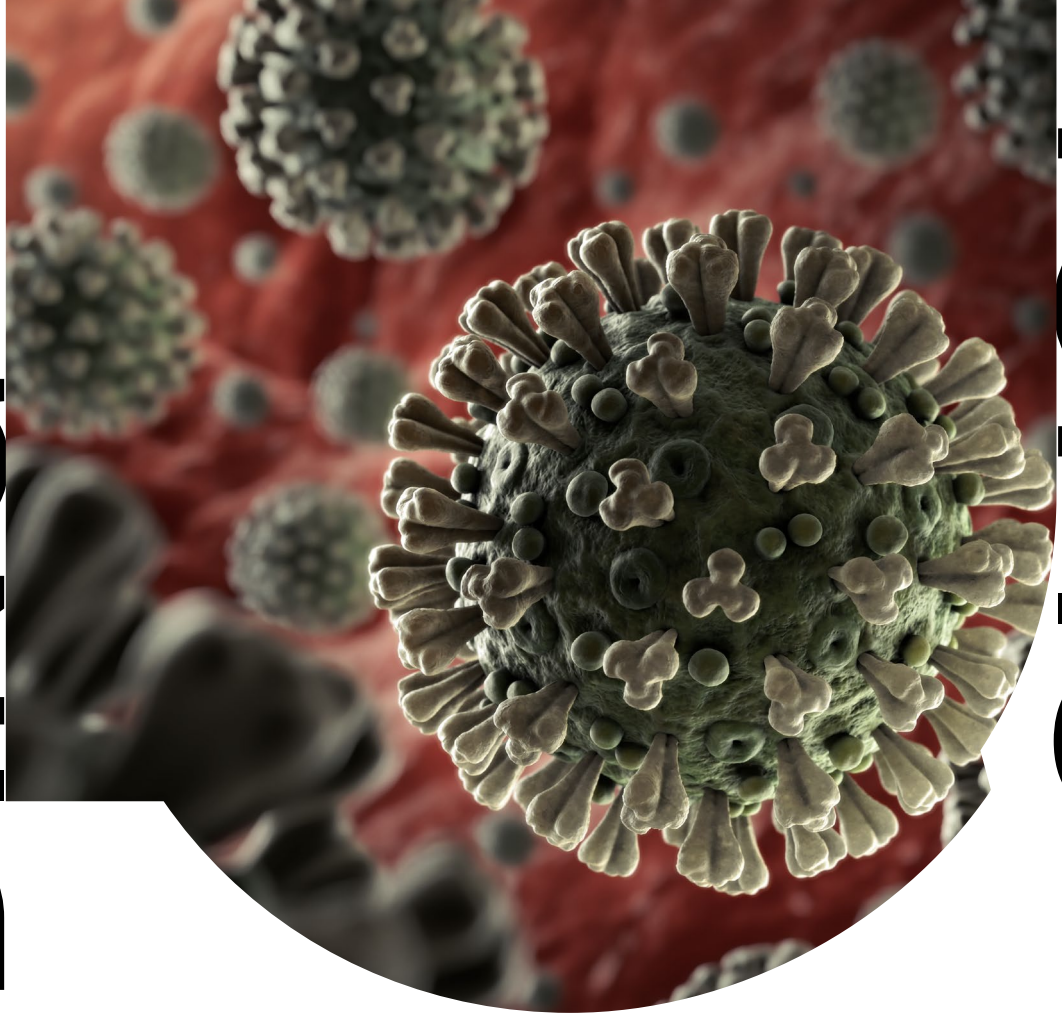
TRENDING TOPIC



13 APR. 20

TECHNOLOGY, MOBILITY AND COMMUNICATIONS

Coronavirus: Privacy in the context of teleworking, e-learning and entertainment

The figures recently published by ANACOM (the Portuguese National Communications Authority) are clear: the spread of COVID-19 and the individual and community protection measures imposed have led to an increase of 50% in electronic communication traffic in Portugal.

PLMJ

Pedro Lomba
Jorge Silva Martins
Carolina Sousa Guerreiro
Rita de Sousa Costa

Fixed network data traffic has increased by 54% and mobile data traffic by 24%. There has also been a particularly significant increase of 94% in fixed network voice traffic. The mass use from home of technological means of communication has gained renewed relevance.

In fact, the increase in electronic communications traffic is happening on a European scale. As a result, the European Commission and BEREC have suggested that, in the event of network congestion, telecoms operators and streaming services should adopt absolutely exceptional traffic management measures. These measures can include a reduction in connection speed and the provision of lower resolution content.

> "Coupled with the increase in electronic communications traffic, in particular, due to new ways of working and providing services at a distance, and to entertainment use, there are also a known set of risks to the privacy of individuals and to the security of information and trade secrets of organisations."

Coupled with the increase in electronic communications traffic, in particular, due to new ways of working and providing services at a distance, and to entertainment use, there are also a known set of risks to the privacy of individuals and to the security of information and trade secrets of organisations. Below, we identify some fundamental issues from a legal perspective that people and organisations should take into account in order to protect themselves.

Some key ideas to protect personal data and for security of information in the context of teleworking, e-learning and entertainment

Eurobarometer published data from a survey on the attitudes of Europeans toward cybersecurity in January 2020, so prior to the health emergency that has hit the country and the world. In that survey, 54% of Portuguese respondents agreed that the main concern underlying the use of internet services relates to the possibility of misuse of their personal data. The Portuguese figure was 8 percentage points above the European average. Eurobarometer also published the results of another survey in January 2020. This survey was on the attitude of Europeans towards the effects of digitalisation on everyday lives and more than 40% of Europeans said they would like to have a more active role in control over their personal data.

The majority of the active population is now teleworking (working from home) and children and young people are also staying at home and having lessons remotely using technological means. At the same time, children, young people and adults have the opportunity to view more entertainment content, such as films and series. They are also taking part in online meetings for work or social reasons. Against this background, we will highlight four key issues in relation to confidentiality, and privacy and security of information of individuals and organisations, in times of a health emergency.

"The legal framework on cyber security establishes a system of compulsory notification of incidents directed at public bodies, operators of critical infrastructures, operators of essential services, and digital services providers."

1. Be especially alert to situations of fraud and, where applicable, report them to the National Cybersecurity Centre or to the police

The National Cybersecurity Centre (CNCS) and ENISA have warned the public about set of cyber threats that have arisen in the context of the pandemic to take advantage of the fragility of people and organisations. These threats include phishing attacks by SMS and social networks, ransomware and other malware contained in certain applications, and the proliferation of fraudulent emails and websites.

The legal framework on cyber security establishes a system of compulsory notification of incidents directed at public bodies, operators of critical infrastructures, operators of essential services, and digital services providers. This framework also establishes rules on voluntary notification of incidents that can be used by any entity that has faced an incident with significant impact on the continuity of the services it provides.

Incidents are notified via the CNCS website. However, this notification does not prevent the person or entity affected from also reporting the incident to the police, because many security incidents are the result of criminal activities provided for and punishable under criminal the laws on cybercrime and on data protection.

2. As a data subject or as the representative of an organisation, always read the privacy policies or statements of any platforms you sign up to and of any subscriptions you acquire

The provision of privacy policies or statements is one of the transparency obligations with regard to processing the data of any data subject that the GDPR imposes on data controllers When the data subject's data are collected from the subject or from a third party, the GDPR establishes a mandatory list of information that the data controller must provide. The privacy policies or statements are one of the ways for data controllers to comply with this legal obligation of transparency.

Therefore, reading the privacy policy or statement allows anyone who wishes to sign up on a platform, or any organisation that wishes to subscribe to a service, to find out about the fundamental details of the data processing carried out by the platform or service. They can also find out the extent to which the platform establishes mechanisms for privacy by design and privacy by default. This also makes it possible, among other things, to compare the standards of privacy between different competitors, when it comes to choosing the (best) service.

Some of the useful information that privacy policies or statements provide is, for example:

- **The purpose of the data processing.** This section informs you about all the (other) purposes for which the platform uses your data, besides merely providing you with the specific service you signed up for. In extreme cases, you can even find out if your data are being "sold" to third parties.

- **The types of personal data collected**. In this section, you can check exactly what data the platform collects. The data collected must be limited to what is necessary to achieve the objectives. It is not good practice to demand multiple data that has no connection with the operation of the service.

- **The recipients or categories of recipients of the data.** This section informs you which entities or categories of entities can access your data and this allows you trace your data to some extent. It covers any subcontractors of the platform, i.e., entities that process data for the platform and with which it has made a personal data processing agreement.

- **The interconnections with other social networks.** This section tells you what data is shared with social networks, either by your choice as data subject (for example, by authentication using a social network account) or, if applicable, through other interconnections.

- **The location of the data and the processing operations.** The location where the data are to be processed may also be an important issue to take into account when choosing a platform. This is because many countries outside the European Economic Area (EEA) have not adopted data protection legislation, or they have legislation in place with standards below the ones that apply in the EEA.

3. As an employee or service provider of an organisation, read carefully the internal regulations on use of devices and platforms produced by your employer or customer

More and more organisations, including those that do not have ISO 27001 certification, are introducing internal regulations on security of information. Among many other provisions, these may regulate the use of devices and platforms, whether in the network of the organisation itself or in other private networks from home, and BYOD regulations in cases where the employee uses their own device. Regulations like these are good practice in the field of information security or even the accountability of the data controller. However, there is no express legal obligation that requires organisations to produce these documents.

The employees or service providers of an organisation that has adopted regulations or an internal policy of this nature should read the document carefully to identify any doubts. If there are any doubts, they should ask the employer/customer when possible.

"The employees or service providers of an organisation that has adopted regulations or an internal policy of this nature should read the document carefully to identify any doubts. If there are any doubts, they should ask the employer/customer when possible."

By virtue of the employment relationship, employees are bound by a set of obligations of diligence, care and loyalty in relation to their employer. They are also required to comply with the employer's orders and instructions.

Failure to follow the rules contained in the regulations or information security policy may, in certain cases, have very damaging consequences for the organisation. For example, it could cause a personal data breach or other infringement of the GDPR. As data controller, the organisation will be liable for any such breach or infringement. Furthermore, situations such as the use of unauthorised software by the organisation may lead to problems not only in the field of information security and personal data protection, but also problems involving intellectual property. However, any such conduct in violation of internal rules of the organisation and, therefore, the duties of employees explained above, may, in a particular case, give rise to disciplinary proceedings.

The same rationale as in preceding paragraph may also apply, with the necessary adaptations, to service providers. In this case, there is no question of the application of disciplinary power, but, ultimately, the possibility to terminate the contract for the provision of services or even to bring an action for civil liability.

4. Pay special attention to any inadvertent disclosure of business secrets of the organisation you represent, or where you work

The concept of trade secrecy refers to business information that is confidential and that the business wishes to remain confidential. Trade secrets are one of the main assets that organisations have, particularly those with an innovative profile, including SMEs and startups.

The legal rules on trade secrets result from the implementation of the Directive on the protection of undisclosed know-how and business information (trade secrets) in the new Portuguese Industrial Property Code. Broadly speaking, this legislation protects information that (i) is secret; (ii) has commercial value because it is secret; and (iii) has been subject to reasonable steps to keep it secret. It is clearly a very broad concept and it seeks to provide consistent protection of information.

Therefore, companies must be able to identify what trade secrets are likely to be more exposed in a situation where so many people are working from home, so they can take additional measures to protect that information, in particular, by restricting the access rights of users who connect to the corporate network.

Additionally, the law sets out a list of unlawful acts relating to obtaining, using, or disclosing trade secrets without consent. It highlights access to or unauthorised copying of documents containing the secret and which are under the control of the person holding them. It also highlights the breach of confidentiality agreements.

In this period of a health emergency, we have set out some of the risks associated with the use of devices and platforms in the context of working from home. These include, in particular, cyber threats or the use of applications or platforms that do not prioritise information security (and, therefore, the confidentiality) of information obtained, which expose the trade secrets of organisations.

This note was drawn up on 3 April 2020. It is not intended to be exhaustive and it should never substitute specific legal advice. ■