Observations and Recommendations on the Council of Europe Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No.108)

Draft Recommendation on the Protection of Personal Data used for Employment Purposes

October 2013

Irish Congress of Trade Unions
31/32 Parnell Square
Dublin 1
www.ictu.ie
Introduction

The Irish Congress Trade Unions is the national representative body for workers and their unions on the island of Ireland. There are 48 unions representing almost 820,000 workers across all sectors and industries, private and public sectors.

Congress welcomes the invitation to comment on the Draft Recommendation on the Protection of Personal Data used for employment purposes. However, the limited time provided (2.5 days) means that the response is necessarily short and some important issues may not be covered at all.

Privacy is a fundamental human right, and is recognised both by the Constitution and the European Convention on Human Rights. However, the mechanisms for the enforcement of that right in Ireland lack clarity and effectiveness in some important respects.

The collection of workers' personal data takes place even before the beginning of the employment relationship for the purposes of recruitment; it continues throughout employment and may extend even after its termination. New technologies make the collection and cross referencing of data available and affordable.

Automated profiling enables employers, employment agencies and others to determine, analyse or predict a worker's personality or aspects of their personality – especially their behaviour, interests and habits. Furthermore, people usually do not know that and to what extent they are being profiled. An individual's internet browsing history alone is capable of exposing his or her most intimate likes, dislikes, activities and thoughts. The widespread availability of personal data and the increasing possibilities of linking such data combined with the fact that technical devices operating on the basis of processing personal data pervade our everyday lives, means that profiling has become one of the biggest challenges facing workers and their unions.

Workers do not give up all of their rights at the door of their workplace, everyone has the right to some degree of privacy in the workplace and data protection law has been there to the forefront in protecting workers' privacy. The Data Protection Act 1988, as amended by the Data Protection (Amendment) Act 2003, gives effect to EC Directive 95/46/EC and affords some protection to employees and other categories of 'workers' in respect of personal data maintained relating to them. The Acts apply if personal information is processed by the employer. The Acts regulate the collection, processing, keeping and disclosure of 'personal data' which is defined as 'data relating to a living individual who can be identified either from the data or from the data in conjunction with other information in the possession of the data controller'.

As a general rule, where employers intend to monitor the activities of staff they should consult with employees and inform them of the monitoring arrangements they plan to introduce. They should also be clear that those arrangements are necessary and that there are no less intrusive alternatives.

Monitoring must be done in a way that is not oppressive to staff. Excessive, routine and unnecessarily intrusive monitoring can be a breach of data protection laws.
Section 6 of the Act provides that 'a decision which produces legal effects concerning a data subject, or otherwise significantly affects a data subject may not be based solely on processing by automatic means of personal data in respect of which he or she is the data subject and which is intended to evaluate certain personal matters relating to him or her such as, for example (but without prejudice to the generality of the foregoing), his or her performance at work, creditworthiness, reliability or conduct’

However some problems have emerged that are relevant to the consideration of the scope and content of the Recommendation and we set this out in summary below:

1. There is an on-going problem with the use of anti-union ‘blacklisting’ and surveillance technologies that aim to interfere with workers’ right to freedom of association and their right to organise or the right to collective action including the right to strike. Recent investigations in the UK and other European States demonstrate widespread use by employers in certain industries and sectors of services provided by individuals or companies who compile ‘blacklists’. The purpose of these blacklists is to ensure that trade union members and others who speak up about exploitation or health and safety at work are kept out of the workforce;

2. Problematic operation of 'consent' in the employment relationship. Consent clauses in employment contracts have sometimes been interpreted in ways which do not benefit workers and often they serve to legitimise inherently objectionable surveillance practices and overly invasive and inappropriate background checks. For example the legal limits on automated decision making can be waived by consent in the employment contract. Against the backdrop of downsizing and increasing job security, the unequal power in the employment relationship means that workers, on their own, without the protection of their union are unlikely to be able to mount an effective defence of their individual data protection rights when faced with an employer’s demand to introduce new data collection or monitoring and surveillance methods. To counteract this imbalance, Congress is recommending that the Recommendation require employers to consult with, (rather than simply inform), the workforce. In addition workers should have the right, (similar to health and safety laws) to establish a workplace data protection committee and elect a data-protection representative equipped with adequate skills and rights to allow proper interventions in the field of data-protection on all levels, including cross-border circumstances in multinational companies;

3. Workers are particularly vulnerable during the recruitment process and the Recommendation needs to be strengthened to reflect this reality. In particular, the Recommendation needs to recognise that when employers use third parties such as employment agencies, there are additional risks present. This calls for a higher level of protection. For example, workers should not have to request information on the data shared about them as they then run the risk being marked out as a ‘trouble maker’. Rather the Recommendation should oblige the employment agency to inform the job seeker of their data that has been communicated to prospective employers along with the identity of the employers that their data has been passed along to;
4. More needs to be done to combat excessive and inappropriate background checks and the inappropriate use of health questionnaires. The Recommendation should set out a requirement that, before an employer can make requests for disclosure of information or to, carrying out a background check, or complete a medical questionnaire they must set out why the collection of the data is objectively justified. Even when there is the employee’s prior consent and agreement the collection and use of personal data for employment purposes should not breach fundamental rights, it should not go beyond what is legitimate and objectively necessary and should only be used when there is no less intrusive way to achieve the justified outcome;

5. There are particular problems associated with the use of automated decision making in the employment context. At first sight, automating decisions may give a sense of fairness. However, at a closer look it becomes clear that the rules underpinning the automatic process can disguise bias and unlawful discrimination. Accountability begins with an acknowledgment that analytics can have a negative impact reflecting the cultural bias of the developers.

For example, Profiling this is any form of automated processing of personal data intended to analyse or predict the personality or certain personal aspects relating to a natural person, in particular the analysis and prediction of the person’s health, economic situation, performance at work, personal preferences or interests, reliability or behaviour, and location or movements. Profiling for an employee’s membership of a trade union is a particular concern.

In his Report Data Protection Law and the Ethical Use of Analytics, Paul M. Schwartz. Professor of Law, Berkeley Law School, highlights how data sets from various sources can be brought together to predict behaviour. He also outlined how AC Milan, a leading soccer team in Europe, uses ‘predictive models to prevent player injuries by analysing physiological, orthopaedic, and psychological data from a variety of sources’.

According to the EU Working Party 29, data controllers should be required to disclose information of rules that how’s personal data will be used in the context of profiling, the purposes for which the profiling is carried out and the logic involved in the automatic processing. The WP29 stated that individuals should also have the right to access, to modify or to delete the profile information attributed to them, and to refuse any measure or decision based on it or have any measure or decision reconsidered with the safeguard of human intervention.

Congress is concerned that the Recommendation does not adequately address the dangers posed to workers arising from automated profiling.

The Regulation seems to allow a broad use of automated processing of personal data for profiling purposes. This raises particular concerns in the employment context. Workers should not be subjected to such measures in the course of the entering into, or performance of, an employment contract. The principle of the right to human intervention should be retained along with a requirement to have in place robust measures to ensure against indirect discrimination. For example, there are particular concerns about unlawful indirect gender discrimination (based on selection for interview according to certain words in CVs), unfair credit worthiness discrimination, (on the basis of being on an insolvency register) and unlawful discrimination on basis of disability (interpreted from on-line activity).

The lack of transparency has to be repaired by guaranteeing additional information rights and a higher level of control for individuals.
Accountability and responsibility of data controllers have to be strengthened by establishing specific safeguards to protect data subjects' equality, privacy and other human rights and to ensure that workers are not prevented or frustrated in their ability to undertake complaints that equality and other human rights have been breached.

6. Constant surveillance in the employment context has serious health and safety implications. Take for example, CCTV, GPS and smart cards, often introduced as a means for buildings security, these can also track workers' movements, monitor rest breaks, and hold personnel and occupational health records. The system records whether the worker is in the lavatory, another workstation, the canteen area etc. Although the surveillance may be intended to capture only security related matters, constant surveillance has the potential to record very personal information, every private activity; even scratching a body part is captured and capable of being replayed. Giving rise to concerns about workers' dignity, matters inherent in the concept of privacy and data protection principles. For example, workplace CCTV footage has made its way into TV programmes (usually with workers faces disguised) or on-line, for example YouTube. Employers or Security Firms releasing CCTV of stressed out workers to third parties for entertainment or 'infotainment' without the workers permission is not acceptable and should be specifically prohibited. This is a very worrying development and the Recommendation should ensure against the use of workers data in this way. The use of footage to catch criminals on serious programmes such as CRIMECALL can be justified;

7. The use of social media surveillance to discipline workers is fraught with difficulty; recently employers have even tried to dismiss workers according to comments made on their personal Facebook or other social media sites. Increasingly the line between work and private and family life is being blurred. Consent to employer surveillance and data processing should not be permitted to extend into what employees consider to be private space e.g. from the place of employment into their homes. (e.g. where GPS is fitted to a vehicle provided by the employer- the employee must be enabled to switch it off during private life);

8. Other areas of concern relate to alcohol and drug testing (including blood, hair and urine samples). Depending on the test used this can disclose off-work and legal use, sometimes going back over a number of months, give rise to involuntary disclosure because the test shows medication taken for illnesseses or in the case of pregnancy;

9. The use of lie detectors in the employment context should be banned.
Finally, in the ILO's Declaration of Philadelphia of 1944, the international community recognised that 'labour is not a commodity'. Work is part of everyone's daily life and is crucial to a person's dignity, well-being and development as a human being. Workers are entitled to respect which requires some attention to privacy and protection from inappropriate intrusions into the personal and family life of the worker. When employers monitor every conversation or move, they create an environment that is more like a prison than a humane workplace. With each new form of surveillance, we become less like individuals and more like automatons, monitored for defects and aberrant behaviour at work and increasingly in our private lives. Without, strong protections automatic decision making and profiling is a strikingly powerful new tool in the bad employer’s armoury.

Esther Lynch
Legislation and Legal Affairs
Irish Congress Trade Unions
ester.lynch@ictu.ie

Bibliography