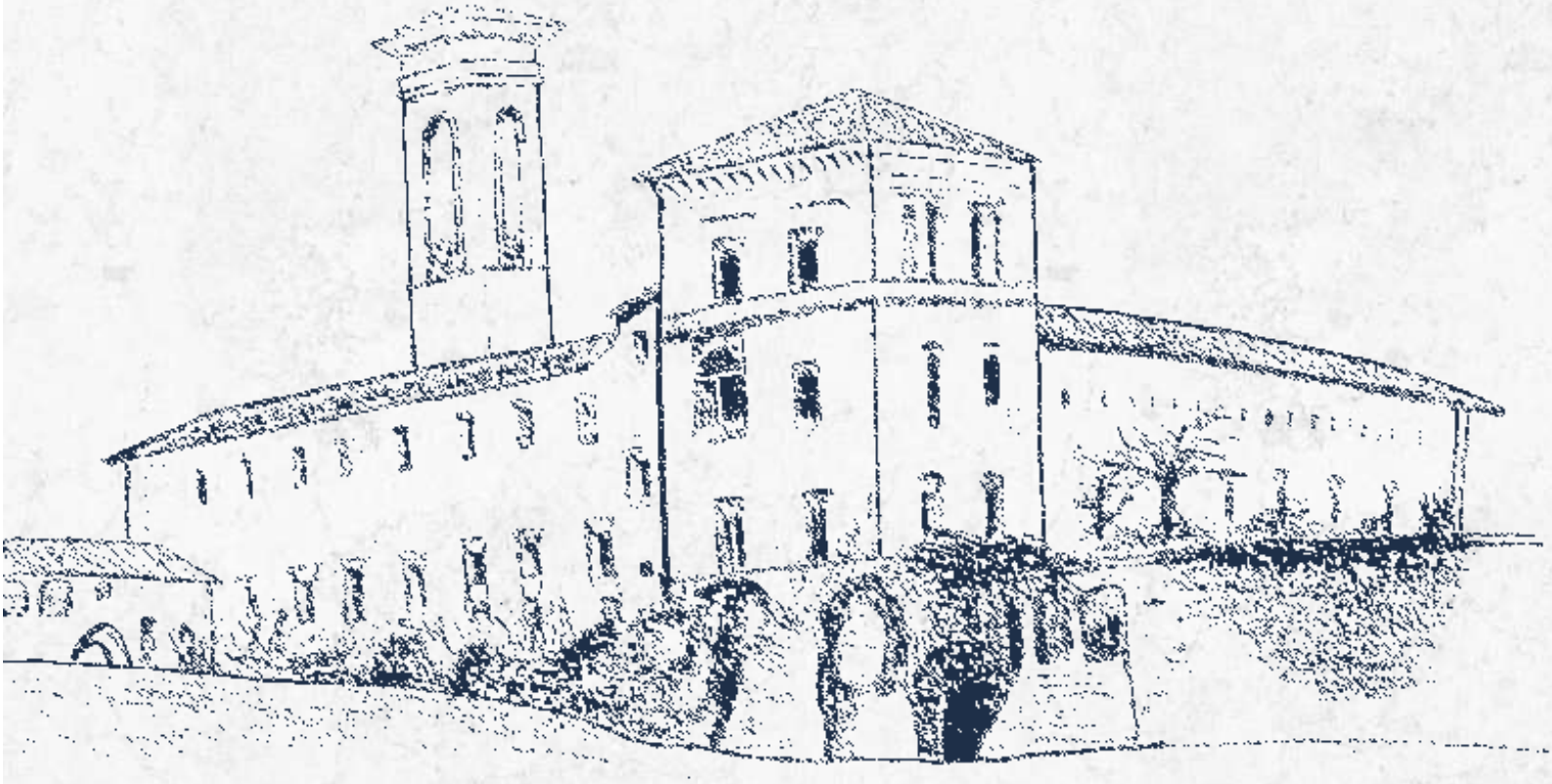
OPEN ACCESS
ISSN 2280-4056

E-Journal of International and Comparative

LABOUR STUDIES

Joint Issue (Vol 10 No. 03/2021 - Vol. 11 No. 01/2022)



ADAPT
www.adapt.it
UNIVERSITY PRESS

E-Journal of International and Comparative **LABOUR STUDIES**

ADAPT *International School of Higher Education in Labour and Industrial Relations*

E-Journal of International and Comparative

LABOUR STUDIES

Joint Issue (Vol 10 No. 03/2021 - Vol. 11 No. 01/2022)

ADAPT www.adapt.it UNIVERSITY PRESS

Online Publication of the ADAPT Series
Registration No. 1609, 11 November 2001, Court of Modena
www.adaptbulletin.eu

Big Data as a Tool to Enhance Recruitment Processes

Roberto Fernández Fernández [*]

Abstract

The selection of workers and the search for talent have become an essential aspect in companies to improve their competitive position in the market, as a proper selection of human resources can make a substantial difference to their competitors. The reality of labour intermediation has been significantly altered by the emergence of the Internet and social networks, so that the virtual space allows headhunters to obtain a large amount of data on candidates quickly, immediately and easily. To provide adequate protection to citizens, first the courts and then the legislator created a number of legal institutions that seek to set limits on the intrusion of new technologies into privacy. One of the best known is the right to be forgotten, which allows the interested party to request the de-indexation of past information that is not relevant at the present time.

Keywords: Social Network Sites; Recruitment; Algorithms; Right to be Forgotten; Privacy.

I. A New Way to Select Candidates: The E-Recruitment

Companies have a powerful weapon when selecting their workers and evaluating the suitability of candidates. That power has been increased by the amount of information that can be tracked through the Internet and

[*] Associate Professor of Law, University of León (Spain). Email address: rferf@unileon.es. This research is part of Proyecto de Investigación I+D+i DER2017-82192-C3-1-R, "Nuevos lugares, distintos tiempos y modos diversos de trabajar: innovación tecnológica y cambios en el ordenamiento social", funded by MCIN/ AEI/10.13039/501100011033/ and FEDER "Una manera de hacer Europa".

social networks, since citizens offer through them, either voluntarily or involuntarily, a large amount of data[1].

This search for data to find or certify the ideal candidate for the job may go further than necessary, with the employer investigating aspects that are inconsequential or very little relevant to determining the worker's professionalism. Information technology introduces a greater risk at this point, since it can lead to the reworking of a large amount of simple data in such a way that, combined with each other, it can practically give the profile of a person, and this not only through the direct collection of data, but also through the collection of fragmented and apparently inconsequential news which, combined, can give quite a lot of information about an individual or group of individuals[2].

In this way, information and communication technologies in general, and social networks in particular, allow access to a large volume of information and its rapid and cheap processing through the creation of corresponding algorithms that through profiling access detailed knowledge of when, how, where and with what result one has worked[3]. Always bearing in mind that it is neither easy nor simple to establish privacy filters on these platforms and to restrict who are the users who can see the content of the same, without prejudice to the fact that the network itself on many occasions requires certain data to be accessible to the general public.

Based on the above premises, one of the areas where companies struggle most in their competitive strategies is in attracting talent. Traditional recruitment mechanisms present a major limitation because the information provided comes from the candidates themselves, which often prevents them from obtaining a complete and reliable profile. Indeed:

---

[1] "These sites invite users to disclose their personal information such as date of birth, gender, hometown and hobbies, for the purposes of creating a profile of themselves. They provide users with the ability to post their own content in the form of videos, pictures and comments which can be made publicly visible. Social networking sites also allow registered users to interact with their contacts, who they have previously invited to become a member of their network of friends. Online social networks differ greatly from offline social interactions; they are more publicised; have the potential to reach a wider audience and can remain in the public domain long after their first publication. For these reasons joining an online social network can prospectively have far reaching implications for the user", T. McDermott, *Legal issues associated with minors and their use of social networking sites*, *Communications Law*, 2012, Vol. 17, núm. 1, p. 19.

[2] J.L. Monereo Pérez y J.A. Fernández Bernat, *"Listas negras" de trabajadores conflictivos*, *Trabajo y Derecho*, 2016, núm. 16, p. 5 (smarteca).

[3] Social Court Decision, number 33, Madrid 11 February 2019.

> with the advent of the era of Big Data, this problem has been resolved successfully. In the context of Big Data, information access and sharing are very convenient, any individual can search the information they want to learn through the network at any time or anywhere easily. In addition, more and more organizations began to develop professional network training courses. Companies can according to its own situation choose purchase these courses directly or customize. Such software programs can record the data of study behaviors of every employee, who can not only use the online system to analyze their own training needs, but also can choose your favorite form of teaching. So that employee can make their training more targeted and improve training efficiency. In addition, employee can accept online test and feedback at any time, which can enhance learning interest effectively and ensure the learning effect. And after a certain time, based on the learning data, the software can also predict an individual's possible improve point. In addition, to keep abreast of staff mastery of new skills, managers can monitor employees' learning situation in the background[4].

For this reason, the Big Data offers hitherto unexplored possibilities and can help to overcome the difficulties identified: firstly, it provides companies with a wider platform, such as the internet and/or social networks, allowing them to build the candidate's fingerprint; secondly, a combination of these new tools with classic recruitment strategies constitutes an unknown source of information for recruiters, who can access personal images, living conditions, social relations, skills, etc., that will allow them to build a more faithful image of the candidate, both personally and professionally.

For the above arguments, it is necessary to be aware of how conduct at one point, which may appear innocent, can over time have a detrimental effect on finding future employment. Tracking of the candidate's comments and the information that the employer can obtain about him or her can constitute the differential element in order to obtain or not a job.

II The Power of the Internet and Social Networks in Candidate Selection

II.a Use of the Social Media in the Recruitment Process

In social networks you can access information such as the age of the candidate, places of study, home, hobbies, religious or political beliefs, sexual orientation, circle of friends and a large number of photos, videos,

[4] S. Zhan y M. Ye, *Human resource management in the era of Big Data*, *Journal of Human Resource and Sustainability Studies*, 2015, Vol. 3, núm. 1, p. 43.

comments and personal opinions capable of generating a profile of the candidate[5]. All circumstances that may predispose the company to hire or not.

In addition, it is necessary to take into account the weak position of the candidates who, in their eagerness to find a job, may be more willing to provide the data requested by the person carrying out the selection process in the desire to get the job. The moment before the conclusion of the employment contract is particularly sensitive and important in terms of the processing of personal data. Common sense tells us that those seeking a job are willing to provide as much data as requested, since the purpose of the employment contract is to meet the vital needs of the candidate and his or her family (art. 35 Spanish Constitution)[6].

For this reason, it is necessary to consider the following two practices as illegal, at least in Spanish law: shoulder surfing, used to obtain access keys or passwords to a social network; asking the candidate to provide the company with access to social networks or to accept the company as a friend on that network[7].

Along with the data provided by generalist social networks, there are some of them (LinkedIn, Infojobs, Monster or Xing, among others) that are only dedicated to the professional field and to facilitate contracts between companies and workers. In this way, they can be used to obtain the professional career of the worker.

In addition, they can offer added value by becoming a business model because the use of premium services in this type of network, unlike other types of platforms, has a high yield of the number of premium users, who pay a monthly amount, to access advanced services[8].

Indeed, these are social networks and online platforms whose mission is to bring together professionals from all over the world so that they can be more productive and successful, and which can bring significant benefits to both workers and employers. In addition, the employer obtains a high degree of optimisation at zero cost because registration in these networks, apart from the subscription to premium services, is free of charge;

[5] J. Llorens Espada, *El uso de Facebook en los procesos de selección de personal y la protección de los derechos de los candidatos*, *Revista de Derecho Social*, 2014, núm. 68, p. 56.

[6] C.H. Preciado Domènech, *El Derecho a la Protección de Datos en el Contrato de Trabajo*, Thomson Reuters – Aranzadi, Cizur Menor, 2017, p. 156.

[7] E.E. Taléns Visconti, *Incidencia de las Redes Sociales en el ámbito laboral y en la práctica procesal*, Francis Lefebvre, Madrid 2020, p. 31.

[8] INTECO y AEPD, *Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales on line*, INTECO-AEPD, León, 2009, p. 44. It is available at the following link: [https://www.uv.es/limprot/boletin9/inteco.pdf].

however, their use should be based on good faith and respect for the fundamental rights of employees, which is not always the case.
In any case:

> employers should not assume that merely because an individual's social media profile is publicly available they are then allowed to process those data for their own purposes. A legal ground is required for this processing, such as legitimate interest. In this context the employer should—prior to the inspection of a social media profile—take into account whether the social media profile of the applicant is related to business or private purposes, as this can be an important indication for the legal admissibility of the data inspection. In addition, employers are only allowed to collect and process personal data relating to job applicants to the extent that the collection of those data is necessary and relevant to the performance of the job which is being applied for[9].

II.b Big Data Analytics Used in Human Resources Practices

There are companies that specialise in searching for information on potential job candidates through the Internet or social networks in order to draw up their personal and professional profile. Likewise, alongside the classic headhunters, nethunters have emerged who are dedicated solely to searching for information in these digital media.
So, "it must be found that, in exploring the internet automatically, constantly and systematically in search of the information which is published there, the operator of a search engine 'collects' such data which it subsequently 'retrieves', 'records' and 'organises' within the framework of its indexing programmes, 'stores' on its servers and, as the case may be, 'discloses' and 'makes available' to its users in the form of lists of search results. As those operations are referred to expressly and unconditionally in Article 2(b) of Directive 95/46, they must be classified as 'processing' within the meaning of that provision, regardless of the fact that the operator of the search engine also carries out the same operations in respect of other types of information and does not distinguish between the latter and the personal data […] Also, the organisation and aggregation of information published on the internet that are effected by search engines with the aim of facilitating their users' access to that information may, when users carry out their search on the basis of an individual's name, result in them obtaining through the list of results a

[9] Article 29. Data Protection Working Party: *Opinion 2/2017 on data processing at work*, 8 June 2017, p. 11. It is available at the following link: [https://ec.europa.eu/newsroom/article29/items/610169].

structured overview of the information relating to that individual that can be found on the internet enabling them to establish a more or less detailed profile of the data subject"[10].

Applications are also increasingly used during the selection procedure to allow for an initial screening of the applications submitted. The applications are fed into software with specific patterns that can quickly and easily select the candidates to move on to the next stages, in an action that can cover all the selective phases, given that the deployment of recruitment algorithms is not limited to background research: every process, from CV analysis to the classification of candidates, the making of offers and the determination of salaries can be automated[11].

These applications make use of the potential of big data, which allows them to "the collection, analysis and the recurring accumulation of large amounts of data, including personal data, from a variety of sources, which are subject to automatic processing by computer algorithms and advanced data-processing techniques using both stored and streamed data in order to generate certain correlations, trends and patterns (big data analytics)"[12].

In any case, and regardless of the model used by the company and the technology employed to select workers, the company must respect the fundamental rights of workers in this process.

For the above reasons, it is necessary to avoid the existence of any discriminatory bias for any reason of a personal nature in the algorithms, given the growing power derived from Big Data, which makes it essential to adopt appropriate mechanisms of a limiting nature capable of combating information asymmetries and their consequences in terms of economic advantages and social control of companies[13].

In this regard, it is not enough to eliminate race, gender, ethnicity or age from the data set, as the algorithm could link other variables to these causes of discrimination, such as the postal code or years of experience, sometimes unknown to those who create, apply or are assessed by them.

---

[10] European Union Court of Justice Decision C-131/12, 13 may 2014, case *Google Spain y Google*.

[11] H. Álvarez Cuesta, *El impacto de la inteligencia artificial en el trabajo: desafíos y propuestas*, Thomson Reuters – Aranzadi, Cizur Menor 2020, p. 31.

[12] European Parliament, *European Parliament resolution of 14 March 2017 on fundamental rights implications of big data: privacy, data protection, non-discrimination, security and law-enforcement (2016/2225(INI))*, It is available at the following link: [https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52017IP0076].

[13] A. Mantelero, *Masters of Big Data: concentration of power over digital information*, 2012, It is available at the following link: [https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2048236].

Moreover, algorithmic decisions can systematically exclude certain people from employment, leaving certain groups virtually unemployable, deepening the digital divide even for jobs that would not require technology[14].

Indeed, artificial intelligence is a tool that must be used ethically by companies. And that ethical sense must be clearly defined by the laws of the various countries or by collective agreements. We must return to the social control of technological change where respect for certain rights and minimum protections are demanded[15].

In this way, the algorithms used cannot establish biases capable of ending up in the application of arbitrariness or inequalities generating discrimination. To avoid any discrimination, it is necessary to allow the participation of workers' representatives in the generation of these algorithms and to audit their results with continuous and dynamic checks. It is also important to inform candidates about the use and scope of data analysis.

This is in compliance with Article 35 of the General Data Protection Regulation when it states as follows: "where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data".

This assessment will therefore be required in the selection of employees by human resources analysis practices, as most (if not all) of the selection processes for future employees will involve "a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person" [art. 35.3.a) GDPR].

Indeed, the need for adequate management of data protection risks can be accounted for when the impact of a factor is very important for the rights and freedoms of citizens, even if the probability of occurrence is very low or negligible[16].

---

[14] H. Álvarez Cuesta, *op. cit.*, pp. 33 y 34.

[15] J.L. Goñi Sein, *Innovaciones tecnológicas, inteligencia artificial y derechos humanos en el trabajo*, *Documentación Laboral*, 2019, Vol. 117, núm. II, p. 67.

[16] Agencia Española de Protección de Datos, *Gestión del riesgo y evaluación de impacto en tratamientos de datos personales*, Agencia Española de Protección de Datos, Madrid, 2021, p. 36.

Consequently, proper compliance with GDPR requires that those who are going to use a system based on Artificial Intelligence and Big Data validate the procedures prior to the design/selection and implementation of the Artificial Intelligence solution for a given processing operation, so that it is possible to identify the privacy requirements to be incorporated and to effectively apply the privacy measures from the design and by default[17].

On the other hand, and to ensure that these procedures are safe and reliable in its execution, a desirable interaction between machine and man could be envisaged, so that, for example, the AI system could take into account measurable properties, such as the number of years of experience of a job applicant, while a human reviewer evaluates the applicants' skills that cannot be captured in the application forms[18]; with this combination it could better fight both the already seen biases of automation and the unconscious biases of individuals[19].

Furthermore, at the final stage of the procedure, the possibility of a human having the final say in all automated decisions should never be ruled out, given that the design of systems with a "dead man's lever" orientation should be avoided and the option should always be given for a human operator to override the algorithm at any given moment, with the procedure for those situations in which this course of action must be chosen[20], thus ensuring a human-centred approach to the subject.

---

[17] Agencia Española de Protección de Datos, *Adecuación al RGPD de tratamientos que incorporan Inteligencia Artificial. Una introducción*, Agencia Española de Protección de Datos, Madrid, 2020, p. 31.

[18] R. Binss y V. Gallo, *Automated Decision Making: the role of meaningful human reviews*, Oficina del Comisionado de Información, Londres 2019. It is available at the following link: [https://ico.org.uk/about-the-ico/news-and-events/ai-blog-automated-decision-making-the-role-of-meaningful-human-reviews/].

[19] J.S. Lublin, *Bringing Hidden Biases Into the Light. Big Businesses Teach Staffers How 'Unconscious Bias' Impacts Decisions*, *The Wall Street Journal*, 9 de enero de 2014. It is available at the following link: [https://www.wsj.com/articles/SB10001424052702303754404579308562690896896].

[20] Agencia Española de Protección de Datos, *Adecuación al RGPD de tratamientos que incorporan Inteligencia Artificial. Una introducción*, Agencia Española de Protección de Datos, Madrid, 2020, p. 28.

III. Right to be Forgotten

We cannot forget the possibility that social networks and the Internet leave a digital footprint that can be followed and tracked many years later and provide information on a perennial basis about a citizen.

"It must be recalled, that the activity of a search engine consisting in finding information published or placed on the internet by third parties, indexing it automatically, storing it temporarily and, finally, making it available to internet users according to a particular order of preference"[21].

In this respect, the right to information self-determination has recently given rise to a fierce debate between two disparate positions, the European and the American, on the opportunity and possible scope of the exercise of an alleged right to be left alone, understood as the right to demand the removal or deletion of personal information which, although true, entails or represents for the data subject an injury or damage that he or she understands he or she does not have a legal duty to bear[22].

Faced with this reality, first the European Courts, and then the Community and Spanish legislators, have acted, establishing a series of limits on the information that can be accessed and the use that can be made of it after a certain period of time[23]. Thus, the Court of Justice of the European Union has created what is known as the right to be forgotten.

Therefore, "the supervisory authority or judicial authority may order the operator of the search engine to remove from the list of results displayed following a search made on the basis of a person's name links to web pages published by third parties containing information relating to that person, without an order to that effect presupposing the previous or simultaneous removal of that name and information — of the publisher's own accord or following an order of one of those authorities — from the web page on which they were published"[24].

---

[21] European Union Court of Justice Decision C-136/17, 24 september 2019, case *GC y otros*.

[22] A.B. Casares Marcos, *El derecho al olvido como facultad integrante del derecho a la autodeterminación informativa del ciudadano*, *CEF Legal*, 2017, núm. 198, p. 57.

[23] "The availability of data from past interactions will undermine our right to oblivion, providing an ever-increasing resource of information about our inclinations that can be held against us at any point in time", M. Hildebrandt, *Ambient intelligence, criminal liability and democracy*, *Criminal Law and Philosophy*, 2008, Vol. 163, p. 166.

[24] European Union Court of Justice Decision C-131/12, 13 may 2014, case *Google Spain y Google*.

And that it is even, "in a case where that name or information is not erased beforehand or simultaneously from those web pages, and even, as the case may be, when its publication in itself on those pages is lawful"[25], so that it will be necessary to evaluate in each individual case "whether the data subject has a right that the information relating to him personally should, at this point in time, no longer be linked to his name by a list of results displayed following a search made on the basis of his name. In this connection, it must be pointed out that it is not necessary in order to find such a right that the inclusion of the information in question in the list of results causes prejudice to the data subject"[26].

For its part, Article 17 of the General Data Protection Regulation of 2016 establishes that the data subject has the right "to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

(a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;

(b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;

(c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);

(d) the personal data have been unlawfully processed;

(e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;

(f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1)".

Thus, the Regulation clarifies the right to have personal data deleted from a particular database containing such data. That, and nothing else, is the right to forget. A right to the deletion of personal data[27].

However, the Community article does not provide a definition of what the right to forget is, nor does it appear in European case law, although it can be taken indirectly from some pronouncements, when it states that its

[25] European Union Court of Justice Decision C-136/17, 24 september 2019, case *GC y otros*.

[26] European Union Court of Justice Decision C-131/12, 13 may 2014, case *Google Spain y Google*.

[27] Spanish Constitutional Court Decision 58/2018, 4 June 2018.

content refers to the removal of links from a list of results when the search criteria is the name of a natural person[28].

In addition, article 17 of the General Data Protection Regulation of 2016 establishes "where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data".

In any case, the general rule of erase finds several exceptions in paragraph 3 of the provision, since the prerogative analysed cannot be invoked in the following cases:

(a) for exercising the right of freedom of expression and information;

(b) for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(c) for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3);

(d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing;

or (e) for the establishment, exercise or defence of legal claims.

In this way, the right to be forgotten means that the person concerned can demand the cancellation of the processing of his or her personal data when a period of time has elapsed that makes it inappropriate in relation to the purpose for which the data was collected, since the person concerned has no public relevance and there is no historical interest in linking the information with his or her personal data[29].

Consequently, the search engine, or the person responsible for the social network, cannot adopt a merely passive attitude, but will have to put in

[28] European Union Court of Justice Decision C-136/17, 24 September 2019, case *GC y otros*.

[29] R. Fernández Fernández, *Redes sociales y Derecho del Trabajo. El lento tránsito desde la indiferencia legislativa a la necesaria regulación legal o convencional*, Thomson Reuters – Aranzadi, Cizur Menor, 2020, p. 106.

place the necessary measures to proceed with the deindexation of the data that is of no interest at the present time.

However, it is not possible to forget the difficulties in achieving such an outcome, because "the critique of the post-Costeja González [*Google Spain* case] paradigm has brought to light numerous issues with regard to its application and implementation. The diverse storage of personal data makes it very hard to identify all of the publications of the data which needs to be removed. The ease of replicability and transferability of data on the internet with technological developments has led to the lack of enforceability, which greatly hinders the implementation of the right to be forgotten"[30].

Indeed, "the prohibition or restrictions relating to the processing of special categories of personal data, […] apply also […] to the operator of a search engine in the context of his responsibilities, powers and capabilities as the controller of the processing carried out in connection with the activity of the search engine, on the occasion of a verification performed by that operator, under the supervision of the competent national authorities, following a request by the data subject"[31].

On balance, the right to be forgotten does not so much imply a total elimination of the data or facts collected in a given repository or social network, as the possibility of requesting search engines not to index certain information if it is not relevant and has already lost its importance[32], because under the new rule "internet users control the data they put online, not the references in media or anywhere else"[33].

Finally, the relevance of the right to be forgotten, both as an appropriate mechanism to control the collection of data through social networks and in the analysis processes by human resources departments, cannot be questioned. In this sense, the prerogative analysed recognises the right of all individuals to have information about them deleted by those who use their data when it is inadequate, inaccurate, irrelevant, out of date or excessive, or when the passage of time has characterised it as such. In this operation, the passage of time, the purposes for which the data were

[30] F.U. Ahmed, *Right to be forgotten: a critique of the post-Costeja Gonzalez paradigm*, *Computer and Telecommunications Law Review*, 2015, Vol. 21, núm. 6, p. 184.

[31] European Union Court of Justice Decision C-136/17, 24 September 2019, case *GC y otros*.

[32] R. Fernández Fernández, *op. cit.*, p. 106.

[33] O. Pastukhov, *The right to oblivion: what's in the name?*, *Computer and Telecommunications Law Review*, 2013, Vol. 19, núm. 1, p. 14.

collected and processed or the nature and public interest of the information must be taken into consideration.

IV. Conclusion

The Internet and social networks have represented a hitherto unseen advance in the way citizens communicate, and their potential should be used as an advantage to improve people's quality of life. Indeed, new technological tools make it possible to obtain information about a person quickly, instantly and easily. Thus, companies have at their disposal a powerful weapon to build the profile of the candidate they consider most optimal for the vacant position.

However, the brightness of the Internet and social networks should not lead to the temptation to sacrifice certain fundamental rights beyond what is tolerable, such as privacy and data protection, because the person wants to occupy a privileged position in these digital devices.

For this reason, it is important to act in three areas: on the one hand, the managers of social networks or the Internet must establish clear and simple privacy policies that guarantee fundamental rights; on the other, citizens must be aware of the dangers that an excess of information may cause in their future professional career; finally, the public authorities must establish legislative provisions aimed at protecting citizens, a good example being the rights to data protection or to be forgotten.

V. Bibliographical References

Agencia Española de Protección de Datos, *Gestión del riesgo y evaluación de impacto en tratamientos de datos personales*, Agencia Española de Protección de Datos, Madrid, 2021.

Agencia Española de Protección de Datos, *Adecuación al RGPD de tratamientos que incorporan Inteligencia Artificial. Una introducción*, Agencia Española de Protección de Datos, Madrid, 2020.

F.U. Ahmed, *Right to be forgotten: a critique of the post-Costeja Gonzalez paradigm*, *Computer and Telecommunications Law Review*, 2015, Vol. 21, núm. 6.

H. Álvarez Cuesta, *El impacto de la inteligencia artificial en el trabajo: desafíos y propuestas*, Thomson Reuters – Aranzadi, Cizur Menor 2020.

Article 29. Data Protection Working Party: *Opinion 2/2017 on data processing at work*, 8 june 2017, p. 11. It is available at the following link: [https://ec.europa.eu/newsroom/article29/items/610169].

R. Binss y V. Gallo, *Automated Decision Making: the role of meaningful human reviews*, Oficina del Comisionado de Información, Londres 2019. It is available at the following link: [https://ico.org.uk/about-the-ico/news-and-events/ai-blog-automated-decision-making-the-role-of-meaningful-human-reviews/].

A.B. Casares Marcos, *El derecho al olvido como facultad integrante del derecho a la autodeterminación informativa del ciudadano*, *CEF Legal*, 2017, núm. 198.

European Parliament, *European Parliament resolution of 14 March 2017 on fundamental rights implications of big data: privacy, data protection, non-discrimination, security and law-enforcement (2016/2225(INI))*, It is available at the following link: [https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52017IP0076].

R. Fernández Fernández, *Redes sociales y Derecho del Trabajo. El lento tránsito desde la indiferencia legislativa a la necesaria regulación legal o convencional*, Thomson Reuters – Aranzadi, Cizur Menor, 2020.

J.L. Goñi Sein, *Innovaciones tecnológicas, inteligencia artificial y derechos humanos en el trabajo*, *Documentación Laboral*, 2019, Vol. 117, núm. II.

M. Hildebrandt, *Ambient intelligence, criminal liability and democracy*, *Criminal Law and Philosophy*, 2008, Vol. 163.

INTECO y AEPD, *Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales on line*, INTECO-AEPD, León, 2009, p. 44. It is available at the following link: [https://www.uv.es/limprot/boletin9/inteco.pdf].

J. Llorens Espada, *El uso de Facebook en los procesos de selección de personal y la protección de los derechos de los candidatos*, *Revista de Derecho Social*, 2014, núm. 68.

J.S. Lublin, *Bringing Hidden Biases Into the Light. Big Businesses Teach Staffers How 'Unconscious Bias' Impacts Decisions*, *The Wall Street Journal*, 9 de enero de 2014. It is available at the following link: [https://www.wsj.com/articles/SB10001424052702303754404579308562690896896].

A. Mantelero, *Masters of Big Data: concentration of power over digital information*, 2012, It is available at the following link: [https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2048236].

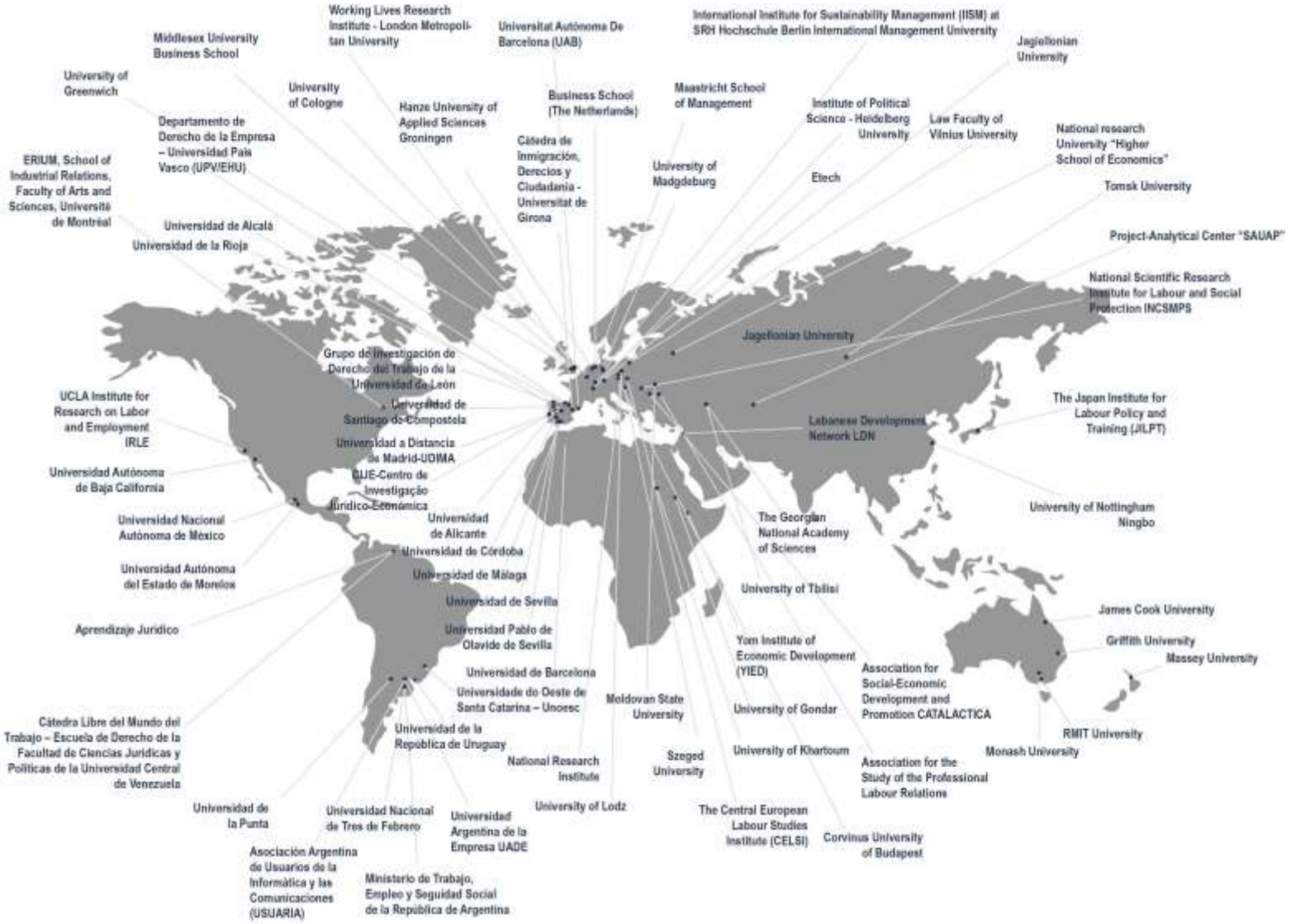
T. McDermott, *Legal issues associated with minors and their use of social networking sites*, *Communications Law*, 2012, Vol. 17, núm. 1.

J.L. Monereo Pérez y J.A. Fernández Bernat, *"Listas negras" de trabajadores conflictivos*, *Trabajo y Derecho*, 2016, núm. 16 (smarteca).

O. Pastukhov, *The right to oblivion: what's in the name?*, *Computer and Telecommunications Law Review*, 2013, Vol. 19, núm. 1.

C.H. Preciado Domènech, *El Derecho a la Protección de Datos en el Contrato de Trabajo*, Thomson Reuters – Aranzadi, Cizur Menor, 2017.
E.E. Taléns Visconti, *Incidencia de las Redes Sociales en el ámbito laboral y en la práctica procesal*, Francis Lefebvre, Madrid 2020.
S. Zhan y M. Ye, *Human resource management in the era of Big Data*, *Journal of Human Resource and Sustainability Studies*, 2015, Vol. 3, núm. 1.

ADAPT International Network



ADAPT is a non-profit organisation founded in 2000 by Prof. Marco Biagi with the aim of promoting studies and research in the field of labour law and industrial relations from an international and comparative perspective. Our purpose is to encourage and implement a new approach to academic research, by establishing ongoing relationships with other universities and advanced studies institutes, and promoting academic and scientific exchange programmes with enterprises, institutions, foundations and associations. In collaboration with the Centre for International and Comparative Studies on Law, Economics, Environment and Work, (DEAL) the Marco Biagi Department of Economics, University of Modena and Reggio Emilia, ADAPT set up the International School of Higher Education in Labour and Industrial Relations, a centre of excellence which is accredited at an international level for research, study and postgraduate programmes in the area of industrial and labour relations. Further information at *www.adapt.it*.

For more information about the E-journal and to submit a paper, please send a mail to *LS@adapt.it*.

DEAL Centre for International and Comparative Studies Law Economics Environment Work
THE MARCO BIAGI DEPARTMENT OF ECONOMICS
UNIVERSITY OF MODENA AND REGGIO EMILIA

ADAPT International.it
Building the Future of Work