Preamble

The workplace is part of the public sphere which includes the right to privacy.

It is generally considered appropriate to balance between the worker's interest to the protection of his privacy and the competing interests of the employer and the society to disclosure of information and to preventive surveillance of workers. These competing interests are most often dictated by security and productivity concerns.

The technological innovations facilitate the employer’s control over the worker’s activities in the workplace and thus increase the risk of conflict between the interests of the enterprise and the worker’s right to privacy. The border that separates professional life from privacy is therefore very fragile and it reveals that the two spheres (private and public) are not perfectly sealed anymore.

Therefore, the purpose of this study is the protection of privacy that a worker can expect both with regard to his future employer (recruitment phase) or his employer (during his employment period), when information about him circulate on social networks (Facebook, LinkedIn, etc...) or on blogs depending on:

- whether the worker is circulating this information by himself or it is done by third parties;
- whether there is a direct and free access to the information (« open profile ») or not (« closed profile »);
- whether we are talking about collecting information or using this information;
- the fact that the gathering and use of information is done by the employer or the information is collected by a third party and then made available to the employer who will use it.
Questions

1-Does your country have laws or regulations that protect the confidentiality of electronic communications?

Yes. We have laws and regulations that protect the confidentiality of electronic communications. These regulations cover gathering, categorizing and usage of all kinds of information belonging persons or related to persons. Violation of the rules set forth in the regulations is subject to penal and administrative sanctions and also may raise liability issue. Some of them may be indicated as follow:

a-Turkish Criminal Code article 132 and cont.

Violation of Communicational Secrecy

ARTICLE 132-(1) Any person who violates secrecy of communication between the parties is punished with imprisonment from six months to two years, or imposed punitive fine. If violation of secrecy is realized by recording of contents of communication, the party involved in such act is sentenced to imprisonment from one year to three years. (2) Any person who unlawfully publicizes the contents of communication between the persons is punished with imprisonment from one year to three years. (3) Any person who openly discloses the content of the communication between himself and others without obtaining their consent, is punished with imprisonment from six months to two years. (4) The punishment determined for this offense is increased by one half in case of disclosure of contents of communication between the individuals through press and broadcast. Tapping and recording of conversations between the individuals ARTICLE 133-(1) Any person who listens non general conversations between the individuals without the consent of any one of the parties or records these conversations by use of a recorder, is punished with imprisonment from two months to six months. (2) Any person who records a conversation in a meeting not open to public without the consent of the participants by use of recorder, is punished with imprisonment up to six
months, or imposed punitive fine. (3) Any person who derives benefit from disclosure of information obtained unlawfully as declared above, or allowing others to obtain information in this manner, is punished with imprisonment from six months to two years, or imposed punitive fine up to thousand days. Violation of Privacy ARTICLE 134- (1) Any person who violates secrecy of private life, is punished with imprisonment from six months to two years, or imposed punitive fine. In case of violation of privacy by use of audio-visual recording devices, the minimum limit of punishment to be imposed may not be less than one year. (2) Any person who discloses audio-visual recordings relating to private life of individuals are sentenced to imprisonment from one year to three years. In case of commission of this offense through press and broadcast, the punishment is increased by one half. Recording of personal data ARTICLE 135-(1) Any person who unlawfully records the personal data is punished with imprisonment from six months to three years. (2) Any person who records the political, philosophical or religious concepts of individuals, or personal information relating to their racial origins, ethical tendencies, health conditions or connections with syndicates is punished according to the provisions of the above subsection. Unlawful delivery or acquisition of data ARTICLE 136-(1) Any person who unlawfully delivers data to another person, or publishes or acquires the same through illegal means is punished with imprisonment from one year to four years. Qualified forms of offense ARTICLE 137- (1) In case of commission of the offenses defined in above articles; a) By a public officer or due influence based on public office, b) By exploiting the advantages of a performed profession and art, the punishment is increased by one half. Destruction of Data ARTICLE 138-(1) In case of failure to destroy the data within a defined system despite expiry of legally prescribed period, the persons responsible from this failure is sentenced to imprisonment from six months to one year. Compliant ARTICLE 139-(1) Excluding recording of personal data, unlawful delivery or acquisition of data and destruction of data, commencement of investigation and prosecution for the offenses listed in this section is bound to complaint. Imposition of security precautions on legal entities ARTICLE 140-(1) Security precautions specific to legal entities are imposed in case of commission of offenses defined in the above articles by legal entities.
b- Personal Data Protection Act: This act came into force on April 7, 2016. However, the effectiveness of some articles of the act have been delayed until October 7, 2016. The rules over transfer of data, individual application to relevant institution which stores personal data to learn whether the information was processed or not, responsibilities of persons who store the information and sanctions to violation thereof, and establishment of supervisory institution will be gone into operation on 7 October, 2016.

c- Turkish Civil Code: Articles of 24, 25, 26.

d-Turkish Code of Obligations: Article of 58 and cont.

e- The Act of Electronic Communication: Article of 51.

f- The Ordinance regarding Proceeding and Protection of confidentiality of Personal Data in Electronic Communication Sector.

2- If so, are these provisions applicable when the information are collected on social networks or blogs?

Yes. In Turkish Law it is forbidden, with some exceptions, to collect and process personal data. The major derogation is consent of relevant person. In this scope, depending on type of gaining shared data and of usage, violation of regulations set forth in above-mentioned acts is subject to penal and administrative sanctions and in some cases compensation may be required.

3- If so, are these provisions protecting the information collected or used by an employer:

   o during the recruitment phase?
   
   o In the course of the employment for disciplinary reasons or others?

Such an act against the regulations aforesaid done by employer is subject to relevant sanctions. There is no difference between whether the information is gathered by employer or by third party at the point of illegality of the act. In Labour law, it is unacceptable to use data collected illegally by employer to establish and proceed labour patterns or affairs and to gain legal benefits or consequences from illegally collected data. However, the information posted
by employee to be seen by anyone on social networks can be used by employer in the course of recruitment and employment. But it must be assessed case by case.

In addition, according to the article 5/2-c of Personal Data Protection Act, the data which belongs to parties to a labour agreement can be stored without their consent on the condition that storage of the data is necessary and it is related to establishment and implementation of the agreement. In this scope, employer can store and process the data gathered from social networks in the course of recruitment and employment.

4-Are the employees allowed to use social networks during working hours? If so, in which way?

Since, in terms of labour law, working hours are specific for work, generally employees are not allowed to use social networks during working hours. On the other hand, pursuant to the nature of job and infrastructure established in working place, employees may use social networks through either their own account or company’s one providing that use of networks be related to described job such as organisation of work, ensuring communication among workers, and advertisement. Even, in some companies, for communicational purposes, infrastructures of international social networks are being used. In such cases, conflict of interests between employees and employers may be more evident. In terms of the consequences of such conflicts regarding labour law each fact are evaluated separately.

5-Can the employer monitor the use of social networks by his employees during working hours? Outside of the working hours?

In labour law, since authority and responsibilities in working place belong to employers, employers can monitor activities of employees during working hours. Here, duration and time of use of social networks are important rather than information itself shared by employees. Employee may access social networks via either their own devices or company’s ones during working hours. In such cases, employer may monitor working place through his representatives like manager, chief or inspectors or camera systems or controlling the devices using by employees. In these inspections, if employer determines that employee uses social networks in stead of doing his own job, employer can exercise several sanctions in the limits of labour law. However, except for information open to everyone, employer cannot access
personal accounts of employees and content of their communication. If he does so employer may be subject to penal and pecuniary sanctions.

Outside working hours since employees are free from employer’s control employer cannot monitor duration of social network use. However, there will be consequenses pursuant to labour law if employees share information that harms order of working place, reveals trade secrets, violates prohibition of competition and duty of loyalty, insults employer or other employees.

***

TURKISH ASSOCIATION OF JUDGES AND PROSECUTORS (YARSAV)