IUS ET SCIENTIA
2021 • Vol. 7 • Nº 1• ISSN 2444-8478
https://editorial.us.es/es/revistas/ius-et-scientia
https://dx.doi.org/10.12795/IETSCIENTIA • © Editorial Universidad de Sevilla 2021

Personal data in artificial intelligence projects: main study elements

DATOS PERSONALES INSERTOS EN PROYECTOS DE INTELIGENCIA ARTIFICIAL: ELEMENTOS PRINCIPALES DE ESTUDIO

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

Recibido: 26 de marzo 2021 | Aceptado: 08 de mayo 2021

ABSTRACT

This research focuses on the impact of the new regulations on the protection of personal data in the scientific field of computer science, which is centered on the creation of programs and mechanisms that can display behaviors considered intelligent. In other words, the necessary respect for the fundamental right to data protection in those technological advances that, progressively, make machines think like human beings, determining what are the possible legal bases that can be found to legitimize all processing of personal data that occur in this new field.

KEYWORDS

General data protection regulation
AI
Personal data
Data processing
LOPDGDD.

RESUMEN

La presente investigación pivota en torno a la la incidencia que tiene la novedosa normativa en materia de protección de datos personales en el campo científico de la informática que se centra en la creación de programas y mecanismos que pueden mostrar comportamientos considerados inteligentes. En otras palabras, el necesario respecto del derecho fundamental a la protección de datos en aquellos avances tecnológicos que, de forma progresiva, consiguen que las máquinas piensen como seres humanos, determinando cuáles son las posibles bases jurídicas que pueden concurrir para legitimar todo tratamiento de datos personales que se produzcan en este novedoso campo.

PALABRAS CLAVE

Reglamento general de protección de datos
IA
Dato personal
Tratamiento
LOPDGDD.

I. Subject matter

It can be said that the principles relating to processing are made up of various rules that stipulate how personal data should be collected, processed and transferred, with the aim of guaranteeing all the fundamental rights of the data subjects. Specifically, in the case of the protection of personal data, these principles go beyond mere fundamentals, since they are of a normative nature and will bring together all the interpretations of this legislation on the protection of personal data, directly replacing the many legal loopholes that may occur in the regulation itself as a result of the unstoppable evolution of technology, which, in many cases, renders useless the attempts of the legislator in his task of regulatory prevention (García, 2018).

Therefore, such principles enjoy in the new 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 (hereinafter, General Data Protection Regulation or GDPR) and in the new Organic Law 3/2018 of December 5, 2018, on the Protection of Personal Data and Guarantee of Digital Rights (hereinafter, LOPDGDD), of particular relevance and transcendence, due to the fundamental character they possess as informers to the institutions that harmonize the legal system on data protection matters serving, at the same time, as a reference to the legal operators involved in the matter so that they can satisfactorily comply with the legal and corporate social responsibility implications linked to the new demands and requirements arising from the protection of personal data.

Some authors (Aldudo, 2018) qualify these principles (especially the principle of lawfulness, fairness and transparency, which is of interest to us here) as obligations for data controllers. However, it is of greater significance, as it affects not only the data controller, but also any natural or legal person involved in the application of personal data, which serves as a normative and interpretative guideline for all legal bodies that manage personal information.

II. Basic reasoning

Article 6 GDPR is dedicated to the lawfulness of processing. In order for such processing (in this case, those arising from the processing of personal data in the scientific field of computer science that focuses on the creation of programs and mechanisms that can display behaviors considered intelligent) to be lawful, the personal data must be handled with the consent of the data subject or covered by a certain legitimacy established by law, either in this Regulation or under the Union law of the Member States to which this Regulation refers, including logically the need to comply with the controller's legal obligation or the need to perform a contract to which the data subject is a party or, where appropriate, to take steps at the request of the data subject prior to the conclusion of a contract (vid. Recital 40 RGPD) (Oroz, 2018).

IUS ET SCIENTIA • 2021
Vol. 7 • Nº 1 • pp. 37 - 47
ISSN 2444-8478 • https://dx.doi.org/10.12795/IETSCIENTIA.2021.i01.04

Specifically, the conditions for such lawfulness condition to be effectively and correctly fulfilled are set out below:

a) whether the data subject has consented to the processing of his or her personal data for one or more specific purposes [Article 6(1)(a) GDPR]. By consent, obviously, it can be interpreted that the processing will be lawful. However, in accordance with the provisions of the Spanish Data Protection Agency, consent can only be used as a legal basis for processing when none of the above legal bases are previously possible.

Moreover, this consent is defined by Article 4(11) of the GDPR as any freely given, specific, informed and unambiguous indication of the data subject's consent to the processing of personal data concerning him or her, either by a statement or by a clear affirmative action. Under this definition, Article 7 GDPR sets out the conditions that must be met in order to properly obtain consent, conditions which establish, in summary, that consent must be obtained:

Separately: consent must be obtained separately from the rest of the terms and conditions.

Unequivocal and affirmative: it will require active behavior, which will exclude unchecked "I do not agree" boxes and pre-checked boxes authorizing processing.

Granular, i.e., vertebrate, where appropriate, between the different treatments.

Nominative. It will be necessary to identify the responsible organization, as well as the third party assignees of the data. However, the Spanish Data Protection Agency, in its own Guide on the duty of information, continues to admit the generic reference to assignees by categories.

Demonstrable, documented: it is necessary to be able to prove a posteriori who consented, when and how he/she did so and what he/she was informed of.

Revocable: it will be just as easy to give consent as to revoke it.

Specifically, consent must be explicit in order to legitimize:

The processing of special categories of data (the most sensitive data, such as ideology, sexual orientation, ethnicity, health data, biometric data, etc.).

The adoption of automated decisions, profiling.

Transfers of personal data to third countries or international organizations.

The processing of personal data whose use has been previously restricted.

Uses related to direct marketing by electronic means.

In any case, if the legal basis for the processing is consent, the affected personal data subjects will have additional rights, such as the right to be forgotten (articles 17 RGPD and 15 LOPDGDD) and the right to data portability (articles 20 RGPD and 17 LOPDGDD).

Consent implies control, freedom on the part of the holder. If the data subject is not really free to choose or if the provision of the service requires (without further possibilities) consent for a processing not related to that service, this consent is neither free nor valid.

IUS ET SCIENTIA • 2021
Vol. 7 • Nº 1 • pp. 37 - 47
ISSN 2444-8478 • https://dx.doi.org/10.12795/IETSCIENTIA.2021.i01.04

The new personal data protection regulations have introduced the concept of accountability or proactive responsibility. Consequently, it is no longer enough not to breach the regulations; now, we need to demonstrate that we have studied our problems, our risks, the measures available to mitigate those risks, we have chosen and implemented the ones we consider most appropriate and why.

Along the same lines, it is not enough to obtain unequivocal (and, when necessary, express) consent. It must be documented in order to be able to prove it to the user and the Administration. It will be necessary to document, at least, the following points:

Who consented: the data owner must be identified by name or other identifier, depending on the case.

When consent was given: in the case of offline consent, a copy of the signed and dated document is required; in the case of online consent, a time-stamped file.

What information the individual received: copy of the signed data capture document, linked to the privacy policy, and other legal notices in effect at the time. Recording of the verbal consent, as well as the information provided to the data subject.

How consent was given: in writing, with a copy of the aforementioned documents: online: copy of the data provided and of the data capture form with its time stamp; verbally: recording.

Whether or not consent has been revoked and, if so, when.

Otherwise, consent is an obvious instrument or manifestation of the holder's control over his data. But that which is given forever, has escaped one's control. This brings us to the following question: how long does the validity of consent last?

Well, the duration, the life of the consent depends on its object (of the authorized processing), as well as on the context, the circumstances in which it has been given (the who, how, when and in the face of what information). A very interesting example is the consent given by parents or guardians, on behalf of the minor (for example, for the processing of their data, in a social network for minors). It is obvious that this consent will lose its validity when the minor reaches the age of majority and acquires the capacity to decide for himself/herself. At this point, it will be necessary to renew that consent, or rather, to obtain it directly from the minor.

On this issue of consent, Article 6 of the new LOPDGDD states that:

1. *In accordance with the provisions of Article 4.11 of Regulation (EU) 2016/679, consent of the data subject means any freely given, specific, informed and unambiguous expression of will by which the data subject agrees, either by a statement or a clear affirmative action, to the processing of personal data concerning him or her.*

IUS ET SCIENTIA • 2021
Vol. 7 • N° 1 • pp. 37 - 47
ISSN 2444-8478 • https://dx.doi.org/10.12795/IETSCIENTIA.2021.i01.04

2. *Where the processing of data is intended to be based on the consent of the data subject for a plurality of purposes, it shall be necessary for it to be specifically and unequivocally stated that such consent is given for all of them.*
3. *The execution of the contract shall not be subject to the condition that the data subject consents to the processing of personal data for purposes unrelated to the maintenance, development or control of the contractual relationship.*

b) Related to this last paragraph of Article 6 LOPDGDD, the processing must be necessary for the performance of a contract to which the data subject is a party or, where appropriate, for the application, at his request, of measures of a pre-contractual nature [Article 6.1.b) RGPD]. The very existence of a relationship of a contractual nature, or the preliminary dealings thereof, would also justify the lawfulness of the processing (Heras, 2018).

c) When the processing is justified as a result of the provisions of a regulation having the force of law [article 6.1.c) RGPD]. In this regard, Article 8.1 LOPDGDD adds that the processing of personal data may only be considered justified in order to comply with a legal obligation that the data controller is required to comply with, in the terms provided for in Article 6.1. c) GDPR, when so provided by a rule of Community law or a rule having the force of law, which may determine the general conditions of the processing and the types of data processed, as well as the transfers that may take place as a result of compliance with the legal obligation; such rule, it adds, may also impose special conditions on the processing, such as the adoption of additional security measures or other measures established in Chapter IV of the General Data Protection Regulation.

d) The need to protect the vital interests of the data subject or of another natural person [Article 6.1.d) GDPR], also justifies such lawfulness.

e) When the processing is necessary for the performance of a task carried out in the public interest or in the exercise of public authority vested in the controller [article 6.1.e) RGPD], although, in these cases, the existence of an enabling rule providing both the public interest of such a task and the exercise of the public authority of such a function is necessary.

The second paragraph of Article 8 LOPDGDD establishes in this regard that the processing of personal data may only be considered to be based on the fulfillment of a mission carried out in the public interest or in the exercise of public powers conferred on the data controller, in the terms provided in Article 6.1 e) RGPD, when it derives from a competence conferred by a rule having the force of law.

For its part, the twelfth Additional Provision LOPDGDD regulates the specific provisions applicable to the processing of public sector personnel records, establishing that the processing of public sector personnel records shall be understood to be carried out in the exercise of public powers conferred on the data controller, in accordance with the provisions of Article 6.1.e) RGPD. To this, it adds that these registers may process personal data relating to criminal offenses and convictions and administrative offenses and sanctions, limited to the data strictly necessary for the fulfillment of their purposes (Rodríguez, 2020; Rodríguez, 2020).

IUS ET SCIENTIA • 2021
Vol. 7 • Nº 1 • pp. 37 - 47
ISSN 2444-8478 • https://dx.doi.org/10.12795/IETSCIENTIA.2021.i01.04

f) When the processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, provided that such interests are not overridden by the fundamental rights and freedoms of the data subject which require the protection of his or her personal data, in particular when the data subject is a child [Article 6.1.f) GDPR]. In the interpretation of this paragraph, the need always arises to specify the qualification of legitimate interest, an unspecified legal concept that must be refined in each case depending on the circumstances of both the data controller and the data subjects. It is very significant to highlight the special importance that the section attaches to the protection of the right to data protection of minors.

With regard to this last paragraph, there is an express mention in the Regulation that excludes from its applicability the processing carried out by public authorities in the exercise of the functions legally entrusted to them.

Legitimate interest is now particularly important for companies that see how the databases they work with have an expiration date in many cases (May 2018). The processing of these databases is based on consents given by their holders in the past; these consents, which were correct when they were obtained, have to meet the new requirements imposed by the personal data protection regulations in order to remain correct.

As already mentioned, the new GDPR and the new LOPDGDD require consent to be unambiguous, specific or separate and, in the most relevant cases, explicit. Consents given yesterday that do not meet today's requirements will not be valid tomorrow.

This is a delicate and controversial situation, especially for companies with few resources. The two-year transitional period prior to the implementation of the GDPR was considered sufficient by Brussels for organizations to refresh or renew their consents, or to seek new grounds for legitimizing their processing, such as legitimate interest.

Companies are faced with the choice of either relying on another of the above-mentioned legitimate grounds or repeating the whole process of obtaining consent again. This is the same as starting all over again. And this second path has disadvantages, derived, in particular, from the possibility that the person concerned, more informed every day, is more selective today than yesterday when it comes to giving his consent and does not give it. In addition, the recruitment procedure must also be in accordance with the new regulation.

In this sense, legitimate interest as a basis for processing is neither new nor extraordinary. It is regulated in the new regulation on personal data protection, of course, but it was already present in the previous one. A priori, the fact that someone can process your data without your consent, because they have a legitimate interest in doing so, is something that, just like that, is quite scary. However, this does not necessarily have to be the case; in fact, we have very clear examples that make this clear:

IUS ET SCIENTIA • 2021
Vol. 7 • N° 1 • pp. 37 - 47
ISSN 2444-8478 • https://dx.doi.org/10.12795/IETSCIENTIA.2021.i01.04

Among these examples is the one relating to the employer's power of control. In this case, it is not the employee's consent (expressed in his employment contract, or captured separately) that legitimizes the supervision or control by the company of the use made by its employees of their cell phones, computers or company vehicles; this control is based rather on the company's power of control provided for by law, in the Workers' Statute and in the interests of the company that exceed what an employment contract, on its own, can authorize.

It should be remembered here that the employee's consent (obtained during the term of the employment relationship) is problematic: its validity is under particular suspicion, given the weak bargaining position vis-à-vis his superior.

Another example would be that relating to video surveillance. In a variation of the above, the obvious interests of the company in protecting itself against fraud or unlawful actions explain why the latest case law (and, with it, the new LOPDGDD) allows video surveillance of workers even without their consent or specific information (due to the obvious legitimate interest of the company in protecting its assets).

Beyond the above, it is clear that the legitimate interest is always a relative authorization, subject to conditions, depending on the circumstances, which must be weighed on a case-by-case basis. The positive and negative aspects of the figure lie in this weighting judgment.

A third example would be the transfer of data that occurs when a party breaches a contract. The aggrieved party may transfer the data of the defaulting party to third parties (lawyers, collection companies) because it has a legitimate interest in the defaulting data subject's compliance. The consent in the contract does not usually include such a transfer of data to a lawyer.

The new LOPDGDD regulates a specific case in Article 19, relating to the processing of contact data of individual entrepreneurs and liberal professionals. It establishes the following:

1. *Unless there is evidence to the contrary, the processing of contact data and, where appropriate, data relating to the function or position held by natural persons providing services in a legal person shall be presumed to be covered by the provisions of Article 6.1 f) of Regulation (EU) 2016/679, provided that the following requirements are met:*
   a) *That the processing relates solely to data necessary for their professional location.*
   b) *That the purpose of the processing is solely to maintain relations of any kind with the legal person in which the data subject renders his services.*
2. *The same presumption shall operate for the processing of data relating to sole proprietors and liberal professionals, when it refers to them solely in that capacity and is not processed for the purpose of entering into a relationship with them as natural persons.*

IUS ET SCIENTIA • 2021
Vol. 7 • N° 1 • pp. 37 - 47
ISSN 2444-8478 • https://dx.doi.org/10.12795/IETSCIENTIA.2021.i01.04

3. *The data controllers or processors referred to in Article 77.1 of this Organic Law may also process the data referred to in the two preceding paragraphs when this arises from a legal obligation or is necessary for the exercise of their powers.*

III. Specially protected information

Articles 9 of the RGPD and 9 of the new LOPDGDD are dedicated to regulating the processing of special categories of personal data. In general, the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, the processing of genetic data, the processing of biometric data intended to uniquely identify a natural person and data relating to the health or sex life or sexual orientation of a natural person are prohibited. It is worth noting, due to the importance that this entails, the specific mentions made in relation to the regulation of genetic data and biometric data, aimed at univocally identifying a natural person (Garrós, 2018).

However, it establishes a series of exceptions to this general and prohibitive pronouncement on the processing of such data of a special nature. These are the following (article 9.2 RGPD):

a) Where the data subject has given his explicit consent to the processing of such personal data for one or more specific purposes, except where Union or Member State law providing that the provision is referred to in the first paragraph, cannot be lifted by the data subject. In this case, it is interpreted that, unless there is a legal unavailability in the terms referred to in this exception, the consent of the data subject himself may allow the processing of personal data, even if it corresponds to this special category of data (Sierra, 2019).

   For its part, article 9.1 of the new LOPDGDD, in development of this section, specifies that, in order to avoid discriminatory situations, the consent of the data subject alone will not be sufficient to lift the prohibition on the processing of data whose main purpose is to identify their ideology, trade union membership, religion, sexual orientation, beliefs or racial or ethnic origin. Consequently, when processing this type of special data, it will be necessary to have, in addition to consent or in the absence of consent, any other of the exceptions provided for in Article 9.2 GDPR and listed below; thus, continues Article 9.1 LOPDGDD, nothing shall prevent the processing of such data under the other cases referred to in Article 9.2 of the General Data Protection Regulation, where appropriate.

b) Where the processing is necessary for the performance of obligations and the exercise of specific rights of the controller or of the data subject in the field of labor law and social security and social protection, insofar as authorized by Union law of the Member States or by a collective agreement under the law of the Member States providing for appropriate safeguards for the respect of the fundamental rights and interests of the data subject.

IUS ET SCIENTIA • 2021
Vol. 7 • N° 1 • pp. 37 - 47
ISSN 2444-8478 • https://dx.doi.org/10.12795/IETSCIENTIA.2021.i01.04

c) When the processing is necessary to protect the vital interests of the data subject or of another natural person, in the event that the data subject is not physically or legally capable of giving his or her consent.
d) Where the processing is carried out, within the scope of its legitimate activities and with the appropriate safeguards, by a foundation, an association or any other non-profit-making body whose purpose is political, philosophical, religious or trade union, provided that the processing relates solely to current or former members of such bodies or to persons who maintain regular contact with them in connection with their purposes, and provided that the personal data are not disclosed to them without the consent of the data subjects.
e) Where the processing relates to personal data which the data subject has manifestly made public.
f) When the processing is necessary for the formulation, exercise or defense of claims, or when the courts act in the performance of their judicial function.
g) Where processing is necessary for reasons of essential public interest, on the basis of Union or Member State law, which must be proportionate to the aim pursued and, in addition, substantially respect the right to data protection and provide for specific appropriate measures to protect the interests and fundamental rights of the data subject.

Pursuant to Article 9.2 of the new LOPDGDD, the processing of data referred to in letters g), h) and i) of Article 9.2 RGPD based on Spanish law must be covered by a regulation having the force of law, which may establish additional requirements relating to its security and confidentiality. In particular, such regulation may cover the processing of data in the field of health when so required for the management of public and private health and social care systems and services, or for the performance of an insurance contract to which the data subject is a party.

h) Where the processing is necessary for the purposes of preventive or occupational medicine, assessment of the worker's capacity to work, medical diagnosis, provision of social health care or treatment or management of health and social care systems and services, on the basis of Union law of the Member States or pursuant to a contract with a health professional and without prejudice to the conditions and guarantees referred to in Article 9.3 RGPD (Davara, 2016).
i) Where processing is necessary for reasons of public interest in the field of public health, such as protection against serious cross-border threats to health or to ensure high standards of quality and safety of healthcare and of medicinal products or medical devices, on the basis of Union or Member State law providing for appropriate and specific measures to protect the rights and freedoms of the data subject, in particular professional secrecy; and,
j) where the processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, in accordance with Article 89(1) GDPR, on the basis of Union or Member State law, which must be proportionate to the aim pursued, respect in essence the right to data protec-

IUS ET SCIENTIA • 2021
Vol. 7 • N° 1 • pp. 37 - 47
ISSN 2444-8478 • https://dx.doi.org/10.12795/IETSCIENTIA.2021.i01.04

tion and provide for appropriate and specific measures to protect the interests and fundamental rights of the data subject.

The special categories of personal data referred to above, concludes article 9. 3 of the General Data Protection Regulation, may be processed for the purposes of preventive or occupational medicine, when such processing is carried out by or under the responsibility of an expert under a duty of professional secrecy, always in accordance with national law, with the regulations imposed by the internal authorities with competence in the matter or by any other subject who is also subject to this duty of secrecy, in accordance with national or community regulations or with the rules established by the internal authorities with competence in the matter (Díaz, 2018). Due to the novelty of the matter, and because of the ideological, religious, philosophical, cultural, legal and any other type of conditioning to which they may be subject, and, at the same time, because they are subject to continuous evolution and development, the possibility is expressly envisaged that the Member States of the European Union may maintain or specifically introduce additional conditions, including through the formulation of corresponding limitations in relation to the processing of genetic data, biometric data and data relating to health in general. The regulatory powers granted to the Member States therefore go in three very different directions: the maintenance of the conditions laid down in the regulations on the protection of personal data, the possibility of establishing additional conditions and, finally, the introduction of limitations to the aforementioned regulations.

Conclusions

Throughout this paper, we have been able to analyse in detail the legal justifications that allow the processing of personal data in the context of Artificial Intelligence projects.

Among them, special emphasis has been placed on consent, due to its regularity, determining not only what its essential features are in detail, but also what the main novelties are in comparison with previous regulations.

Similarly, we have studied the most important issues surrounding compliance with an obligation arising from a regulation with the status of law for the data controller or derived from compliance with obligations arising from a contractual relationship between the parties, both of which are also basic when we are talking about processing derived from this type of project.

In addition, we have tried to examine in depth the difficulty of justifying processing operations on the basis of legitimate interest, which always requires a weighting of interests that is far from simple. The public interest or vital interest are also less frequent, but equally in need of study.

Finally, we have dissected the elements that, in a complementary manner, must be present in order to be able to carry out processing of special categories of data, especially sensitive because they are more intrinsically linked to the privacy or intimacy of the data subjects as holders of the personal data to be processed.

IUS ET SCIENTIA • 2021
Vol. 7 • N° 1 • pp. 37 - 47
ISSN 2444-8478 • https://dx.doi.org/10.12795/IETSCIENTIA.2021.i01.04

Bibliography

Aldudo, P. (2018). Seguridad y protección de datos: el análisis de riesgo y la evaluación de impacto. *I+S: Revista de la sociedad española de informática y salud*, 128, 70.

Davara Rodríguez, A (2016). Reglamento Europeo sobre protección de datos. *Actualidad administrativa*, 7-8, 15-30.

Díaz García, J. (2018). Seguridad y protección de datos: el análisis de riesgo y la evaluación de impacto. *I+S: Revista de la sociedad española de informática y salud*, 128, 32.

García Garnica, M. C. (2018). La protección de los datos personales frente a su tratamiento "on line" por motores de búsqueda: el derecho al olvido digital. En J. Valls Prieto (Coord.), *Retos jurídicos por la sociedad digital* (107 a 135). Aranzadi.

Garrós Font, I. (2018). El principio de transparencia y el derecho a la protección de datos personales: comentarios a propósito del Reglamento sobre protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. *Actualidad administrativa*, 2, 17 a 42.

Heras Carrasco, R. (2018). RGPD: Evaluaciones de impacto. *I+S: Revista de la Sociedad Española de Informática y Salud*, 127, 24 a 27.

Oroz Valencia, L. (2018). Aproximación a la obligación de la protección de datos desde el diseño y por defecto. *Actualidad administrativa*, 1, 1 a 15.

Rodríguez Ayuso, J. F. (2020). Control de la privacidad por parte de las autoridades sanitarias ante situaciones de emergencia. *Revista de bioética y Derecho*, 50, 353-368.

Rodríguez Ayuso, J. F. (2020). Protección de datos personales en el contexto de la Covid-19: legitimación en el tratamiento de datos de salud por las Administraciones Públicas. *Revista catalana de Dret públic*, 3, 137-152.

Sierra Benítez, E. M. (2019). El delegado de protección de datos en la industria 4.0: funciones, competencias y las garantías esenciales de su estatuto jurídico. *Revista internacional y comparada de relaciones laborales y Derecho del empleo*, 1, 236 a 260.

IUS ET SCIENTIA • 2021
Vol. 7 • N° 1 • pp. 37 - 47
ISSN 2444-8478 • https://dx.doi.org/10.12795/IETSCIENTIA.2021.i01.04