LEGAL IMPLICATIONS OF WORKERS' ONLINE ACTIVITY ON THE EMPLOYMENT RELATIONSHIP: ITALY AND SPAIN IN COMPARISON

IMPLICACIONES LEGALES DE LA ACTIVIDAD EN INTERNET DE LA PERSONA TRABAJADORA EN LA RELACIÓN DE EMPLEO: COMPARACIÓN ESPAÑA-ITALIA

Lisa Cetrano
Ph.D. candidate in civil and labour law.
University of Pisa and Göttingen
l.cetrano@studenti.unipi.it

Recibido: 04/02/2020 Aceptado: 19/05/2020

Laburpena: Lan hau Europar Batasuneko estatu kideek emandako epaietan oinarritzen da. Izan ere, langile baten ekintza sarean, batik bat sare sozialetan, askotan, inpaktu garrantzitsua izan dezake enplegu pribatuaren harremanetan ezezik, sektore publikoan ere ondorioa mugatuz edo baita harreman horren ezarketa eragotziz ere. Ikerketaren xedea da prozesu judizial hauei lotutako oinarrizko lege-kontu bien hausnarketa egitea: lehenik eta behin, enplegu-emailearen aldetik langilearen datuen trataerarekin lotutako arazoak aipatzen dira eta, bigarrenik, langileen jokabideei era egokian lege-garrantzia ematen zaion planteatzen da, zerbitzutik kanpo daudenean, lan harremanean. Azterlanaren galdera hauek era eraginkorrean erantzun daitezke zuzenbide alderatuaren metodologia erabilita, europar diziplinaren birsorketa sistematikoa barne: Datuen Babeserako Erregelamendu Orokorrak legegile nazionalari baimentzen baitio datuen trataera, lan-harremanaren barnean. Lege-ekimenen azterketatik aurrera, bereziki Italian eta Espainian, possible da aspektu kritiko batzuk adieraztea langilearen datuen trataera zein lege-baldintzen menpe egon behar denari buruz, enplegu emailearen aldetik, baita kontratuaren gaineko zein ondorio aplikatu diezaiokeen enplegatu bati, sektore pribatuan. Ikus daitekeen bezala, lan honen ondorio eta proposamenei dagokienez, Lantaldearen 29. artikuluan agertzen diren printzipio nagusiek «datu pertsonalen trataerari buruz lan-testuinguruan», enplegatuarentzat babes handiagoa proposatzen dute, «eskubide indikatiboaren egite ez loteslea»-ren partaide izateari utzi gabe.

Gako-hitzak: zerbitzutik kanpo egindako jokabideengatik kaleratzea, enplegatuaren datuen babesa, Datuak Babesteko Erregelamendu Orokorra (DBEO), betebehar osaga-rriak.

Resumen: El presente trabajo se basa en sentencias recientes dictadas en los Estados miembros de la Unión Europea según las cuales la actividad de un trabajador en la red, especialmente en las redes sociales, a menudo puede tener un impacto importante en el destino no solo de las relaciones de empleo privado sino también del sector público, determinando la conclusión o incluso impidiendo de entrada el establecimiento de esta relación. El propósito de la investigación es reflexionar sobre las dos cuestiones legales fundamentales involucradas en estos procesos judiciales: primero, los problemas relacionados con el tratamiento de datos del trabajador por parte del empleador y, segundo, la relevancia legal que se puede asignar de manera válida a las conductas fuera de servicio de los empleados en la relación laboral. Estas preguntas de investigación se pueden responder de manera efectiva mediante el uso de una metodología de derecho comparado, incluida una reconstrucción sistemática de la disciplina a nivel europeo, ya que el Reglamento General de Protección de Datos permite al legislador nacional la regulación específica del tratamiento de datos dentro de la relación laboral. A partir del análisis de las iniciativas legislativas, específicamente en Italia y España, es posible delinear algunos aspectos críticos con respecto a qué condiciones legales debe estar sujeto el tratamiento de los datos del trabajador por parte del empleador y qué consecuencias contractuales pueden asignarse a la conducta de un empleado del sector privado. Como puede verse, de acuerdo con las conclusiones y propuestas de este trabajo, los principios rectores establecidos en el artículo 29 del Grupo de trabajo «sobre el tratamiento de datos personales en el contexto laboral» proponen una mayor protección para el empleado, sin dejar de formar parte de la denominada «elaboración de derecho indicativo no vinculante».
Palabras clave: despido debido a conductas fuera de servicio, protección de datos del empleado, Reglamento General de Protección de Datos (RGPD), obligaciones auxiliares.

Abstract: The present work takes a cue from recent judgments in European Member States, according to which the activity of a worker on the net, especially on social networks, can often have an important impact on the fate of the private but also public employment relationships, determining the conclusion or even preventing the establishment of this relationship in the first place. The purpose of the research is to reflect upon the two fundamental legal issues involved in these court cases: first, the problems related to the worker's data processing by the employer and, second, the legal relevance that can be validly assigned to the employee's off-duty conduct on the employment relationship. These research questions can be answered effectively by using legal comparison methodology, including a systematic reconstruction of the discipline at the European level, since the General Data Protection Regulation allows the domestic legislator the specific regulation of data processing within the employment relationship. From the analysis of the legislative initiatives, specifically in Italy and Spain, it is possible to outline some critical aspects with regard to which legal conditions the processing of worker's data by the employer must be subject and what contractual consequences can be assigned to a private employee's behavior. As can be seen, according to the conclusions and proposals of this work the guiding principles stated in article 29 Working Party *«on the processing of personal data in the employment context»* propose a greater protection to the employee, while remaining a so-called «soft-law making».
Keywords: dismissal due to off-duty conducts, employee's data protection, General Data Protection Regulation (GDPR), ancillary obligations.

Summary

1. Introductory remarks

Nowadays, the widespread use of computer technologies in the workplace facilitates the accomplishment of work-related duties, which can very often be carried out far from workplaces and outside of working hours. A recent example of this phenomenon is the new form of smart working, characterized by the absence of temporal and spatial boundaries.

One of the most relevant consequences of these new forms of work contracts without a fixed working time and location is the implicit difficulty in distinguishing between private and professional life (Barnes, 2006; Marcus, Machilek & Schütz, 2006; Zimmer, 2010; Spiekermann, Krasnova, Koroleva & Hildebrand, 2010; Katsabian, 2018). Closely tied to this difficulty is the issue that the private use of computer technologies makes personal data potentially accessible by anyone. The future of work seems to be very close to an idea of reciprocal permeability between private and working life, with increasingly frequent cases in which one can lead to the end of the other. This background not only gives rise to the necessity for a policy on work-life balance and disconnection right but also provides a new opportunity to reflect on the hypothesis of dismissal due to inappropriate private use of computer technologies. In particular, the courts are called to establish whether a dismissal based on an employee's online activity is legitimate or not (an example could be the case of an inappropriate comment, photo, or like on Facebook or Twitter). To mention only a few cases: in 2009, the Rome Court of Justice considered lawful the dismissal of a well-known Italian airline hostess, of whom some pornographic material was accessible in Internet, easily found by typing the name of the airline and the noun of «hostess» (Pisani, 2009); in 2015, the Ivrea Court of Justice considered rightful the dismissal of an employee who had insulted his colleagues and his employer through a post on his personal Facebook page (Salazar, 2015); the Baden-Württemberg Regional Labour Court of Appeal ruled in a judgment on 14 March 2019 that the dismissal of an employee who had accused a colleague of rape in a WhatsApp conversation with other colleagues was justified (Weller, 2019); in February 2010, the Court of Palma de Mallorca declared lawful the dismissal of an employee who had shared images through his Facebook profile in which he mocked the horrors of the war in Syria (Superior Court of Justice of Andalusia, Seville, Sala de lo Social, sec. I, ruling of 8 June 2017, n. of complaint: 2275/2016 (resolution n. 1736/2017)).

The phenomenon concerning an employer's choices on the grounds of a worker's information gained on the network involves several legal matters with critical implications for the civil law related basis of the employment relationship. The court dealing with cases of dismissals due to online off-duty conducts, reviewing the legality of the employer's decision and the facts and circumstances upon which the measure is based, must maintain a balance between opposing interests, such as the employer's power of control over working time and respect for the employee's personal sphere, with reflections on the extent of the obligations levied on the employee himself.

Specifically, from the employee's perspective, it can be argued that what is on his social media profile is precluded to third parties outside the circle of virtual friends. Furthermore, along this line, it can be supported that the content, even if considered inappropriate on a professional level, must be protected as

an exercise of the freedom of expression. The linking of these claims suggests the idea that the employee's personal information accessible on the web should be included in the protection of the private sphere. This argumentation finds confirmation in several studies in sociology and in psychology aimed at understanding what human impulse is hidden under the tendency to share private information on social networks. Research conducted by the Department of Cognitive and Psychological Neuroscience at Harvard University has shown that the activity of providing self-information within a virtual community in which each user can build their own virtual identity by sharing personal content and interacting with other subjects, stimulates the same areas of pleasure that are activated by food, money, and sex (Tamir & Mitchell, 2012).

There may be several reasons for this: the desire to establish new friendships, to stay in touch with old friends, and to feel like part of a community. Ultimately, it can be said that based on the social network's use, there is a primordial human need to show oneself to the world. In this case, sharing information on the network has become a way of creating one's own individual identity (Brandtzæg & Heim, 2009; Nadkarni & Hofmann, 2012; Mills, 2017). This approach is confirmed by the doctrine that the employer's power of control, exercised through the screening of employee's social network profiles, should not harm the worker's right to data protection. Given this premise, the respect for the employee's private sphere should be increased, especially if the employer monitors the worker's off-duty conduct, which is, by definition, unrelated to the employment relationship and for this reason ineligible as a yardstick of non-compliance to contractual obligations (Sanseverino, 1978).

Conversely, from the employer's perspective, it can be argued that the employee's online reputation should not damage the company's public image, given that the employee also should behave properly in his private life. According to this second thesis, the employee's private life, even if formally distinct from the employment relationship, should be oriented towards the employer's interests (Colucci, 2002). This approach is confirmed by the doctrine that, as soon as private information is shared and becomes potentially publicly visible online, it must be supposed that it no longer belongs to the employee's private sphere, resulting in possible damage to the employer. The premise of this hypothesis is that the online off-duty conduct is relevant to the fulfillment of contractual performance and to the professional evaluation of the employee's competence both for the instauration of the employment relationship and for the prosecution itself (Salazar, 2015).

2. Practical Needs

For the phenomenon under examination, it is also worth mentioning cases in the American legal system, where more and more employees report that they lost their job due to private behavior on social networks, e.g., comments, photos, or likes on Facebook and Twitter, which were considered as inappropriate by their employers. Perhaps the most well-known case of loss of work due to an online post is that of the PR chief Justine Sacco, who tweeted during a holiday trip to South Africa the following sentence: *«Going to Africa. Hope I don't get AIDS. Just kidding, I'm white»*. The tweet on her account became a trending hashtag and was retweeted thousands of times, after which her company fired her for her unfortunate judgment. Something similar happened to Ashley Payne, who was fired from her job as a teacher after a parent complained of a picture posted by the teacher on her Facebook account, in which she was portrayed with alcohol in her hands.

These cases are clearly borderline, but the daily use of social media has been continually trending upwards, and most social media users, particularly teenagers (Barnes, 2006; Bringué & Sádaba, 2009), share very private aspects of their identity (Marcus, Machilek & Schütz, 2006; Zimmer, 2010), such as photos and videos, but also texts concerning their habits, experiences, and political views (Krasnova, 2010). The shared information can then rebound from one user to another and become viral, or at least available to an indefinite number of people (Katsabian, 2018), with evident negative consequences when the one who to acquires this information is the employer. Within this context, a paradox arises: social media users tend to consider the information they share on social networks as private until the information leaves the small group of followers with whom the social media users assumed they had exclusively shared the content (Awad & Krishnan, 2006).

What emerges indistinctly from the participation of thousands of users on social media is a new form of control that seems to be needed for personal information shared voluntarily in a semi-public sphere, especially online (Skinner-Thompson, 2017). Precisely in relation to the right to express one's own personality, it seems that one of the reasons for the global success of social network sites is their capacity to allow its users to process their own public identity (Iaquinta & Ingrao, 2014; Tamir & Mitchell, 2012) through the open sharing to a digital audience of a vast range of information, which remains available on the social network and is collectible by other online web databases (Di Fraia, 2012).

With regard to the employer's form of control over employees, these cases raise a series of questions to which the legal experts are invited to respond. The main legal issue concerns the employee's data protection within the employment relationship. Specifically, when any information (i.e., «personal data») relating to the employee, as an identified or identifiable natural person (i.e., «data subject»), is available and processable by the employer, the employee's condition is twofold, as an employee and as a data subject, with the consequence that the contrast between the employer and the employee increases (Rota, 2017). In other words, the usual position of weakness in which the data subject is placed is accompanied by the inherent subordinate position of the employee (Mantelero, 2015; Ruotolo, 2018; Rota, 2017). This convergence between the two different *status* of employee and data subject requires a multilevel approach. For this reason, an orientation has begun to take hold more and more in the doctrine, which raises strong worries about the protection of fundamental personal rights in relation to the diffusion of big data analysis, based on the potential discriminatory practices to which an increased availability of personal data could lead (Tullini, 2016; Kim, 2017).

In this framework, it is interesting to investigate the real legal nature of information shared on social networks to discover if, as personal data, they should enjoy the same kind of data protection. In other words, it is fundamental to understand whether the employer who handles this kind of information, without caution, is committing a violation of data protection (Katsabian, 2018). The second issue under discussion is related to the power of control assigned to the employer and if the type of control that he can exercise through the social networks should be subject to the rules that discipline a lawful employer's control. In a nutshell, in a contest where the employees' rights are increasingly called into question, we must know how to balance the employees' rights and companies' interests.

3. The legal nature of information shared on social networks

The fundamental legal question that must be answered first is about the legal nature of information shared by the data subject itself on social networks.

The General Data Protection Regulation at paragraph 2, letter e) of article 9 regulates the instance by which the *«processing relates to personal data which are manifestly made public by the data subject.»* This hypothesis this could include personal data shared on social networks. In particular, the article 9 of Regulation 2017/679/EU generally prohibits the processing of special categories of personal data (such as those that can reveal: racial or ethnic origin; political opinions; religious or philosophical beliefs; trade union membership; genetic and biometric data through which it is possible to identify a natural person uniquely; data concerning health or a natural person's sex life or sexual orientation) unless —and this is one of the exceptions to the prohibition— the processing relates to personal data which are manifestly made public by the data subject.

In the wording of article 9 of the General Data Protection Regulation, if the data subject makes public his special personal data concerning, for example, his political opinion, that specific personal data can be processed without any apparent limitations. Therefore, it might seem that the right of data protection is a renounceable right —if personal information is published by the data subject, that information can flow freely— but this is not correct. Indeed, the GDPR has to be read according to a systematic interpretation that takes into account first the general principles of safeguarding personal data processing and second, the guidelines, recommendations, and best practices developed by the article 29 Working Party (and in specific its Opinion 2/2017 *«on the processing of personal data in the employment context»*).

The key principle regarding personal data processing is the consent of the data subject, who is not a passive subject, but an active one, and indeed one who has the power of control and intervention (Ogriseg, 2017). Yet the consent in the specific work context cannot be considered unconditional and free due to the imbalance of power that characterizes the employment relationship, as the Opinion 2/2017 expressly highlights at point 6.2 (Ogriseg, 2017): *«Employees are almost never in a position to freely give, refuse or revoke consent, given the dependency that results from the employer/employee relationship. Given the imbalance of power, employees can only give free consent in exceptional circumstances, when no consequences at all are connected to acceptance or rejection of an offer. The legitimate interest of employers can sometimes be invoked as a legal ground, but only if the processing is strictly necessary for a legitimate purpose, and the processing complies with the principles of proportionality and subsidiarity. A proportionality test should be conducted prior to the deployment of any monitoring tool to consider whether all data are necessary, whether this processing outweighs the general privacy rights that employees also have in the workplace and what measures must be taken to ensure that infringe-*

ments on the right to private life and the right to secrecy of communications are limited to the minimum necessary.» For this reason, the consent is not enough, and the consequent principles regulating the personal data processing (in the employment context, but also in general) are aimed at balancing the employee's position of inequality. On the one hand, there are the employee's rights, such as the right to a private life and the right to the confidentiality of communications and, on the other hand, there are the company's legitimate interests; both have to be taken into account in the processing of employee's data.

The other great guiding principle concerns the explicitness and the legitimacy of purpose determining the personal data processing, and the necessity, proportionality, and the transparency of measures adopted for the personal data processing. Specifically, above all, the employees should always have full awareness about the legitimate reasons behind the personal data processing, which in turn *«should be carried out in the least intrusive manner possible and be targeted to the specific area of risks»* (Opinion 2/2017 WP29, 3.1.1 legal grounds (article 7), Legitimate interest (article 7(f)). Along this line, according to article 35 Regulation 2016/679/EU, if a specific type of processing due to its nature, scope, and context is likely to undermine 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»* (article 35 Regulation 2016/679/EU). The GDPR itself imposes the Data Protection Impact Assessment (DPIA) when the employer puts in place *«any form of automated processing of personal data evaluating the personal aspects relating to a natural person, in particular, to analyze or predict aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behavior, location or movements»* (Recital 71 Regulation 2016/679/EU).

Furthermore, the DPIA, according to the WP29, should be adopted if there is *«a company systematically monitoring its employees' activities, including the monitoring of the employees' work station, internet activity, etc...»* (WP29, *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is «likely to result in a high risk» for the purpose of Regulation 2016/679*, of 4 October 2017).

From this general picture of the principles, the personal data collected through the screening of employees' social media profiles represents an extremely interesting circumstance for at least two reasons. First, because the monitoring of social media by the employer can occur even before the establishment of the employment relationship, i.e., during the recruitment phase; second, because of this kind of control, any sort of surveillance can allow the employer to acquire sensitive personal data regarding private opinions, interests, and habits.

In Opinion 2/2017 issued by article 29 Working Party, the oversight of candidates' social media profiles is considered licit only on certain conditions. The personal data collection and processing must be *«necessary and relevant to the performance of the job which is being applied for»* (Opinion 2/2017 WP29, 5.1 *«Processing operations during the recruitment process»*) and *«the individual must also be correctly informed of any such processing before they engage with the recruitment process»* (Opinion 2/2017 WP29, 5.1 *«Processing operations during the recruitment process»*). This means that the employer can screen candidates' social media profiles only in the absence of *«other less invasive manners»* to protect the employer's legitimate interests, and the monitoring must be carried out in a transparent way and be accompanied by the candidate's full awareness.

As a general rule, the Opinion 2/2017 of WP29 states that the employees' personal data, in those cases in which the data collection and processing are allowed, should never be used for illegitimate processing, such as the tracking and evaluation of employees themselves.

For all the above observations, a different approach to the employee as a «data subject» emerges between the GDPR and the Opinion 2/2017 (*«on the processing of personal data in the employment context»*). Indeed, in Regulation 2016/679/EU, the weak position of the employee is not sufficiently considered in terms of protection instruments (Ogriseg, 2017). Nevertheless, the legal nature of personal data voluntarily shared on social networks is undeniably falling within the personal data's definition, and, therefore, their collection and processing are subject to the GDPR regulations.

The Regulation 2016/679/EU at article 88 par. 1 assigns to the member States the competence to provide, by law or by collective agreements, more specific rules to ensure the protection of the rights and the freedoms in the processing of employees' personal data, in particular for the purposes of: recruitment; performance of the employment contract, including the discharge of obligations laid down by law or by collective agreements; general and specific organization of work; equality and diversity in the workplace; health and safety at work; protection of employer's or customer's property; the exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment; and the termination of the employment relationship. As highlighted by the article 88 of the Regulation 2017/679/EU, the employee's right to data protection must cover a wide timeframe

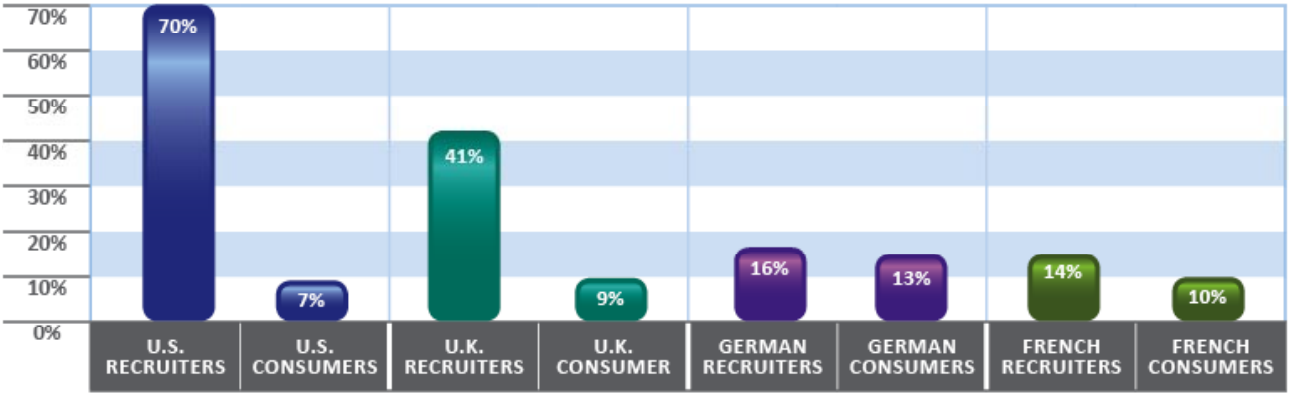
for the employment relationship, starting from the recruitment phase, when the employment relationship has not even been established (Sprague, 201; Online Reputation in a Connected World, 2010). Indeed, according to research commissioned by Microsoft (Online Reputation in a Connected World, 2010), recruiters are deciding more and more to accept or reject a job application after consulting the information about the candidates available on the web. Recruiters expect that within the next five years, this trend will significantly increase (Online Reputation in a Connected World, 2010).

As can be observed from the diagram below, candidates often tend to underestimate the relevance that their own online reputation could have to their professional future, considering that personal information accessible on the web is reviewed increasingly often during the recruitment process. This phenomenon is particularly widespread, although with different incidences, in the countries covered by this research.

Specifically, in the United States and England, there is a wide gap between the impact of online data on professional careers perceived by the surveyed consumers and the percentage, admitted by the interviewed recruiters, of cases where an application was rejected based on data found online. The perception of consumers interviewed about the impact of their online reputation and the statements of the recruiters correspond more closely in Germany and France. Indeed, *«in Germany, 13% of consumers surveyed believe information found online about them could influence a hiring decision. Their perceptions closely parallel the 16% of recruiters and HR professionals surveyed who report having rejected candidates based on information they found online. Similarly, 10% of French consumers surveyed believe information about them online could affect their hiring while 14% of recruiters and HR professionals report they have rejected a candidate based on that information»* (Online Reputation in a Connected World, 2010).

Table 1

Recruiters and HR professionals who have rejected candidates based on data found online *vs.* consumers who think online data affected their job search (Cross-tab trasforming market services. (2010). Online Reputation in a Connected World. Retrieved from https://www.job-hunt.org/guides/DPD_Online-Reputation-Research_overview.pdf)



An interesting aspect, highlighted in the table below, concerns the nature of the information that has the greatest impact on the final decision to reject a job application. In point of fact, the information that appears to have a particularly negative impact is of a strictly personal nature, such as lifestyle, previous economic status, inappropriate comments, and photos.

Table 2

Types of online reputational information that influenced decisions to reject a candidate (Cross-tab trasforming market services. (2010). Online Reputation in a Connected World. Retrieved from https://www.job-hunt.org/guides/DPD_Online-Reputation-Research_overview.pdf)

Types of Online Reputational Information That Influenced Decisions to Reject a Candidate				
	U.S.	U.K.	Germany	France
Concerns about the candidate's lifestyle	58%	45%	42%	32%
Inappropriate comments and text written by the candidate	56%	57%	78%	58%
Unsuitable photos , videos, and information	55%	51%	44%	42%
Inappropriate comments or text written by friends and relatives	43%	35%	14%	11%
Comments criticizing previous employers, co-workers, or clients	40%	40%	28%	37%
Inappropriate comments or text written by colleagues or work acquaintances	40%	37%	17%	21%
Membership in certain groups and networks	35%	33%	36%	37%
Discovered that information the candidate shared was false	30%	36%	42%	47%
Poor communication skills displayed online	27%	41%	17%	42%
Concern about the candidate's financial background	16%	18%	11%	0%

It is reasonable to assume that online resources, such as social network sites, allow recruiters to become aware of that category of information about which questions cannot be asked, but which are of interest to the employer because they could reveal elements of the candidate's personality that could potentially conflict with the company's values (Cara, 2011).

The statistics mentioned above show the spread of the phenomenon, to such an extent that in 2010, a proposal was submitted in the German legal system to amend the Federal Workers' Data Protection Act, with the scope to prohibit recruiters from processing candidates' data on social networks, even if the data itself is public unless the candidate has given his or her consent to the processing (German Federal Data Protection Act in the version of the government draft of the Federal Workers' Data Protection Act of 15.12.2010, BT-Drucks. 17/4230, article 1, paragraph 7, number 6). The proposed amendment to the Federal Workers' Data Protection Act was rejected by parliamentary opposition and, therefore, the so-called phenomenon of «social recruitment» has not found a legislative solution in the German legal system, leaving unresolved many legal issues about which the European doctrine in general still has many questions (Finkin, Krause & Okuno, 2015).

The questions raise concerns, in general terms, about the legitimacy of such research carried out by the employer on the Internet, and particularly on social network sites, during the selection of personnel. For instance, some doubts arise about the conditions to which the «social recruitment» should be subject and if any information circulating on the network concerning the candidate is likely to be processed by the employer. On closer inspection, the nature of the information is not at all a secondary aspect, considering that strictly personal and intimate information is very often easy to find on the Internet, with the consequence that precisely this kind of information, linked to the applicant's most private sphere, could lead to exclusion on

Núm. 18 zk./2020. Págs. 154-169 or.
ISSN: 2173-6405 e-ISSN: 2531-2103

purely discriminatory grounds. If the Internet should reveal that the potential new employee is homosexual, this sensitive data should not play a role in the recruitment decision (Oberwetter, 2008). Still, the candidate would hardly be made aware of the actual reason why he/she was discarded, with the consequence that he/she would be unable to appeal against the refusal and assert his/her reasons in legal proceedings (Forst, 2010). For this reason, there is still no case law on the hypothesis of rejection of applications based on information about the candidate found online by the employer (Finkin, Krause & Okuno, 2015).

As seen, this trend, called «potential employee's vetting», raises several legal issues, even if formally, the employer is not legally required to justify a candidate's rejection. Yet, at the same time, the extended protection provided by the Regulation 2017/679/EU, going from the recruitment phase to the termination of the employment relationship, reflects a sophisticated vision of personality, which is also a result of an evolution of German case law (Finkin, 2010), according to which, the right to express one's own personality must be guaranteed by sufficient data protection within and outwith the contractual performance (Del Punta, 2019). In other terms, the new technological context suggests the need to safeguard the employee's person, not only inside the working environment, considered in a strict sense, but to rethink the borders of the employment relationship since the purpose of most common technologies is to break down the spatial and temporal limits.

This last aspect, concerning the protection of rights and freedoms in the processing of employees' personal data for the termination of the employment relationship, is the key issue underlying the increasingly frequent cases in which the employer's legitimate interests and the employee's fundamental rights and freedoms conflict to such a degree that the employee loses his job.

4. The action of member States: Spain and Italy in comparison

Regarding Spain's experience, on 21 November 2018, a large majority of the Spanish Senate approved the Organic Law Act on data protection and digital rights guarantee (LOPDGDD), which was adopted on 6 December 2018. This legislative intervention has the merit of enhancing the security guarantees of the employee's personal data in the digital employment context. Particularly, it sets out in article 87 to 91 five fundamental provisions aimed at clarifying the digital employee's rights in relation to: the use of digital tools; the video and audio surveillance; the use of geolocation systems; the right to disconnection from work-relating electronic communications; and the new digital area's rights in collective bargaining (Bel Antaki, 2018).

The organic law on data protection and digital rights guarantee (LOPDGDD) does not expressly consider the case of dismissal due to unbecoming digital conduct. Still, it does regulate the collection and the processing of employees' personal data related to the use, for private purposes, of digital devices provided to the employees themselves for the fulfillment of the job duties, as well as the right to disconnection. According to article 87, n. 3, paragraph 2: *«the employees' use of digital devices for private purposes must be authorized, and guarantees to protect employees' privacy must be established with the involvement of employees' legal representatives, such as, if applicable, the specific indication of timing when the use of devices for private purposes is allowed; only then the employee can access to their contents.»* This recognition may be the most significant innovation in the employees' digital rights because, for the first time in Spain, it was officially ruled that off-hours should be sheltered from continuing work-related solicitations from the web (Weiss, 2016; Perrone, 2017).

Another interesting issue for the Spanish legislator, in which the work-life borders are questioned by the pervasive use of IT tools, is the case of employees' video surveillance and audio recording (with an explicit ban to install cameras in areas destined for the employees' rest). The requirement to provide explicit, clear and concise information is stressed as a general principle. Still, the law at article 89 n. 1 paragraph 2, foresees a mitigation of the disclosure requirement if an employee's infringement is captured. Indeed, if a worker's infringement is registered, the duty of information is considered accomplished by placing an informative symbol, in a visible space, that indicates the possibility of surveillance, the identity of the data handler, and the faculty of exercising the rights of access, rectification, erasure, and restriction of processing, provided for in articles 15 to 22 of Regulation (EU) 2016/679, such as an internet link to this information that may be provided.

From the analysis of the Spanish organic law on data protection and digital rights guarantee emerges a legislative consciousness-raising about the danger of a

mutual permeability between working and private life to which the immoderate use of electronic devices may lead. To weigh the adverse interests of the employee and the employer, the Spanish legislator has provided a system of safeguards and corresponding mitigations.

With reference to the collection and processing of an employee's personal data, which is somehow related to the private sphere of the employee himself, the organic law considers three cases: the minimum protection standards for the case of electronic devices' use for private purposes in the workplace; the necessity to preserve the rest hours from working electronic communications; and the ban on surveillance of the employee in the zones designated for the employees' rest, such as locker rooms, toilets, dining rooms, and similar (Bel Antaki, 2018). In response to such protective measures, the Spanish organic law on data protection and digital rights guarantee provides for the above mitigation to the disclosure's duty in the case in which an employee's infringement is registered. In this case, it is evident that the priority is granted to the employer's interests in preserving the industrial property and connected goods, in that the employer is required to place an informative symbol with only the essential indications. This provision, if extensively interpreted, could legitimate other cases of collection and processing of employees' personal data through safeguards' alleviated modalities (cases which could receive a mitigated protection), such as the hypothesis of personal data collected through the screening of employees' social media profiles, given that this kind of information is voluntarily published by the employee himself and is not the result of work-context supervision (in fact, as specified above, according to a *stricto sensu* interpretation, they would be covered by article 9 of Regulation 2017/679/EU).

Regarding the Italian experience, the legislative decree of 10 August 2018 has transposed the GDPR's novelties in the Italian privacy codex (Cuffaro, 2018) by consequently harmonizing the discipline in the field of employer's forms of controls, a subject regulated in the Italian legal system in article 4 of the workers' statute (Law Act n. 300 of 1970). This provision has been modified by the legislative decree n. 151/2015.

According to the previous version of article 4 of Italian workers' statute, the installation of audio-visual equipment and other tools aimed solely at the employees' control was prohibited unless 1) the installation of these instruments was necessary to safeguard the organizational needs and production requirements, such as those of work safety and the protection of corporate asset; and 2) as long as a trade-union agreement or, failing that, the territorial Italian Labor Direction authorized the installation in this regard. The legislative decree n. 151/2015 has modified the paragraph 2 of article 4, introducing a derogation to the authorization procedure, which establishes that such authorization is not necessary when the instruments are intended to be used by the employee to carry out the job performance or to register the employees' access and attendances.

In 2016 (the following year of the entry into force of the legislative decree n. 151/2015), the legislator intervened once more in paragraph 3 of article 4 of Italian workers' statute with the legislative decree n. 185/2016, ruling that the employee's personal data, when lawfully collected (according to the paragraphs 1 and 2), can be processed, with respect to the Italian privacy codex, for any of the purposes related to the employment relationship, provided that the employee has been previously and properly informed about how these controls are carried out (Rovignoli, 2018).

The legislative decree of 10 August 2018, implementing in the Italian legal system of the Regulation (EU) 2016/679, substantially confirmed a sanction system that the legislative decree n. 151/2015 had already established in the case of infringements to the provisions of article 4 of Italian workers' statute about employer's power of control. Indeed, in the case of infringements on the provisions regulating the employer's control in the work context and investigations into the employee's political, religious, or trade union-related opinions, as well as issues not relevant for the evaluation of the professional attitude, the employer is punished (unless the fact constitutes a more serious crime) with a minimum fine of 154 € to a maximum of 1.549 € or with an arrest from a minimum of 15 days to a maximum of a year (article 38 of Italian workers' statute, Law Act n. 300 of 1970).

From the analysis of the Italian legislative decree of 10 August 2018, the preference of the Italian legislator emerges for the imposition of administrative fines for injuries of data protection in the employment context. As a matter of fact, the same Regulation (EU) 2016/679 at article 83 lays down a maximum standard (from 10.000.000 € to 20.000.000 € or, in the case of an undertaking, 2% to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher), to which amount each European member State must adapt their legislations (Vásquez & Suhren, 2018) as a sanction. This is also applicable to public authorities, because of incompliance with the GDPR's specific provisions, except for the articles of the Regulation (EU) 2016/679 concerning the working relationship. Indeed, the case of infringements on the provisions preserving the employee's personal data falls under the article 84 of Regulation (EU) 2016/679,

which states that: *«each member State shall lay down the rules on other penalties applicable to infringements of the GDPR for infringements which are not subject to administrative fines pursuant to article 83; these penalties shall be effective, proportionate and dissuasive, and the member State shall take all measures necessary to ensure that the sanctions are implemented.»*

With reference to the Spanish organic law on data protection and digital rights guarantee (LOPDGDD), this source of law does not seem to have given effect to article 84 Regulation (EU) 2016/679, introducing a specific penalty system for those cases in which the employer, as data controller, does not observe the limits in collecting and processing employees' personal data. The Spanish courts will have to clarify if it is licit to sustain that provisions must be applied to the employer, in the role of the data controller, regarding the sanctions' system for general infringements of the GDPR's provisions and the national implementation's norms of Regulation (EU) 2016/679 itself.

In conclusion, from the above comparison between the Italian and the Spanish legal system on the subject of personal data collection and processing in the employment context, it is reasonable to assume that in both legal systems, the employer must observe «preventive» prescription. The employee must be informed, and the consent of trade union representatives must be released.

It is to be hoped that in both legal systems, effective implementation will be given to the discloser's duty and that the trade union representatives and data processing authorities will supervise and eventually impose the relative fines in case of infringements, in order to apply the principle of effectiveness.

5. The role of supervisory authorities

As has already emerged in the context of the reflection above, the role of national supervisory authorities is crucial in several respects, not only in relation to the supervisory power over compliance with the provisions introduced by the Regulation (EU) 2016/679 but also in terms of promoting a legal culture of sensitive data protection (Pizzetti, 2018).

The first fundamental role reserved to the supervisory authorities is to monitor the data processing. Indeed, the data controller is obliged, first of all, to notify the national supervisory authority promptly of any violation that occurred in the processing of data. The authority is also attributed, pursuant to Art. 41, 35, and 36 Regulation (EU) 2016/679, a role of monitoring the codes of conduct and assessing the impact of possible treatments carried out with the aid of new technologies.

The most innovative role that the Regulation (EU) 2016/679 assigns to the national supervisory authority is introduced by Art. 57 letter i), which provides that *«each supervisory authority shall on its territory monitor relevant developments, insofar as they have an impact on the protection of personal data, in particular, the development of information and communication technologies and commercial practices.»*

This provision confirms the renewed role of national supervisory authorities as careful controllers of compliance with the new European provisions on data processing, but also as vigilant surveillance of possible new protection needs arising from the forthcoming technologies.

6. Ancillary obligations in a work contract

In reference to the exanimated cases of dismissals due to unbecoming digital conduct, another legal issue involved in the present analysis appears, namely: What are the borders of working obligation? How must the eventual ancillary obligations be individuated? And on the basis of which normative assumption can the working obligation, and the ancillary obligations that belong to it, be considered claimable beyond the spatial and temporal border of the relationship? In other words, regarding the above cases: Is it legitimate to expect that the employee to behave responsibly on his own private social media profiles?

The answer to these questions requires thought on the civil law related concept of working contract.

The first doctrine assumed that the element of the *intuitus personae* prevailed in the employment contract and that the employment relationship would arise from the employer's personal satisfaction to the employee (Angela, 2010; Persiani, 1971; Napoli 1980). According to the opposite theory, job performance would not involve aspects of the employee's personal iden-

tity, such as gender identity, political opinion, and sexual orientation (De Luca Tamajo, Carinci, Tosi & Treu, 2016).

According to the first theory, the employment contract's component of loyalty could be prejudiced by facts and behaviors not directly related to job performance. For this reason, dismissals on the ground of conduct related to the employee's personal sphere could be considered licit. According to the second reconstruction, however, only the working performance restrictively considered is the object of the contract, and any private conduct could justify a lawful dismissal.

Part of the European doctrine embraces an intermediary reconstruction, a thesis also adopted by the European Court of Human Rights (European Court of Human Rights, Grand Chamber, ruling of 5 September 20187 case of *Bărbulescu v. Romania*. *Mantouvalou*, n. of application: 61496/08). According to this assumption, only the ancillary obligations related to employee performance could justify a lawful dismissal due to off-duty conduct. From this point of view, first, the contract's component of loyalty would be very relevant, considering that the alleged violation would be qualified as a breach of contract (in terms of ancillary obligations). Second, to evaluate the seriousness of the conduct, it would be necessary to privilege the specificities of every singular and concrete case to identify the ancillary obligation reputed as infringed by the employer.

Essentially, the court seised to assess the legitimacy of a dismissal based on off-duty conduct, should first check, considering the specific position held by the employee, whether the employee is under that specific ancillary obligation, set as the dismissal's justification, and if so, whether the ancillary obligation can be considered breached by the employee's conduct. Therefore, only a case by case evaluation that takes into account each concrete circumstance can establish if the dismissal based on off-duty conduct is proportional. Factors to be considered are: the position of the employee in the company; the degree of reliance required by the tasks carried out by the employee himself; the enterprise's nature run by the employer; the duration of the abuse; content and transparency of the company's policy (Del Punta, 2019).

In conclusion, a dismissal based on off-duty conduct is lawful only if the infringement is one which causes a serious, current, manifest, and negative impact on employer business interests and if the dismissal is proportional as a punitive measure to the transgression (Mantouvalou, 2008).

7. Public sector and social networks

The processing of data by public administrations poses further legal questions for two main reasons: first, because public administrations can collect data provided directly by the citizens, and second because on the basis of legislative provisions, public administrations are entitled to collect *ex officio* data from the users of public office services (Costantino, 2019). The availability by public administrations of large quantities of data, even if stored in different databases but very often related by means of algorithms capable of predicting future needs and social behaviors (Kerr, Earle, 2014) , can be in contrast with data protection and citizens' privacy (Costantino, 2019). The difficult balance between public interests and the protection of individuals' data is therefore necessary, since forms of discrimination based on data processing and automated choices, based on algorithms, could occur. For instance, if the data collection by public administrations is established by a legislative provision, the consent of the data subject is not required, moreover, public administrations, can often become aware of strictly personal aspects of individuals by means of crossing of data (Costantino, 2019).

The Regulation (EU) 2016/679 has also intervened to regulate this matter with the intent of limiting the risks inherent in the processing of data by public administrations, which, like private companies, deal with both the data of external users to whom the public services are addressed and the data of their employees. Public administrations are called to take a series of measures to increase the degree of security and transparency that their users' data are processed (Del Pizzo & Lo Bello, 2018). Most importantly, the Regulation establishes that the processing of data by public administrations can only take place on the basis of the law and for the exercise of public functions. On closer inspection, however, where there is a reason of public interest, the requirement of the legislative provision that legitimises data treatment is no longer present (Gatt, Montanari, & Caggiano 2017).

Public administrations are to do so through methods such as: the designation of a Data Protection Officer and expert in privacy management (art. 37 GDPR); the adoption of a Register of processing activities; the preparation of information for the acquisition of consents; a risk and impact analysis system for any violations.

Núm. 18 zk./2020. Págs. 154-169 or.
ISSN: 2173-6405 e-ISSN: 2531-2103

The innovations introduced by the Regulation (EU) 2016/679 also concern the category of data processing carried out by the public administration in regards to its employees. Indeed, manifestations of the court cases considered so far are also recorded in the public sector, which, due to the peculiarities that distinguish it —such as, above all, the protection of the public interest— requires a further reflection (Guarnaccia, 2017). Interesting Italian and Spanish jurisprudential rulings have had to face controversies regarding, for instance, the value to be attributed to a «Facebook friendship» as a cause of incompatibility of a commissioner in a public competition (Regional Administrative Court of Sardinia, sec. I, ruling of 3 Mai 2017, n. 281 & Regional Administrative Court of Liguria, sec. II, ruling of 3 September 2014, n. 1330); or the configurability as a disciplinary offense of sharing photographs of the state of the workplace by a civil servant on his Facebook profile (Regional Administrative Court of Friuli Venezia Giulia, ruling of 12 December 2016, n. 562).

As already mentioned, for the rulings in relation to private work relationships, the aforementioned cases also reveal in the public sector the category of off-duty behaviors conducted by the employee on the net, often attributable to the manifestation of his own thoughts, to which an injury to the employer's image can be traced back and, in the case of public administration, to the dignity of the administration (Guarnaccia, 2017).

On the subject of criticisms expressed by a public official considered damaging to the image of the function held, the Italian Court of Cassation was invested with the question of the legitimacy of a sanction imposed on a judge for having openly criticized the Mayor of Rome from his Facebook profile (Joined Chambers of the Italian Court of Cassation, ruling of 31 July 2017, n. 18987). In a similar situation, a Spanish official of the municipal police of Tías was subject to the sanction of a suspension for six months from the service for having expressed on Facebook critical statements against the mayor (Superior Court of Justice of Las Palmas de Gran Canaria, Contentious Chamber, sec. I, ruling of 10 Juli 2018, n. of complaint: 372/2017 (resolution n. 404/2018)).

The phenomenon in question, as can be seen, occurs both in the private sector and in the public sector, with the difference that in the public sector, the public official is, by force of law obliged, to refrain from any behavior that could damage the dignity and prestige of the administration.

In this context, it is interesting to note that some rulings considered decisive the settings for the access by virtual friends and third parties to the contents shared on the net by the worker himself. Indeed, the behavior would be less detrimental if the online content could only be viewed by a restricted number of people and under certain conditions. Conversely, the employee's conduct would be more harmful if the activity on the net were easily available to other users (Council of State, sec. III, ruling of 21 February 2014, n. 848). From the picture outlined so far, it is clear how often the dismissal's hypotheses for the online off-duty conduct of the worker are starting to be registered in the public administration. In the face of the relevant public interests that an employee's online conduct could affect, the Italian legislator has provided for public administrations to implement personnel training aimed at the knowledge and use of information and communication technologies by civil servants (art. 13 of the digital administration code). In addition, some Italian and Spanish administrations have begun to acquire so-called social media policies, or specific regulations governing the use of social platforms by employees.

8. Conclusions

The new scenario of work digitalization will increasingly call into question most of the fundamental employees' rights, such as the right to rest, the right of association, and the freedom of expression.

Regarding the cases of dismissal due to online private conducts considered above, it is evident that the impressive spread of social media, making the worker's personal data (concerning lifestyle, personal opinions, or even political and sexual orientations) easily available on the web, ends up satisfying the employer's tendency to collect as much information as possible about the candidates or employees. In other words, the employer is now able to obtain a large amount of information simply by typing the candidates' or employees' names into a search engine and, on the basis of this information, he is then very often persuaded to take measures, which he would not otherwise have taken, about the future course of the employment relationship.

As can be seen, the phenomenon also shows manifestations in the public sector. In this respect, given that the interests at stake are of public nature, the legislator has already proceeded, in part, to dictate guidelines that could lead the future efforts of public administrations regarding the private use by public employees of social networks.

Among the most relevant initiatives, there is the possible establishment of courses for public employees aimed at raising their awareness of the risks inherent in the use of social networks and clarifying the precautions to be taken to make one's own activity on the net least harmful to the image and prestige of the public administration. In this sense, many employers have also adopted company policies or codes of conduct regulating the use of these electronic tools by the employee in his private sphere. If, on the one hand, these forms of self-regulation can offer a valuable tool to reduce the risk of unlawful data processing, on the other hand, the legislative initiative should be aimed at guaranteeing a greater transparency in data processing, especially when this is implemented by public administrations.

Indeed, it is interesting to observe that data processing by public administrations is becoming more and more a concrete reality, despite the fact that a capillary regulation has not yet been provided by either the European or the national legislator (Costantino, 2019). On this point, the Regulation 2017/679/EU provides formal and substantive conditions which public administrations must observe in order to guarantee a legitimate data processing. However, some fundamental legal aspects are left unresolved, especially in relation to those hypotheses of data processing that do not require the consent of the data subject because they are required by law.

On the privacy and data protection side, as regards both private and public employment relationships, the recent provisions introduced by the Regulation 2017/679/EU also extend the application of the general principles to the processing by the employer of worker's data. In this regulatory framework, therefore, despite the controversial nature of the information voluntarily shared on the network, the data available on the employee's social websites cannot be processed by the employer without the prior consent of the worker, to whom the purposes (which must be legitimate) of the treatment must also be known. In this sense, the measures introduced by the Regulation 2017/679/EU on data processing have the clear objective of setting a juridical defense against an employer's arbitrary intrusions.

The discussion on the recognition of worker data protection in the increasingly penetrating technological context must also be accompanied by an investigation into the contractual boundaries of the working performance and contractual obligation. Indeed, in this scenario, it is urgent not only to ask what regulatory requirements the employer must observe whenever a worker's data processing is necessary, but also what repercussions the private conduct of the employee could have on the employment relationship and, in particular, on the image of the employer.

To conclude, the topic analyzed here raises multiple legal issues, the solution for which often involves the balancing of conflicting interests. On the one hand, the absence of specific regulation of the matter cannot lead to illicit processing of the employee's data by the employer. On the other hand, the worker's openly visible activity on the net should not be harmful to the image of the employer.

Therefore, the most appropriate way forward appears to be to ensure the implementation of the provisions laid down by the Regulation 2017/679/EU within the employment relationship and to empower the employees on the private use of social networks, offering courses or adopting internal regulations about the use of social platforms.

The regulation of data processing in the context of employment relationships, both private and public, is left to the competence of each member State in accordance with the provisions of art. 88 of the Regulation 2017/679/EU. In the light of the considerations, the legislative path that seems to be most desirable is that of a regulation, shared with the social partners and the supervisory authorities, which guarantees the protection of the worker's data throughout the entire duration of the relationship (including the staff selection phase), recognizing a private space for the employees, in which they can freely express their thoughts, but which also sets out measures of a deterrent nature that dissuade the worker from using any expression that could cause unfair damage to the image of the employer.

9. References

ARTICLE 29 DATA PROTECTION WORKING PARTY. (2017). Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is «likely to result in a high risk» for the purposes of Regulation 2016/679 (Adopted on 4 April 2017 As last Revised and Adopted on 4 October 2017).

Awad, N.F., & Krishnan, M.S. (2006). The Personalization Privacy Paradox: An Empirical Evaluation of Information Transparency and the Willingness to be Profiled Online for Personalization. *MIS Quarterly*, 30(1), 13-28.

Barnes, S.B. (2006, September). A Privacy Paradox: Social Networking in the United States. *First Monday*, 11(9). doi: https://doi.org/10.5210/fm. v11i9.1394.

Bel Antaki, J. (2018, 11 December). The digital privacy of employees: a key concern in the new Spanish data protection law. [Blog post]. Retrieved from https://blog.cuatrecasas.com/laboral/digital-privacy-of-workers-data-proctection-lopd/?lang=en.

Brandtzæg, P. B. & Heim, J. (2009). Why People Use Social Networking Sites. In A.Ant Ozok & Panayiotis Zaphiris (Ed.s), *OCSC Online Communities and Social Computing. Lecture Notes in Computer Science*, 5621, (143-152). Berlin, Heidelberg: Springer.

Bringué, X. & Sádaba, Ch. (2009). La generación Interactiva en España. Niños y jóvenes ante las pantallas. Barcelona: Colección Fundación Telefónica, Ariel. https://www.researchgate.net/publication/40902023_La_generacion_interactiva_en_Mexico_Ninos_y_adolescentes_frente_a_las_pantallas/citations.

Cara, R.S. (2011). The References of the Twenty-First Century: Regulating Employers' Use of Social Networking Sites as an Applicant Screening Tool. *Southern Illinois University Law Journal*, 35, 499-516.

Carinci, F., Tosi P., Treu T., De Luca Tamajo R. (2016). *Diritto del lavoro. Il rapporto di lavoro subordinato*. Vol. II. Torino: Giuridica.

Colucci, M. (2002). The Impact of the Internet and New Technologies on the Workplace. A Legal Analysis from a Comparative Point of View. In Roger Blanpain (ed.), *Bulletin of Comparative Labour Relations*, 43, xi-186. The Hague/London/New York: Kluwer Law International.

Costantino, F. (2019). Rischi e opportunità del ricorso delle amministrazioni alle predizioni dei «big data». *Diritto Pubblico*, (1), 43-70.

Council of State, sec. III, ruling of 21 February 2014, n. 848.

Cuffaro, V. (2018). Quel che resta di un codice: il D.Lgs. 10 agosto 2018, n. 101 detta le disposizioni di adeguamento del codice della privacy al regolamento sulla protezione dei dati. *Corriere giuridico*, (10), 1181-1185.

Del Pizzo, L. & Lo Bello, P. (2018, May 17) GDPR nella PA, la lezione del MEF per adegaursi. *Agenda digitale*. Retrieved in: https://www.agendadigitale.eu/sicurezza/privacy/gdpr-il-piano-di-adeguamento-per-le-pubbliche-amministrazioni/.

Del Punta, R. (2019). Social Media and Workers' Rights: what is at Stake? *International Journal of Comparative Labour Law and Industrial Relations*, 35(1), 79-100.

Di Fraia, G. (2012). Social network e racconti identitari. *Minorigiustizia*, 4, 14-20.

European Court of Human Rights, Grand Chamber, ruling of 5 September 20187 case of *Bărbulescu v. Romania. Mantouvalou*, n. of application: 61496/08.

Finkin, M.W. (2010, 29 March). Some Further Thoughts on the Usefulness of Comparativism in the Law of Employee Privacy. *Employee Rights & Employment Policy Journal*, 14, 101-146.

Finkin, M.W., Krause, R. & Okuno, H.T. (2015). Employee autonomy, privacy, and dignity under technological oversight. In M.W. Finkin & G. Mundlak (Ed.s), *Comparative Labor Law* (153-194). Cheltenham, Northampton: Edward Elgar Publishing.

Forst, G. (2010). Bewerberauswahl über soziale Netzwerke im Internet?. *Neue Zeitschrift für Arbeitsrecht (NZA)*, 427-433.

Gabriele, A. (2010). Giusta causa oggettiva di licenziamento e inidoneità morale sopravvenuta: brevi riflessioni. *In Rivista italiana di diritto del lavoro,* (1/2), 40-48.

Gatt, L., Montanari, R. & Caggiano, I.A. (2017). Consenso al trattamento dei dati personali e analisi giuridico-comportamentale. Spunti di riflessione sull'effettività della tutela dei dati personali. *Politica del diritto*, (2), 363-379.

German Federal Data Protection Act in the version of the government draft of the Federal Workers' Data Protection Act of 15.12.2010, BT-Drucks. 17/4230, article 1, paragraph 7, number 6.

Guarnaccia, C. E. (2017). La prima giurisprudenza sul rapporto tra pubblico impiego e social media. *Informatica e diritto*, (1-2), 367-382.

Iaquinta, F. & Ingrao, A. (2014). La «privacy» e i dati sensibili del lavoratore legati all'utilizzo di «social networks». Quando prevenire è meglio che curare. *Diritto delle relazioni industriali*, 4, 1027-1028.

Joined Chambers of the Italian Court of Cassation, ruling of 31 July 2017, n. 18987.

Katsabian, T. (2018, 29 March). Employees' Privacy in the Internet Age – Towards a New Procedural Approach. *Hebrew University of Jerusalem Legal Research*, 18-19, 203-255. doi: http://dx.doi.org/10.2139/ssrn.3152404.

Kerr, I., Earle, J. (2014). *Prediction, Preemption, Presumption: How Big Data Threatens Big Picture Privacy*, *Stanford Law Review Online*, 66, 65-72.

Kim P.T. (2017, 19 April). Data-Driven Discrimination at Work. *William & Mary Law Review*, 58(3), 857-936. Retrieved from https://ssrn.com/abstract=2801251.

Krasnova, H., Spiekermann, S., Ksenia, K. & Hildebrand T. (2010). Online Social Networks: Why We Disclose. *Journal of Information Technology,* 25(2), 109-125.

Law Act of 20 may 1970, n. 300, rules on the protection of workers' freedom and dignity, trade union's freedom and activity, in the workplace and rules on employment (Official Gazette n. 131 of 27/5/1970).

Mantelero, A. (2015). Rilevanza e tutela della dimensione collettiva della protezione dei dati personali. *Contratto e impresa. Europa*, 1, 137-158.

Mantouvalou, V. (2008). Human Rights and Unfair Dismissal: Private Acts in Public Spaces. *Modern Law Review,* 71/6, 912-939. doi:http://dx.doi.org/10.1111/j.1468-2230.2008.00722.x.

Mantouvalou, V. (2014). The Protection of the Right to Work Through the European Convention on Human Rights. *Cambridge Yearbook of European Legal Studies*, 16, 313-332. doi: https://doi.org/10.1017/S1528887000002639.

Marcus, B., Machilek, F. & Schütz, A. (2006). Personality in Cyberspace: Personal Web Sites as Media for Personality Expressions and Impressions. *Journal of Personality and Social Psychology,* 90(6), 1014-1031.

Mills M. (2017). Sharing privately: the effect publication on social media has on expectations of privacy. *Journal of Media Law*, 9(1), 45-71.

Miño-Vásquez, V. & Suhren, P. (2018). Liability for injuries according to GDPR. Datenschutz Datensich, 42, 151-155. doi: https://doi.org/10.1007/s11623-018-0926-0.

Nadkarni, A., & Hofmann, S. G. (2012). Why Do People Use Facebook? *Personality and individual differences*, 52(3), 243-249. doi: https://doi.org/10.1016/j.paid.2011.11.007.

Napoli, M. (1980). *La stabilità reale del rapporto di lavoro*. Milano: Franco Angeli.

Oberwetter, C. (2008). Bewerberprofilerstellung durch das Internet – Verstoß gegen das Datenschutzrecht?. *Betriebs-Berater (BB)*, 29, 1562-1566.

Ogriseg, C. (2017). GDPR and Personal Data Protection in the Employment Context. *Labour & Law Issues,* (2), 1-24. Retrieved from: https://labourlaw.unibo.it/article/view/7573.

Cross-tab trasforming market services (2010). Online Reputation in a Connected World. Retrieved from https://www.job-hunt.org/guides/DPD_Online-Reputation-Research_overview.pdf

Organic Law Act of 6 December 2018 on data protection and digital rights guarantee (LOPDGDD), n. 3/2018.

Perrone, R. (2017). Il «diritto alla disconnessione» quale strumento di tutela di interessi costituzionalmente rilevanti. *federalismi.it,* 24, 1-20. Retrieved from: https://www.federalismi.it/ApplOpenFilePDF.cfm?artid=35324&dpath=document&dfile=17122017194655.pdf&content=Il%2B%27diritto%2Balla%2Bdisconnessione%27%2Bquale%2Bstrumento%2Bdi%2Btutela%2Bdi%2Binteressi%2Bcostituzionalmente%2Brilevanti%2B%2D%2Bstato%2B%2D%2Bdottrina%2B%2D%2B.

Persiani, M. (1971). La tutela dell'interesse del lavoratore alla conservazione del posto. In L. Riva Sanseverino L. & G. Mazzoni (Eds), *Nuovo trattato di diritto del lavoro*, (Vol. II, 678-681). Padova: Cedam.

Phlips, L. (1988). *The economics of imperfect information*. Cambridge, New York: Cambridge University Press.

Pisani, C. (2009). La hostess «allegra»: licenziamento per inidoneità morale. Massimario di giurisprudenza del lavoro, 5, 324-38.

Pizzetti, F. (2018). La protezione dei dati personali dalla direttiva al nuovo regolamento: una sfida per le Autorità di controllo e una difesa per la libertà dei moderni. *La rivista di diritto dei media*, (1), Retrieved from: http://www.medialaws.eu

Regional Administrative Court of Friuli Venezia Giulia, ruling of 12 December 2016, n. 562.

Regional Administrative Court of Liguria, sec. II, ruling of 3 September 2014, n. 1330.

Regional Administrative Court of Sardinia, sec. I, ruling of 3 Mai 2017, n. 281.

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).

Rota, A. (2017). Rapporto di lavoro e big data analytics: profili critici e risposte possibili. *Labour & Law Issues,* 3(1), 32-52. doi:10.6092/issn.2421-2695/6861.

Rovignoli, C. (2018, September 21). Il D.Lgs 101/2018 attuativo del GDPR. I controlli a distanza del lavoratore: novità o conferma dell'impianto normativo?. [Blog post]. Retrieved from http://www.studiolegaleroviglioni.it/2018/09/21/il-d-lgs-101-2018-attuativo-del-gdpr-i-controlli-a-distanza-del-lavoratore-novita-o-conferma-dellimpianto-normativo/.

Ruotolo, G.M. (2018). I dati non personali: l'emersione dei big data nel diritto dell'Unione europea. Studi sull'integrazione europea, 1(XIII), 97-116. Retrieved from https://www.studisullintegrazioneeuropea.eu/Scarico/Rivista%20Studi%200118.pdf.

Salazar P. (2015). «Facebook» e licenziamento per giusta causa: quando si travalicano i limiti del privato influendo sul rapporto di lavoro. Il lavoro nella giurisprudenza, (8-9), 838-843.

Salazar, P. (2015). Facebook e rapporto di lavoro: quale confine per l'obbligo di fedeltà. *Il lavoro nella giurisprudenza,* 3, 291-296.

Sanseverino R. L. (1978). *Diritto del lavoro* (13th ed.). Padova: CEDAM.

Skinner-Thompson, S. (2017). Performative Privacy. *UC Davis Law Review*, 50(4), 1673-1739. Retrieved from: https://ssrn.com/abstract=2929030.

Spence, M.A. (1974). *Market Signaling: Informational Transfer in Hiring and Related Screening Process.* Cambridge, Massachusetts: Harvard University Press.

Spiekermann, S., Krasnova, H., Koroleva, K. & Hildebrand, T. (2010). Online Social Networks: Why We Disclose. *Journal of Information Technology*, 25(2), 109-125. doi: https://doi.org/10.1057/jit.2010.6.

Sprague, R. (2011). Invasion of the Social Networks: Blurring the Line between Personal Life and the Employment Relationship. *University of Louisville Law Review*, 50, 1-42. Retrieved from https://ssrn.com/abstract=1773049.

Superior Court of Justice of Andalusia, Seville, Sala de lo Social, sec. I, ruling of 8 June 2017, n. of complaint: 2275/2016, (resolution n. 1736/2017).

Superior Court of Justice of Las Palmas de Gran Canaria, Contentious Chamber, sec. I, ruling of 10 Juli 2018, n. of complaint: 372/2017 (resolution n. 404/2018).

Tamir, D.I. & Mitchell, J.P. (2012, 22 May). Disclosing information about the self is intrinsically rewarding. *PNAS Proceedings of the National Academy of Sciences of the United States of America*, 109(21), 8038-8043. doi: 10.1073/pnas.1202129109.

Tullini, P. (2009). Comunicazione elettronica, potere di controllo e tutela del lavoratore. *Rivista italiana di diritto del lavoro*, 3(1), 323-352.

Tullini, P. (2016). Economia digitale e lavoro non-standard. *Labour & Law Issues*, 2, 1-15. doi: 10.6092/issn.2421-2695/6489.

Weiss, M. (2016). Digitalizzazione: sfide e prospettive per il diritto del lavoro. *Diritto delle relazioni industriali,* (3), 651-663.

Weller, B. (2019). Kommentar zu LAG Baden-Württemberg, Ruling of 14.03.2019, 17 Sa 52/18. *Betriebs-Berater*, 40, 2368. Retrieved in https://online.ruw.de/suche/bb/BB-Kommentar-f44c851705ad118a44ffc824f15bcb1a.

Zimmer, M. (2010, December). But the Data is already Public: on the Ethics of Research in Facebook. *Ethics and Information Technology*, 12(4), 313-325. doi: https://doi.org/10.1007/s10676-010-9227-5.