IUS ET SCIENTIA
2020 • Vol. 6 • Nº 2 • ISSN 2444-8478
https://editorial.us.es/es/revistas/ius-et-scientia
https://dx.doi.org/10.12795/IETSCIENTIA • © Editorial Universidad de Sevilla 2020

Risk assessment as a fundamental criterion for extensive interpretation in determining the suitability of telework

LA EVALUACIÓN DE RIESGOS COMO CRITERIO FUNDAMENTAL PARA UNA INTERPRETACIÓN AMPLIA A LA HORA DE DETERMINAR LA IDONEIDAD DEL TELETRABAJO

Juan Francisco Rodríguez Ayuso
Universidad Internacional de La Rioja
juanfrancisco.rodriguez@unir.net 0000-0003-4721-1465

Recibido: 17 de noviembre 2020 | Aceptado: 21 de diciembre 2020

ABSTRACT

This study offers an exhaustive analysis of new developments which, from an eminently technical perspective, brings with it the entry into force of Royal Decree Law 28/2020, of 22 September, on distance working. More specifically, it sets out those measures which, in favour of the integrity, confidentiality and availability of information, must be implemented by companies in order to guarantee the adequate protection of the data processed by employees who, exceptionally or regularly, have to carry out their tasks outside the installations of the organization to which they belong in the form of teleworking.

KEYWORDS

Distance working
Teleworking
Information security
Privacy
COVID-19

RESUMEN

El presente estudio ofrece un análisis exhaustivo de novedades que, desde una perspectiva eminentemente técnica, trae consigo la entrada en vigor del Real Decreto-ley 28/2020, de 22 de septiembre, de trabajo a distancia. Más concretamente, expone aquellas medidas que, en pro de la integridad, confidencialidad y disponibilidad de la información, deberán implementarse por parte de las empresas con el fin de garantizar la adecuada protección de los datos tratados por los empleados que, de forma excepcional o regular, hayan de desarrollar sus cometidos fuera de las instalaciones de la organización a la que pertenecen en la modalidad de teletrabajo.

PALABRAS CLAVE

Trabajo a distancia
Teletrabajo
Seguridad de la información
Privacidad
COVID-19

I. INTRODUCTION

It seems appropriate to start by analysing what is meant by *risk*. In general, risk is defined as the probability of a threat materialising and the impact it would have if it did, with a threat being understood as any risk factor likely to cause harm or prejudice to the data subjects whose personal data are processed. As we can easily deduce, the risk will always be present and will condition any type of decision that we have to take, which determines the need to identify that risk and proceed to its evaluation in order to be able to reduce it[1]. In terms of data protection, the risk would be the likelihood of harm to the data subject as a result of processing operations on his or her personal data.

We refer, in this way, to the risk that may be involved in carrying out processing operations on personal data owned by the data subject in relation to his or her fundamental rights and freedoms, in particular the fundamental right to the protection of his or her personal data. Thus, it is essential to take into account the risk involved in any processing of personal data, as well as any other risk that may arise from situations such as security breaches, which may entail physical, material or immaterial damages to individuals, such as loss of control over their personal data or limitations on their rights, discrimination, identity theft, financial losses, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data subject to professional secrecy or any other economic or social damage relevant to the data subject.

No definition is provided of what is to be understood by *high risk*, it being advisable that it be the European Data Protection Committee, as established in recital 77 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, RGPD or GDPR)[2], which issues those guidelines relating to processing operations considered unlikely to involve a high risk to the rights and freedoms of data subjects, indicating, likewise, what measures may be sufficient, in these cases, to deal with the risk.

On the other hand, the new legislation on the protection of personal data does provide certain criteria for understanding this high risk, such as the sensitivity of the personal data and the consequences that the processing of the data may entail for the data subject, which implies that the controller must carry out an impact assessment and, where appropriate, a prior consultation of the supervisory authority.

In the specific field of data protection, as indicated above, risk-based approximation is not a novelty, since it was already incorporated in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals

1. LLANEZA GONZÁLEZ, P., "Nuevo marco de cumplimiento en las obligaciones de protección de datos: la gestión de la privacidad desde la mitigación del riesgo", *Revista de Privacidad y Derecho Digital*, nº 4, 2016, p. 146.

2. Official Journal of the European Union L 119/1 of 04 May 2016.

IUS ET SCIENTIA • 2020
Vol. 6 • Nº 2 • pp. 42 - 53
ISSN 2444-8478 • https://dx.doi.org/10.12795/IETSCIENTIA.2020.i02.04

with regard to the processing of personal data and on the free movement of such data[3], which highlights the importance of this concept, to the extent that it now constitutes a core element of the principle of proactive liability. In this sense, the risk-based approach is interconnected with other principles, such as the principle of privacy by design and by default, and with obligations that fall on the controller, such as that which establishes the duty to draw up and keep a register of processing activities. However, we can affirm that the concept of a risk-based approach takes on its highest expression in the new regulation on data protection.

In an international context, this recognition also takes place in international instruments on data protection. More specifically, the revised and updated version of the OCDE Guidelines on privacy protection and transborder flows of personal data of 2013 specifically incorporates risk assessment among the principles of application, referring specifically to its relevance in the development of policies and safeguards to ensure privacy. This risk assessment is one of the essential pillars for the development of appropriate safeguards that are the subject of privacy management programmes, so that the impact assessment is the measure that will make it possible, where appropriate, to identify, analyze and evaluate the risk.

II. LEGAL-TECHNICAL ECOMMENDATIONS FOR DISTANCE WORKING ARRANGEMENTS

The emergence of the current emergency health crisis resulting from COVID-19 has, among other things, restricted the freedom of movement of natural persons. This has had an immediate effect in the professional field, as has been the decision, on the part of organisations, that all or part of the activities carried out should be carried out in teleworking situations, having, given the urgency of the situation, implemented them on a provisional basis and without prior planning[4].

In these cases, it is essential, in parallel with the implementation of this modality of work, to reflect on the resilience of the organisation to the adaptation and continuity of the business processes. All this while maintaining the rights and freedoms of the interested parties.

For this reason, the controller and the personnel involved in the processing must take into consideration the following basic technical recommendations[5]:

3. Official Journal of the European Communities L 281/31 of 23 November 1995.

4. BENTLEY, "Knowledge work and telework: an exploratory study", *Internet research: electronic networking applications and policy*, Nº 4, 2000, PP. 346-356.

5. SPANISH DATA PROTECTION AGENCY, Recommendations to protect personal data in mobility and teleworking situations, 2020.

IUS ET SCIENTIA • 2020
Vol. 6 • Nº 2 • pp. 42 - 53
ISSN 2444-8478 • https://dx.doi.org/10.12795/IETSCIENTIA.2020.i02.04

1. List of specific measures to promote information security within organisations

From the moment the controller chooses to adapt his business purpose to this form of teleworking, he must implement at least the following controls:

A) Development of a policy for the formal determination of guidelines

This general policy must include, as an integral part, a specific policy that regulates mobility in situations, such as this one, that are certainly exceptional and that establishes the specific needs and the unique risks that arise from the access that will have to be produced to the organisation's resources from areas that are beyond its control. These specific needs should include the types of remote access allowed, the devices that can be used for each type and the level of access allowed depending on the mobility profile defined.

In addition to the above, it is also necessary to prepare and send to the people affected the functional guides that have been adapted to train them, which are derived from these policies and which must include, as a minimum, the recommendations addressed to employees who specifically participate in personal data processing operations, which must also respect the other rules and procedures that develop them, especially with regard to the duty of confidentiality in relation to the personal data to which they have access in the performance of their work duties.

With regard to the specific threats that may arise from the performance of professional activity in the form of teleworking, it will be necessary for the organisation's employees to be informed of these and the main effects that may occur if the guidelines transmitted by the organisation are not complied with. To this end, it is necessary that, for the purposes of testing, each employee signs a teleworking agreement that includes the commitments acquired by carrying out their tasks under this modality[6]. In this respect, it is also advisable to have and communicate a contact point and the corresponding channels and formats through which any person can communicate any incident of which they are aware and which affects the personal data of the interested party.

B) Third-party service providers with access to corporate information: conditions

In order to comply with this measure, it will be necessary to use teleworking applications and solutions that provide adequate guarantees and that avoid the exposure of the personal information of the data subjects and corporate services of the controller, in particular with regard to e-mail and messaging services.

6. ARAÚJO, S. A./FRANCA, F. S./CAVALCANTE, G. F../MEDEIROS, J. W., "Teletrabalho (Telework)", *Informação em pauta*, nº 2, 2019, pp. 132-151.

IUS ET SCIENTIA • 2020
Vol. 6 • Nº 2 • pp. 42 - 53
ISSN 2444-8478 • https://dx.doi.org/10.12795/IETSCIENTIA.2020.i02.04

In addition to the above, and thanks to the principle of proactive responsibility that must permanently govern the actions of the controller, the latter may only use service providers that offer sufficient guarantees to apply appropriate technical and organisational measures (Article 28.1 GDPR) before proceeding to the necessary conclusion of the contract or equivalent legal act that describes the object, duration, nature and purpose of the processing, the type of personal data and categories of data subjects, and the obligations and rights of the controller. They must therefore provide secure solutions which, among other things, avoid the disclosure of the data subject's personal data and confidential information of the organisation processed by the processor.

The GDPR addresses the definition of the processor in its Article 4(8), which provides, literally, that the processor is the natural or legal person, public authority, service or other body that processes personal data on behalf of the controller.

As we can see, the definition of a treatment provider consists of three essential aspects[7]:

Firstly, an allegedly broad subjective component, comprising both legal subjects with their own legal personality and entities or bodies lacking that status, whether public or private in nature.

Secondly, an objective component, which refers to the processing of personal data per se.

Thirdly, an extra component, perhaps the most important and decisive, which outlines the figure of the processor and distinguishes him from other subjects who are also included in the data protection legislation, such as the fact that he carries out processing of personal data on behalf of the controller.

C) Policies for controlled and restricted access to information belonging to the organisation

In this case, the profiles or levels of access to the information and, more specifically, to the personal data, must be configured in such a way that it takes into account the role of each employee. It is also logical that this configuration should be more restrictive when the work is carried out from an external network, as is the case with teleworking[8].

Similarly, the organisation will have to implement complementary access limitations depending on the type of device (secure corporate laptops, external personal equipment and mobile devices, such as smartphones or tablets) through which access to personal data is produced and the place from which such access is produced.

7. POVEDANO ALONSO, D., "Responsabilidad activa en la protección de datos: el responsable y el encargado del tratamiento en el ámbito local", CAMPOS ACUÑA, M. C. (Dir.), *Aplicación práctica y adaptación de la protección de datos en el ámbito local: novedades tras el RGPD y la LOPDGDD*, Madrid, Wolters Kluwer, p. 359.

8. PASCALE PETERS, P. E./LIGHTHART, E. A./ANNE BARDOEL, E. P., "'Fit' for telework'? Cross-cultural variance and task-control explanations in organizations' formal telework practices", *The International Journal of Human Resource Management*, nº 21, 2016, p. 2587.

IUS ET SCIENTIA • 2020
Vol. 6 • Nº 2 • pp. 42 - 53
ISSN 2444-8478 • https://dx.doi.org/10.12795/IETSCIENTIA.2020.i02.04

D) Periodic review of equipment and devices used to process information

The servers through which the information is remotely accessed will have to be regularly reviewed and properly updated and configured in order to ensure the satisfaction of the data protection and information security policy in a teleworking context. The access profiles that have been defined will also have to be controlled.

Specifically, the organisation's equipment used as clients will have to be updated at application and operating system level, have services that are not necessary disabled, have a default configuration of minimum privileges defined by the ICT services that cannot be deactivated or modified by the employee, install only the applications authorised by the organisation, have updated antivirus software, have a local firewall activated, have only communications activated (WiFi, bluetooth, etc.)) and ports (USB or others) necessary to carry out the tasks assigned and incorporate information encryption mechanisms.

In the event that the use of employees' personal devices is allowed and authorised, taking into account the greater risk involved (derived from the fact that they do not have the same controls as corporate devices), it will be necessary to implement additional guarantees[9]. In particular, in addition to requiring minimum requirements for the use of remote connections (for example, having an original and updated operating system and software), the organisation will have to analyse the possibility of restricting the connection to a segregated network that only allows restricted access to those resources that have been identified as less critical and subject to a lower level of risk.

E) Control of telematic access to corporate information from places outside the organisation's facilities

It seems obvious that, in order to secure access from outside the organisation by employees, monitoring will be essential for the identification of abnormal patterns of behaviour in network traffic carried in the context of the remote access solution to prevent the spread of malicious programs over the corporate network and the unauthorised access to and use of resources.

To this end, as we will see, security breaches of personal data must be notified to the supervisory authority and, in addition, in certain cases, communicated to the data subjects (Articles 33 and 34 GDPR) to ensure a resilient teleworking environment. This should be preceded by the communication to employees, within the framework of the data protection and information security policy, of the existence and scope of these actions aimed at monitoring their remote activity[10]; nevertheless, if the control and supervision actions by the controller extend to the verification of the fulfilment

9. DE LAS HERAS GARCÍA, A., "Relaciones colectivas y teletrabajo", *Revista internacional y comparada de relaciones laborales y Derecho del empleo*, nº 2, 2017, pp. 32-33.

10. SALA FRANCO, T., El teletrabajo, Valencia, Tirant lo Blanch, 2020.

IUS ET SCIENTIA • 2020
Vol. 6 • Nº 2 • pp. 42 - 53
ISSN 2444-8478 • https://dx.doi.org/10.12795/IETSCIENTIA.2020.i02.04

of the employees' labour obligations, he must provide timely and prior information, and must do so in a clear, express and concise manner, This proactive activity is included in the measures adopted in the context of the control functions envisaged and the respect for digital rights provided for in the LOPDGDD (in particular, the right to privacy and the use of digital devices and the right to digital disconnection in the workplace - Article 87), exercised within its legal framework and with the limits inherent therein.

F) Regular monitoring of the technical and legal measures implemented to manage risk

The determination of the risk involved in the processing of personal data by telematic means, i.e. in the teleworking modality, requires the prior performance of a risk analysis in which it is established in what proportion the advantages derived from remote access compensate for the threats resulting from access to personal data of data subjects from outside the organisation. Consequently, the information that employees can access will have to be limited by the risk of losing the devices that allow such access and the exposure or unauthorised access to the information handled.

In addition, within the policy defined by the organisation, internal procedures must be contemplated that allow the provision and auditing of remote access client devices, the procedures for the administration and monitoring of the infrastructure, the services provided by those responsible for the processing and the way in which this policy will be reviewed and updated to be able to adapt to the risks existing at any given time.

G) Reliable use of computer systems and devices used for access to corporate information

Employees who, through the corporate devices of the organisation acting as controller, access personal information of the data subjects, will have to configure and use robust access passwords different from those used for access to personal e-mail accounts, social networks or any other type of applications used in the scope of their personal life[11].

In addition, it is forbidden to download or install applications or software that have not been previously authorised by the person responsible for the processing, and it is recommended by the organisation that connections of devices to the organisation's network produced in public places or through open WiFi networks that are not secure should be avoided.

It will also be essential to maintain previously defined authentication mechanisms (certificates, passwords, tokens, two-factor systems, etc.) that serve to validate the organisation's remote information access control systems. Likewise, if employees have corporate devices,

11. DE LA VILLA GIL, E., "Trabajo a distancia", GOERLICH PESET, J. M. (Coord.), *Comentarios al Estatuto de los Trabajadores: Libro homenaje a Tomás Sala Franco*, Valencia, Tirant lo Blanch, 2016, p. 307.

IUS ET SCIENTIA • 2020
Vol. 6 • N° 2 • pp. 42 - 53
ISSN 2444-8478 • https://dx.doi.org/10.12795/IETSCIENTIA.2020.i02.04

these should not be used for personal purposes, in order to avoid access to social networks, personal e-mail, web pages with complaints and shocking advertising, as well as other sites that may contain viruses or favour the execution of harmful code; on the other hand, if the devices used for remote access belong to the employee himself, it will be necessary to avoid simultaneous development of personal activities and professional tasks, also defining separate and independent profiles for the development of each one of them[12].

Furthermore, anti-virus systems must be installed that are operational and up-to-date, and we must verify that the e-mails received are legitimate by checking that the electronic domain from which they come is valid and known, and by rejecting the downloading of attachments with unusual extensions or the establishment of connections through links included in the body of the e-mail that show any unusual pattern. In addition, in the event that WiFi, bluetooth or similar connections are managed by the employee himself, he must deactivate them when they are not being used and must, as soon as the working day ends, disconnect the remote access session and turn off or block access to the device.

H) Integrity and confidentiality of information as fundamental principles regarding processing

Where teleworking is taking place, appropriate precautions will need to be taken to ensure that the information being accessed is kept confidential.

When working with documents in physical format, it will be necessary to reduce their entry and exit to a minimum, providing extreme safeguards to prevent unauthorised access by third parties, and to avoid discarding them without being sure that they are properly destroyed. In addition, we should prohibit the throwing of whole or chunky papers into hotel bins, public places or household waste where someone could access and retrieve personal information.

We may also not leave information visible in public places and we must block devices used when not in use. More specifically, we will have to prevent the screen from being exposed to the gaze of unauthorised third parties and use a privacy filter for it, and it is advisable to ensure that nobody can listen in on conversations by using headphones or using spaces where the employee concerned is not accompanied.

I) Adequate storage of data in appropriate places provided by the specific company

The local storage of the personal information of the data subjects must be prohibited, and it must be stored in shared spaces, or in the cloud, provided by the controller. In

12. SIERRA BENÍTEZ, E. M., "El derecho del trabajo en el nuevo trabajo a distancia", GARRIDO PÉREZ, E. (Coord.), *Constitución Española y relaciones laborales ante el actual escenario social y económico. Comunicaciones (en CD-ROM): XXXI Jornadas universitarias andaluzas de Derecho del trabajo y relaciones laborales*, 2013, pp. 153-154.

IUS ET SCIENTIA • 2020
Vol. 6 • Nº 2 • pp. 42 - 53
ISSN 2444-8478 • https://dx.doi.org/10.12795/IETSCIENTIA.2020.i02.04

this respect, if the devices used are personal[13], no applications may be used that are not authorised in the entity's policy for sharing information.

It will also be essential to prevent compliance with the corporate backup policy defined for each device by the organisation, in addition to periodically reviewing and deleting any residual information that may be stored on the device, such as temporary files from the browser or downloads of the documents.

J) Effective and efficient management of security breaches on the basis of guidelines drawn up and communicated in advance

Finally, if the employee working remotely detects any irregularities that may compromise the security of the personal data of the data subjects, he or she must notify the organisation, without undue delay and in the shortest possible time. This notification shall be made through the channels created for this purpose by the controller, who shall then inform the data protection officer and the security officer, sending them all the information of which he has the knowledge.

2. Corporate attacks from third parties outside the organization in distance work situations: regulation and procedure

A) Detection of the incident and bringing it to the attention of the competent authority

Article 33 GDPR provides that, in the event of a security breach, the controller will have the duty to notify it to the competent supervisory authority, pursuant to that established in Article 55 GDPR[14]. And he shall do so without undue delay, specifically, within seventy-two hours following knowledge of the same; if it is not made within the period described, the reasons that prevented it must be accompanied, stating them in a reasoned manner[15].

However, this notification obligation is not necessary if it is unlikely that such a security incident would pose a risk to the rights and freedoms of the data subjects.

As to the content of the notification, it must be made:

13. MAHFOOD, P. E., Trabajo a distancia: selección, dirección y control de trabajadores a distancia, Barcelona, Ed. Ediciones S., 1995.

14. LLANEZA GONZÁLEZ, P., "Nuevo marco de cumplimiento en las obligaciones de protección de datos: la gestión de la privacidad desde la mitigación del riesgo", *op. cit.*, p. 147.

15. LÓPEZ BALAGUER, M., "Artículo 13. Trabajo a distancia", CRUZ VILLALÓN, J./GARCÍA-PERROTE ESCARTÍN, I./GOERCLICH PESET, J. M./MERCADER UGUINA, J. R. (Dirs.), *Comentarios al Estatuto de los Trabajadores*, Valladolid, Lex Nova, 2016, pp. 208-209.

IUS ET SCIENTIA • 2020
Vol. 6 • Nº 2 • pp. 42 - 53
ISSN 2444-8478 • https://dx.doi.org/10.12795/IETSCIENTIA.2020.i02.04

> "(a) describe the nature of the personal data security breach, including, where possible, the categories and approximate number of data subjects concerned, and the categories and approximate number of records of personal data concerned;
>
> (b) communicate the name and contact details of the data protection officer or other contact point where further information can be obtained;
>
> (c) describe the possible consequences of a breach of the security of personal data;
>
> (d) describe the measures adopted or proposed by the controller to remedy the breach of the security of personal data, including, if appropriate, the measures taken to mitigate any negative effects.

In addition to the above, the controller must document any breach of data security, including the facts related to it, the impact it has had and the corrective measures, of whatever nature, implemented. This documentation will enable the supervisory authority to verify the satisfaction of such regulatory requirements.

The processor will also be required to notify, in this case to the corresponding controller, any breach of security of personal data (that is, any incident affecting the integrity, confidentiality and availability of the data subject's personal information) of which he becomes aware, as soon as he becomes aware.

B) Exceptional cases of communication of incidents to the natural persons concerned

In addition to the above, Article 34 GDPR provides that, when there is a probability that the security breach involves and determines a high risk to the rights and freedoms of data subjects, the controller must make a communication to the holders of the personal data concerned, and must do so without undue delay. This communication must consist of a description, in clear and simple language, of the nature of the security breach and must include at least the information described in points (b), (c) and (d) of the immediately preceding provision.[16]

However, this communication to the data subject will cease to be obligatory (it is otherwise convenient thanks to the principle of proactive responsibility that configures the new regulation on data protection) when any of the following conditions occur:

> "(a) the controller has adopted appropriate technical and organisational protection measures and these measures have been applied to the personal data affected by the breach of the security of the personal data, in particular those which render the personal data unintelligible to any person not authorised to access them, such as encryption;
>
> (b) the controller has taken further steps to ensure that the high risk to the rights and freedoms of the data subject referred to in paragraph 1 is no longer likely to materialise;
>
> (c) it involves a disproportionate effort. In this case, a public communication or similar measure informing the data subjects in an equally effective manner shall be chosen instead'.

16. CABEZA PEREIRO, J., "Trabajo a distancia y relaciones colectivas", MELLA MÉNDEZ, L. (Dir.), *El teletrabajo en España: aspectos teórico-prácticos de interés*, Madrid, Wolters Kluwer, 2017, pp. 179-214; POVEDANO ALONSO, D., "Responsabilidad activa en la protección de datos: el responsable y el encargado del tratamiento en el ámbito local", *op. cit.*, p. 361.

IUS ET SCIENTIA • 2020
Vol. 6 • Nº 2 • pp. 42 - 53
ISSN 2444-8478 • https://dx.doi.org/10.12795/IETSCIENTIA.2020.i02.04

Furthermore, in the event that the controller has not yet communicated the security breach to the data subject, the supervisory authority shall have the possibility, taking into account the likelihood that the breach represents a high risk to the rights and freedoms of the data subject, to compel him to do so or, where appropriate, to decide that one of the above conditions is fulfilled.

Finally, the ninth additional provision LOPDGDD refers to the processing of personal data with respect to the notification of security incidents, providing the following:

> "Where, in accordance with the provisions of the applicable national legislation, security incidents must be notified, the competent public authorities, computer emergency response teams (CERTs), computer security incident response teams (CSIRTs), providers of electronic communications networks and services and providers of security technologies and services may process the personal data contained in such notifications only for the time and to the extent necessary for their analysis, detection, protection and response to incidents and by adopting appropriate security measures proportionate to the level of risk identified".

III. CONCLUDING REMARKS

This article focuses on the new developments in the field of distance work and teleworking, which have been encouraged or, rather, accelerated by the global health crisis resulting from the COVID-19 crisis.

With the legal regulation of this new modality for the development of professional activity, the need arises to protect the information, personal and/or confidential, treated by employees in their work place, far from the traditional physical business location. For this reason, and in order to protect, above all and very especially, the fundamental right of the data subjects to the protection of their fundamental rights, more specifically, the principle of integrity and confidentiality which forms one of the principles relating to processing, this article arises, which proposes a series of basic and necessary security measures to achieve this objective.

In this respect, a series of obligations are established which affect both the organisation or employer, in its capacity as controller, and the employee. In addition, many of them will be provisional, while others may be consolidated if this new form of work is consolidated once the pandemic that has brought so many effects in all areas, hopefully soon, has passed.

BIBLIOGRAPHY

ARAÚJO, S. A./FRANCA, F. S./CAVALCANTE, G. F../MEDEIROS, J. W., "Teletrabalho (Telework)", *informação em pauta*, nº 2, 2019, pp. 132-151.

BENTLEY, "Knowledge work and telework: an exploratory study", *Internet research: electronic networking applications and policy*, Nº 4, 2000, PP. 346-356.

CABEZA PEREIRO, J., "Trabajo a distancia y relaciones colectivas", MELLA MÉNDEZ, L. (Dir.), *El teletrabajo en España: aspectos teórico-prácticos de interés*, Madrid, Wolters Kluwer, 2017, pp. 179-214

IUS ET SCIENTIA • 2020
Vol. 6 • Nº 2 • pp. 42 - 53
ISSN 2444-8478 • https://dx.doi.org/10.12795/IETSCIENTIA.2020.i02.04

DE LA VILLA GIL, E., "Trabajo a distancia", GOERLICH PESET, J. M. (Coord.), *Comentarios al Estatuto de los Trabajadores: Libro homenaje a Tomás Sala Franco*, Valencia, Tirant lo Blanch, 2016, p. 307.

DE LAS HERAS GARCÍA, A., "Relaciones colectivas y teletrabajo", *Revista internacional y comparada de relaciones laborales y Derecho del empleo*, nº 2, 2017, pp. 32-33.

LLANEZA GONZÁLEZ, P., "Nuevo marco de cumplimiento en las obligaciones de protección de datos: la gestión de la privacidad desde la mitigación del riesgo", *Revista de privacidad y Derecho digital*, nº 4, 2016, p. 146.

LÓPEZ BALAGUER, M., "Artículo 13. Trabajo a distancia", CRUZ VILLALÓN, J./GARCÍA-PERROTE ESCARTÍN, I./GOERCLICH PESET, J. M./MERCADER UGUINA, J. R. (Dirs.), *Comentarios al Estatuto de los Trabajadores*, Valladolid, Lex Nova, 2016, pp. 208-209.

MAHFOOD, P. E., Trabajo a distancia: selección, dirección y control de trabajadores a distancia, Barcelona, Ed. Ediciones S., 1995.

PASCALE PETERS, P. E./LIGHTHART, E. A./ANNE BARDOEL, E. P., "'Fit' for telework'? Cross-cultural variance and task-control explanations in organizations' formal telework practices", *The International Journal of human resource management*, nº 21, 2016, pp. 2582-2603.

POVEDANO ALONSO, D., "Responsabilidad activa en la protección de datos: el responsable y el encargado del tratamiento en el ámbito local", CAMPOS ACUÑA, M. C. (Dir.), *Aplicación práctica y adaptación de la protección de datos en el ámbito local: novedades tras el RGPD y la LOPDGDD*, Madrid, Wolters Kluwer, p. 359.

SALA FRANCO, T., El teletrabajo, Valencia, Tirant lo Blanch, 2020.

SIERRA BENÍTEZ, E. M., "El derecho del trabajo en el nuevo trabajo a distancia", GARRIDO PÉREZ, E. (Coord.), *Constitución Española y relaciones laborales ante el actual escenario social y económico. Comunicaciones (en cd-rom): xxxi jornadas universitarias andaluzas de derecho del trabajo y relaciones laborales*, 2013, pp. 153-154.

SPANISH DATA PROTECTION AGENCY, *Recommendations to protect personal data in mobility and teleworking situations*, 2020.

IUS ET SCIENTIA • 2020
Vol. 6 • Nº 2 • pp. 42 - 53
ISSN 2444-8478 • https://dx.doi.org/10.12795/IETSCIENTIA.2020.i02.04