الجوانب القانونية لتقنية تحديد الموقع الجغرافي

Legal aspects of geolocation technology

إعداد

الدكتور/ ياسر محمد النيداني

مدرس القانون المدني

معهد العجمي العالي للعلوم الإدارية

البريد الإلكترونى : yasermoh014@gmail.com

ملخص البحث

تتناول هذه الدراسة موضوع الجوانب القانونية لتقنية تحديد الموقع الجغرافي ، وذلك من خلال البحث في اللائحة الأوربية لحماية البيانات الشخصية(GDPR) ، مع الاسترشاد بالأحكام القضائية الصادرة عن محكمة العدل الأوربية ومحكمة التمييز الفرنسية وكذلك الاسترشاد بآراء فرق العمل الأوربية المعنية بموضوع تحديد الموقع الجغرافي، وآراء اللجنة الوطنية لتكنولوجيا المعلومات والحريات الفرنسية(CNIL).

وقد تناولت هذه الدراسة تقنية تحديد الموقع الجغرافي من منظور تكنولوجي بطريقة مبسطة ؛ حتى يتمكن غير المتخصص من فهم الخصوصيات التكنولوجية لهذه التقنية. كما تمت دراسة الإطار التشريعي لتقنية تحديد الموقع الجغرافي ، ليلحقها بعد ذلك دراسة معالجة البيانات الناتجة عن تحديد الموقع الجغرافي والتي تم التطرق فيها لموافقة الشخص المعني ، والغرض من المعالجة ، وحقوق صاحب بيانات تحديد الوقع الجغرافي.

عرضت الدراسة شروط معالجة بيانات تحديد الموقع الجغرافي وفق متطلبات اللائحة العامة لحماية البيانات(GDPR) ، وكذلك الاستخدامات المختلفة لهذه التقنية.

خلصت هذه الدراسة إلى أن بيانات تحديد الموقع الجغرافي تخضع لأحكام اللائحة العامة لحماية البيانات باعتبارها بيانات شخصية.

الكلمات المفتاحية : تحديد الموقع الجغرافي ، البيانات الشخصية ، اللائحة العامة لحماية البيانات (GDPR)، معالجة بيانات الموقع الجغرافي.

Abstract of the research

This study deals with the legal aspects of geolocation technology, by examining the European Data Protection Regulation (GDPR), with guidance from the judicial rulings issued by the European Court of Justice and the French Court of Cassation, as well as the opinions of the European working groups concerned with geolocation, and the opinions of the French National Commission for Information Technology and Liberties (CNIL). This study addressed geolocation technology from a technological perspective in a simplified manner; so that non-specialists can understand the technological specificities of this technology. The legislative framework for geolocation technology was also studied, followed by the processing of data resulting from geolocation, which addressed the consent of the person concerned, the purpose of processing, and the rights of the owner of the geolocation data.

The study also presented the conditions for processing geolocation data in accordance with the requirements of the General Data Protection Regulation (GDPR), as well as the various uses of this technology.

This study concluded that geolocation data is subject to the provisions of the General Data Protection Regulation as personal data.

Keywords: geolocation, personal data, General Data Protection Regulation (GDPR), processing geolocation data.

٩- الجوانب القانونية لتقنية تحديد الموقع الجغرافي

مقدمة

يتميز مجتمعنا بشكل رئيسي بتكنولوجيا المعلومات والاتصالات ، والتي نستخدمها بشكل يومي ؛ لتمكين التواصل بين الناس ؛ لذلك يتم نقل جميع أنواع المعلومات وتبادلها ومشاركتها. من بين هذه المعلومات ، واحدة منها ذات طبيعة فيزيائية لا مثيل لها، وهي الموقع الجغرافي.

من خلال جهاز إلكتروني سيتمكن الشخص من تحديد موقعه في بيئته الحقيقية من خلال تفسير معلومات موقعه على خريطة جغرافية افتراضية. هذه المعلومات إذا كانت مقروءة ومفيدة للشخص الذي يطلبها، فهي مفيدة أيضًا للآخرين.

كانت القدرة على تحديد موقع الشخص عن طريق الفضاء حاجة محسوسة منذ آلاف السنين. ثم تطورت ببطء شديد على مر القرون مع ظهور البوصلة ، ورسم الخرائط ، وعلم الفلك والكرونومتر. لم يتم إحراز تقدم كبير إلا في القرن العشرين ، مع تطور موجات الراديو، التي مكنت من تحديد اتجاه الراديو، قبل وصول أنظمة الملاحة الراديوية الأرضية الكبيرة مثلDECCA ، وLORAN، ثم أوميغا.

تم استخدام الأقمار الصناعية من قِبل نظام ترانزيت في الستينيات ، وسرعان ما تبعه نظام تحديد المواقع العالمي (GPS) ، وقد أعطت أنظمة الملاحة هذه لكل شخص موقعه ، بشكل أكثر دقة مع مرور الوقت.

في الحقيقة فإن الموقع لا يمكن أن يعرفه الآخرون إلا عن طريق نقله إليهم : عن طريق السعاة في العصور القديمة ، أو عن طريق رسائل الراديو في العصر الحديث.

تحديد الموقع الجغرافي ، أي القدرة على تحديد موقع كائن أو شيء ، كان قادرًا على الظهور حقًا بفضل تطور تكنولوجيات المعلومات والاتصالات.

عندما يتعلق الأمر بتحديد المواقع الجغرافية إلكترونيا لا بد من التوضيح منذ البداية أنه يوجد الكثير من التقنيات ، وأنها ليست جميعها لها نفس الاستخدامات.

تختلف تقنية تحديد الموقع الجغرافي في الهواء الطلق عن تلك المستخدمة في الداخل، تمامًا كما يتم استخدام تقنيات معينة في المناطق الريفية تختلف في تقنياتها وعددها عن المناطق الحضرية.

تعتمد جميع عمليات تحديد الموقع الجغرافي هذه على أنواع مختلفة من البنية التحتية المخصصة ؛ لتمكين تشغيلها.

يتم الحصول على الموقع بشكل عام عن طريق رابط مادي ، أو لاسلكي ، أو لاسلكي مع نقطة وصول واحدة أو أكثر إلى شبكة معروفة إحداثياتها الجغرافية (عنوان IP لجهاز الكمبيوتر ، وهوائيات ترحيل الهاتف المحمول ، ومحطات الاتصالات اللاسلكية ...) والذي يعمل أيضًا على نقل هذا الموقع إلى من يحتاج إليه.

تختلف دقة هذه التقنيات باختلاف نطاق الاتصال بين الكائن المتصل ونقطة الوصول إلى الشبكة ، أو الإشارة. ويمكن تحسينه عن طريق التثليث عندما يمكن توصيل الكائن بعدة نقاط ، وعن طريق الجمع بين عدة تقنيات.

٩- الجوانب القانونية لتقنية تحديد الموقع الجغرافي

سمح ظهور شبكات الهاتف المحمول في التسعينيات بتحديد المواقع الجغرافية لأول مرة بدقة استمرت بعد ذلك في الزيادة مع تكثيف مرحلات الهاتف ، ومع الجمع بين موضع "GSM" وموضع محطات WiFi القريبة.

في الوقت نفسه أتاحت تقنية RFID (التعرف على الترددات الراديوية) التتبع الجغرافي للأشياء ، أو الكائنات الحية المجهزة بعلامة RFID أثناء مرورها بالقرب من البوابات المخصصة.

شهد تطور الإنترنت في العقد الأول من القرن الحادي والعشرين أيضًا إمكانية تحديد الموقع الجغرافي لمستخدم الإنترنت ، أو كائن متصل بعنوان IP الخاص به . كما تطورت تقنيات تحديد الموقع الجغرافي الأخرى في السنوات الأخيرة باستخدام إشارات البلوتوث.

أتاح تطوير تقنيات تحديد الموقع الجغرافي الجديدة الاستجابة لأربعة أنواع محددة من الاستخدامات: تحديد الموقع الجغرافي، وتحديد الموقع الجغرافي الداخلي، والموقع الجزئي ، وتحديد الموقع الجغرافي عبر الإنترنت.

يعد تحديد الموقع الجغرافي أداة ذات أهمية بالغة سواء للمؤسسات العامة أو الأشخاص العاديين.

تستخدم الشخصيات العامة تحديد الموقع الجغرافي عالميًا بهدف خدمة المصلحة العامة. تم تناول تحديد الموقع الجغرافي في البداية تحت رعاية البحث عن التوازن بين الجوانب الاجتماعية ، والاقتصادية ، والبيئية المطبقة في مجال النقل ، وقد تم استنتاج استخدام تحديد الموقع الجغرافي من مفهوم التنقل المستدام. من خلال هذا

المفهوم ، ترغب الجهات الفاعلة المؤسسية في تسهيل التنقل في وسائل النقل العام ، وغيرها من وسائل النقل المنخفضة ، أو غير الملوثة.

تعد نظم المعلومات الجغرافية والمعلومات السياقية في الوقت الحالي أحد العوامل الرئيسية في تحسين الرحلات الفردية وبالتالي فإن مراقبة وتحديد بيانات حركة المرور وإدارة الوقت بشكل أفضل بالإضافة إلى المساهمة في توفير راحة أفضل لسفر المواطنين ، ستوفر لهم الاستفادة من المعلومات المحلية الأساسية ، مثل موقع أقرب مستشفى.

من خلال الجمع بين مفهوم التنقل المستدام وتطوير تكنولوجيا المعلومات والاتصالات تمكنت السياسة الأوروبية من تحديد دور تحديد الموقع الجغرافي في النقل ، والتي قامت بتحسين التدفقات المادية التي كانت في تطور وزيادة مستمرة.

كما تم استخدام تحديد الموقع الجغرافي من قبل السلطات العامة في تخطيط المدن ، علاوة على ذلك يتبين أن للشخصيات العامة استخدامات أخرى وذلك لأغراض أكثر حساسية: كالمسائل الجنائية، حيث يكون لتحديد الموقع الجغرافي وظائف واضحة من حيث تعقب المشتبه بهم، على سبيل المثال ، ومن ناحية أخرى، فيما يتعلق بمكافحة الإرهاب.

بخصوص الأشخاص العاديين فلم يقتصر استخدامهم لتحديد الموقع الجغرافي على المساهمة في الوصول إلى الخدمات العامة الضرورية للجميع ، حيث إن المستخدمين الأفراد لديهم تصور قصير المدى لاستخدام تطبيقات تحديد الموقع الجغرافي . حيث إنهم ببساطة يحتاجون إلى القدرة على تحديد موقعهم وتحسين رحلاتهم ، أو ببساطة

٩- الجوانب القانونية لتقنية تحديد الموقع الجغرافي

لتجنب الضياع في منطقة غير معروفة ؛ لذلك أصبحت تطبيقات تحديد الموقع شائعة وواسعة النطاق بين الأفراد العاديين.

في عالم العمل يقدم تحديد الموقع الجغرافي مزايا واضحة للمستخدمين. حيث إن عددًا كبيرًا من المهن مثل شركات النقل ، وسائقي الشاحنات ، وممثلي المسافرين ، والمرشدين ، وسيارات الأجرة والسيارات السياحية ، تستفيد بلا شك من مزاياه الكثيرة في عملهم.

في إطار علاقة الأعمال التجارية مع المستهلك تستفيد الشركات من جانبها إلى حد كبير من تقنيات تحديد الموقع الجغرافي ؛ لتقديم منتجاتها وخدماتها على أساس القرب من العميل المحتمل.

من المؤكد أن تحديد الموقع الجغرافي له مزايا لا يمكن إنكارها من حيث النقل وتخطيط المدن وسهولة حركة الأفراد كما أنه بمثابة مراقبة "مبررة" في المسائل الجنائية في بعض الحالات. مع ذلك فإن هناك دائما درجة من التدخل الخفي في المجال الخاص للفرد.

تظل هذه المراقبة من قبل الغير سرية وتحدث دون علم المستخدمين ، ولكنها أيضًا مضللة بمعنى أن الأفراد ينسون أحيانًا أن إعداداتهم الخاصة بأجهزتهم المحمولة الذكية قد تركت الموقع نشطًا. كما أن النشر المنتظم للمعلومات بطريقة متعمدة يعرضهم لمخاطر جديدة.

في الحقيقة يشكل التلاقح المحتمل للمعلومات التهديد الأكثر أهمية للحق في الخصوصية وحماية البيانات الشخصية ؛ لأنه يزيد من خطر إعادة تحديد الهوية في المستويات الأعلى من معالجة البيانات.

إننا نعلم أن وجود ارتباط واحد أو استنتاج واحد بين قطعتين من البيانات من نفس المجموعة أو من مجموعتين منفصلتين يكفي لاعتبار الشخص محددًا.

مهما كانت المعلومات الناتجة عن كل معالجة مجهولة ومعزولة ، فإن المرافق الثانوية ستجعل من الممكن إعادة بناء ملف تعريف دقيق جدًا للسكان ، وبالتالي إعادة التعرف عليهم. وهذا صحيح أكثر بالنظر إلى تنوع هذه المعلومات وأصلها ، خاصة إذا تم التواصل مع بعضها طوعًا.

ستكون بيانات تحديد الموقع الجغرافي (تسجيل الوصول) وكذلك الآراء التي ينشرها مستخدمو الإنترنت حول الأماكن التي يترددون عليها جميعها عناصر تُثري تلك التي تم جمعها تلقائيًا لتحديد عادات أسلوب حياتهم ، أو حتى علاقاتهم الاجتماعية. من ثم يمكن بسهولة إثبات وجود عدة أشخاص في نفس المكان ، ومن الممكن أن يظل أولئك الذين لا يستخدمون هذه التطبيقات "عالقين" في شبكة الإسناد الترافقي للبيانات.

يعد تحديد الموقع الجغرافي أيضًا جزءًا لا يتجزأ من مجال الرفاهية والصحة، خاصة مع ظهور الأجهزة الإلكترونية القابلة للارتداء **مثل سوار** FitBit ، والذى يقوم والتطبيقات المصاحبة له بتسجيل وتجميع كافة الأنشطة التي يتم تنفيذها في اليوم، مثل عدد الخطوات ، أو السعرات الحرارية المحروقة ، أو المسافة ، والمسار المقطوع خلال السباق.

٩- الجوانب القانونية لتقنية تحديد الموقع الجغرافي

في كثير من الأحيان تشجع هذه التطبيقات المستخدمين على مشاركة أعمالهم ورحلاتهم على شبكات التواصل الاجتماعي ، وهو ما لا يتردد الكثيرون في القيام به ؛ من أجل الحصول على رسائل التشجيع ، أو الاستحسان من أقرانهم.

بشكل أكثر عمومية تشجع الشبكات الاجتماعية المستخدمين على مشاركة مواقعهم مما يسمح لهم بمعرفة موقع المستخدم وأصدقائه.

إن هذه البيانات المفتوحة التي سيكون من الممكن الوصول إليها بشكل متزايد ستجعل من الممكن تحسين تصنيف الأفراد ، وسيكون من المرجح دائمًا أن يزداد خطر إعادة تحديد الهوية مع التقدم في تكنولوجيات المعلومات والاتصالات.

من خطر إعادة تحديد الهوية هذا ينشأ الخوف من شكل جديد من المراقبة الجماعية على نطاق حضري حيث يمكن متابعة أي مقيم دون علمه ، والتخلي عن عدم الكشف عن هويته التقليدية للحشد ، من خلال الجمع الآلي والإحالة المرجعية لبياناته ، ويمكن أن ينتهي الأمر بهذه الأمور في أيدي السلطات العامة ، أو الشركات الخاصة لجميع أنواع الأغراض.

إن الخصوصية مفهوم اجتماعي تعلمناه خلال حياتنا. لدينا الكثير من العلاقات والأصدقاء ، والمعارف ، والعائلات المختلفة ، والتي يمكن أن تكون رسمية ، وغير رسمية.

عندما نشارك بعض المعلومات لدينا فإننا نعتمد على التوقعات حول ما سيحدث مع هذه المعلومات بناءً على مستوى العلاقة الحميمة ، والثقة التي لدينا مع كل مجموعة

اجتماعية ، والمشكلة هي أن نفس التفكير لا يمكن تطبيقه على الإفصاحات المرتبطة بالتكنولوجيا.

عندما نقرر تنزيل تطبيق ما على سبيل المثال وتقديم معلوماتنا الشخصية فإننا نشاركها مع توقع أنها سيتم استخدامها فقط لغرضنا المحدد. في معظم الأحيان ليس هذا ما يحدث. لذا فمن الأهمية بمكان تغيير وجهة النظر بشأن الخصوصية.

إن ما نشاركه ومع من وكيف نشاركه يلعب دورًا مهمًا فيما يمكن أن يكون خاصًا ، وما لا يكون خاصًا.

إننا نحاول الحماية من الكشف غير المرغوب فيه عن الحقائق الخاصة مثل: الأفكار والعواطف ، وكيف ، ومتى ، وإلى متى يمكن للآخرين توصيل هذه المعلومات الشخصية؟.

مع الاستخدام المكثف للهواتف الذكية وتطبيقاتها أصبح من السهل نسبيًا جمع كل هذه المعلومات ، وتخزينها ، ومشاركتها. بينما في الوقت نفسه ، يكاد يكون من المستحيل حماية جميع المعلومات التي يمكن للآخرين الوصول إليها.

يسعى هذا البحث لاكتشاف ما إذا كانت الحماية الهادفة للخصوصية يتم تعزيزها من خلال إعدادات الموقع الافتراضية وممارسة طلب إذن المستخدمين من خلال طلب الموافقة على الشروط والأحكام العامة ، أو إذا كانت هذه الشروط ، والأحكام تتسبب بدلاً من ذلك في مشاركة المستخدمين لبيانات الموقع دون علمهم.

ويتساءل البحث أيضًا عما إذا كانت هذه الممارسات تتوافق مع قانون حماية البيانات الشخصية في الاتحاد الأوروبي؟.

٩- الجوانب القانونية لتقنية تحديد الموقع الجغرافي

علاوة على ذلك يناقش البحث ما إذا كان من الممكن اعتماد خطوات شفافة صريحة ومحددة ؛ لتأمين خصوصية المستخدم على جميع مستويات استخدام الهاتف الذكي ، ويجادل بأن المستخدمين يجب أن يتمتعوا ببعض التحكم في البيانات الشخصية المرتبطة باستخدام الهاتف الذكي، بما في ذلك الموقع ، وأنه يجب تنفيذ هذا التحكم بموجب ترتيب قانوني يؤمن أيضًا خصوصية المستخدمين ويمكّن مطوري التطبيقات ، أو موفري أنظمة التشغيل من الأغراض القانونية فيما يتعلق بمعالجة بيانات الموقع.

أهمية الدراسة : تظهر الأهمية العلمية لموضوع هذا البحث في أنه يقودنا إلى محاولة إدراك وفهم تقنية تحديد الموقع الجغرافي ومدى الاستجابات القانونية الإيجابية لحماية بيانات الموقع الجغرافي للشخص الطبيعي.

إشكالية الدراسة: تظهر المشكلة الرئيسة لموضوع هذا البحث في أن معالجة بيانات الموقع الجغرافي تكشف عن العديد من البيانات الحساسة من خلال معرفة الأماكن والأفراد الذين يترددون بالإضافة إلى المدة المرتبطة بهذه الاتصالات والتي من المرجح أن يكشف الموقع الجغرافي للشخص عن ميوله الجنسية ، أو انتمائه السياسي ، أو النقابي ، أو الديني.

هذا الكشف يستدعى النظر في معرفة مدى الحماية القانونية الممنوحة لصاحب بيانات الموقع الجغرافي و شروط معالجة هذه البيانات ، وحقوق صاحب البيانات على بياناته.

فرضيات الدراسة : يثير موضوع هذا البحث بعض التساؤلات التي تتطلب إجابة عليها وهي على النحو التالي :

١–هل تخضع بيانات الموقع الجغرافي لحماية اللائحة الأوربية العامة لحماية البيانات(GDPR) باعتبارها بيانات شخصية ؟

٢– ما هي شروط معالجة بيانات تحديد الموقع الجغرافي؟ وما هي حقوق صاحب البيانات ؟

منهج الدراسة : سوف أعتمد في تناول هذا البحث على المنهج الاستنباطي إذ سأقوم باستنباط بعض الأحكام التي وردت في اللائحة الأوربية العامة لحماية البيانات (GDPR) التي تُعنى بحماية البيانات الشخصية، وكذلك ما ورد عن الفقه القانوني والأحكام القضائية بشأن بيانات تحديد الموقع الجغرافي ، وكذلك الاسترشاد بآراء فرق العمل الأوربية المعنية بموضوع تحديد الموقع الجغرافي ، وآراء اللجنة الوطنية لتكنولوجيا المعلومات والحريات الفرنسية(CNIL) ؛ وذلك من أجل الوصول لنتيجة منطقية بخصوص مدى اعتبار بيانات الموقع بيانات شخصية ، ومدى خضوعها لحماية اللائحة الأوربية العامة لحماية البيانات(GDPR).

كما أنني سأستخدم المنهج الوصفي التحليلي حيث سأقوم بتحليل كامل مفصل ومبسط لتكنولوجيا تقنية تحديد الموقع الجغرافي ، على أن نتبع ذلك بتحليل معالجة بيانات تحديد الموقع الجغرافي من حيث شروط المعالجة ، وحقوق صاحب البيانات على بياناته ، على أن ننهى الدراسة ببعض استخدامات تقنية تحديد الموقع الجغرافي ، وسوف نعرض لاستخدام تقنية الموقع الجغرافي في مكافحة وباء فيروس كورونا (COVID–19)، وفى مراقبة سيارة العمل ، وفى الأعمال التجارية.

٩- الجوانب القانونية لتقنية تحديد الموقع الجغرافي

نطاق الدراسة : سوف نقتصر نطاق الدراسة على حماية بيانات تحديد الموقع الجغرافي في دول الاتحاد الأوربي باعتباره النطاق المكاني لتطبيق اللائحة الأوربية العامة لحماية البيانات (GDPR).

خطة البحث :

مقدمة

المبحث الأول: الاطار التشريعي لتقنية تحديد الموقع الجغرافي

المبحث الثاني: معالجة البيانات الناتجة عن تحديد الموقع الجغرافي

.المبحث الثالث: استخدامات تقنية تحديد الموقع الجغرافي.

المبحث الأول

الإطار التشريعي لتقنية تحديد الموقع الجغرافي

يجسد تحديد المواقع الجغرافية حالة كائن أو شخص مادي في مساحة معينة. وهو في حد ذاته يرتكز بالضرورة على عالم ثلاثي الأبعاد ويشكل نتيجة لقراءة الإحداثيات الجغرافية التي هي المسافة الزاوية لإسقاط نقطة ما على المستوى الأساسي، والتعبير عن الموقع الشرقي والغربي لنقطة ما. وعلاقتها بخط غرينتش، أي خط الطول، مع التعبير عن الموقع بين الشمال والجنوب بالنسبة إلى خط الاستواء، أي خط العرض. وبالتالي فإن القراءة المجمعة لهذين الإحداثيين تجعل من الممكن تحديد موقع على الخريطة.

إن المعلومات الناتجة عن تحديد المواقع الجغرافية لها أغراض متنوعة للغاية ومن الصعب دحض طبيعتها الأساسية في مجتمع المعلومات. مع ذلك إذا كانت جميع الأنشطة البشرية لها بعد جغرافي فقد يبدو من المفاجئ أن نرى أن الاستخدام المحتمل للإحداثيات الجغرافية يعزز جودتها الجوهرية ، أو بالأحرى يمنحها قيمة مضافة كبيرة. وأي دراسة ترسم نتائجها رقميًا أو نصيًا تزودنا بمعلومات ذات أهمية أكبر؛ لذلك فإننا نتحدث عن علم الجيوماتكس وهو عبارة عن "مجموعة من التخصصات الحاسوبية التي تسمح بجمع وتمثيل وتحليل البيانات الجغرافية المحلية".

تشكل الخرائط الجغرافية توليفة ناجحة للبحث ؛ لأنها تسلط الضوء على مجموعة كاملة من البيانات المنسقة المتأصلة في العالم الحقيقي. ومن الواضح أنها قبل كل

شيء أداة يجب أن تكون جاهزة للاستخدام ، ويمكن لمستخدميها الوصول إليها ؛ لذلك فمن الضروري فهم الطبيعة النفعية لرسم الخرائط من أجل فهم القضايا التي تنشأ من المعلومات التي تقدمها.

تتعلق هذه المعلومات ذات الطبيعة المتنوعة بشكل ملموس بالصحة ، والأمن وحركة الجيش ، والنقل بشكل عام ، أو حتى ببساطة حركة الأفراد ، أو السكان ، ويمكن أن تكون هذه المعلومات سياسة مالية ، واجتماعية واقتصادية ، وما إلى ذلك.

توفر هذه المحطات العديد من الأدوات وأكثرها شيوعًا هو تحديد الموقع الجغرافي. تُستخدم هذه الأداة الأخيرة وهي موضوع الدراسة هنا في المقام الأول لتحديد الموقع الجغرافي للمستخدم.

سوف نستعرض في هذا المبحث تقنيات تحديد الموقع الجغرافي والتي لا شك أنها أساسية وأولية قبل الانتقال لدراسة الإطار القانوني لتحديد الموقع الجغرافي في نطاق الاتحاد الأوربي ، وذلك في مطلبين متتاليين على النحو التالي:

المطلب الأول : تقنيات تحديد الموقع الجغرافي

المطلب الثاني : الإطار القانوني الأوروبي لمعالجة بيانات تحديد الموقع الجغرافي

المطلب الأول

تقنيات تحديد الموقع الجغرافي

تمهيد

عندما يتعلق الأمر بتحديد المواقع الجغرافية إلكترونيا لا بد من التوضيح منذ البداية أنه يوجد الكثير من تقنيات تحديد الموقع الجغرافي ، كما أنها ليست جميعها لها نفس الاستخدامات.

على سبيل المثال تختلف تقنية تحديد الموقع الجغرافي في الهواء الطلق عن تلك المستخدمة في الداخل ، تمامًا كما يتم استخدام تقنيات معينة في المناطق الريفية أكثر من المناطق الحضرية.

تعتمد جميع عمليات تحديد الموقع الجغرافي هذه على أنواع مختلفة من البنية التحتية المخصصة لتمكين تشغيلها ؛ لذلك فمن المناسب التمييز بين التقنيات الرئيسية المستندة إلى هذه الجوانب المختلفة.

ما يهمنا في هذه الدراسة هو عرض تقنيات تحديد الموقع الجغرافي المعترف بها عالميًا باعتبارها تقنيات الاستخدام الرئيسية والتي ستظل راسخة بشكل جيد للاستخدامات المستقبلية ؛ للمساعدة في توضيح الإطار القانوني بشكل أكبر. ويتم إيلاء اهتمام خاص لتلك المطبقة على المحطات الطرفية المتنقلة ، وخاصة الأجهزة المحمولة الذكية.

٩- الجوانب القانونية لتقنية تحديد الموقع الجغرافي

تقنيات تحديد الموقع الجغرافي المختلفة

هناك العديد من تقنيات تحديد الموقع الجغرافي ، مع ذلك نحن لا نهدف إلى أن نستعرض كل هذه التقنيات ؛ ذلك أننا نستهدف من هذه الدراسة محاولة فهم آلية هذه التقنيات ، وحدودها ، وخاصة تلك المعتمدة على الهواتف المحمولة ، وهذا الاختيار له ما يبرره في ضوء انتشار تطبيقات الهاتف المحمول وتطور السوق.

علاوة على ذلك فإن تراكم هذه التقنيات وتفاعلها مع مختلف المحطات الطرفية داخل مجتمع المعلومات يطرح أسئلة معقدة بشكل خاص، وبالتالي، فإننا نميز بين تحديد الموقع الجغرافي عن طريق التثليث الذي يتعلق ببيانات المحطة الأساسية، وعن طريق نظام تحديد المواقع العالمي (GPS)، وعن طريق wifi وعن طريق تحديد الهوية الراديوية (RFID) وعن طريق عنوانIp ، وأخيراً عن طريق البلوتوث.

١ : تحديد الموقع الجغرافي عن طريق التثليث

هذه التكنولوجيا والتي تسمى أيضًا تحديد الموقع الجغرافي بواسطة "المحطة الأساسية" هي تلك الناتجة عن المناطق المختلفة التي يغطيها مشغلو الاتصالات.

هذه المناطق عبارة عن تغطيات جغرافية تسمى الخلايا ويتم تحديدها بواسطة المجال الكهرومغناطيسي لهوائيات الترحيل ، وهو أحد العناصر الأساسية لنظام تشغيل الهاتف المحمول للنظام العالمي للهواتف المحمولة (GSM). من خلال هوائيات

الترحيل هذه يجب أن تمر الإشارة المنبعثة من الجهاز المحمول لإجراء مكالمات هاتفية أو الاتصال بالإنترنت عبر ثلاث هوائيات[١].

عندما نقوم بتنشيط البيانات الخلوية لنظام GSM الخاص بنا أي شبكة G3 ، من أجل الاتصال بالإنترنت ، أو بكل بساطة عندما نستخدمها لإجراء مكالمات هاتفية، يجب أن يتصل جهازنا المحمول حتماً بقاعدة المحطة التي تغطي هذه الخلية[٢].

تعتمد فعالية هذه الطريقة على عدد الهوائيات التي يتصل بها الهاتف ، وفي حالة استخدام هوائي واحد ، أو اثنين يظل الموقع تقريبيًا للغاية ، ولهذا السبب يلزم وجود ثلاثة هوائيات

وبفضل قوة ودقة إشارة الهوائي التي يستقبلها الهاتف من الممكن إنشاء دائرة حول كل هوائي خلوي فنحصل على ثلاث دوائر، واحدة حول كل هوائي ، وتقاطع هذه الدوائر هو الذي يمثل موقع الهاتف[٣].

في الواقع طوال فترة تشغيل الجهاز المحمول يكون الأخير مرتبطًا بمحطة قاعدة معينة ، وسيتم تسجيل روابطه باستمرار بواسطة مشغل الاتصالات، وسوف يكون هذا

[1] - M. Henri BarbIerk, Les Enjeux, de L'encadrement Juridique de la geolocalisation master, faculte de droit et de science politique, nstitut de recherches en droit de L’information et DE la communication, 2013-2014. p.10

[2]- Komur, Neslin, La géolocalisation dans la relation de travail :un dispositif de surveillance sans limite(s) mettant en péril le droit au respect de la vie privée du travailleur ?Master . faculte De droit et de criminologie, universite uclouvain Année académique 2018-2019 p.6

[3] - Michael Laranj Mise en relation des données de géolocalisation lors de procédures pénales, Haute École de Gestion de Genève (HEG-GE) Filière Informatique de Gestion 2014 p.8.

الأخير، بالإضافة إلى عدد كبير جدًا من الأجهزة المحمولة ، قادرين على استخدام إشارات من خلايا متداخلة (محطات قاعدة مجاورة) لتقدير موضع الجهاز المحمول بدقة أفضل"[١].

يمكن لهوائيات الترحيل هذه المرادفة للمحطات القاعدة أن تغطي عمومًا محيطًا يمكن أن يصل إلى ٣٥ كم في المناطق الريفية ، ومن ٥٠٠ متر إلى ٢ كم في المناطق الحضرية. ويجب أن يؤخذ في الاعتبار أن الخلايا تختلف حسب حجم منطقة التغطية والعوائق الطبوغرافية الطبيعية ، أو الاصطناعية، مثل الجبال ، أو المباني[٢].

اصطلاحا تسمى هذه التقنية التثليث والبيانات الناتجة عن هذه التقنية هي البيانات من المحطات الأساسية والتي يمكن استخدامها بطريقة إبداعية على وجه الخصوص للكشف عن الاختناقات المرورية[٣].

يتكون **التثليث** من عبور البيانات من ثلاث محطات لتحديد الموقع الجغرافي. بشكل ملموس يكون الاتصال بين المحطة الأساسية والجهاز المحمول الذكي ثابتًا منذ لحظة تشغيل الأخير، وسيظل كذلك طالما لم يتم إيقاف تشغيله.

مع ذلك أثناء الاتصال يمكن لمشغل الاتصالات الوصول إلى التبادلات الموجودة فيه وتسجيلها دون انقطاع.

[1] - Groupe Article 29 Avis n°13/2011 du 16 mai 2011 sur les services de géolocalisation des dispositifs mobiles intelligents, 881/11/FR, WP185,p. 4.
[2] - M. Henri BarbIerk, op cit p.10.
[3] - Groupe Article 29 Avis n°13/2011 du 16 mai 2011, op cit p.4.

تتمتع المحطات الأساسية بمعرف فريد وهي ليست متنقلة بل هي ثابتة وبالتالي يتم تحديد موقعها مرة واحدة وإلى الأبد.

تسمح هذه العملية بتقدير سريع لموقع المحطة بدقة نسبية في المدينة بحوالي ٥٠ مترًا بالنسبة لموقعها وعدة كيلومترات في الريف. وتظل أقل دقة بكثير من نتائج تقنيات GPS و WiFi [١].

٢. تحديد الموقع الجغرافي عن طريق نظام تحديد المواقع(GPS).

يتكون تحديد الموقع الجغرافي عبر الأقمار الصناعية من حساب الموقع الحالي على وجه الأرض لمحطة مجهزة بشريحة متوافقة. تتم بعد ذلك ترجمة هذا الموقع من حيث خطوط الطول والعرض ويمكن بعد ذلك تمثيله فعليًا على الخريطة، ويعد أشهر شبكة لتحديد المواقع عبر الأقمار الصناعية هـ GPS(نظام تحديد المواقع العالمي) [٢].

تم تشغيل تقنية نظام تحديد المواقع العالمي (GPS) عام ١٩٩٤ ووصلت إلى القدرة التشغيلية الكاملة في أوائل عام ١٩٩٥ عندما كانت كوكبة الأقمار الصناعية المنتجة البالغ عددها ٢٤ موجودة بالكامل وتم الانتهاء من الاختبارات الشاملة لجزء التحكم

[1] - M. Henri BarbIerk, op cit p.10

[2] - Ismail Slimani Toufik Habireche , Conception et réalisation d’un système de géolocalisation et de suivi, Cas NAFTAL,Mémoire de Fin d’Etudes de master ,Universite Mouloud Mammeri de Tizi-ouzou ,Faculte du Genie electrique et d’informatique departement d’informatique ,Algérienne 2016 p.22

الأرضي وتفاعلاته مع هذه الأقمار الصناعية[١]، وأصبح استخدامها مرجعًا متكررًا للغاية في مجال النقل[٢].

يتكون نظام تحديد المواقع العالمي والمعروف باسم تقنية GPS من أقمار صناعية تدور كل منها في واحد من ستة مدارات مختلفة حول الأرض والتي تنقل إشارة راديوية بدقة شديدة.

تشكل هذه الأقمار الصناعية شبكة في السماء وتكون بمثابة معايير لملاحي نظام تحديد المواقع العالمي (GPS) في عملية حساب مواقعهم. لكي تتمكن المحطة من تحديد موقعها الجغرافي باستخدام شبكة نظام تحديد المواقع العالمي (GPS) ، يجب أن تكون مجهزة بشريحة إلكترونية لنظام تحديد المواقع العالمي (GPS)[٣].

بالتالي، فإن **الأجهزة المحمولة الذكية** التي تتضمن شريحة مدمجة مزودة بجهاز استقبال GPS يسمح لها بتحديد موقعها ويمكنها بسهولة تحديد موضعها في الفضاء عندما يلتقط مستشعر GPS الخاص بها أربع إشارات راديوية على الأقل[٤].

من حيث المبدأ فإن تركيب تكنولوجيا نظام تحديد المواقع العالمي (GPS) على المحطات الطرفية المتنقلة سيسمح بتحديد موقعها عبر شرائح نظام تحديد المواقع العالمي (GPS) المتوافقة والمدمجة في نظام هذه المحطات الطرفية.

---

[1] - Elliott Kaplan,Understanding GPS: principles and applications/[editors], Christopher Hegarty.—2nd ed.2005 p.4

[2] - M. Henri BarbIerk, op cit p.11

[3] - Ismail Slimani Toufik Habireche, op cit p.22.

[4] - Komur, Neslin, op cit p.7 - S. FARMER, « European Privacy Body Opines on Geolocation Services on Smart Mobile Devices », in C.T.L.R, vol. 17., New-York, Thomson Reuters, 2011, p.115

بشكل ملموس تستخدم هذه التكنولوجيا من ٢٤ قمرًا صناعيًا مستقرًا بالنسبة إلى الأرض، أي على بعد ٣٦٠٠٠ كيلومتر من الأرض، والتي تدور في أحد المدارات الستة المختلفة حول الأرض، وتنقل إشارة دقيقة بشكل خاص[١].

تصبح هذه الأقمار الصناعية من خلال إنشاء شبكة في السماء معايير مرجعية لملاحي نظام تحديد المواقع العالمي (GPS) ؛ حتى يتمكنوا من تحديد موقعهم الخاص، والذي يتم ترجمته مباشرة من حيث خطوط الطول والعرض.

يعمل نظام تحديد المواقع العالمي (GPS) بشكل أساسي باستخدام الأقمار الصناعية التي أطلقتها الولايات المتحدة في البداية للأغراض العسكرية قبل أن يتم استخدامه لتحديد المواقع للمدنيين. من جانبها، أطلقت المفوضية الأوروبية شبكتها الخاصة المكونة من ١٨ قمراً صناعياً في عام ٢٠١١ من خلال برنامج غاليليو ، الذي يسمح بتقديم خدمة تحديد المواقع العالمية عبر الأقمار الصناعية للاستخدام غير العسكري.

بفضل هذه الأقمار الصناعية يمكن للمحطة تحديد موقعها طالما أن مستشعر GPS يكتشف أربعًا على الأقل من هذه الإشارات، وبالتالي أربعة أقمار صناعية. كما أن الإشارة تكون صحيحة لا لبس فيها؛ وذلك لأنها تنتقل في اتجاه واحد فقط ، ولا يستطيع مديرو الأقمار الصناعية تتبع الأجهزة التي استقبلت الإشارة[٢].

[1] - Elliott Kaplan, op cit p.3.
[2] - M. Henri BarbIerk, op cit p.11.

يوفر النظام للمستخدمين- على مستوى العالم- باستخدام معدات الاستقبال المناسبة معلومات دقيقة مستمرة وثلاثية الأبعاد عن الموقع والسرعة. كما يقوم أيضا بنشر شكل من أشكال التوقيت العالمي المنسق ، ويقدم خدماته لعدد غير محدود من المستخدمين ؛ نظرًا لأن أجهزة استقبال المستخدم تعمل بشكل سلبي (أي تستقبل فقط) ، حيث يستخدم النظام مفهوم تحديد وقت الوصول في اتجاه واحد (TOA)[١].

٣. تحديد الموقع الجغرافي عبر شبكة Wi-Fi

تعد شبكة Wi-Fi تقنية أكثر تعقيدًا من تكنولوجيا نظام تحديد المواقع العالمي (GPS) السابقة[٢].

Wi-Fi تعني الإخلاص اللاسلكي و هي شبكة عالية السرعة يُقصد من تغطيتها أن تكون واسعة مثل الهاتف المحمول وهي مخصصة للاتصال بالإنترنت[٣].

يعد نظام Wi-Fi واحدًا من أشهر الأنظمة على الإطلاق لكن القليل من الناس يعرفون أنه لفترة قصيرة تم استخدام نقطة الوصول إلى Wi-Fi كمصدر للمعلومات وتحديد الموقع الجغرافي ؛ لأنها تعمل باستمرار يشير إلى وجوده عن طريق إرسال اسم الشبكة الخاصة به ، وعنوان MAC الخاص به[٤] ، حتى لو لم يكن هناك أحد

[1] - Elliott Kaplan, op cit p.3.
[2] - M. Henri BarbIerk, op cit p.12.
[3]- Merabtene Amel et Agred Nouara, Système de géolocalisation pour les réseaux mobiles, diplôme de Master en informatique,Faculté de Génie Electrique et Informatique ,Université Mouloud Mammeri de Tizi-Ouzou, Algérienne 2012-2013 p.26
[4] - Groupe Article 29 Avis n°13/2011 du 16 mai 2011, op cit p 4 - 6.

يستخدم الاتصال و"يتم تشفير محتويات الاتصال اللاسلكي باستخدام نظام WEP ، أو WPA ، أو WPA2[1].

تحت اسم Wi–Fi توجد مجموعة من المعايير للشبكات اللاسلكية ويعتبر استخدامها لأغراض تحديد الموقع الجغرافي حديثًا نسبيًا[2].

أما بالنسبة لمبدأ تشغيله فهو مشابه أيضًا لمبدأ تحديد الموقع الجغرافي عن طريق التثليث.

في الواقع يمكن التعرف على هاتين التقنيتين من خلال معرف فريد (أحدهما يتعلق بالمحطة الأساسية والآخر يتعلق بنقطة الوصول إلى Wi–Fi) والذي يمكن اكتشافه من خلال عدد وافر من المحطات الطرفية.

فيما يتعلق بنقطة وصول Wi Fi فإن المعرف المخصص لها يتوافق مع عنوان MAC (التحكم في الوصول إلى الوسائط). هذا هو معرف آخر يتم تعيينه لواجهة الشبكة المسجلة بشكل عام على مكونات الأجهزة (أجهزة الكمبيوتر ، والهواتف المحمولة ، ونقطة الوصول وما إلى ذلك). يُطلق على هذا المعرف على وجه التحديد اسم معرف مجموعة الخدمة الأساسية لنقاط الوصول إلى Wi–Fi.

حقيقة أن نقاط الوصول هذه تبث إشاراتها بشكل مستمر يجعلها مثيرة للاهتمام بشكل خاص لتحديد الموقع الجغرافي. نظرًا لأن معظمها يستخدم في أوروبا، يتم تمكين الاتصال افتراضيًا، لذا فهم يرسلون إشاراتهم باستمرار حتى لو لم يكن هناك أحد

[1] - Komur, Neslin, op cit p.7.
[2] - M. Henri BarbIerk, op cit p.12

٩- الجوانب القانونية لتقنية تحديد الموقع الجغرافي

يستخدم الاتصال؛ ذلك أن الأجهزة المحمولة تكتشف وجود نقاط الوصول إلى شبكة Wi-Fi تلقائيًا تقريبًا، عن طريق المسح النشط أو السلبي، وتجمع البيانات عنها بشكل ميكانيكي تقريبًا. لذلك، ليست هناك حاجة لهذه الأجهزة المحمولة للاتصال بنقاط اتصال Wi-Fi لجمع معلومات "Wi-Fi"[١].

إن حقيقة تمكن المستخدم من العثور على نقاط وصول Wi Fi باستخدام أجهزته الطرفية والقدرة على الاتصال بها تظهر بوضوح استمرارية الإشارة.

علاوة على ذلك تتمتع الهواتف الذكية والأجهزة اللوحية بإمكانية اكتشاف نقاط وصول Wifi تلقائيًا لجمع المعلومات[٢]، ولا سيما البيانات المتعلقة بها، أي ذات طبيعة شخصية، إما عن طريق "المسح النشط"، أو عن طريق "المسح السلبي[٣].

يتضمن المسح النشط إرسال إطار استعلام إلى جميع نقاط وصول Wi-Fi المحيطة وتسجيل الردود وتخزينها والتي لا تتضمن معلومات حول الأجهزة المتصلة بنقطة وصول Wi-Fi.

علاوة على ذلك يتكون المسح السلبي من إطارات طلب التسجيل المرسلة بواسطة كل نقطة وصول ، حيث يمكن أن يؤدي هذا المسح بسهولة إلى جمع البيانات المتبادلة

---

[1] - Komur, Neslin, op cit p.8.

[٢] – قد تنتمي قواعد البيانات هذه إلى شركات خاصة ، أو إلى مجتمعات تنشرها مجانًا. يتم إنشاء قواعد البيانات هذه باستخدام طريقة تسمى War Driving، والتي تتكون من القيادة في شوارع المدينة باستخدام جهاز كمبيوتر محمول مزود بشبكة Wi-Fi ومتصل بجهاز استقبال GPS، من أجل تحديد أكبر عدد ممكن من نقاط الوصول اللاسلكية.

Ismail SLIMANI Toufik HABIRECHE , op cit p.24.

[3] - Groupe Article 29 Avis n°13/2011 du 16 mai 2011,p. 6

بين نقاط الوصول والأجهزة المرتبطة بها. وبالتالي يمكن بعد ذلك تسجيل عناوين MAC لمجموعة متنوعة من المحطات الطرفية ، وأجهزة الكمبيوتر المكتبية ، وأجهزة الكمبيوتر المحمولة والطابعات دون أن يلاحظ المستخدم أن هناك هجومًا على خصوصيته[١].

يتم تحديد الموقع الجغرافي بوضوح إذا كانت الإشارة مكثفة وهذا يعتمد على قربها من نقطة الوصول إلى شبكة Wi–Fi للمحطات المجهزة بهوائي ؛ نظرًا لأن مستخدمي خدمات تحديد الموقع الجغرافي يقومون تلقائيًا بجمع عناوين IP التي تلتقطها أجهزة Wi–Fi الخاصة بهم للعثور على طريقهم في الفضاء، ثم يتم إرسال العديد من معلومات التعريف بواسطة الهاتف الذكي إلى موفري خدمة تحديد الموقع الجغرافي (عنوان MAC، معرف SSID، IMEI أو IMSI، و أيضًا بيانات GPS وبيانات المحطة الأساسية).

تسمح هذه البيانات لمقدمي الخدمات المذكورين بحساب موضع نقاط وصول Wi–FI الجديدة ، أو تحسين تلك الموجودة بالفعل.

تتسم عملية جمع البيانات ومعالجتها بواسطة مراقبي البيانات بأنها لا مركزية تمامًا وفعالة للغاية وغالبًا ما يتم تنفيذها دون علم المستخدمين[٢].

تتيح هذه التقنية تحديد موقع سريع للغاية ودقيق بشكل متزايد خاصة إذا كان حساب الموقع مستمرًا. نظرًا لأن شبكة Wi–Fi أثبتت نجاحها بشكل خاص فإن دمجها مع

[1] - M. Henri BarbIerk, op cit p.12

[2] - Komur, Neslin, op cit p.8. - Groupe Article 29 Avis n°13/2011 du 16 mai 2011, p.7

تقنيات GPS وGSM يميل إلى جعل الهواتف الذكية أكثر المحطات الطرفية استهدافًا من قبل الغير المهتم ، حيث يشكل هذا المزيج بوابات متعددة لمحتوى الهواتف الذكية ، وبالتالي للبيانات الشخصية[١].

٤- تحديد الموقع الجغرافي بواسطة شريحة RFID

يعرف الراديو، الذي يشار إليه غالبًا بالاختصار RFID بأنه وسيلة لتخزين واسترجاع البيانات عن بعد باستخدام علامات تسمى علامات الراديو. (علامة RFID أو جهاز إرسال واستقبال RFID").

يتكون نظام RFID من أجهزة إرسال واستقبال (وتسمى أيضًا الملصقات والعلامات والمعرفات وما إلى ذلك) ، ومستجوب واحد ، أو أكثر (يُسمى أيضًا المقرنات وهوائي القارئ ..)[٢].

تعد هذه التقنية أقدم من التقنيات الثلاثة الأولى كما أنها أكثر تحديدًا منها ؛ لأنها تستخدم لتحديد الموقع الجغرافي الداخلي. كما أنها تقنية منتشرة في كل مكان بمواصفات تقنية أبسط ولكنها لا تقتصر على تحديد الموقع الجغرافي[٣].

يتيح تحديد الترددات الراديوية أو RFID (التعرف على ترددات الراديو) التعرف عن بعد على الأشياء أو الأفراد الثابتين أو المتحركين، وتبادل البيانات معهم اعتمادًا على التطبيقات المتوخاة[٤].

---

[1] - M. Henri BarbIerk, op cit p.13
[2] - Ismail SLIMANI Toufik HABIRECHE , op cit p.25.
[3] - M. Henri BarbIerk, op cit p.14.
[4] - MERABTENE Amel et AGRED Nouara op cit p.22

يسمح تحديد الموقع الجغرافي بواسطة RFID بتحديد موضع الجهاز الذي يصدر موجات على ترددات مشابهة للأجهزة الأخرى القريبة إلى حد ما.

في التطوير الكامل في المباني الكبيرة المفتوحة للجمهور مثل مراكز التسوق[١] حيث يستخدم التجار هذا النظام بشكل أساسي في سياق تحليلات البيع بالتجزئة ، أو تتبع المتسوقين. تتكون هذه الطريقة من وضع مستشعر RFID على بطاقة ولاء العميل ويسمح من خلال قارئات الشرائح المثبتة ، والمنتشرة في جميع أنحاء السوبر ماركت، بتشكيل مناطق استراتيجية ، وبالتالي متابعة تحركات العميل في المتجر ، وقياس الوقت الذي يقضيه في الأقسام المختلفة. بهذه الطريقة، فإن البيانات المخزنة ستجعل من الممكن تنفيذ ملفات تعريف العملاء ، وبالتالي "تحسين معرفة العملاء ، وعاداتهم الاستهلاكية"[٢]. كما يتم أيضًا وضع شرائح RFID هذه على عربات التسوق الخاصة بالمؤسسة بهدف تحديد موقع العميل في المتجر حتى لو كانت المعلومات التي تم جمعها بهذه الطريقة ليست دقيقة تمامًا[٣].

الميزة التي تعود على التجار من استخدام هذه التكنولوجيا هي أنها تعمل بشكل جيد للغاية في الداخل. مع ذلك فإن هذه التكنولوجيا تعاني من جمع غير متناسب، إن لم يكن ضخمًا، لجميع أنواع البيانات[٤].

---

[1] - Ibid

[2] - C., COLIN et Y., POULLET, « Du consommateur et de sa protection face à de nouvelles application des technologies de l'information : risques et opportunités », D.C.C.R, 2010/3, n°88, p. 100

[3] - Komur, Neslin, op cit p.9.

[4] - M. Henri BarbIerk, op cit p.14.

٩- الجوانب القانونية لتقنية تحديد الموقع الجغرافي

٥- تحديد الموقع الجغرافي عن طريق عنوان ip.

تتيح هذه الطريقة تحديد الموقع الجغرافي لجهاز الكمبيوتر أو أي محطة متصلة بالإنترنت بناءً على عنوان IP (بروتوكول الإنترنت) الخاص به[١].

عنوان IP (بروتوكول الإنترنت) هو رقم تعريف يتم تعيينه بشكل دائم أو مؤقت لكل جهاز متصل بشبكة كمبيوتر باستخدام بروتوكول الإنترنت. و هو أساس نظام تسليم (توجيه) الرسائل على الإنترنت.

تتم إدارة عناوين IP بواسطة IANA (هيئة الأرقام المخصصة للإنترنت) وهي منظمة مسؤولة عن تقطيع مجموعات عناوين IP المتاحة وتوزيعها بطريقة خاضعة للرقابة للغاية على البلدان التي تطلبها[٢].

نظرًا لأن كل هذه السمات موثقة جيدًا فمن الممكن معرفة البلد الذي توجد فيه محطة متصلة بالإنترنت بفضل عنوان IP الخاص بها. يمكننا أيضًا الحصول على مستوى من الدقة لترتيب المدينة استنادًا إلى توزيع عناوين IP التي يقوم بها موفرو الوصول إلى الإنترنت[٣].

بالنسبة لعنوان IP المرتبط بتاريخ ووقت محددين يمكن للسلطات المعنية الحصول من مزود خدمة الإنترنت على الموقع الجغرافي الدقيق والاسم والعنوان الذي أبلغه

---

[1] – MERABTENE Amel et AGRED Nouara op cit p.22

[٢] – IANA (هيئة الأرقام المخصصة للإنترنت) هي منظمة أمريكية يتمثل دورها في إدارة أسماء نطاقات المستوى الأعلى (TLDs)، ومساحة عنوان IP للإنترنت، وموارد الترقيم المشتركة الأخرى التي تتطلبها بروتوكولات الاتصال على الإنترنت، أي للتوصيل البيني الشبكات إلى الإنترنت.

[3]- Ismail SLIMANI Toufik HABIRECHE , op cit p.25

صاحبه. ولكن يتم الاحتفاظ بهذه البيانات لفترة محدودة فقط، وتختلف مدتها حسب البلد. وبالمثل بالنسبة لمساحة الوصول التجارية إلى الإنترنت ("مقهى الإنترنت")، اعتمادًا على البلد، قد يُطلب من التاجر الاحتفاظ بالتواريخ والأوقات ومستندات الهوية الممسوحة ضوئيًا لفترة معينة[١].

قامت شركة جوجل بأتمتة هذه العملية من خلال دمجها في محرك البحث الخاص بها ؛ ليحصل المستخدم على النتائج حسب موقعه الجغرافي. تعرض "خرائط"Google ، أثناء استعلام عام مثل "مطعم"، خريطة Google مع النتائج ذات الصلة.

حاليا تعرض خريطة جوجل المصغرة المنطقة التي يتواجد فيها المستخدم حتى لو لم يحدد موقعه بناءً على عنوان IP الخاص بمستخدم الإنترنت[٢].

كما أطلقت مواقع الويب، مثل Twitter وFacebook، أيضًا خيارات تتبع الموقع من خلال تحديد عنوان IP الخاص بالمستخدم.

تختلف دقة تحديد الموقع الجغرافي عبر IP وفقًا لعدة عوامل بما في ذلك المنطقة ونوع الاتصال بالإنترنت. فعلى سبيل المثال، يمكن تحديد موقع المستخدمين المتصلين عبر شبكات الهاتف المحمول بشكل أكثر دقة من أولئك الذين يستخدمون اتصالات الخطوط الأرضية في المنزل.

---

[1]- Ibid.

[2] - Géolocalisation et télécommunications fr.
https://www.lagbd.org › Géolocalisation_et_télécommuni .

٦- تحديد الموقع الجغرافي بواسطة البلوتوث(Bluetooth)

البلوتوث هو معيار لتقنية لاسلكية قصيرة المدى يستخدم لتبادل البيانات بين الأجهزة الثابتة والمتنقلة على مسافات قصيرة ، وبناء شبكات المناطق الشخصية.

تتمتع تقنية البلوتوث بميزة إمكانية استخدامها في البيئات الخارجية والداخلية[١]، ومع ذلك فإنها من بين تقنيات تحديد الموقع الجغرافي تشكل الوسيلة التقنية الأكثر ملاءمة لفكرة لسياج الجغرافي.

يتكون السياج الجغرافي في تشغيله من إنشاء منطقة محددة بإشارات كهرومغناطيسية أو صوتية.

تلعب تقنية البلوتوث دورا مهما في تحديد الموقع الجغرافي الداخلي والذى يتيح تحديد معرفة موقع شخص ، أو منتج بدقة أكبر ، أو أقل في مساحة ، أو مكان لا يتوفر فيه الوصول إلى بيانات الأقمار الصناعية ونظام تحديد المواقع العالمي (GPS).

نجد اليوم أنظمة تحديد الموقع الجغرافي الداخلية في عدة أنواع من الأماكن المغلقة مثل المطارات، مراكز التسوق ، أو المراكز الثقافية، مراكز المعارض ، في بعض الجامعات وكذلك في المستشفيات[٢]، والذي يتيح للزوار إرشادهم داخل المكان ؛ لتحسين زيارتهم من خلال تحديد النقاط المثيرة للاهتمام الموجودة في مكان قريب.

[1] - Observatoire du Monde Cybernétique , NOUVELLES TECHNIQUES DE GEOLOCALISATION ET RISQUES CYBER, Lettre no 67 octobre 2017. P.4.

[2] - http://www.journaldunet.com/ebusiness/internet-mobile/1133686-geolocalisation-indoor-comment-ca-marche/

أدى نشر محطات WiFi أو Bluetooth في مراكز التسوق أو المطارات إلى تمكين المرء من تحديد موقعه في هذه البيئات منذ فترة طويلة[١].

في الواقع فإن المدى القصير لهذه التقنية يجعل من الممكن تحديد موقع جسم أو شخص بدقة باستخدام القليل من الطاقة وبتكلفة أقل.

مع ذلك ونظرًا للقيود المفروضة في البيئات الداخلية المعقدة في كثير من الأحيان، لا يمكن لتقنية البلوتوث ضمان تحديد الموقع الجغرافي الداخلي الحقيقي في الوقت الفعلي ، وبدقة كبيرة إلا من خلال نشر العديد من المحطات الطرفية ، أو من خلال الجمع بين الحلول التقنية ، وهو ما يمكن أن يمثل تكلفة عالية[٢].

المطلب الثاني

الإطار القانوني الأوروبي لمعالجة بيانات تحديد الموقع الجغرافي

نظرة عامة على الموضوع

تعد الخصوصية مصدر قلق بالغ فيما يتعلق بتطبيقات الهواتف الذكية (التطبيقات) واستخدام الأجهزة المحمولة بشكل عام في جميع أنحاء العالم.

تخضع خصوصية الموقع، على وجه الخصوص، للتدقيق ؛ نظرًا لأنه يمكن استخلاص معلومات خاصة أخرى من المعلومات المتعلقة بالموقع.

[1] - Observatoire du Monde Cybernétique , op cit p.5.
[2]- Observatoire du Monde Cybernétique , op cit p.6

٩- الجوانب القانونية لتقنية تحديد الموقع الجغرافي

تشير خصوصية بيانات الموقع إلى الحق في عدم التعرض لجمع أو الاحتفاظ أو الاستخدام أو التوزيع غير المصرح به ، وكذلك تجهيز الأفراد ببيانات الموقع الفعلية أو التنظيمية[١].

لا يشير مفهوم خصوصية بيانات الموقع إلى إخفاء المعلومات – بل إنه يحمي معلومات الموقع الحالية ، أو السابقة للشخص من الاستخدام لأغراض تجارية ، أو غيرها دون علم الشخص[٢].

يصبح العديد من مستخدمي الهواتف الذكية والأجهزة المحمولة الأخرى مترددين في تثبيت تطبيقات الهاتف المحمول ، أو إلغاء تثبيتها بعد أن أدركوا أن بياناتهم الشخصية قد تم الكشف عنها للآخرين بسبب تثبيت تطبيقات معينة[٣].

علاوة على ذلك في كثير من الحالات، نظام تشغيل الهاتف المحمول يقوم بنفسه بجمع البيانات التي يمكن اعتبارها بيانات شخصية، وقد يكون من المستحيل بسبب قيود نظام التشغيل الاستفادة من الوظائف الكاملة لأجهزة الجهاز دون تمكين جمع بعض البيانات.

---

[1] - Location Forum, Location Data Privacy Guidelines, Assessments and Recommendations (Version 2, 1 May 2013)

[2]-Bu-Pasha, Shakila & Alén, Anette & Mäkinen, J. & Guinness, Robert & Korpisaari, Päivi. (2016). EU Law Perspectives on Location Data Privacy in Smartphones and Informed Consent for Transparency. European Data Protection Law Review. 2. 312-323. 10.21552/EDPL/2016/3/7 p.312..
https://doi.org/10.21552/EDPL/2016/3/7 -

[3] - Jan Lauren Boyles et al, 'Privacy and Data Management on Mobile Devices' (Pew Research Center, 5 September 2012)
<http://www.pewinternet.org/2012/09/05/privacy-and-data-man-agement-on-mobile-devices

كما يمكن انتهاك الحق في خصوصية مستخدمي الهواتف الذكية بعدة طرق، على سبيل المثال من خلال تتبع عادات الويب ، ومراقبة قوائم الاتصال، وتتبع الموقع، وفحص الملفات دون علم المالك، وجمع المعلومات التقنية بما في ذلك عناوين IP وبيانات المعاملات الأخرى[١].

عندما تميل منصات الإنترنت وأنظمة تشغيل الأجهزة المحمولة ، أو مطورو التطبيقات ، أو الناشرون إلى معالجة بيانات موقع المستخدمين، يتعين عليهم القيام بذلك بما يتوافق مع القانون.

بشكل عام يشمل مصطلح "بيانات الموقع" أي معلومات تشير ضمنيًا ، أو صراحةً إلى الموقع الجغرافي ، أو المكاني.

من أجل فهم دور بيانات الموقع في ظل الأطر القانونية المختلفة من المهم التمييز بين الحالات التي تكون فيها بيانات الموقع تشكل إما بيانات شخصية ، أو بيانات حساسة (أي فئة خاصة من البيانات الشخصية). من تلك الحالات التي تكون فيها البيانات مجهولة المصدر بشكل فعال، وبالتالي لا تعتبر بيانات شخصية ، أو حساسة[٢].

في الواقع في الوقت الذي كان فيه تطور تكنولوجيا المعلومات والاتصالات وخاصة الإنترنت، في مراحله الأولى، كان المشرع الأوروبي قد أدرك بالفعل في عام ١٩٩٥

[1] - Bu-Pasha, Shakila & Alén, Anette & Mäkinen, J. & Guinness, Robert & Korpisaari, Päivi. (2016).op cit p.313.
[2] - Bu-Pasha, Shakila & Alén, Anette & Mäkinen, J. & Guinness, Robert & Korpisaari, Päivi. (2016).op cit p.314.

المشاكل والقضايا المرتبطة بالبيانات الشخصية[١] والتي أصبحت في الواقع، العنصر الاقتصادي الأساسي للكون الرقمي، وهي متاحة بطريقة فورية وعالمية بفضل التقدم التكنولوجي[٢].

مع ذلك فإن "الاستخدام لأغراض تجارية أو حتى سوء الاستخدام الذي قامت به شركات الإنترنت الكبرى قد جعل الجميع يدركون تدريجيًا الخطر الذي يمكن أن يسببه تداول البيانات الشخصية دون عوائق في إطار احترام الحياة الخاصة"[٣].

عندما تتطور تكنولوجيا معلومات جديدة في الممارسة العملية ينبغي منطقيا أن تخضع لاحترام مبدأ الحياد التكنولوجي ، بحيث يكون تطبيق القانون واسعا ، دون التمييز بين محتوى ومصدر ووجهة المعلومات التي تحملها هذه التكنولوجيا.

بخصوص القوانين المتعلقة بتحديد الموقع الجغرافي في الاتحاد الأوربي فسوف نتعرض أولا لميثاق الحقوق الاساسية للاتحاد الأوربي ، ثم نستعرض قوانين حماية البيانات الأوربية :

أولا : ميثاق الحقوق الأساسية للاتحاد الأوروبي (CFR)

بخصوص حقوق الانسان والحق في الخصوصية فقد تم الاعتراف بميثاق الحقوق الأساسية للاتحاد الأوروبي (CFR)[١] باعتباره القانون الأساسي للاتحاد الأوروبي منذ

[1] - Komur, Neslin, op cit p.39.
[2] - Komur, Neslin, op cit p.39 - Christophe Radé, [Brèves] A propos de la géolocalisation des salariés : la CNIL et la Cour de cassation à l'unisson, Lexbase Social, novembre 2011, n°462.
[3] - Komur, Neslin, op cit p.40.- S. PEYROU, « Le nouveau règlement général européen relatif à la protection des données à caractère personnel : un texte à la hauteur de ses ambitions », R.A.E., 2016. P.103.

عام ٢٠٠٩ ، وبالتالي يعتبر ملزمًا قانونًا وله قيمة مماثلة للمعاهدات. بموجب هذا الميثاق فإن احترام الحياة والحقوق الخاصة والعائلية وحماية البيانات الشخصية مكفولة في المادة ٧ ، والمادة ٨، على التوالي، كما تضمن المادة ٨ (٢) من قانون اللوائح الفيدرالية حق أصحاب البيانات في الوصول إلى البيانات الشخصية التي تم جمعها وتصحيحها ، وتسمح بمعالجة البيانات الشخصية مع موافقة أصحاب البيانات على أسس عادلة ، ومحددة لبعض الأغراض القانونية ، وتنص المادة ٥٢ على قيود على الحقوق والحريات المنصوص عليها في الميثاق أيضًا.

تضمن المادة ٨ من الاتفاقية الأوروبية لحقوق الإنسان الحق في الخصوصية والذي يشمل خصوصية مستخدمي الإنترنت أيضًا. كما قررت المحكمة الأوروبية لحقوق الإنسان (ECtHR) أن انتهاكات الحقوق والحريات الأساسية التي تكفلها الاتفاقية، والتي تحدث في العالم الرقمي ، أو عبر الإنترنت، ويمكن أن تحددها المحكمة الأوروبية لحقوق الإنسان[٢].

من ثم فإنه ينبغي احترام الخصوصية المنصوص عليها في كل من قانون العلاقات الخارجية والاتفاقية الأوروبية لحقوق الإنسان بغض النظر عن مصدر تهديد الغزو، بما في ذلك الهواتف الذكية ، أو تطبيقات الهاتف المحمول – وينطبق الشيء نفسه على بيانات الموقع.

[1] - CHARTER OF FUNDAMENTAL RIGHTSOF THE EUROPEAN UNION (2000/C 364/01.

[2] - Ashby Donald and others v France App no 36769/08 (ECtHR, 10 January 2013).

مع ذلك فإن الحق في الخصوصية ليس حقًا مطلقًا بموجب المادة ٨ من الاتفاقية الأوروبية لحقوق الإنسان، ولا يُسمح بالتدخل في هذا الحق من قبل السلطات العامة إلا لأسباب مشروعة، مثل حماية الأمن القومي ، أو الرفاهية الاقتصادية ، والسلامة العامة ، الصحة ، أو الأخلاق ، أو حقوق الآخرين ، وحرياتهم ، أو منع ارتكاب جرائم أخرى.

في قضية أوزون ضد ألمانيا تم تحديد المراقبة عبر نظام تحديد المواقع العالمي (GPS) وبالتالي معالجة واستخدام بيانات موقع مقدم الطلب على أنها تدخل متناسب في الحياة الخاصة بموجب المادة ٨ من الاتفاقية الأوروبية لحقوق الإنسان[١].

كما أن قيام الدولة بمعالجة بيانات الموقع من أجل مكافحة الإرهاب ودون الحصول على موافقة صاحب البيانات ، كان مبررا بمصالح الأمن القومي والسلامة العامة ، وكان "ضروريًا في مجتمع ديمقراطي" وفقًا للاستثناءات المنصوص عليها في المادة ٨ (٢)[٢].

ثانيا- قوانين حماية البيانات الأوربية.

مر الإطار القانوني الأوربي لحماية البيانات الشخصية بمرحلتين مختلفتين: في المرحلة الأولى كانت التشريعات عبارة عن توجيهات للدول أعضاء الاتحاد الأوربي ،

[1] - UUzun v Germany App no 35623/05, IHRL 1838 (ECtHR, 2 September 2010). 105a, note 81eA Law Review 1701er data protection system when the GDPR comes into force.e twork cell connected with the termina

[2] - Council of Europe/European Court of Human Rights, Research Division, Internet: case-law of the European Court of Human Rights (2011, Updated: June 2015),p.7

ثم أصبح من الضروري إعادة تحديد إطار قانوني مناسب ، وأكثر صرامة وتكيفًا مع التقدم التكنولوجي السريع[١]؛ لذلك تم اعتماد اللائحة الأوروبية رقم ٢٠١٦/٦٧٩ الخاصة بحماية البيانات الشخصية فى٢٧ أبريل ٢٠١٦ التي أطلق عليها(GDPR).

١–التوجيهات الأوربية:

على الرغم من أن النصوص الأوروبية والتي هي في الأساس توجيهات لم تركز فقط على تحديد الموقع الجغرافي ولكن على معالجة البيانات الشخصية في مجملها ، إلا أن فريق العمل المعني بحماية البيانات بموجب المادة ٢٩ قد ناقش الإطار الذي يمكن تطبيقه بشكل خاص على تحديد الموقع الجغرافي ، وانتهى إلى أن الإطار القانوني ذو الصلة هو توجيه حماية البيانات (EC/٤٦/٩٥)(DPD) وينطبق ذلك عندما تتم معالجة البيانات الشخصية بعد معالجة بيانات الموقع[٢].

في عام ١٩٩٠، قدمت المفوضية الأوروبية أول مشروع لتنظيم حماية البيانات الشخصية، مما أدى في عام ١٩٩٥ إلى اعتماد التوجيه EC/٤٦/٩٥ الصادر عن البرلمان الأوروبي والمجلس فيما يتعلق بحماية الأشخاص الطبيعيين فيما يتعلق بالبيانات الشخصية، معالجة البيانات الشخصية ، وحرية حركة هذه البيانات[٣].

[1] - Charlotte SIKIVIE, Comment les entreprises traduisent-elles les obligations légales contenues dans le Règlement (UE) 2016/679 relatif à la protection des données en obligations de compliance ? Analyse comparative entre PME et grandes structures.Master en droit.à U Liège. Année académique 2019-2020 p.10.

[2] - Groupe Article 29 Avis n°13/2011 du 16 mai 2011. op cit. p.8

[3] - B. VAN ALSENOY, Data Protection Law in the EU: Roles, Responsibilities and Liability, Cambridge, Intersentia, 2019, p. 261 à 263

٩- الجوانب القانونية لتقنية تحديد الموقع الجغرافي

رغم أن مصطلح بيانات الموقع لم يتم ذكره على وجه التحديد في هذا التوجيه إلا أن هذا التشريع له أهمية قصوى ؛ نظرًا لأن أحكامه تنطبق على حماية ومعالجة البيانات الشخصية، بما في ذلك بيانات الموقع التي تعتبر مثل هذه البيانات ، وكذلك بيانات الموقع التي يتم جمعها عبر تطبيقات الهاتف المحمول والهواتف الذكية[١].

بالتالي فإن التوجيه EC/٤٦/٩٥ المتعلق بحماية البيانات الشخصية الصادر في ٢٤ أكتوبر ١٩٩٥، يشكل بالفعل الأساس الرئيسي من خلال تسليط الضوء على الالتزامات الملقاة على عاتق بعض مديري معالجة بيانات الموقع.

كما ينطبق توجيه الخصوصية والاتصالات الإلكترونية (EC/٥٨/٢٠٠٢، بصيغته المعدلة بموجب التوجيه EC/١٣٦/٢٠٠٩ ، فقط على معالجة بيانات المحطة الأساسية بواسطة خدمات وشبكات الاتصالات الإلكترونية العامة (مشغلي الاتصالات)[٢].

تم تعريف بيانات الموقع بموجب التوجيه EC/١٣٦/٢٠٠٩ – الذى يعتبر تعديلا للتوجيهEC/٤٦/٩٥ – في المادة ٢، فقره ٣ بأنه: جميع البيانات التي تتم معالجتها في شبكة اتصالات إلكترونية ، أو بواسطة خدمة اتصالات إلكترونية تشير إلى الموقع الجغرافي للمعدات الطرفية لمستخدم خدمة اتصالات إلكترونية متاحة للجمهور.

[1] - Bu-Pasha, Shakila & Alén, Anette & Mäkinen, J. & Guinness, Robert & Korpisaari, Päivi. (2016).op cit p.316.

[2] – Groupe Article 29 Avis n°13/2011 du 16 mai 2011. op cit. p.8

فإذا كان مشغل الاتصالات يقدم خدمة تحديد الموقع الجغرافي المختلطة والتي تعتمد أيضًا على معالجة أنواع أخرى من بيانات الموقع مثل بيانات GPS أو Wi–Fi، فإن هذا النشاط يعتبر خدمة اتصالات إلكترونية عامة، ويجب على مشغل الاتصالات الحصول على موافقة مسبقة من عملائه إذا قدم بيانات تحديد الموقع الجغرافي هذه إلى الغير[١].

مع ذلك يجب أيضًا التأكيد على أنه من الناحية العملية لم يكن تبديل التوجيه واضحًا. ففي الواقع كانت هناك تناقضات داخل الدول الأعضاء في الاتحاد الأوروبي، مما أدى إلى "مشهد قانوني مجزأ نسبيًا ، وتنافر في تطبيق قانون المجتمع"[٢].

علاوة على ذلك بعد سنوات قليلة فقط من اعتماده، فقد هذا التشريع الأوروبي الرئيسي الأول بشأن البيانات الشخصية أهميته بسبب التقدم التكنولوجي المستمر الذي مكن من ظهور ممارسات جديدة مثل البيانات الضخمة، والحوسبة السحابية، وإنترنت الأشياء، وما إلى ذلك، والذى لم يكن متوقعًا في التسعينيات ، وبالتالي توافرت فرصًا جديدة في استغلال البيانات الشخصية[٣].

كان من الضروري والعاجل تحديث النص التأسيسي مع مراعاة ما ورد أعلاه من أجل تحسين حماية البيانات الشخصية للأفراد ، وفي هذا السياق تم اعتماد اللائحة العامة لحماية البيانات.

---

[1] – Groupe Article 29 Avis n°13/2011 du 16 mai 2011op cit. p.8

[2] - S. PEYROU, op. cit., p. 103.

[3] - Komur, Neslin, op cit p.40.

٢-اللائحة الأوربية العامة لحماية البيانات الشخصية رقم ٢٠١٦/٦٧٩(GDPR)

نظرًا لأن التوجيه CE/٤٦/٩٥ وتعديلاته أصبحا غير متكيفين مع القيود الناجمة عن وصول التقنيات الجديدة. فمع ظهور التقنيات الجديدة، أصبح الوصول إلى البيانات الشخصية أسهل من أي وقت مضى.

علاوة على ذلك حدث كثيرًا أن المواطنين الأوروبيين شاهدوا بياناتهم الشخصية تستخدم من قبل كيانات لا تخضع للوائح الأوروبية . كما حاولت محكمة العدل الأوروبية، من خلال سوابقها القضائية، تحديث هذه الثغرات وسدها، ولكن هذا لم يجدى ، وأصبح من الضروري إعادة تحديد إطار قانوني مناسب يكون أكثر صرامة وتكيفًا مع التقدم التكنولوجي[1]؛ لذلك تمت زيادة حماية معالجة البيانات الشخصية بشكل كبير من خلال اعتماد اللائحة الأوروبية الخاصة بحماية البيانات الشخصية فى٢٧ أبريل ٢٠١٦.

تحافظ هذه اللائحة ككل على المبادئ العامة للتوجيه EC/٤٦/٩٥ ، علاوة على ذلك، تخلق شروطًا جديدة.

اختار المشرع الأوروبي هذه المرة لائحة وليس توجيها كما كان الحال في عام ١٩٩٥، والتي ستستهدف جميع المواطنين الأوروبيين.

فيما يتعلق بالتطبيق المباشر تعكس اللائحة الرغبة في المضي قدمًا داخل الاتحاد الأوروبي نحو تنسيق حقيقي للقواعد المطبقة بطريقة ملزمة وتسمح، بحكم الأمر الواقع، بتجنب الاختلافات في التشريعات داخل مختلف الدول الأعضاء ، كما تم

[1] - Charlotte SIKIVIE, op cit p.10.

توسيع نطاق اللائحة بشكل أكبر ، بمعنى أنها تستهدف أيضًا مراقب البيانات الذي ليس لديه "مؤسسات داخل الاتحاد، ولكنه يقوم بمعالجة بيانات الأشخاص الموجودين في الاتحاد" ، وبعبارة أخرى ، فإن جنسية الأشخاص الذين تخضع بياناتهم للمعالجة أصبح لا أهمية له في تطبيق اللائحة[١].

توفر اللائحة الأوروبية المزيد من الدقة لموافقة الشخص الذي تخضع بياناته الشخصية للمعالجة من خلال اشتراط موافقة لا لبس فيها ، والتي يتم استخلاصها من قانون واضح[٢]. علاوة على ذلك، أصبح الأمر الآن متروكًا لمراقب البيانات لتقديم دليل على هذه الموافقة[٣]، والتي، علاوة على ذلك، يمكن للشخص سحبها في أي وقت[٤].

بالمقارنة مع التوجيهات السابقة تنص اللائحة على التزام أكبر بالشفافية. ففي الواقع تسرد اللائحة العام لحماية البيانات الفرضيات المختلفة التي يجب التواصل فيها مع الأشخاص المعنيين "بطريقة موجزة ، وواضحة ، ومفهومة ، ويمكن الوصول إليها بسهولة"، والمعلومات (مثل أغراض المعالجة، وتفاصيل الاتصال بمراقب البيانات، وما إلى ذلك) ؛ مما يتيح لهم أن يفهموا بسهولة ما إذا كانت بياناتهم تتم معالجتها،

[1] - A. DELFORGE, « Comment (ré)concilier RGPD et big data ? », R.D.T.I, 2018, n°70, p.15-29

[2] – Art. 4 (11) du RGPD

[3] – Art. 7 (1) du RGPD

[4] - Art. 7 (3) du RGPD

وبأي طريقة ، ولأي سبب[١]. تساعد هذه المعلومات في إبلاغ صاحب البيانات بالتأثير الذي قد تحدثه المعالجة على حقوقه وحرياته المختلفة المنصوص عليها في اللائحة.

إن مبدأ الشفافية يقودنا مباشرة إلى مبدأ المساءلة. ففي الواقع، الأمر متروك لمراقب البيانات لإثبات أنه يحترم المبادئ العامة للائحة العامة لحماية البيانات، ومن بينها مبدأ الشفافية[٢]. في الوقت نفسه، "يتطلب مبدأ المساءلة شفافية عمليات المعالجة حتى يتمكن مراقبو البيانات من إثبات أنهم يفون بالتزاماتهم بموجب اللائحة العامة لحماية البيانات ، وهذا جديد على اللائحة العامة لحماية البيانات ، ويعد أحد "أهم التغييرات التي تمت مواجهتها خلال الإصلاح[٣].

لا يزال في "المبادئ المتعلقة بمعالجة البيانات الشخصية" (المادة ٥ من اللائحة العامة لحماية البيانات)، يتم تقديم مبدأ تقليل البيانات والذي بموجبه يمكن معالجة البيانات الشخصية التي تبدو ضرورية فقط لتحقيق الغرض، أيضًا كالتزام بضمان أمن وسرية المعالجة. علاوة على ذلك، تحدد اللائحة بمزيد من التفصيل عن توجيه عام ١٩٩٥ حقوق الوصول والتصحيح للأشخاص المعنيين.

[1] - Groupe Article 29, Guidelines on transparency under Regulation 2016/679 (WP260 rev.01), 11 avril 2018

[2] - Charlotte SIKIVIE,op cit p.18

[3] - S. PARSA, « Le R.G.P.D. et la profession d'avocat, au-delà du secret professionnel et du principe de confidentialité », Le Règlement général sur la protection des données (R.G.P.D./G.D.P.R.) : premières applications et analyse sectorielle, H. Jacquemin (dir.), vol. 195, Liège, CUP, Anthemis, 2020, p. 133.

أخيرًا قامت اللائحة العامة لحماية البيانات أيضًا بتبسيط ممارسة حق المعارضة من خلال فرض عبء الإثبات على مراقب البيانات. وفي الواقع، فإن الأخير هو الذي يجب أن يثبت أن المعالجة مبررة "بأسباب مشروعة ومقنعة تسود على حقوق ومصالح الشخص المعني".

كما كرست اللائحة العامة لحماية البيانات حقوقا جديدة حيث تم تقديم ميزتين جديدتين مهمتين بشكل خاص من خلال هذه اللائحة ، ولا سيما "الحق في إمكانية نقل البيانات الشخصية" ، و"الحق في النسيان".

يمنح المبدأ الأول أي شخص الحق في إزالة البيانات الشخصية المتعلقة به ، والتي يحتفظ بها المراقب. كما ينص أيضًا على إمكانية طلب نقل هذه البيانات مباشرة إلى وحدة تحكم أخرى عندما يكون ذلك ممكنًا من الناحية الفنية.

أما المبدأ الثاني المنصوص عليه صراحة في المادة ١٧ بعنوان الحق في المحو فقد أثار الكثير من التعليقات عند صياغته ، وما زال يثير العديد من الأسئلة.

بموجب هذا الحق يحق لأي شخص أن يطلب، بعد فترة زمنية معينة وفي ظروف معينة محو المعلومات المتعلقة به ، وهذا هو الحال بشكل خاص عندما يمارس الشخص المعني حقه في الاعتراض على المعالجة ، أو عندما تكون الأخيرة غير قانونية ؛ لذلك سيُطلب من مراقب البيانات مسح البيانات المعنية ، وربما تنفيذ الوسائل اللازمة لتحذير وحدات التحكم الأخرى التي تستخدم هذه البيانات أيضًا.

المبحث الثاني

معالجة البيانات الناتجة عن تحديد الموقع الجغرافي

تمهيد : هل بيانات تحديد الموقع تعد بيانات شخصية؟

بداية يجب علينا قبل أن نتطرق لدراسة معالجة بيانات تحديد الموقع الجغرافي أن نحدد طبيعة بيانات تحديد الموقع ، وهل هي بيانات شخصية وفقا للمعنى المقصود في القانون أم لا؟

البيانات الشخصية هي أي معلومات تتعلق بشخص طبيعي محدد ، أو يمكن تحديد هويته.

يمكن تحديد هوية الشخص إذا كان من الممكن التعرف عليه بشكل مباشر ، أو غير مباشر خاصة بالرجوع إلى معرف مثل الاسم ، ورقم التعريف ، وبيانات الموقع ومعرف الإنترنت وما إلى ذلك.

بيانات الموقع تأخذ بعدًا محددًا بشكل واضح وهو ما لم يكن موجودًا بشكل مباشر في التشريعات السابقة عليها ، حيث تشير اللائحة العامة لحماية البيانات صراحةً إليها بالمادة الرابعة.

البيانات الشخصية معلومات تتعلق بفرد يمكن تحديد هويته ، وهذا يعنى الأخذ بتفسير واسع ؛ لذلك فإن أي بيانات "تهم" الشخص ليس فقط عندما تتعلق بذلك الشخص، ولكن أيضًا عندما تؤثر عليه ، أو يمكن أن ترتبط به[١].

على الرغم من أن الموقع الجغرافي في حد ذاته لا يرتبط بشخص ما (على عكس اسمه ، أو رقم التأمين الاجتماعي، على سبيل المثال)، فمن الممكن بشكل عام ربطه بفرد يمكن تحديد هويته. في الواقع، غالبًا ما ترتبط بيانات تحديد الموقع الجغرافي – مثل العديد من البيانات الأخرى – بمعرف فريد ، أو بحساب المستخدم. على سبيل المثال، وفقًا لسياسة الخصوصية الخاصة بتطبيق Waze، ترتبط جميع البيانات المتعلقة بالمستخدم بمعرف فريد حتى لو لم يقم المستخدم بإنشاء حساب[٢].

اقترحت مجموعة ال٢٩ ثلاثة معايير تسمح بتحديد هوية الشخص ، أو إعادة تحديد هويته: التفرد ، والارتباط ، والاستدلال[٣] ، ويجب على مراقب البيانات وضع التدابير التنظيمية والفنية التي تحول دون هذه الاحتمالات[٤].

في حزمة الامتثال "للمركبات المتصلة والبيانات الشخصية تعتبر اللجنة الوطنية لتكنولوجيا المعلومات والحريات الفرنسية(CNIL) أن بيانات تحديد الموقع الجغرافي

[1] - Vincent Bergeron et Thomas Gagnon -van Leeuwen , Geolocalisation et Application mobilles: Mode D'emploi pour une Geolocalisation eloignee des problemes juridiques! Robic, LLP ,CIPS 2015 p.26

[2] - IbId

[3] - GROUPE DE TRAVAIL «ARTICLE 29» SUR LA PROTECTION DES DONNÉE, Avis 05/2014 sur les Techniquesd'anonymisation, Adopté le 10 avril 2014.

[4] - Michèle Guilbot, ,op cit p.26

والبيانات الفنية المرتبطة بحالة السيارة ، وأجزائها ،وبيانات القياسات الحيوية للسائق ، والبيانات المرتبطة بمثابة معرف لاستخدام السيارة من قبل السائق ، أو الركاب.

كما أن جميع البيانات التي يمكن ربطها بشخص طبيعي محدد ، أو يمكن التعرف عليه ، ولا سيما عبر رقم لوحة الترخيص ، أو الرقم التسلسلي للمركبة، هي بيانات شخصية محمية.

كذلك تشكل البيانات المتعلقة بالرحلات التي تمت، وحالة استخدام الأجزاء، وتواريخ الفحص الفني، وعدد الكيلومترات ، أو أسلوب القيادة بيانات شخصية عندما يكون من المحتمل أن تكون مرتبطة بشخص طبيعي[١].

بالنظر إلى أن الأجهزة المحمولة تُستخدم عمومًا من قبل شخص واحد، فمن الممكن في كثير من الأحيان ربط المعلومات المتعلقة بالجهاز بفرد[٢].

من المهم ملاحظة أنه من خلال جمع بيانات الموقع ، يستطيع مطورو التطبيقات ، أو الجهات الفاعلة الأخرى استنتاج أنواع عديدة من المعلومات الشخصية بصرف النظر عن مجرد الموقع، مثل الانتماء الديني ، أو السياسي. على سبيل المثال، إذا كان شخص ما يزور الكنيسة بانتظام ، أو يذهب إلى حانة للمثليين في عطلات نهاية الأسبوع ، فيمكن استخلاص استنتاجات حول دين ذلك الشخص ، أو تفضيلاته الجنسية[٣].

---

[1] - CNIL, Véhicules connectés : un pack de conformité pour une utilisation responsable des données 16 octobre 2017

[2] - Vincent Bergeron et Thomas Gagnon -van Leeuwen op cit p.27.

[3] - CJEU Oct. 6, 2020, La Quadrature du Net, nos . C-511/18, C-512/18 and C-520/18.

نظرًا لأن العديد من السمات المحمية بالخصوصية ترتبط بشكل فريد بالأماكن أو الأحداث ، فإن جمع البيانات التي تظهر أن شخصًا ما يزور مكانًا ما بشكل متكرر، أو يحضر حدثًا معينًا يمثل وسيلة قوية لرسم صورة شاملة للفرد[١].

خلصت لجنة حماية البيانات الشخصية (CVPC) مؤخرًا إلى أن موقع الجهاز المحمول عبارة عن معلومات يمكن ربطها بفرد بمفرده ، أو بمعلومات أخرى يمكن لشركة Google الوصول إليها، وبالتالي تشكل معلومات شخصية. كما قررت أن البيانات الواردة من نظام تحديد المواقع العالمي (GPS) المثبت في مركبات عمل الموظفين تشكل معلومات شخصية ؛ لأنه "يمكن إنشاء رابط بين المعلومات التي تم جمعها والموظفين الذين يقودون المركبات"[٢]

في حين أن بيانات تحديد الموقع الجغرافي قد تبدو غير ضارة ، إلا أنها لديها القدرة على الكشف عن تفاصيل حميمة وحساسة.

كما ذكر فريق عمل حماية البيانات "المادة ٢٩" التابع للمفوضية الأوروبية، يمكن أن تشكل بيانات تحديد الموقع الجغرافي ملفًا شخصيًا للشخص يكشف عن عادات أسلوب حياته والأماكن التي يتردد عليها[٣].

يتيح ذلك لمقدمي الخدمات القائمة على تحديد الموقع الجغرافي الحصول على نظرة عامة تفصيلية عن عادات وأنماط مالك هذا الجهاز ، وإنشاء ملفات تعريف واسعة

[1] - Bu-Pasha, Shakila & Alén, Anette & Mäkinen, J. & Guinness, Robert & Korpisaari, Päivi. (2016).op cit p.315

[2] - Vincent Bergeron et Thomas Gagnon -van Leeuwen op cit p.27.

[3] - Groupe de l'article 29 Avis n° 13/2011 sur les services de géolocalisation des appareils mobiles intelligents p.7.

النطاق ، ومن نمط عدم النشاط ليلاً يمكن استنتاج مكان النوم ، ومن نمط السفر المنتظم في الصباح يمكن استنتاج موقع صاحب العمل.

قد يتضمن النمط أيضًا بيانات مستمدة من أنماط حركة الأصدقاء ، بناءً على ما يسمى بالرسم البياني الاجتماعي.

وقد يتضمن النمط السلوكي أيضًا فئات خاصة من البيانات إذا كانت على سبيل المثال تكشف عن زيارات إلى المستشفيات ، والأماكن الدينية ، أو التواجد في المظاهرات السياسية ، أو التواجد في مواقع محددة أخرى تكشف عن بيانات حول الحياة الجنسية للمستخدم[١].

من أجل فهم دور بيانات الموقع في ظل الأطر القانونية المختلفة من المهم التمييز بين الحالات التي تكون فيها بيانات الموقع تشكل إما بيانات شخصية ، أو بيانات حساسة (أي فئة خاصة من البيانات الشخصية) من تلك الحالات التي تكون فيها البيانات مجهولة المصدر بشكل فعال، وبالتالي لا تعتبر بيانات شخصية ، أو حساسة.[٢].

منذ لحظة دمج بيانات تحديد الموقع الجغرافي مع البيانات الشخصية ستخضع المعالجة المتعلقة بها لنظام اللائحة العامة لحماية البيانات (GDPR) مع كل العواقب التي ينطوي عليها ذلك.

[1] - Vincent Bergeron et Thomas Gagnon -van Leeuwenop cit p.28..
[2]- Bu-Pasha, Shakila & Alén, Anette & Mäkinen, J. & Guinness, Robert & Korpisaari, Päivi. (2016).op cit p.314

في الوقت الحاضر يمكن أن تكون معالجة البيانات التي يتم تنفيذها داخل التطبيقات مبهمة. وعلى وجه الخصوص، غالبًا ما تكون المعلومات المتعلقة بوجود مجموعات البيانات ، وأغراضها غير واضحة.

بالمثل، قد يواجه المستخدم صعوبة في فهم طبيعة التفويضات المطلوبة منه ، مما يُعقد التعبير عن خياراته.

أخيرًا تحمل الهواتف المحمولة متعددة الوظائف العديد من أجهزة الاستشعار المعروفة إلى حد ما للمستخدمين (الكاميرا، ، ونظام تحديد المواقع العالمي (GPS)، وقاعدة بيانات جهات الاتصال، ومقاييس التسارع ، وما إلى ذلك) والتي يمكن أن تسمح للتطبيقات بالوصول إلى البيانات التي يمكن أن يكون جمعها تطفليًا للغاية.

لذلك من الضروري أن يضمن المشاركون في توفير تطبيقات الهاتف المحمول الامتثال لالتزاماتهم فيما يتعلق بحماية البيانات ، وحقوق المستخدم[1].

لكي تكون معالجة البيانات المتعلقة بتحديد الموقع الجغرافي قانونية يجب أن تستند إلى أحد الأسس القانونية الستة التي تقدمها اللائحة العامة لحماية البيانات.

تمت صياغة المادة ٦ الفقرة ١ من اللائحة العامة للبيانات على النحو التالي: "لا تكون المعالجة قانونية إلا في حالة استيفاء شرط واحد على الأقل من الشروط التالية: (أ) وافق صاحب البيانات على معالجة بياناته الشخصية من أجل واحد ، أو أكثر من الأغراض المحددة.

[1]- CNIL.Projet de recommandation Relative aux applications mobiles, Version soumise à consultation publique jusqu’au 8 octobre 2023 p.4

(ب) المعالجة ضرورية لأداء العقد الذي يكون موضوع البيانات طرفًا فيه ، أو لتنفيذ تدابير ما قبل التعاقدية المتخذة بناءً على طلب موضوع البيانات.

ج) المعالجة ضرورية للامتثال للالتزام القانوني الذي يخضع له المراقب.

(د) المعالجة ضرورية لحماية المصالح الحيوية لصاحب البيانات ، أو لشخص طبيعي آخر.

(هـ) المعالجة ضرورية لأداء مهمة لتحقيق المصلحة العامة ، أو في ممارسة السلطة العامة المخولة للمراقب.

(و) المعالجة ضرورية لأغراض المصالح المشروعة التي يسعى إليها المراقب ، أو طرف ثالث، ما لم يتم تجاوزها بالمصالح ، أو الحقوق والحريات الأساسية لصاحب البيانات ، والتي تتطلب حماية البيانات الشخصية ، لا سيما عندما يكون الشخص المعني طفل.

كما يجب على القائمين على هذا النوع من المعالجة أن يلتزموا ببعض الالتزامات وهى :

١-الحصول على موافقة الشخص المعني (مستخدم تطبيق الهاتف المحمول، مستخدم الإنترنت، وما إلى ذلك) لجمع بيانات تحديد الموقع الجغرافي الخاصة به.

٢-احترام الغرض من المعالجة الذي يجب أن يكون واضحًا ومشروعًا.

٣–تزويد أصحاب البيانات بمعلومات عن مدة الاحتفاظ بالبيانات ، والغرض، والمستلمين، والحقوق التي يتمتعون بها (حق التصحيح، وحق المعارضة، وحق الوصول، وقابلية النقل ، وما إلى ذلك)

وهذه الالتزامات الثلاثة هي شروط أساسية لكى يستطيع مراقب البيانات معالجة البيانات الناتجة عن تحديد الموقع الجغرافي ، وهى ما سوف نتناوله في هذا المبحث من خلال المطالب التالية :

المطلب الأول : الموافقة على معالجة البيانات الناتجة عن تحديد الموقع الجغرافي

المطلب الثاني : الأغراض المقبولة لتحديد الموقع الجغرافي

المطلب الثالث : حقوق أصحاب بيانات تحديد الموقع الجغرافي

المطلب الأول

الموافقة على معالجة البيانات الناتجة عن تحديد الموقع الجغرافي

تمهيد

قررت المادة السادسة فقرة ١(أ) أنه عندما لا تحقق معالجة بيانات تحديد الموقع الجغرافي أحد الأغراض التي حددتها اللائحة، فإن الحصول على موافقة صاحب البيانات يعد أحد الأسس الأساسية لتنفيذ مثل هذا النظام ، حيث إنه "بدون موافقة، لا يوجد تحديد للموقع الجغرافي"[1].

[1] - Komur, Neslin, op cit p.56.

٩- الجوانب القانونية لتقنية تحديد الموقع الجغرافي

موافقة الشخص المعني هي أي مظهر من مظاهر الإرادة الحرة ، والمحددة ، والمستنيرة ، ولا لبس فيها يقبلها الشخص المعني عن طريق إعلان ، أو عن طريق عمل إيجابي واضح يحدد أن البيانات الشخصية المتعلقة به تخضع للمعالجة[١].

في هذا المطلب ، سنتناول واجب الموافقة الذي يعتبر أساس قانون حماية البيانات الشخصية[٢] ويعتبره البرلمان الأوروبي "العنصر الأساسي في نهج الاتحاد الأوروبي لحماية البيانات ؛ لأنها أفضل طريقة للأفراد للتحكم في أنشطة معالجة البيانات"[٣].

الأسس الرئيسية للشرعية التي يتذرع بها مراقبو البيانات هي، وفقًا للجنة حماية الخصوصية : الموافقة، والعقد، والامتثال لالتزام قانوني، والمصلحة المشروعة.

يعد التزام الموافقة أحد الأسباب الشرعية لمعالجة البيانات التي يقوم بها مراقب البيانات ؛ خاصة وأن قيمته الجوهرية في سياق معالجة بيانات الشركات بصفة خاصة تعطيها طابعا حساسا بشكل خاص؛ لذلك يجب طلب الموافقة من المستخدم قبل المعالجة المتوخاة[٤].

هذه الموافقة وهي مفهوم مركزي في قانون حماية البيانات تؤدي إلى عدد من التعليقات ، وستكون مطلوبة بشكل أقل مما قد يُعتقد ؛ نظرًا للقسوة الشديدة لشروط

---

[1] - De Terwangne, , Les principes relatifs au traitement des données à caractère personnel et à sa licéité Dans Le règlement général sur la protection des données (RGPD/GDPR): analyse approfondie. Cahiers du CRIDS, Numéro 44, Larcier , Bruxelles, 2018 p. 122

[2] - Y. POULLET, « Consentement et RGPD : des zones d'ombre ! », *D.C.C.R.* n° 122-123, 2019 p. 4

[3] - Charlotte SIKIVIE,op cit p.20.

[4] - M. Henri BarbIerk, op cit p.29.

صحة الموافقة. على سبيل المثال من الشائع أن تختار الشركات الاعتماد على فرضيات أخرى تتعلق بالمشروعية ، ولا سيما التي تجعل المعالجة قانونية بشرط أن تكون ضرورية لأغراض تحقيق المصالح المشروعة[١] .

وفقًا لرأى مجموعة عمل المادة ٢٩ فإنه يجب على مراقب البيانات اختيار الأساس القانوني الأكثر ملاءمة ، ويجب اعتبار الموافقة بمثابة أساس فرعي، والذي سيتم استخدامه فقط "لما لا يمكن تبريره من قبل الطرف الآخر[٢].

كما قررت أنه بخصوص غالبية معالجات البيانات في العمل فلا ينبغي أن يكون الأساس القانوني هو موافقة العمال ؛ نظرا لطبيعة العلاقة بين صاحب العمل والعامل[٣] والتي قد تجعل الموافقة أساسًا قانونيًا غير مؤكد[٤].

"إذا كان الإغراء كبيرًا بالنسبة للمسؤولين عن المعالجة لصالح الموافقة فقد يكون من الحكمة أيضًا تفضيل قواعد أخرى أكثر أمانًا إذا كان ذلك ممكنًا" ، ومع ذلك، هناك حالات يتطلب فيها القانون وجود الموافقة بشكل محض وببساطة، وعلى الرغم من الاستخدام المحدود لها على ما يبدو، يبدو من الضروري بالنسبة لنا التوسع في هذه الفكرة.

[1] - Charlotte SIKIVIE,op cit p.21 - art. 6 (1) du RGPD).
[2] - Groupe de l'article 29, « Avis n°15/2011 sur la définition du consentement », WP 187
[3] - Groupe de l'article 29, « Opinion 2/2017 on data processing at work», Adopted on 8 June 2017 p.6
[4]- Charlotte SIKIVIE,op cit p.21.

٩- الجوانب القانونية لتقنية تحديد الموقع الجغرافي

دعونا نوضح أن الحصول على الموافقة لا يعفي مراقب البيانات من التزام التناسب وبالتالي من الموازنة بين مصالح مراقب البيانات من جهة، ومصالح صاحب البيانات من جهة أخرى[١].

كذلك فإن الإشارة إلى أنه ستتم معالجة البيانات على أساس الموافقة عندما تعتمد المعالجة على أساس قانوني آخر، فسيكون غير عادل بشكل أساسي لأصحاب البيانات.

بعبارة أخرى لا يمكن لمراقب البيانات الانتقال من الموافقة إلى أساس قانوني آخر. فعلى سبيل المثال لا يُسمح باستخدام الأساس القانوني للمصالح المشروعة بأثر رجعي لتبرير المعالجة عند مواجهة مشاكل تتعلق بصحة الموافقة ؛ نظرًا لأن مراقبي البيانات ملزمون بالإبلاغ عن الأساس القانوني الذي يعتمدون عليه في وقت جمع البيانات. فيجب عليهم تحديد أساسهم القانوني قبل الجمع المذكور[٢].

شروط الموافقة على معالجة بيانات الموقع الجغرافي :

سنناقش الالتزام الذي يقع على عاتق مراقب البيانات ؛ ليكون قادرًا على إثبات في أي وقت أن موافقة الشخص المعني على معالجة بيانات تحديد موقعه الجغرافي قد تم منحها بالفعل وأنها صالحة بموجب القانون.

---

[1] - De Terwangne, op. cit. p.42.

[2] - Lignes directrices 5/2020 sur le consentement au sens du règlement (UE) 2016/679 , Version 1.1 Adoptées le 4 mai 2020 p.29

أولا : الموافقة الحرة

إن شرط الموافقة الحرة قديم قدم القوانين تقريبًا ويعني أنه لا يجب أن يتم تقديمه تحت التهديد أو الإكراه. وبعبارة أخرى، "بشكل مستقل عن أي ضغط، اقتصادي ، أو معنوي ، يمارسه طرف ثالث"[١].

يلتزم مراقب البيانات في بعض الحالات، بالحصول على "موافقة الشخص المعني على معالجة معلوماته".

يجب أن تأتي الموافقة من اختيار حقيقي للشخص المعني، ويجب ألا يكون قد تعرض لأي إكراه. لذلك لن تعتبر الموافقة صحيحة إذا تعرض صاحب البيانات ، من خلال عدم الموافقة على معالجة بياناته ، لعواقب سلبية[٢] ، حيث يجب أن يكون صاحب البيانات قادرا على رفض موافقته ، أو سحبها دون التعرض لأي عواقب[٣].

فيما يتعلق برفض الشخص المعني ، فإن الموافقة لا يمكن وصفها بأنها مجانية وحرة إذا "تم تقديمها كجزء من الشروط العامة غير قابل للتفاوض ، وتعتبر غير ممنوحة بحرية، ويكون معيار تحديد ما إذا كانت الموافقة تُمنح بحرية أم لا، هو مراعاة الوضع المحدد المتمثل في دمج الموافقة في العقد ، أو ربطها بتقديم خدمة[٤].

---

[1] - Komur, Neslin, op cit p.58.

[2] - Groupe de l'article 29, « Lignes directrices sur le consentement au sens du règlement (UE) 2016/679 » WP 259 rev.01, p. 6.

[٣] .a - Considérant 42 du RGPD.

[4] - Lignes directrices 5/2020 sur le consentement au sens du règlement (UE) 2016/679 , op cit p.8.

٩- الجوانب القانونية لتقنية تحديد الموقع الجغرافي

يتضح هذا الشرط في قرار هيئة حماية البيانات بمعاقبة أحد التجار ، والمتعلق باستخدام العملاء لبطاقة الهوية كبطاقة للولاء والتخفيضات ، وفي هذه الحالة، لم يقدم التاجر أي بديل آخر للعملاء للحصول على بطاقة الولاء. فالشخص الذي يرفض الموافقة على نقل بياناته الشخصية من خلال قراءة بطاقة هويته ، لن يتمكن بالتالي من الاستفادة من بطاقة الولاء ، وبالتالي التخفيض[١].

كذلك عندما يطلب أحد تطبيقات تحرير الصور على الهاتف المحمول من مستخدميه تنشيط موقع GPS الخاص بهم ؛ من أجل استخدام خدماته ، كما يخبر التطبيق مستخدميه أنه سيستخدم البيانات التي تم جمعها لأغراض إعلانية سلوكية.

في هذه الحالة لا يعد تحديد الموقع الجغرافي ، أو الإعلان السلوكي عبر الإنترنت ضروريًا لتوفير خدمات تحرير الصور، وبالتالي يتجاوز كلاهما توفير الخدمة الأساسية المقدمة ، وبما أنه لا يمكن للمستخدمين استخدام التطبيق دون الموافقة على هذه الأغراض، فلا يمكن اعتبار الموافقة ممنوحة بحرية[٢].

---

[1] - Charlotte SIKIVIE,op cit p.22.- Article 29 Working Party Guidelines on consent under Regulation 2016/679 Adopted on 28 November 2017 As last Revised and Adopted on 10 April 2018
Groupe de l'article 29, « Lignes directrices sur le consentement au sens du règlement (UE) 2016/679 » WP 259 rev.01, p. 6.
A.P.D. (ch. contentieuse), decision 06/2019 du17 septembre 2019, https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/BETG06_2019ANO

[2] - Lignes directrices 5/2020 sur le consentement au sens du règlement (UE) 2016/679 , op cit p.8

أخيرًا، وهذه النقطة تمثل إشكالية بشكل خاص، يجب أن يكون هناك توازن معين بين الطرفين (مراقب البيانات وصاحب البيانات) ؛ لذلك لا ينبغي أن تشكل الموافقة أساسًا قانونيًا صالحًا لمعالجة البيانات الشخصية في حالة معينة حيث يوجد خلل واضح بين صاحب البيانات والمراقب ، على وجه الخصوص عندما يكون المراقب سلطة عامة ومن غير المرجح أن يتم منح الموافقة بحرية في ضوء جميع الظروف الخاصة بهذا الموقف بالذات[1].

في علاقة العمل يمكننا بطبيعة الحال أن نتساءل عما إذا كانت موافقة العامل على معالجة بياناته من قبل صاحب العمل تعتبر صالحة وحرة ؟.

الواقع أن الموافقة كأساس مشروع للمعالجة تعتبر مشكلة في السياق المهني ، وقد كتب فريق عمل المادة ٢٩ في رأيه بشأن معالجة البيانات الشخصية في السياق المهني: "إذا كانت موافقة العامل ضرورية وكان عدم الموافقة قد يؤدي إلى ضرر فعلي ، أو محتمل للعامل ، فإن الموافقة غير صالحة إلى الحد الذي لا يتم منحه بحرية. فإذا لم تتاح للعامل فرصة الرفض، فهذه ليست موافقة. (...) كما قد يكون هناك حجر عثرة إذا كانت الموافقة شرطًا للتوظيف.

يمكن للعامل من الناحية النظرية أن يرفض إعطاء الموافقة ، لكنه قد يفقد بعد ذلك فرصة العمل. وفي هذه الظروف فإن عدم منح الموافقة بحرية لا يكون صحيحًا.

[1] - Considérant 42 du RGPD

٩- الجوانب القانونية لتقنية تحديد الموقع الجغرافي

لذلك بدلاً من طلب الموافقة يجب على أصحاب العمل النظر فيما إذا كان من الممكن إثبات أن هناك حاجة لرصد الموقع الدقيق للعمال لغرض مشروع وموازنة هذه الحاجة مع الحقوق والحريات الأساسية للعمال.

في حالة تبرير الضرورة على النحو الواجب يمكن أن يستند الأساس القانوني لهذه المعالجة إلى المصلحة المشروعة للمراقب[١].

تدرك مجموعة الـ ٢٩ أن الموافقة الممنوحة في السياق المهني هشة للغاية ولكنها تجيزها شريطة وجود ضمانات كافية بأن الموافقة حرة حقًا. بالتالي، لا يتم استبعاد الموافقة كأساس قانوني لمعالجة البيانات في هذا السياق بالذات[٢]، حيث يكون هناك حالات يكون فيها صاحب العمل قادرًا على إثبات أن موافقة العامل تُمنح بحرية بحكم الواقع ، بخاصة عندما لا تنجم أي عواقب سلبية على الإطلاق عن رفض العامل إعطاء الموافقة[٣].

بخصوص معالجة تحديد الموقع الجغرافي للأطفال في الأحوال التي تستلزم ذلك فيجب الحصول على موافقة الأطفال أنفسهم ، أو من قبل الوالدين ، أو غيرهم من الممثلين القانونيين.

---

[1]- ARTICLE 29 Data Protection Working Party,Opinion 13/2011 on Geolocation services on smart mobile devices, Adopted on 16 May 2011, p.14.

[2] - Groupe de l'article 29, « Avis n°15/2011 sur la définition du consentement », WP 187, p. 16

[3] - Manuel de droit européen en matière de protection des données Édition 2018,Agence des droits fondamentaux de l'Union européenne et Conseil de l'Europe, 2019 p.10.

يحدد القانون العام لحماية البيانات مستوى إضافيًا من الحماية عند معالجة البيانات الشخصية للأشخاص الضعفاء ، ولا سيما الأطفال، وتقدم المادة الثامنة التزامات إضافية ؛ لضمان مستوى أفضل من حماية البيانات الشخصية للأطفال فيما يتعلق بخدمات مجتمع المعلومات.

تم تحديد أسباب هذه الحماية المحسنة في الحيثية ٣٨ من اللائحة العامة لحماية البيانات الشخصية (RGPD) والتي تنص على أنه " يستحق الأطفال حماية خاصة فيما يتعلق ببياناتهم الشخصية ؛ لأنهم قد يكونون أقل وعيًا بالمخاطر، والعواقب ، والضمانات المعنية ، وحقوقهم المتعلقة بمعالجة البيانات الشخصية ، وينبغي أن تنطبق هذه الحماية المحددة، على وجه الخصوص، على استخدام البيانات الشخصية المتعلقة بالأطفال لأغراض التسويق ، أو إنشاء ملفات تعريف الشخصية ، أو المستخدمين ، وجمع البيانات الشخصية المتعلقة بالأطفال عند استخدام الخدمات المقدمة مباشرة إلى الطفل. لا ينبغي أن تكون موافقة صاحب المسؤولية الأبوية ضرورية في سياق خدمات الوقاية ، أو الاستشارة المقدمة مباشرة للطفل"[١].

تشير كلمة على وجه الخصوص إلى أن هذه الحماية المحددة لا تقتصر فقط على التسويق ، أو التنميط، ولكنها تشمل "جمع البيانات الشخصية المتعلقة بالأطفال" بالمعنى الواسع[٢].

[1] - considérant 38 du RGPD

[2] - Lignes directrices 5/2020 sur le consentement au sens du règlement (UE) 2016/679 , op cit p.30.

٩- الجوانب القانونية لتقنية تحديد الموقع الجغرافي

تنص المادة ٨ (١) على أنه في حالة تطبيق الموافقة فيما يتعلق بتقديم خدمات مجتمع المعلومات للأطفال بشكل مباشر، تكون معالجة البيانات الشخصية المتعلقة بالطفل قانونية عندما يبلغ عمر الطفل ١٦ عامًا على الأقل.

عندما يكون عمر الطفل أقل من ١٦ عامًا تكون هذه المعالجة قانونية فقط إذا تم منح الموافقة ، أو التصريح بها من قبل صاحب المسؤولية الأبوية للطفل.

يتسم القانون العام لحماية البيانات بالمرونة فيما يتعلق بالحد الأدنى لسن الموافقة الصحيحة ، حيث يجيز للدول الأعضاء أن تنص بموجب القانون على سن أقل، ولكن لا يمكن أن تكون في جميع الأحوال أقل من ١٣ عامًا .

وهذا يعني، على سبيل المثال، أنه يجب على مقدم تطبيق تحديد الموقع الجغرافي عند تقييم الجمهور المستهدف بخدماته ، وبخاصة الأطفال ، أن يكون على دراية بالقوانين الوطنية المختلفة ، وأن يبذل جهودا معقولة للتحقق من أن المستخدم فوق الحد الأدنى لسن الموافقة الرقمية ، و أن تكون هذه الجهود متناسبة مع طبيعة أنشطة المعالجة والمخاطر المرتبطة بها[1].

كما يجب عليه إخطار أولياء الأمور بجمع واستخدام بيانات تحديد الموقع الجغرافي عن أطفالهم والحصول على موافقتهم قبل جمع واستخدام المعلومات المتعلقة بأطفالهم لاحقًا.

[1] - Lignes directrices 5/2020 sur le consentement au sens du règlement (UE) 2016/679 , op cit p.31-32.

هذا وقد تم تصميم بعض تطبيقات تحديد الموقع الجغرافي خصيصًا للمراقبة الأبوية، على سبيل المثال من خلال الكشف بشكل دائم عن موقع الجهاز على موقع ويب ، أو عن طريق إصدار تنبيه إذا غادر الجهاز منطقة محددة مسبقًا. استخدام مثل هذه التطبيقات يمثل مشكلة.

لا ينبغي أبدًا أن يتعرض الأطفال لأسباب أمنية لمراقبة مفرطة تحد من استقلاليتهم. وفي هذا السياق لا بد من تحقيق التوازن بين حماية خصوصية الأطفال وسلامتهم.

ينص الإطار القانوني على أن الآباء مسؤولون عن حماية حق أطفالهم في الخصوصية. على أقل تقدير، إذا كان الآباء يعتقدون أن استخدام مثل هذا التطبيق له ما يبرره في ظروف معينة ، فيجب إبلاغ الأطفال بذلك ، ويجب أن يكونوا قادرين على المشاركة، في أقرب وقت ممكن بشكل معقول ، في قرار استخدام مثل هذا التطبيق[١].

ثانيا : الموافقة الصريحة والمحددة.

يجب أن تكون موافقة صاحب البيانات على معالجة بيانات تحديد الموقع الخاص به موافقة صريحة. بالتالي لا ينبغي أن يشكل صمت المستخدم قبولًا لوحدة التحكم في البيانات ، وإذا لم يتقدم المستخدم بمحض إرادته، فلا ينبغي اعتبار الموافقة ممنوحة[٢].

[1] - Groupe Article 29 Avis n°13/2011 du 16 mai 2011op cit. p.15 - ARTICLE 29 DATA PROTECTION WORKING PARTY,Opinion 2/2009 on the protection of children's personal data (General Guidelines and the special case of schools) Adopted on 11 February 2009.

[2] - M. Henri BarbIerk, op cit p.29. .

٩- الجوانب القانونية لتقنية تحديد الموقع الجغرافي

بخصوص الاعتماد على نوع التكنولوجيا المستخدمة ، قد يلعب جهاز المستخدم دورًا نشطًا نسبيًا في معالجة بيانات تحديد الموقع الجغرافي.

قد يكون الجهاز قادرًا على نقل بيانات الموقع من مصادر مختلفة إلى الغير، ووجود هذه القدرة التقنية لا يعني أن معالجة البيانات قانونية تلقائيًا ، وفي حالة ما إذا كانت الإعدادات الافتراضية لنظام التشغيل تسمح بنقل بيانات الموقع ، فلا ينبغي اعتبار عدم التدخل من جانب المستخدمين بمثابة موافقة حرة ، وصريحة من المستخدمين[١].

على الرغم من أهمية وجود سياسة خصوصية بسيطة وشاملة إلا أن الحصول على موافقة علنية مستنيرة في عصر تطبيقات الأجهزة المحمولة غالبًا ما يتطلب أكثر من مجرد نشر هذه السياسة على موقع الويب الخاص بالتطبيق ، وافتراض أن مستخدميه سيقرؤونها . حيث إنه من النادر أن يأخذ المستخدمون الوقت الكافي لقراءة سياسة الخصوصية.

يتمثل التحدي في أن نوضح للمستخدمين بطريقة إبداعية ومفهومة الغرض الحقيقي من استخدام معلوماتهم الشخصية. حيث إنه وبشكل عام لا أحد يريد قراءة عشرون صفحة من سياسات الخصوصية على شاشة صغيرة[٢].

في فرنسا قررت لجنة حماية البيانات الشخصية (CVPC) في شكوى ضد Google أن التفويض البسيط في حد ذاته لا يشكل موافقة على جمع المعلومات الشخصية

---

[1] - Groupe Article 29 Avis n°13/2011 du 16 mai 2011op cit. p.14

[2] - Vincent Bergeron et Thomas Gagnon -van Leeuwen op cit. p.33.

واستخدامها والكشف عنها ؛ لأن "التفويضات لا تصف جمع المعلومات الشخصية ، أو استخدامها ، أو الكشف عنها بواسطة Google". بل تشير بدلاً من ذلك إلى بيانات ووظائف الجهاز المحمول الذي يُسمح للتطبيق بالاطلاع عليه"[١].

علاوة على ذلك قد يؤدي رفض الوصول إلى خدمات تحديد الموقع الجغرافي في بعض الحالات إلى إعطاء المستخدم انطباعًا خاطئًا بأن التطبيق لا يجمع بيانات تحديد الموقع الجغرافي. فعلى سبيل المثال، تحدد Uber في سياسة الخصوصية الخاصة بها أنه يتم جمع بيانات الموقع الدقيقة للرحلات التي يتم إجراؤها من الجهاز المحمول للسائق حتى لو رفض العميل السماح لتطبيق Uber بالوصول إلى خدمات الموقع الخاصة به[٢].

كذلك فإن اللائحة العامة لحماية البيانات تنص على أن الموافقة يجب أن تكون لا لبس فيها وبالتالي لا يمكن أن تكون هناك موافقة في حالة الصمت أو تحديد المربعات بشكل افتراضي أو في حالة عدم النشاط ، وينطوي هذا الشرط على ضرورة وجود عمل إيجابي واضح من جانب الشخص المعني[٣].

---

[1] - Rapport de conclusions en vertu de la LPRPDE no 2014-008: Le fait qu'un utilisateur accorde des« autorisations » à une application ne signifie pas, en soi, qu'il consent à la collecte, à l'utilisation et à la communication de renseignements personnels – Nous encourageons Google à donner plus de précisions aux utilisateurs pour éviter toute interprétation erronée, 2014 CanLII 77274 (CVPC) au para 68.

[2] - Uber, « Déclaration de confidentialité applicable aux utilisateurs » (en vigueur le 15 juillet 2015),
en ligne : <https://www.uber.com/legal/privacy-proposed/users/fr>.

[3] - Considérant 32 du R.G.P.D

وتضيف مجموعة ال٢٩ أن " صمت الشخص المعني ، أو عدم نشاطه فضلاً عن مجرد استمراره في استخدام الخدمة ، لا يمكن اعتباره مؤشراً نشطاً على الاختيار"[١]. ومع ذلك وفقًا لإرشادات مجموعة الـ ٢٩، لا يمكن اعتبار الموافقة قد تم الحصول عليها بشكل صحيح إذا تم منحها عن طريق نفس الإجراء كما هو الحال عندما يقبل صاحب البيانات عقدًا ، أو الشروط العامة للخدمة.

لذلك، يجب على الأشخاص المتأثرين بأجهزة تحديد الموقع الجغرافي التعبير عن موافقتهم الصريحة بشكل فردي ، وكتابي قبل تنفيذ المعالجة.

مبدأ الموافقة المسبقة والصريحة منصوصا علية في قانون الاتصالات البريدية والإلكترونية الفرنسي (CPCE) ، والذى قرر أنه يجب على الأشخاص المتأثرين بأجهزة تحديد الموقع الجغرافي التعبير عن موافقتهم الصريحة[٢].

على هذا النحو توصي CNIL بأن تتم الموافقة بشكل فردي وكتابي قبل تنفيذ المعالجة مع ضرورة إرفاق مستند محدد بالعقد ، أو بند تعاقدي قياسي مدرج في العقد، يشير إلى أن توقيع العميل يشكل موافقة على تنفيذ معالجة تحديد الموقع الجغرافي[٣].

[1] - Groupe de l'article 29, « Lignes directrices sur le consentement au sens du règlement (UE) 2016/679 » WP 259 rev.01, p. 18
[2] - Art.34/1-4 (CPCE)
[3] - CNIL Délibération n° 2010-096 du 8 avril 2010

كما لا يجوز استخدام هذه البيانات التي تتيح تحديد موقع المعدات الطرفية للمستخدم أثناء الاتصال لأغراض أخرى غير التي وافق عليها ، ولا يمكن الاحتفاظ بها ومعالجتها بعد اكتمال الاتصال إلا بموافقة المشترك فقط مع علمه بفئات البيانات المعنية ، ومدة المعالجة ، وأغراضها ، وما إذا كان سيتم نقل هذه البيانات إلى مقدمي خدمات آخرين أم لا[١].

لن تكون الموافقة صحيحة إلا إذا كانت محددة ، أي أعطيت "لواحد أو أكثر من الأغراض المحددة"[٢].

"الموافقة العامة دون تحديد الغرض من معالجة البيانات بشكل دقيق غير مقبولة ، حيث يجب طلب الموافقة لسبب محدد ، و لا يمكن طلب موافقة عامة مرة واحدة فقط ، فإذا ما تم تعديل جانب مهم يتعلق بجمع المعلومات الشخصية ، واستخدامها وإبلاغها بعد موافقة المستخدم ، فيجب على الشركة إخطاره بالتغيير ، والحصول على موافقته مرة أخرى[٣]. فعلى سبيل المثال إذا كان مراقب البيانات يرغب في تعديل المعالجة الأولية للبيانات الشخصية، عن طريق نقل هذه البيانات إلى مزود خدمة جديد لتحديد الموقع الجغرافي ، فيحب عليه الحصول على موافقة جديدة بذلك النقل[٤].

[1] - Art.34/1-5 du (CPCE)
[2] - Groupe de l’article 29, « Lignes directrices sur le consentement au sens du règlement (UE) 2016/679 » WP 259 rev.01, p. 13
[3] - Vincent Bergeron et Thomas Gagnon -van Leeuwen op cit. p.35..
[4] - M. Henri BarbIerk, op cit p.29..

٩- الجوانب القانونية لتقنية تحديد الموقع الجغرافي

كذلك إذا كان التطبيق ينوي الوصول إلى قائمة جهات الاتصال الخاصة بالهاتف المحمول الخاص بالمستخدم فيجب أن يكون هناك خيار للمستخدم لتحديد جهات اتصال معينة ينوي التواصل معها ، أو مشاركة موقعها[١].

علاوة على ذلك في حالة أن المعالجة تسعى إلى أكثر من غرض واحد ، يجب أن يكون صاحب البيانات قادرًا على الموافقة على بعضها ، وليس على البعض الآخر[٢].

كما أوصي فريق عمل المادة ٢٩ بأن يسعى مقدمو التطبيقات أو الخدمات المستندة إلى الموقع إلى الحصول على موافقة الشخص مرة أخرى (حتى في حالة عدم إجراء أي تغيير على طبيعة المعالجة) بعد فترة زمنية مناسبة. فعلى سبيل المثال قد يكون من المناسب التوقف عن معالجة بيانات الموقع إذا لم يستخدم الشخص الخدمة بشكل نشط خلال آخر ١٢ شهرًا. حتى في حالة استخدام الخدمة، يجب التذكير بطبيعة معالجة بياناتهم الشخصية مرة واحدة على الأقل سنويًا أو في كثير من الأحيان إذا كانت طبيعة المعالجة تبرر ذلك[٣].

كذلك فإن مراقب البيانات مقيد بما هو أبعد من الموافقة حتى أننا نجده مقيدا عند الحصول على موافقة حرة ومستنيرة من المستخدمين ، فلا يتمتع مطورو تطبيقات الهاتف المحمول بتفويض مطلق لجمع المعلومات الشخصية ، أو استخدامها أو،

---

[1] - Bu-Pasha, Shakila & Alén, Anette & Mäkinen, J. & Guinness, Robert & Korpisaari, Päivi. (2016).op cit p.321.- Groupe Article 29 Avis n°13/2011 du 16 mai 2011op cit. p.15.

[2]- Charlotte SIKIVIE,op cit p.29.

[3]- Groupe Article 29 Avis n°13/2011 du 16 mai 2011op cit. p.53

توصيلها على النحو الذي يرونه مناسبًا. فعلى الرغم من الموافقة الحرة ، والمستنيرة للمستخدمين، إلا أنهم يمكنهم فقط "جمع المعلومات الشخصية ، أو استخدامها ، أو توصيلها للأغراض التي يعتبرها شخص عاقل مقبولة في هذه الظروف[١].

ثالثا : الموافقة المستنيرة

يعزز القانون العام لحماية البيانات شرط أن تكون الموافقة مستنيرة. وفقًا للمادة ٥ من اللائحة العامة لحماية البيانات، فإن متطلبات الشفافية، المرتبطة ارتباطًا وثيقًا بمبادئ الولاء والمشروعية، هي أحد مبادئها الأساسية.

يعد توفير المعلومات لأصحاب البيانات قبل الحصول على الموافقة أمرًا ضروريًا ؛ لتمكينهم من اتخاذ قرارات مستنيرة وفهم ما يوافقون عليه.

على سبيل المثال، ممارسة حقهم في سحب الموافقة إذا لم يوفر مراقب البيانات معلومات يمكن الوصول إليها، حيث يصبح تحكم المستخدم وهميًا ولن تشكل الموافقة أساسًا صالحًا للمعالجة[٢].

ترتبط صحة الموافقة بقوة وجودة وكفاية المعلومات المقدمة من مراقب البيانات للمستخدمين فيما يتعلق بالمعالجة ؛ وذلك حتى يتمكن صاحب بيانات الموقع الجغرافي من حسب تأثير اختياراته[٣].

---

[1] - Vincent Bergeron et Thomas Gagnon -van Leeuwen op cit. p.35...

[2] – Lignes directrices 5/2020 sur le consentement au sens du règlement (UE) 2016/679 , op cit p.17.

[3]- CNIL.Projet de recommandation Relative aux applications mobiles, Version soumise à consultation publique jusqu'au 8 octobre 2023 p.77.

٩- الجوانب القانونية لتقنية تحديد الموقع الجغرافي

عند طلب الموافقة ينبغي لمراقبي البيانات التأكد من أنهم يستخدمون بشكل منهجي مصطلحات واضحة وبسيطة وهذا يعني أن الرسالة يجب أن تكون سهلة الفهم لرجل الشارع وليس للقانونين فقط . فلا يمكن لمراقبي البيانات استخدام سياسات خصوصية طويلة يصعب فهمها ، أو بيانات مليئة بالجوانب القانونية[١].

يجب أن تكون الموافقة واضحة مقدمة بشكل مفهوم ويمكن تمييزها عن المسائل الأخرى يمكن الوصول إليه بسهولة ، ويعني هذا الشرط أساسًا أنه لا يمكن إخفاء المعلومات اللازمة لاتخاذ قرارات مستنيرة فيما يتعلق بالموافقة في الشروط والأحكام[٢].

تكون موافقة الطرف المعني صالحة فقط إذا كان من المعقول توقع أن يفهم الفرد المستهدف بأنشطة المنظمة طبيعة ، وأغراض ، وعواقب جمع ، أو استخدام ، أو إرسال المعلومات الشخصية التي تمت الموافقة على معالجتها[٣].

يتطلب قانون الاتحاد الأوروبي أن تتم معالجة البيانات الشخصية "بطريقة تتسم بالشفافية بالنسبة لصاحب البيانات"[٤].

---

[١] – يجب أن تكون المعلومات واضحة وشاملة ومفهومة لجمهور كبير وغير مطلع، ويمكن الوصول إليها بسهولة وبشكل دائم.

Groupe Article 29 Avis n°13/2011 du 16 mai 2011op cit. p.17.

[2] - Lignes directrices 5/2020 sur le consentement au sens du règlement (UE) 2016/679 , op cit p.18.

[3] - Vincent Bergeron et Thomas Gagnon -van Leeuwen op cit. p.31..

[4] - Manuel de droit européen en matière de protection des données Édition 2018,op cit p.134.

يفرض هذا المبدأ على مراقب البيانات الالتزام باتخاذ جميع التدابير المناسبة لتزويد أصحاب البيانات – الذين قد يكونون مستخدمين ، أو عملاء – بمعلومات حول كيفية استخدام بياناتهم[١].

يمكن أن تشير الشفافية إلى المعلومات المقدمة للشخص قبل بدء المعالجة [٢] وإلى المعلومات التي ينبغي أن يكون من السهل الوصول إليها لأصحاب البيانات أثناء المعالجة [٣]، و أيضًا إلى المعلومات المقدمة لأصحاب البيانات بعد طلب الوصول إلى البيانات المتعلقة بهم[٤].

لكي تكون الموافقة صحيحة يجب أن يحصل الشخص المعني على جميع المعلومات التي يحتاجها بعبارات واضحة وبسيطة ومفهومة. كما يجب على مراقب البيانات تقييم نوع الجمهور الذي يقدم البيانات الشخصية لمؤسسته حتى يتمكن من إعطاء الموافقة المستنيرة[٥]..

يجب أن تكون اللغة المستخدمة مناسبة للمستلمين. حيث يختلف مستوى ونوع اللغة المستخدمة اعتمادًا على ما إذا كان الجمهور المستهدف بالغًا ، أو طفلًا، من عامة

[1] - art. 12du RGPD.
[2] - art. 13 et 14.du RGPD.
[3] - Groupe de travail « Article 29 », Avis 2/2017 sur le traitement des données au travail, p. 23.
[4] - RGPD, art. 15.
[5] - Groupe de l'article 29, « Lignes directrices sur le consentement au sens du règlement (UE) 2016/679 » WP 259 rev.01, p. 14 - C p.31 - A p.30

الناس أو خبيرًا أكاديميًا[١]. فعلى سبيل المثال إذا كان الجمهور المستهدف يضم قاصرين ، فيجب على مراقب البيانات التأكد من أن المعلومات مفهومة لهم[٢].

أيد فريق عمل المادة ٢٩ فكرة الإعلانات المقدمة في شكل متعدد الطبقات ؛ مما يسمح للشخص المعني بتحديد مستوى التفاصيل التي يفضلها[٣].

يجب شرح المعالجة للأشخاص المعنيين بشكل استباقي بطريقة يسهل الوصول إليها ؛ لضمان فهمهم لما سيحدث لبياناتهم ، وهذا يعني أن صاحب البيانات يجب أن يعرف الغرض المحدد من معالجة البيانات الشخصية عند جمع البيانات المتعلقة به.

تتطلب شفافية المعالجة استخدام مصطلحات واضحة ، وبسيطة ، بحيث يكون أصحاب البيانات على علم بوضوح بالمخاطر ، والقواعد ، والضمانات ، والحقوق المرتبطة بمعالجة بياناتهم الشخصية[٤].

وضعت مجموعة ال٢٩ في مبادئها التوجيهية قائمة بالمعلومات التي تعتبرها ضرورية[٥]. من بينها هوية مراقب البيانات[١] والغرض[٢] وأنواع البيانات[٣] ووجود الحق في سحب الموافقة[٤] وما إلى ذلك.

---

[1] - Manuel de droit européen en matière de protection des données Édition 2018,op cit p.238.

[2] - Lignes directrices 5/2020 sur le consentement au sens du règlement (UE) 2016/679 , op cit p.19..

[3] - Groupe de travail « Article 29 » (2004), Avis 10/2004 sur les « Dispositions davantage harmonisée en matière 'informations », WP 100, Bruxelles, 25 novembre 2004

[4] - Manuel de droit européen en matière de protection des données Édition 2018,op cit p.135.

[5] - Groupe de l'article 29, « Lignes directrices sur le consentement au sens du règlement (UE) 2016/679 » WP 259 rev.01, p. 15.

كذلك فإنه وفقا للمادة ٤٢ من اللائحة العامة لحماية البيانات إذا تم طلب الموافقة في سياق إعلان مكتوب يتعلق بمسألة أخرى (على سبيل المثال، كما هو الحال غالبًا، قبول الشروط العامة) في مثل هذه الحالة فمن المناسب التأكد من أن الشخص المعني على علم بالموافقة الممنوحة ونطاقها، وبعبارة أخرى يجب تمييز الموافقة بوضوح بين جميع المعلومات[٥].

لم تحدد اللائحة العامة لحماية البيانات الشكل الذي يجب تقديم المعلومات به من أجل تلبية متطلبات الموافقة المستنيرة ، وهذا يعني أنه يمكن تقديم المعلومات القيمة بعدة طرق، على سبيل المثال في شكل اتصالات مكتوبة ، أو شفهية ، أو رسائل صوتية ، أو فيديو[٦].

رابعا : القدرة على اثبات الموافقة

تنص المادة السابعة ، الفقرة ١ من اللائحة العام لحماية البيانات (R.G.P.D) على أن مراقب البيانات يجب أن يكون "قادرًا على إثبات أن صاحب البيانات قد أعطى موافقته على معالجة البيانات الشخصية المتعلقة به".

[1]- Considérant 42 du R.G.P.D.
[2]- Considérant 42 du R.G.P.D.
[3] - Groupe de l'article 29, « Avis n°15/2011 sur la définition du consentement », WP 187, p. 21 à 22
[4] - R.G.P.D Art. 7, § 3.
[5] - Charlotte SIKIVIE,op cit p.29.
[6] - Lignes directrices 5/2020 sur le consentement au sens du règlement (UE) 2016/679 , op cit p.18.

كما تنص الحيثية ٤٢ من ذات اللائحة على أنه "حيثما تعتمد المعالجة على موافقة صاحب البيانات، يجب أن يكون المراقب قادرًا على إثبات أن صاحب البيانات قد وافق على عملية المعالجة."

يتمتع مراقبو البيانات بالحرية في تطوير أساليب تتكيف مع عملياتهم اليومية ؛ للامتثال لهذا الحكم. في الوقت نفسه، لا ينبغي أن يؤدي التزام المراقب بإثبات أنه تم الحصول على الموافقة الصحيحة إلى زيادة أحجام المعالجة الإضافية المفرطة ، وهذا يعني أن مراقبي البيانات يجب أن يكون لديهم ما يكفي من البيانات لإنشاء رابط للمعالجة ؛ لإثبات أنه تم الحصول على الموافقة ، ولكن لا ينبغي لهم جمع معلومات أكثر من اللازم.

يقع على عاتق المراقب مسؤولية إثبات أنه تم الحصول على موافقة صالحة من صاحب البيانات . لم تصف اللائحة العامة لحماية البيانات (GDPR) بدقة كيفية القيام بذلك ، ومع ذلك يجب أن يكون مراقب البيانات قادرًا على إثبات أن صاحب البيانات قد أعطى الموافقة في حالة معينة.

ينطبق الالتزام بإظهار الموافقة طالما استمر نشاط المعالجة المعني ، وبمجرد اكتمال نشاط المعالجة ، لا ينبغي الاحتفاظ بإثبات الموافقة لفترة أطول من اللازم تمامًا للامتثال لالتزام قانوني ، أو لإنشاء مطالبات قانونية ، أو ممارستها ، أو الدفاع عنها وفقًا للمادة ١٧ (٣) (ب) و (هـ).

يجوز لمراقب البيانات على سبيل المثال الاحتفاظ بسجل لإعلانات الموافقة المستلمة ؛ حتى يتمكن من إثبات كيفية الحصول على الموافقة ، ومتى تم الحصول عليها ، وما هي المعلومات المقدمة إلى صاحب البيانات في ذلك الوقت.

كما يجب أن يكون مراقب البيانات قادرًا على إثبات أن صاحب البيانات قد تم إبلاغه وأن سير العمل يتوافق مع جميع المعايير ذات الصلة للحصول على موافقة صالحة. السبب وراء هذا الالتزام الذي حددته اللائحة العامة لحماية البيانات هو أن مراقبي البيانات يجب أن يكونوا مسؤولين عن الحصول على موافقة صالحة من أصحاب البيانات وعن آليات الموافقة التي أنشأوها[1].

لم تحدد اللائحة العامة لحماية البيانات مدة محددة تظل الموافقة سارية خلالها. تعتمد مدة صلاحية الموافقة على السياق ، ونطاق الموافقة الأولية ، وتوقعات الشخص المعني. إذا تغيرت عمليات المعالجة ، أو تطورت بشكل كبير، فإن الموافقة المبدئية لم تعد صالحة ، وفي هذه الحالة يجب الحصول على موافقة جديدة.

خامسا : سحب الموافقة.

تولي اللائحة العامة لحماية البيانات مكانة مهمة لسحب الموافقة. يمكن اعتبار أحكام واعتبارات اللائحة العامة لحماية البيانات بشأن سحب الموافقة بمثابة تدوين للتفسير الحالي لهذا الموضوع في آراء مجموعة عمل المادة ٢٩[2].

[1] - Lignes directrices 5/2020 sur le consentement au sens du règlement (UE) 2016/679 , op cit p.26

[2] - l’avis 15/2011 sur la définition du consentement (WP 187), p. 10, 14-15, 22, 31 et 37-38] et, entre autres, dans son avis sur l’utilisation de données de

بموجب أحكام المادة السابعة ، الفقرة ٣ من اللائحة العامة لحماية البيانات "يحق لصاحب البيانات سحب الموافقة في أي وقت" ؛ وينتج هذا عن حقيقة أن صاحب البيانات يجب أن يتحكم في بياناته الشخصية.

يجب إبلاغ صاحب البيانات بهذا الحق قبل إعطاء الموافقة ، كما لا يكون للانسحاب أثرا رجعيا. لكن لاحظ أن هذه النقطة يجب أن تكون مؤهلة بحق الشخص المعني في محو البيانات المتعلقة به.

تنص المادة السابعة، فقرة (٣) من اللائحة العامة لحماية البيانات على أنه يجب على المراقب التأكد من سهولة سحب البيانات الخاضعة للموافقة ، وامكانية القيام بذلك في أي وقت. لا ينص القانون العام لحماية البيانات على أن صاحب البيانات يجب أن يكون قادرًا دائمًا على منح الموافقة وسحبها من خلال نفس الإجراء ، ومع ذلك، عندما يتم الحصول على الموافقة إلكترونيًا فقط عن طريق النقر أو التمرير، ينبغي أن يكون أصحاب البيانات قادرين، من الناحية العملية، على سحب الموافقة بنفس الوسائل.

عندما يتم الحصول على الموافقة من خلال واجهة مستخدم (على سبيل المثال من خلال موقع ويب أو تطبيق أو حساب تسجيل دخول أو واجهة جهاز إنترنت الأشياء أو عبر البريد الإلكتروني) فمن الواضح أن صاحب البيانات يجب أن يكون قادرًا على

localization - l'avis 5/2005 sur l'utilisation de données de localisation aux fins de fourniture de services à valeur ajoutée (WP 115), p. 7

سحب الموافقة من خلال نفس البوابة الإلكترونية (الواجهة) ؛ نظرًا لأن تغيير الواجهات لغرض وحيد هو سحب الموافقة سيتطلب جهدًا غير ضروري[١].

يجب أن يكون صاحب البيانات قادرًا أيضًا على سحب الموافقة دون التعرض لأي ضرر[٢]. وهذا يعني، من بين أمور أخرى، أن مراقب البيانات يجب أن يوفر إمكانية سحب الموافقة مجانًا ، أو دون أن يؤدي ذلك إلى أي تأثير سلبى على استخدام أجهزته[٣] ، أو أي انخفاض في مستوى الخدمة[٤].

كقاعدة عامة، في حالة سحب الموافقة، تظل جميع عمليات معالجة البيانات بناءً على الموافقة التي تمت قبل سحب الموافقة – والامتثال للائحة العامة لحماية البيانات – قانونية ، ولكن يجب على مراقب البيانات التوقف عن أنشطة معالجة البيانات إذا لم يكن هناك أساس قانوني آخر لمعالجة البيانات (مثل فترة الاحتفاظ)، فيجب حذف البيانات من قبل وحدة التحكم[٥].

[1] - Lignes directrices 5/2020 sur le consentement au sens du règlement (UE) 2016/679 , op cit p.27

[2] - Considérant 42 du R.G.P.D

[3] -Groupe Article 29 Avis n°13/2011 du 16 mai 2011op cit. p.16.

[4] - l'avis 4/2010 du G29 sur le code de conduite de la FEDMA relatif à l'exploitation de données à caractère personnel dans le cadre d'opérations de marketing direct (WP 174) et l'avis sur l'utilisation de données de localisation aux fins de fourniture de services à valeur ajoutée (WP 115).

[5] - Lignes directrices 5/2020 sur le consentement au sens du règlement (UE) 2016/679 , op cit p.28.

المطلب الثاني

الأغراض المقبولة لتحديد الموقع الجغرافي

تمهيد :

إن بيانات الموقع الجغرافي تشكل بالضرورة بيانات شخصية ، وبالتالي تقع ضمن نطاق اللائحة العامة لحماية البيانات ، وبالتالي، عندما يقوم معالج البيانات بمعالجة هذه البيانات فيجب عليه بلا شك احترام الشروط العامة التي تحددها هذه اللائحة[١].

بموجب الحق في الحصول على المعلومات ، يجب على مراقبي البيانات ، أو المعالجين إبلاغ الأشخاص الذين تتم معالجة بياناتهم المتعلقة بالموقع الجغرافى بشكل استباقي من حيث المبدأ ، و قبل بدء المعالجة ، بأغراض المعالجة ، ومدتها ، والوسائل المستخدمة[٢] ، وأن تكون بيانات الموقع مناسبة ، وذات صلة ، ومحدودة بما هو ضرورى لأغراض المعالجة.

أولا : مبدأ تحديد الغرض

يعني مبدأ تحديد الغرض أن أي معالجة لبيانات تحديد الموقع الجغرافى يجب أن تتم لغرض معين ومحدد جيدًا، ولأغراض إضافية محددة متوافقة مع الغرض الأولي فقط. ويعد مبدأ تحديد الغرض أحد المبادئ الأساسية لقانون حماية البيانات الأوروبي ، ويرتبط ارتباطًا وثيقًا بالشفافية ، والقدرة على التنبؤ ، والتحكم من قبل المستخدم، ففي

[1] - Komur, Neslin, op cit p.50.
[2] - Manuel de droit européen en matière de protection des données Édition 2018,op cit p.136.

الواقع إذا كان الغرض من المعالجة دقيقًا ، وواضحًا بدرجة كافية ، يعرف الناس ما يمكن توقعه ، ويتم تعزيز الشفافية ، واليقين القانوني.

وفي الوقت نفسه يعد التحديد الواضح للغرض أمرًا مهمًا ؛ لتمكين أصحاب البيانات من ممارسة حقوقهم بشكل فعال، مثل الحق في الاعتراض على المعالجة[١].

بموجب المادة الخامسة (١– ب) من اللائحة العامة لحماية البيانات يتعين على معالج بيانات تحديد الموقع متابعة ما يسمى بالأغراض ، والتي يجب أن تكون محددة وصريحة ومشروعة ؛ من أجل التأكد من أن تحديد الموقع الجغرافي صحيح بالفعل.

يجب أن تتعلق المعلومات المسبقة بالغرض (الأغراض) التي تسعى إليها المعالجة، وفئات البيانات التي تم جمعها، ومدة الاحتفاظ ببيانات تحديد الموقع الجغرافي المتعلقة بهم ، والمستلمين ، أو فئات مستلمي البيانات ، ووجود حق الوصول، والتصحيح ، والمعارضة وطرق ممارستها ، وعند الاقتضاء نقل البيانات الشخصية إلى دولة غير عضو في الاتحاد الأوروبي[٢].

في الواقع يبدو من الضروري "تحديد نطاق عمليات المعالجة والتعبير عنها بشكل واضح لا لبس فيه"[٣].

[1] - Manuel de droit européen en matière de protection des données Édition 2018,op cit p.137.
[2] - Christophe Radé, [Brèves] A propos de la géolocalisation des salariés : la CNIL et la Cour de cassation à l'unisson, Lexbase Social, novembre 2011, n°46.
[3] - Komur, Neslin, op cit p.50.

٩- الجوانب القانونية لتقنية تحديد الموقع الجغرافي

تسرد المادة السادسة (١) من اللائحة العامة لحماية البيانات خمسة أسباب مشروعة للمعالجة بالإضافة إلى الموافقة وهي أن معالجة البيانات الشخصية ضرورية لتنفيذ عقد ، أو لأداء مهمة تتعلق بممارسة السلطة العامة، **والامتثال** مع التزام قانوني لأغراض المصالح المشروعة التي يسعى إليها المراقب ، أو الغير ، أو تكون ضرورية لحماية المصالح الأساسية للشخص المعني.

يتطلب مبدأ تحديد الغرض أن تتم أية معالجة لبيانات تحديد الموقع الجغرافى لغرض محدد ، ومحدد جيدًا ، ولأغراض إضافية متوافقة مع الغرض الأولي فقط.

وفقا لما سبق فإن معالجة بيانات تحديد الموقع الجغرافى لأغراض غير محددة ، أو غير محدودة تعتبر غير قانونية وفي غياب غرض محدد فإن معالجة البيانات بناءً على فكرة أن البيانات قد تكون مفيدة في وقت ما في المستقبل تعتبر غير قانونية[1] ؛ حيث تعتمد شرعية معالجة بيانات تحديد الموقع الجغرافى على الغرض منها، والذي يجب أن يكون محددًا ، وصريحًا ، ومشروعًا.

ومن ثم يجب أن يكون لكل غرض جديد لمعالجة البيانات لا يتوافق مع الغرض الأصلي أساس قانوني خاص به ، ولا يمكن أن يستند إلى حقيقة أن البيانات تم جمعها أو معالجتها في البداية لغرض مشروع آخر.

في المقابل تقتصر المعالجة المشروعة على الغرض المحدد في البداية ، وسيتطلب أي غرض جديد أساسًا قانونيًا جديدًا ومتميزًا. على سبيل المثال يجب النظر بحذر في

[1]- Manuel de droit européen en matière de protection des données Édition 2018,op cit p.137

إرسال البيانات الشخصية إلى الغير لغرض جديد ؛ لأن الكشف عنها سيتطلب أساسًا قانونيًا جديدًا يختلف عن أساس جمع البيانات.

إذا كان مراقب البيانات يرغب في تعديل المعالجة الأولية للبيانات الشخصية عن طريق نقل هذه البيانات إلى مزود خدمة جديد لتحديد الموقع الجغرافي فيحب عليه الحصول على موافقة جديدة بذلك النقل[١]، وبالمثل اذا تم اخبار أصحاب البيانات من البداية بأن الشركة لن تشارك البيانات الشخصية مع شركة أخرى ، لكنها ترغب الآن في مشاركتها فيجب عليها الحصول على موافقة جديدة مسبقة من كل عميل قبل مشاركتها البيانات الشخصية للعملاء[٢].

لتقييم مدى وحدود غرض معين، تعتمد اللائحة العامة لحماية البيانات على مفهوم التوافق، والذى يسمح باستخدام البيانات لأغراض متوافقة.

تنص اللائحة العامة لحماية البيانات على أن "المعالجة اللاحقة لأغراض الأرشفة للمصلحة العامة ، أو لأغراض البحث العلمي ، أو التاريخي ، أو للأغراض الإحصائية" ، تعتبر –بداهة– متوافقة مع الغرض الأولي[٣].

ومع ذلك يجب تطبيق الضمانات المناسبة مثل إخفاء الهوية ، أو التشفير ، أو إخفاء الهوية للبيانات ، وتقييد الوصول إلى البيانات عند معالجة البيانات الشخصية بشكل إضافي[١].

[1] - M. Henri BarbIerk, op cit p.29..

[2] - Groupe Article 29 Avis n°13/2011 du 16 mai 2011. op cit. p.15.

[3] - art. 5, para. 1, point b.du RGPD.

٩- الجوانب القانونية لتقنية تحديد الموقع الجغرافي

حتى لو كان الغرض من جمع بيانات تحديد الموقع الجغرافي مشروعًا على ما يبدو، فإنه لا يزال من الضروري، كما هو موضح في اللائحة العامة لحماية البيانات، أنه لن تتم معالجة هذه البيانات لاحقًا بطريقة غير متوافقة مع هذه الأغراض[٢].

كذلك فإن CNIL تتبع نفس الرأي الذى تبنته اللائحة العامة لحماية البيانات ، وتعطي بشكل خاص مثالاً على الاختلاس من خلال النص على أن "صاحب العمل الذي يستخدم جهاز تحديد الموقع الجغرافي للتحكم في نشاط موظفيه ، في حين أن الغرض المعلن في CNIL هو مكافحة السرقة من شأنه أن يرتكب تحويل الغرض في مثل هذه الحالة ، ويعد مرتكبا لجريمة جنائية بصفته مراقبا للبيانات[٣].

وقد طُلب من محكمة النقض الفرنسية أن تبت في مسألة تحويل الغرض ، وكان بائعاً مسؤولاً عن بيع طفايات الحريق ، وكانت سيارته مزودة بجهاز تحديد الموقع الجغرافي. برر صاحب العمل تركيب هذا الجهاز من أجل تحسين عملية الإنتاج من خلال دراسة بأثر رجعي لتحركاته ، والسماح للإدارة بتحليل الوقت اللازم لرحلاته ؛ من أجل تحسين الزيارات المنفذة بشكل أفضل ، ومع ذلك استخدم صاحب العمل النظام بعد ذلك للتحكم في وقت عمل موظفه وبالتالي تقليل أجره .

---

[1] - Manuel de droit européen en matière de protection des données Édition 2018,op cit p.28.

[2] - article 5. 1. b du RGPD

[3] - (CNIL), Guide de la géolocalisation des salariés, Droits et olbigations en matière de géolocalisation des employés par un dispositif de suivi G.S.M/G.P.S. p.4.

وقد وجدت محكمة النقض أن صاحب العمل قد أساء استخدام النظام ، حيث كان يتحكم في وقت عمل الموظف دون أن يكون الأخير على علم بهذا الوضع وبطرق المراقبة[١].

ثانيا : مبدأ تناسب الأغراض.

تم تضمين شرط التناسب هذا في اللائحة العامة لحماية البيانات في المادة الخامسة فقرة ١/ج والذي بموجبه "يجب أن تكون البيانات الشخصية مناسبة ، وذات صلة ، ومحدودة بما هو ضروري فيما يتعلق بالأغراض التي تتم معالجتها من أجل تقليل البيانات إلى الحد الأدنى".

وبتطبيق هذا المبدأ على تحديد الموقع الجغرافي فإنه ينطوي على سلسلة كاملة من العواقب.

يجب أن تكون البيانات التي يتم جمعها كجزء من تطبيق نظام تحديد الموقع الجغرافي كافية ، وذات صلة ، وغير مفرطة فيما يتعلق بالأغراض التي يتم تنفيذ المعالجة من أجلها[٢].

كما يجب تحديد البيانات التي يجب جمعها لكل عملية معالجة بالإضافة إلى مستوى الدقة التي يجب أن يعالجها التطبيق من أجل تقليل البيانات التي تتم معالجتها(على

[1] - Cass. Soc,, 3 novembre 2011, 10-18.036, Publié au bulletin;
[2] - CNIL Délibération n° 2010-096 du 8 avril 2010

٩- الجوانب القانونية لتقنية تحديد الموقع الجغرافي

سبيل المثال من الأفضل تخزين سنة الميلاد فقط بدلا من تاريخ الميلاد كاملا إذا كان التطبيق يحتاج السنة فقط)[١].

فيما يتعلق بالمراقبة في العمل فيجب على صاحب العمل أن يختار أقل وسائل الرقابة الممكنة تدخلاً في الحياة الخاصة لعامله ، وهذا يعنى "الحاجة إلى مراقبة العمال بأقل طريقة تدخليه ممكنة[٢].

فلا يجوز لأحد أن يضع قيوداً على حقوق الأفراد- الحقوق والحريات الفردية والجماعية- التي لا تبررها طبيعة المهمة المطلوب إنجازها ولا تتناسب مع الهدف المنشود[٣]؛ لذلك فإن استخدام نظام تحديد الموقع الجغرافي لضمان التحكم في ساعات العمل يكون قانونيًا فقط عندما لا يمكن القيام بهذه السيطرة بأية وسيلة أخرى[٤].

كما أن شرط التناسب يعنى أن تحديد الموقع الجغرافي دقيق ولا يمكن تفعيله خارج ساعات العمل وإلا فإنه سيشكل انتهاكًا حقيقيًا للحق في احترام الحياة الخاصة[٥].

ذهبت محكمة النقض الفرنسية إلى أن نظام تحديد الموقع المثبت على سيارة العمل المتاحة للعامل ، والمخصص للحماية من السرقة ، والتحقق من المسافة المقطوعة ، قد استخدمه صاحب العمل لمراقبة العامل المعنى ، والتحقق من موقعه خارج وقت

---

[1]- CNIL.Projet de recommandation Relative aux applications mobiles, Version soumise à consultation publique jusqu'au 8 octobre 2023 p.29.

[2] - Avis n°5/2005 du 25 novembre 2005 du Groupe de l'Article 29 sur l'utilisation de données de localisation aux fins de fourniture de services à valeur ajoutée, 2130/05/FR, WP115, p.10, disponible sur www.europa.EU.

[٣] – المادة ١/١٢٢١ من قانون العمل الفرنسي.

[4] - Cass. Soc19 décembre 2018, 17-14.631, Publié au bulletin - Cass. Soc. 20 mars 2024, 22-13.129, Inédit

[5] - Komur, Neslin, op cit p.54.

عمله ، مما يعد انتهاكا لحياته الخاصة ؛ لذلك يعد تحديد الموقع الجغرافي في هذه الحالة وسيلة إثبات غير قانونية[١].

إن صاحب العمل لا يمكنه الادعاء بأنه ليس لديه وسيلة أخرى غير نظام تحديد الموقع الجغرافي لضمان مراقبة وقت عمل موظفيه.

كما أن مكان تنفيذ معالجة تحديد الموقع الجغرافي لمركبات الشركة لا يمكن أن يكون هدفه السيطرة الدائمة على الموظف ، من خلال جمع البيانات المتعلقة بموقع مركبته خارج ساعات ، وأيام عمله ؛ لذلك فإن المراقبة الدائمة للعامل مع القراءة المنهجية للبيانات المسجلة بواسطة نظام تحديد الموقع الجغرافي يجب من حيث المبدأ اعتبارها غير متناسبة" ؛ حيث يجب ألا يخضع سفر الموظفين للمراقبة المستمرة[٢].

وقد تم فرض عقوبة قدرها ١٢٥٠٠٠ يورو من قبل الCNIL ضد شركة CITYSCOOT لتسببها على وجه الخصوص في هجوم غير متناسب على الحياة الخاصة لعملائها من خلال تحديد الموقع الجغرافي لهم بشكل دائم تقريبًا.

وقد تم اتخاذ هذا القرار بالتعاون مع سلطات حماية البيانات الإسبانية والإيطالية. حيث تقدم الشركة أيضًا هذه الخدمات في هذه البلدان[٣].

من ثم يجب إيجاد التوازن بين جميع المصالح المعنية في جميع مراحل المعالجة. وبعبارة أخرى يجب اعتبار البيانات التي قد تكون كافية ، وذات صلة ، ولكن من

[1] - Cass. Soc. 22 mars 2023, 21-22.852, Inédit.
[2] - Ibid - Komur, Neslin, op cit p.54.
[3] - CNIL Délibération de la formation restreinte n° SAN-2023-003 du 16 mars 2023 concernant la société CITYSCOOT

شأنها أن تؤدي إلى تدخل غير متناسب في الحقوق والحريات الأساسية المعرضة للخطر، مفرطة ، ولا تتم معالجتها[١].

أما بخصوص عقد التأمين فتشير اللجنة الوطنية لتكنولوجيا المعلومات والحريات الفرنسيةCNIL إلى أنه إذا كان من الممكن تشجيع تنفيذ الإجراءات الرامية إلى تطوير السلامة على الطرق لصالح السائقين الشباب ، إلا أن استخدام جهاز تحديد الموقع الجغرافي المجهز بكل مركبة من مركبات حاملي وثائق التأمين يؤدي بشكل مباشر أو غير مباشر إلى قيام MAAF بتنفيذ المعالجة التي تتيح تسجيل مجمل الرحلات التي قام بها حاملو وثائق التأمين المعنيون.

كما أن الجمع المنهجي للبيانات المتعلقة بموقع المركبات المستخدمة بشكل خاص لأغراض تعديل أسعار التأمين على السيارات يعد غير مبرر ، ومن المرجح أن يقوض حرية القدوم ، والذهاب ؛ لذلك ترى CNIL أن المعاملة التي قدمتها وزارة الزراعة والغابات لا تفي بشرط التناسب[٢].

كذلك فإن مبدأ التناسب ينطبق على الاحتفاظ بالبيانات. ففي الواقع يجب أن تكون مدة الاحتفاظ ببيانات الموقع الجغرافي لفترة متناسبة ، ولازمة لتحقيق الهدف المنشود من المعالجة[٣].

---

[1] - Manuel de droit européen en matière de protection des données Édition 2018,op cit p.142.

[2] - CNIL. Délibération 2005-278 du 17 novembre 2005

[3] - CNIL.Projet de recommandation Relative aux applications mobiles, Version soumise à consultation publique jusqu'au 8 octobre 2023 p.4

مبدأ الحد من فترة الاحتفاظ يعني أنه يجب حذف البيانات الشخصية ، أو جعلها مجهولة المصدر بمجرد أن تصبح غير ضرورية للأغراض التي تم جمعها من أجلها[١].

وفي السنوات الأخيرة قضت محكمة العدل الأوربية في عدة أحكام بشأن الاحتفاظ بالبيانات الشخصية ، والوصول إليها في مجال الاتصالات الإلكترونية والتي رأت فيها المحكمة أنه لا يجوز للدول الأعضاء أن تطلب من مقدمي خدمات الاتصالات الإلكترونية الاحتفاظ ببيانات حركة المرور وبيانات الموقع بشكل عام وبطريقة عشوائية[٢].

وقد أثارت هذه الأحكام مخاوف بعض الدول من احتمال حرمانها من أداة تعتبرها ضرورية لحماية الأمن القومي ، ومكافحة الجريمة.

في علاقات العمل وفقا لـ CNIL ستكون المدة سنة واحدة كحد أقصى لمراقبة سيارة العامل إذا كان الغرض من النظام هو تحسين المسارات[٣].

[1] - Manuel de droit européen en matière de protection des données Édition 2018,op cit p.144

[2] - JEU Case C-623/17 6 October 2020 - CJEU Case C-511/18 6 October 2020- CJEU Case C-512/18 6 October 2020- CJEU Case C-520/18 6 October 2020.

[3]- CNIL, Délibération n°2006- 066 du 16 mars 2006 portant adoption d'une recommandation relative à la mise en œuvre de dispositifs destinés à géolocaliser les véhicules automobiles utilisés par les employés d'un organisme privé ou public, art. 5, disponible sur www.cnil.fr

من ناحية أخرى إذا كان الغرض من النظام هو مراقبة نشاط العمال ترى CNIL أنه في هذه الحالة يجب أن تكون مدة الاحتفاظ ببيانات الموقع معقولة و لا تزيد عن شهرين[١].

المطلب الثالث

حقوق أصحاب بيانات تحديد الموقع الجغرافي.

تمهيد

رأينا سابقا أنه منذ لحظة دمج بيانات تحديد الموقع الجغرافي مع البيانات الشخصية ستخضع المعالجة المتعلقة بها لنظام اللائحة العامة لحماية البيانات (GDPR) مع كل العواقب التي تنطوي عليها ؛ لذلك يجب على القائمين على هذا النوع من المعالجة أن يقوموا بتزويد أصحاب البيانات بمعلومات عن الحقوق التي يتمتعون بها[٢] وهي : حق الوصول إلى البيانات الشخصية ، الحق في تقديم شكوى إلى سلطة حماية البيانات ، حق الاعتراض، حق التصحيح، حق المحو("الحق في النسيان")، الحق في تقييد المعالجة ، والحق في قابلية نقل البيانات[٣].

[1] - CNIL, Guide de la géolocalisation des salariés, Droits et obligations en matière de géolocalisation des employés par un dispositif de suivi G.S.M/G.P.S., op. cit., p.9

[2]- Christophe Radé, [Brèves] A propos de la géolocalisation des salariés : la CNIL et la Cour de cassation à l'unisson, Lexbase Social, novembre 2011, n°462

[3] - Komur, Neslin, op cit p.61.

أولا : الحق في الوصول

في قانون الاتحاد الأوروبي يتم الاعتراف صراحةً بحق الفرد في الوصول إلى البيانات الخاصة به في المادة ١٥ من اللائحة العامة لحماية البيانات (GDPR).

كما أن هذا الحق منصوص عليه كحق أساسي في المادة ٨ الفقرة ٢ من ميثاق الاتحاد الأوروبي للحقوق الأساسية ، وفى المادة ١٠ من توجيه حماية البيانات (EC/٤٦/٩٥).

يجب اعتبار حق الوصول حقًا أساسيًا في قانون حماية البيانات الأوروبي ؛ نظرًا لأنه شرطًا أساسيًا لممارسة أي من الحقوق الأخرى لصاحب البيانات[١].

ويحق لأصحاب البيانات المتعلقة بالموقع الجغرافي حق الوصول إلى هذه البيانات باعتبارها بيانات شخصية خاضعة للمعالجة[٢].

يجب أن تكون بيانات الموقع المقدمة من خلال المحطات الطرفية ، وكذلك أغراض المعالجة والمستلمين قادرة على لفت انتباه المستخدم من خلال جعلها في متناول صاحب البيانات[٣]: بحيث يكون الأخير قادرًا على الوصول إلى البيانات من جهاز

[١] - راجع تفاصيل حقوق صاحب البيانات الشخصية : ياسر محمد على النيدانى ، حماية البيانات الشخصية عبر تقنية البلوك تشين ، مجلة روح القوانين المجلد ٣٦ العدد ١٠٧ ، يوليو ٢٠٢٤ صفحة ١١٢١ وما بعدها.

[2] - Art. 15 du RGPD - M. Henri BarbIerk op cit p.30 - Komur, Neslin, op cit p.61

[3] - M. Henri BarbIerk, op cit p.30.

٩- الجوانب القانونية لتقنية تحديد الموقع الجغرافي

تحديد الموقع الجغرافي المتعلق به عن طريق الاتصال بالخدمة أو بالشخص المعنى بالمعالجة[١].

يجب على مختلف وحدات التحكم في معلومات تحديد الموقع الجغرافي من الأجهزة المحمولة السماح لعملائها بالوصول إلى بيانات موقعهم. مع تسليم المعلومات في نسخة قابلة للقراءة : أي في شكل مواقع جغرافية ، وليست أعدادا مجردة[٢].

كما يحق لأصحاب البيانات الوصول الآمن إلى الملفات الشخصية المحتملة بناءً على بيانات الموقع هذه. فإذا تم تخزين معلومات الموقع فيجب السماح للمستخدمين بتحديث هذه المعلومات ، أو تصحيحها ، أو حذفها.

وقد أوصت مجموعة عمل المادة ٢٩ بضرورة أن يبحث مراقبو البيانات عن طرق آمنة لتوفير الوصول المباشر عبر الإنترنت إلى بيانات الموقع والملفات الشخصية المحتملة ، وأن يتم توفير هذا الوصول دون طلب بيانات شخصية إضافية للتحقق من هوية أصحاب البيانات[٣].

كما لا يمكن لمراقب البيانات تدمير المعلومات الموجودة في مصدر البيانات ؛ لإعفاء نفسه من الالتزام بإبلاغها إلا إذا حدث المحو على الرغم من استلام طلب الوصول . كما يجب أن يظل ملتزمًا بمتطلبات المسؤولية العامة.

---

[1] - Christophe Radé, op,cit. n°462.- CNIL Délibération n° 2010-096 du 8 avril 2010

[2] - M. Henri BarbIerk, op cit p.30.

[3] - Groupe Article 29 Avis n°13/2011 du 16 mai 2011op cit. p.18 et 21.

كذلك لا يمكن تقييد الحق في الوصول إلى بيانات تحديد الموقع بشكل غير مبرر بحدود زمنية. بل يجب أن يتمتع أصحاب البيانات بإمكانية معقولة للحصول على معلومات حول عمليات المعالجة التي تم تنفيذها في الماضي[١].

ثانيا : الحق في التصحيح

تنص المادة السادسة عشر من اللائحة العامة لحماية البيانات على أن أصحاب البيانات لهم الحق في تصحيح البيانات الشخصية المتعلقة بهم[٢].

تعد دقة البيانات الشخصية أمرًا ضروريًا ؛ ليضمن أصحاب البيانات مستوى عالٍ من حماية البيانات.

غالبا ما يكون طلب صاحب بيانات الموقع الجغرافي بحقه في الوصول للبيانات المتعلقة بتحديد الموقع الجغرافي من أجل تصحيحها ، أو حذفها[٣].

في حالة معالجة بيانات الموقع الشخصي يحق لمستخدمي الهواتف الذكية أن يتم إعلامهم بهوية موفر نظام التشغيل ، أو ناشر التطبيق ، أو مطور التطبيق باعتباره مراقبا، وبأغراض معالجة البيانات ، ومتلقي تلك البيانات ، ومدة الاحتفاظ ببيانات تحديد الموقع الجغرافي المتعلقة بهم مع وجود حق التصحيح ، وطرق ممارسته[٤].

---

[1]- Manuel de droit européen en matière de protection des données Édition 2018,op cit p.344.

[٢] – كما أن الحق في تصحيح البيانات الشخصية منصوص عليه في المادة ١٠ من توجيه حماية البيانات (EC/٤٦/٩٥).

[3] - M. Henri BarbIerk, op cit p.30.

[4] - Bu-Pasha, Shakila & Alén, Anette & Mäkinen, J. & Guinness, Robert & Korpisaari, Päivi. (2016).op cit p.319 - Christophe Radé, op,cit,n°462- CNIL Délibération n° 2010-096 du 8 avril 2010.

وفي بعض حالات التصحيح يكفي أن يطلب الشخص المعني ببساطة تصحيح كتابة الاسم ، أو تغيير العنوان ، أو رقم الهاتف على سبيل المثال.

بموجب قانون الاتحاد الأوروبي يجب تصحيح البيانات الشخصية غير الدقيقة دون تأخير غير مبرر ، ومع ذلك إذا كانت طلبات التصحيح تتعلق بمسائل قانونية ذات أهمية كبيرة مثل الهوية القانونية لصاحب البيانات ، أو مكان الإقامة الصحيح لغرض الحصول على خدمة المستندات القانونية : فقد لا تكون طلبات التصحيح كافية ، ويجوز للمراقب أن يطلب دليلاً على عدم الدقة المزعومة[١].

ثالثا : الحق في المحو ("الحق في النسيان")

إن منح أصحاب البيانات الحق في محو بياناتهم له أهمية كبيرة وعلى وجه الخصوص مبدأ تقليل البيانات وبحيث يجب أن تقتصر البيانات الشخصية على ما هو ضروري للأغراض التي من أجلها تتم معالجة هذه البيانات.

وقد أكدت محكمة العدل الأوروبية على أهمية الحق في المحو ؛ لضمان مستوى عال من حماية البيانات[٢].

تُفعِّل المادة ١٧ من اللائحة العامة لحماية البيانات (GDPR) طلبات حذف أصحاب البيانات، ويطبق الحق في الحصول على حذف البيانات الخاصة بصاحب البيانات دون تأخير لا مبرر له عندما :

[1] - Manuel de droit européen en matière de protection des données Édition 2018,op cit p.245-246.

[2] - CJUE, C-131/12, Google Espagne SL, Google Inc. c. Agence espagnole de protection des données (AEPD), Mario Costeja González [GC], 13 mai 2014, points 55 à 58

• لم تعد البيانات الشخصية ضرورية فيما يتعلق بالأغراض التي تم جمعها ، أو معالجتها بطريقة أخرى.

لذلك يجب تحديد فترة الاحتفاظ ببيانات تحديد الموقع بوضوح ، وحذف هذه البيانات بعد تاريخ انتهاء الصلاحية. على سبيل لا يمكن الاحتفاظ بالبيانات المتعلقة بموقع السيارة إلا لفترة ذات صلة بغرض المعالجة التي تبرر تحديد موقعها الجغرافي[١].

علاوة على ذلك يجب حذف البيانات السرية مثل كلمات المرور من جميع وحدات التخزين[٢].

• يقوم صاحب البيانات بسحب الموافقة التي تستند إليها المعالجة ، ولا يوجد أي أساس قانوني آخر للمعالجة.

• يعترض صاحب البيانات على المعالجة ، ولا توجد أسباب مشروعة للمعالجة.

• خضعت البيانات الشخصية لمعالجة غير قانونية.

---

[1] - CNIL. Délibération n° 2010-096 du 8 avril 2010

[٢] - استخدم مهندسو Uber تقنية تسمى بصمة الإصبع، والتي تترك أثرًا صغيرًا قطعة من التعليمات البرمجية على الهاتف الذكي حتى لو تم حذف التطبيق. المشكلة في هذه التقنية؛ يمكن للمطور معرفة ما إذا كان التطبيق قد تم تثبيته مسبقًا على نفس الهاتف الذكي نظرًا لأن العديد من برامج تشغيل المسار كانت تحذف التطبيق وتعيد تثبيته لتحقيق تصنيفات أعلى وتجنب المراجعات السيئة. علاوة على ذلك، تمكنت الشركة من تتبع موقع المستخدمين الذين قاموا بحذف التطبيق مما أدى إلى انتهاك فترة الاحتفاظ بالبيانات.

Mike Isaac, Uber's CEO Plays With Fire, NY. TIMES (Apr. 23, 2017), https://nyti.ms/2pSAyyu.

Tselekidis Dimitrios, Privacy and Data Protection in Mobile Applications, Master of Science (MSc) in Information and Communication Systems Internatinonal Hellenic University JANUARY 2022 p.50

٩- الجوانب القانونية لتقنية تحديد الموقع الجغرافي

• يجب محو البيانات الشخصية ومنها بيانات تحديد الموقع الجغرافي للامتثال للالتزام القانوني المنصوص عليه في قانون الاتحاد ، أو قانون الدولة العضو التي يخضع لها المراقب.

في الواقع أن محو بيانات تحديد الموقع الجغرافي موضع شك من الناحية التكنولوجية بسبب الصعوبات التقنية، ذلك أن هناك مشكلة بين القانون والحقائق التقنية ؛ لأنه من الصعب تنفيذ المتطلبات القانونية في التقنيات التكنولوجية التي لديها فهم مختلف لمفاهيم مثل الذاكرة والنسيان ، حيث يمكن استعادة قواعد البيانات بسهولة إلى حالاتها السابقة ؛ بسبب سهولة نسخ المعلومات وتخزينها في نسخ احتياطية تجعل محوها الدائم ، وتأمينها شبه مستحيل ؛ لأنها تحتوي على سجلات مفصلة لهذه الحالات.

لذلك من الضروري سد الفجوات بين القانون والتكنولوجيا حتى نتمكن من حماية الحق في النسيان من جميع الجوانب[١].

رابعا : الحق في تقييد المعالجة

وفقًا للمادة ١٨ من اللائحة العامة لحماية البيانات فإن صاحب بيانات الموقع الجغرافي لديه الحق في الحصول من مراقب البيانات على تقييد معالجة بياناته الشخصية[٢].

فيجوز لصاحب البيانات أن يطلب من وحدة التحكم تقييد المعالجة عندما تكون:

• دقة البيانات الشخصية محل نزاع.

---

[1] - Tselekidis Dimitrios,op cit p.25.
[2] - Komur, Neslin, op cit p.61.

• المعالجة غير قانونية ويعترض صاحب البيانات على محوها ويطالب بدلاً من محوها بتقييد استخدامها.

• يجب الاحتفاظ بالبيانات لممارسة الحقوق القانونية ، أو الدفاع عنها.

• لا يزال القرار معلقًا بشأن ما إذا كانت الأسباب المشروعة التي تتبعها وحدة التحكم تتجاوز تلك الخاصة بصاحب البيانات.

كما يجب على مراقب البيانات إخطار صاحب البيانات قبل نقل البيانات ، أو وضع قيود على المعالجة ، أو محو البيانات.

فقد تتضمن الطرق التي قد يقوم مراقب البيانات من خلالها بتقييد معالجة البيانات الشخصية نقل البيانات المحددة مؤقتًا إلى نظام معالجة آخر، أو جعل البيانات غير قابلة للوصول للمستخدمين ، أو إزالة البيانات الشخصية مؤقتًا.

في مثل هذه الحالات يجب على مراقب البيانات إبلاغ كل مستلم أرسل إليه البيانات الشخصية بأي تصحيح ، أو محو لهذه البيانات ، أو أي قيود على المعالجة ما لم يثبت أن ذلك الابلاغ مستحيلاً أو يتطلب جهداً غير متناسب.

خامسا : الحق في الاعتراض

يجوز لأصحاب بيانات الموقع الجغرافي وفقا لنص المادة ٢١ (١) من اللائحة العامة لحماية البيانات المطالبة بحقهم في الاعتراض على معالجة بيانات الموقع الجغرافي

المتعلقة بهم لأسباب تتعلق بوضعهم الخاص ، ومعالجة البيانات لأغراض التنقيب ، وليس لهم الحق العام في الاعتراض على معالجة بياناتهم[١].

يهدف الحق في الاعتراض لأسباب تتعلق بالوضع الخاص لصاحب البيانات إلى تحقيق توازن عادل بين حقوق صاحب البيانات في حماية بياناته ، والحقوق المشروعة للغير في معالجة البيانات.

مع ذلك أوضحت محكمة العدل الأوروبية أن حقوق صاحب البيانات لها الأسبقية كقاعدة عامة" على المصالح الاقتصادية لمراقب البيانات اعتمادًا على طبيعة المعلومات المعنية ، وحساسيتها للحياة الخاصة للشخص المعني". فضلا عن المصلحة العامة في إتاحة هذه المعلومات"[٢].

وفقًا للائحة العامة لحماية البيانات يجب إبلاغ صاحب بيانات الموقع الجغرافي قبل تنفيذ المعالجة بالغرض الذى تسعى إليها معالجة تحديد الموقع الجغرافي، وبفئات بيانات الموقع التي ستتم معالجتها ، وبوجود حقه في الاعتراض على المعالجة وطرق ممارسته[٣].

في حال استمرار المعالجة رغم اعتراض صاحب البيانات فيقع عبء الإثبات على عاتق مراقبي البيانات ، الذين يجب عليهم إعطاء أسباب مقنعة تبرر استمرار

---

[1] - Komur, Neslin, op cit p.61.

[2] - CJUE, C-131/12, Google Spain SL, Google Inc. c. Agencia Española de Protección de Datos (AEPD), Mario Costeja González [GC], 13 mai 2014, point 81

[3] - Christophe Radé, op,cit,n°462.- CNIL. Délibération n° 2010-096 du 8 avril 2010.

المعالجة والتي قد تتجاوز حق صاحب البيانات في الاعتراض، وهذه المبررات يجب إثباتها على أساس كل حالة على حدة[١].

بخصوص الاعتراض الناجح فلن يستطيع معالج البيانات القيام بمعالجة البيانات المعنية بواسطة وحدة التحكم.

مع ذلك، فلا ينطبق الحق في الاعتراض (المادة ٢١) عندما تكون المعالجة مبنية على الموافقة على الرغم من أن الحق في سحب الموافقة قد يؤدي إلى نتيجة مماثلة[٢].

سادسا : الحق في إمكانية نقل البيانات.

لصاحب بيانات الموقع الجغرافي الحق في إمكانية نقل بياناته خارج الاتحاد الأوربي وفقًا للمادة ٢٠ من اللائحة العامة لحماية البيانات[٣].

يجب إبلاغ صاحب بيانات الموقع الجغرافي قبل تنفيذ المعالجة بالغرض الذى تسعى إليه المعالجة ، وفئات بيانات الموقع الذى يتم معالجته ، وبحقه في نقل بيانات الموقع الجغرافي إلى دولة غير عضو في الجماعة الأوروبية[٤].

يهدف مبدأ قابلية نقل البيانات الشخصية تمكين أصحاب البيانات فيما يتعلق ببياناتهم الشخصية ؛ لأنه يسهل قدرتهم على نقل البيانات الشخصية ، أو نسخها ، أو نقلها بسهولة من بيئة تكنولوجيا معلومات إلى أخرى[١].

---

[1] - Manuel de droit européen en matière de protection des données Édition 2018,op cit p.257.

[2] - Lignes directrices 5/2020 sur le consentement au sens du règlement (UE) 2016/679 , op cit p.37.

[3] - Komur, Neslin, op cit p.61.

[4] - Christophe Radé, op,cit,n°462.- CNIL Délibération n° 2010-096 du 8 avril 2010

٩- الجوانب القانونية لتقنية تحديد الموقع الجغرافي

يحق لأصحاب البيانات إمكانية نقل البيانات عندما تتم معالجة البيانات الشخصية التي قدموها إلى وحدة التحكم باستخدام عمليات آلية ، أو بناءً على الموافقة ، أو عندما تكون معالجة البيانات الشخصية ضرورية لأداء مهمة ما ، وهذا يعني أن الحق في إمكانية نقل البيانات لا ينطبق عندما تعتمد معالجة البيانات الشخصية على أساس قانوني غير الموافقة ، أو العقد[٢].

عندما ينطبق الحق في إمكانية نقل البيانات، يحق لأصحاب البيانات نقل بياناتهم الشخصية مباشرة من وحدة تحكم إلى أخرى ، حيثما يكون ذلك ممكنًا من الناحية الفنية.

ووفقًا للمبادئ التوجيهية للفريق العامل بموجب المادة ٢٩، فإن الحق في إمكانية نقل البيانات يشجع اختيار المستخدم ، والتحكم ، والمساءلة ؛ من أجل منح أصحاب البيانات السيطرة على بياناتهم[٣].

ولا تخل ممارسة الحق في إمكانية نقل البيانات بأي حق آخر كما هو الحال بالنسبة لأي حق آخر منصوص عليه في اللائحة العامة لحماية البيانات.

---

[1] - Groupe de travail Article 29 (5 avril 2017), Lignes directrices sur le droit à la portabilité WP 16/EN, WP 242 rév.01, 4 p.4

[2] - Art. 20, para. 1 du RGPD - considérant 68. du RGPD

[3] - Groupe de travail « Article 29 » (2016), Lignes directrices relatives au droit à la portabilité des données, WP 242, 13 décembre 2016, version révisée et adoptée le 5 avril 2017, p. 13.

المبحث الثالث

استخدامات تقنية تحديد الموقع الجغرافي

تتنوع تطبيقات وأغراض تحديد الموقع الجغرافي بدءًا من المساعدة في الملاحة ، إلى ربط الأشخاص ، وإدارة الوقت الفعلي لموظفي الشركة ، والمركبات.

وتحظى هذه التقنيات بشعبية كبيرة لدى أصحاب الأعمال في القطاعين العام والخاص حيث تسمح لهم أن يصبحوا على علم بالموقع الجغرافي في لحظة معينة ، أو بشكل مستمر من خلال الموقع للأشياء التي يستخدمونها (الشارات، الهواتف المحمولة) أو مركبات العمل الموكلة للعمال.

وقد تطور تحديد الموقع الجغرافي بشكل كبير وأصبح جزءًا لا يتجزأ من مجتمعنا ، وأصبح من المستحيل تحديد عدد الاستخدامات المحتملة التي يمكن أن يغطيها.

مع ذلك فإن تحديد الموقع الجغرافي مثل جميع الأنشطة البشرية البارزة ، يجب أن يخضع لتطبيق القانون.

يمكن لتقنية تحديد الموقع الجغرافي أن تلعب دورًا مهمًا في المسائل الجنائية : فتساعد في تحقيق الأمن الداخلي من خلال تمكين مراقبة المشتبه بهم، وتعقب الأشياء المسروقة (خاصة السيارات). كما يمكن أيضًا استخدامها في مسائل الإرهاب.

تعد نظم المعلومات الجغرافية ، والمعلومات السياقية في الوقت الفعلي أحد العوامل الرئيسية في تحسين الرحلات الفردية ، وبالتالي مراقبة وتحديد بيانات حركة المرور ،

وإدارة الوقت بشكل أفضل ، بالإضافة إلى المساهمة في توفير راحة أفضل لسفر المواطنين.

سرعان ما تم استخدام تقنية تحديد الموقع الجغرافي في بيئة العمل حيث وجدت مكانها ومزاياها داخل الشركات ، وفي إطار علاقة الأعمال التجارية مع المستهلك حيث استفادت الشركات من جانبها إلى حد كبير من هذه التقنية لتقديم منتجاتها ، وخدماتها على أساس القرب من العميل المحتمل.

كما أثبتت هذه التقنية نجاحها في أثناء أزمة كورونا في تحديد أماكن مصابي فيروس كورونا ، وتحديد بؤر الاصابات ، واعتمدت عليها السلطات العامة في الكثير من دول العالم لرصد تطور الوباء والسيطرة على السكان.

ويتضح جليا أن استخدامات تقنية الموقع الجغرافي كثيرة ومتعددة ، ولا يمكن إحصاؤها ؛ لذلك سوف نقوم في هذا المبحث بدراسة ثلاث استخدامات هامه جدا لتقنية تحديد الموقع الجغرافي وهى : دراسة تحديد الموقع الجغرافي وسيارة العمل ، ثم دراسة دور تحديد الموقع الجغرافي في مكافحة وباء كورونا ، على أن ننهى هذا المبحث بدراسة تحديد الموقع الجغرافي في الأعمال التجارية ، وذلك في ثلاثة مطالب على النحو التالي:

المطلب الأول: تحديد الموقع الجغرافي وسيارة العمل

المطلب الأول: تحديد الموقع الجغرافي ومكافحة الأوبئة

المطلب الأول: تحديد الموقع الجغرافي والأعمال التجارية

المطلب الأول

تحديد الموقع الجغرافي وسيارة العمل

إن التبني السريع لتقنيات المعلومات الجديدة في مكان العمل من حيث البنية التحتية ، والتطبيقات ، والأجهزة الذكية يسمح بأنواع جديدة من معالجة البيانات المنهجية ، والمحتملة في العمل.

يمكن الآن تنفيذ التقنيات التي تتيح معالجة البيانات في العمل بجزء صغير من التكاليف التي كانت سائدة منذ عدة سنوات مضت بينما زادت القدرة على معالجة البيانات الشخصية بواسطة هذه التقنيات بشكل كبير[١].

الأشكال الجديدة للمعالجة، مثل تلك المتعلقة باستخدام بيانات الموقع من جهاز ذكي تكون أقل وضوحًا للموظفين مقارنة بالأنواع التقليدية الأخرى مثل كاميرات الدوائر التلفزيونية المغلقة العلنية. وهذا يثير تساؤلات حول مدى وعي الموظفين بهذه التقنيات.

في علاقة العمل أصبحت الحدود بين المنزل ، والعمل غير واضحة بشكل متزايد. عندما يعمل الموظفون عن بعد (على سبيل المثال من المنزل)، أو أثناء سفرهم للعمل يمكن أن تتم مراقبة الأنشطة خارج بيئة العمل المادية ، ويمكن أن تشمل مراقبة الفرد في سياق خاص.

[1]- Groupe de l’article 29, « Opinion 2/2017. P.3

٩- الجوانب القانونية لتقنية تحديد الموقع الجغرافي

إن تركيب مثل هذه التقنية في سيارة العمل يمكن أن يكون ذا أهمية خاصة في الفرضية القائلة بأن كل ، أو جزء من العمال العاملين داخل الشركة يمارسون وظائفهم خارج مباني هذه الشركة. فهو يحتوي على إمكانات عديدة سواء لخدمات الإسعاف ، أو شركات سيارات الأجرة ، أو شركات البناء ، أو النقل ، أو بشكل أعم لجميع مندوبي المبيعات الزائرين ، والعملاء المحتملين[١].

بالإضافة إلى ذلك، هذه التقنية الجديدة تحدد موقع سيارة العامل بدقة، وتتيح تحديد المسار ، ومتوسط السرعة ، ووقت القيادة ، ووقت التوقف ، وأوقات بدء وإيقاف المحرك ، أو حتى في بعض الحالات نوع السلوك الذي يعتمده العامل.

بسبب كل هذه الإمكانيات الجذابة التي توفرها أجهزة تحديد الموقع الجغرافي سارع أصحاب العمل إلى تجهيز سيارات العمال بمثل هذا النظام ، لدرجة أننا نرى الآن ظهور المزيد ، والمزيد من الشركات المتخصصة في تقديم مثل هذه الخدمات.

على الرغم من المزايا العديدة التي يمكن أن تقدمها تقنية تحديد الموقع الجغرافي، تظل الحقيقة أن هذه التكنولوجيا التي تتيح متابعة العامل في جميع تحركاته، علاوة على جمع ومعالجة البيانات الشخصية المتعلقة به تشكل تعبيرا خاصا عن التوتر الواضح بين سلطة صاحب العمل في المراقبة والحق في احترام الحياة الخاصة للعامل[٢].

نتيجة لذلك يلزم إجراء تقييم جديد فيما يتعلق بالتوازن بين المصلحة المشروعة لصاحب العمل في حماية أعماله ، والتوقع المعقول لخصوصية العمال.

---

[1] - Komur, Neslin op. cit.p.19
[2] - Komur, Neslin op. cit.p.19

في هذا السياق سوف نتعرض لمعالجة بيانات تحديد الموقع الجغرافي لسيارة العمل ، حيث سنعرض على التوالي للغرض من تحديد الموقع الجغرافي لسيارة العامل ، ومبدأ شفافية معالجة البيانات ، والتناسب وتقليل الأغراض لبيانات موقع السيارة.

١–الغرض من المعالجة

قد يؤدي استخدام تحديد الموقع الجغرافي لمراقبة العمال إلى ظهور مشكلات بعيدة المدى تتعلق بمعالجة البيانات الشخصية ، مثل نطاق الحصول على البيانات وشفافيته ، أو أغراض معالجة البيانات.

يجب أن يكون نطاق الحصول على البيانات متناسب مع احتياجات الجهة التي تحصل عليها.

بيانات الموقع هي المعلومات التي يجمعها تطبيق ، أو مزود خدمة حول مكان تواجد الجهاز المحمول الخاص بالمستخدم في وقت معين. مع ذلك، توفر الأنظمة المعاصرة قدرات أكبر بكثير. فقد يقومون بجمع بيانات حول رمز المرور، وأماكن وقوف السيارات، ومحطات التوقف ، وما إلى ذلك.

بالإضافة إلى ذلك، قد يساعد الحصول المستمر على البيانات في معرفة نماذج من سلوك الموظفين، وطرقهم المفضلة، وأماكن الراحة ، ووجهات استراحة الوجبات، وما إلى ذلك ؛ لذلك من المهم تقييد نطاق الحصول على بيانات العمال[1].

[1] - Krzysztof Stefański, Employee geolocation versus the GDPR praca I zabezpieczenie spoleczne/labour and social securtty journal 4/2021 p.16

٩- الجوانب القانونية لتقنية تحديد الموقع الجغرافي

القضية الأساسية هي أنه يجب على أصحاب العمل الحصول على البيانات التي تتوافق مع أغراض معالجة البيانات (مبدأ تقليل البيانات) ، ومن ثم يتعين على صاحب العمل أن يحدد بوضوح الغرض من الحصول على البيانات.

يجب أن يقتصر جمع البيانات على البيانات الضرورية ، والمتناسبة لتحقيق الأغراض فقط ، بحيث تكون البيانات كافية ، وذات صلة ، وغير مفرطة فيما يتعلق بالأغراض التي يتم جمعها من أجل معالجتها.

حددت المادة ٦ الفقرة ١ من اللائحة العامة لحماية البيات ست فئات يمكن أن تبرر معالجة البيانات ، وستعتبر الأغراض التي تندرج ضمن هذه الفئات مشروعة من قبل سلطة حماية البيانات.

ويعد من بين الأغراض المعقولة والمقبولة تحديد الموقع الجغرافي بقصد حماية المعلومات السرية التي تمثل سر العمل ، أو لحماية ممتلكات صاحب العمل ، أو لمنع التصرفات التي تضر بمكان العمل ، أو للإشراف على أداء العمل المناسب ، بما في ذلك الالتزام بوقت العمل.

كما يمكن تطبيق أنظمة المراقبة كإجراء وقائي لضمان سلامة العمال والبضائع[١] ، أو ردًا على أي مخالفات يتم اكتشافها[٢].

[1]- Komur, Neslin op. cit.p.51- CNIL, La géolocalisation des véhicules des salariés, 30 mai 2023.
[2] - Krzysztof Stefański op. cit.p.16.

يمكن كذلك أن يعمل مثل هذا النظام على تحسين تنظيم العمل و بخاصة تحركات العمال المتجولين ، وهنا يمكن لصاحب العمل أن يعين للعميل العامل الأقرب جغرافيا للقيام بالعمل[١].

كما يمكن أن يكون لنظام تحديد الموقع الجغرافي للعمال مزايا كبيرة في قطاع النقل بحيث يكون الغرض هو تخصيص أفضل للخدمات التي سيتم تقديمها في مواقع متفرقة ، وخاصة للتدخلات العاجلة مثل شركات سيارات الأجرة ، وتلك التي تقدم خدمات توصيل الوجبات، وما إلى ذلك[٢].

وفد تم استبعاد بعض الأغراض لتبرير تركيب جهاز تحديد الموقع الجغرافي. بالتالي، وفقًا لـ CNIL فلا يمكن تثبيت مثل هذا الجهاز بهدف مراقبة العامل بشكل دائم ، أو مراقبة الامتثال لحدود السرعة ، وما إلى ذلك.

بشكل أكثر تحديدًا لا يمكن أيضًا استخدام هذه الآلية لجمع الموقع خارج وقت العمل حتى لو أنها تنطوي على مكافحة السرقة ، أو التحقق من الامتثال لشروط استخدام السيارة[٣].

٢–مبدأ الشفافية

المبدأ الأساسي الثاني لمعالجة بيانات الموظفين بالإضافة إلى مبادئ التقليل والتناسب هو مبدأ الشفافية.

---

[1]- Komur, Neslin op. cit.p.51

[2] - Komur, Neslin op. cit.p.51

[3]- Komur, Neslin op. cit.p.52- CNIL, La géolocalisation des véhicules des salariés, 30 mai 2023.

٩- الجوانب القانونية لتقنية تحديد الموقع الجغرافي

مع التقنيات الجديدة أصبحت الحاجة إلى الشفافية أكثر وضوحًا ؛ لأنها تتيح جمع ومعالجة كميات هائلة من البيانات الشخصية بطريقة سرية[١].

وتنطبق متطلبات الشفافية الواردة في المادتين ١٠ و١١ على معالجة البيانات في العمل ؛ لذلك يجب إبلاغ الموظفين بوجود أي مراقبة ، والأغراض التي سيتم من أجلها معالجة البيانات الشخصية ، وأي معلومات أخرى ضرورية لضمان المعالجة العادلة.

وهذا يعني أنه يجب إبلاغ الموظفين بأنهم يخضعون لتحديد الموقع الجغرافي ، وعلى وجه الخصوص، ينبغي توعية الموظفين بما يلي:

١-أنه يتم تركيب جهاز مراقبة GPS على مركبات الشركة.

٢- ماهية البيانات التي يجمعها الجهاز المذكور (مثل سرعة السفر، الموقع الحالي، المسافة المقطوعة ، مدة التوقف، الأماكن التي يتم زيارتها ، وما إلى ذلك)

٣-ما هو الغرض من الحصول على البيانات (على سبيل المثال لزيادة سلامة العمال، وتحسين العمليات اللوجستية، وما إلى ذلك).

والأهم من ذلك يجب تمرير هذه المعلومات إلى العمال قبل بدء تشغيل النظام ، كما يجب إخطار العمال الجدد بوجود النظام عند قبولهم للعمل[٢]، وقد لفتت فرقة العمل المعنية بالمادة ٢٩ الانتباه إلى أن المعلومات ، والسياسات ، والقواعد المتعلقة بالمراقبة المشروعة المرسلة إلى الموظفين يجب أن تكون واضحة ، ومفهومة ، ويمكن

[1] - Groupe de l'article 29, « Opinion 2/2017. P.8
[2]- Krzysztof Stefański op. cit.p.16

الوصول إليها بسهولة مع التوصية بإشراك عينة تمثيلية من العمال في إنشاء وتقييم هذه القواعد والسياسات ؛ وذلك لأن معظم عمليات المراقبة لديها القدرة على التعدي على الحياة الخاصة للموظفين[١].

كما يجب أن يتم وضع علامات مناسبة على المركبات المجهزة بأجهزة GPS ، على سبيل المثال عن طريق ملصقات إشعار تحديد الموقع الجغرافي الخاصة[٢].

ويجب التأكيد على أنه على الرغم من قيام صاحب العمل بتسمية المركبات المحددة جغرافيًا، ومن وضعه علامات مميزة على هذه المركبات ، فإن هذا لا يعفيه من واجب تزويد الموظف ، بصفته صاحب البيانات، بأية معلومات مطلوبة بموجب اللائحة العامة لحماية البيانات ، والتواصل معه فيما يتعلق بمعالجة بياناته الشخصية. كما لا يعفى من واجب المعلومات المنصوص عليه في المادة ١٣ من اللائحة العامة لحماية البيانات.

و من المسلم به أنه لأغراض تحديد الموقع الجغرافي العادي للموظفين يكفي مجرد إخطارهم بهذه الحقيقة. مع ذلك في بعض الأحيان تكون موافقة الموظف مطلوبة لمعالجة بياناته. سينطبق هذا عند استخدام تحديد الموقع الجغرافي بعد ساعات العمل ، أو أثناء فترات الراحة. على سبيل المثال أثناء الرحلات الخاصة للموظف[٣] يجب أن

[1] - Groupe de l’article 29, « Opinion 2/2017 p.23
[2] - Krzysztof Stefański op. cit.p.16
[3] - Krzysztof Stefański op. cit.p.16

تكون هذه الموافقة واضحة وصريحة ، ومن الأفضل التعبير عنها كتابيًا ، أو بالوسائل الإلكترونية[١].

كما يجب أن يحدد إعلان الموافقة على معالجة بيانات الموقع الغرض من معالجة هذه البيانات ، والمراقب الذي سيقوم بمعالجتها، وحقوق صاحب البيانات.

قد تنشأ شكوك حول الطبيعة الطوعية لموافقة الموظف على معالجة بيانات موقعه الجغرافي خاصة وأن المشرع في الاتحاد الأوروبي يشير بالتأكيد إلى أن هذه الموافقة لا ينبغي أن توفر أساسًا قانونيًا صالحًا لمعالجة البيانات الشخصية في حالة محددة حيث يوجد سبب واضح لعدم التوازن بين موضوع البيانات ووحدة التحكم[٢].

وهذا ما يؤكده موقف فرقة العمل المعنية بالمادة ٢٩ والذي أكد على أن الموظفين ليسوا أحرارًا" في الأساس في منح مثل هذه الموافقة على معالجة بياناتهم ، ومن غير المرجح إلى حد كبير أن يتم منح موافقة صريحة صالحة قانونًا لتتبع هذه البيانات ، أو مراقبتها ؛ لأنهم لا يكونون أبدًا في وضع يسمح لهم بإعطاء الموافقة ، أو رفضها ، أو إلغائها بحرية ؛ نظرًا للتبعية التي تنتج عن العلاقة بين صاحب العمل والموظف ، ونظراً لاختلال توازن القوى ، وبالتالي لا يمكن للموظفين إعطاء الموافقة الحرة إلا في ظروف استثنائية عندما لا تكون هناك أية عواقب على الإطلاق مرتبطة بقبول

[1] - Ibid- preamble to the GDPR 58
[2] - preamble to the GDPR 43

العرضأو رفضه ؛ لذلك إذا لم تكن معالجة البيانات متناسبة فلن يكون لدى صاحب العمل أساس قانوني[١].

علاوة على ذلك لا يمكن اعتبار الإعدادات الافتراضية على الأجهزة ، أو تثبيت البرامج التي تسهل معالجة البيانات الشخصية الإلكترونية بمثابة موافقة مقدمة من الموظفين ، حيث تتطلب الموافقة تعبيرًا نشطًا عن الإرادة ، وبالتالي لا يمكن اعتبار عدم اتخاذ إجراء (أي عدم تغيير الإعدادات الافتراضية) بمثابة موافقة محددة للسماح بهذه المعالجة[٢].

٣- التناسب وتقليل البيانات[٣].

تم تضمين شرط التناسب في اللائحة العامة لحماية البيانات ، والذي بموجبه يجب أن تكون البيانات الشخصية كافية ، وذات صلة ، ومحدودة بما هو ضروري فيما يتعلق بالأغراض التي تتم معالجتها من أجلها[٤].

بتطبيق هذا المبدأ على تحديد الموقع الجغرافي ، فيجب على صاحب العمل أن يختار أقل وسائل الرقابة الممكنة تدخلاً في الحياة الخاصة لعامله[٥].كما شددت مجموعة المادة ٢٩، والتي أصبحت اللجنة الأوروبية لحماية البيانات مع دخول اللائحة العامة

[1] - Groupe de l’article 29, Opinion 2/2017" p.18 et 21 et 23
[2] - Groupe de l’article 29, Opinion 2/2017 p.7
[3] - Groupe de l’article 29, Opinion 2/2017 p.23
[4] - Article 5§1er , c du R.G.P.D
[5] - Komur, Neslin op. cit.p.53

لحماية البيانات (GDPR) حيز التنفيذ ، على الحاجة إلى مراقبة العمال بأقل طريقة تدخلية ممكنة[١] .

ويجب أن يتوافق الحصول على البيانات مع مبدأ التناسب ، وهذا يعني أن التدابير المتخذة يجب أن تكون متناسبة مع غرض الرصد.

لا يمكن اعتبار المعالجة ضرورية ، أو متناسبة إذا كانت المصلحة التي تخدمها المعالجة ذات أهمية قليلة فقط ، في حين أن التأثير على الخصوصية كبير، ويعني ذلك أيضًا أنه يجب على صاحب العمل إجراء عمليات المعالجة فقط التي يمكنها تحقيق الغرض المقصود مع أقل تأثير على الخصوصية[٢].

على سبيل المثال إذا أكد العميل من خلال إقرار بالاستلام أن الموظف قد أكمل خدمته بنجاح ، وبهذه الطريقة يحقق نفس أغراض نظام تحديد الموقع الجغرافي. ففي هذه الحالة يكون عمل الموظف هو الحل الأولي الذي يجب تفضيله ؛ لأنه أقل ضررًا بكثير بالحياة الخاصة للعامل[٣].

في أحد السوابق القضائية قررت المحكمة أن تحديد الموقع الجغرافي للسيارة يجب أن يكون متناسبًا مع الهدف المنشود ، وأن المراقبة الدائمة لتحركات الموظفين غير متناسبة عندما يمكن إجراء عمليات التحقق بوسائل أخرى كما هو الحال في هذه القضية ؛ نظرًا لأن صاحب العمل يمكنه إجراء دراسات استقصائية بين العملاء الذين

[1]- Groupe de l’article 29, "Opinion 2/2017" p.6 et 7
[2] - Krzysztof Stefański op. cit.p.16
[3] - O. MORENO et F. SCHAPIRA, « La surveillance des travailleurs par géolocalisation », in Discipline et surveillance dans la relation de travail (S. GILSON dir.), Limal, Anthemis, 2013, p.465.- Komur, Neslin op. cit.p.54

كان من المفترض أن يزورهم الموظف ، و يترتب على هذه العناصر أن تنفيذ نظام تحديد المواقع العالمي (GPS) كان غير قانوني ، وغير متناسب مع الغرض المقصود ، ولا يمكن قبوله كدليل[١].

ويتطلب القانون العام لحماية البيانات (GDPR) أيضًا من أصحاب العمل تنفيذ الخصوصية حسب التصميم وبشكل افتراضي.

الخصوصية حسب التصميم تعني أنه كلما تم تطوير أنظمة ، أو تطبيقات ، أو تقنيات جديدة ، يجب أخذ التأثير على الخصوصية في الاعتبار منذ البداية.

وتعني الخصوصية افتراضيًا أن الإعدادات الافتراضية للأنظمة ، أو التطبيقات ، أو التقنيات يجب أن تقلل من كمية ، وحساسية البيانات الشخصية التي تتم معالجتها تلقائيًا ؛ لذلك تساعد الخصوصية حسب التصميم وبشكل افتراضي على ضمان معالجة البيانات الشخصية فقط إذا كان ذلك ضروريًا ومتناسبًا[٢].

يعني شرط التناسب كذلك أن تحديد الموقع الجغرافي دقيق ، ولا يمكن تفعيله خارج ساعات العمل ، وإلا فإنه سيشكل انتهاكًا حقيقيًا للحق في احترام الحياة الخاصة.

[1] - A Agen, 3 août 2005, n° 04/00356, Pierre YC/SAS Seco Le Longeron Numéro de règle Lex : A9980DTS

[2] - Krzysztof Stefański op. cit.p.16
Privacy and monitoring at work under the GDPR.
https://legalict.com/factsheets/privacy-monitoring-work-gdpr

٩- الجوانب القانونية لتقنية تحديد الموقع الجغرافي

في الواقع ترى لجنة حماية الخصوصية أن لمراقبة الدائمة مع القراءة المنهجية للبيانات المسجلة بواسطة نظام تحديد الموقع الجغرافي، يجب من حيث المبدأ اعتبارها غير متناسبة[١]، وتشترط CNIL أيضًا ألا يخضع سفر الموظفين للمراقبة المستمرة[٢].

في قضية تتعلق بمندوب مبيعات تم تجهيز سيارة الشركة، والتي يمكن استخدامها لأغراض خاصة ، بجهاز تحديد الموقع الجغرافي الذي يحدد موقعه بشكل مستمر، بما في ذلك أثناء الليل ، وفي عطلات نهاية الأسبوع.

وقد رأت محكمة العمل في Gand أن هذه المراقبة والتي كانت أغراضها غير معروفة وغير متناسبة بسبب طبيعتها الدائمة ، تتعدى على الحياة الخاصة للعامل[٣].

إن أحد الحلول الممكنة هو تثبيت نظام يعمل على انفراد في وضعين: وضع السفر ، ووضع العمل. تماشيا مع مبدأ "الخصوصية الافتراضية" الذي قدمته اللائحة العامة لحماية البيانات يجب أن يكون وضع السفر الخاص هو الإعداد الافتراضي على نظام تحديد المواقع العالمي (GPS).

ومع ذلك فإن هناك سيناريوهات يمكن أن يكون فيها الرصد المستمر مفيدا لأسباب تتعلق بالسلامة ، ولا سيما عندما يتعلق الأمر بنقل البضائع الخطرة مثل المنتجات النووية.

---

[1] - CNIl , Avis n°12/2005 relatif à la proposition de loi visant à encadrer la surveillance des travailleurs par l'utilisation d'un système de monitoring associé au système de navigation G.P.S sur véhicules de service, dans le respect de la loi du 8 décembre 1992 relative à la protection de la vie privée, 7 septembre 2005, p.5

[2] - CNIL, La géolocalisation des véhicules des salariés, 30 mai 2023.

[3] - C. trav. Gand, 14 novembre 2011, J.T.T., 2012, p. 190

تتفق مجموعة المادة ٢٩ مع موقف المفوضية الأوربية بشأن هذه النقطة ، وتوصي أيضًا بتزويد المعدات المهنية ، وخاصة المركبات ، والتي يمكن استخدامها أيضًا خارج علاقة العمل بنظام يسمح للمستخدمين بإلغاء تنشيط وظيفة الموقع[١].

المطلب الثاني

تحديد الموقع الجغرافي ومكافحة فيروس كورونا (COVID-19)

تمهيد

واجه العالم في عام ٢٠١٩ أزمة صحية عامة لم يشهدها منذ أكثر من مائة عام وهى تفشى فيروس كورونا(COVID-19).

نظراً للحاجة الملحة للاستجابة للجائحة، ونظرا لعالمية الأزمة ؛ فقد تطلب الأمر تضافر دول العالم في اتخاذ التدابير التي تحد من حجم الأزمة . ذلك أن التدابير التي لا يمكن تصورها في الأوقات العادية قد يُنظر إليها على أنها خيارات قابلة للتطبيق للمساعدة في احتواء تفشي المرض[٢]، والتي سيكون لها تأثير يتجاوز هذه الحالة الطارئة.

[1] - Groupe de l’article 29 « Opinion 2/2017 p.20

[2] - Paige Backman and Stephanie D’Amico,Geolocation and the Fight Against COVID-19,Could the Emergencies Act Overrule Privacy Law Protections for Cellphone Location Data? 2020 no.5
https://www.everestlegalmarketing.com › 2023/06

٩- الجوانب القانونية لتقنية تحديد الموقع الجغرافي

سوف نتعرض في هذا المطلب لدراسة إدارة العالم لوباء كورونا ، وبخاصة الدول الأسيوية ، والأوربية، وكيفية استخدام تقنية الموقع الجغرافي في مكافحة هذا الوباء ، ومدى مشروعية معالجة بيانات الموقع الجغرافي لرصد الأوبئة وانتشارها.

١: إدارة وباء كورونا : تطلبت إدارة الوباء منذ البداية التوفيق بين الحجر الصحي وغياب إغلاق الأعمال الأساسية ؛ حيث إن حماية صحة كل واحد منا ، والحفاظ على نشاط ريادة الأعمال هي الممارسة الدقيقة ، والمحفوفة بالمخاطر في كثير من الأحيان، والتي واجهتها الدول، والتي كشفت مدى قدرتها على التكيف[١].

إن مكافحة تفشى فيروس كورونا (COVID-19) كأحد أخطر الأمراض المعدية في تاريخ البشرية كان هدفًا قيمًا تتقاسمه جميع دول العالم ، وبالتالي تم دعمه بأفضل طريقة ممكنة ؛ حيث إن من مصلحة البشرية كانت في الحد من انتشار المرض ، فكان الأمل في العلم في مواجهة عدو غير مرئي ، واستخدام التقنيات الحديثة في مكافحة الفيروس الذى أصاب أجزاء كبيرة من العالم[٢].

كانت الدول الأسيوية سباقة في استخدام البيانات في تتبع تفشي فيروس كورونا ، والحد من انتشاره عن طريق استخدام بيانات مشغلي الهاتف المحمول ، وتطوير

---

[1] - Marie Romani, Prévenir ou l'impact de la crise sanitaire planétaire et inédite de l'année 2020Anne https://www.airdberlis.com

[2] - Comité européen de la protection des données, Statement on the Processing of Personal Data in the Context of the Covid-19 Outbreak 2020 p.1.

التطبيقات ، وقد أثبتت النتائج الأولية فعالية الطريقة ، بينما كانت الدول الأوروبية تفكر في تبني نهج مماثل.

وقد اعتمدت السلطات العامة في الكثير من دول العالم على بيانات الاتصالات لرصد تطور الوباء والسيطرة على السكان.

وكان من المرجح أن يثير استخدام هذا النوع من البيانات توترا كبير بين الصالح العام ، والحرية الشخصية ؛ لذلك كان يجب اقامة توازن دقيق بين السلامة العامة والحق في الخصوصية[١].

في فرنسا تلقى العديد من المواطنين على أجهزة التليفون المحمول رسائل نصية قصيرة موقعة من الحكومة بخصوص تفشى الفيروس ، وقد اثار ذلك العديد من التساؤلات عن وضع الدولة يديها على أرقام الهواتف المحمولة لجميع السكان؟ وهل كان هذا حقًا قانونيا ؟[٢].

من المناسب الإجابة على هذا السؤال بشكل لا لبس فيه بالإيجاب ؛ لأن هذا الإرسال كان يشكل إحدى الطرق الممكنة للدولة للوفاء بالتزامها القانوني، باعتبارها الضامن للأمن المدني على المستوى الوطني.

---

[1]- Paige Backman and Stephanie D'Amico, op cit. no.1

[2] Yoann Gonthier Le Guen. La protection des données personnelles en situation de crise sanitaire exceptionnelle : L'hypothèse du traçage géographique des citoyens à fin de lutte épidémique. Revue des droits et libertés fondamentaux, 2020, pp.chron. n° 27. halshs-0254107 p.1

٩- الجوانب القانونية لتقنية تحديد الموقع الجغرافي

الحقيقة أنه على الرغم من أن هذا التصرف قد يبدو تدخليا إلا أنه لا يشكل أي تهديد للخصوصية حيث يقوم مشغلو الهاتف بناءً على أوامر من الدولة ، ووفقًا لما يقتضيه القانون بإرسال رسالة إلى جميع مشتركيهم دون الحاجة إلى نقل بياناتهم إلى السلطات العامة[١].

كما أن المفوضية الأوروبية طلبت من مشغلي الهاتف ، بما في ذلك أورانج فرنسا توصيل بيانات مجمعة من أجل التحقق من الامتثال لتدابير الاحتواء وتوقع ذروة الفيروس[٢].

٢: **تحديد بيانات الموقع ومكافحة الجائحة** : الحل الأخر الذى أخذت به الكثير من الدول الأسيوية ، والأوربية كان حلا تكنولوجيا أكثر إثارة للقلق من وجهة نظر الحق في احترام الحياة الخاصة ، وهو مكافحة الجائحة عن طريق بيانات تحديد الموقع الجغرافي ، بتتبع حركات كل شخص ليلا ، ونهارا طالما أن هاتفه المحمول معه ، وقيد التشغيل[٣].

رأى مجلس حماية البيانات الأوروبي أن اتجاه الحكومات ، والجهات الفاعلة الخاصة نحو استخدام الحلول القائمة على البيانات كجزء من الاستجابة لجائحة COVID-19 يثير العديد من المخاوف المتعلقة بالخصوصية.

---

[1] - Art. L. 33 1, V. CPCE
[2] - Yoann Gonthier Le Guen op cit. p.3.
[3]- Paige Backman and Stephanie D'Amico, op cit. no.1

كما أكد أن الإطار القانوني لحماية البيانات صُمم ليكون مرنًا ، وبالتالي فهو قادر على تحقيق استجابة فعّالة في الحد من الوباء ، وحماية حقوق الإنسان ، والحريات الأساسية ، ولأن الفيروس لا يعرف حدودًا يبدو من الأفضل تطوير نهج أوروبي مشترك استجابة للأزمة ، أو على الأقل وضع إطار عمل مترابط[١].

في فرنسا ظهرت وسائل الاعلام التي كانت تنصب نفسها على أنها الرقيب على الديمقراطية ، إلا إنها مع ذلك دافعت عن استخدام التتبع الجغرافي للمواطنين لأغراض مكافحة الأوبئة ، على الرغم من أن هذه الممارسة فيها انتهاكات خطيرة للخصوصية ؛ مبررة ذلك بأن ذلك الحل تم تنفيذه بالفعل في عدد من البلدان الآسيوية مثل الصين تايوان وسنغافورة[٢].

على الصعيد العالمي تم استخدام بيانات شركات الاتصالات المتنقلة بمجموعة من الطرق المختلفة لدعم جهود السلطات الصحية لمكافحة فيروس كورونا (COVID-19)[٣].

بشكل عام استخدمت بيانات تحديد الموقع الجغرافي لضمان الامتثال لبروتوكولات الحجر الصحي ، والتباعد الاجتماعي، وللمراجعة بأثر رجعي لتحركات أولئك الذين

[1]- The European Data Protection Board: Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak, Adopted on 21 April 2020 p.3

[2] - Yoann Gonthier Le Guen op cit. p.3

[3] - Paige Backman and Stephanie D'Amico, op cit. no.2

ثبتت إصابتهم بالفيروس ؛ من أجل منع انتشاره في المجتمع ، وليتم تقديم تنبيهات في الوقت الفعلي للأشخاص القريبين من شخص ثبتت إصابته بالفيروس[١].

في هذه الحالة فإن السؤال الذي يطرح نفسه من منظور قانوني هو ما إذا كان ينبغي اعتبار هذه المعلومات بيانات شخصية بموجب اللائحة الأوربية العامة لحماية البيانات(GDPR) ؟

إن اللائحة الأوروبية تطبق فقط على معالجة البيانات الشخصية[٢]، وتشكل البيانات الشخصية المعلومات المتعلقة بشخص محدد ، أو يمكن التعرف عليه ، بشكل مباشر ، أو غير مباشر بالرجوع إلى معرف[٣].

المعلومات المتعلقة بتحديد الموقع الجغرافي لشخص ، أو معدات تابعة له تشكل بلا شك بيانات شخصية ؛ ذلك أن اللائحة العامة لحماية البيانات تعتبر بيانات الموقع بمثابة معرف ؛ لذلك فإن المعلومات المتعلقة بالشخص الذي يمكن تحديد هويته بالرجوع إلى المعرف تشكل بيانات شخصية.

[١] – شوهدت بعض الاستخدامات الأكثر تطرفًا لبيانات تحديد الموقع الجغرافي في الصين، حيث يتم تقييد وصول المواطنين إلى نقاط التفتيش بناءً على رمز الاستجابة السريعة القائم على اللون والذي يتوافق مع الحالة الصحية للشخص.

Paige Backman and Stephanie D'Amico, op cit. no.2

[2] - Art. 2 du RGPD

[3] - Art. 4 (1) du RGPD

إن حماية البيانات الشخصية من خلال حماية المعلومات المتعلقة بالمكان تشكل على وجه الخصوص في فترة الأزمة دعما ضروريا ؛ لضمان الحقوق والحريات الأساسية الأخرى بما في ذلك حرية التنقل ، أو الحق في الحياة العائلية.

نظرًا لأنه من المفترض أن يكون الجميع في المنزل خلال هذه الفترة ، فلا يبدو أن بيانات الموقع يمكن إخفاء هويتها إذا تمت معالجتها بشكل فردي[١].

في الواقع ومن خلال ربط البيانات من قوائم المشتركين في شبكة الهاتف مع تلك الموجودة في قاعدة العناوين الوطنية ، فمن السهل جدًا تحديد هوية الفرد بناءً على موقعه الجغرافي ، على الأقل بالنسبة لأولئك الذين يشغلون مسكنًا فرديًا.

كما أن هذه المعالجة ستكشف عن العديد من البيانات الحساسة ، من خلال معرفة الأماكن ، والأفراد الذين يترددون عليها بالإضافة إلى المدة المرتبطة بهذه الاتصالات والتي من المرجح أن يكشف جمع الموقع الجغرافي للشخص في الوقت الفعلي عن ميوله الجنسية ، أو انتمائه السياسي ، أو النقابي ، أو الديني[٢].

إن البيانات الصحية تنتمى لطائفة البيانات الحساسة ، ومن المناسب التذكير بما يشكل أحد الأحكام الأساسية في اللائحة العامة لحماية البياناتت ، وهو حظر معالجة البيانات الحساسة من حيث المبدأ[٣] ، ومع ذلك يوفر النص للدول مجالًا

[1] - Yoann Gonthier Le Guen op cit. p.4.
[2]- Yoann Gonthier Le Guen op cit. p.6- CJEU Oct. 6, 2020, La Quadrature du Net, nos . C-511/18, C-512/18 and C-520/18.
[3] Yoann Gonthier Le Guen op cit. p.6 - REGULATIONS REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE

للمناورة ويعترف بالاستثناءات حيث يمكن معالجة البيانات الصحية في حال الموافقة من صاحب البيانات ، أو في حال سيادة المصالح العليا ، والتي تتوافر في حال كانت المعالجة ضرورية لأسباب تتعلق بالمصلحة العامة في مجال الصحة العامة[١]، أو عندما تسعى إلى تحقيق أغراض متعلقة بالصحة عندما يكون ذلك ضروريًا لتحقيق هذه الأغراض لصالح الفرد والمجتمع ككل[٢].

٣: **مشروعية معالجة بيانات الموقع:** بهذا المعنى وبصراحة تامة تعترف اللائحة الأوروبية بمشروعية المعالجة المطبقة لرصد الأوبئة وانتشارها[٣] ، وكذلك إمكانية الانتقاص من الحقوق المنصوص عليها في هذا النص في فرضية التهديدات الصحية الخطيرة العابرة للحدود[٤]، وبالتالي يمكن تنفيذ المعالجة المتوخاة من قبل السلطة العامة دون الحاجة إلى موافقة الأشخاص المعنيين ، والتي تجد أساس مشروعيتها في تنفيذ مهمة ذات مصلحة عامة ، أو تتعلق بممارسة السلطة العامة المنوطة بالمراقبة بشرط النص على ذلك بنص قانوني[٥].

COUNCIL- Art. 9 (1) RGPD- Considérant 51 du RGPD of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the freemovement of such data, and repealing Directive 95/46/EC

[1] - Art. 9 (2) du RGPD - Considérant 52 du RGPD - preamble to the GDPR 54

[2] - Art. 9 (2) du RGPD - Considérant 53 du RGPD

[3] - Art. 9 (2) du RGPD - Considérant 46 du RGPD

[4] - Art. 9 (2) i du RGPD

[5] - Art. 6, e. du RGPD

إن مثل هذا الاستخدام للبيانات الوبائية التي يتم حقنها عند الضرورة في أنظمة المعلومات الجغرافية ليس جديدًا ، مع ذلك يبدو أن الحل الوحيد لإخفاء الهوية يتعلق بعدم توصيل البيانات الناتجة عن تحديد الموقع الجغرافي في صورة فردية ، وإنما في صورة بيانات مجمعة ، والتي تم تأكيد عدم الكشف عن هويتها من قبل المشرف الأوروبي على حماية البيانات.

كما أنها لا تشكل مشكلة قانونية ؛ لأن البيانات مجهولة المصدر تفقد طابعها الشخصي مما يجعل النصوص المتعلقة بحماية الحياة الخاصة غير قابلة للتطبيق[١].

وتؤكد هيئة حماية البيانات الأوروبية أنه عندما يتعلق الأمر باستخدام بيانات الموقع يجب إعطاء الأفضلية دائمًا لمعالجة البيانات المجهولة الهوية بدلاً من البيانات الشخصية[٢].

يجب أن يتجاوز إخفاء الهوية مجرد إزالة أرقام الهواتف وأرقام تعريف محطات الهاتف المحمول (IMEI) من جميع البيانات المرسلة ، ويجب أن تمنع التقنية المستخدمة بشكل لا رجعة فيه من تحديد هوية الأشخاص[٣].

ويشير إخفاء الهوية إلى استخدام مجموعة من التقنيات من أجل إزالة القدرة على ربط البيانات بشخص طبيعي محدد ، أو قابل للتحديد مقابل أي جهد معقول[١].

[1] - Yoann Gonthier Le Guen op cit. p.5

[2] - Comité européen de la protection des données, Statement on the Processing of Personal Data in the Context of the Covid-19 Outbreak 2020 p.2.

[3] - Ibid - Groupe de travail «Article 29», Avis 5/2014 sur les techniques d’anonymisation (2014), p. 7.

٩- الجوانب القانونية لتقنية تحديد الموقع الجغرافي

الواقع أن مجموعة كبيرة من الأبحاث أظهرت أن بيانات الموقع التي يُعتقد أنها مجهولة الهوية قد لا تكون كذلك. في الحقيقة إن آثار تنقل الأفراد بطبيعتها مترابطة للغاية وفريدة من نوعها ، وبالتالي يمكن أن تكون عرضة لمحاولات إعادة التعريف في ظل ظروف معينة. فلا يمكن إخفاء هوية نمط بيانات شخص يتم تتبع موقعه على مدى فترة زمنية طويلة[٢].

لتحقيق إخفاء الهوية يجب معالجة بيانات الموقع بعناية ؛ من أجل تلبية اختبار المعقولية. بهذا المعنى، تتضمن هذه المعالجة النظر في مجموعات بيانات الموقع ككل، فضلاً عن معالجة البيانات من مجموعة كبيرة ، إلى حد معقول من الأفراد باستخدام تقنيات إخفاء الهوية القوية والمتاحة شريطة تنفيذها بشكل مناسب وفعال[٣].

كما سبق القول فإنه إذا كانت مكافحة فيروس كورونا هدف قيم تتقاسمه جميع الدول ، وبالتالي ينبغي دعمه بأفضل طريقة ممكنة ؛ ذلك أن من مصلحة البشرية الحد من انتشار الأمراض ، إلا أنه ينبغي التأكيد على أنه ، حتى في هذه الأوقات الاستثنائية ، يجب على مراقب البيانات والمعالج ضمان حماية البيانات الشخصية لأصحاب البيانات ، وضرورة مراعاة أن أي إجراء يتم اتخاذه في هذا السياق يجب أن يحترم المبادئ العامة للقانون ، وألا يكون رجعيا[٤].

---

[1] - The European Data Protection Board: Guidelines 04/2020 op cit. p.5
[2]- The European Data Protection Board: Guidelines 04/2020 op cit. p.6
[3] - Ibid
[4] - Comité européen de la protection des données, Statement on the Processing of Personal Data in the Context of the Covid-19 Outbreak 2020 p.1.

كان لدى مجلس حماية البيانات الأوروبي اعتقادًا راسخًا أنه عندما تكون معالجة البيانات الشخصية ضرورية لإدارة جائحة كوفيد–١٩ ، فإن حماية البيانات أمر لا غنى عنه لبناء الثقة وخلق الظروف للقبول الاجتماعي لأي حل ، وبالتالي ضمان فعالية هذه التدابير[١].

كما أن البيانات والتكنولوجيا المستخدمة للمساعدة في مكافحة كوفيد–١٩ يجب استخدامها لتمكين الأفراد ، وليس للسيطرة عليهم ، أو وصمهم ، أو قمعهم ، وعلاوة على ذلك، فإن البيانات والتكنولوجيا يمكن أن تكون أدوات مهمة ، إلا أنها مقيدة بقيود جوهرية ويمكنها فقط الاستفادة من فعالية تدابير الصحة العامة الأخرى.

يجب أن تسترشد أي تدابير تتخذها الدول الأعضاء و مؤسسات الاتحاد الأوروبي التي تتضمن معالجة البيانات الشخصية لمكافحة كوفيد–١٩ بالمبادئ العامة للفعالية والضرورة ، والتناسب.

توضح هذه المبادئ التوجيهية الشروط ، والمبادئ للاستخدام المتناسب لبيانات الموقع ، وأدوات تتبع المخالطين لغرضين محددين : استخدام بيانات الموقع لدعم الاستجابة للجائحة من خلال نمذجة انتشار الفيروس ؛ لتقييم الفعالية الإجمالية لتدابير الاحتجاز ، وتتبع المخالطين، والذي يهدف إلى إخطار الأفراد بحقيقة أنهم كانوا على مقربة من شخص تم تأكيد إصابته بالفيروس ؛ من أجل كسر سلاسل التلوث في أقرب وقت ممكن[٢].

[1] - The European Data Protection Board: Guidelines 04/2020 op cit. p.3
[2] - The European Data Protection Board: Guidelines 04/2020 op cit. p3

٩- الجوانب القانونية لتقنية تحديد الموقع الجغرافي

علاوة على ذلك يجب أن تكون المعالجة متناسبة تمامًا مع المخاطر الصحية المتكبدة ومناسبة لظروف الزمان والمكان[١]. بالإضافة إلى ذلك فيما يتعلق بمبدأ تقييد الغرض يجب أن تكون الأغراض محددة بما يكفي لاستبعاد المعالجة الإضافية لأغراض غير ذات صلة بإدارة أزمة الصحة COVID-19 (على سبيل المثال، الأغراض التجارية ، أو إنفاذ القانون).

بمجرد تحديد الهدف بوضوح سيكون من الضروري التأكد من أن استخدام البيانات الشخصية مناسب وضروري ومتناسب[٢].

كذلك لا ينبغي استخدام الأزمة الصحية كفرصة لإنشاء تفويضات غير متناسبة للاحتفاظ بالبيانات ويجب أن يأخذ حد التخزين في الاعتبار الاحتياجات الحقيقية والأهمية الطبية (قد يشمل ذلك الاعتبارات ذات الدوافع الوبائية مثل فترة الحضانة، وما إلى ذلك)

علاوة على ذلك يجب إنهاء المعالجة دون تأخير عندما لا تصبح ضرورية[٣]. كما أن الاحتفاظ بالبيانات الشخصية مرتبط فقط بمدة أزمة COVID-19. بعد ذلك كقاعدة عامة يجب محو جميع البيانات الشخصية أو إخفاء هويتها[٤].

كذلك فإن حث الإدارة على زيادة تنفيذ التدابير ، أو الوسائل المناسبة في فترة الوباء يمكن أن يكون موضوع دعوى أمام القضاء ، حيث أمرت المحكمة العليا الفرنسية

---

[1] - Yoann Gonthier Le Guen op cit. p.8
[2]- The European Data Protection Board: Guidelines 04/2020 op cit. p.7.
[3] - Yoann Gonthier Le Guen op cit. p.8.
[4] - The European Data Protection Board: Guidelines 04/2020 op cit. p.8

الحكومة مؤخراً بزيادة التدابير التي تقيد الحرية ، وهكذا اختار القضاء إعطاء الأولوية لحماية الصحة العامة – وبالتالي الحق في الحياة – بدلاً من حرية القدوم ، والذهاب[١].

في احدى الدعاوي القضائية كان تنفيذ التدابير أو الوسائل المناسبة لمجابهة وباء كورونا(COVID-19) موضوع دعوى أمام القضاء ، وهذا يعد انقلاب للنموذج السائد حيث طلبت نقابة الأطباء الشباب من قاضي مجلس الدولة الفرنسي إجراءات مستعجلة بأن يأمر الوزير الأول ، ووزير التضامن والصحة بالإعلان عن الحجر الصحي الكلي للسكان من خلال تنفيذ تدابير تهدف إلى الحظر الشامل على الخروج ، مع إيقاف وسائل النقل العام ، ووقف الأنشطة المهنية غير الحيوية (الغذاء، الماء، الطاقة، المجالات السيادية) وإنشاء الإمدادات الغذائية للسكان في ظروف صحية تهدف إلى ضمان سلامة الموظفين المسؤولين عن هذه الإمدادات.

وقد قبلت المحكمة الطلب ، وأمرت الحكومة بزيادة التدابير التي تقيد الحرية ، وهكذا اختار القضاء إعطاء الأولوية لحماية الصحة العامة – وبالتالي الحق في الحياة – بدلاً من حرية القدوم ، والذهاب[٢].

و لضمان المساءلة ينبغي تحديد الجهة المسؤولة عن أي تطبيق لتتبع المخالطين. ترى هيئة حماية البيانات الأوروبية أن السلطات الصحية الوطنية يمكن أن تكون الجهات المسؤولة عن مثل هذا التطبيق، ويمكن تصور جهات مسؤولة أخرى أيضًا.

[1] - Yoann Gonthier Le Guen op cit. p.8

[2]- Conseil d'État, Juge des référés, formation collégiale, 22/03/2020, 439674.

في كل الأحوال إذا كان نشر تطبيقات تتبع المخالطين ينطوي على جهات فاعلة مختلفة فيجب تحديد أدوارها ومسؤولياتها بوضوح منذ البداية ، وشرحها للمستخدمين[١].

المطلب الثالث

تحديد الموقع الجغرافي والأعمال التجارية

تمهيد : تطورت المساعدة البسيطة لتحديد الموقع الجغرافي والملاحة تدريجيًا ، خاصة مع تطور الويب ليتم دمجها في منصات برمجية قادرة على معالجة التدفقات الهائلة من البيانات وربط مجموعة من الوظائف[٢].

لكن بشكل عام سندرك بسرعة أن تحديد الموقع الجغرافي أصبح الآن موجودًا في الحياة اليومية لكل شخص لأسباب مهنية وشخصية على حد سواء ، وأن مجالات تطبيقه الواسعة بشكل متزايد ستجعله على الأرجح أحد الأدوات الأساسية التي يجب أن تمتلكها أي شركة[٣].

في السياق الاقتصادي العالمي الحالي لكي تظل الشركات قادرة على المنافسة ليس لديها خيار آخر سوى تحسين نشاطها ، وجميع العمليات المتأصلة فيها قدر الإمكان.

---

[1] - The European Data Protection Board: Guidelines 04/2020 op cit. p.7.

[2] - Livre blanc,Géolocalisation , Comment la géolocalisation améliore-t-elle la productivité globale de l'entreprise ? **Masternaut** , Novembre 2010 p.8. https://www.masternaut.com

[3]- Livre blanc,Géolocalisation op cit p.6

يتعلق هذا التحسين الذي يهدف قبل كل شيء إلى تحسين الربحية ، والآليات التنظيمية بالموارد البشرية والمادية ، وعلى جميع مستويات الشركة.

في السنوات الأخيرة تم تحديد الموقع الجغرافي تدريجيًا، وأصبح اليوم أحد الروابط المركزية في الإدارة والتنظيم اليومي للنشاط[١].

في إطار علاقة الأعمال التجارية مع المستهلك تستفيد الشركات من جانبها إلى حد كبير من تقنيات تحديد الموقع الجغرافي ؛ لتقديم منتجاتها وخدماتها على أساس القرب من العميل المحتمل[٢].

يسلط تقارب المستهلكين العالميين ونمط الحياة المتقارب الضوء على أن المستهلكين على عكس كل التوقعات يتسامحون بشكل متزايد مع استغلال بياناتهم الشخصية مما يوفر فرصًا جديدة لجميع اللاعبين الاقتصاديين[٣].

سوف نتطرق في هذا المطلب لدراسة تحديد الموقع الجغرافي كأداة تسويقية ، على أن يعقبه دراسة تحديد الموقع الجغرافي والشركات ، ثم دراسة تحديد الموقع الجغرافي وخصوصية المستهلك.

١: تحديد الموقع الجغرافي كأداة تسويقية : بدأت الشركات في إدراك الفوائد والفرص التي يمكن أن تقدمها تطبيقات ، وخدمات تحديد الموقع الجغرافي كأدوات تسويقية:

---

[1] - Livre blanc,Géolocalisation op cit p.3.

[2] - A p.25

[3] - Goncalves, Lucie & de Pechpeyrou, Pauline & Benavent, Christophe. (2014). JUSQU'OÙ LES CONSOMMATEURS ACCEPTENT-ILS D'ÊTRE GÉOLOCALISÉS ? REVUE FRANÇAISE DU MARKETING - Septembre 2014 - N° 248 - 3/5 p.28.

٩- الجوانب القانونية لتقنية تحديد الموقع الجغرافي

فهي تسمح للشركات بتقديم إعلانات وخدمات أكثر استهدافًا لعملائها، حيث تقوم الشركات بإصدار خصومات على أساس الموقع ، وعروض خاصة للعملاء الجدد والحاليين وبالتالي زيادة التفاعل والتحويل[١].

توفر الشعبية المتزايدة للجيل الجديد من الهواتف الذكية المجهزة بخدمات تحديد الموقع الجغرافي فرصًا جديدة للمسوقين للوصول إلى المستهلكين استنادًا إلى موقعهم[٢].

نعلم أن هواتفنا الذكية هي أدوات تجسس رائعة نأخذها معنا في كل مكان. تتيح دراستها معرفة عادات أسلوب حياتنا ، واهتماماتنا، وهواياتنا، وأسفارنا، وما إلى ذلك. وكما كان متوقعًا فإن الاهتمام بهذه الجوهرة التكنولوجية لا يهم أجهزة المخابرات العالمية فحسب بل أيضًا المسوقين الذين سارعوا إلى استغلال هذا المخزون الجديد من الذهب الأسود للقرن الحادي والعشرين . ذلك أن الهواتف الذكية مليئة بالتطبيقات وكل منها يقوم بمعالجة البيانات الخاصة به[٣].

يرتبط كل هاتف ذكي برقم معرف فريد للتعرف على مستخدمه ، وقد سمحت هذه المعرفات للمطورين بإجراء اختبارات على التطبيقات ، وتحديد الحوادث المحتملة قبل وضعها في الإنتاج على المتجر.

---

[1]- PLC Media, Geo-location apps, privacy and data protection by , Published on 22-Aug-2012 https://uk.practicallaw.thomsonreuters.com › contextDat.

[2] - Goncalves, Lucie & de Pechpeyrou, Pauline & Benavent, Christophe. op cit p28.

[3] - Gérard HAAS et Florian, PERRETIN RGPD : Géolocalisation et Marketing, une question de consentement! https://www.haas-avocats.com

لكن حقيقة أن هذه المعرفات الفريدة مشتركة بين جميع التطبيقات تمنحها قيمة نادرة وثمينة ، ومن خلال الإسناد الترافقي للبيانات يمكن معرفة نوع التطبيقات التي تم استخدامها ، أو يستخدمها هذا الشخص ، أو ذاك وبالتالي عزلها ضمن فئة مستهدفة. سنتمكن بعد ذلك من التمييز بين المراهق المعرض لحب الشباب ، والمحب لتطبيقات الألعاب عبر الإنترنت ، وبين الثلاثيني الذي يبحث دائمًا عن مطعم جيد[١].

جميع الجهات الفاعلة اليوم – بما في ذلك المنظمات غير الربحية – تقوم بشكل روتيني بجمع ، واستخدام المعلومات الخاصة بعملائها ، ومستقبليها.

مع ذلك، إذا كان موقعنا قد اعتبر في السابق العنوان البريدي لنا ، فقد أصبح اليوم موقعًا في الوقت الفعلي يمكن استخدامه لصياغة عرض ملائم وموجه[٢].

تساعد إعلانات الهاتف المحمول المستندة إلى الموقع على إزالة الحواجز الجغرافية والمعلوماتية بين المستهلكين وعروض الأعمال ، من خلال الوصول إلى المتسوقين عندما يكونون بالقرب من مواقع التجار[٣].

٢: تحديد الموقع الجغرافي والشركات: يستهدف تحديد الموقع الجغرافي جميع أنواع الشركات ، طالما أن تحسين نشاطها يتطلب مراقبة البضائع ، أو الأشخاص في الوقت الفعلي.

[1] - Gérard HAAS et Florian, op cit
[2] - Goncalves, Lucie & de Pechpeyrou, Pauline & Benavent, Christophe. op cit p28
[3] - Goncalves, Lucie & de Pechpeyrou, Pauline & Benavent, Christophe. op cit p28

٩- الجوانب القانونية لتقنية تحديد الموقع الجغرافي

لكن نظرا للاستثمارات التي تنطوي عليها فإن تحديد الموقع الجغرافي قد أثبت بسرعة أنه يشكل أولوية بالنسبة لقطاعات معينة من النشاط ، في حين سيظل ثانويا ؛ لأنه لا يفعل الكثير لتحسين ربحية بعض المهن[١].

بخصوص أساطيل المركبات التجارية هناك بشكل أساسي أربع قطاعات رئيسية من النشاط تتعلق بشكل مباشر بتحديد الموقع الجغرافي وإدارة الأسطول: الفنيون (الصيانة، خدمة ما بعد البيع، وما إلى ذلك)، والتسليم والنقل (البضائع، والأشخاص، وما إلى ذلك) والمركبات والمعدات الخاصة (البناء والتنظيف والإصلاحات) ، و قوى المبيعات.

بالنسبة لهذه القطاعات يعد تحديد الموقع الجغرافي أمرًا ضروريًا ؛ لأنه يحتل جزءًا مهمًا من الإدارة اليومية للنشاط ، ويصبح رابطًا مركزيًا في الشركة.

بالنسبة لهذه المهن فإن مراقبة المهام ، ومراقبة البضائع ، وإدارة الوقت ، وحساب الطرق المثلى هي جميعها وظائف ناتجة مباشرة عن حلول تحديد الموقع الجغرافي والتي أصبحت ضرورية اليوم من حيث تنظيم النشاط ، وتحسين إنتاجية الشركة[٢].

يعد تحديد الموقع الجغرافي الاحترافي قبل كل شيء وسيلة لتحسين النشاط ، بدءًا من إنشاء منتج ، أو خدمة حتى تقديمها إلى العميل النهائي.

[1]- Livre blanc,Géolocalisation op cit p.5
[2] - Livre blanc,Géolocalisation op cit p.5

يتمثل التحدي الأول المتأصل في تحديد الموقع الجغرافي في الحصول على معلومات في الوقت الفعلي ، أو في فترة زمنية قصيرة جدًا عن موقع الممتلكات ، أو الأشخاص ، أو المركبات.

بالتالي فإن المعلومات هي أساس تحديد الموقع الجغرافي، أو بالأحرى هذا التدفق المستمر للمعلومات بين المقر الرئيسي للشركة ومواردها المتنقلة هي التي ستسمح لها بإدارة النشاط في الوقت الفعلي، وتعديله وفقًا لتطوره ساعة بساعة ، أو حتى دقيقة بدقيقة.

منذ ذلك الحين أصبح من الممكن للشركات أن تتفاعل بشكل فوري من خلال التنبيهات الآلية، والمجدولة لجميع أشكال الأحداث غير المتوقعة ، والتأخيرات ، وتقليل ، أو حتى القضاء على تأثيرها على السلسلة بأكملها.

هذه الاستجابة السريعة ستساعد الشركات على أساس يومي سواء في تنظيمها ، أو في إدارتها للمهنة ، وأيضًا في العلاقة التي تحافظ عليها مع عملائها أو شركائها ، أو مقدمي الخدمات ، وباختصار مع جميع الجهات الفاعلة وعلى جميع المستويات[1].

إن القدرة البسيطة على معرفة وضعية الشخص ، أو السيارة (واستقراء حالته فيما يتعلق بيوم عمله) تجعل من الممكن متابعة أي نشاط مهني تلقائيًا ، بمساعدة منصات البرامج ، لتصحيحه إذا لزم الأمر ، أو تحسينه إن أمكن ، وذلك خلال فترات

[1]- Livre blanc,Géolocalisation op cit p.10

زمنية قصيرة للغاية مع تأثير فوري على جودة الخدمة الشاملة والخدمة المقدمة ، وفي نهاية المطاف على ربحية الشركة[١].

إن تحديد الموقع الجغرافي، سواء كان مدمجًا في منصة برمجية عبر الإنترنت ، أو في مقر الشركة ، أو حتى في شكل ملاحة على محطة متنقلة ، أو نظام تحديد المواقع العالمي (GPS) يسمح على سبيل المثال بتصور الشلل غير الطبيعي للسيارة.

من خلال الحصول على هذه المعلومات وإلقاء نظرة سريعة على الخريطة التي تظهر على الشاشة يمكن للمدير الرد على الفور ، وتنفيذ العمليات التي ستمكنه من التعويض عن أي تأخير يضر بالعميل.

كما يمكن مشاركة هذه المعلومات من تحديد الموقع الجغرافي ببساطة ، وبسرعة أولاً مع جميع الموظفين وصناع القرار في الشركة ، ومع مختلف الوكالات ، أو الشركات التابعة التي قد تشكلها ، أو حتى مع المقاولين من الباطن ، أو الشركاء الخارجيين.

يتمثل الهدف المذكور سابقا في تجميع البيانات وتبادلها ؛ من أجل توفير استجابة مشتركة للجهات الفاعلة في السلسلة ، وبالتالي تحسين الإنتاجية والربحية[٢].

بالنسبة العملاء تتيح أدوات تحديد الموقع الجغرافي لهم تقديم خدمات مخصصة لهم مرتبطة بالتوفير الأولي للشركات. سواء كانت رسائل ، أو تنبيهات ، أو تقارير يتم

[1] - Ibid
[2] - Livre blanc, Géolocalisation op cit p.11

إرسالها إلى العملاء عبر قنوات اتصال مختلفة : رسائل البريد الإلكتروني ، والوصول الآمن إلى الويب ، والرسائل النصية القصيرة ، والرسائل التلقائية التي يتم عرضها على الشاشة وما إلى ذلك[١].

تعد أدوات تحديد الموقع الجغرافي أيضًا جزءًا من احترام البيئة. إلى جانب الجانب التشغيلي البحت ، والخدمة المقدمة للعملاء.

إن امتلاك تقنيات قادرة على تحديد الرحلات ، أو خطط الرحلات ، وتاريخها يوفر أيضًا إمكانية تقليل استهلاك الوقود ، وانبعاثات ثاني أكسيد الكربون. عن طريق تحسين المسارات على أساس القواعد ، والقيود بهدف القيام برحلات تستهلك أقل قدر ممكن من الوقود ، مما ينتج عنه تلوث أقل.

تتطلب هذه العمليات استخدام برامج محددة ، ولكنها تعتمد بشكل أساسي على القدرة على تحديد موضع المركبات ، وتتبع مساراتها التي يوفرها تحديد الموقع الجغرافي[٢].

من هذا التحسين للمسارات بهدف تقليل الكيلومترات الخارجية ، واستهلاك الوقود والانبعاثات الملوثة، يأتي أيضًا تحسين المركبات مع تقليل التآكل.

أخيرًا يلعب تحديد الموقع الجغرافي دورًا رئيسيًا في تأمين البضائع ، والأشخاص والمركبات. بفضل أدوات تحديد الموقع الجغرافي ، ولا سيما إشارات GPS أو SIM المدفونة في السيارة ، أو الملتصقة بالبضائع ، أو المدمجة في محطة متنقلة.

[1] - Ibid
[2]Livre blanc, Géolocalisation op cit p.11

تُمكن هذه الأدوات من العثور على سيارة مسروقة ، أو بضائع مفقودة ، أو حتى شخص في خطر ، وبحيث يتم إرسال بيانات تحديد الموقع هذه على الفور إلى خدمات إنفاذ القانون التي يمكنها بعد ذلك التدخل بسرعة[١].

٣: تحديد الموقع الجغرافي وخصوصية المستهلك : لا شك أن تطبيقات وخدمات تحديد الموقع الجغرافي ذات قيمة للمستهلكين ، والشركات على حدٍ سواء. مع ذلك فإن جمع معلومات الموقع ، وتخزينها يثير مخاوف تتعلق بالخصوصية.

نظرًا لأن الأفراد غالبًا ما يحملون أجهزتهم المحمولة معهم ، فقد يتم جمع بيانات الموقع في كل مكان ، وفي أي وقت ، وربما دون تفاعل المستخدمين ، أو معرفتهم[٢].

إن مفتاح القضايا المتعلقة بالخصوصية الناشئة عن تحديد الموقع الجغرافي هو إخفاء الهوية : على وجه التحديد ، ما إذا كانت بيانات الموقع يمكنها تحديد هوية الفرد شخصيًا، وإذا كان الأمر كذلك ، فما مدى حساسية هذه المعلومات. وقد تصف البيانات ما يفعله الشخص ، وأين يفعل ذلك مما قد يكشف عن الزيارات إلى وجهات حساسة مثل العيادات الطبية ، أو المحاكم ، أو التجمعات السياسية[٣].

كما أن حساسية معلومات الموقع تعرضها لخطر سوء الاستخدام من قبل الشركات والحكومات. يمكن أن تكشف بيانات الموقع عن دين الفرد ، وحياته الجنسية وانتماءاته السياسية ، وصحته ، وكلها يمكن اعتبارها بيانات شخصية حساسة.

---

[1] - Livre blanc, Géolocalisation op cit p.12
[2] - PLC Media, Geolocation apps, privacy and data protection op cit
[3]- Ibid..

إذا كان مفهوم الخصوصية متعدد الأبعاد ، فإن الخصوصية المعلوماتية تعطى الفرد الحق في تحديد كيف ، ومتى ، وإلى أي مدى يمكن نقل المعلومات المتعلقة به إلى شخص ، أو منظمة أخرى[١].

يتم تصور فقدان الخصوصية في سياق التجارة في كل مكان من ناحيتين: من ناحية يمكن تتبع المستهلكين بشكل مستمر ، ومن ناحية أخرى يمكن بسهولة نشر المعلومات ، أو استخدامها[٢].

إن وسائل المعلومات ، والتحكم من قبل المستخدمين محدودة. بل ويمكن أن تكون غير موجودة في تطبيقات الأجهزة المحمولة الذكية . كما أن المستخدم قد يكون على علم بأن العديد من الجهات الفاعلة الاقتصادية تشارك عند استخدام التطبيق ، إلا أن هذه الجهات الفاعلة تظل غير مرئية بالنسبة له[٣].

رغم ذلك فإن من مفارقات الخصوصية أن هناك فجوة واضحة بين المخاوف المعلنة ، والسلوكيات الفعلية ، والتي ستقودنا إلى التساؤل عن العوامل التي تؤدي إلى قبول أكبر من قبل المستهلكين للتطفل على خصوصياتهم ؟.

من الممكن أن تتعرض الخصوصية للتهديد في عالم حيث يعتبر بعض مستخدمي الإنترنت ، الذين نشأوا في بيئة قانونية ، أنه من الطبيعي المطالبة بالشفافية الكاملة.

[1] - Goncalves, Lucie & de Pechpeyrou, Pauline & Benavent, Christophe. op cit p.29
[2]- Ibid
[3] - M. Henri BarbIerk, op, cit. p..57-58.

٩- الجوانب القانونية لتقنية تحديد الموقع الجغرافي

فإذا لم يكن لدي ما أخفيه ، فلماذا لا أتقبل أن الآخرين، سواء كانوا أصدقاء ، أو علامات تجارية يمكنهم دائمًا معرفة مكاني ومع من أتحدث[١].

مع ذلك فكلما زاد اهتمام المستهلكين بخصوصيتهم قل قبولهم للخدمات القائمة على تحديد الموقع الجغرافي ، وكلما زاد استخدام المستهلك لعدد كبير من الميزات على هواتفه الذكية كلما زاد قبوله للخدمات القائمة على تحديد الموقع الجغرافي[٢].

يشير مفهوم الخصوصية إلى الموافقة الحرة للفرد للسماح للأفراد ، والعلامات التجارية ، والشركات الأخرى بالوصول إلى المساحة التي يعتبرها خاصة.

لذلك يجب على جميع الشركات والتطبيقات أن تلتزم بمعالجة جميع البيانات المتعلقة بتحديد الموقع الجغرافي ، وأن تحصل على موافقة مسبقة من صاحب البيانات[٣].

ويجب أن تكون هذه الموافقة تعبيرًا حرًا ، ومحددًا ، ومستنيرًا لا لبس فيه عن الإرادة التي يقبل من خلالها صاحب البيانات – من خلال إعلان ، أو من خلال عمل إيجابي واضح – خضوع بياناته الشخصية للمعالجة.

في ١٩ يوليو ٢٠١٨، أصدرت CNIL إشعارًا رسميًا إلى شركتي FIDZUP وTEEMO – كانت الشركتان تقومان بإثراء البيانات التي تقوم بشرائها من خلال الارتباطات مع قواعد بيانات أخرى ، ثم تعيدا بيعها إلى شركة ثالثة – لقيامهما بجمع ومعالجة بيانات تحديد الموقع الجغرافي من الهواتف الذكية لمستخدميهم دون الحصول

[1]- Goncalves, Lucie & de Pechpeyrou, Pauline & Benavent, Christophe. op cit p.29

[2] - Goncalves, Lucie & de Pechpeyrou, Pauline & Benavent, Christophe. op cit p.31 et 32

[3] - Gérard Haas et Florian, op cit

على موافقتهم بالمعنى المقصود في اللائحة العامة لحماية البيانات ، وقانون حماية البيانات، حيث كانتا تقومان بتسويق المحطات الطرفية الموجودة في المتاجر والتي تستخدم معرفات الإعلانات هذه ؛ لاكتشاف متى يمر مستخدم الإنترنت بالقرب من المتجر. كما قاموا أيضًا بتخزين بيانات تحديد الموقع الجغرافي لفترة طويلة جدًا (ثلاثة عشر شهرًا) هذا الاحتفاظ بهذه المعلومات يشكل خطر انتهاك خصوصية الأشخاص المعنيين.

ترى CNIL أن التسويق المستهدف غير محظور ، بل هو وقود الاقتصاد الرقمي الذي يتطلب بشكل متزايد البيانات الشخصية مع تطور تحديد الموقع الجغرافي[1].

في هذه الحالة كان الحصول على موافقة صالحة هو ما ينقص بشكل أساسي للأسباب الأتية :

بالنسبة إلىTEEMO لم يتم إبلاغ الأشخاص المعنيين عند تنزيل تطبيقات الهاتف المحمول بأنه من الممكن جمع بيانات موقعهم.

بالنسبة إلىFIDZUP فإن المعلومات المقدمة للمستخدمين في شروط وأحكام التطبيق أو على شاشات العرض في المتجر لم تحدث إلا بعد جمعها.

[1] - CNIL un rapport public sur ces différentes techniques de publicité ciblée en ligne, sur leurs risques d'atteintes à la vie privée et les parades possibles. 17 novembre 2010.

بالإضافة إلى ذلك لم يتم إبلاغ المستخدمين بالغرض الإعلاني المستهدف من المعالجة المنفذة ، ولا بهوية مراقب البيانات ؛ لأن هاتين المعلومتين إلى جانب حقوق الأشخاص تعد معلومات أساسية وفقًا لـ CNIL والتي يجب العثور عليها في كل ذكر للمعلومات.

كذلك عدم وجود طبيعة محددة للموافقة على الرغم من مطالبة المستخدمين بالموافقة على استخدام بيانات تحديد الموقع الجغرافي الخاصة بهم بواسطة تطبيق الهاتف المحمول إلا أنه لم يتم الحصول على موافقتهم على استخدام هذه البيانات لأغراض استهداف الإعلانات ، وكان يتعين على FIDZUP و TEEMO الحصول على موافقة إضافية ؛ لجعل جمع بيانات تحديد الموقع الجغرافي قانونيًا.

كما فرضت CNIL عقوبات على TEEMO لتنفيذها فترة الاحتفاظ بالبيانات لمدة ١٣ شهرًا وهو ما يتوافق مع فترة الاحتفاظ المطبقة على ملفات تعريف الارتباط وليس على بيانات تحديد الموقع الجغرافي[١].

في حين تعتبر مجموعة الـ ٢٩ بيانات الموقع شخصية للغاية ويجب أن يكون الاحتفاظ بهذه البيانات محدودًا للغاية ، ولا تزيد عن الوقت اللازم للأغراض التي تم جمع البيانات من أجلها[٢] ؛ لذلك يتعين على مراقب البيانات تحديد فترة الاحتفاظ

[1] - Gérard HaaS et Florian, op cit
[2] - Groupe de l'article 29 Avis n° 13/2011 sur les services de géolocalisation des appareils mobiles intelligents p.19.

بالبيانات الشخصية التي يجمعها بموجب المادة ٢٥ من اللائحة العامة لحماية البيانات.

في نهاية هذا المطلب نستطيع أن نرى بأن تحديد الموقع الجغرافي مستقبل مليء بالطموح الذي يصبح أكثر واقعية كل يوم.

بعد مرحلة توحيد تحديد الموقع الجغرافي والتي أصبحت اليوم راسخة في عادات الشركات ، يتجه اللاعبون في السوق نحو تطوير حلول مصممة خصيصًا ، ويمكن الوصول إليها بسهولة أكبر من أي وقت مضى من الناحية التقنية –لا سيما بفضل شبكة الإنترنت– وتتسم بالشفافية للمستخدمين.

يتم دمج تحديد الموقع الجغرافي مع أدوات برمجية للتحليل وإعداد التقارير في الوقت الفعلي ، أو اليومي ، هدفها بسيط وهو تزويد الشركات ببيانات استراتيجية يتم إنشاؤها بطريقة تستجيب على الفور لاحتياجاتها التشغيلية ؛ بهدف زيادة الإنتاجية ، وتحسين النشاط ، والذى يترتب علية بالطبع تحسين الربحية.

كذلك فإن تطورات تكنولوجيا المعلومات التي تركز على خدمات الويب وبوابات الإنترنت توفر لمديري الأعمال والمديرين إمكانية الوصول البسيط في كل مكان تقريبًا إلى البيانات من متصفح ويب بسيط في أي مكان تتوافر فيه وسائل التكنولوجيا.

خاتمة الدراسة

في ختام هذه الدراسة يمكن استخلاص النتائج التالية :

١: من خلال جهاز إلكتروني سيتمكن الشخص من تحديد موقعه في بيئته الحقيقية من خلال تفسير معلومات موقعه على خريطة جغرافية افتراضية.

تحديد الموقع الجغرافي هو عملية لتحديد موضع كائن ما على مخطط ، أو خريطة باستخدام إحداثياته الجغرافية تتم هذه العملية باستخدام محطة طرفية قادرة على تحديد موقعها ، ونشر إحداثياتها الجغرافية (خط العرض/خط الطول). يمكن تخزين المواقع المسجلة داخل المحطة ثم استخراجها لاحقًا ، أو نقلها في الوقت الفعلي إلى منصة برمجيات تحديد الموقع الجغرافي.

بشكل عام يشمل مصطلح بيانات الموقع أي معلومات تشير ضمنيًا ، أو صراحةً إلى الموقع الجغرافي ، أو المكاني.

٢: يوجد الكثير من تقنيات تحديد الموقع الجغرافي ، كما أنها ليست جميعها لها نفس الاستخدامات.

تختلف تقنية تحديد الموقع الجغرافي في الهواء الطلق عن تلك المستخدمة في الداخل ، تمامًا كما يتم استخدام تقنيات معينة في المناطق الريفية أكثر من المناطق الحضرية.

٣: من المهم التمييز بين الحالات التي تكون فيها بيانات الموقع تشكل إما بيانات شخصية ، أو بيانات حساسة (أي فئة خاصة من البيانات الشخصية) عن تلك

الحالات التي تكون فيها البيانات مجهولة المصدر بشكل فعال ، وبالتالي لا تعتبر بيانات شخصية ، أو حساسة.

٤: بيانات الموقع تأخذ بعدًا محددًا بشكل واضح في اللائحة العامة لحماية البيانات. من خلال جمع بيانات الموقع يستطيع مطورو التطبيقات ، أو الجهات الفاعلة الأخرى استنتاج أنواع عديدة من المعلومات الشخصية بصرف النظر عن مجرد الموقع ، مثل الانتماء الديني ، أو السياسي ، أو الهوية الجنسية.

من لحظة دمج بيانات تحديد الموقع الجغرافي مع البيانات الشخصية ستخضع المعالجة المتعلقة بها لنظام اللائحة العامة لحماية البيانات (GDPR) مع كل العواقب التي ينطوي عليها ذلك.

٥: يعد التزام الموافقة أحد الأسباب الشرعية لمعالجة بيانات تحديد الموقع التي يقوم بها مراقب البيانات.

يجب شرح المعالجة للأشخاص المعنيين بشكل استباقي بطريقة يسهل الوصول إليها ؛ لضمان فهمهم لما سيحدث لبياناتهم ، وهذا يعني أن صاحب البيانات يجب أن يعرف الغرض المحدد من معالجة البيانات الشخصية عند جمع البيانات المتعلقة به.

تتطلب شفافية المعالجة استخدام مصطلحات واضحة وبسيطة بحيث يجب أن يكون أصحاب البيانات على علم بوضوح بالمخاطر ، والقواعد ، والضمانات ، والحقوق المرتبطة بمعالجة بياناتهم الشخصية.

٩- الجوانب القانونية لتقنية تحديد الموقع الجغرافي

ويقع على عاتق مراقب البيانات إثبات أن موافقة الشخص المعني على معالجة بيانات تحديد موقعه الجغرافي قد تم منحها بالفعل ، وأنها صالحة بموجب القانون.

يجب أن تأتي الموافقة من اختيار حقيقي للشخص المعني ، ويجب ألا يكون قد تعرض لأي إكراه ؛ لذلك فإن الموافقة لا يمكن وصفها بأنها مجانية ، وحرة إذا "تم تقديمها كجزء من الشروط العامة غير قابل للتفاوض.

كما يجب أن يكون هناك توازن معين بين الطرفين (مراقب البيانات وصاحب البيانات) ؛ لذلك لا ينبغي أن تشكل الموافقة أساسًا قانونيًا صالحًا لمعالجة البيانات الشخصية في حالة معينة حيث يوجد خلل واضح بين صاحب البيانات والمراقب، على وجه الخصوص عندما يكون المراقب سلطة عامة ، ومن غير المرجح أن يتم منح الموافقة بحرية في ضوء جميع الظروف الخاصة بهذا الموقف بالذات.

٦: بخصوص غالبية معالجات البيانات في العمل فلا ينبغي أن يكون الأساس القانوني هو موافقة العمال ؛ نظرا لطبيعة العلاقة بين صاحب العمل والعامل ، والتي قد تجعل الموافقة أساسًا قانونيًا غير مؤكد.

يمكن للعامل من الناحية النظرية أن يرفض إعطاء الموافقة ، لكنه قد يفقد بعد ذلك فرصة العمل ، وفي هذه الظروف فإن عدم منح الموافقة بحرية لا يكون صحيحًا.
لذلك بدلاً من طلب الموافقة يجب على أصحاب العمل النظر فيما إذا كان من الممكن إثبات أن هناك حاجة لرصد الموقع الدقيق للعمال لغرض مشروع ، وموازنة هذه الحاجة مع الحقوق ، والحريات الأساسية للعمال.

٧: بخصوص معالجة تحديد الموقع الجغرافي للأطفال في الأحوال التي تستلزم ذلك فيجب الحصول على موافقة الأطفال أنفسهم ، أو من قبل الوالدين ، أو غيرهم من الممثلين القانونيين.

٨: يجب أن تكون موافقة صاحب البيانات على معالجة بيانات تحديد الموقع الخاص به موافقة صريحة وبالتالي لا ينبغي أن يشكل صمت المستخدم قبولًا.

في حالة ما إذا كانت الإعدادات الافتراضية لنظام التشغيل تسمح بنقل بيانات الموقع فلا ينبغي اعتبار عدم التدخل من جانب المستخدمين بمثابة موافقة حرة ، وصريحة منهم.

لا يمكن اعتبار الموافقة قد تم الحصول عليها بشكل صحيح إذا تم منحها عن طريق نفس الإجراء كما هو الحال عندما يقبل صاحب البيانات عقدًا ، أو الشروط العامة للخدمة" ؛ لذلك يجب على الأشخاص المتأثرين بأجهزة تحديد الموقع الجغرافي التعبير عن موافقتهم الصريحة بشكل فردي ، وكتابي قبل تنفيذ المعالجة.

علاوة على ذلك في حالة المعالجة التي تسعى إلى أكثر من غرض ، يجب أن يكون صاحب البيانات قادرًا على الموافقة على بعضها ، دون البعض الآخر.

٩: منذ لحظة دمج بيانات تحديد الموقع الجغرافي مع البيانات الشخصية ستخضع المعالجة المتعلقة بها لنظام اللائحة العامة لحماية البيانات (GDPR) مع كل العواقب التي ينطوي عليها ذلك ؛ لذلك يجب على القائمين على هذا النوع من المعالجة أن يقوموا بتزويد أصحاب البيانات بمعلومات عن الحقوق التي يتمتعون بها

٩- الجوانب القانونية لتقنية تحديد الموقع الجغرافي

وهي حق الوصول إلى البيانات الشخصية ، الحق في تقديم شكوى إلى سلطة حماية البيانات، حق الاعتراض، حق التصحيح، حق المحو(الحق في النسيان)، الحق في تقييد المعالجة، الحق في قابلية النقل.

١٠: استخدامات تقنية الموقع الجغرافي كثيرة ومتعددة ولا يمكن إحصاؤها :

يمكن لتقنية تحديد الموقع الجغرافي أن تلعب دورًا مهمًا في المسائل الجنائية . فتساعد في تحقيق الأمن الداخلي من خلال تمكين مراقبة المشتبه بهم ، وتعقب الأشياء المسروقة (خاصة السيارات). كما يمكن أيضًا استخدامها في مسائل الإرهاب.

تُعد نظم المعلومات الجغرافية ، والمعلومات السياقية في الوقت الفعلي أحد العوامل الرئيسية في تحسين الرحلات الفردية .

تم استخدام تقنية تحديد الموقع الجغرافي في بيئة العمل حيث وجدت مكانها ومزاياها داخل الشركات ، وفي إطار علاقة الأعمال التجارية مع المستهلك : حيث استفادت الشركات إلى حد كبير من هذه التقنية ؛ لتقديم منتجاتها وخدماتها على أساس القرب من العميل المحتمل.

كما أثبتت هذه التقنية نجاحها في أثناء أزمة كورونا في تحديد أماكن مصابي فيروس كورونا ، وتحديد بؤر الاصابات ، واعتمدت عليها السلطات العامة في الكثير من دول العالم لرصد تطور الوباء ، والسيطرة على السكان.

قائمة المراجع

أولا : المراجع باللغة الفرنسية

A- Ouvrages speciaux et theses

1- A. DELFORGE, « Comment (ré)concilier RGPD et big data ? », R.D.T.I, 2018, n°70.

2- Bu-Pasha, Shakila & Alén, Anette & Mäkinen, J. & Guinness, Robert & Korpisaari, Päivi. (2016). EU Law Perspectives on Location Data Privacy in Smartphones and Informed Consent for Transparency. European Data Protection Law Review. 2. 312-323. 10.21552/EDPL/2016/3/7 p.312..

https://doi.org/10.21552/EDPL/2016/3/7.

3- B. VAN ALSENOY, Data Protection Law in the EU: Roles, Responsibilities and Liability, Cambridge, Intersentia, 2019

4- C.COLIN et Y., POULLET, « Du consommateur et de sa protection face à de nouvelles application des technologies de l'information : risques et opportunités », D.C.C.R, 2010/3, n°88..

5- CHARTER OF FUNDAMENTAL RIGHTSOF THE EUROPEAN UNION (2000/C 364/01)

6- Charlotte Sikivie, Comment les entreprises traduisent-elles les obligations légales contenues dans le Règlement (UE) 2016/679 relatif à la protection des données en obligations de compliance ? Analyse comparative entre PME et grandes structures.Master en droit.à U Liège. Année académique 2019-2020

7- Christophe Radé, [Brèves] A propos de la géolocalisation des salariés : la CNIL et la Cour de cassation à l'unisson, Lexbase Social, novembre 2011, n°46..

8- Comité européen de la protection des données, Statement on the Processing of Personal Data in the Context of the Covid-19 Outbreak 2020.

9- De Terwangne, , Les principes relatifs au traitement des données à caractère personnel et à sa licéité Dans Le règlement général sur la protection des données (RGPD/GDPR): analyse approfondie. Cahiers du CRIDS, Numéro 44, Larcier , Bruxelles, 2018.

10- Elliott Kaplan,Understanding GPS: principles and applications/[editors], Christopher Hegarty.—2nd ed.2005

11- Gérard Haas et Florian, PERRETIN RGPD : Géolocalisation et Marketing, une question de consentement !
https://www.haas-avocats.com

12- Goncalves, Lucie & de Pechpeyrou, Pauline & Benavent, Christophe. (2014). JUSQU'OÙ LES CONSOMMATEURS ACCEPTENT-ILS D'ÊTRE GÉOLOCALISÉS ? REVUE FRANÇAISE DU MARKETING - Septembre 2014 - N° 248.

13- Ismail Slimani Toufik Habireche , Conception et réalisation d'un système de géolocalisation et de suivi, Cas NAFTAL,Mémoire de Fin d'Etudes de master ,Universite Mouloud Mammeri de Tizi-ouzou ,Faculte du Genie electrique et d'informatique departement d'informatique ,Algérienne 2016.

14- Jan Lauren Boyles et al, 'Privacy and Data Management on Mobile Devices' (Pew Research Center, 5 September 2012)
<http://www.pewinternet.org/2012/09/05/privacy-and-data-man-

15- Komur, Neslin, La géolocalisation dans la relation de travail :un dispositif de surveillance sans limite(s) mettant en péril le

droit au respect de la vie privée du travailleur ?Master . faculte De droit et de criminologie, universite uclouvain Année académique 2018-2019.

16- Krzysztof Stefański, Employee geolocation versus the GDPR PRACA I ZABEZPIECZENIE SPOŁECZNE/LABOUR AND SOCIAL SECURITY JOURNAL 4/2021

17- Lignes directrices 5/2020 sur le consentement au sens du règlement (UE) 2016/679 , Version 1.1 Adoptées le 4 mai 2020.

18- Manuel de droit européen en matière de protection des données Édition 2018,Agence des droits fondamentaux de l'Union européenne et Conseil de l'Europe, 2019

19- Marie Romani, Prévenir ou l'impact de la crise sanitaire planétaire et inédite de l'année 2020Anne

https://www.airdberlis.com

20- M. Henri BarbIerk, Les Enjeux, de L'encadrement Juridique de la geolocalisation master, faculte de droit et de science politique, nstitut de recherches en droit de L'information et DE la communication, 2013-2014.

21- Michael Laranj Mise en relation des données de géolocalisation lors de procédures pénales, Haute École de Gestion de Genève (HEG-GE) Filière Informatique de Gestion 2014.

22- Merabtene Amel et Agred Nouara, Système de géolocalisation pour les réseaux mobiles, diplôme de Master en informatique,Faculté de Génie Electrique et Informatique ,Université Mouloud Mammeri de Tizi-Ouzou, Algérienne 2012-2013.

23- O. MORENO et F. SCHAPIRA, « La surveillance des travailleurs par géolocalisation », in Discipline et surveillance dans la relation de travail (S. GILSON dir.), Limal, Anthemis, 2013

24- Paige Backman and Stephanie D'Amico,Geolocation and the Fight Against COVID-19,Could the Emergencies Act Overrule Privacy Law Protections for Cellphone Location Data? 2020 no.5

25- S. FARMER, « European Privacy Body Opines on Geolocation Services on Smart Mobile Devices », in C.T.L.R, vol. 17., New-York, Thomson Reuters, 2011

26- S. PEYROU, « Le nouveau règlement général européen relatif à la protection des données à caractère personnel : un texte à la hauteur de ses ambitions », R.A.E., 2016.

27- S. PARSA, « Le R.G.P.D. et la profession d'avocat, au-delà du secret professionnel et du principe de confidentialité », Le Règlement général sur la protection des données (R.G.P.D./G.D.P.R.) : premières applications et analyse sectorielle, H. Jacquemin (dir.), vol. 195, Liège, CUP, Anthemis, 2020.

28- Vincent Bergeron et Thomas Gagnon -van Leeuwen, Geolocalisation et Application mobilles: Mode D'emploi pour une Geolocalisation eloignee des problemes juridiques! Robic, LLP ,CIPS 2015

29- Yoann Gonthier Le Guen. La protection des données personnelles en situation de crise sanitaire exceptionnelle : L'hypothèse du traçage géographique des citoyens à fin de lutte

épidémique. Revue des droits et libertés fondamentaux, 2020, pp.chron. n° 27. halshs-0254107.

B-Rapports et équipes de travail

1- CNIL, Guide de la géolocalisation des salariés, Droits et olbigations en matière de géolocalisation des employés par un dispositif de suivi G.S.M/G.

2- CNIl , Avis n°12/2005 relatif à la proposition de loi visant à encadrer la surveillance des travailleurs par l'utilisation d'un système de monitoring associé au système de navigation G.P.S sur véhicules de service, dans le respect de la loi du 8 décembre 1992 relative à la protection de la vie privée, 7 septembre 2005.

3- CNIL, Délibération n°2006- 066 du 16 mars 2006 portant adoption d'une recommandation relative à la mise en œuvre de dispositifs destinés à géolocaliser les véhicules automobiles utilisés par les employés d'un organisme privé ou public, art. 5, disponible sur www.cnil.fr

4- CNIL,Délibération n° 2010-096 du 8 avril 2010 portant recommandation relative à la mise en œuvre, par les compagnies d'assurance et les constructeurs automobiles, de dispositifs de géolocalisation embarqués dans les véhicules.

5- CNIL, un rapport public sur ces différentes techniques de publicité ciblée en ligne, sur leurs risques d'atteintes à la vie privée et les parades possibles. 17 novembre 2010

6-CNIL, Véhicules connectés : un pack de conformité pour une utilisation responsable des données 16 octobre 2017.

7- CNIL, Délibération de la formation restreinte n° SAN-2023-003 du 16 mars 2023 concernant la société CITYSCOOT

8- CNIL, La géolocalisation des véhicules des salariés, 30 mai 2023.

9- CNIL.Projet de recommandation Relative aux applications mobiles, Version soumise à consultation publique jusqu'au 8 octobre 2023.

10--Groupe de travail « Article 29 » (2004), Avis 10/2004 sur les « Dispositions davantage harmonisée en matière 'informations », WP 100, Bruxelles, 25 novembre 2004

11-Groupe de l'article 29 Avis n°5/2005 du 25 novembre 2005 du Groupe de l'Article 29 sur l'utilisation de données de localisation aux fins de fourniture de services à valeur ajoutée, 2130/05/FR, WP115, p.10, disponible sur www.europa.EU

12-Groupe de l'article 29 l'avis 4/2010 du G29 sur le code de conduite de la FEDMA relatif à l'exploitation de données à caractère personnel dans le cadre d'opérations de marketing direct (WP 174) et l'avis sur l'utilisation de données de localisation aux fins de fourniture de services à valeur ajoutée (WP 115)

13-Groupe Article 29 Avis n°13/2011 du 16 mai 2011 sur les services de géolocalisation des dispositifs mobiles intelligents, 881/11/FR, WP185.

14-Groupe de l'article 29, « Avis n°15/2011 sur la définition du consentement », WP 187

15-GROUPE DE TRAVAIL «ARTICLE 29» SUR LA PROTECTION DES DONNÉE, Avis 05/2014 sur les Techniques d' anonymisation, Adopté le 10 avril 2014

16-Groupe de l'article 29, « Lignes directrices sur le consentement au sens du règlement (UE) 2016/679 » WP 259 rev.01.Adoptées le 28 novembre 2017, Version révisée et adoptée le 10 avril 2018

17-Article 29 Working Party Guidelines on consent under Regulation 2016/679 Adopted on 28 November 2017 As last Revised and Adopted on 10 April 2018

18-Groupe de travail « Article 29 », Avis 2/2017 sur le traitement des données au travail, Adopté le 8 juin 2017

ثانيا : مراجع باللغة الانجليزية

1- The European Data Protection Board: Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak, Adopted on 21 April 2020.

2- Groupe Article 29, Guidelines on transparency under Regulation 2016/679 (WP260 rev.01), 11 avril 2018.

3-Location Forum, Location Data Privacy Guidelines, Assessments and Recommendations (Version 2, 1 May 2013)

ثالثا: المواقع الالكترونية

1- https://www.lagbd.org . Géolocalisation_et_télécommuni

2- https://archives.defense.gouv.fr

3-http://www.journaldunet.com/ebusiness/internet-mobile/1133686-geolocalisation-indoor-comment-ca-marche/

4- https://www.uber.com/legal/privacy-proposed/users/fr .

5- https://www.masternaut.com

6- https://uk.practicallaw.thomsonreuters.com.