Geolocation software for employees under scrutiny

On 10 July 2015, the Argentine National Labour Court of Appeals ('the Court') issued a decision ('the Decision') in *Pavolotzki Claudio et al v. Fischer Argentina S.A.* (File N° 48538/2012) upholding employees' rights to have their employers refrain from installing geolocation softwares on their mobile phones. Florencia Rosati, María Eduarda Noceti and Manuela Adrogué, Partner and Attorneys respectively at Estudio Beccar Varela, describe and analyse the Decision both from a labour law standpoint and through a privacy lense.

Introduction

The facts are as follows: plaintiffs filed a lawsuit against their employer, Fischer Argentina S.A. ('Fischer'), claiming the re-establishment of the working conditions prior to the introduction by Fischer of a software named 'Show Position' ('the Software') on the mobile phones provided by Fischer to its employees. The Software allowed Fischer to monitor the exact geographical location of the employees who were travelling salesmen that had been working for Fischer for periods of time going from nine to 36 years.

Plaintiffs' position was that the Software resulted in an extension of their duties (as they had to press different buttons notifying when they arrived at the office of a client, when they executed a sale, when they were ill, etc.) but, mainly, it resulted in an intrusion into their private lives. In addition, plaintiffs claimed this caused a risk to their property and families since the former did not know who collected such data or its destination or use.

Fischer's position was that the resistance of the employees resulted from their intention not to reveal how many visits they conducted, since many of their operations were carried out by phone, a technique that Fischer considered not to be as persuasive as the personal visit. Likewise, Fischer alleged that the Software was not a control system but a business management system intended to optimise usual duties (such as the development of routes without unnecessary duplication and the transmission of news about visits, sales, collections and causes of absenteeism) and secure employees' safety since the Software had an emergency button. The Court of Appeals understood that the Software was an inadmissible intrusion in the employees' private lives and that it was unacceptable that employees did not know who had access to the collected information.

Labour standpoint

In Argentina employers are granted the ability to control employees' activities, though this control must be executed reasonably and respect employees' rights. Even when there are parameters through which an employer could analyse the reasonability of a control method, the final decision in this regard lies with the Labour Courts' judgement.

In this specific example, the Court did recognise that employers have the right to control their employees, even through technical means. However, the Court understood that the control method selected by Fischer was unreasonable and infringed employees' constitutional rights (mainly their right to privacy). In reaching that conclusion the Labour Court made special consideration of the following circumstances:

- There was no evidence that employees acted as 'exclusive' travelling salesperson for Fischer.
- Employees did not have a specific work schedule.
- Fischer had access at all times and immediately to highly sensitive and accurate information as to the geographic location of employees, even after working hours, unless the employees turned off the device, which appears to be abusive considering that employees bear the costs of the use of the device.
- Fischer had not requested the employees' authorisation nor had it explained the need to implement this Software in order to fall within the exception set forth by Section 5 of Data Protection Law 25,326 (see data protection and privacy standpoint below).
- Employees were not provided with information regarding the destination of the data collected through the Software.

Considering these circumstances we can conclude that, from a labour law standpoint, the Court's decision was foreseeable, mainly taking into consideration that (a) control could be executed 24 hours a day and not only during working hours when employees were rendering their duties for Fischer and (b) employees were unaware of the destination of the data collected through the Software.

Data protection and privacy standpoint

Processing of personal data in Argentina is strictly regulated by the Personal Data Protection Law 25,326 ('the Law'), its regulatory Decree, and certain provisions issued by the National Directorate for Personal Data Protection, which is Argentina's data protection authority.

As a preliminary comment, it should be highlighted that the Law is applicable to any data processing that takes place within the Argentine territory. Therefore, we

will firstly analyse whether Fischer's behaviour can be understood as personal data processing.

The Law defines 'personal data' as information of any kind referred to individuals or legal entities, whether identified or identifiable by an associative process. It is important to point out that the Law protects all personal data and not just sensitive data. Therefore, the GPS location of employees is certainly understood as personal data under the Law and thus protected by it. On the other hand, 'data processing' is defined by the Law as any "systematic operations and procedures, either electronic or otherwise, that enable the collection, preservation, organization, storage, modification, relation, evaluation, blocking, destruction, and in general, the handling of personal information, as well as its communication to third parties through reports, inquiries, interconnections or transfers." The wide scope of application conferred by the Law leads us to the conclusion that Fischer was actually processing employees' personal data.

In this connection, the Court of Appeals understood that Fischer was not processing such personal data in a lawful manner because (i) the employees had not given their consent for the installation of the Software in their mobile phones and (ii) Fischer's activity did not fall under the exception to the consent rule set forth in Section 5 of the Law.

According to Section 5, paragraph 2 (d) of the Law ('the Exception'), consent to process personal data is not necessary when the data arises from a contractual, scientific or professional relationship of the data owner and is necessary for the development or compliance of such relationship. The Court understood that the aforementioned requirements did not apply since it deemed the Software to be an excessive tool used by the employer and that overrode employees' privacy without proper justification for its use.

In our opinion, and from a personal data protection standpoint, Fischer could have had sufficient arguments to fall within the Exception of the Law, should the Software had been installed in a device provided by Fischer for use during working hours exclusively

In our opinion, and from a personal data protection standpoint, Fischer could have had sufficient arguments to fall within the Exception of the Law, should the Software have had been installed in a device provided by Fischer for use during working hours exclusively. Our view is based on the fact that the employees rendered services as travelling salespeople and worked outside Fischer's facility, thus the implementation of the Software seemed to be a useful tool for organising their duties and controlling their performance. If that had been the case, the lack of prior, written and informed consent of the employees would not had been an impediment for the data processing since the installation of the Software in the employees' mobile phones should have comfortably fit in the Exception.

Conclusion

In view of all the above, we can conclude in first instance that this specific Court precedent does not invalidate employers' ability to monitor employees' activities through technological means, though the legality of these technological means should be analysed carefully.

In this regard, the Decision helps to set some guidelines that could be useful when implementing a monitoring system similar to the one in this case for it to be considered legal, reasonable and respectful of employees' rights.

The doctrine established by this precedent is that the use of monitoring tools, when reasonable according to the duties to be performed by employees, should be limited to working hours, should be preferably installed in devices granted by the employer as working tools exclusively, limiting their use only for rendering services for the employer, and employees should be informed in writing about the existence of the monitoring tool, the reasons for its implementation, its limitations and the destination of the data that would be collected through it. In addition, the employer should secure that the technological tool is inviolable, i.e. through passwords, 'firewall' systems, etc., so as to secure employees' safety.

Florencia Rosati Partner
Manuela Adrogué Attorney
María Eduarda Noceti Attorney
Beccar Varela, Buenos Aires
frosati@ebv.com.ar
adroguem@ebv.com.ar
mnoceti@ebv.com.ar