Available online at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

EU update

Kit Burden *

DLA Piper UK LLP, United Kingdom

Keywords:
EU law
Intellectual property
Information technology law
Telecommunications law

A B S T R A C T

This is the latest edition of the DLA Piper column on developments in EU law relating to IP, IT and telecommunications. This news article summarises recent developments that are considered important for practitioners, students and academics in a wide range of information technology, e-commerce, telecommunications and intellectual property areas. It cannot be exhaustive but intends to address the important points. This is a hard copy reference guide, but links to outside web sites are included where possible. No responsibility is assumed for the accuracy of information contained in these links.

1. Europe: Article 29 Working Party issues opinion on usage of technologies at work

Giulio Coraggio, *Partner, DLA Piper Milan*

Privacy risks can arise from the usage of new technologies by employees at work and require a deep assessment especially in the light of the General Data Protection Regulation.

The Article 29 Working Party, a European advisory body made by European data protection authorities, issued an opinion on the usage of technologies at work, which considers both current privacy laws and the upcoming General Data Protection Regulation.

1.1. *The privacy principles applicable at work*

According to the Article 29 Working Party:

- **consent cannot and should not be the legal basis of the data processing at work** – this is a quite often mistake, the potential consent from employees would not be freely given because of the employment relationship and therefore would not be valid;
- **processing may be necessary for the performance of a contract** where the employer has to process personal data of the employee **to meet contractual obligations** – this means that such legal basis cannot be used to justify data processing activities that go beyond what is necessary for the performance of the employment contract;
- **legitimate interest can be the legal basis of the data processing**, but the chosen method or specific technology must be necessary, proportionate and implemented in the least intrusive manner possible and **accompanied by mitigating measures to protect employees' privacy** – the balancing test necessary to rely on legitimate interest will be tricky and legitimate interest is definitely not a strong legal basis of data processing as it is open to different interpretations;
- **employees should be clearly and fully informed of the processing of their personal data**, including the existence of any monitoring – this is something already provided in Italy by the guidelines of the Italian data protection authority on the monitoring of the usage of Internet and emails on the workplace. The provision of adequate information on the type of data processing activities performed by means of technologies is not just a recommendation, but an obligation;
- **principles of privacy by design, by default and of data minimisation shall be followed** in building technologies that can monitor employees – this means that such technologies shall by default adopt the most privacy-friendly settings; and

* DLA Piper UK LLP, 3 Noble Street, London EC2V 7EE, UK.
E-mail address: kit.burden@dlapiper.com; For further information see: http://www.dlapiper.com/.

https://doi.org/10.1016/j.clsr.2017.10.001
0267-3649/

- a privacy impact assessment has to be run when technologies can lead to high risk for individuals such as in case of potential profiling or decisions taken by means of automated systems.

1.2. *The potential scenarios occurring on the workplace*

The European privacy authorities adopted a very practical approach listing frequent scenarios occurring on the workplace and giving instructions on how they should be handled:

- Processing during the recruitment process

Information about a candidate on social media can be reviewed only if necessary and relevant to the performance of the job which is being applied for, can be performed only on social media related to business (e.g. LinkedIn, but not Facebook) and data should be deleted once it appears clear that an offer of employment will not be made or is not accepted by the individual concerned;

- Screening of employees' social media profiles

The review of social media profiles of employees, of their contacts/friends, opinions, beliefs, interests, habits, whereabouts, attitudes and behaviours should not take place and should not be required to employees and applicants.

- Monitoring of electronic devices on the workplace

These technologies not only include the monitoring of emails and of Internet usage, but include among others

- data loss prevention (DLP) tools,
- security applications and measures that involve logging employee access to the employer's systems; and
- technologies enabling the monitoring of personal devices (e.g., PCs, mobile phones, tablets), that employees supply for their work in accordance with the Bring-Your Own-Device (BYOD), as well as Mobile Device Management (MDM) technology which enables the distribution of applications, data and configuration settings, and patches for mobile devices.

In relation to the technologies above, the Article 29 Working Party recommends to:

- run a privacy impact assessment in order to also understand whether the technology complies with **the principle of proportionality and changes are needed to reduce the scale of the data processing**; and
- provide employees with acceptable use of policies that describe in details **the processing that takes place and the rules of functioning of the system**.

The second point above is at least arguable and risks to vanish in some circumstances the purpose of monitoring systems. Indeed, if in case of data loss prevention technologies, it is indicated in detail when it is triggered and in case of action triggering the monitoring a prior notification is sent to the employee in order to enable him to cancel it, the risk is that **the technology will "educate" the employee on how to avoid the alert to be triggered**. This would result in a potential higher risk of data breaches that want to be avoid by means of such technologies.

Likewise, if it is given on the workplace the possibility to employees of sending private communications or in any case keeping such activities private, **the risk is to create a channel for potentially illegal activities**.

The above is difficult to explain in a regime that under the General Data Protection Regulation will oblige to implement "*appropriate technical technical and organisational measures to ensure a level of security appropriate to the risk*", also introducing burdensome obligations in case of data breach.

The privacy authorities state, "*prevention should be given much more weight than detection*" which I fully agree. But in relation to the scenario above for instance, it is difficult to argue that employees should be given to mark some appointments as "*private*" and offered with "*alternative unmonitored access*" when in the 21st century basically everyone has a smartphone with a data plan and a private email.

In relation to the labour law approvals required for the usage of such technologies, a higher level of flexibility was given in Italy by means of the provisions of the so-called Jobs Act.

1.3. *Monitoring of electronic devices outside the workplace*

This is a practice that is becoming exponentially common with the growth of home working, remote working and "bring your own device" policies. The position of the Article 29 Working Party is the following:

- **Monitoring of home and remote working**

There is a higher risk of unsecure usage of personal data outside of working premises, but monitoring tools may be considered disproportionate and unjustified. The risk should be addressed in a proportionate and non-excessive manner, but the Article 29 Working Party does not give indications on how such goal can be achieved.

- **Bring your own device (BYOD)**

It is prohibited to use technologies that perform a complete scanning of private devices and areas that are meant to be used for private purposes should be skipped.

Likewise monitoring the location and traffic of private devices may be justified by legitimate interest, but the technologies able to distinguish private and business usage shall be in place.

A secure transfer of data between the private device and the business network can be ensured by means for instance of a VPN, but again it should be avoided that such measure leads to privacy issues during private usage of the device.

An interesting point is that according to the Article 29 Working Party:

> "*the employer must also* ***consider the prohibition of the use of specific work devices for private use*** *if there is no way to prevent*