة الأوروبية لحماية البيانات GDR، والمادة (٣) بند ٣ من قانون حماية البيانات المصري، والمادة ١١٦ بند ٨ من قانون المعلوماتية والحريات الفرنسي المعدل.

(ISSN: 2537- 0758)

مناسبة، مع ضمان توفير جميع المعلومات المتعلقة بالموافقة مرة أخرى، لضمان بقاء صاحب البيانات على اطلاع كامل بكيفية استخدام بياناته وتمكينه من ممارسة حقوقه[٣٨١].

هذا ويلاحظ انه تظل الموافقة الصادرة من صاحب البيانات قبل صدور قوانين حماية البيانات الشخصية سارية المفعول، بشرط أن تتوافق مع أحكام القواعد القانونية المطبقة. وفي حال عدم توافقها، يتعين على المتحكم استكمال الموافقة الأصلية لتلبي الاشتراطات القانونية المطلوبة.

وتحقيقاً لذلك، تستمر الموافقة الصادرة قبل نفاذ اللائحة العامة لحماية البيانات الأوروبية (GDPR) في ٢٥ مايو ٢٠١٨ في السريان، بشرط أن تستوفي متطلبات اللائحة. وفي حال عدم تحقق هذا الاستيفاء، يقع على عاتق المتحكم اتخاذ الإجراءات اللازمة لتلبية هذه المتطلبات.

وينطبق ذات النهج سالف الذكر بشان الموافقة في إطار قانون حماية البيانات المصري، إذ تبقى الموافقة الصادرة قبل صدور القانون سارية المفعول، مع إلزام المتحكم بتوفيق أوضاعه وفقًا لأحكام القانون ولائحته التنفيذية. ويُمنح المتحكم مهلة مدتها سنة واحدة من تاريخ صدور اللائحة التنفيذية (المادة ٦ من القانون) لتلبية المتطلبات المتعلقة بالموافقة الواردة في القانون ولائحته. وتُعتبر هذه المدة كافية لتمكين المتحكم من تحقيق الامتثال الكامل للشروط القانونية المتعلقة بالموافقة.

## ثانياً- مضمون الحق في العدول عن الموافقة وأساسه القانوني:

باستثناء البيانات الشخصية التي تُعالج استنادًا إلى قواعد قانونية خاصة تفرض معالجتها، يحق للشخص المعني بالبيانات في أي وقت سحب موافقته، أو بعبارة أخرى العدول عن موافقته السابقة على معالجة بياناته الشخصية، دون أن يكون لهذا السحب أثر رجعي.

وينتج عن طلب الشخص بالعدول التزام يقع على عاتق المتحكم باتخاذ الإجراءات اللازمة فورًا لوقف أنشطة المعالجة الجارية على البيانات. كما يلتزم

(381)- Lignes directrices 5/2020 sure le consentement au sen du réglement (UE) 2016/679, op. cit., no 110 et 111, p. 27 .

بحذف البيانات الشخصية أو محوها من أنظمته الرقمية لضمان تنفيذ طلب السحب بشكل كامل.

ويُعد حق صاحب البيانات في العدول عن موافقته أحد الحقوق القانونية المقررة بموجب اللائحة العامة لحماية البيانات الأوروبية (GDPR) والقوانين الفرنسية والمصرية والاماراتية المتعلقة بحماية البيانات الشخصية. وقد اكتسب هذا الحق أهمية بارزة في اللائحة الأوروبية، حيث يُعرف بـ "الحق في سحب الموافقة[٣٨٢] "le droit de retirer du consentement". وتنص المادة (٣/٧) من اللائحة الأوروبية على أن: "يكون لصاحب البيانات الحق في سحب موافقته في أي وقت، دون أن يؤثر هذا السحب على مشروعية المعالجة التي تمت بناءً على الموافقة الصادرة قبل السحب. ويجب إعلام الشخص المعني بهذا الحق قبل التعبير عن موافقته، كما يجب أن يكون السحب بنفس سهولة التعبير عن الموافقة"[٣٨٣].

وتوضيحاً لأساس الحق في العدول عن الموافقة وأهدافه، تربط الحيثية رقم (٤٢) من اللائحة العامة لحماية البيانات الأوروبية(GDPR)، كما أشرنا سابقًا، تحقق شرط الموافقة الحرة– كأحد شروط صحة التعبير عن الموافقة– بقدرة صاحب البيانات على سحب موافقته دون أن يلحق به أي ضرر. كما أن المادة (٢) فقرة ثانية من قانون حماية البيانات الشخصية المصري تنص على أن للشخص المعني بالبيانات الحق في "العدول عن الموافقة المسبقة على الاحتفاظ ببياناته الشخصية أو معالجتها". وهذا يعني أن المشرّع منح الشخص الحق في العدول عن موافقته السابقة

---

[٣٨٢]– يمكن اعتبار أحكام اللائحة العامة لحماية البيانات وحيثياتها بشأن سحب الرضاء بمثابة تدوين للتفسير الحالي لهذا الموضوع في آراء مجموعة عمل "المادة ٢٩" بشأن تعريف الرضاء، انظر:

Lignes directrices 5/2020, op. cit., no 110, p. 27 .

[٣٨٣]– تحيل المادة (٥) بند ١ من قانون المعلوماتية والحريات المعدل المعنية بشروط مشروعية المعالجة إلى أحكام المادة (٤) بند ١١ والمادة (٧) من اللائحة الأوروبية فيما يتعلق بشرط الحصول على الرضاء.

(ISSN: 2537- 0758)

على معالجة بياناته الشخصية، أي سحبها في أي وقت، بالنظر إلى ارتباط هذا الحق بالحقوق اللصيقة بشخصية الفرد.

ويبدو أن الهدف من إقرار هذا الحق هو معالجة الحالات التي قد يتسرع فيها الشخص في منح موافقته للمتحكم على معالجة بياناته دون التروي الكافي. فإتاحة الحق في العدول تمكن الشخص من التراجع عن قراره بعد إعادة النظر فيه وتدبير أمره، مما يوفر له حماية إضافية تجاه أي استغلال محتمل من قبل المتحكم في البيانات[٣٨٤].

ومن ناحية اخرى تشترط المادة (١٧) بند (٥) من قانون حماية البيانات الشخصية المصري أنه لإجراء أي اتصال إلكتروني بغرض التسويق المباشر للشخص المعني بالبيانات، يجب توافر عدة شروط، من بينها توفير آليات واضحة وميسرة تتيح للشخص المعني بالبيانات الحق في رفض الاتصال الإلكتروني أو العدول عن موافقته المسبقة في هذا السياق.

ويجب أن يصدر طلب العدول عن الموافقة من الشخص المعني بالبيانات نفسه أو ممن له صفة قانونية في تقديم الطلب نيابة عنه. كما يجب توجيه الطلب إلى المتحكم، أو المعالج، أو الحائز على البيانات. ويلتزم الطرف المُوجه إليه الطلب بالرد عليه في غضون ستة أيام عمل من تاريخ استلامه، وذلك وفقًا للمادة (٢٢) من القانون[٣٨٥]. كما يكون للشخص المعني بالبيانات، وكذلك لكل ذي صفة أو مصلحة مباشرة، الحق في التقدم بشكوى في حال الامتناع عن تمكين الشخص المعني من ممارسة حقه في العدول عن الموافقة، مع عدم الإخلال بحقه في اللجوء إلى القضاء.

---

[٣٨٤]– قريب من ذلك: د. طارق جمعة السيد راشد: الحماية القانونية لخصوصية البيانات الشخصية في القانون القطري والمقارن، المجلة القانونية والقضائية، مركز الدراسات القانونية والقضائية، وزارة العدل، قطر، ص ١١، ع ٢، ٢٠١٧، ص٢٨.

[٣٨٥]– تنص المادة (٣٢) من قانون حماية البيانات المصري على أن: "يجوز للشخص المعني بالبيانات ولكل ذي صفة أن يتقدم إلى أي حائز أو متحكم أو معالج بطلب يتعلق بممارسة حقوقه المنصوص عليها في القانون، ويلتزم المقدم إليه الطلب بالرد عليه خلال ستة أيام عمل من تاريخ تقديمه إليه.

وتُقدم الشكوى إلى مركز حماية البيانات، الذي يتولى اتخاذ ما يلزم من إجراءات التحقيق بشأنها. ويتعين على المركز إصدار قراره بشأن فحص الشكوى خلال مدة لا تتجاوز ثلاثين يوم عمل من تاريخ تقديمها، مع إخطار كل من الشاكي والمشكو في حقه بقرار المركز. ويلتزم المشكو في حقه بتنفيذ قرار المركز خلال سبعة أيام عمل من تاريخ الإخطار، على أن يقوم بإفادة المركز بالإجراءات التي اتخذها لتنفيذ القرار. (المادة ٣٣ من القانون).

## ثالثاً- ضوابط ممارسة الحق في العدول عن الموافقة:

اكتفى المشرّع المصري و المشرع الاماراتى بإقرار الحق في العدول عن الموافقة دون أن يحدد ضوابطه أو باقي أحكامه. وفي المقابل، أولت اللائحة الأوروبية، في المادة (٣/٧)، عناية خاصة بتحديد هذه الضوابط، والتي يمكن أن يسترشد بها المشرّع المصري والمشرع الاماراتى. **وتتمثل هذه الضوابط فيما يلي:**

- **جواز العدول في أي وقت:** لصاحب البيانات الحق في العدول عن الموافقة في أي وقت، ويمارس هذا الحق شخصيًا متى بلغ السن القانونية للموافقة وتمتع بقواه العقلية، أو عن طريق ممثله القانوني إذا كان قاصرًا. ولا يُشترط لتفعيل هذا الحق التقيد بوقت معين أو تقديم أسباب أو مبررات. ويُوجه طلب العدول إلى المسؤول عن المعالجة، ويجب البت فيه على وجه السرعة. ومع ذلك، يُراعى أن هذا الحق، كغيره من الحقوق، لا يجوز إساءة استخدامه على نحو يسبب أضرارًا جسيمة للمتحكم.
- **العدول دون إلحاق ضرر بصاحب البيانات:** ينبغي أن يتمكن صاحب البيانات من ممارسة حقه في العدول دون أن يتعرض لأي ضرر، وفقًا للحيثية رقم (٤٢) من اللائحة الأوروبية. ويشمل ذلك أن يكون العدول مجانيًا دون تحميل صاحب البيانات أية تكاليف مالية إضافية أو تقليل جودة الخدمة المقدمة له[٣٨٦].
- **سهولة إجراء العدول:** يجب أن يكون طلب العدول سهلاً في تنفيذه ومماثلًا في ذلك لسهولة التعبير عن الموافقة في المقام الأول. تؤكد اللائحة الأوروبية ضرورة

(386)- Lignes directrices 5/2020 sur le consentement au sens réglement (UE) 2016/679, op. cit., no 46-48, pp. 14-15 .

(ISSN: 2537- 0758)

تيسير عملية سحب الموافقة بحيث تكون بنفس سهولة إصدارها. ويُعد هذا الأمر شرطًا جوهريًا لصحة الموافقة. وعليه، إذا لم تكن ضوابط الحق في العدول تلبي متطلبات اللائحة الأوروبية، فإن آلية الموافقة التي يضعها المتحكم تُعتبر غير متوافقة مع أحكام اللائحة[٣٨٧].

وعن تيسير عملية العدول عن الموافقة وآلية الإبلاغ، لا يُفهم من نصوص اللائحة الأوروبية أنها تشترط أن يتم التعبير عن الموافقة وسحبها بالطريقة أو الوسيلة ذاتها. بل ينصب اهتمام اللائحة على تيسير عملية سحب الموافقة. ومع ذلك، تُشير إرشادات مجلس حماية البيانات الأوروبي إلى ضرورة أن يتمكن أصحاب البيانات من سحب موافقتهم بالوسيلة نفسها التي تم من خلالها منح الموافقة، خصوصًا إذا تم الحصول على الموافقة إلكترونيًا، مثل النقر على خانة اختيار على الشاشة أو الكتابة عليها.

وعندما تُمنح الموافقة من خلال واجهة إلكترونية، سواء عبر موقع ويب، تطبيق، أو البريد الإلكتروني، فإن تمكين أصحاب البيانات من سحب موافقتهم باستخدام نفس الواجهة يُعد أمرًا منطقيًا. ذلك أن تغيير الواجهة لغرض وحيد هو سحب الموافقة قد يتطلب جهدًا إضافيًا غير مبرر ويُشكل عبئًا على صاحب البيانات[٣٨٨].

---

[٣٨٧]– فعلى سبيل المثال، قد يتم تذاكر حقل موسيقي من خلال منصة بيع التذاكر عبر الإنترنت، ومع كل تذكرة يتم بيعها، يطلب المتكم رضاء المشترى على استخدام تفاصيل الاتصال الخاصة به لأغراض تجارية، وللتعبير عن رضائهم بهذا الغرض، يمكن لعملاء اختيار إما الرفض (لا) أو القبول (نعم)، ويُخطر المتحكم العملاء بأنهم سيكونون قادرين على سحب رضائهم من خلال الاتصال بمركز الخدمة مجانًا في أيام العمل الرسمية بين الساعة ٨ صباحًا والساعة ٥ مساءًا، وفي هذا المثال، نجد أن المتحكم لا يلتزم بالمادة (٣/٧) من اللائحة الأوروبية، إذ يتطلب سحب الموافقة هنا إجراء مكالمة هاتفية خلال ساعات العمل المحددة فقط، وهو أكثر إرهاقًا من نقرة الماوس اللازمة لصدور الرضاء على منصة بيع التذاكر عبر الإنترنت، والتي يمكن الوصول إليها في أي وقت طوال اليوم، وبالتالى لا يكون سحب بالرضاء بذات سهولة التعبير عنه، في هذا الخصوص، انظر:

Lignes directrices 5/2020, op. cit., no 115, pp. 27-28 .

[388]- Lignes directrices 5/200, op. cit., no 114, p. 27 .

وعن التزام المتحكم بإبلاغ صاحب البيانات بحق العدول، فإنه يتعين على المتحكم إبلاغ صاحب البيانات بحقه في سحب الموافقة قبل طلب الحصول عليها. يتوافق هذا الالتزام مع مبدأ الشفافية الذي يُعد من المبادئ الأساسية التي تحكم اللائحة الأوروبية. وتدعم الحيثية (٣٩) من اللائحة هذا المبدأ، حيث تُلزم المتحكم بإبلاغ أصحاب البيانات بحقوقهم المرتبطة بالمعالجة، بما في ذلك طرق ممارستها. ومن بين هذه الحقوق، بطبيعة الحال، الحق في العدول عن الموافقة[٣٨٩].

## رابعاً- الآثار المترتبة على ممارسة الحق في العدول عن الموافقة:

ان ممارسة حق صاحب البيانات فى العدول عن الموافقة بمعالجة البيانات يرتب بلا شك الكثير من الاثار التى تكون بحاجة للمعالجة القانونية، حيث يرتيب حقوق والتزامات قد تؤثر فى ارادة الفرد **وهو ما سوف نناقشه فيما يلى:**

- **التزام المتحكم بوقف أنشطة المعالجة ومحو البيانات الشخصية:**

عند ممارسة صاحب البيانات حقه في العدول عن الموافقة، يُحظر على المتحكم أو المعالج الاحتفاظ بالبيانات الشخصية أو الاستمرار في معالجتها. يُصبح المتحكم ملتزمًا بوقف أنشطة المعالجة فورًا، ومحو البيانات الشخصية التي تمت معالجتها على أساس تلك الموافقة بمجرد العدول عنها. و هذا الالتزام مشروط بعدم وجود أساس قانوني آخر يبرر استمرار معالجة البيانات أو الاحتفاظ بها. فقد نصت اللائحة الأوروبية لحماية البيانات على حق صاحب البيانات في طلب محو البيانات المتعلقة به (Droit à l'effacement) أو "الحق في النسيان (Droit à l'oubli)"[٣٩٠] حال عدوله عن الموافقة، مع غياب أي أساس قانوني آخر يبرر المعالجة.

---

[٣٨٩]– تقرر الحيثية ٣٩ من اللائحة الأوروبية أن: ".... ينبغي إبلاغ الأشخاص الطبيعيين بالمخاطر والقواعد والضمانات والحقوق المرتبطة بمعالجة البيانات الشخصية وكيفية ممارسة حقوقهم فيما يتعلق بهذه المعالجة...".

[٣٩٠]– لمزيد من التفصيل في شأن الحق في النسيان، راجع: د. عبد الهادي فوزى العوضى، الحق في الدخول في طي النسيان على شبكة الإنترنت" دراسة قانونية تطبيقية مقارنة"، دار النهضة العربية، القاهرة، الطبعة الأولى، ٢٠١٤ وأيضًا:

(ISSN: 2537- 0758)

هذا مع وجوب المحو دون تأخير، حيث انه وفقًا للمادة (١/١٧) من اللائحة الأوروبية، يلتزم المتحكم بمحو البيانات دون أي تأخير لا مبرر له فور طلب العدول عن الموافقة(٣٩١).

---

Claire MARSOLLIER Le droit à l'oubli numérique approche comparative franco-canadienne, Université Laval, Québec-Canada. Et Université ParisScalay Cachan-France, 2020. Sur le site :
https: //corpus. ulaval. ca/jspui/bitstream/20. 500. 11794/67322/36714. pdf .

(٣٩١)- تنظم المادة (١٧) من اللائحة الحق في محو البيانات أو الحق في النسيان، حيث يجرى نصها على أن:

"١-يكون لصاحب البيانات الحق في أن يحصل من المتحكم على محو البيانات الشخصية المتعلقة به، في أقرب وقت ممكن، ويلتزم المتحكم بمسح هذه البيانات الشخصية في أقرب وقت ممكن، حال توافر أحد الأسباب التالية:

أ- لم تعد البيانات الشخصية ضرورية فيما يتعلق بالأغراض التي تم جمعها أو معالجتها من أجلها،

ب- قيام صاحب البيانات بسحب الرضاء الذي تستند إليه المعالجة وفقًا للفقرة الأولى من المادة (٦)، أو الفقرة الأولى من المادة (٩)، وحيث لا يوجد أساس قانوني آخر للمعالجة.

ج- اعتراض صاحب البيانات على المعالجة وفقًا للمادة (١/٢١) ولا توجد أسباب مشروعية تبرر المعالجة، أو اعتراضه على المعالجة وفقًا للمادة (١/٢١).

د- إذا جرى معالجة البيانات الشخصية بشكل غير قانوني.

هـ- وجوب محو البيانات الشخصية للوفاء بالتزام قانوني وارد في قانون الاتحاد الأوروبي أو قانون الدولة العضو التي يخضع لها المتحكم.

و-تم جمع البيانات الشخصيةي في سياق عرض خدمات مجتمع المعلومات المشار إليها في المادة (١/٨) من اللائحة.

٢- وفي حالة قيام المتحكم بإتاحة البيانات الشخصية للجمهور، وكان ملزمًا بمحو البيانات الشخصية، يجب عليه، مع مراعاة التكنولوجيا المتاحة وتكلفة التنفيذ، اتخاذ خطوات معقولة، بما في ذلك التدابير التقنية، لإبلاغ المتحكمين في معالجة البيانات الشخصية بأن صاحب البيانات قد طلب محو أي روابط لديهم أو نسخ لهذه البيانات الشخصية....".

وفي المقابل تنص المادة (٥١) فقرة أولى من قانون المعلوماتية والحريات الفرنسي على ممارسة الحق في المحور وفقًا للشروط المنصوص عليها في المادة (١٧) من اللائحة الأوروبية، كما تلقي الفقرة الثالثة التزامًا على المتحكم في البيانات بالاستجابة إلى طلب شهر

وعن نطاق تطبيق الحق في النسيان في البيئة الرقمية، فانه ينحصر نطاق تطبيق الحق في النسيان بشكل رئيسي في البيئة الرقمية، فيما يتعلق بالآثار أو الذكريات الرقمية، وهي كل المعلومات المرتبطة بنشاط الشخص أثناء استخدامه لنظام معلوماتي أو وسيلة إلكترونية من أي نوع، مثل مواقع التواصل الاجتماعي، محركات البحث، المدونات، أو مواقع التجارة الإلكترونية. وتُسهم هذه المعلومات في تحديد الهوية الرقمية للشخص[٣٩٢] وتشمل مشاركاته وآرائه على الإنترنت مهما كان نوعها.

وعن حدود ونطاق الحق في العدول والمحو، فإنه يقتصر الحق في العدول على البيانات التي جُمعت استنادًا إلى الموافقة فقط، ويترتب على ذلك أن البيانات المعالجة على هذا الأساس وحدها تكون محلاً للمحو في حالة عدول الشخص عن موافقته. أما إذا كانت المعالجة تستند إلى أكثر من أساس قانوني، مثل العقد أو الالتزام القانوني إلى جانب الموافقة، فإن المتحكم لا يكون ملزمًا بحذف البيانات.

وعن التزام المتحكم بالشفافية بشأن أغراض المعالجة، فإنه لتفادي أي التباس أو نزاعات مستقبلية، يجب على المتحكم أن يُوضح منذ البداية أغراض معالجة البيانات والأساس القانوني الذي يعتمد عليه كمرجع لهذه المعالجة[٣٩٣]. ويساعد هذا الإجراء في ضمان حقوق أصحاب البيانات ويوضح نطاق التزامات المتحكم في حالة العدول عن الموافقة.

وعن معالجة البيانات الشخصية بعد العدول عن الموافقة، فإنه يجب مراعاة الالتزام بالإخطار عند تغيير الأساس القانوني للمعالجة، حيث انه في حال عدول صاحب البيانات عن موافقته ورغبة المتحكم في مواصلة معالجة البيانات الشخصية

---

من تاريخ تقديم الطلب، فيجوز لصاحب البيانات أ نيتقدم بتظلم إلى اللجنة الوطنية للمعلومات والحريات، التي يتعين عليها البت في الطلب خلال ثلاثة أسابيع من تاريخ استلام المطالبة. راجع أيضًا المادة (١٨) من قانون المعلوماتية والحريات المعدل.

(٣٩٢)– راجع: د. عبد الهادي فوزي العوضي، مرجع سابق، ص ٨١ وما بعدها.

(٣٩٣)– في هذا الخصوص، راجع:

Lignes directrices 5/2020, op. it., no 117-118, p. 28 .

(ISSN: 2537- 0758)

على أساس قانوني آخر، لا يجوز للمتحكم تبديل أساس المعالجة دون إخطار صاحب البيانات بهذا التغيير. يتعين على المتحكم توضيح الأساس الجديد للمعالجة وأهدافها، بما يتماشى مع مبدأ الشفافية وحماية حقوق صاحب البيانات[٣٩٤].

كما يجب مراعاة التزام المتحكم بمحو بيانات القاصر، فبالنسبة للبيانات الشخصية الخاصة بالقاصرين، يكون المتحكم ملزمًا بحذفها أو وقف معالجتها بناءً على طلب الولي أو النائب القانوني للقاصر. يُعد هذا الالتزام جزءًا من الحماية الخاصة الممنوحة للقاصرين نظرًا لضعف موقفهم القانوني واحتياجهم لمزيد من العناية في سياق معالجة بياناتهم الشخصية.

هذا و يجب مراعاة ان الاصل هو عدم ترتيب أثر رجعي للعدول عن الموافقة، حيث حماية لمصالح المتحكم في البيانات، أكدت اللائحة الأوروبية بوضوح على حماية مصالح المتحكم الذي قام– حتى وقت العدول– بمعالجة البيانات التي تم جمعها بشكل قانوني. فقد نصت المادة (٣/٧) من اللائحة على أن العدول عن الموافقة لا يؤثر على صحة أو قانونية معالجة البيانات التي تمت بناءً على الموافقة السابقة.

وبذلك ينتفى الاثر الرجعى للعدول و يقوم فقط الأثر المستقبلي للعدول، و يترتب على هذا أن جميع عمليات المعالجة التي أجريت استنادًا إلى الموافقة السابقة تظل صحيحة ومنتجة لآثارها القانونية. بينما ينصرف أثر العدول إلى المستقبل فقط، [٣٩٥] مما يعني أن العدول لا يبطل أو يُلغي الأنشطة المعالجة التي تمت في ظل الموافقة السابقة.

ويمكن تبرير ما تقد بفكرة مراعاة الاستقرار القانوني، حيث يُفسر هذا التوجه على أن المعالجة التي تمت وقت إجرائها كانت مستوفية لشروط صحتها القانونية، بما في ذلك الحصول على موافقة صحيحة من صاحب البيانات. ويُعد هذا النهج ضروريًا لضمان استقرار المراكز القانونية التي نشأت بشكل صحيح بناءً على تلك المعالجة.

(394)- Lignes directrices 5/2020 sur le consentement ay sens du règlement (UE) 2016/679, op. cit., no 120, p. 29.
(395)- Lignes directrices 5/2020, op. cit., no 117, p. 28.

## الخاتمة

في ختام هذه الدراسة، يتضح أن الموافقة الرقمية على معالجة البيانات الشخصية أصبحت محور اهتمام المشرعين الأوروبي والفرنسي والمصري و الاماراتى. ويعود ذلك إلى إدراكهم لأهمية الموافقة كوسيلة لتحقيق رقابة الفرد على بياناته الشخصية التي تنتشر عبر المواقع والتطبيقات الإلكترونية في العالم الرقمي الحديث. وحمايتها وقد ركزت الدراسة على بيان خصوصية الاحكام المنظمة للموافقة الرقمية على معالجة البيانات الشخصية، باعتبارها مفهومًا حديث النشأة، ذات ماهية مختلفة عن ماهية الموافقة فى النظرية العقدية التقليدية من حيث التعريف والاساس القانونى، وشروطها، وكيفية التعبير عنها، والأهلية المطلوبة لإبداءها، وتحديد اثارها، وسبل إثباتها، وإمكانية العدول عنها. وفى نهاية استعرض تلك الدراسة والمسائل القانونية، ننتهى الى مجموعة من النتائج والتوصيات نعرضها كما يلى:

**من اهم نتائج البحث**:

أن البيانات الشخصية، أو ما يُعرف بالبيانات ذات الطابع الشخصي، تشمل أي معلومات ترتبط بشخص طبيعي محدد أو يمكن تحديده، سواء كان ذلك بصورة مباشرة أو غير مباشرة.

أن المشرع المصري والمشرع الإماراتي قصر نطاق حماية البيانات الشخصية على الأشخاص الطبيعيين دون أن تشمل الأشخاص الاعتباريين مالم تكن مرتبطة بشخص طبيعى لدى الاخير.

أن قانون حماية البيانات الشخصية في كل من النظامين المصري والإماراتي قد ركّز بشكل رئيسي على حماية ومعالجة البيانات الشخصية الرقمية، متجاهلًا البيانات الشخصية التقليدية.

أن البيانات الشخصية ليست فقط هدفًا للحماية القانونية، بل هي أيضًا محلًا رئيسيًا لتطبيقات الذكاء الاصطناعي–قيمية اقتصادية–، مما يُبرز أهمية تحقيق

(ISSN: 2537- 0758)

التوازن بين استثمار البيانات في تطوير هذه التطبيقات وضمان الالتزام بالضوابط القانونية والأخلاقية التي تكفل حقوق الأفراد في حماية خصوصيتهم.

ان التعريف المقترح للموافقة الرقمية بالمعالجة هو: كل تعبير عن الإرادة في صورة إلكترونية أو رقمية، يصدر عن صاحب البيانات أو نائبه القانوني، يكون حرًا، واضحًا، محددًا، مستنيرًا، وقاطعًا، ويدل على رضائه بصورة صريحة وإيجابية بقيام أو بإتمام عملية رقمية أو الكترونية تتناول بياناته الشخصية.

أن الطبيعة القانونية للموافقة الرقمية تخلص فى انها نوع خاص من الموافقة، تختلف عن الموافقة التعاقدية وكذلك عن التصرف بالإرادة المنفردة كمصدر للالتزام. وللموافقة الرقمية طابعًا غير ملزم. حيث تجيز احكام القوانين الخاصة إجراء المعالجة دون الحصول على الموافقة في الأحوال المصرح بها قانونًا. كما تجيز الرجوع فى الموافقة ان كانت الموافقة شرط للمعالجة.

ان الموافقة الصحيحة تتطلب أن يكون التعبير عن الإرادة الصادر عن صاحب البيانات، حرًا، ومستنيرًا، ومحددًا، وقاطعًا.

انه يلزم للموافقة على المعالجة ان يكون التعبير عنها صريح، و من ثم لا يجوز الاعتداد بالموافقة الضمنية لصاحب البيانات، كما انه لا يصلح السكوت ان يكون تعبيرا عن الارادة بالموافقة على معالجة البيانات.

ان معيار توافر الأهلية الرقمية للموافقة على المعالجة للبيانات الشخصية هو قدرة الشخص على فهم طبيعة ما يوافق عليه من معالجة للبيانات وتقدير آثارها. ويتحقق هذا المعيار عندما يكون الشخص كامل الأهلية الرقمية، أي قد بلغ سن الموافقة الرقمية المحدد قانوناً، "١٨ سنة فى مصر والامارات، و ١٦ سنة فى لائحة الاتحاد الاوربى وتجيز تنزله الى ١٣ سنة"، ويتمتع بقواه العقلية.

ان هناك فراغ تشريعى فى القوانين الخاصة بحماية البيانات موضوع الدراسة "مصر والامارات" لتنظيم الوسيلة المناسبة للحصول على هذه الموافقة، وما إذا كان

من الضروري أن تتم بطريقة إلكترونية أو رقمية حصراً، أو يمكن قبولها بوسائل أخرى.

أن موافقة صاحب البيانات لا تُعطى الأولوية المطلقة ضمن شروط معالجة البيانات. كما أنها لا تُعتبر بالضرورة الأساس المفضل بالنسبة للمسؤولين عن المعالجة، إذ يتم الاعتماد بشكل متزايد على أسس قانونية أخرى تتيح المرونة في التعامل مع البيانات الشخصية.

ان عبء إثبات صدور الموافقة من صاحب البيانات يقع على عاتق المتحكم أو المعالج بحسب الاحوال. ويبقى الالتزام بإثبات الموافقة قائمًا طالما استمر نشاط المعالجة المحدد. ومع ذلك لم ينظم القانون المصرى والاماراتى اثبات صدور الموافقة.

ان حق صاحب البيانات في العدول عن موافقته هو أحد الحقوق القانونية المقررة بموجب اللائحة العامة لحماية البيانات الأوروبية (GDPR) والقوانين الخاصة الفرنسية والمصرية والاماراتية المتعلقة بحماية البيانات الشخصية.

## ومن اهم التوصيات:

وجوب اعتبار الموافقة شرطًا أساسيًا لمشروعية معالجة البيانات الشخصية، و ذلك من خلال النص بوضوح على أن الموافقة هي الأساس القانوني الرئيسي لمعالجة البيانات الشخصية، مع تحديد الحالات القانونية التي يمكن فيها الاستثناء من شرط الحصول علي الموافقة.

ضرورة منع المعالجة دون موافقة مسبقة من صاحب البيانات، للحد من التلاعب بهذا الأساس القانوني.

ضرورة إدراج تعريف دقيق للموافقة الرقمية في القانون المصرى و الاماراتى، و بيان اساسها القانونى. ، وذلك من خلال تضمين تعريف للموافقة الرقمية في المادة الخاصة بالتعريفات في قانون حماية البيانات الشخصية على غرار اللائحة الأوروبية.

(ISSN: 2537- 0758)

وجوب النص على شروط ومعايير تفصيلية للتعبير عن الموافقة الرقمية، مثل أن تكون الارادة مستنيرة، صريحة، وقائمة على إرادة حقيقية، ومحددة وقاطعة وتحديد شكلها (كتابي، إلكتروني، إلخ).

وجوب تنظيم مسألة اثبات الموافقة الرقمية على المعالجة الرقمية بنصوص تفصيلية خاصة تتماشى والطبيعة القانونية للموافقة الرقمية.

ضرورة إنشاء مجلس على غرار مجلس حماية البيانات الأوروبي لتقديم الإرشادات اللازمة لتفسير أحكام القانون ولائحته التنفيذية فى مصر و الامارات مع التركيز على توضيح مفهوم ودور الموافقة الرقمية.

ضرورة وضع قواعد قانونية خاصة تنظم الاهلية الرقمية اللازمة لصحة الموافقة الرقمية على معالجة البيانات الشخصية بما يشملها من تنظيم للنيابة عن عديم الاهليه و القاصر و غيرهم فى اصدار الموافقة الرقمية.

وجوب فرض قواعد تفصيلية لتنظيم العدول عن الموافقة الرقمية بمعالجة البيانات من جميع جوانبها المختلفة.

ضرورة فرص قواعد تنظم و تضبط تعريف دقيق ومحدد لعبارة "الأحوال المصرح بها قانونًا" التي تتيح الخروج على شرط الموافقة للمعالجة، لتجنب إساءة استخدامها، مع الاسترشاد باللائحة الأوروبية في هذا السياق.

# قائمة المراجع

## أولاً- المراجع باللغة العربية:


- احمد ابو الحسن، "الطبيعة الخاصة لبعض الجهات كمتحكمين في البيانات الشخصية أثناء تحولهم الرقمي"، مجلة القانون والتقنيات الناشئة، المجلد ٣، العدد ٢، ٢٠٢٣، ص ٤٦٩-٥٢٤، متاح على الرابط: https: //doi. org/10. 54873/jolets. v3i2. 135.
- احمد الزرعوني. ، "خصوصية المعلومات الجينية والتحديات التي تواجه حمايتها"، مجلة جامعة الشارقة للعلوم القانونية، المجلد ٢١، العدد ٢، ٢٠٢٤، متاح على الرابط: https: //doi. org/10. 36394/jls. v21. i2. 13.
- أحمد سلامة، المدخل لدراسة القانون، الكتاب الثاني، مقدمة القانون المدني أو نظرية الحق الطبعة الخامسة، مكتبة عين شمس، القاهرة، بدون سنة نشر.
- أحمد مختار عمر وآخرون، "معجم اللغة العربية المعاصرة"، المجلد الثاني، عالم الكتب، الطبعة الأولى، ٢٠٠٨.
- بطيحي نسمة، الجرائم المتعلقة بانتهاك الأحكام الإجرائية المقررة لحماية الحق في الخصوصية الرقمية في التشريع الجزائري، بحث منشور بمؤتمر الخصوصية في مجتمع المعلوماتية، طرابلس- لبنان، ١٩-٢٠ يولي ٢٠١٩، مركز جيل البحث العلمي، سلسلة كتاب أعمال المؤتمرات، العام السابع، العدد ٢٦، يوليو ٢٠١٩.
- تامر محمد الدمياطى، الرضاء الرقمى بمعالجة البيانات الشخصية، دراسة مقارنة، مجلة القانون والتكنولوجيا، المجلد ٢، العدد ١، ابريل ٢٠٢٢.
- تقرير اللجنة المشتركة من لجنة الاتصالات وتكنولوجيا المعلومات ومكاتب لجان الشئون الدستورية والتشريعية والخطة والموازنة والدفاع والأمن القومي، حول مشروع قانون بشأن إصدار قانون حماية البيانات الشخصية، بتاريخ ٩ يوليو ٢٠١٩:
- جلال على العدوي، و. رمضان أبو السعود، و. محمد حسن قاسم، الحقوق والمراكز القانونية، منشأة المعارف، الإسكندرية، ١٩٩٦.
- جلال على العدوي، أصول الالتزامات، مصادر الالتزامات، مشأة المعارف، الإسكندرية، ١٩٩٧.
- جلال محمد إبراهيم، مصادر الالتزام، دار النهضة العربية، القاهرة، ٢٠١١، الطبعة الثالثة.

(ISSN: 2537- 0758)


- جميل الشرقاوي، النظرية العامة للالتزام، مصادر الالتزام، دار النهضة العربية، القاهرة، ١٩٩٥.
- حسام الدين كامل الأهواني: نحو نظام قانوني لجسم الإنسان، مجلة العلوم القانونية والاقتصادية، كلية الحقوق، عين شمس، المجلد ٤٠، العدد الأول، يناير ١٩٩٨.
- حسام الدين كامل الأهواني، الحق في احترام الحياة الخاصة "الحق في الخصوصية" دراسة مقارنة، دار النهضة العربية، القاهرة، بدون سنة نشر.
- حسام الدين كامل، الأهواني، المدخل للعلوم القانونية، الجزء الثاني نظرية الحق، بدون دار نشر، الطبعة الثالثة، ١٩٩٧.
- حسن كيره، الموجز في المدخل للقانون، مقدمة عامة "النظرة العامة للقاعدة القانونية– النظرية العامة للحق". الطبعة الثانية، منشأة المعارف، الإسكندرية، ١٩٦٣.
- حمدي عبد الرحمن، الوسيط في النظرية العامة للالتزامات، الكتاب الأول– المصادر الإرادية للالتزام، دار النهضة العربية، القاهرة، ١٩٩٩.
- خالد صلاح حنفي محمود، "حماية الطفل العربي على الإنترنت في ضوء الاتجاهات العالمية المعاصرة: دراسة تحليلية"، مجلة الطفولة والتربية، يصدرها المجلس العربي للطفولة والتنمية، القاهرة، العدد ٣٤، ٢٠١٩.
- دراسة نقدية لقانون حماية البيانات الشخصية رقم ١٥١ لسنة ٢٠٢٠، إعداد مركز بحوث القانون والتكنولوجيا بكلية القانون بالجامعة البريطانية، ٢٠٢٠.
- رائد محمد فليح النمر، حماية خصوصية مستخدمي مواقع التواصل الاجتماعي على ضوء التشريعات في مملكة البحرين، بحث منشور بمؤتمر الخصوصية في مجتمع المعلوماتية، طرابلس– لبنان، ١٩–٢٠ يوليو ٢٠١٩، مركز جيل البحث العلمي، سلسلة كتاب أعمال المؤتمرات، العام السابق، العدد ٢٦، يوليو ٢٠١٩.
- سارة الشريف، خصوصية البيانات الرقمية، سلسلة أوراق الحق في المعرفة تصدر عن مركز دعم لتقنية المعلومات، القاهرة، ١٣ مارس ٢٠١٤.
- سامح عبد الواحد التهامي، "ضوابط معالجة البيانات الشخصية: دراسة مقارنة بين القانون الفرنسي والقانون الكويتي"، مجلة القانون الكويتية العالمية، العدد ٩، السنة ٣، مارس ٢٠١٥.
- سامح عبد الواحد التهامي، الحماية القانونية للبيانات الشخصية: دراسة في القانون الفرنسي (القسم الأول)، مجلة الحقوق، جامعة الكويت، المجلد ٣٥، العدد ٣، سبتمبر ٢٠١١.

- سامح عرابي، "المسئولية الجنائية عن انتهاك الخصوصية المعلوماتية عبر مواقع التواصل الاجتماعي"، مجلة القانون والتقنيات الناشئة، المجلد ٢، العدد ٢، ٢٠٢٢، ص ٢١٣-٢٦٧، متاح على الرابط: https: //doi. org/10. 54873/jolets. v2i2. 115.
- سليمان غانم، في النظرية العامة للالتزام، مصادر الالتزام، الجزء الاول، العقد والإرادة المنفردة، مكتبة عبد الله وهبه، القاهرة.
- شريف فهمي بدوى، معجم مصطلحات الكمبيوتر والإنترنت والمعلوماتية، إنجليزي- فرنسي-عربي، دار الكتاب المصري- القاهرة، دار الكتاب اللبناني- بيروت، الطبعة الأولى، ٢٠٠٧.
- صادقي، م. ، "النيابة في التعاقد وآثارها على أطراف العقد"، مجلة *كوفة للفنون*، المجلد ١، العدد ٥٦، ٢٠٢٣، ص ٢٤٥-٢٦٣، متاح على الرابط: https: //doi. org/10. 36317/kaj/2023/v1. i56. 11619.
- طارق جمعة السيد راشد، "الحماية القانونية لخصوصية البيانات الشخصية في القانون القطري والمقارن"، المجلة القانونية والقضائية، مركز الدراسات القانونية والقضائية، وزارة العدل، قطر، العدد ٢، ٢٠١٧.
- طارق جمعة السيد راشد، الحماية القانونية للحق في خصوصية البيانات الجينية (دراسة تحليلية مقارنة)، المجلة القانونية، كلية الحقوق فرع الخرطوم، جامعة القاهرة، المجلد ٨، العدد ١٢، الخريف ٢٠٢٠.
- عادل عبد الصادق، البيانات الشخصية الصراع على نفط القرن الحادي والعشرين، المركز العربي لأبحاث الفضاء الإلكتروني، ٢٠١٨.
- عاقلي فضيلة، الحماية القانونية للحق في حرمة الحياة الخاصة، دراسة مقارنة، رسالة دكتوراه، كلية الحقوق جامعة الإخوة منتوري-قسنطينة، الجزائر، ٢٠١١-٢٠٢١.
- عبد الحي حجازى، المدخل لدراسة العلوم القانونية، الجزء الثاني الحق وفقًا للقانون الكويتي "دراسة مقارنة"، مطبوعات جامعة الكويت، ١٩٧٠.
- عبد الرحمن جمال، "الحق المشترك في البيانات في ظل تقنية الذكاء الاصطناعي: دراسة نقدية لتنظيم البيانات الشخصية"، مجلة القانون والتقنيات الناشئة، العدد الرابع، الجزء الثاني، ٢٠٢٤، متاح على الرابط: https: //doi. org/10. 54873/jolets. v4i2. 206.

(ISSN: 2537- 0758)


- عبد الرزاق السنهوري، الوسيط في شرح القانون المدني، الجزء الأول: نظرية الالتزام بوجه عام، مصادر الالتزام، تنقيح المستشار/ أحمد مدحت المراغي، طبعة نادي قضاة مجلس الدولة، ٢٠٠٨.
- عبد الفتاح عبد الباقي، موسوعة القانون المدني المصري، نظرية العقد والإرادة المنفردة، دراسة معمقة ومقارنة بالفقه الإسلامي، الكتاب الأول، دار نهضة مصر للطباعة والنشر، ١٩٨٤.
- عبد الكريم مأمون، حق الموافقة على الأعمال الطبية وجزاء الإخلال به، دار النهضة العربية، القاهرة، ٢٠٠٦.
- عبد الهادي فوزى العوضى، الحق في الدخول في طي النسيان على شبكة الإنترنت" دراسة قانونية تطبيقية مقارنة"، دار النهضة العربية، القاهرة، الطبعة الأولى، ٢٠١٤.
- عصام محمد رشيد منصور، "قوانين حماية خصوصية الأطفال على الإنترنت: قراءة في القانون الأمريكي COPPA مع استعراض للموقف العربي من مثل هذه القوانين"، مجلة دراسات المعلومات، جمعية المكتبات والمعلومات السعودية، العدد السادس، سبتمبر ٢٠٠٩.
- علاء الدين عبد الله فواز الخصاونة، "الحماية القانونية للخصوصية والبيانات الشخصية في نطاق المعلوماتية"، مجلة جامعة الشارقة للعلوم الشرعية والقانونية، جامعة الشارقة، المجلد ٨، العدد ٢، ٢٠١١.
- علاء عيد طه، "الحماية القانونية للأشخاص الطبيعيين فيما يتعلق بمعالجة البيانات الشخصية وتداولها: دراسة في ضوء اللائحة التنظيمية رقم ٢٠١٦/٦٧٩ الصادرة عن البرلمان والمجلس الأوروبي"، مجلة كلية الحقوق للبحوث القانونية والاقتصادية، العدد ٢، ٢٠١٩.
- على حسن نجيده، دور الإرادة والتعبير عنها في الفقهين: الإسلامي والوضعي، مجلة معهد الإدارة العامة، الرياض– السعودية، ص ٢٥، العدد ٤٩، ١٩٨٦.
- عمار ياسر محمد زهير البابلي، "توظيف تقنيات الذكاء الاصطناعي في العمل الأمني: دراسة تطبيقية"، مجلة الأمن والقانون، المجلد ٢٨، العدد ١، ٢٠٢٠.
- عمرو طه بدوي، "التنظيم القانوني لمعالجة البيانات الشخصية: دراسة تطبيقية على معالجة تسجيلات المراقبة البصرية"، أكاديمية أبوظبي القضائية، ٢٠١٩.

- فارس محمد القادري، "العمل الطبي ومشروعيته والخطأ الناتج عنه"، مجلة جامعة صنعاء للعلوم الإنسانية، العدد ١، الجزء ١، ٢٠٢٤، متاح على الرابط: https: //doi. org/10. 59628/jhs. v1i1. 601.
- لقاط لبيب. ، هاشمي حسن، "حماية المعطيات ذات الطابع الشخصي للطفل: قراءة على ضوء أحكام القانون رقم ١٨-٧"، مجلة العلوم القانونية والسياسية، جامعة الشهيد حمة لخضر- الوادي، الجزائر، المجلد ١١، العدد ١، إبريل ٢٠٢٠.
- محمد أحمد المعداوي، "حماية الخصوصية المعلوماتية للمستخدم عبر شبكات مواقع التواصل الاجتماعي: دراسة مقارنة"، مجلة كلية الشريعة والقانون، جامعة طنطا، المجلد ٣٣، العدد ٤، ديسمبر ٢٠١٨.
- محمد حسام محمود لطفي، النظرية العامة للالتزام، مصادر الالتزام، النسر الذهبي للطباعة، القاهرة، الطبعة الثانية، ٢٠٠٢.
- محمد حسن قاسم، القانون المدنى، الالتزامات، المصادر، ١- العقد، المجلد الاول- دراسة فقهية قضائية مقارنة في ضوء التوجهات التشريعية والقضائية الحديثة وقانون العقود الفرنسي الجديدة ٢٠١٦، دار الجامعة الجديدة، ٢٠١٧.
- محمد حسين منصور، نظرية الحق، دار الجامعة الجديدة، الإسكندرية، ٢٠٠٤.
- محمد حماد مرهج الهيتي، "البحث عن حماية جنائية للبيانات والمعلومات الشخصية (الأسمية المخزنة في الحاسب الآلي)"، مجلة كلية الشريعة والقانون الإمارات، العدد ٢٧، يوليو ٢٠١٦.
- محمد سامي عبد الصادق، شبكات التواصل الاجتماعي ومخاطر انتهاك الحق في الخصوصية، دار النهضة العربية، القاهرة، ٢٠١٦.
- محمد عرفات الخطيب، ضمانات الحق في العصر الرقمي: "من تبدل المفهوم. . لتبدل الحماية" قراءة في الموقف التشريعي الأوروبي والفرنسي وإسقاط على الموقف التشريعي الكويت، مجلة كلية القانون الكويتية العالمية، المجلد ٦، ملحق خاص بأبحاث المؤتمر السنوي الدولي الخامس ٩-١٠ مايو ٢٠١٨، العدد ٣، الجزء الاول، مايو ٢٠١٨.
- محمد عزمى البكري، موسوعة الأحوال الشخصية، المجلد الأول، دار محمود للنشر، القاهرة، ٢٠١٧.
- محمد عيد الغريب، "التجارب الطبية والعلمية وحرمة الكيان الجسدي للإنسان: دراسة مقارنة"، مطبعة أبناء وهبة حسان، القاهرة، الطبعة الأولى، ١٩٨٩.

(ISSN: 2537- 0758)


- محمد غالي العنزي، الولاية على نفس الطفل بين الشريعة الإسلامية ومنظومة القوانين الكويتية، مجلة الشريعة والدراسات الإسلامية، مجلس النشر العلمي– جامعة الكويت، المجلد ٣٥، العدد ١٢٢، سبتمبر ٢٠٢٠
- محمد محمد أبو زيد، نظرية الحق "مقدمة القانون المدنى". بدون سنة نشر، الدار المحمدية للطباعة، القليوبية.
- محمود جمال الدين زكي، الوجيز في نظرية الالتزام في القانون المدني المصري، الجزء الأول، في مصادر الالتزام، مطبعة لجنة التأليف والترجمة والنشر، ١٩٦٨.
- محمود سلامة عبد المنعم الشريف، "الطبيعة القانونية للتنبؤ بالجريمة بواسطة الذكاء الاصطناعي ومشروعيته"، المجلة العربية لعلوم الأدلة الجنائية والطب الشرعي، المجلد ٣، ٢٠٢١.
- محمود عبد الرحمن، التطورات الحديثة لمفهوم الحق في الخصوصية (الحق في الخصوصية المعلوماتية)، مجلة كلية القانون الكويتية العالمية، العدد التاسع، السنة الثالثة، مارس ٢٠١٥.
- محمود عبد العظيم، بيزنس البيانات الشخصية يغزو السوق المصرية، جريدة الإتحاد الإمارتية، بتاريخ ٨ يناير ٢٠٠٦، متاح على: http: //www. alittihad. ae/details. php?id=44592&y=2006
- محمود فياض، "قواعد مساعدات الدولة للاتحاد الأوروبي لقطاع النقل الجوي في ضوء المادة ١٠٧ من معاهدة الاتحاد الأوروبي"، مجلة JOL، المجلد ٤٨، العدد ١، ٢٠٢٤، ص ٣٥٩–٤٠٤، متاح على الرابط: https: //doi. org/10. 34120/jol. v48i1. 183.
- مريم الدهماني، ايمن زين. (٢٠٢٤). آثار العقد الفاسد وَفْقًا لقانون المعاملات المدنية الإماراتي "دراسة على ضوءٍ من أحكام الفقه الإسلامي". مجلة جامعة الشارقة للعلوم القانونية،٢١(١). https: //doi. org/10. 36394/jls. v21. i1. 4
- مطلق العميري، "استراتيجيات الإعلام الإلكتروني في الكويت تجاه الأمن السيبراني"، المجلة العربية للعلوم الإنسانية، المجلد ٤٢، العدد ١٦٥، ٢٠٢٤، ص ١١–٤٢، متاح على الرابط: https: //doi. org/10. 34120/ajh. v42i165. 359.
- المعجم الوجيز"، مجمع اللغة العربية، طبعة خاصة بوزارة التربية والتعليم.

- منصور مصطفى منصور، ج. جلال محمد إبراهيم: الوجيز في مصادر الالتزام، بدون بدون ناشر ٢٠٠٠/ ٢٠٠١.
- منى أبو بكر الصديق محمد حسان، الحق في الرجوع في العقد كإحدى الآليات القانونية لحماية المستهلك في مجال التعاقد عن بعد، دراسة تحليلية في ضوء القانون الفرنسي والتوجيهات الأوروبية، مجلة البحوث القانونية والاقتصادية، كلية الحقوق، جامعة المنصورة، العدد ٦٥، أبريل ٢٠١٨.
- منى الأشقر جبور ومحمود جبور، "البيانات الشخصية والقوانين العربية: الهمّ الأمني وحقوق الأفراد"، المركز العربي للبحوث القانونية والقضائية، مجلس وزراء العدل، جامعة الدول العربية، الطبعة الأولى، بيروت– لبنان، ٢٠١٨.
- هوزان عبد المحسن عبدالله، "عقود الإطار: دراسة مقارنة في ضوء مرسوم قانون رقم (١٣١-٢٠١٦) للقانون المدني الفرنسي"، مجلة JOL، المجلد ٤٦، العدد ٥، ٢٠٢٢، متاح على الرابط: https: //doi. org/10. 34120/jol. v46i5. 2881.
- هوزان عبد المحسن عبدالله، "مضمون العقد في ضوء التعديلات الحديثة للقانون المدني الفرنسي (دراسة مقارنة بالفقه المالكي)"، مجلة جامعة الشارقة للعلوم القانونية، المجلد ١٧، العدد ٢، ٢٠٢١، ص ٦١٥-٦٤١، متاح على الرابط: https: //doi. org/10. 36394/jls. v17. i2. 21.
- وهبة الزحيلي، الفقه الإسلامي وأدلته، الجزء السابع، الأحوال الشخصية، دار الفكر للطباعة والنشر والتوزيع بدمشق، سوريا. ط٢، ١٩٨٥.


## ثانياً- المراجع الاجنبية:


- abrogeant la directive 95/46/CE (règlement general sur la protection des données). Journal official de l'Union européenne, L 119/1, 4 mai 2016.
- Agathe LEPAGE, Droit de la personnalitém Répertoire de droit civil Dalloz, 2009.
- Alain BENSOUSSAN, Informatique et libertés, Editions Francis Lefebvre, Paris, 2e édition, 2010.
- Allah Rakha, N. (2024). Constitutional safeguards for digital rights and privacy. Irshad J. Law and Policy, 2(4), 31-43. https: //doi. org/10. 59022/ijlp. 172.

(ISSN: 2537- 0758)


- AllahRakha, N. (2024). "Constitutional safeguards for digital rights and privacy. " Irshad J. Law and Policy, 2(4), 31-43. https: //doi. org/10. 59022/ijlp. 172.
- Andropova, T. (2018). "Testamentary: untypical forms of the will and the use of new technologies. " Ex Jure, (1), 30-44. https: //doi. org/10. 17072/2619-0648-2018-1-30-44.
- ang, W., and Newman, A. (2021). "Enforcing European privacy regulations from below: Transnational fire alarms and the General Data Protection Regulation. " JCMS Journal of Common Market Studies, 60(2), 283-300. https: //doi. org/10. 1111/jcms. 13215.
- Anne DEBET, Jean MASSOT et Nathalie METALLINOS, Informatique et libertés: La protectiob des données à caractère en droit français et européen, Lextenso, 2015.
- Anne DEBET, LE consentement dans le Règlement Général sur la Protection des données, Rôle et definition, Revue Communication commerce électronique. 2018, Eude n$^{o}$ 9.
- Astrid MARAIS, Droits des personnes, 3e éd., Dalloz, 2018.
- Avram, R., So, D., Iturriaga, E., Byrne, J., Lennon, R., Murthy, V., … & Pereira, N. (2022). Patient onboarding and engagement to build a digital study after enrollment in a clinical trial (tailor-pci digital study): intervention study. Jmir Formative Research, 6(6), e34080. https: //doi. org/10. 2196/34080.
- Baldemir, R. (2023). "An overview of the concept of medical intervention and informed consent according to Turkish law. " Journal of Pulmonology and Intensive Care, 1(2), 42-45. https: //doi. org/10. 51271/jopic-0010.
- Bathalie MARTAL-BRAZ, Le renforecement des droit de la personne concernée, Dalloz IP/T 2017.
- Benjamin BÉNÉZETH et all, Protection des données personnelles, Éditions Francis Lefebvre, Paris, 2018.
- Benjamin CHARRIER, LE consentement exprimé pa les mineurs en ligne, Dalloz IP/IT, 6 juin 2018.

- Bhattacharya, S., Singh, A., & Hossain, M. (2019). "Strengthening public health surveillance through blockchain technology. " Aims Public Health, 6(3), 326-333. https: //doi. org/10. 3934/publichealth. 2019. 3. 326.
- Breen, S., Ouazzane, K., & Patel, P. (2020). Gdpr: is your consent valid?. Business Information Review, 37(1), 19-24. https: //doi. org/10. 1177/0266382120903254.
- Breuer, J., Zeeland, I., & Pierson, J. (2023). Walkshops– testing a low threshold methodology for participatory city making. Aoir Selected Papers of Internet Research. https: //doi. org/10. 5210/spir. v2022i0. 12978
- Cécile DE TERWANGNE et Karen ROSIER, Le Règlement général de protection des données (RGPD/ GDPR), coll. Du CRIDS, Larcier, 1re édition, 2018.
- Célia SCAULTZ, La protection du mineur à l'aune des réseaux sociaux, Mémoire, Université de Grenoble Aples, 2020. Disponible sur le site: https: //dumas. ccsd. cnrs. fr/dumas-02960116/ document.
- Céline CASTETS-RENARD, Brève analyse du règlement general de la protection des données, Dalloz IP/IT, Juillet-Août 2016.
- Chauke, T. (2024). Skills learnt in youth work practice necessary for the digital age: a qualitative study of neet youth. Research in Social Sciences and Technology, 9(1), 351-368. https: //doi. org/10. 46303/ressat. 2024. 20.
- Claire MARSOLLIER Le droit à l'oubli numérique approche comparative franco-canadienne, Université Laval, Québec-Canada. Et Université ParisScalay Cachan-France, 2020. Sur le site: https: //corpus. ulaval. ca/jspui/bitstream/20. 500. 11794/67322/36714. pdf.
- Claire QUENNESON, Mineur et secret, Université de Bordeaux, 2017.

(ISSN: 2537- 0758)


- Clifford, D., Graef, I., & Valcke, P. (2018). Pre-formulated declarations of data subject consent citizen-consumer empowerment and the alignment of data, consumer and competition law protections. SSRN Electronic Journal. https: //doi. org/10. 2139/ssrn. 3126706.
- Cour de justice de l'Union européenne (2ème chamber), Arrêt du 11 novembre 2020, Affaire C-61/19, Journal official de l'Union européenne, 18 janvier 2021/ C 19/4.
- Cour de justice fr l'Union europénne (grande chamber), Arrêt du ler octobre 2019, Planet49 GmbH, Afaire C-673/17, Journal official de l'Union européenne, 9 décembre 2019/C 413/04.
- Cythia CHASSIGNEUX, L'encadrement juridique du traitment des données personnelles sur les sites de commerce en ligne, Thèse de doctorat, Université de Montréal, Paris, 2003.
- Dempsey, J., Sim, G., & Cassidy, B. (2018). Designing for gdpr-investigating children's understanding of privacy: a survey approach. . https: //doi. org/10. 14236/ewic/hci2018. 26.
- Directive 95/46/CE du parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitment des données à caractère personnel et à la libre circulation de ces données, JOCE, no. L. 281/31, 23 nov. 1995.
- Directive 95/46/CE du parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitment des données à caractère personnel et à la libre circulation de ces données, JOCE, no. L. 281/31, 23 nov. 1995.
- Doan, X., Florea, M., & Carter, S. (2023). Legal-ethical challenges and technological solutions to e-health data consent in the eu. . https: //doi. org/10. 3233/faia230088.
- Drozd, O. (2023). A conceptual consent request framework for mobile devices. Information, 14(9), 515. https: //doi. org/10. 3390/info14090515.

- Ellis, L. (2023). Digital consent in gynecology: an evaluation of patient experience. Archives of Gynecology and Obstetrics, 309(2), 611-619. https: //doi. org/10. 1007/s00404-023-07304-1.
- Emmanuel NETTER, L'extinction du contrat et le sort des données personnelles, AJ Contrat (Actualité Juridique Contrat), Dalloz, no 10-Octobre 2019.
- Fanny ROGUE, Capacité et consentement au traitement de données à caractère personnel et au contrat, AJ Contrat (Actualité Juridique Contrat), Dalloz, Août-Septembre 2019.
- Fitriana, D. (2023). "The role of informed consent as legal protection for doctors in conducting medical procedures. " Law, 1(3), 235-245. https: //doi. org/10. 61194/law. v1i3. 101.
- Florence GAULLIER, Le principe de finalité dans le RGPD: beaucoup d'ancien et un peu de nouveau, communication commerce électronique, no 4, 2018.
- Fox, G., Lynn, T., & Rosati, P. (2022). Enhancing consumer perceptions of privacy and trust: a gdpr label perspective. Information Technology and People, 35(8), 181-204. https: //doi. org/10. 1108/itp-09-2021-0706.
- François TERRÉ, Philippe SIMLER, Yves LEQUETTE, et François CHÉNEDÉ, Droit civil, Les obligations, 12e éd., Dalloz, 2018.
- Françoise BETAILLOLE-GONTHIER, La capacité naturelle, Thèse Bordeaux 4, 1999.
- Friemel, T. (2014). The digital divide has grown old: determinants of a digital divide among seniors. New Media & Society, 18(2), 313-331. https: //doi. org/10. 1177/1461444814538648.
- Fukui, N. (2024). Mixed methods approach to examining the implementation experience of a phone-based survey for a sars-cov-2 test-negative case-control study in california. Plos One, 19(5), e0301070. https: //doi. org/10. 1371/journal. pone. 0301070.

(ISSN: 2537- 0758)


- Georgopoulou, A. (2024). Social media platforms and general data protection regulation violation for minor users. BMMCONF, 1(1), 1-12. https: //doi. org/10. 33422/bmmconf. v1i1. 258.
- -Géraldine CRIQUI-B-BARTHALAIS, La protection des libtertés individuelles sur le réseau Internet, Thèse Paris II- Panthéon-Assas, 2018.
- Gérard CORNU, L'âge civil, in, Mélanges en l'honneur de Paul ROUBIER, T. II. Librairie Dalloz et Sirey, 1961.
- Harjono, D. (2022). Legal development of the validity of electronic mortgage certificates in the land registration system in indonesia. Yustisia Jurnal Hukum, 11(2), 110. https: //doi. org/10. 20961/yustisia. v11i2. 61111
- Iswari, D. (2023). Examining the legal standing of digital signatures under civil and ite laws. Policy Law Notary and Regulatory Issues (Polri), 2(2), 142-154. https: //doi. org/10. 55047/polri. v2i2. 603.
- Jean CARBONNIER, Droit civil, Les obligation, Tom 4, Théme droit privé, 2e edition, PUF, Paris, 2000.
- Jean-Michel BRUGUIERE, Bérengère GLEIZE, Droits de la personnalité, Ellipses édition, 2015.
- Joan E. Rigdon, Internet Users Say They'd Rather Not Share Their Cookies, Wall Street Journal, 14. Feb,1996.
- Kassam, I., Ilkina, D., Kemp, J., Roble, H., Carter-Langford, A., & Shen, N. (2023). Patient perspectives and preferences for consent in the digital health context: state-of-the-art literature review. Journal of Medical Internet Research, 25, e42507. https: //doi. org/10. 2196/42507.


- Kassam, I., Ilkina, D., Kemp, J., Roble, H., Carter-Langford, A., & Shen, N. (2023). Patient perspectives and preferences for consent in the digital health context: state-of-the-art literature review. Journal of Medical Internet Research, 25, e42507. https: //doi. org/10. 2196/42507.

- Keyes, M. (2019). Optional choice of court agreements in private international law: general report., 3-48. https: //doi. org/10. 1007/978-3-030-23914-5_1.
- Kurteva, A., Chhetri, T., Pandit, H., & Fensel, A. (2024). Consent through the lens of semantics: state of the art survey and best practices. Semantic Web, 15(3), 647-673. https: //doi. org/10. 3233/sw-210438.
- Kurteva, A., Chhetri, T., Pandit, H., & Fensel, A. (2024). Consent through the lens of semantics: state of the art survey and best practices. Semantic Web, 15(3), 647-673. https: //doi. org/10. 3233/sw-210438.
- Kwasny, M., Caine, K., Rogers, W., and Fisk, A. (2008). "Privacy and technology. " Available at: https: //doi. org/10. 1145/1358628. 1358846.
- Kyi, L. (2024). “it doesn’t tell me anything about how my data is used”: user perceptions of data collection purposes., 1-12. https: //doi. org/10. 1145/3613904. 3642260.
- Laure MARINO, Les nouveaux territoires des droits de la personnalité, Gazette du Palais, no. 139, 18-19 mai 2007.
- Laurélenn BEGNY, Règlement général sur la protection des données personnelles: vers une remise en cause du modèle français? Mémoire pour le Master, Université de Poitiers, 2017.
- Le, Q. (2023). "The social contract model in the digital era: revisiting Rousseau and Locke. " ISSLP, 2(3), 15-26. https: //doi. org/10. 61838/kman. isslp. 2. 3. 3.
- Loi n$^{o}$ 2018- 493 du 20 Juin 2018 relative à la protection des données personelle.
- Loi n$^{o}$ 78-17 du 6 janvier 1978 relative à l'informtaique, aux fichiers et aux libertés, JORF du 7 janvier 1978.
- Lutomski, J., Rainey, L., Jong, M., Manders, P., & Broeders, M. (2023). "Expanding the boundaries of previously obtained informed consent in research: Views from participants in the

(ISSN: 2537- 0758)

personalised risk-based mammoscreening study. " Health Expectations, 26(3), 1308-1317. https: //doi. org/10. 1111/hex. 13746.

- Macnamara, J., Zerfaß, A., Adi, A., & Lwin, M. (2018). "Capabilities of PR professionals for key activities lag: Asia-Pacific study shows theory and practice gaps. " Public Relations Review, 44(5), 704-716. https: //doi. org/10. 1016/j. pubrev. 2018. 10. 010.
- Marie LIFRANGE, Protection des données à caractère personnel: le concentement à l'épreuve de l'ère numérique, Master en droit, Faculté de Droit, LiÈGE Université, 2017- 2018.
- Michels, J., and Millard, C. (2022). "The new things: property rights in digital files?" The Cambridge Law Journal, 81(2), 323-355. https: //doi. org/10. 1017/s0008197322000228.
- Murielle BENEJAT, Les droits sur les données personnelles, in Jean-Christophe SAINT-PAU et all, Droit de la personnalité, Lexis-Nexis, 2013.
- Nayeri, N. and Aghajani, M. (2010). "Patients' privacy and satisfaction in the emergency department: a descriptive analytical study," Nursing Ethics, Vol. 17, No. 2, pp. 167-177. Available at: https: //doi. org/10. 1177/0969733009355377.
- Noémie WEINBAUM, La prevue du consentement à l'ère du RGPD et de la blockchain, La semaine juridique, Entreprises et affaires, no 10. 2018.
- Novitsky, A., Bondarev, A., Dobritsky, A., Tyurin, I., & Komarov, Y. (2022). "Legal support for the digital economy in the Russian Federation: legal policy priorities. " Revista De Investigaciones Universidad Del Quindío, 34(S3), 244-255. https: //doi. org/10. 33975/riuq. vol34ns3. 1074.
- Olphert, W. and Damodaran, L. (2013). Older people and digital disengagement: a fourth digital divide?. Gerontology, 59(6), 564-570. https: //doi. org/10. 1159/000353630.

- Ordonnance n° 2018- 1125 du 12 décembre 2018 prise en application de l'article 32 de la loi no 2018- 493 du 20 juin 2018 relative à la protection des données personnelles et portant modification de la loi no 78- 17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et diverses disposition concernant la poritection des données à caractère personnel, JORF no 0288 du 13 décembre 2018, Text 5.
- Palviainen, Å. and Räisä, T. (2021). The winding road to accessing the voices of one thousand schoolchildren: a nexus analysis of collecting data for a survey. Scandinavian Journal of Educational Research, 66(5), 793-807. https: //doi. org/10. 1080/00313831. 2021. 1939137.
- Partick WERY, Droit des obligations, Volume II, Les sources des obligations extracontractuelles, Le régime general des obligations Collection des Précis de la Faculté de droit de l'U. C. L., Bruxelles, Larcier.
- Paterick, T., Carson, G., Allen, M., & Paterick, T. (2008). "Medical informed consent: general considerations for physicians. " Mayo Clinic Proceedings, 83(3), 313-319. https: //doi. org/10. 4065/83. 3. 313.
- Pawluczuk, A. (2020). Digital youth inclusion and the big data divide: examining the scottish perspective. Internet Policy Review, 9(2). https: //doi. org/10. 14763/2020. 2. 1480.
- Payne, D., and Kennett-Hensel, P. (2017). "Combatting identity theft: a proposed ethical policy statement and best practices. " Business and Society Review, 122(3), 393-420. https: //doi. org/10. 1111/basr. 12121.
- Philippe BONFILS et Adeline GOUTTENOIRE, Droit des mineurs, Précis Dalloz, 2008
- Philippe MOURON, Pour ou contre la ptrimonialité des données personnelles, Revueve Européenne des Médias et du Numérique,

(ISSN: 2537- 0758)

no 46-47, Printemps-Été 2018, pp. 90-96. Disponible sur le site: - https: //hal/amu. archives-ouvertes. Fr/hal-0182390/document.

- Pierre KAYSER, Les droits de la personnalité: aspects théoriques et pratiques, RTD. Civ., 1971.
- Pierre STORRER, Pour un droit commercial de l'exploitation des données à caractère personnel, Recueil Dalloz, no 27, 25 Juillet 2013.
- portant modification de la loi n$^{o}$ 78-17 6 janvier 1978 relative à l'informatique, aux fichers et aux libertés et diverses dispositions concernant la protection des données à carcatère personnel, JORF n$^{o}$ 0 141 du 21 juin 2018.
- Rad, D., Dughi, T., Roman, A., & Ignat, S. (2019). Perspectives of consent silence in cyberbullying. Postmodern Openings, 10(2), 57-73. https: //doi. org/10. 18662/po/71
- Règlement (UE) 2016/679 du Parment européen du Conseil du 27 avril 2016, relative à la protection des personnes physiques à l'égard du traitment des données à caractère personnel et à la libre circulation de ces données,
- Ribeiro, A., Dias, V., Ribeiro, S., Silva, J., & Barros, H. (2022). "Geoprivacy in neighbourhoods and health research: A mini-review of the challenges and best practices in epidemiological studies. " Public Health Reviews, 43. https: //doi. org/10. 3389/phrs. 2022. 1605105.
- Roman-Martinez, I., Calvillo-Arbizu, J., Mayor-Gallego, V., Madinabeitia-Luque, G., Estepa, A., & Estepa, R. (2023). Blockchain-based service-oriented architecture for consent management, access control, and auditing. Ieee Access, 11, 12727-12741. https: //doi. org/10. 1109/access. 2023. 3242605.
- Roman-Martinez, I., Calvillo-Arbizu, J., Mayor-Gallego, V., Madinabeitia-Luque, G., Estepa, A., & Estepa, R. (2023). Blockchain-based service-oriented architecture for consent

management, access control, and auditing. Ieee Access, 11, 12727-12741. https: //doi. org/10. 1109/access. 2023. 3242605.

- Sarva, E., Slišāne, A., Oļesika, A., Daniela, L., & Rubene, Z. (2023). Development of education field student digital competences—student and stakeholders' perspective. Sustainability, 15(13), 9895. https: //doi. org/10. 3390/su15139895.
- Stavleu, D., Winter, P., Veenstra, X., Stralen, K., Coninck, D., Matthijs, K., … & Toelen, J. (2021). Parental opinions on medical decision-making in adolescence: a case-based survey. Journal of Developmental & Behavioral Pediatrics, 43(1), 17-22. https: //doi. org/10. 1097/dbp. 0000000000000978.
- Suzanne VERGNOLLE, L'effectivité de la protection des personnes par le droit des données à caractère personne,, Thèse Université Paris II, 2020.
- Talib, H., Silver, E., & Alderman, E. (2016). Challenges to adolescent confidentiality in a children's hospital. Hospital Pediatrics, 6(8), 490-495. https: //doi. org/10. 1542/hpeds. 2016-0011.
- Thibault DOUVILLE, La protection des données à caractére personnel des mineurs et des majeurs protégés, Revue Lamy Droit Civil (RLDS), septembre 2018.
- Thierry LÉONARD, "Yves tit u exploitais tes données?", in Droit norms et libertés dans le cybermonde: Liber Amicorym Yves Poullet, Larcier, Bruxelles, 2018.
- Tikkinen-Piri, C., Rohunen, A., & Markkula, J. (2018). Eu general data protection regulation: changes and implications for personal data collecting companies. Computer Law & Security Review, 34(1), 134-153. https: //doi. org/10. 1016/j. clsr. 2017. 05. 015.
- Tona, O., Someh, I., Mohajeri, K., Shanks, G., Davern, M., Carlsson, S., … & Kajtazi, M. (2018). Towards ethical big data

(ISSN: 2537- 0758)

artifacts: a conceptual design. . https: //doi. org/10. 24251/hicss. 2018. 571.

- Vanwymelbeke, J., Coninck, D., Matthijs, K., Leeuwen, K., Lierman, S., Boone, I., … & Toelen, J. (2022). Clinical adolescent decision-making: parental perspectives on confidentiality and consent in belgium and the netherlands. Ethics & Behavior, 33(5), 371-386. https: //doi. org/10. 1080/10508422. 2022. 2086873.
- Weisleder, P. (2004). The right of minors to confidentiality and informed consent. Journal of Child Neurology, 19(2), 145-148. https: //doi. org/10. 1177/08830738040190021101.
- Wieczorkowski, J., and Polak, P. (2017). "Big data and privacy: the study of privacy invasion acceptance in the world of big data. " Online Journal of Applied Knowledge Management, 5(1), 57-71. https: //doi. org/10. 36965/ojakm. 2017. 5(1)57-71.
- Yves POULLET, Concentement et RGPD: des zones d'ombre!, DCCR (Droit de la consomation consumentenrecht), 2019.
- Zainab Sattar Jabbar Kazem. (2022). "Civil Protection of Personal Data on the Internet (Comparative Study). " Misan Journal of Comparative Legal Studies, 1(5), 132-169. https: //doi. org/10. 61266/mjcls. v1i5. 86.