Alain Bensoussan Avocats
Le droit du numérique et des technologies avancées

*Le réseau Lexing vous informe – The Lexing ® network informs you*

JTIT Internationale n°13 – décembre 2016
JTIT Special international issue #13– December 2016

# LA GÉOLOCALISATION DES SALARIÉS

# *GEOLOCATION OF EMPLOYEES*

## DONNÉES GÉOGRAPHIQUES ET RISQUES D'ATTEINTE A LA VIE PRIVÉE

▪ L'utilisation de données de localisation dans le contexte professionnel a connu un accroissement spectaculaire. Parce qu'ils coûtent de moins en moins chers et peuvent s'avérer très utiles, les dispositifs de géolocalisation, qui peuvent être installés sur les appareils fournis aux salariés (téléphones portables, etc.) ou dans les véhicules (de fonction ou personnel) utilisés par ces derniers, ont séduit les chefs d'entreprises. Or, la géolocalisation des salariés comporte des risques inhérents à leur liberté d'aller et de venir et à leur vie privée. Conscients de ces risques et animés par la volonté de préserver les droits fondamentaux du salarié, de nombreux pays ont ainsi encadré les modalités de mise en œuvre des dispositifs de géolocalisation par les employeurs.

▪ Les membres du réseau Lexing® dressent un tableau de la situation actuelle à travers le monde. Les pays suivants ont contribué à ce numéro : Afrique du Sud, Allemagne, Belgique, Costa Rica, Espagne, France, Grèce, Nouvelle-Calédonie.

## GEOGRAPHICAL DATA AND PRIVACY RISKS

▪ *There has been a spectacular increase in the use of location data in the employment context. As they cost less and less and can prove very useful, geolocation systems, which can be installed on devices carried by employees (e.g. mobile telephone) and/or on (corporate or private) vehicles used by them, are now widely used by companies. But the geolocation of employees creates inherent risks to their right to come and go and to privacy. Many countries have thus set up a framework for the use of location devices by employers in order to manage risks for and preserve the fundamental rights of employees.*

▪ *The Lexing® network members provide a snapshot of the current state of play worldwide. The following countries have contributed to this issue: South Africa, Germany, Belgium, Costa Rica, Spain, France, Greece, New Caledonia.*

### A propos de Lexing®

Lexing® est le premier réseau international d'avocats spécialisés en droit du numérique et des technologies avancées.
Créé sur une initiative d'Alain Bensoussan, Lexing® permet aux entreprises internationales de bénéficier de l'assistance d'avocats alliant la connaissance des technologies, des métiers et du droit qui leur sont applicables dans leur pays respectifs.

### *About Lexing®*

*Lexing® is the first global network of attorneys specialized in digital and emerging technology law.*
*Created on an initiative of Alain Bensoussan, Lexing® allows multinationals to benefit from the assistance of seasoned lawyers worldwide who each combines unique expertise in technology and industry with a thorough knowledge of law in their respective country.*

EMMANUEL WALLE

▪ La géolocalisation, qui est un procédé permettant de déterminer la position géographique d'un objet ou d'une personne, présente de nombreux avantages. Imaginez que vous ayez besoin de voir une personne de toute urgence, mais que vous ne savez pas où elle est. Avec la géolocalisation, vous pourrez facilement identifier l'immeuble dans lequel elle se trouve et même repérer qu'elle est au 15e étage, en salle de conférence A. Si la géolocalisation d'un objet (un ordinateur, par exemple) ne soulève généralement pas de question en matière de confidentialité, il en va autrement lorsqu'elle concerne une personne physique, et plus particulièrement un salarié. Un employeur est-il autorisé à géolocaliser ses salariés ? Quels sont les risques pour les salariés ? Qu'en est-il des cas de géolocalisation indirecte d'une personne, c'est-à-dire via un objet qu'elle détient, tel un téléphone professionnel ?

## Pourquoi utiliser la géolocalisation ? Comment ça marche ?

▪ La géolocalisation offrant de multiples possibilités, de nombreuses personnes y ont recours, chacune pour des raisons très différentes : les entreprises pour localiser leurs équipements ou leurs salariés, les agences de marketing à des fins de prospection, ou encore les agriculteurs pour le suivi de leur bétail.

▪ La position géographique s'obtient en combinant des données provenant de diverses sources, le plus souvent les coordonnées GPS et les signaux des antennes-relais de téléphonie mobile, afin de trianguler la position d'un objet ou d'une personne. Il existe plusieurs autres techniques de géolocalisation, avec une granularité plus ou moins fine, comme celle qui consiste à exploiter les adresses IP (Internet Protocol).

## Est-il légal de géolocaliser ses employés ?

▪ La géolocalisation des salariés est, en principe, légale, sous réserve de respecter certaines conditions, détaillées ci-après.

▪ Ces conditions sont principalement posées par le droit à la protection de la vie privée et à la protection des données à caractère personnel. En Afrique du Sud, il s'agit de la loi sur protection des données à caractère personnel **(1)** (dite loi « POPI »). En Europe, c'est le Règlement général sur la protection des données (RGPD) **(2)**, par ailleurs très similaire à la POPI. Quant aux États-Unis, le gouvernement travaille actuellement à l'adoption de deux nouvelles lois **(3)** relatives à la géolocalisation au regard de la vie privée (Geolocation Privacy and Surveillance Act) et des communications en ligne (Online Communications and Geolocation

(1) "Protection of Personal Information Act Summary", https://www.michalsons.com/focus-areas/privacy-and-data-protection/protection-of-personal-information-act

(2) "What is the GDPR and Why is it Important?", https://www.michalsons.com/blog/what-is-the-gdpr/18552

(3) "Geolocation Privacy Legislation", http://www.gps.gov/policy/legislation/gps-act/

Protection Act). Le RGPD et la POPI définissent tous deux les données de localisation comme des données à caractère personnel. La légalité de la géolocalisation des salariés doit donc être évaluée à l'aune de la réglementation en matière de protection des données.

▪ Cette règlementation précise les conditions requises pour traiter les données de localisation de manière licite, dans le respect des droits des personnes concernées. Le terme « traiter » s'entend au sens large et englobe différentes opérations pouvant être effectuées sur les données telles que la collecte, l'utilisation ou le stockage. Notamment, pour qu'un traitement soit licite :

- les données doivent être complètes et exactes,
- la personne concernée doit être informée des finalités du traitement, et
- le traitement doit être justifié (par exemple, la personne concernée a consenti au traitement, le traitement est nécessaire au respect d'une obligation légale, ou bien est réalisé au bénéfice de la personne concernée).

▪ La licéité du traitement dépend également de nombreux autres facteurs, dont la liste exhaustive ne peut être dressée ici. Il suffit de noter qu'il convient de mettre en place des mesures de sécurité appropriées, ou raisonnables selon la terminologie de la POPI, au regard des risques présentés par le traitement des données.

### Avant de se lancer : les questions clés à se poser

▪ En vertu de la loi sur la protection des données, toutes les personnes concernées, salariés compris, doivent être informées du traitement des données personnelles les concernant. Le chef d'entreprise doit donc veiller à les informer de l'existence d'un traitement de leurs données de localisation et des finalités de ce traitement. Les objectifs poursuivis peuvent être variés : par exemple, suivre les déplacements des salariés qui travaillent en dehors des locaux de l'entreprise afin de s'assurer qu'ils honorent bien leurs rendez-vous professionnels, ou bien surveiller la présence et le temps de travail des salariés en contrôlant leur connexion au système informatique.

▪ Outre l'information des salariés, d'autres démarches importantes doivent également être envisagées :

- Obtenir le consentement des salariés au traitement de leurs données de localisation
- Mettre en place les mesures de sécurité adéquates (règles, procédures, systèmes…) permettant de protéger toutes les données de localisation faisant l'objet d'un traitement
- Appliquer une charte de confidentialité, une politique en matière

de géolocalisation, ou une politique de gestion des incidents

- Identifier et comprendre la législation à respecter – la POPI ou le RGPD, par exemple
- S'assurer de la base légale du traitement
- Disposer d'une procédure pour procéder à la suppression des données des systèmes informatiques
- Mettre en place des contrôles destinés à empêcher l'utilisation des données par des tiers non autorisés et pour d'autres finalités que celles prévues initialement

▪ Autant de questions qu'un employeur doit se poser avant de mettre en œuvre un dispositif de géolocalisation afin de s'assurer de la licéité du traitement des données personnelles de son personnel. A défaut, l'entreprise s'expose à des poursuites de la part de ses salariés, qui risquent de tenir son image de marque et sa réputation.

### Les données de géolocalisation sont-elles utilisables à titre de preuve ?

▪ En Afrique du Sud, il est tout à fait possible d'utiliser les données de localisation à titre de preuve dans le cadre de procédures judiciaires ou disciplinaires **(4)**. Cette possibilité est néanmoins encadrée, notamment, par la POPI, la Constitution, et la loi sur les communications et les transactions électroniques (loi ECT). Cette dernière confirme l'admissibilité des données de localisation **(5)** en précisant que des éléments de preuve ne peuvent être déclarés inadmissibles au seul motif qu'ils se présentent sous une forme électronique.

▪ Il convient, bien entendu, au préalable de s'assurer que les données de localisation ne peuvent souffrir de contestation. Il est donc nécessaire de vérifier que les données en question n'ont pas été obtenues au mépris de la loi sur la protection des données ou du droit à la vie privée tel que consacré dans la Constitution de la République d'Afrique du Sud.

### Plan d'action pour les chefs d'entreprise

- S'informer sur l'état de la législation en matière de géolocalisation et en suivre les évolutions, par exemple en participant à des sessions de formations **(6)**.
- Veiller à bien respecter cette législation dans l'entreprise.
- Sécuriser les pratiques, notamment en les encadrant par une politique de géolocalisation.
- Prendre en compte les dispositions adéquates du droit du travail.
- Disposer d'une politique de confidentialité des salariés qui couvre la géolocalisation, ainsi que toutes les activités de traitement général.
- Gérer les failles de sécurité en amont, en se dotant d'un plan de gestion des incidents.

(4) "Better Disciplinary Hearings save Time and Money", https://www.michalsons.com/focus-areas/labour-law-services/better-procedure-disciplinary-hearings-save-time-money

(5) "Electronic Evidence in Criminal and Civil Proceedings", https://www.michalsons.com/focus-areas/information-technology-law/electronic-evidence-in-criminal-and-civil-proceedings

(6) Michalsons Protection of Personal Information Act (POPI) Workshops, https://www.youtube.com/watch?v=OrKc40fff6c

JOHN GILES

*Geolocation is the identification of the geographic location of an object (like a computer) or a person (like an employee). It is obviously very useful to know where something is. Knowing that John is on the 15th floor in boardroom A when you urgently need to speak to him is very useful. There aren't usually privacy concerns when you identify the location of an object, but what about the location of a person (like an employee)? Is it lawful to geolocate your employees? Are employees exposed to risks if some people can track their movements? What if you can track a person by tracking an object that they always have with them (like a phone)?*

### *Who uses Geolocation Data?*

- *Many people use it, but for different reasons. Organisations may use this data to locate their assets or employees. Marketing agencies can also use this data for marketing purposes. Even farmers can use it for tracking their livestock.*
- *Geographic location relies on gathering data from many different sources. GPS coordinates and cell phone tower signals are very useful and are some of the most widely used methods to successfully track an object or a person. When GPS coordinates are not available, users depend on cell phone tower signals to triangulate an object or person's position. Internet Protocol (IP) addresses are also quite useful, because geolocation pairs this address with a geographical location.*

### *Is Geolocation of Employees Lawful?*

- *The short answer to this question is: Yes, but it depends on a few factors. What factors does lawfulness depend on, you ask?*
- *Privacy and data protection law is the most relevant. In South Africa, the Protection of Personal Information Act* ***(1)*** *(or POPI Act) is the law that applies to this question. In Europe, it is the General Data Protection Regulation (GDPR)* ***(2)*** *– which is very similar to POPI. In the US, the government is in a process of passing two new laws* ***(3)*** *that relate to geolocation. One is the Geolocation Privacy and Surveillance Act and the other is the Online Communications and Geolocation Protection Act. Both the GDPR and POPI include location information in the definition of personal information or data, so data protection law does have an impact on geolocation.*

(1) "Protection of Personal Information Act Summary", https://www.michalsons.com/focus-areas/privacy-and-data-protection/protection-of-personal-information-act

(2) "What is the GDPR and Why is it Important?", https://www.michalsons.com/blog/what-is-the-gdpr/18552

(3) "Geolocation Privacy Legislation", http://www.gps.gov/policy/legislation/gps-act/

▪ *They set the requirements for processing lawfully so that data subjects can be safe from harm. Processing includes the collection, use, and storage of geolocation data. The requirements for lawful processing include ensuring that the personal information is:*

- *complete and accurate,*
- *that the data subject knows why it is being processed, and*
- *that there's a good reason for the processing (for example the data subject consented, it is the responsible party's duty to process, or it is to the benefit of the data subject).*

▪ *The list of factors to consider does not end here. Data protection laws require you to ensure that the security of the information is adequate for the level of risk it is exposed to. POPI, of course, also requires you to ensure that the security is reasonable, not just appropriate.*

### *Questions you need to ask yourself*

▪ *If all data subjects need to know why their personal information is being processed, your employees clearly enjoy the same rights under data protection law. You need to let them know that you are processing their location information and also give them the reasons behind the processing. So what are your reasons? Do you want to use geolocation, for example, to track the movements of employees who work away from the office, to ensure that they're where they need to be? Do you want it to track the time of your office employees to ensure that they're present at work and logging onto the system at the right times?*

▪ *But what are some of the other important questions you need to ask:*

- *Do you get your employees' consent to process their location information?*
- *Do you have adequate security measures (such as workplace policies and systems) in place that protect all the location information you process?*
- *Do you have a privacy policy, geolocation policy, or even an incidence response policy, for example?*
- *Do you understand which laws you have to comply with – POPI or the GDPR, for example?*
- *Do you only process the location information for good reasons?*
- *Do you have measures in place for safely removing the information from your systems?*
- *Do you have controls in place to prevent others using the data for other purposes?*

▪ *By asking yourself these questions, you are a few steps closer to lawfully processing your employees' personal information. You reduce the risk of your organization suffering reputational damage, and possibly having to deal with lawsuits from angry employees who suffered harm, because of your non-compliance with data protection law.*

### *Can you use Geolocation Data as Evidence?*

▪ *In South Africa, the answer is: Yes, you can use location information as evidence in court proceedings or at disciplinary hearings* ***(4)****, but it depends on various factors. The provisions, for example, of the Electronic Communications and Transactions Act (ECT Act), POPI and the Constitution of the Republic of South Africa apply and are important. The ECT Act gives you even more power to use location information as electronic evidence* ***(5)*** *by stating that it cannot be disregarded just because it is in electronic form. The accuracy of the location information is a key factor. If you are going to use location information as evidence against your employee at a disciplinary hearing, make sure that it is accurate. You don't want your employee to challenge its accuracy in court and win.*

▪ *Other factors to consider in using location information as evidence, include whether or not you obtained the information in violation of data protection law or, ultimately, the right to privacy in the constitution.*

### *Actions you can take*

- *Find out more about the law related to geolocation by attending a workshop* ***(6)****.*
- *Use geolocation lawfully in your workplace.*
- *Manage your geolocation activities with a legally compliant geolocation policy.*
- *Comply with labour laws.*
- *Have an employee privacy policy that covers all you processing activities (including geolocation).*
- *Be ready for data breaches by having a legally compliant incidence response policy.*

(4) "Better Disciplinary Hearings save Time and Money", https://www.michalsons.com/focus-areas/labour-law-services/better-procedure-disciplinary-hearings-save-time-money

(5) "Electronic Evidence in Criminal and Civil Proceedings", https://www.michalsons.com/focus-areas/information-technology-law/electronic-evidence-in-criminal-and-civil-proceedings

(6) Michalsons Protection of Personal Information Act (POPI) Workshops, https://www.youtube.com/watch?v=OrKc40fff6c

JOHN GILES

▪ La dématérialisation fait désormais partie de la vie quotidienne et force est de constater qu'elle bien ancrée dans le monde de l'entreprise. D'énormes quantités de données personnelles relatives aux salariés peuvent ainsi être recueillies et traitées par les employeurs. En particulier, les dispositifs (mobiles) intelligents dont sont équipés les salariés collectent et transmettent automatiquement certaines données. Parmi elles figurent les données de localisation issues des requêtes Internet effectuées ou des services de géolocalisation utilisés par les salariés. Or, avec ces données, l'employeur accède à toutes sortes d'informations, qu'il peut analyser afin de créer des profils individuels de ses salariés, portant entre autres sur leur comportement et leurs relations sociales **(1)**. Il est, par conséquent, apparu indispensable de protéger les salariés contre toute atteinte à leur droit à l'autodétermination informationnelle et tout profilage illégal.

(1) Art. 2 par.1 de la Loi fondamentale (Grundgesetz ou « GG », qui est la Constitution de la République fédérale d'Allemagne)

▪ En droit allemand, la collecte de données de localisation par un fournisseur de services de télécommunication requiert le **consentement** de la personne concernée, sauf si ces données sont anonymisées. **(2)** Indépendamment de la question de savoir si l'employeur peut être considéré comme un fournisseur de services de télécommunication (ce qui peut être le cas lorsqu'il fournit à son employé un appareil intelligent et/ou l'infrastructure technique lui permettant de l'utiliser), on peut s'interroger sur la validité du consentement donné par un salarié à son employeur. En effet, d'une part, ce consentement doit reposer sur **une décision éclairée**, supposant une clarification technique approfondie des données personnelles relatives aux services, clarification qui fait défaut dans plupart des cas. D'autre part, compte tenu du déséquilibre structurel entre l'employeur et le salarié, le **caractère volontaire du consentement d'un salarié** est bien souvent contestable, car il ne saurait être exclu que l'employé se sente forcé de consentir au traitement de ses données de localisation et n'ose donc pas désactiver la collecte et la transmission des données sur l'appareil intelligent qui lui a été fourni.

(2) Sec. 98 de la loi sur les télécommunications (Telekommunikations-gesetz ou « TKG »)

▪ A défaut de consentement, la collecte et le traitement des données de localisation peuvent néanmoins être légitimés par la **règle générale en matière de protection des données des salariés (3)**. Aux termes de cette règle, les données personnelles d'un salarié peuvent être collectées, traitées ou utilisées pour des finalités liées à l'emploi lorsque cela est nécessaire pour prendre des décisions avant son embauche ou, ultérieurement, pour exécuter ou résilier son contrat de travail. A cette occasion, une mise en balance des intérêts des deux parties sera effectuée, en tenant dûment compte des finalités du traitement en question. S'agissant plus particulièrement des données de localisation, l'idée-force est que les salariés ne **doivent pas faire l'objet d'une géolocalisation** lorsqu'ils se trouvent **dans une zone relevant de la sphère privée**, par exemple les zones de repos, les toilettes ou un local privé, et **ne doivent pas être observés en permanence** pendant leurs heures

(3) Sec. 32 de la loi fédérale sur la protection des données (Bundesdatenschutz-gesetz ou « BDSG »)

de travail. Les opérations de traitement et d'analyse des données de localisation recueillies doivent être limitées aux besoins spécifiques de l'employeur à des fins de contrôle ou d'organisation, c'est-à-dire pour la coordination des processus de travail. Même dans ces hypothèses, les données de localisation doivent toujours être stockées sous une forme anonyme, afin d'éviter la création de profils individuels à partir des données des salariés.

▪ Les salariés **doivent être informés** de la collecte et du traitement de leurs données de localisation à caractère personnel et des finalités poursuivies, à moins que le salarié ne dispose déjà de ces informations **(4)**. En l'absence de transparence, l'employeur est tenu de supprimer les données personnelles se rapportant aux salariés et est **passible d'une amende** pouvant aller jusqu'à 50.000,00 € pour les infractions administratives **(5)**.

▪ Par ailleurs, il convient de réaliser les démarches requises auprès du comité d'entreprise. En effet, en Allemagne, le **comité d'entreprise** a un droit de codétermination en ce qui concerne les règles de fonctionnement de l'entreprise et de conduite des salariés **(6)**, et notamment lors de l'introduction et de l'utilisation de dispositifs techniques conçus pour surveiller le comportement ou la performance des salariés **(7)**. Les dispositions de la loi sur la protection des données ne font pas obstacle aux prérogatives du comité d'entreprise **(8),** qui s'étendent à tous les dispositifs techniques, dès lors qu'ils permettent objectivement de contrôler le comportement ou la performance des salariés, peu importe que l'employeur les utilise à ces fins ou non **(9)**. Dans ce contexte, la conclusion d'un **accord d'entreprise** entre le comité d'entreprise et l'employeur **(10)** précisant les principes et le champ d'application du traitement de données associé, sera généralement requis pour constituer la base légale de la collecte et de l'analyse des données de localisation par le chef d'entreprise.

▪ Enfin, il faut garder à l'esprit le principe général de **minimisation des données**, qui s'applique quelle que soit la base légale du traitement. Ce principe préconise de réduire au strict minimum les données personnelles collectées, traitées et utilisées **(11)**. A cet égard, il peut être envisagé de mettre en œuvre des systèmes informatiques qui s'auto-localisent et ne transfèrent les données de localisation ainsi collectées que sur demande d'une autorité dûment habilitée, tout offrant éventuellement au salarié la possibilité de les désactiver **(12)**. En tout état de cause, le moyen le plus efficace de satisfaire aux exigences en matière de protection des données est de mettre en œuvre des technologies visant à minimiser la collecte et le traitement de données à caractère personnel. C'est la raison pour laquelle la protection des données dès la conception, ou « **privacy by design** », est en passe de devenir l'instrument de protection des données de prédilection des acteurs de l'industrie 4.0.

(4) Sec. 33 par. 1 BDSG

(5) Sec. 43 par. 1 et 2 BDSG

(6) Sec. 87 No. 1 de la loi sur l'organisation des entreprises (Betriebsverfassungs-gesetz ou « BetrVG »)

(7) Sec. 87 al. 6 BetrVG

(8) Sec. 32, par. 3, de la loi sur la BDSG

(9) Jurisprudence constante des juridictions fédérales en matière de droit social depuis la décision du 9-9-1975, AP BetrVG 1972 Sec. 87 Überwachung No. 2

(10) Sec. 77 BetrVG

(11) Sec. 3a al. 1 BDSG

(12) Hofmann, "Smart factory – Employees' data protection in Industry 4.0", in DSRITB 2015, 209 (220)

ANDREAS LOBER
&
SUSANNE KLEIN



▪ *It is a known fact that digitalization reaches every part of life and society, and in particular the world of employment. This leads to enormous amounts of employees' personal data being collected and processed by the employer. In particular, the use of smart (mobile) devices offers new possibilities of accessing and analyzing such data by employers because very often location data ("geo-data") of the user based on internet queries or location based services are collected and automatically transmitted by smart devices. As such data allows the employer to draw his conclusions about the behavior and social relationships of his employee, the employee's right to informational self-determination **(1)** may easily be affected. Thus, the employee needs to be protected from the unlawful creation of data profiles.*

(1) Art. 2 par. 1 Grundgesetz ("GG" – Basic Law for the Federal Republic of Germany)

▪ *According to German Law the collection of geo-data by a provider of telecommunication services requires, if such data is not anonymized, the **consent** of the data-subject **(2)**. Independent of the question whether the employer can be considered as telecommunication services' provider, which may be the case when he provides his employee with the smart device and/or the technical infrastructure to use it, the validity of the employee's consent may be doubted. On the one hand, such consent must base on an **informed decision** which presupposes a – in most cases missing – thorough technical clarification about any personal data affecting services. On the other hand, in consideration of the structural imbalance between employer and employee the **voluntariness of an employee's consent** may often be questionable as it cannot be ruled out that the employee feels himself forced to consent to the data processing and therefore does not dare to deactivate the collection and transmission of geo-data on his smart device.*

(2) Sec. 98 Telekommunikationsgesetz ("TKG" – Telecommunications Law)

▪ *In default of consent the collection and processing of geo-data may be legitimized by the **general permissive rule of employees' data protection law (3)**. According to this, personal data of an employee may be collected, processed or used for employment-related purposes where necessary for hiring decisions or, after hiring, for carrying out or terminating the employment contract. This requires a comprehensive weighing of interests of both parties with due regard to the purposes of the specific data processing. In respect of geo-data the rule is that employees **must not be located in their protected area of life**, e.g. in break, sanitary or private rooms, and must usually **not be permanently observed** during their working time. Hence, processing and analyzing employees' geo-data are limited to specific information needs of the employer for either controlling or organizational purposes, i.e. for the coordination of*

(3) Sec. 32 Bundesdatenschutzgesetz ("BDSG" – Federal Data Protection Act)

*working processes. Even in that case the storage of geo-data should always be realized in anonymous form to avoid the creation of employees' data profiles.*

▪ *Furthermore, the employee has to be* ***informed*** *about the collection and processing of his personal geo-data and the purposes of such activities, if he is not already aware of these facts anyway* ***(4).*** *The consequence of lacking transparency is the employer's obligation to delete any personal data referring to such employee, and the* ***risk of a punishment fine*** *up to 50,000.00 € for an administrative offence* ***(5)****.*

▪ *Apart from this, with respect to all geo-data processing activities potential* ***works council's rights*** *have to be taken into account. In general, the works council has a right of co-determination in matters relating to the rules of operation and the conduct of employees in the establishment* ***(6)****, and, what is even more relevant for the processing of employees' personal data, at the introduction and use of technical devices designed to monitor the behavior or performance of the employees* ***(7)****. These rights remain unaffected by the data protection law provisions* ***(8)****, and already apply when the technical devices are objectively suitable to control the employees' behavior or performance so that the surveillance only depends on the employer's volition* ***(9)****. Against this background, the processing of employees' geo-data will usually require a so-called* ***work agreement*** *between the works council and the employer* ***(10)*** *containing specific regulations on the preconditions and the scope of such data processing which may then serve as legitimization for the collection and analyzation of geo-data by the employer.*

▪ *In conclusion, no matter of the statutory basis of the data processing the general principle of* ***data reduction and data economy*** *must always be kept in mind. This means that any data processing activities shall pursue the aim of collecting, processing and using as little personal data as possible* ***(11)****. Concerning geo-data this can be realized best by implementing IT-systems which locate themselves and transfer the self-collected geo-data only on request of an authority, and which enable the employee to even deactivate geo-tracking services* ***(12)****. In any case, the most effective way to cope with data protection requirements is to implement economical technology as regards the collection and processing of personal data. This is why the so-called* ***"privacy by design"*** *evolves into the most effective instrument of data protection in the Industry 4.0.*

(4) Sec. 33 par. 1 BDSG

(5) Sec. 43 par. 1 and 2 BDSG

(6) Sec. 87 No. 1 Betriebsverfassungsgesetz ("BetrVG" – Works Constitution Act)

(7) Sec. 87 No. 6 BetrVG

(8) Sec. 32 par. 3 BDSG

(9) Constant jurisdiction of the German Federal Labour Court since judgement of 9.9.1975, AP BetrVG 1972 Sec. 87 Überwachung No. 2

(10) Sec. 77 BetrVG

(11) Sec. 3a sentence 1 BDSG

(12) Hofmann, "Smart factory – Employees' data protection in Industry 4.0", in DSRITB 2015, 209 (220)

ANDREAS LOBER
&
SUSANNE KLEIN

REFERENCES

▪ Le droit belge n'aborde pas spécifiquement la question de la géolocalisation des travailleurs. Les lois et principes généraux en matière de surveillance des travailleurs et de protection de leur vie privée doivent donc être examinés.

▪ Il faut donc vérifier la base légale ou la justification de la géolocalisation, ses finalités et le caractère proportionné de sa mise en œuvre au regard des finalités.

▪ Il est tout d'abord très clair que cette géolocalisation n'est autorisée que pendant les heures de travail, et ce même si le travailleur dispose d'un véhicule ou d'un smartphone de société, comme c'est souvent le cas en Belgique.

▪ Il n'existe pas de base légale imposant ou permettant explicitement la géolocalisation. L'on recherchera la base légale dans la loi du 8 décembre 1992 relative aux traitements de données à caractère personnel. La géolocalisation – qui constitue un tel traitement – ne pourra en conséquence intervenir que si elle est nécessaire à l'exécution du contrat de travail, moyennant le consentement du travailleur ou imposée par une obligation légale.

(1) art. 9 de la loi du 8 décembre 1992

▪ Quand bien même le consentement du travailleur ne serait pas expressément requis, l'information du travailleur est obligatoire **(1)**. La procédure d'information et de concertation sur les conséquences sociales de l'introduction de nouvelles technologies, organisée par la convention collective de travail **(2)**, peut être suivie pour assurer une meilleure sécurité juridique. S'il existe un conseil d'entreprise, celui-ci doit être informé et consulté préalablement à la mise en place d'un tel système.

(2) CCT n°39 du 13 décembre 1983

▪ L'employeur doit définir les finalités du traitement des données (l'optimisation de l'exécution du contrat de travail, la sécurité des personnes et des biens,…) et les moyens de géolocalisation mis en œuvre doivent être proportionnés aux finalités visées. Il s'agit d'une question d'appréciation, et la jurisprudence belge est encore assez pauvre à ce sujet.

▪ La géolocalisation des véhicules utilisés par les travailleurs pendant les heures de travail est maintenant passée dans les mœurs et bien encadrée par la doctrine. Les quelques cas de jurisprudence concernent d'ailleurs cette pratique. Même si elle tacitement autorisée, il est toutefois sans doute prématuré d'envisager une géolocalisation personnelle des travailleurs, sauf dans des hypothèses très particulières. Il est en effet probable que ce type de géolocalisation très intrusive entraine un tollé des représentants des travailleurs et ne soit pas validé par les magistrats en cas de litige.

ALEXANDRE CASSART

▪ *Belgian law does not specifically address the issue of the geolocation of workers. Then, law and general principles related to surveillance of workers and protection of their privacy should be examined.*

▪ *One must therefore check the legal ground or the justification of this geolocation, its purpose and the proportionality of its implementation in relation to purposes.*

▪ *First of all it is clear that geolocation is allowed only during working hours, even if the employee has a company vehicle or smartphone, as it is often the case in Belgium.*

▪ *There is no legal basis for explicitly imposing or allowing geolocation. The legal basis could then be found in the Act of 1992 relating to personal data processing. Geolocation will only be allowed, if it is necessary for the performance of the employment contract, with the consent of the worker or if it is imposed by a legal obligation associated to the employment contract.*

*(1) article 9 of the Law of 8 December 1992)*

▪ *Even though the worker's consent is not expressly required, prior information of worker is mandatory* ***(1)****. The information and consultation procedure on the social consequences of the introduction of new technologies, organized by a collective labor agreement* ***(2)*** *can be followed to ensure greater legal certainty and clarity. If there is a works council, it must be informed and consulted prior to the establishment of such a system.*

(2) *CCT No 39 of 13 December 1983*

▪ *The employer must define the purpose of the data processing (optimizing the performance of the employment contract, the safety of people and goods...) and the geolocation-means used should be proportionate to the purposes referred to. This is a matter of interpretation, and Belgian case law is still quite poor on this.*

▪ *The geolocation of vehicles used by workers during working hours is now a standard practice and well described by the doctrine. Besides, the few existing case law on this subject concern this specific practice. Even if it is tacitly authorized, at this point, it is still probably premature to even consider a personal geolocation of workers, except in very special circumstances. It is indeed likely that such highly intrusive geolocation would cause an outcry of workers' representatives and consequently would not be validated by any judge in case of dispute.*

ALEXANDRE CASSART



▪ En perpétuelle évolution, les technologies de l'information progressent bien plus vite que le législateur, qui a du mal à suivre ce rythme effréné et à avoir le recul nécessaire pour en saisir toutes les composantes. En matière de droit social, comme dans d'autres domaines, il est ainsi bien souvent nécessaire d'attendre que les juges se prononcent sur des cas concrets pour décrypter comment tirer parti des nouvelles technologies dans l'entreprise tout en garantissant le respect des droits constitutionnels des salariés, et notamment le droit à la protection des données à caractère personnel.

**Droit costaricain**

▪ Au Costa Rica, un employeur peut tout à fait, afin d'améliorer ses activités, utiliser des méthodes destinées à optimiser l'efficacité et la fiabilité des tâches réalisées par ses salariés.

▪ La technologie est un outil précieux pour les chefs d'entreprise : grâce à elle, ils sont en mesure non seulement de communiquer plus rapidement avec leurs salariés (la plupart d'être eux sont équipés de smartphones leur permettant d'être joignables à tout instant et de répondre instantanément aux courriels reçus) mais aussi de localiser ceux dont le travail est essentiellement effectué à l'extérieur des locaux de l'entreprise, comme par exemple les coursiers, les VRP, etc.

▪ D'une manière générale, les employeurs ont le droit de surveiller et de contrôler le travail de leurs salariés. A cet effet, ils peuvent par exemple équiper leur flotte automobile de dispositifs GPS, autant pour des raisons de sécurité que d'efficacité du travail. Il leur est également possible d'installer certaines applications sur les téléphones portables fournis aux salariés, les rendant ainsi « virtuellement » disponibles pendant leurs heures de travail.

▪ Les pouvoirs de l'employeur sont toutefois limités par le droit constitutionnel à la vie privée, inhérent à tout individu, et auquel il ne peut porter atteinte. En effet, selon l'article 24 de la Constitution du Costa Rica : « *Le droit à l'intimité, à la liberté et au secret des communications est garanti. [...]* ». Le pays est, en outre, signataire de plusieurs traités internationaux, garantissant les mêmes droits **(1)**. Le Costa Rica a également adopté, en 2011, la loi n°8968 sur la protection des données personnelles, qui précise le droit à l'autonomie informationnelle et le principe de consentement éclairé.

(1) **Déclaration universelle des droits de l'homme** : Article 12 : « Nul ne sera l'objet d'immixtions arbitraires dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes à son honneur et à sa réputation. Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes ».

**Déclaration américaine des droits et devoirs de l'homme** : Article V : « Toute personne a droit à la protection de la loi contre les attaques abusives envers son honneur, sa réputation et sa vie privée et familiale ».

**Convention américaine relative aux droits de l'homme :** Article 11 : **Protection de l'honneur et de la dignité de la personne** :
« 1. Toute personne a droit au respect de son honneur et à la reconnaissance de sa dignité.
2. Nul ne peut être l'objet d'ingérences arbitraires ou abusives dans sa vie privée, dans la vie de sa famille, dans son domicile ou sa correspondance, ni d'attaques illégales à son

## Le GPS et autres méthodes de localisation des salariés

▪ La collecte, par l'employeur, de données personnelles au moyen d'un système GPS ou de tout autre appareil, est spécifiquement soumise à la loi n°8968, visée ci-dessus, ainsi qu'à son décret d'application. Les entreprises doivent donc veiller à prendre en considération les implications juridiques du traitement des données à caractère personnel de leurs salariés obtenues par des dispositifs de géolocalisation. Les employeurs sont tenus de traiter ces données de manière appropriée et de vérifier que le fournisseur du service de géolocalisation respecte bien les normes de sécurité requises pour garantir leur protection. A défaut, le dirigeant de l'entreprise s'expose inutilement à de nombreux risques.

▪ Les méthodes de géolocalisation les plus répandues au Costa Rica sont le GPS, le Wi-Fi ainsi que certaines applications mobiles. Les données recueillies concernent les trajets effectués par une personne, avec indication de l'itinéraire pris, de l'heure de chaque arrêt, des lieux visités etc., y compris en dehors des heures de travail, ce qui constitue incontestablement une intrusion dans la vie privée.

▪ Dans sa résolution n°14-01574300007-CO datée du 24 octobre 2014, la Cour constitutionnelle costaricaine a estimé que : « *La vie privée est constituée des circonstances, comportements, données et situations d'un individu qui ne sont généralement pas connus des tiers et dont la divulgation porterait atteinte à l'honneur ou la dignité de cet individu, sauf si ledit individu a accepté de les partager. Relève de la vie privée tout ce qui se passe non seulement à l'intérieur du domicile d'un individu, mais également dans les bureaux, les domiciles d'amis ainsi que tout autre endroit privé. A cet égard, les droits constitutionnels d'inviolabilité du domicile, des documents privés et des autres correspondances et données existent dans le seul but de protéger la vie privée en général [...]* ».

▪ En l'espèce, s'agissant un salarié du secteur public, la Cour a également précisé que « *la garantie d'un droit fondamental ne dépend pas de qui est le propriétaire de l'équipement [utilisé], et en au contraire, totalement indépendante (En ce sens, voir la décision de la Cour européenne des droits de l'homme 827/1997 du 24 août 1998, Lambert c/ France). En travaillant dans le secteur public, les fonctionnaires ne renoncent pas à leur vie privée ou à la protection de leurs données, ils s'attendent au contraire à bénéficier d'un certain degré d'intimité sur leur lieu de travail où ils développent des relations personnelles... »*.

▪ Enfin, un avis émis par le service juridique du Ministère du travail (DAJ-AE-108-11) est venu préciser qu'un dispositif GPS ne peut être installé que sur des véhicules de fonction, et en aucun cas sur le véhicule personnel du salarié. Cet avis fixe aussi le régime applicable aux

honneur et à sa réputation.
3. Toute personne a droit à la protection de la loi contre de telles ingérences ou de telles attaques ».

**Pacte international relatif aux droits civils et politiques** : Article 17 :
« 1. Nul ne sera l'objet d'immixtions arbitraires ou illégales dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes illégales à son honneur et à sa réputation.
2. Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes ».

**Convention de sauvegarde des Droits de l'Homme et des Libertés fondamentales** : Article 8 : Droit au respect de la vie privée et familiale :
« 1. Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance.
2. Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté

« *Empleado de Confianza* », c'est-à-dire aux salariés occupant un poste confiance, tels les agents, les commerciaux, et autres membres du personnel qui exercent leur activité principalement en dehors des locaux de l'entreprise, et qui à ce titre peuvent effectuer jusqu'à 12h de travail par jour sans être rémunérés pour leurs heures supplémentaires. L'installation d'un GPS dans le véhicule de fonction de ces salariés autonomes, qui les rend géolocalisables à tout moment, emporte la perte de ce statut et impose, de fait, la limitation de leurs heures de travail à 8 heures par jour.

publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui ».

## Conclusion

▪ En résumé, la géolocalisation des salariés est autorisée au Costa Rica dans les limites suivantes :

- l'utilisation d'un dispositif GPS ou de tout autre appareil de géolocalisation est justifiée par le besoin de l'employeur d'améliorer son entreprise et ses activités ;
- le GPS doit être installé exclusivement sur le véhicule de fonction, et en aucun cas sur le véhicule personnel du salarié ;
- le salarié doit être préalablement informé de l'existence du dispositif GPS, des données qu'il collecte et de ses heures d'utilisation ;
- l'employeur doit indiquer, par écrit, que les données recueillies sont susceptibles d'être utilisées à l'encontre du salarié pour des sanctions disciplinaires, une procédure de licenciement, voire des poursuites pénales, en fonction de la gravité de la faute commise ;
- lorsqu'une application de géolocalisation est installée sur un smartphone, son fonctionnement doit être limité aux heures de travail ;
- l'employeur doit tout mettre en œuvre pour éviter toute atteinte à la vie privée du salarié, et empêcher toute utilisation des données collectées par le dispositif de géolocalisation pour des finalités non liées à la performance du salarié ;
- les salariés qui font l'objet d'une géolocalisation par un GPS ou tout autre dispositif similaire ne peuvent bénéficier du statut de « Empleado de Confianza ».

GABRIEL LIZAMA

*Information Technology changes every day and very fast. Unfortunately, local legislations are not always hand-to-hand with those changes, and there is a need to wait for Court precedents that help us understand how technology and specifically protection of personal data can be included in the labor relationships without breaching constitutional rights.*

***Costa Rican Law***

- *According to Costa Rican Labor Law, employers have the right to improve their businesses by including some methods to make the work done by their employees more efficient, reliable and in a secure manner.*

- *Technology is a great asset nowadays, as it makes communications faster –one expects to have quick answer to an email sent, as most people have smart phones, which makes you available at any time- and also can help you tracking down employees whose work is basically done outside the employer's premises, such as carriers, agents, etc.*

- *In general terms, employers have the prerogative of supervision and control over the employees work, and in so doing they are allowed to install GPS devices in their fleet, for security purposes or increasing the efficiency of the work done. It is also possible, to install certain apps in the mobile phones given by the employer to employees, in order to make them "virtually" available during working hours.*

- *However, the employer's faculties or prerogatives given by law, cannot supersede the constitutional rights of privacy inherent to all individuals. Our Constitution in its article 24, partially states: "***Article 24:** The right to intimacy, to freedom and to the secrecy of communications is guaranteed. …" *In addition, Costa Rica is also signatory and part of the following treaties **(1)**. Moreover, Costa Rica passed in 2011 the Protection of Personal Data Law # 8968, which describes the right to the informational self-determination and the principle of informed consent.*

***Use of GPS and other methods for tracking employees***

- *Said that, the personal data collected by the employer –through GPS or any other device- is subject specifically to the Protection of Personal Data Law abovementioned and its bylaw. However, employers are not considering the legal implications of dealing with personal data of their employees obtained through localization devices. Every employer should*

## REFERENCES

(1) ***Universal Declaration of Human Rights:*** *Article 12: No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.*

***American Declaration of Duties and Rights of Men****: Article 5: Every person has the right to the protection of the law against abusive attacks upon his honor, his reputation, and his private and family life.*

***American Convention of Human Rights:*** *Article 11: Right to Privacy:*
*1. Everyone has the right to have his honor respected and his dignity recognized.*
*2. No one may be the object of arbitrary or abusive interference with his private life, his family, his home, or his correspondence, or of unlawful attacks on his honor or reputation.*
*3. Everyone has the right to the protection of the law against such interference or attacks.*

*give a proper treatment of said personal data and verify that the provider of such service (localization), meet with the security standards in order to protect the information. The non-observation of said regulation, could generate unnecessary risks to the employer's operation.*

- *The most common devices for tracking employees in the country are GPS, Wi-Fi and some apps installed in the smart phones. The information gathered with their use, includes routes taken to keep a record of the user's movements and time in each stop, places attended etc., inclusive in non-working hours, which is definitely an intrusion to user's privacy.*

- *Our Constitutional Court, in the resolution #14-01574300007-CO, dated October, 24th, 2014, establishes the following:* "Privacy is formed by those circumstances, behaviors, data and situations of an individual which is not normally known by third parties and if known will trouble its owner's moral or dignity, unless said person has agreed to share it. We can say that whatever happens inside any person's house is considered as private life, but also we can also include in this scenario, offices, friend's houses and any other private place. Said that, constitutional rights of inviolability of home, of private documents and other communications and data, exist for the sole purpose of protecting said privacy in general. *…".*

- *In the same resolution, making reference to a public employee says: "The guarantee of a fundamental right does not depend whose the owner of the mean, on the contrary it is totally independent. (In that sense, review the sentence of the EU Tribunal of Human Rights of August 24th, 1998, #827/1997, Lambert vs. France). Public workers does not relinquish their privacy sphere or their data protection because of being public workers, on the contrary, they also expect to have certain degree of privacy in their jobs, since they develop interpersonal relationships there …".*

- *According to a Legal Opinion issued by the Legal Department of the Labor Department, DAJ-AE-108-11, GPS can only be installed in the employer's vehicles, never on the personal automobile of the employee. This opinion also establishes, that the agents, salesman/saleswomen, and all personnel that performs the work most of the time outside the workplace and known as "Trusted Employee" (Empleado de Confianza), which working hours can be up to 12 without paying over time; if a GPS is installed in the employer's vehicle will no longer be considered as Trusted Employee and therefore, the working hours will be diminished to 8 working hours, as the employer can be "virtually" located at any time.*

***International Pact of Civil and Political Rights:*** *Article 17:*
*1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.*
*2. Everyone has the right to the protection of the law against such interference or attacks.*

***European Convention for the Protection of Human Rights and Fundamental Freedoms:*** *Article 8: Right to respect for private and family life: Everyone has the right to respect for his private and family life, his home and his correspondence. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.*

*Conclusion*

- *Geolocation of employees in Costa Rica is possible if met the following:*
  - *The use of GPS or any other tracking device must be validated as a need of the employer to improve the security of the business and/or the core of business itself.*
  - *The GPS must be installed in the employer's fleet, never on the persona vehicle of the employee.*
  - *The employee must be previously informed of the existence of the GPS, the data to be collected and the hours of use.*
  - *Employer must also state in writing, that the information gathered could be used for admonished purposes and even the discharge of the company. Depending on the magnitude of the fault could also be used to file criminal charges.*
  - *If a tracking app is installed in the smartphone, should be limited to operate during working hours.*
  - *Employer must do whatever is in his power to avoid the intrusion of the employee's privacy and the use of the data gathered with the tracking device for purposes other than those related to how the employee performed his work.*
  - *Employer cannot argue under Costa Rican Labor Law, employees that can be tracked down with GPS and/or any other device are Trusted Employees.*

GABRIEL LIZAMA

▪ Il est de plus en plus courant pour les entreprises de recueillir les données de localisation d'un travailleur, soit directement (localisation du travailleur lui-même), soit indirectement (localisation d'un véhicule qu'il utilise, ou d'un produit ou d'un bien dont il a la charge), et ce moyennant l'utilisation d'outils de plus en plus performants qui permettent aux entreprises de déterminer la position géographique d'un travailleur à un moment donné ou continuellement. Ces informations peuvent provenir du traitement des données provenant de satellites (GPS), d'un réseau de communications électroniques (téléphonie mobile, réseau Wi-Fi) ou de tout autre dispositif (par exemple, par un lecteur RFID).

▪ L'article 2 de la Directive « Vie Privée et Communications Électroniques » (1) définit les données de localisation comme « *toutes les données traitées dans un réseau de communications électroniques indiquant la position géographique de l'équipement terminal d'un utilisateur d'un service de communications électroniques accessible au public* ». Cette définition est reprise à l'article 64 b) du Règlement espagnol sur les conditions pour la prestation de services de communications électroniques, le service universel et la protection des usagers **(2)**.

▪ Par conséquent et tenant compte du fait que les données de localisation concernent toujours une personne physique identifiée ou identifiable, l'accès par l'entreprise aux données de localisation de son personnel constitue un traitement de données à caractère personnelle soumis à la loi espagnole sur la matière **(3)**.

▪ Selon la jurisprudence espagnole et les résolutions de l'AEPD **(4)**, le traitement des données de localisation des travailleurs doit respecter les principes de nécessité (surveiller les travailleurs de la manière la moins intrusive possible) et de proportionnalité (la mesure doit être proportionnée à la finalité qui justifie le traitement des données de localisation).

▪ Cette analyse doit se faire cas par cas, mais un tel traitement serait justifié lorsqu'il est effectué aux fins de la surveillance du transport de personnes ou de marchandises, d'une meilleure affectation des ressources pour des prestations à fournir en des lieux dispersés (par exemple, planification en temps réel des opérations) ou de la poursuite d'un objectif de sécurité, qu'il s'agisse de celle du travailleur lui-même ou des marchandises ou véhicules dont il a la charge. Par contre, le traitement serait considéré comme excessif si les travailleurs sont libres d'organiser leurs déplacements comme ils l'entendent ou si le contrôle de leur travail constitue la seule finalité dudit traitement alors que ce contrôle pourrait être réalisé par d'autres moyens. En tout état de cause, il est interdit à un employeur de recueillir les données de localisation d'un travailleur en dehors des horaires de travail de ce dernier.

▪ L'AEPD, conformément aussi à l'Avis du groupe de l'article 29, recommande que la durée de conservation des données de localisation soit raisonnable (pas plus de 2 mois). Au cas où un employeur souhaite traiter les données de localisation pendant plus de 2 mois, l'AEPD recommande que ces données soient préalablement rendues anonymes.

## REFERENCES

(1) Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques

(2) Approuvé par le Real Decreto 424/2005 du 15 avril

(3) Ley Orgánica 15/1999, du 13 décembre, sur la protection des données à caractère personnel

(4) Entre autres, l'arrêt de la Cour Constitutionnelle n°186/2000 et l'arrêt n°186/2001 de la Cour Suprême. Cf. également le rapport n°613/2009 de l'Agencia Española de Protección de Datos qui reprend en partie l'Avis 5/2005 du G29 sur l'utilisation de données de localisation aux fins de fourniture de services à valeur ajoutée

MARC GALLARDO

- *It is increasingly common for companies to collect data on the location of an employee, either directly (location of the employee himself) or indirectly (location of the vehicle used by the employee or of a product or asset in his charge) through the use of increasingly powerful tools that allow companies to identify the geographic position of their staff at a given moment or continuously. This information can be based on the processing of data from satellites (GPS), from an electronic communications network (mobile telephone, Wi-Fi network) or from any other device (such as an RFID reader).*

- *Article 2 of the Directive on privacy and electronic communications* ***(1)*** *defined 'location data'* as any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service*". This definition is included in Article 64(b) of the Spanish Regulation on conditions for the provision of electronic communications services, universal service and protection of users* ***(2)****.*

- *Since location data always relate to an identified or identifiable natural person, the access by a company to the location data of its employees constitutes personal data processing and is subject to Spanish law on personal data* ***(3)****.*

- *According to Spanish law and the resolutions of the data protection authority, the AEPD* ***(4)****, the processing of location data on employees must respect the principles of necessity (surveillance of workers must be carried out in the least intrusive way possible) and proportionality (the measure must be appropriate in view of the purpose advanced as justification for processing location data).*

- *Such analysis has to be made on a case-by-case basis, but such processing would be justified where it is done as part of monitoring the transport of people or goods or improving the distribution of resources for services in scattered locations (e.g. planning operations in real time), or where a security objective is being pursued in relation to the employee himself or to the goods or vehicles in his charge. Conversely, data processing would be excessive where employees are free to organise their travel arrangements as they wish or where it is done for the sole purpose of monitoring an employee's work where this can be monitored by other means. In any event, an employer should not collect location data relating to an employee outside the latter's working hours.*

- *In accordance with the Opinion of the Article 29 Working Party, the AEPD recommends that the location data retention period be reasonable (i.e. no longer than 2 months). Where an employer wishes to process location data for longer than two months, the AEPD recommends that the data first be rendered anonymous.*

## REFERENCES

(1) Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector

(2) Approved by Real Decreto 424/2005 of 15 April

(3) Ley Orgánica 15/1999 of 13 December on the protection of personal data

(4. Among others, judgment No. 186/2000 of the Constitutional Court and No. 186/2001 of the Supreme Court. See also Report No. 613/2009 of the Agencia Española de Protección de Datos which partly relied on Opinion 5/2005 of the Article 29 Working Party on the use of location data with a view to providing value added services

MARC GALLARDO

La géolocalisation des salariés est devenue une pratique répandue dans le monde du travail. L'encadrement législatif d'un tel dispositif constitue un enjeu majeur au regard du droit au respect de la vie privée des salariés. L'heure a sonné de faire un état du droit sur la géolocalisation des salariés en France.

## Définition

▪ La géolocalisation est une technologie associée à un traitement de données personnelles, qui a pour but de déterminer la localisation d'un objet ou d'une personne par le biais d'un système GPS ou d'un téléphone mobile. Installé dans le téléphone ou le véhicule d'un salarié, la géolocalisation constitue un outil de traçage du salarié, et risque, de manière inhérente, de porter atteinte à sa liberté d'aller et de venir et à sa vie privée.

▪ Conscient de ces risques et animé par la volonté de préserver les droits fondamentaux du salarié, le législateur a encadré les modalités de mise en œuvre des dispositifs de géolocalisation des salariés. La Commission Nationale de l'Informatique et des Libertés (ci-après, la « Cnil »), témoin de l'évolution des usages, est venue en préciser les règles.

## Sacro-saint principe de proportionnalité

▪ La légitimité du traitement de données personnelles issu d'un dispositif de géolocalisation est appréciée à la lumière du principe de proportionnalité tel qu'il résulte de l'article L. 1121-1 du Code du travail. En se fondant sur cet article, la Cour de cassation **(1)** a considéré que l'employeur qui géolocalise en permanence ses salariés organise une filature. Une telle géolocalisation, mise en œuvre sans limite, est disproportionnée. En conséquence, les moyens de preuve issus du dispositif sont illicites, sans considération de l'information des salariés.

(1) Cass. soc. 26-11-2002 n°00-42.401

## Obligation d'information

▪ L'information préalable à l'installation d'un système de géolocalisation est multiple. D'une part, l'employeur doit respecter la procédure d'information-consultation des institutions représentatives du personnel. En effet, le Code du travail impose le respect de la procédure d'information-consultation du comité d'entreprise **(2)** et du CHSCT **(3)**. D'autre part, dès lors que la géolocalisation constitue un

(2) C. trav. art. L. 2323-29

(3) C. trav. art. L. 4612-9

traitement de données à caractère personnel au sens de l'article 2 de la loi informatique et libertés, l'employeur doit en informer les salariés. Chaque salarié concerné par la géolocalisation doit donc être destinataire de l'ensemble des informations de l'article 32 de la loi informatique et libertés, notamment de l'identité du responsable de traitement, des finalités poursuivies par le traitement de données et des destinataires des données **(4)**.

(4) https://www.legifrance.gouv.fr/affichTexteArticle.do;jsessionid=DFABA807388D3939CB8EE14CE5F7CD7F.tpdila23v_1?idArticle=LEGIARTI000024506226&cidTexte=LEGITEXT000006068624&dateTexte=20160920

### Finalités autorisées

▪ Par la délibération n° 2006-067 du 16 mars 2006, la Cnil a adopté la norme simplifiée n° 51 concernant les traitements automatisés de données à caractère personnel mis en œuvre par les organismes publics ou privés destinés à géolocaliser les véhicules utilisés par leurs employés. L'évolution des usages a rapidement conduit la Cnil à adapter la réglementation de la géolocalisation des salariés. C'est ainsi que dans le prolongement d'une recommandation du Conseil de l'Europe du 1er avril 2015, la Commission a modifié la norme simplifiée n° 51, par une délibération du 4 juin 2015 **(5)**. L'employeur est désormais autorisé à installer un dispositif de géolocalisation dans les véhicules de ses employés pour répondre aux finalités suivantes :

(5) https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000030741771

- suivre, justifier et facturer une prestation de transport de personnes, de marchandises ou de services directement en lien avec l'utilisation du véhicule ;
- assurer la sécurité du salarié, des marchandises ou des véhicules dont il a la charge ; cette finalité inclut notamment la recherche du véhicule en cas de vol ;
- maximiser l'allocation des moyens déployés pour des prestations à accomplir en des lieux dispersés ;
- contrôler le respect des règles d'utilisation du véhicule par le salarié ;
- respecter une obligation légale ou réglementaire imposant la mise en œuvre d'un dispositif de géolocalisation en raison du type de transport ou de la nature des biens transportés ;
- suivre le temps de travail du salarié, uniquement lorsque cette finalité ne peut être accomplie par un moyen alternatif.

### Finalités exclues

▪ Au nom de la protection de la vie privée du salarié, un dispositif de géolocalisation ne peut avoir pour finalité de contrôler le respect des limitations de vitesse. Il est également interdit de contrôler en permanence un salarié, en particulier s'il dispose d'une liberté dans l'organisation de ses déplacements, à l'instar du VRP. Les

représentants du personnel bénéficient également d'une protection renforcée puisque l'employeur ne peut collecter les données de localisation dans le cadre de l'exercice de leur mandat. Enfin, il est interdit à l'employeur de collecter les données de localisation des salariés en-dehors du temps de travail. Cette interdiction s'applique à tous les salariés sans distinction.

### Désactivation obligatoire de la collecte de données

▪ Par la délibération du 4 juin 2015, la Cnil a accordé une garantie supplémentaire aux salariés, en rendant obligatoire pour l'employeur la mise en œuvre d'un mécanisme permettant de désactiver la collecte des données. Tout au long de la désactivation du dispositif, notamment sur les temps de pause du salarié ou ses trajets domicile-travail, l'employeur est privé de l'accès au suivi détaillé des trajets de ses salariés. Cette garantie supplémentaire participe de la protection renforcée de la vie privée des salariés.

### Durée de conservation limitée

▪ Aux termes de l'article 5 de la délibération du 4 juin 2015, une durée de conservation de deux mois est considérée par la Cnil comme adéquate. L'employeur ne peut conserver les données de traçage de ses salariés que pour une durée limitée, ce qui participe, là encore, de la protection de leur vie privée.

### Formalités Cnil

▪ Un dispositif de géolocalisation des salariés doit être déclaré à la Cnil, sous réserve d'être inopposable aux salariés. L'employeur peut remplir cette formalité par un engagement de conformité à la norme simplifiée n° 51, ou par une déclaration normale. Dans l'hypothèse où l'entreprise dispose d'un correspondant informatique et libertés (ci-après, « Cil »), aucune formalité n'est nécessaire auprès de la Cnil, mais le Cil doit inscrire le dispositif de géolocalisation dans son registre.

▪ La protection du droit à la vie privée du salarié et le rétablissement de la frontière entre vie professionnelle et vie personnelle sont au cœur de l'écosystème du droit du travail. L'encadrement de la géolocalisation des salariés ou la consécration du droit à la déconnexion par la loi travail en sont des illustrations patentes. La protection de la vie privée du salarié devient le centre de gravité des enjeux liés au droit du travail.

EMMANUEL WALLE
&
CLÉMENTINE JOACHIM

*The geolocation of employees is a common practice in the working environment. Establishing a legal framework for the use of such a process constitutes a major stake in regards to the right of privacy. It is now time to review the legislation surrounding the geolocation of employees in France.*

### *Definition*

▪ *Geolocation is a technology associated with the processing of personal data, which goal is to determine the location of an object or a person through a GPS or a mobile phone. Geolocation is a tool that allows tracking the employee through his phone or vehicle, which might inherently threaten his right to come and go as well as his privacy.*

▪ *The legislator, aware of these risks and dedicated to preserving the fundamental rights of employees, has set up a framework surrounding the use of devices to locate employees. The French data protection authority ("CNIL"), after witnessing the progress of practices, has clarified the rules pertaining to geolocation.*

### *The sacrosanct principle of proportionality*

▪ *The lawfulness of the processing of personal data collected through a geolocation device must be assessed in light of the principle of proportionality, as defined by article L.1121-1 of the Labour Code. Based on this article, the Cour de cassation **(1)** has determined that an uninterrupted geolocation of employees equates to tailing them. Such tracking, implemented with no limit, is disproportionate. Therefore, the evidence that is obtained by this method is unlawful, regardless of the employees' information.*

(1) Cass. soc. 26-11-2002 n°00-42.401

### *The notification requirement*

▪ *The obligation to provide notification prior to the use of geolocation devices is broad. First, the employer must comply with the procedure for information and consultation of the employees' representative body. Indeed, the Labour Code requires compliance with the procedure for information and consultation of the Works Council **(2)** and the Workplace Health and Safety Committee **(3)**. Second, since geolocation involves the processing of personal data within the ambit of Article 2 of the Data Protection Act, the employer must inform the*

(2) Labour Code, art. L. 2323-29

(3) Labour Code, art. L. 4612-9

*employees. Each employee that is subject to geolocation must therefore receive all the information stated in Article 32 of the Data Protection Act, in particular the identity of the data controller, the purposes for which the data are processed and the recipients of these data* ***(4)****.*

### *Authorized purposes*

▪ *In Deliberation n°2006-067 of 16 March 2006, the CNIL adopted Simplified Standard n°51 regarding the automatic processing of personal data by public or private organisations in order to locate vehicles used by their employees. Technological progress quickly led the CNIL to adapt the law on geolocation of employees. That is why, in the extension of a recommendation by the Council of Europe from 1 April 2015, the CNIL has modified the Simplified Standard n°51 by a Deliberation from 4 June 2015* ***(5)****. The employer is now authorized to install a geolocation device in his employees' vehicles for the following purposes:*

- *follow, prove and bill the transport of people or goods, or the supply of services directly in line with the use of the vehicle;*
- *ensure the security of the employee himself or of the goods or vehicles in his charge, including for vehicle theft protection;*
- *maximize the distribution of resources deployed for the performance of services in scattered locations;*
- *monitor employee's compliance with the vehicle's rules of use;*
- *comply with a legal or regulatory requirement to implement a geolocation device due to the type of transportation or the nature of the goods transported;*
- *monitor the working hours of the employee, but only when this cannot be done otherwise.*

### *Prohibited purposes*

▪ *To protect the privacy of employees, a geolocation device may not have the purpose of monitoring compliance with speed limits. It is also forbidden to continuously monitor an employee, especially if he is free to organize his travel arrangements as he wishes, as is the case with a sales representative. Staff representatives also benefit from enhanced protection as the employer cannot collect location data in connection with the exercise of their duties. Finally, an employer must not collect the location data of employees outside their working hours. This prohibition applies to all employees, without distinction.*

(4) https://www.legifrance.gouv.fr/affichTexteArticle.do;jsessionid=DFABA807388D3939CB8EE14CE5F7CD7F.tpdila23v_1?idArticle=LEGIARTI000024506226&cidTexte=LEGITEXT000006068624&dateTexte=20160920

(5) https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000030741771

*Obligation to switch off*

▪ *By Deliberation of 4 June 2015, the CNIL granted an additional guarantee to employees, by requiring the employer to implement a mechanism to switch off the collection of data by the location device. When the device is off, such as during employee's break or commuting time, employers may not access detailed location data of their employees. This additional guarantee bolsters the protection of employees' privacy.*

*Limited shelf life*

▪ *Under Article 5 of Deliberation of 4 June 2015, a two-month retention period is considered adequate by CNIL. The employer may retain his employees tracking data only for a limited period, again for the purposes of protecting their privacy.*

*CNIL formalities*

▪ *An employee geolocation device must be notified to the CNIL; otherwise, it cannot be enforced against employees. The employer may fulfil this notification formality either by self-certifying to simplified standard No. 51, or by filing a normal notification. If the company has a data protection officer ("DPO", also known as "CIL" in France), no formalities are necessary with the CNIL, but the DPO must enter the geolocation device in his register.*

▪ *The protection of employees' right to privacy and the maintenance of a work-life balance are at the heart of the employment law ecosystem, as perfectly illustrated by the supervision of employee geolocation devices, or by the 'right to disconnect' (that is, the right to be disconnected from work-related digital tools during non-working hours) enshrined in the recent Labour Act. The protection of employee privacy has thus become the centre of gravity of the stakes related to labour law.*

EMMANUEL
WALLE
&
CLEMENTINE
JOACHIM



▪ Les systèmes de géolocalisation des salariés mis en œuvre par les employeurs impliquant la collecte et le traitement d'informations constituées en grande partie de données à caractère personnel, ils sont donc soumis à la règlementation relative à la protection des données. Au reste, le Règlement général sur la protection des données (Règlement (UE) 2016/679) **(1)** inclut expressément les « données de localisation » dans la définition des « données à caractère personnel ».

▪ Dans un contexte professionnel, ces systèmes peuvent être installés sur les appareils fournis aux salariés (téléphones portables, etc.) ou dans les véhicules (de fonction ou personnel) utilisés par ces derniers. Les données qu'ils recueillent proviennent généralement de satellites (GPS) et de réseaux de communications électroniques (mobile, Wi-Fi), principalement à des fins de sécurité, de surveillance, d'évaluation de la productivité et d'optimisation du travail. Tant et si bien que la géolocalisation rend la frontière entre vie privée et vie professionnelle particulièrement tenue, et parvenir à un équilibre entre ces deux sphères de vie est désormais un défi de taille pour le législateur.

## Les avis du G29

▪ Le groupe de travail « Article 29 » (G29) **(2)** a déjà étudié la question à maintes reprises, et notamment dans ses avis 5/2005 sur l'utilisation de données de localisation aux fins de fourniture de services à valeur ajoutée **(3)** et 13/2011 sur les services de géolocalisation des dispositifs mobiles intelligents **(4)**.

▪ Il est ressort de ses analyses que la légitimité du traitement des données de localisation ne doit pas reposer exclusivement sur le consentement du travailleur. Par conséquent, dans la mesure où le consentement du salarié est problématique, les employeurs ne peuvent utiliser la technologie de géolocalisation « *que lorsqu'il est possible de prouver qu'elle est nécessaire pour une finalité légitime, et que les mêmes objectifs ne peuvent pas être atteints à l'aide de moyens moins intrusifs* ».

(1) Le Règlement général sur la protection des données est entré en vigueur le 24 mai 2016 et sera applicable à partir du 25 mai 2018 http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32016R0679

(2) Ce groupe de travail a été institué par l'article 29 de la directive 95/46/CE. Il s'agit d'un organe consultatif européen indépendant dédié à la protection des données et au respect de la vie privée. Ses missions sont définies par l'article 30 de la directive 95/46/CE et l'article 15 de la directive 2002/58/CE

(3) http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2005/wp115_fr.pdf

(4) http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp185_fr.pdf

▪ En outre, le G29 estime que « *le traitement des données de localisation des travailleurs doit répondre à un besoin spécifique de l'entreprise, lié à son activité* » et que ce traitement peut être justifié lorsqu'il est effectué « *aux fins de la surveillance du transport de personnes ou de marchandises, d'une meilleure affectation des ressources pour des prestations à fournir en des lieux dispersés (par exemple, planification en temps réel des opérations) ou de la poursuite d'un objectif de sécurité, qu'il s'agisse de celle du travailleur lui-même ou des marchandises ou véhicules dont il a la charge* ».

## Le cadre juridique grec

▪ La loi grecque 2472/1997 sur la protection des données prévoit un cadre réglementaire horizontal, sans mentionner expressément l'utilisation des techniques de géolocalisation. Toutefois, ces dernières entrent bien dans le champ de compétence de l'autorité grecque de protection des données, laquelle a publié à ce sujet, sur son site web **(5)**, plusieurs décisions pertinentes (entre autres, 162/2014, 163/2014, 165/2014), une directive 115/2001 sur le respect de la vie privée au travail **(6)** ainsi que des principes directeurs.

▪ Selon ces principes directeurs, les systèmes de géolocalisation ne portent pas atteinte à la vie privée du salarié à condition qu'ils ne soient pas utilisés dans le but de le contrôler, mais afin de favoriser l'efficacité d'une opération commerciale (par exemple, l'optimisation des trajets) et d'améliorer la sécurité du salarié.

▪ Il est à noter que si le système est en place uniquement pour le confort du salarié, ce dernier doit pouvoir le désactiver librement.

▪ Enfin, du point de vue de l'autorité grecque de protection des données, lorsque l'évaluation de la performance des salariés repose sur une surveillance effectuée à l'aide de moyens techniques, elle constitue, en principe, « *un traitement excessif et une violation du principe de proportionnalité* ».

(5) http://www.dpa.gr/portal/page?_pageid=33,125890&_dad=portal&_schema=PORTAL

(6) La directive grecque reprend le document de travail 55/2002 du G29, concernant la surveillance des communications électroniques sur le lieu de travail

GEORGE A. BALLAS
&
THEODORE KONSTANTAKOPOULOS



▪ *Collection and processing of employees' geographic location data essentially involves processing of employees' personal data, falling therefore within the scope of applicable data protection regulation. Notably, in the General Data Protection Regulation [Regulation (EU) 2016/679]* **(1)** *'location data' are specifically included in the definition of 'personal data'.*

▪ *Geolocation systems can be installed on devices carried by employees (e.g. mobile telephone, etc.) and/or (corporate or private) vehicles used by employees. Such systems usually process data from satellites (GPS) and electronic communications networks (mobile, Wi-Fi), basically serving security, monitoring, productivity evaluation and work optimisation purposes. The use of geolocation technologies can effectively blur the line between work and private life, while striking a balance can be a challenging task for regulators.*

### *Working Party 29 Opinions*

▪ *Working Party 29* **(2)** *has repeatedly reviewed the issue in question; relevant are Opinion 5/2005 on the use of location data with a view to providing value added services* **(3)** *and Opinion 13/2011 on Geolocation services on smart mobile devices* **(4)***.*

▪ *The general principle adopted in the above mentioned Opinions is that the lawfulness of such processing operations should not rely exclusively on the employee's consent; in light of the problematic nature of employee consent, employers may only adopt such technology* "when it is demonstrably necessary for a legitimate purpose, and the same goals cannot be achieved with less intrusive means".

▪ *Moreover, Working Party 29 takes the view that "*processing of location data on employees must correspond to a specific need on the part of the company which is connected to its activity*" and it can be justified "*where it is done as part of monitoring the transport of people or goods or improving the distribution of resources for services in scattered locations (e.g. planning

(1) The General Data Protection Regulation entered into force on 24 May 2016 and it shall apply from 25 May 2018. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC

(2) Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC.

(3) http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2005/wp115_en.pdf

(4) http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp185_en.pdf

operations in real time), or where a security objective is being pursued in relation to the employee himself or to the goods or vehicles in his charge*".*

### *Greek legal framework*

▪ *The Greek Data Protection Law 2472/1997 provides a horizontal regulatory framework without specifically referring to the use of geolocation technologies. However, geolocation technologies have been within the scope of the Greek Data Protection Authority (DPA)'s mission and work, having issued a number of relevant Decisions (inter alia, 162/2014, 163/2014, 165/2014), DPA Directive 115/2001 on privacy at work* ***(5)*** *and also having published relevant Guidelines on its website* ***(6)****.*

▪ *According to the said DPA Guidelines, the installation of geolocation systems does not violate the privacy of the employee if it is not used in order to monitor the employee, but in order to facilitate a more efficient business operation (e.g. route optimization) and enhance employee safety.*

▪ *It is also noted that if the system is in place only for the employee's convenience, then the latter must be able to disable it at will.*

▪ *In the DPA's view, employee performance evaluation based on monitoring via technical means constitutes, in principle, "excessive processing and violation of the principle of proportionality*".

(5) Based on the Article 29 Working Party 55/2002, working document on the surveillance of electronic communications in the workplace.

(6) http://www.dpa.gr/portal/page?_pageid=33,125890&_dad=portal&_schema=PORTAL

GEORGE A. BALLAS
&
THEODORE
KONSTANTAKOPOULOS

La géolocalisation des salariés présente un intérêt particulier en Nouvelle-Calédonie, dans la mesure où certains sites d'entreprise sont extrêmement vastes, en particulier certains domaines miniers peuvent couvrir plusieurs milliers d'hectares, et le cumul des concessions minières représentent à ce jour près de 300.000 hectares.

## 1. Les conditions de recours a un système de géolocalisation

▪ **Le Code du Travail de la Nouvelle-Calédonie :** Si le cas particulier de la géolocalisation n'est pas directement prévu par le Code du travail, en revanche, certaines dispositions posent des limites quant à son application dans le cadre professionnel. C'est dans le cadre du principe énoncé à l'article **Lp. 131-4 du CTNC**, que la légitimité de la mise en œuvre d'un dispositif de géolocalisation des salariés doit être appréciée. En effet, ce texte relatif au contenu du règlement intérieur, réduit la marge de manœuvre de l'employeur en ce qu'il prévoit que celui-ci ne peut contenir :

> 1° De dispositions contraires aux lois et règlements, ainsi qu'aux stipulations des conventions et accords collectifs de travail applicables dans l'entreprise ou l'établissement ;
> 2° De dispositions apportant aux **droits des personnes et aux libertés individuelles** et collectives des **restrictions** qui ne seraient pas **justifiées par la nature de la tâche** à accomplir ni **proportionnées** au but recherché.

▪ A notre connaissance, la jurisprudence locale ne s'est pas encore prononcée sur cette question. Cependant, la jurisprudence métropolitaine qui s'est prononcée sur la question au regard des mêmes dispositions prévues en métropole, veille à faire respecter ces règles dans le cadre de l'utilisation d'un dispositif de géolocalisation. **(1)**

(1) Cass. Soc. 17 décembre 2014, n°13-23.645

▪ **Les Délibérations de la CNIL :** La loi du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, entièrement applicable à la Nouvelle-Calédonie, prévoit en son article 22 que les traitements automatisés de données à caractère personnel doivent faire l'objet d'une **déclaration** auprès de la Commission Nationale de l'Informatique et des Libertés, (**CNIL**).

▪ L'article 24 de la même loi prévoit que la CNIL est habilitée à établir des normes destinées à **simplifier l'obligation de déclaration**. La Commission a adopté, le 16 mars 2006, une norme permettant de simplifier la déclaration des traitements visant à géolocaliser un véhicule utilisé par un employé. Constatant le développement des dispositifs de géolocalisation, permettant de prendre connaissance de la position géographique des employés par la localisation des véhicules mis à leur disposition, la CNIL a récemment adopté une nouvelle délibération venant compléter celle de 2006. Il s'agit de la **délibération n°2015-165 du 4 juin 2015**. Ces règles sont **applicables à la Nouvelle-Calédonie**.

▪ Il convient de préciser que les obligations découlant de ces règles ne s'imposent pas aux traitements issus de la mise en œuvre des appareils de contrôle dans le domaine du transport routier, ceux-ci bénéficiant d'une dispense de déclaration en application de la délibération n°2014-235 du 27 mai 2014 de la CNIL.

**Quelles sont les conditions pour instaurer un système de géolocalisation des salariés ?**

▪ **Les motifs de recours.** La CNIL permet la mise en œuvre d'un dispositif de géolocalisation au sein de l'entreprise pour les motifs suivants :

**Le respect d'une obligation légale ou réglementaire** imposant la mise en œuvre d'un dispositif de géolocalisation en raison du type de transport ou de la nature des biens transportés ;

**Le suivi et la facturation** d'une prestation de transport de personnes ou de marchandises ou d'une prestation de services directement liée à l'utilisation du véhicule, ainsi que la justification d'une prestation auprès d'un client ou d'un donneur d'ordre ;

**La sûreté ou la sécurité** du salarié lui-même ou des marchandises ou véhicules dont il a la charge, en particulier la lutte contre le vol du véhicule ;

**Une meilleure allocation des moyens** pour des prestations à accomplir en des lieux dispersés, notamment pour les interventions d'urgence ;

**Le contrôle du respect des règles d'utilisation du véhicule** définies par l'employeur ;

**A titre accessoire uniquement, le suivi du temps de travail**, lorsque ce suivi ne peut être réalisé par un autre moyen et que les salariés ont été dûment informés de sa finalité.

▪ **Les données collectées**. Dans sa dernière délibération de 2015, la CNIL précise les données pouvant être collectées dans le cadre d'un dispositif de géolocalisation. Il s'agit des données suivantes :

**L'identification du salarié** (nom, prénom, coordonnées professionnelles, matricule interne, numéro de plaque d'immatriculation du véhicule) ;

**Les données relatives à ses déplacements** (données de localisation, historique des déplacements effectués) ;

**Des données complémentaires associées à l'utilisation du véhicule** (vitesse de circulation du véhicule, nombre de km parcourus, durées d'utilisation du véhicule, temps de conduite, nombre d'arrêts).

▪ **Les usages prohibés.** Par ailleurs, pour ne pas porter atteinte au respect de l'intimité de la vie privée, il n'est pas possible de collecter une donnée de localisation en dehors du temps de travail du conducteur, en particulier lors des trajets effectués entre son domicile et son lieu de travail ou pendant ses temps de pause.

▪ En ce sens **le texte n'autorise pas le traitement de la vitesse maximale**, sauf si une disposition légale venait à l'autoriser, en raison de l'application de l'article 9 de la loi de 1978, interdisant aux personnes privées de mettre en œuvre des traitements visant à faire directement apparaître des données relatives aux infractions. Or, comme mentionné en préambule, au-delà de la localisation des salariés, la mise en place d'un tel dispositif en Nouvelle-Calédonie permettrait également de s'assurer du bon respect des règles de conduite des véhicules instituées par les entreprises sur des zones privatives, telles les limitations de

vitesse. Il s'agit de prérogatives appartenant aux autorités concernées, disposant du pouvoir de constater les infractions, mais qui bien entendu ne dispose pas du pouvoir de contrôle de règles internes de sociétés sur des routes privatives. Il s'agit là d'une difficulté sur laquelle l'attention de la CNIL a été attirée.

▪ Toutefois, la géolocalisation peut quand même servir à mesurer les vitesses moyennes des véhicules utilisés. Ainsi, sans pouvoir servir de preuve à l'appui d'une sanction en cas d'excès de vitesse, la géolocalisation peut avoir pour but de promouvoir la sensibilisation des salariés à la sécurité routière, par le biais des informations collectées.

**2. La procédure de mise en place d'un outil de géolocalisation**

▪ La mise en place d'un dispositif de géolocalisation des salariés en entreprise doit préalablement respecter un certain nombre de formalités obligatoires.

▪ En premier lieu, les représentants du personnel doivent impérativement être informés et consultés sur la mise en place d'un tel dispositif. Il s'agit d'un préalable obligatoire qui doit donc être réalisé avant la mise en place du dispositif. Dans ce cadre-là, la finalité du dispositif, les salariés concernés et toutes les informations relatives à la collecte des données doivent être communiquées aux représentants du personnel.

▪ L'employeur doit ensuite procéder à la déclaration prévue à cet effet par la CNIL.

▪ Les salariés doivent être informés collectivement (par affichage) et individuellement de la mise en place de ce dispositif. L'information porte sur la finalité du traitement, les catégories de données de localisation traitées, la durée de conservation des données, les destinataires des données, l'existence d'un droit d'accès et de rectification et d'un droit d'opposition ainsi que leurs modalités d'exercice. **L'information individuelle des salariés doit avoir lieu avant l'installation du système**.

▪ Par ailleurs, il sera rappelé que les salariés doivent avoir la possibilité de désactiver la fonction de géolocalisation des véhicules à l'issue de leur temps de travail lorsque ces véhicules peuvent être utilisés à des fins privées.

▪ De plus, les salariés investis d'un mandat électif ou syndical ne doivent pas être l'objet d'une opération de géolocalisation lorsqu'ils agissent dans le cadre de leur mandat.

▪ A titre d'illustration, dans un arrêt du 9 avril 2013, la Cour d'appel de Chambéry a eu l'occasion de rappeler que :

> « *Quel que soit le motif invoqué pour justifier l'installation de ce système [de géolocalisation], notamment la traçabilité des déplacements en cas d'accident, la Société Y avait néanmoins* ***l'obligation d'effectuer une déclaration*** *selon la norme simplifiée n°51, conformément à la délibération de la CNIL du 16 mars 2006 [...] Une telle utilisation destinée à collecter de manière illicite des données personnelles qui portent* ***atteinte à la liberté individuelle,*** *constitue dès lors une* ***faute suffisamment grave*** *pour justifier à elle seule la* ***rupture du contrat de travail aux torts de l'employeur***. »

FRANCK ROYANEZ

*The geolocation of employees is of particular interest in New Caledonia, where some corporate sites are extremely large: certain mining areas can cover several thousand hectares and the cumulated areas of mining concessions total nearly 300,000 hectares.*

***1. Requirements for using a GPS system in New Caledonia***

▪ ***The Labor Code of New Caledonia ("CTNC"):*** *While geolocation is not specifically mentioned in the CTNC, certain provisions have the effect of restricting its application in the workplace, and the legitimacy of an employee geolocation device should thus be assessed under* ***Article Lp. 131-4 of CTNC****. This Article, which relates to company's internal rules and regulations, reduces the employer's leeway by providing that such rules and regulations may not contain:*

> *1° Provisions contrary to laws and regulations and to the collective bargaining agreements applicable in the enterprise or the establishment;*
> *2° Provisions imposing on the* ***rights of individuals*** *and on* ***individual and collective liberties*** *restrictions that are neither* ***justified by the nature of the task*** *to be performed nor* ***proportionate*** *to the objective pursued.*

▪ *To our knowledge, there is no New Caledonian case law on this issue yet. However, the French Metropolitan courts, which have already ruled on this topic under similar provisions, stress that compliance with those rules is required where a geolocation device is used.* ***(1)***

(1) Cass. Soc. 17 December 2014, No. 13-23645

▪ ***CNIL decisions****: The Data Protection Law of 6 January 1978, fully applicable in New Caledonia, provides in its Article 22 that automatic processing of personal data must be* ***notified*** *to the data protection authority, the Commission Nationale Informatique et Libertés (****CNIL****).*

▪ *Article 24 of the Act further provides that the CNIL may establish standards to* ***simplify the notification requirement****. On 16 March 2006, the CNIL adopted a standard to simplify the notification of processing to geolocate a vehicle used by an employee. Noting the development of location-based devices allowing to know the location of employees through the location of their vehicles, the CNIL subsequently adopted a new deliberation to supplement that of 2006:* ***deliberation No. 2015-165 of 4 June 2015****. The rules contained therein are* ***applicable to New Caledonia****.*

▪ *Note, however, that the above rules do not apply to processing resulting from the implementation of monitoring devices in the sector of road transport, as they are exempt from notification pursuant to CNIL deliberation No. 2014-235 of 27 May 2014.*

*What are the requirements to use an employee geolocation system?*

▪ ***Reasons.*** *The CNIL authorizes employers to use geolocation systems for the following reasons:*

> ***Comply with a legal or regulatory requirement*** *to implement a geolocation device due to the type of transportation or the nature of the goods transported;*
>
> ***Follow and bill*** *a service for the transport of people or goods or the supply of services directly related to the use of the vehicle, and prove a service to a client;*
>
> ***Ensure security or safety*** *of the employee himself or of the goods or vehicles in his charge, including for vehicle theft protection;*
>
> ***Better distribute resources*** *for services to be performed in scattered locations, including for emergency response;*
>
> ***Monitor compliance with the vehicle's rules of use*** *such as defined by the employer;*
>
> ***As an alternative only, monitor working hours****, if such monitoring cannot be achieved by other means and employees have been duly informed.*

▪ ***Data collected.*** *In its 2015 deliberation, the CNIL lists the data that can be collected through a geolocation device. These are the following:*

> ***The identification of the employee*** *(full name, work contact information, employee ID, vehicle license plate number);*
>
> ***Data on the employee travels*** *(location data, travel history);*
>
> ***Additional data associated with the use of the vehicle*** *(vehicle speed, number of kilometers traveled, vehicle operating times, driving time, number of stops).*

▪ ***Prohibited uses****. To ensure the respect for privacy, it is forbidden to collect location data outside the working hours of the drivers, especially during journeys between home and the workplace or during break time.*

▪ *In this sense, unless otherwise authorized by law,* ***it is not permitted to process data on a vehicle's maximum speed****, in accordance with Article 9 of the 1978 Data Protection Act prohibiting private individuals from processing data directly relating to offenses. But as mentioned in the introduction, beyond knowing the location of employees, using a location device in New Caledonia may also be a means to ensure proper observance by employees of driving rules — such as speed limits — when driving company vehicles on large private areas. The processing of data relating to offences is reserved for law enforcement authorities, but the latter do not have the power to control private roads. This situation, which may be problematic, has been brought to the attention of the CNIL.*

▪ *That being said, geolocation can still be used to measure the average speed of the vehicles. Thus, even if it cannot be used as evidence to support a penalty in case of excessive speed, the data collected through geolocation can nonetheless serve to raise employees' awareness about road safety.*

***2. Procedure to set up a geolocation tool***

▪ *Some mandatory steps should be taken before introducing a geolocation device in a company in New Caledonia.*

▪ *First, staff representatives must always be informed and consulted on the implementation of such a device. It is a mandatory prerequisite that must be fulfilled before the implementation of the device. Staff representatives should be provided with details on the purpose of the device, the employees concerned and all information relating to the collection of data.*

▪ *Second, the employer must file a notification with the CNIL.*

▪ *Third, employees must be informed collectively (through posting) and individually of the introduction of the device. The information relates to the purpose of the processing, the categories of location data processed, the data retention period, the data recipients, the existence and conditions of exercise of a right of access rectification and objection.* ***The individual information of employees must occur before the system is installed****.*

▪ *Employees should be also informed that they have the ability to switch off the geolocation of the vehicles at the end of their working hours, when these vehicles can be used for private purposes.*

▪ *A location device cannot be used to monitor employees acting as staff representatives when they act within the framework of their duties.*

▪ *Finally, below is an example of case law relating to the geolocation of employees: in a judgment of 9 April 2013, the Court of Appeals of Chambéry ruled as follows:*

> *"Whatever the reason given for the installation of this [geolocation] system, including traceability of movements in case of accident, Company Y was nonetheless* ***required to file a notification*** *under simplified standard No. 51, in accordance with CNIL deliberation of 16 March 2006 [...] Such a use intended to illegally collect personal data that* ***violate individual freedom*** *therefore constitutes a sufficiently* ***serious misconduct*** *to justify alone the* ***termination of the employment contract for cause at the sole expense of the employer****."*

FRANCK ROYANEZ

LEXING NETWORK

| PAYS / COUNTRY | CABINET / FIRM | CONTACT | TELEPHONE | EMAIL |
|---|---|---|---|---|
| Afrique du Sud *South Africa* | Michalsons Attorneys | John Giles | +27 (0) 21 300 1070 | john@michalsons.com |
| Allemagne *Germany* | Beiten Burkhardt | Andreas Lober | +49 69 756095-0 | andreas.lober@bblaw.com |
| Angleterre *UK* | Preiskel & Co LLP | Danny Preiskel | + 44 (0) 20 7332 5640 | dpreiskel@preiskel.com |
| Belgique *Belgium* | Lexing Belgium | Jean-François Henrotte | +32 4 229 20 10 | jf.henrotte@lexing.be |
| Brésil *Brazil* | Melchior, Micheletti e Amendoeira Advogados | Silvia Regina Barbuy Melchior | + 55 113 8451511 | melchior@mmalaw.com.br |
| Canada *Canada* | Langlois avocats, S.E.N.C.R.L. | Jean-François De Rico | +1 (418) 650 7000 | jean-francois.derico@langlois.ca |
| Chine *China* | Jade & Fountain PRC Lawyers | Jun Yang | +86 21 6235 1488 | jun.yang@jadefountain.com |
| Colombie *Colombia* | Marrugo Rivera & Asociados | Ivan Dario Marrugo Jimenez | +57 1 4760798 | imarrugo@marrugorivera.com |
| Costa Rica *Costa Rica* | Lexing Costa Rica | Gabriel Lizama | +506 2253-1726 | glizama@lexing.legal |
| Espagne *Spain* | Lexing Spain | Marc Gallardo | + 34 93 476 40 48 | marc.gallardo@lexing.es |
| États-Unis *USA* | Greenberg Traurig | Françoise Gilbert | +1 650-804 1235 | gilbertf@gtlaw.com |
| France *France* | Alain Bensoussan-Avocats | Alain Bensoussan | +33 1 82 73 05 05 | paris@lexing.law |
| Grèce *Greece* | Ballas, Pelecanos & Associates L.P.C. | George A. Ballas | + 30 210 36 25 943 | central@balpel.gr |
| Inde *India* | Poovayya and Co | Siddhartha George | +91 80 4115 6777 | siddhartha@poovayya.net |
| Israël *Israel* | Livnat, Mayer & Co. | Russell D. Mayer | +972 2 679 9533 | mayer@lmf.co.il |
| Italie *Italy* | Studio Legale Zallone | Raffaele Zallone | + 39 (0) 229 01 35 83 | r.zallone@studiozallone.it |
| Japon *Japan* | Hayabusa Asuka Law Office | Koki Tada | +81 3 3595 7070 | koki.tada@halaw.jp |
| Liban *Lebanon* | Kouatly & Associates | Rayan Kouatly | + 961 175 17 77 | info@kouatlylaw.com |
| Maroc *Morocco* | Fayçal Elkhatib et Associés S.C.P.A | Hatim Elkhatib | +212 5 39 94 05 25 | hatim.elkhatib@elkhatiblawfirm.ma |
| Mexique *Mexico* | Carpio, Ochoa & Martínez Abogados | Enrique Ochoa De Gonzälez Argüelles | + 52 55 25 91 1070 | eochoa@carpio.law |
| Nouvelle-Calédonie *New Caledonia* | Cabinet Franck Royanez | Franck Royanez | + 687 24 24 48 | fr.avocat@cabinetroyanez.com |
| Norvège *Norway* | Advokatfirmaet Føyen Torkildsen AS | Arve Føyen | +47 21 93 10 00 | af@foyentorkildsen.no |
| Portugal *Portugal* | Alves Pereira & Teixeira de Sousa | João P. Alves Pereira | + 351 21 370 01 90 | jpereira@alvespereira.com |
| Sénégal *Senegal* | SCP Faye & Diallo | Cheikh Faye Mamadou Seye | :(+221) 33 823 60 60 | fayetdiallo@orange.sn seyemamadou9@gmail.com |
| Suisse *Switzerland* | Sébastien Fanti | Sébastien Fanti | + 41 (0) 27 322 15 15 | sebastien.fanti@sebastienfanti.ch |
| Tunisie *Tunisia* | Younsi & Younsi International Law Firm | Yassine Younsi | +216 98 37 37 28 | yassine.younsi@younsilawyers.com |

La JTIT est éditée par Alain Bensoussan Selas, société d'exercice libéral par actions simplifiée, 58 boulevard Gouvion-Saint-Cyr, 75017 Paris, président : Alain Bensoussan
Directeur de la publication : Alain Bensoussan – Responsable de la rédaction : Isabelle Pottier
Diffusée uniquement par voie électronique – gratuit –
ISSN 1634-0701
Abonnement à partir du site : http://www.alain-bensoussan.com/outils/abonnement-petit-dejeuner-juristendance/