PRIVACY AND WORKPLACE MONITORING – PERSPECTIVES OF AZERBAIJANI DATA PROTECTION LAWS

Araz Poladov
(*araz.poladov1@gmail.com*)
Ph.D Candidate
(Baku State University)

Abstract

Rapid expansion of information technologies nowadays, collection and processing of personal data through the use of new technologies makes inevitable to ensure the protection of the personal data on the international and regional levels. One of the main activities which comes into a conflict with personal privacy is workplace (employee) monitoring. Workplace monitoring is the act of employers surveying employee activity through different surveillance methods for different reasons, such as to track performance, to avoid legal liability, to protect trade secrets, and to address other security concerns. Since monitoring can put the personal privacy of employees in jeopardy, the main purpose of this article is to analyze legal basis and requisite safeguards of this activity.

Keywords: *Data protection, personal data, data subject, monitoring, surveillance, workplace.*

Roots of personal data protection

The 21st century has emerged within a globally connected world where geographical borders are becoming more blurred day by day. At the heart of this new era is the liberalization of trade, which allows greater access to goods, services and knowledge, fostering constant innovation [1, 122].

Through the development of new technologies and the democratization of the internet, the concept of "digital economy" has evolved. Using communication services as the platform and computer services as the enabler, almost any type of good or service can be instantly traded online [2, 357]. This digital trading system is built on the exchange of data, as a consequence of which information becomes a tradable and valuable commodity [3, 1].

Tensions between the global economic benefits derived from the transfers and processing of personal data, and the adverse impact these activities represent with regard to citizens privacy will always be at the core of personal data protection laws. Currently, almost all online activities involve the collection of data intended for purposes of processing. However, there is a tremendous lack of awareness, or perhaps of interest, about the extent to which our personal information is collected, stored and used. Although individuals are keen on stating that they believe their personal information should be protected, it is doubtful whether many would sacrifice the services they enjoy for greater privacy [4, 9].

What is privacy at work?

Any person has the general right to privacy under various normative legal acts. However, respecting the privacy of employees and protecting their personal data is equally important.

As most people spend a significant amount of their time at work, and the right to privacy is recognized as a fundamental right that is essential to the well-being of every human being, it is crucial to maintain a reasonable level of privacy at work. While new (digital) technologies offer tremendous capabilities to help organizations and their employees improve work performance, and also enable opportunities like working from home, they can also blur the line between work and private life, creating significant challenges to privacy and data protection.

Every employer processes personal data of all employees, such as names, contact details, bank account numbers, social security payments and salary data. The need to process such data is self-evident, and processing such data is often mandatory for employers.

Besides such minimal mandatory data processing, employers may process a substantial amount of personal data of their employees. For example, personal data can be accrued automatically every day, as a by-product of employees' every-day use of digital equipment and applications provided by the employer (e-mails, calendars, special software). Some employers even process personal data using specific monitoring or surveillance technologies. These may include installation of video surveillance cameras at workplaces, special software allowing control and analysis of internet traffic, collection of location data via special equipment.

What are the legal boundaries of workplace monitoring? Is the employer entitled to monitor or intercept all the means of communication and correspondence of the employees without any safeguards?

The answer is no. Existence of these technical possibilities for monitoring employees, and storing and analyzing information, does not automatically endorse the legality of these activities. A valid legal basis is required for all processing of personal data. This article is set to examine general legal basis of privacy, including privacy at work, evaluate competing interests of employer and employee and define the legal framework of monitoring activities.

Legal basis of privacy at work

In general, the primary legal source of individual's (including an employee's) right to privacy stems from the Constitution of the Republic of Azerbaijan [5]. The Constitution provides that "[e]veryone shall have the right of inviolability of private life, personal and family secrets [5, art. 32]. Except in cases specified by law, interference with a person's private or family life is prohibited. Everyone has a right to protection against unlawful interference with his or her private or family life."

Moreover, the State guarantees everybody's right to secrecy of correspondence, telephone conversations and information transmitted by mail, telegraph or other means of communication, except in cases prescribed by law (when interference with such information is reasonably required for criminal law purposes). It is also prohibited to obtain, keep, use and disseminate information about a person's private life without his or her consent. With the exception of cases envisaged by law, no one may be subject to being surveilled, videotaped or photographed, tape recorded or subjected to other similar actions without being informed or despite his/her objection [5, art. 32].

A more comprehensive and detailed regulation of the discussed matter is provided in the Law of the Republic of Azerbaijan "On Personal Data" [6], which deals with the issues of collection, processing, storage and protection of personal data.

Under the Personal Data Law, personal data is any information allowing direct or indirect identification of a person, whereas the Law of the Republic of Azerbaijan "On Obtaining Information" [7] further provides that personal data is an aggregate of private life and family life information and clarifies what information shall be considered as such, and thus be subject for special regulation. In particular, (i) information on ethnic and racial identity; (ii) information on special traits, skills and other features of the character; (iii) tax related information, except information on tax debts; (iv) information on financial transactions shall be also considered as personal data [7, art. 38.2]

Legal basis of monitoring activities

As mentioned above, employers might wish to monitor or intercept email content, email traffic, internet use and telephone use. This could include checking the number, destination, source and content of emails, websites visited and destination, duration and content of phone calls. Types of monitoring can also include one off spot checks, which look at communications across an organization but which do not refer to individual usage, spot checks on individual employees and more continuous monitoring of organizational or individual usage, either on a targeted or random basis [8, 213]. These processing and monitoring activities, however, are not arbitrary – the processing has to have a legal ground/basis in order to be legitimate.

Articles 8.2 and 11.2 of the Personal Data Law provide that except in a limited number of cases, collection and processing of personal data is only permitted upon (i) written notice of the controller or operator collecting personal data (i.e. an employer) to the personal data subject (e.g. an employee), and (ii) written consent of the personal data subject. Although the Personal Data Law is silent on the legal elements of consent, one of the most crucial conditions of a valid consent is the exercise of "free will". In other words, the consent has to represent the will of the data subject – no duress, force or coercion has to affect the will of the data subject.

With these considerations, while consent generally may be the most important and most widely used legal ground for the processing of personal data, this is not the case at the workplace. Because the employer has authority over the employee and the employee is financially dependent on the employer, permission from an employee to an employer in principle cannot be considered as freely given.

As such, since employers cannot justify processing of personal data of employees on the ground of consent, another legal ground must apply.

Without consent, there are only a number of other ways an employer can process data, which include legal obligations of the controllers and protection of vital interests of data subjects [6, art.9.6].

Since the latter only applies where processing of personal data is necessary to protect someone's life, for example where medical treatment is required and the data subject is incapable of providing it or of giving consent to the processing, the only legal basis of lawful protection is legal obligation of the employer.

Article 222.1 of the Labor Code of the Republic of Azerbaijan [9], among others, provides that employers shall organize monitoring (supervision) of healthy and safe working conditions at workplace and shall provide employees with information on any changes concerning work conditions in a timely manner.

The Labor Code neither specifies the means of monitoring nor puts any restrictions in this respect. Therefore, in order to fulfil such monitoring obligation, an employer may, for instance, videotape the workplace or hold out a separate employee who would in person monitor health and safety conditions at the workplace.

Save for monitoring of health and safety conditions at workplace, neither the Labor Code, nor any sector-specific legal act provide for any other statutory requirement for private companies to carry out monitoring of the workplace.

When it comes to sector-specific laws, Article 14 of the Law of the Republic of Azerbaijan "On Freedom of Information" [10] prohibits (i) the use the technical devices intended for hidden collection of information, (ii) examination of postal and telegraphic correspondence, and (iii) interception of phone calls, except for the circumstances envisaged in law. These exceptions are primarily established in the Criminal Procedure Code of the Republic of Azerbaijan [11] and the Law "On Detective-Search Measures" [12].

Likewise, under Article 14 of the Law "On Freedom of Information", except when detective-search measures are conducted, it is prohibited to (i) to surveil, (ii) videotape, (iii) photograph, (iv) tape-record a person, or (v) subject such person to other similar actions without informing him or despite his objection.

It is safe to conclude that workplace monitoring does not fall into the scope of police or investigative measures under the Code of Criminal Procedure or Law on Detective-Search Measures, nor could it be justified on the basis of employees' valid consent. Since there is not any legal obligation or basis for employers to monitor or intercept employee data, employers can only resort to Article 222.1 of the Labor Code as their "safe heaven"– organization of monitoring (supervision) of healthy and safe working conditions at workplace.

Thus, under Azerbaijani law, employers are absolutely prohibited to:

a) to monitor or intercept communications of its employees through technical devices intended for hidden collection of information;

b) to check private postal and telegraph correspondence of its employees, including private e-mail correspondence;

c) listen to private phone calls of its employees;

d) conduct hidden surveillance, video recording, photographing, and audio recording of employees;

e) conduct open surveillance, video recording, photographing, and audio recording of employees despite their objection.

Requirement of prior registration

Under the Personal Data Law, personal data information systems shall be registered with the Ministry of Communications and High Technologies of the Republic of Azerbaijan (the "MCHT"). Collection and processing of personal data shall be prohibited without registering the personal data information systems.

Registration of personal data information systems shall be carried out by MCHT within 1-month period based on the application of the owner of such system (e.g. the employer) [6, art. 15.4]. However, certain personal data information systems are exempt from registration requirement. Among others, the exemption relates to the information systems of (a) personal data related to personal data subjects who are in employment relations with the owner or operator of the personal data information base or (b) the

personal data necessary for providing access to work premises of personal data owner or operator [6, art. 15.3].

Therefore, in an employment context, private companies in Azerbaijan are not required to notify or obtain approval from any third party (e.g. a financial regulator or data protection authority) in order to monitor their employees or intercept communications of employees.

Conclusion

With no doubt, surveillance of employee data presents several benefits to employer: it may promote safe working environment, enhance protection of know-how and commercial secrets of employers, address security concerns, along with detection of unacceptable behavior at workplaces. On the other hand, as the line between employee information which is of an exclusive proprietary interest of the employer, and the personal data of employees is becoming increasingly vague, monitoring and interception of emloyee data has to take competing interests in account and commit to principle of lawfulness.

Employee and employer relationship has always been reflective of disproportionate allocation of power. Employee, being financially dependent and "inferior" to the employer, does not exercise free will when consenting to videosurveillance or correspondence interception. Therefore, consent, as a legal basis for processing of personal data, is a shaky basis for processing of employee data.

Sector-specific laws, such as Freedom of Information Law, Law on Obtaining Information also establish absolute prohibitions with regard to covert collection of information, including examination and interception of correspondence and phone calls. To this end, the only provision employers resort to is "organization of monitoring of healthy and safe working conditions" under article 222.1 of the Labor Code. Absence of means of monitoring in this article makes it diffuclt to assert the legality of certain means of surveillance and monitoring. However, this provision has to interpreted strictly in the light of "healthy and safe working environment".

Finally, employers are not legally required to go through prior registration procuders, as the collection, storage and monitoring activities fall into the exception of employment relations under article 15.3 of Personal Data Law.

References:

1. "GDPR adequacy decisions vs GATS: how may the EU's privacy and digital trade commitments be conciliated within a GDPR adequacy decision on cross-border personal data flows?" Jessica Lauren Koffel, International Trade Law & Regulation 2018.

2. L. Tuthill, "Cross-Border Data Flows: What role for Trade Rules?" in P. Sauve and M. Roy (eds), Research Handbook on Trade in Services (Cheltenham: Edward Elgar Publishing, 2016).

3. S. Aaronson, "The Digital Trade Imbalance and Its Implications for Internet Governance", Global Commission on Internet Governance No.25, (2016).

4. Mitchell and Mishra, "Data at the Docks: Modernizing International Trade Law for the Digital Economy" (2018) 20 Vanderbilt Journal of Entertainment and Technology Law.

5. Constitution of the Republic of Azerbaijan dated12 November 1995, № 00, available at: http://www.e-qanun.az/framework/897

6. Personal Data Law of the Republic of Azerbaijan dated 11 May 2010, № 998-IIIQ, available at: http://www.e-qanun.az/framework/19675

7. Law of the Republic of Azerbaijan on Obtaining Information dated 30 September 2005, № 1024-IIQ, available at: http://www.e-qanun.az/alpidata/framework/data/11/c_f_11142.htm

8. "Monitoring employee communications: data protection and privacy issues", Anthony Sakrouge, Kate Minett, Daniel Preiskel and Jose Saras, Computer and Telecommunications Law Review 2011, p. 213

9. Labor Code of the Republic of Azerbaijan, was approved by the Law of the Republic of Azerbaijan on "Approval, enforcement of Labor Code of the Republic of Azerbaijan and regulation of legal issues in this respect" dated 1 February 1999, №618-IQ (Legislation compilation of the Republic of Azerbaijan dated 1999, № 4, Section 213), available at: http://www.e-qanun.az/code/7

10. Law of the Republic of Azerbaijan on Freedom of Information dated 19 June 1998, № 505-IQ, available at: http://www.e-qanun.az/framework/3420

11. Criminal Procedure Code of the Republic of Azerbaijan dated 14 July 2000, № 907-IQ, was approved by the Law of the Republic of Azernaijan on "Approval, enforcement of Criminal Procedure Code of the Republic of Azerbaijan and regulation of legal issues in this respect" (Legislation compilation of the Republic of Azerbaijan dated 2000, № 8 (second edition), Section 585), available at: http://www.e-qanun.az/code/14

12. Law of the Republic of Azerbaijan on Detective-Search measures activity dated 28 October 1999, № 728-IQ, available at: http://www.e-qanun.az/framework/2938

Date of receipt of the article in the Editorial Office
(19.07.2019)