Technology in the Workplace – An Overview of Employment Law Issues in Europe

Summary:
We can no longer imagine our professional lives without modern information and communication technology. It is common for employers to provide employees with technology such as smartphones or notebooks. These communication and productivity tools are also used for social media – in both business and personal use – and are often not switched off by employees, even in their leisure time. Employees receive e-mails and calls in the evenings, on weekends, and during holidays. While mobile devices promote flexible working, they carry the risk that employees are “always online” in violation of working time regulations. Employers use modern surveillance tools to monitor their employees for regulatory compliance, safety and security. In this article, we discuss the key issues relating to technology in the workplace in various European jurisdictions.

1. Social media
(Isabel Meyer-Michaelis, CMS Germany, and Katrien Leijnen, CMS Belgium)

In Europe, 80% of all internet users are registered on social networks, and 70% are active users. This new norm is having a growing impact on the world of employment. For employers and employees, rights and obligations relating to the use of social media depend on the purpose of its use and whether it affects private or business social network accounts.

Business use of business network accounts
Employers often use social networks such as Facebook or LinkedIn for marketing or recruitment. When using business social media to these ends, employees must follow employer instructions concerning how they communicate with customers and the way they present the company over the social network.

Private use of private network accounts
As an employer’s right to control employee behaviour does not extend to off-duty activities, employers may not dictate or regulate their employees’ private use of social networks during leisure time. Nevertheless, employees are obligated to respect their employer’s legitimate interests when using social networks for private use. Trade and business secrets must be kept confidential, and defamation of an employer, supervisor or colleague is forbidden. Employees must not spread false information or make damaging assertions about their employers. Breach of these duties – which are often subject to social media guidelines – can justify the termination of the employment relationship.

But is an employee’s comment over a private network really “public”, and can it be used as justification for termination? The answer depends mainly on the confidentiality settings of the social network account (was the account accessible to all, or was it restricted to a private circle?) and whether the employee intended to make their assertions public.

Establishing clear guidelines covering the use of social media is recommended – for the benefit of employers and employees. A recent decision by Germany’s Federal Employment Court highlights the balance that needs to be struck when dealing with social media in the working context. In December 2016, the court ruled...
that if an employer allows visitor posts on its Facebook page that refer to the conduct or performance of individual employees, the settings for this function are subject to the works council's co-determination right.

2. **E-mail monitoring**

(Maité Ollivier, Raphael Bordier and Marie-Sophie Eminet, CMS France, Michał Tutaj, CMS Poland, Alyssia Mechalikh, CMS Luxembourg)

Most European countries limit the monitoring of employee e-mail and internet traffic. The approaches taken in France, Poland and Luxembourg illustrate a range of measures taken to this key interface between business and personal privacy.

**France** has very strict laws. Employers are required to faithfully execute employment contracts while respecting the privacy of their employees. The right of an employer to "monitor" the workforce is limited by mandatory compliance with the principle of individual freedom.

Key principles established under French statutory and case law include:

- **Data processing rules** – Setting up a system for monitoring the workforce often involves processing personal data. If employers want to record employees' telephone conversations, the telephone numbers called by employees, or track each employee's computer use, the EU General Data Protection Regulation (GDPR) must be respected when processing personal data, and no prior declaration must be made before implementing any of these systems (accountability principle).

- **Consulting employee representatives** – The employer must consult the works council or the social and economic council, (works councils are gradually being phased out and replaced by social and economic councils) before implementing a system for recording employees' telephone conversations or the telephone numbers called by employees, or for tracking each employee's computer use, in order to justify a disciplinary procedure. The system must be detailed in an IT policy to ensure its validity in support of sanctioning an employee for misuse of IT equipment.

- **Informing employees** – French law requires that employees be informed of the implementation of a "system for processing data containing names". The information supplied must cover: the system's properties and purpose; the people accessing the data; and the employee's right to access the data collected, refuse its collection (where possible), and rectify it. The French courts have held that information obtained from a computer system that was not brought to the attention of the employees is deemed to be unlawful proof, which may not be used against the employee.

- **Access to employee e-mails** – According to recent case law, an employer may not access private e-mail messages sent and received by an employee on a computer made available for professional purposes. In principle, employers may access professional correspondence without the employee being present. However, if the correspondence is marked as private, the employer must require the employee to be present before opening any files. If the employee refuses to be present, the employer may access the correspondence but must prove that the employee's presence had been duly requested and refused.

At every stage of the procedure, the employer must be able to justify its monitoring project on legitimate grounds and must take particular care to distinguish between private and professional correspondence. There are two ways to identify personal or private correspondence or data: either by distinctively marking them as such or by storing them in a clearly labelled file.

The distinction between professional and private correspondence must be based on the content of the e-mail. In other words, if some correspondence is deemed to be professional at first sight – i.e. it is not marked as private and is stored in a professional file – the employer may not produce the e-mail in court if its content is private.

In short, an employer may monitor professional communication and files stored on a company computer, provided that the information is not private. In **Poland**, new data protection legislation sets out rules on e-mail monitoring. The law is less strict than in France, but it obliges employers to define the scope, method
and purpose of monitoring in internal by-laws. The use of e-mail monitoring is restricted to situations when it is necessary to ensure the full utilisation of working time, or the proper use of working tools (such as business e-mail).

E-mail monitoring cannot infringe personal rights and secrecy of correspondence. Employers cannot monitor private e-mails. For this reason, companies sometimes prohibit using company e-mail for private purposes. Alternatively, employers require staff to store private messages in folders marked as private.

**Luxembourg** is a hybrid of French and Polish approaches. Employees must be informed if their e-mails are monitored. Incoming and outgoing e-mails not marked “personal” are deemed “professional”.

To avoid a breach of correspondence secrecy, which carries a criminal sanction, the Luxembourg regulator recommends one or more of the following practices:

- setting up a separate inbox for private and professional e-mails; or
- filing personal e-mails in a folder marked “personal”; or
- using the term “private and personal” in e-mail subject lines.

However, the employer is entitled to open a so-called private e-mail if there is a serious doubt over its real nature. The employer may also be entitled to access the employees’ e-mail boxes for business continuity purposes, especially when the employee is absent due to sickness.

In the **Czech Republic**, the employer may only subject the employee to open or secret monitoring, monitoring and recording of telephone calls, control of e-mails or control of letters addressed to the employee, when there is a serious reason to do so and must not inappropriately interfere with the privacy of the employee. The inspection must be carried out in an appropriate manner and after written information is provided to all the employees concerned about the extent of the control and the methods of its implementation.

Regarding the e-mail monitoring of e-mails, the opinion of the Czech authority implies that the employer is entitled to monitor only the number of received and sent e-mails. If there is a suspicion of misuse of the work e-mail system, the header may also be monitored (i.e. information relating to whom employees send messages and from whom they receive them). The Czech authority distinguishes between private and generic e-mail addresses. Unlike situations when the e-mail address is generic (e.g. info@domain.cz), if the e-mail address is composed of the name and surname of the employee, the e-mail delivered is considered to be a private e-mail and an employee’s expectation of privacy is higher.

### 3. Video and telephone surveillance

*(Tim Wilms, Guus Lemmen and Stephanie Dekker, CMS Netherlands, Ivana Meštrović, CMS Croatia, Michał Tutaj, CMS Poland, Alyssia Méchalikh, CMS Luxembourg, and Amelia Žrt, CMS Slovenia)*

Camera and telephone surveillance seem to be a logical solution to monitoring what goes on in the workplace. For example, employees often do not mind if retail stores use camera surveillance to guard against theft by outsiders. But what if the employees themselves are being monitored? Is this lawful? And can information obtained by such surveillance be used in a dismissal case?

**Known camera and telephone surveillance**

Surveillance requires that employers respect the privacy rights of employees, as set out in Article 8 of the European Convention on Human Rights (ECHR). As camera and telephone surveillance involves processing personal data, the employer must also comply with the GDPR and related national laws.

In general, the employer will need to be able to show that:

3.1 it is pursuing a legitimate purpose and interest – e.g. using camera surveillance to protect company property, employees and visitors, or using telephone monitoring of call centre employees for quality control.
3.2 Surveillance is necessary to achieve this purpose and to pursue the legitimate interests concerned. If there is a less intrusive way to achieve the purpose, surveillance is not considered necessary. In the Netherlands, for example, the continuous recording of telephone conversations (e.g. of call centre employees) for the purposes of training is not considered necessary.

3.3 Employee interests do not override the legitimate interests of employers. For example, camera surveillance is not allowed in bathrooms or changing rooms.

The employer should inform employees, in an appropriate and timely manner, about the surveillance, all related data processing activities, and their rights as data subjects. This can be achieved through the company’s employee privacy notice or a dedicated policy for the use of camera or telephone surveillance. For telephone surveillance, the Dutch Data Protection Authority's position is that it is not sufficient to inform the employee once only that calls may be recorded – the employee must be informed prior to each recorded call, for example by a sound signal.

The employer should also make a record of its data processing and establish a retention period for camera footage and phone recordings to ensure that they are not kept longer than is necessary to achieve the purpose for which they were collected.

Specific national requirements may apply in different jurisdictions. In the Netherlands, works council consent is required for implementing, amending or withdrawing regulations for camera or telephone surveillance. For large scale or systemic surveillance, a data protection impact assessment (DPIA) is necessary.

Hidden surveillance represents a considerable intrusion into the private life of employees and should be used with great caution. In the Netherlands, hidden surveillance is only allowed if, in addition to the general requirements outlined above:

3.1 It is used as a last resort and is based on serious cause such as suspicion of theft or fraud. Hidden surveillance may not be used for performance assessments (e.g. a mystery shopper with a camera).

3.2 Other less invasive efforts to establish the facts have not been successful.

3.3 The surveillance is limited in time and scope and is in line with the regulations agreed with the works council.

3.4 For camera surveillance, employees have been informed in advance that the employer may use hidden surveillance in certain situations. Informing employees about the possibility of hidden surveillance in advance may also legitimize hidden telephone surveillance.

3.5 Employees are informed about the actual use of hidden surveillance as soon as the investigation permits.

3.6 The employer has performed a DPIA and has consulted the Dutch Data Protection Authority prior to the use of hidden surveillance if according to the DPIA the privacy risk remains high despite mitigating measures.

In Poland, new GDPR-related legislation set boundaries for video monitoring. As a result, employers can only use video monitoring to ensure: employee safety; protection of property; production control; or confidentiality of information whose disclosure might damage an employer’s interests. Employers must clarify these general purposes in internal by-laws (i.e. workplace regulations).

Employers must also mark areas and rooms where video monitoring occurs and fulfill other duties to inform. As a result, the use of hidden cameras remains highly controversial in Poland. The minority opinion, expressed by some authorities, is that such monitoring is always illegal in employment relationships. However, the dominant opinion in Poland, supported by European case law, permits covert monitoring in extraordinary circumstances.
Restrictions on storing video recordings significantly limit an employer's ability to make effective use of video monitoring. Employers can only store video recordings for up to three months from the date of the recording, unless the employer has learnt that the tapes constitute or may constitute evidence in legal proceedings.

**Luxembourg**’s regulations on the surveillance of employees were amended following the entry into force of the GDPR. Surveillance is now possible in these six situations foreseen in the GDPR:

- the employee has given consent to the processing of his or her personal data for one or more specific purposes.
- the processing is necessary under the employment contract or for entering into the contract.
- the processing is necessary because of a legal obligation of the employer.
- the processing is necessary to protect the vital interests of the employee or of another natural person.
- the processing is necessary to carry out a task in the public interest or in the exercise of official authority vested in the employer.
- the processing is necessary to protect the legitimate interests of the employer.

Prior approval by the Luxembourg regulator is no longer required for the implementation of surveillance. Instead, prior information of it must be given to the employees concerned and their representatives, and must include: a detailed description of the purpose of the processing; the arrangements for implementing the supervision system; the duration or criteria for storing the data; and a formal undertaking by the employer that the data collected will not be used for a purpose other than that explicitly provided for.

Once informed, the employee's representative has a right to appeal to the Luxembourg regulator if the conformity of the processing is in doubt.

In **Slovenia**, the Personal Data Protection Act covers video surveillance. It has separate rules for *video surveillance of access* to the business premises and for conducting video surveillance *within working spaces*.

Companies may conduct *video surveillance of access* to their official office or place of business if it is necessary to safeguard people or property, ensure control of entry or exit to or from the premises, or – depending on the nature of the work – there is a possible threat to employees. The employees must be informed about its implementation. The act also specifies the data which may be collected and the maximum duration of storing the data (one year after its occurrence).

*Video surveillance of working spaces* can be carried out only in exceptional cases: where it is indispensable for safeguarding people or property; for protecting classified information and business secrets; and where these purposes cannot be achieved by other means. In certain premises – such as changing rooms, elevators and toilet facilities – video surveillance is absolutely forbidden. Employees must be informed about video surveillance within working spaces, and the employer must also consult with a trade union representative prior to its commencement.

Telephone recordings of employee conversations are not explicitly regulated by law, but generally are not permitted. The only employee personal data that can be collected is provided for by law, and is necessary for the exercise of the rights and obligations of the employment relationship. Employees also have the constitutional right to protect the confidentiality of letters and “other media”.

In **Croatia**, the use of video and telephone surveillance is regulated by the Labour Act, the Occupational Health and Safety Act and, more recently, by the Act on the Implementation of the General Data Protection Regulation.

Under the Occupational Health and Safety Act, it is only permissible to monitor employees entering and exiting the business premises, and when such monitoring reduces the risk of an employee's exposure to burglary, armed robbery, theft and similar occurrences at the workplace. Monitoring employees for any other
reason is generally not permitted under Croatian law. There is also a strict legal prohibition on placing monitoring devices in employee changing rooms, designated rest areas and spaces for personal hygiene.

Depending on the monitoring’s scope, consent of the works council – or the trade union representative acting as the works council – is required by law. Works council’s consent is needed if the planned monitoring of employees is continuous (i.e. if video cameras will monitor employee movements for the duration of the work day). If the works council or trade union representative withholds its consent to the monitoring of employees, the employer can seek an arbitral decision to substitute the works council’s consent. If the planned monitoring is not constant, the employer must still consult the works council or trade union representative, but their negative response is not binding.

Employers should include rules on video and telephone surveillance in employment by-laws, specifying the scope and purpose of the surveillance. Formal rules on the adoption of employment by-laws also include the employer’s obligation to consult the works council or trade union representative. Employers must also give prior written notice before conducting video or telephone surveillance of employees.

Croatian law does not allow employers to use hidden video or telephone surveillance. However, as EU case law has shown, hidden monitoring may be justified if an employer’s interests clearly prevail over an employee’s right to privacy.

Evidence acquired by the employer based on video or telephone surveillance may be used in dismissal cases, provided that the surveillance is performed according to relevant laws and regulations. In the case of evidence gathered through hidden surveillance, it remains to be seen how the Croatian courts would judge its permissibility, since there is currently insufficient court practice to provide a clearer view on the issue.

From a purely data processing perspective, additional obligations may be imposed on the employer under the Croatian Labour Act and the GDPR, including but are not limited to: the appointment of a data protection officer; determination of specific data retention periods; and implementation of an automated system for data access.

**Legal consequences in court proceedings**

What if the permitted criteria are not met and employers collect evidence unlawfully via hidden cameras or telephone recordings?

**Dutch** case law indicates that ascertaining the truth is, in principle, considered more important than preventing a violation of an employee’s right to privacy or data protection laws. Therefore, such evidence is often considered admissible and can, in principle, be used in court.

Employers breaching permitted surveillance criteria, however, do so at their own risk. If the employer infringes on the GDPR, for example by unlawfully processing personal data, the relevant data protection authority may impose a penalty of up to EUR 20m, or 4% of the worldwide annual revenue of the prior financial year, whichever is higher. Employers are therefore likely to attach the utmost importance to ensuring the lawful use of technology.

In **Poland**, there is no case law based on the new legislation. However, in light of recent legal developments on unlawful video evidence (the so-called “fruit of the poisonous tree”), courts are likely to accept such evidence. For employers, this judicial approach may offer some consolation given the quite restrictive law on workplace monitoring.

In **Slovenia**, if surveillance is in line with the law and all necessary conditions are met, there is no obstacle to using it in labour court proceedings. However, if recordings used as evidence were not obtained lawfully, the answer is not straightforward. According to Slovenian case law, the use of evidence acquired in violation of human rights (i.e. the right to privacy) in an employment dispute is not necessarily unlawful. The evidence may be permissible if circumstances justify it and if the evidence has a special meaning for the execution of some other right protected by the constitution. In these cases, the court employs the principle of proportionality to decide which right should be given priority.
4. Confidentiality and protection of business secrets

(Patricia Jares, CMS Germany, and Dario Hadžisaković, CMS Bosnia and Herzegovina)

The increased use of technology in the workplace has created new data privacy concerns: for employees, it is the storage and use of their personal information; for employers, it is protecting business secrets.

In many jurisdictions, non-disclosure and confidentiality agreements must be concluded between employers and employees in order to protect business secrets. Under German law, however, every employee has a contractual obligation of confidentiality during the employment relationship. This means the employee is obligated to take the interests of the employer into account and, even without explicit agreement, to maintain secrecy about internal company issues. This includes all matters that employees become aware of in connection with their work, especially where the employer has a legitimate interest in the matters being kept secret. Business secrets can mean information about a wide range of issues, including: technical matters and know-how, sales, suppliers, accounts and HR, computer programs and technology. How someone passes on protectable information to third parties, including the medium used, is generally irrelevant – the obligation of confidentiality therefore also applies to the transmission of information via electronic communication systems.

In Bosnia and Herzegovina (BiH), there is no explicit legal obligation for employees to protect and safeguard employers’ business secrets. Employees are liable, however, if they breach their work duties and responsibilities. This means the employees guilty of wrongful acts or gross negligence are liable for damages to their employers. This liability indirectly applies to an employee’s confidentiality obligation to safeguard his employer’s business secrets, if disclosure of those secrets can damage the employer.

In general, most employers in BiH impose confidentiality obligations on employees, which require them to treat all business-related data and information as business secrets, regardless of the type of media through which they are provided, for the duration of employment and afterwards. The confidentiality obligation covers information on commercial, financial, technical and strategic aspects of the employer’s business, as well as all other business secrets of the employer and its clients. It applies to other affairs of the employer, individuals associated with the employer, and other information and data related to the employer’s business operations. If a confidentiality provision is not part of an employment agreement, the employer and the employee may conclude a separate confidentiality agreement at any time during employment or after its termination.

Legal consequences of violation

If confidentiality is broken, employers in Germany have a right to apply for a prohibitory injunction. Violations of secrecy can also justify dismissal. For example, according to case law, unauthorised copying of data from an employer’s database onto private data storage devices constitutes good cause for dismissal without notice. In addition, damage claims and consequences under criminal law come into consideration. Special rules apply, particularly to persons subject to professional secrecy whose liability risk was taken into account by reform of the relevant criminal norms in 2017.

Under BiH law, violating a contractual obligation of confidentiality represents a serious breach of work duties and responsibilities, and is grounds for dismissal without notice. If the breach has caused damage to the employer, the employee must compensate the employer for the damage incurred.

Post-contractual non-disclosure obligation

Under German law in general, there is also an obligation in the post-contractual period for the former employee not to disclose business secrets. However, the protection is comparatively weak. A comprehensive non-disclosure obligation requires a specific post-contractual confidentiality agreement. Depending on the scope of the post-contractual confidentiality agreement, compensation is required for the duration of the prohibition if it impedes the employee’s professional career. Otherwise, these confidentiality agreements would not be enforceable.
Similarly, in BiH, employers generally prefer to maintain the contractual obligation of confidentiality after the termination of employment relationships. The post-contractual obligation of confidentiality is generally stipulated in one of: the employment agreement; the confidentiality agreement; or in employment termination documents (e.g. decision on termination of employment or agreement on mutual termination of employment agreement). However, a lack of viable court practice means the enforceability of confidentiality provisions and confidentiality agreements remains uncertain.

**Contractual penalty**

Generally under German law, the (post-)contractual non-disclosure obligation can also be "secured" by a contractual penalty agreement. However, there are strict requirements for an effective contractual penalty agreement and it must not unreasonably disadvantage the (former) employee. As a rule of thumb, court rulings deem contractual penalties amounting to one month's salary to be appropriate.

In BiH, contractual penalties may be agreed within employment agreements, confidentiality agreements or employment termination documents. The scope and amount of penalties are quite restrictive – contractual penalties agreed must be reasonable and must not put the former employee in a disadvantaged position.

**Uniform protection under European law**

In the Trade Secrets Directive (EU 2016/943 of 8 June 2016), the European Commission provided for uniform protection throughout the EU, including more strict requirements on the protection of business secrets. The main legal innovation is that anyone who wants to claim a violation of protected rights must be able to demonstrate and prove that all reasonable measures were taken to protect business secrets. It is therefore necessary to define “business secrets” very precisely.

EU member states were obligated to pass legislation to comply with the directive by 9 June 2018. To date, the directive has not yet been implemented into German national law. This means the existing national provisions must be interpreted in the light of the directive. A new law (GeschGehG) is planned to implement the directive, but no date has yet been set for its enactment. The draft law sets out that companies may assert civil claims for injunctive relief and damages in the event of the unauthorised acquisition, use or disclosure of trade secrets. At the same time, the draft provides justifications for whistleblowers.

5. **Employee representation**

(Luisa Wangler, CMS Germany; Caroline Froger-Michon and Madeleine Benistan, CMS France, Tomasz Sanczewicz, CMS Poland, Daniela Krömer and Tanja Schmadl, CMS Austria)

IT technology is intrusive, and staff privacy needs some protection. One safeguard is to involve employee representatives in the process of setting up IT systems, particularly those used for monitoring staff. Many EU countries require that an employer discusses IT issues with employee representatives before the technology is up and running.

Two legal approaches have emerged across the EU. In some countries – including the Netherlands and Germany – employee representatives have real decisive powers. They must agree to the use of modern IT technology or it is illegal. In other jurisdictions, employee representatives must be consulted about technology, but they cannot block its introduction or use.

In Germany, the works council has extensive co-determination rights for technology matters in the workplace. If a given technology can be used to supervise or monitor employees, the works council must be involved. This applies to all technical equipment, such as software or any IT mechanism collecting or recording personal data (e.g. a time recording system). Therefore an employer must conclude an agreement with the works council before launching monitoring software. The agreement sets out the technical system and the legitimate purpose of the software's data collection. If the parties fail to reach an agreement, a conciliation board must help settle the matter. If there is no works agreement, the works council may seek a preliminary cease and desist injunction to block the use of the technology.

In France, employee representatives are also involved in projects implementing new technologies, such as the acquisition of new information technology equipment, although employers make the final decisions. A
consultation process must be carried out for any important project introducing new technologies that could have consequences on employment, qualification, compensation or working conditions. The consultation must also deal with the consequences of the project on employee health and safety. Under the French Labour Code, employee representatives can also appoint a technical expert to give an opinion on the project. In this case, prior consultation is required, meaning that employee representatives must deliver an opinion, but they have no veto rights.

**Poland** is an example of a country at the other end of the co-determination spectrum. Trade unions or a works council (if it exists) must be consulted on various matters, including IT and video monitoring issues. But they cannot legally block the use of a given technology or a system. When the negotiations or consultations fail to produce an agreement, the employer can implement the monitoring systems unilaterally. Still, the employer must indicate the scope, method and purpose of monitoring in workplace by-laws (e.g. workplace regulations). The employer must also provide information to staff, even when it has already consulted with employee representatives on monitoring-related matters.

In **Austria**, a works council has different levels of involvement when implementing new technology in the workplace. The key criterion generally is whether a certain technology affects human dignity. This is particularly the case when the personality rights of employees are touched by the system in question.

If a technological system affects human dignity, consent of the works council – more precisely a works agreement – is obligatory. If no works agreement has been concluded, the works council may at any time file an injunction against the use of the technology by court order. If there is no works council within the company and it is a system that affects human dignity, individual consent by each employee is needed. Technology that violates human dignity is forbidden, whereas technology that does not affect human dignity may be implemented freely – unless the technology requires the conclusion of a works agreement for another legal reason.

If a technology determines, processes and transfers employee personal data systematically, a works agreement must be concluded with the works council (if one exists). If the works council refuses to conclude a works agreement, the agreement may be replaced by the decision of a specific arbitration board.

6. **Private use of company devices (internet, e-mail, smart and mobile phones) and BYOD**

(Maximilian Koschker, CMS Germany, Andrea Červenková, CMS Czech Republic, Vincent Delage and Titrite Baamouche, CMS France)

Day-to-day work is virtually impossible nowadays without IT and electronic data processing (EDP) systems. Employees spend many hours in front of PC and laptop screens, call clients or colleagues via smart phones when they are on the road, or use other IT gadgets provided by their employer. It is therefore no surprise that employees also wish to use work communication appliances for private purposes – a quick e-mail or Facebook message to friends, an Instagram post, reading the latest sports results or making a quick call to a family member.

Companies often know that the devices they provide are also used by staff for private purposes from time to time. Even if they do not like it, they often tolerate private use in order not to jeopardise employee satisfaction. Given the ongoing war for talent, employers cannot afford to appear old-fashioned or inflexible, especially in the eyes of so-called "digital natives". The result is that clear work instructions covering whether and to what extent private use is permitted tend to be the exception rather than the rule. This then leads to a complicated situation in which neither management nor staff know exactly what is permitted and what is not.

From the company's point of view, this uncertainty constitutes the greatest risk. In **Germany**, for example, the question of whether employees are legally entitled to use communication devices for private use if the employer tolerates such use for a long period of time without objecting ("company practice") is disputed. If a legal entitlement arises, the employer cannot in most situations unilaterally eliminate this entitlement (i.e. ban private use) at a later stage. Therefore, the employer's aim must be to exclude such claims from the outset. This can only be ensured if there is an express written provision – in a contractual agreement, unilateral
employer guideline, or works agreement – setting out the employer’s position on the private use of company devices.

However, where the employer actually decides to permit the private use of company devices, this may give rise to further risks and uncertainties. In Germany and before the GDPR, the prevailing, if greatly disputed, view has been that the employer becomes the provider of telecommunications services – comparable to telecommunications companies under the German Telecommunication Act (TKG) and the German Telemedia Act (TMG) – as soon as it allows its employees to use company communication devices for private purposes. Consequently, the employer has widely been considered to be bound to telecommunication secrecy, which considerably restricts the company’s ability to control the conduct of employees online and the way they use its devices. However, it is questionable whether the concept of the employer as provider of telecommunications services can be upheld with the GDPR in force. Some legal commentators in Germany believe the company’s right to control employee usage of the company devices will exclusively be governed by GDPR standards and requirements in the future – because national laws such as the TKG or the TMG may not set stricter requirements for data processing measures than the GDPR. And yet, many legal commentators in Germany clearly advise employers not to permit the private use of company IT and EDP systems and devices in the first place, arguing it is simply not worth the hassle (as an alternate approach, see “BYOD” below).

There is a clear need for employers in Germany to act to avoid unregulated and uncontrolled private use. At the same time employers must carefully consider whether they wish to permit private use of work IT at all since, even at this stage, it is still unclear whether such permission means employers are providers of telecommunications services under the German TKG and TMG.

In the Czech Republic, there is a general prohibition on employees using the employer’s property for private purposes without the employer’s consent. This rule applies to all kinds of production and working instruments belonging to the employer, including computer technology and the employer’s telecommunication equipment. Use of the employer’s property for private purposes without the employer’s consent is a breach of the employee’s obligations. If the employer tolerates such use for a long period of time without objecting (“common practice”), implied consent of the employer can be inferred. However, if the employer declares different rules (e.g. stipulates a general prohibition in by-laws), employees are obliged to respect the prohibition in place of previous common practice. Therefore, it is highly recommended to set out the rules in writing, for example in by-laws, contractual agreements or their equivalent. The employer is authorised to check compliance with the prohibition in an appropriate manner. Any checks must be proportionate to the objective and must only interfere with the privacy of the employee to the extent necessary to perform the check or to protect the employer's property.

In France, employers also need to find a fair balance between the professional use of company devices – which remains the general rule – and personal use of these devices. French case law gives companies some benchmarks for determining a “fair” balance.

Firstly, employers cannot prohibit personal use of company devices – they must allow the possibility of reasonable use. This tolerance does not mean that employees cannot limit the use of their work devices. Case law has confirmed, for example, that a disciplinary sanction was justified against an employee who used a large part of his professional computer’s storage space for personal purposes. Likewise, a sanction was upheld against an employee who had a total of 10,000 internet connections for personal purposes in just over 15 days.

Second, if employers have the right to consult a professional file, e-mail, or document saved on a company device, they must act very carefully where these items are expressly identified as “personal” or “private”. The employer cannot open the files without the presence of the employee. Failure to take this approach could result in the employee seeking damages on the grounds of violation of the right to privacy or, if appropriate, the secrecy of correspondence.
Given the impact that the digital revolution is having on companies, it is highly recommended that employers implement an IT charter mapping out best practices, including measures concerning the processing of personal data, in compliance with the GDPR.

**Bring your own device (BYOD)**

"Bring your own device (BYOD)" refers to the practice of allowing employees to use their private and personally owned mobile devices – smartphones, tablets, laptops and so on – for business purposes by being granted access to their employer’s IT infrastructure, such as e-mail systems, company servers and the intranet. Studies show that BYOD leads to increased productivity, efficiency and employee satisfaction, especially as they no longer need to carry two separate devices (one for business and another for private use). From the company’s perspective, BYOD may lead to significant savings as it removes the need to acquire dedicated business devices and dramatically cuts maintenance costs. However, it may raise IT security risks if the corporate IT infrastructure can be accessed via private devices.

In **Germany**, if the employer allows BYOD it must ensure that it complies with statutory data protection provisions – particularly German Federal Data Protection Act (*BDSG*) and European GDPR. These national and international data protection regulations apply because employees may have access to the personal data of other employees in the company (i.e. e-mail addresses, telephone numbers and other personal information) when accessing the company network via their private devices. In contrast, it is the prevailing view in Germany that the German *TKG* and the German *TMG* laws do not apply, as the employer does not offer telecommunications services in connection with BYOD – it only offers access to its business data and IT infrastructure.

Under data protection law, the employer must ensure that technical and organisational measures are in place, such as controlling the access to and transfer of data. For regulatory and technical reasons, it is therefore highly recommended that employers use so-called “container apps”. These programs allow for a strict separation of private and business content by creating two separate data areas (“containers”) on the mobile device – effectively creating two phones in one. For the separated business container, the employer can ensure that it fulfils all statutory data control and protection obligations. However, in order to do so and because the device is solely owned by the employee, the employer must ensure that its BYOD agreement with the employee grants access rights to the employee’s device.

Introducing BYOD means the employer must involve various departments – e.g. IT, Legal, HR, Compliance. The employer also must respect the co-determination rights of an existing works council, as BYOD is likely to concern employee conduct and technical monitoring systems, as covered by the German Works Constitution Act (*BetrVG*). If a works council exists in the company, a works agreement containing all relevant details is usually the best way of implementing BYOD. However, it is not possible to force employees to make their private devices available for business purposes by means of a works agreement – the employee’s consent to BYOD must be obtained by the employer on an individual level.

Other legal problems raised by the practical use of BYOD include the issue of working time, particularly observance of the German Working Hours Act (*ArbzG*). The use of a private device for business purposes can *de facto* lead to permanent round the clock employee availability, as employees typically keep their private mobile devices switched on at all times and also use them for business communication way beyond normal working hours. The employer must ensure that employees comply with the statutory maximum working time per day, for example, and do not use their private devices for business purposes in violation of these statutory limits.

While BYOD has several advantages for both employer and employee, it also carries risks – including IT security concerns for the employer and excessive working hours for the employee. The complex legal environment, particularly concerning data privacy and working time restrictions, must be respected and observed. Employers in Germany should therefore consider carefully whether they wish to introduce BYOD.

In **France**, while there is no specific legal framework for BYOD, it still raises practical questions and legal issues. Unlike company devices, with BYOD the employer does not have the same amount of control over the use of devices that belong to employees. However, French case law has confirmed that an employer can
access a personal device if the employee is present or at least duly summoned. The case in question concerned a dictating device, and it is not certain the same conclusion would apply to a personal phone or laptop.

BYOD can also raise issues about psychosocial risks. For some employees, using a personal device can blur the boundary between effective work time and effective rest time and, consequently, between professional and personal life. However, under French law, employers must ensure that employees are working in safe and healthy conditions, which can be complicated by BYOD.

Companies considering BYOD could be challenged by employees on the grounds of inequality. The most productive devices are generally the most expensive ones, which means that employees who can’t afford high-end devices may have a lower productivity rate at work than those who can afford to buy a premium device.

Companies should frame BYOD practices within an IT charter that aims to avoid any risks and covers all GDPR issues.

7. Working time issues

(Isabel Meyer-Michaelis, CMS Germany, and Martina Novysedlakova, CMS Slovakia and Sinan Abra, CMS Turkey, Eva Ceca and Lucia Campillo Jaen, CMS Spain)

Generally speaking, home and remote working does not take place on a 9 to 5 (eight hours) daily working time basis. In most cases, people work whenever they need to from a business perspective, or when it is convenient for them personally. Conflicts with EU working time law are therefore unavoidable.

At the EU level, the Working Time Directive (2003/88/EC) requires EU countries to guarantee minimum standards to protect worker health and safety. Weekly working hours are limited to 48 hours on average, including any overtime. In addition to a minimum daily rest period of 11 hours, a minimum rest period of 24 uninterrupted hours is required for each seven-day period. This directive has been widely implemented throughout the EU.

In Germany, a statutory eight-hour day, not including breaks, applies under the Working Hours Act (Arbeitszeitgesetz). Daily working hours may be extended up to ten hours if an average of eight hours per workday is not exceeded within six calendar months or 24 weeks. Based on six working days a week (Monday to Saturday), the maximum temporary number of permissible weekly working hours is 60 (6 x 10) hours in general, while the average number of working hours allowed over a longer period is a maximum of 48 (6 x 8) hours per week.

According to the Working Time Directive, employees must be given 11 hours of uninterrupted rest. For employment or work with special health hazards, both the daily working time and the duration of this rest period may be extended or shortened accordingly. However, an employer may agree to an extension or shortening in a collective bargaining agreement or in a works agreement endorsed by the local authority. Periods during which employees are free to choose how they spend their time, but must be available to start work immediately or soon after they are called, may be counted as rest periods. If the rest period of 11 hours is interrupted, a new full period must be granted after the interruption.

In Slovakia, the rules on uninterrupted daily rest are stricter: employees must be given 12 hours of uninterrupted rest (14 hours for minors) over 24 hours. The rest period may be shortened to eight hours, but only for employees over 18 years of age who work in continuous operations, seasonal work, urgent agricultural work, universal post services, urgent repair work aimed at averting danger to employee life or health, and during emergencies. If the employer shortens an employee’s uninterrupted daily rest, it must provide the employee with the equivalent uninterrupted rest within 30 days.

Employers are obligated to record working hours that exceed the daily working hours limit. The flexible nature of mobile work makes proper documentation of working hours necessary so that this recording duty can be satisfied. The employer may transfer this documentation duty to the employees. This does not
release employers from their responsibility to ensure that the recording duty is duly satisfied. Hence it is advisable to make spot checks.

In **France**, the recent Act of 8 August 2016 (*Loi Travail*) gives employers with more than 50 employees a new yearly obligation to negotiate the right to disconnect, in order to guarantee rest periods and respect for private and family life. Negotiations should focus on ways each employee can fully benefit from the right to disconnect and on regulating the use of digital tools. If a negotiation fails, the employer is required to prepare and implement a charter about the terms and conditions of the right to disconnect. The charter should include information and training measures for employees and management concerning the reasonable use of communication tools. The existence of an agreement or charter is a condition for the validity of contracts that reference an annual number of working days (*forfait jours*) rather than working hours.

In **Spain**, pursuant to the Workers’ Statute, the maximum working time per week is 40 hours on an annual average. Likewise, the maximum working day may be extended to up to nine hours unless otherwise agreed in the collective bargaining agreement, observing a minimum uninterrupted rest of 12 hours between each working day. In addition, employees have the right to take a weekly rest of at least an uninterrupted day and a half (to be accumulated in periods of 14 days).

Any hours of work beyond the maximum ordinary hours are considered overtime, which will be compensated according to the collective bargaining agreement or the employment contract (offering equivalent time off or economic compensation equivalent to the salary during ordinary hours). In any event, overtime may not exceed 80 hours per year (excluding overtime compensated with equivalent time off within the following four months or overtime needed to repair accidents or other extraordinary and urgent damages).

In addition, the new Spanish Data Protection Act published in the Official State Gazette on 6 December 2018 has just introduced the right of employees to disconnect out of working hours. However, the law does not clarify how employees should exercise this right, leaving the decision to the collective bargaining agreements or to agreements with employees’ representatives. According to this new law, the employer, after meeting the employees’ representatives, must elaborate an internal policy for the employees, including managers, that defines the ways the right to disconnect will be exercised, as well as the proper actions necessary to train and raise awareness about the reasonable use of IT equipment.

In **Turkey**, according to Turkish Labour Law, the maximum working time for full-time employees is 45 hours per week and 11 hours per day.

However, where the employer and the employee agree to do so, the employer may ask the employee to work for more than 45 hours a week, provided that the average working time over a two-month period does not exceed 45 hours on average. This two-month period may be increased up to four months under collective bargaining agreements.

In each case, it is mandatory under the Turkish law for employers to grant employees a 24-hour period of uninterrupted rest for each week of work.

Unless otherwise agreed upon between employee and employer, every day of the week except Sunday is considered a working day. An employer may ask an employee to work during weekdays and Saturdays, if working hours remain within weekly and daily limits.

In addition, it is possible for the employer to request overtime work without additional compensation if employees have given written consent under the original employment agreement or a separate one. Even in such cases, however, overtime work is limited to 270 hours per year. Furthermore, employees who receive minimum wage must consent to and be compensated for any overtime work.

If the 270-hour overtime limit is included in the employment agreement, an employer may ask an employee to work more than the 45-hour weekly limit. However, even in this case, the daily work cannot exceed the 11-hour limit.
Where employment agreements do not include the 270 hours or where the overtime work performed by an employee exceeds this limit, the employee is entitled to receive overtime payment or receive time off in lieu of overtime pay.

Any work performed on a mobile basis or out of the regular work place will count towards the working hours indicated above, and are also subject to the above rules.

Pursuant to social security legislation, an employer is obligated to record employee overtime work and include this in the employee’s pay slip. If the employee signs the corresponding pay slip without any reservations, he accepts the extent of the overtime work indicated (i.e. the employee will not be able to claim that he performed further overtime work). If the employee signs the pay slip with a reservation, then he may resort to other evidence (e.g. witness statements) to prove that he performed more overtime than that specified on the pay slip.

8. Flexible working

(Val Dougan and Jessica Joel, CMS UK)

As technology evolves, employees are increasingly requesting flexible working conditions, such as home-based working and flexible working arrangements.

In the UK, there is a statutory right for employees with at least 26 weeks’ continuous employment to make a request for flexible working for any reason, regardless of caregiving responsibilities. Flexible and home-based working can bring many benefits to employers, including reduced overhead costs, increased productivity and better motivation of their workforce. However, when considering flexible working requests, employers must consider a range of other factors, including how the work will be carried out in practice.

An employee request for flexible working time should include details of the change they are seeking, the effect they think the change will have and how the employer might deal with the new arrangements.

Employees are entitled to make only one statutory flexible working request in any 12-month period, and the maximum period for dealing with the request is three months between receipt and the employer’s final decision.

Under the law, an employer can refuse a request for flexible working on one of the eight prescribed grounds, including the burden of additional costs, detrimental effect on ability to meet customer demand, inability to re-organise work among existing staff, and planned structural changes.

The maximum amount of compensation for a breach by the employer under the statutory scheme – for example that it failed to deal with the application in a reasonable manner or that it rejected the application for a reason other than one of the statutory prescribed grounds – is eight weeks’ pay which is capped at statutory rates, rather than actual wages. However, in considering any request for flexible working, whether under the statutory scheme or otherwise, employers need to remain mindful of any potential discrimination claim (for which compensation is uncapped) arising from any rejection.

For example, it is common for women to argue – often, but not always, at the point they return from maternity leave – that the refusal to grant flexible working amounts to indirect sex discrimination, in addition to any claim under the statutory procedure. Before refusing a request from a woman to work flexibly for childcare reasons, employers should consider the “objective justification” threshold for defending a claim, which means being able to demonstrate that the decision was a proportionate means of achieving a legitimate aim.

Issues such as employee health, working time legislation, data privacy and confidentiality are also significant considerations for an employer when allowing employees to work flexibly from home. Employers should carry out (or ask the employee to carry out) a risk assessment, which considers various health and safety-related risks for home-based workers. Performance management is also important, and this can in some circumstances involve employee monitoring (see section 2. above).

Advances in technology mean that employees are potentially contactable around the clock, regardless of where they are located. This ‘digital overload’ can have an impact on employee mental health and in turn increase the pressure on businesses when staff is absent due to workplace-related health issues. In France,
the “right to disconnect” obliges businesses to negotiate with staff on their rights to switch off their work devices, and to consider ways to reduce the intrusion of work into their private lives. Although there is no such law in the UK, employers have a duty to provide a safe working environment, and there is pressure on employers to improve their management of employee digital technology use to reduce workplace-related stress.

In this digital age, the increase in home-based working and flexible working arrangements means employers must ensure their workers are afforded the 48-hour maximum working week protection under the Working Time Regulations 1998. The law applies to most workers in the UK, unless they opt out. In a recent Irish case, an employee was awarded EUR 7,500 for working in excess of 48 hours a week as she regularly received and responded to work e-mails outside working hours. The court found her employer did not keep records of the hours the employee worked, but was aware of the excessive hours worked and failed to take any action to curtail them. Employers must ensure they keep proper records of hours worked to assist with defending such claims and take active steps to reduce excessive working hours.

Where flexible and home-based working arrangements are introduced for the first time, employers should consider the effect on several policies. In light of increased fines for data breach under the GDPR, putting procedures in place to protect the company’s confidential information and ensure the secure disposal of any paperwork taken out of the office are key risk issues. Up-to-date employee handbooks and formally documented home-based working arrangements assist employers in protecting their business needs and the wellbeing of employees who work flexibly or remotely.

9. Working with “the cloud”

(Emina Mameledžija and Dario Hadžisaković, CMS Bosnia and Herzegovina)

The somewhat misleading term of “cloud computing” refers to data storage, management and processing using remote servers hosted on the internet. Due to its many advantages, this method of data management makes storing data on local servers or personal computers obsolete.

From an employment law perspective, companies increasingly use cloud computing to manage employee personal data for purposes of payroll accounting, maintenance of pension scheme plans, employee participation in shares trading, and so on. Especially for large corporations, this often involves processing and transferring employee personal data onto servers outside the country of origin.

These activities raise privacy questions concerning the protection of personal data. Even though cloud computing is not legally regulated per se in BiH and in many other European countries, the protection of personal data is a legal requirement for all legal entities that process personal data. However, cloud computing of personal data is treated within the meaning of the legal definition of data processing, which entails the storage and management of data. The matter becomes more sensitive when it relates to processing and transferring employee personal data, which is subject to strict data protection rules.

In BiH, the Law on Protection of Personal Data prescribes that personal data transfer (including transfer of personal data outside BiH) and processing is registered with the competent authority, the Agency on Data Protection of BiH. As a precondition for registration, it is mandatory that a personal data processing and transfer agreement is concluded between the processor and the controller. Under the agreement, the controller is considered to be the local employer and the processor is the legal entity (including foreign legal entities) using the cloud computing system for the processing of personal data. An important element of this agreement is the obligation and duty of the processor to guarantee the highest EU standards of personal data protection and privacy, especially concerning technical equipment and processing methods. This agreement is subject to review and approval by the Agency on Data Protection of BiH.