Social Media and Workers' Rights: What Is at Stake?

Riccardo Del Punta*

This article addresses the way in which the growing use of social media is changing the employment relationship. Technology has given rise to a huge increase in the amount of information about employees available to employers, while allowing them to engage in invasive monitoring of employee access to the internet and social media. This highlights the importance of regulatory techniques, as employees have become more exposed to monitoring by the employer and potentially to discrimination. In certain cases, the employee's freedom of expression is at risk. To counteract these tendencies, privacy laws, recently reinforced in the EU by the General Data Protection Regulation or GDPR, and more generally the principle of proportionality, can represent effective instruments to prevent technology from exacerbating the condition of subordination of employees.

1 INTRODUCTORY REMARKS

As a labour lawyer who grew up in the pre-Social Media era, in approaching the topic of social media and workers' rights, I might be tempted to argue that despite appearances there is nothing really new under the sun. At first glance, this assumption might seem to be well founded. In fact, the question of free speech in the workplace and its limitations, that has attracted increasing attention with the rise in the number of cases of employees being fired for using Facebook or other social media, is anything but new. It may be said that in the past while public criticism of the employer could be made by giving an interview to newspapers or speaking in public, it can still be made today by posting a comment on Facebook or Twitter. At the same time, the question of the relevance of the private behaviour of the employee in relation to the employment contract, as a possible justification for disciplinary dismissal, cannot be said to be original.

Another aspect of the topic under examination concerns the question of whether and to what extent the employer can openly access the employee's personal information posted on social media, once again forming part of a broader and long-standing debate concerning technological monitoring of employees, in search of a balance that has yet to be struck between the employers' prerogatives

* Full professor of labour law, University of Florence (Italy). Email; delpunta@studio-lex.it

Del Punta, Riccardo. 'Social Media and Workers' Rights: What Is at Stake?'. *International Journal of Comparative Labour Law and Industrial Relations* 35, no. 1 (2019): 79–100.

and the employees' rights to privacy. Incidentally, this debate has been relaunched within the EU with the entry into force of the GDPR.[1]

In other words, it may seem on the one hand that the issues raised by employees posting comments on social media could be managed using the criteria already laid down by legislation and further elaborated by the courts. On the other hand, the question of employers monitoring their employees on social networks could be seen as just one of the many facets of the Big Brother debate currently underway.

However, a serious intellectual conservatism would be evident in the event of a failure to see that the astonishing success of social media, and as a result the massive use of such media by employees (inside and outside the workplace), is giving rise to an information revolution at work, determining an exponential increase in both the amount and quality of information that circulates around employment (i.e., both in job applications and in the development of the employment relationship).

It is impossible to pretend that the world of employment can be insulated from this overwhelming mass of information. Rather, the problem is how, and according to what kind of balancing with workers' rights (naturally including privacy but also other types of freedom that are at the heart of the personal sphere of the worker), it should be managed by the employer.

In this perspective, the increasing penetration of social media in the workplace becomes one of the many aspects of the ongoing transformation of work driven by IT, with which labour law regulations have difficulty keeping pace. In addition, from a more technical perspective, the topic under discussion, like any IT topic, poses intrinsic challenges to regulation, that has to cope with an elusive reality. The chances of implementing effective regulations are thus limited.

Against this backdrop, this article is structured as follows: section 2 examines the European legal framework concerning the protection of personal data and its essential difference from the American model, albeit in broad terms; sections 3 and 4 address the investigation of employees by means of social networks and monitoring of their access to social media, leading to an examination of the issue of dismissals arising from the social media activities of employees (section 5); finally, section 6 puts forward some concluding remarks.

2 THE EUROPEAN LEGAL FRAMEWORK ON PRIVACY

The use of social media by employees for private purposes[2] immediately evokes the question of the respect of their privacy in the specific context of the

[1] For more details, *see infra*.

[2] The use of social media by employees is considered here exclusively when it is of a private nature (regardless of whether or not it occurs via use of a computer provided by the employer and during or outside working hours). Access to social media for work reasons (which is more and more frequent,

employment relationship. As argued below,[3] in relation to this not everything can be solved by means of privacy, though it remains the first and preliminary frontier to be defended. The term 'preliminary' is used here in a strictly legal sense, as a source of preliminary issues between the parties in legal proceedings.

Whatever the definition of privacy adopted, either (in the negative) as a mere restriction of others' knowledge about oneself, or (in the affirmative) as having control over information about ourselves,[4] the fact remains that privacy defines the boundaries of legitimate knowledge of personal information or data. As a result, if such data have come into the possession of others in violation of data protection regulations, they will have no legal relevance in proceedings, as evidence of certain types of conduct on which disciplinary dismissals have been based. This is not just the logical implication of privacy as a right, that I will discuss below, but also a consequence explicitly provided by some legal systems.[5]

However, from an EU perspective, the status of the right to protection of personal data has been consolidated over the years. In fact, this is a fundamental right, as stated both by Article 8(1) of the Charter of Fundamental Rights of the European Union, and Article 16(1) of the Treaty on the Functioning of the European Union. These additional safeguards come in the wake of Directive 95/46/EC that paved the way for specific legislation enacted by the Member States. This Directive has been replaced, since 25 May 2018, by Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, which provided the new GDPR.

It is worth noting that as it is contained in a Regulation, capable of both direct and horizontal effects in the national systems, the GDPR has taken effect in the Member States, although they are also allowed to adopt national legislation in order to specify or further implement the EU rules.[6] As a result, each national law will result from a (complex) mix of European and domestic regulations.

This is not the place for examining the numerous rules provided by the Regulation with regard to the processing of personal data, which amount, in general terms, to a modernization and further strengthening of privacy protection (e.g. with an improvement in information procedures and a restriction on the use of the data subject's consent as a basis for data processing).

---

e.g. for marketing purposes) remains outside the focus of this analysis. On this subject, *see* A. Ingrao, *Il controllo a distanza realizzato mediante Social network*, 2(1) Lab. L. Issues 115–117 (2016).

3 *See* especially s. 5.

4 *See* V. Mantouvalou, *Human Rights and Unfair Dismissal: Private Acts in Public Spaces*, 71(6) Mod. L. Rev. 924 (2008), while discussing Charles Fried's classical conception, as expressed in 'Privacy', *Philosophical Dimensions*.

5 *See* for instance, Art. 2-*decies* of the Italian Legislative Decree no. 101/2018, n. 6 *infra*.

6 In Italy this regulation was implemented with Legislative Decree no. 101/2018.

Suffice it to mention the main principles, as stated in Article 6(1), according to which personal data must be processed:

Personal data shall be: (a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('*lawfulness, fairness and transparency*'); (b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes … ('*purpose limitation*'); (c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('*data minimisation*'); (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('*accuracy*').

Neither the previous Directive nor the GDPR contains specific provisions about privacy protection in employment. However, Article 88 of GDPR establishes that:

Member States may, by law or by collective agreements, provide for more specific rules to ensure the protection of the rights and freedoms in respect of the processing of employees' personal data in the employment context, in particular for the purposes of the recruitment, the performance of the contract of employment, including discharge of obligations laid down by law or by collective agreements, management, planning and organization of work, equality and diversity in the workplace, health and safety at work, protection of employer's or customer's property and for the purposes of the exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment, and for the purpose of the termination of the employment relationship.

In any case, the application of privacy protections to employment relationships is undisputed in the EU area, and a number of regulations concerning privacy in the workplace have been adopted at various levels by the Member States.

The European framework is completed, on a broader scale than the EU,[7] by the European Convention of Human Rights, adopted by the Council of Europe, Article 8(1) of which states that 'Everyone has the right to respect for his private and family life, his home and his correspondence'.

On several occasions, as reaffirmed once again in *Barbulescu v. Romania* (see below), the European Court of Human Rights (hereinafter, ECtHR) has ruled that the concept of 'private life' includes 'professional activities' and that employment relationships falls within the scope of the above-mentioned Article 8.

In the end, the point to be underlined is that under the European rules the worker is also considered a full citizen in the workplace (however defined), since, to quote Article 2 of the Italian Constitution, the citizen's fundamental rights must also be safeguarded within the 'social formations' in which the individual's

[7] Forty-seven Member States, compared to the twenty-eight EU Member States prior to Brexit.

personality is developed. As a result, employees can legitimately expect respect for their privacy by the employer, although that right – as clarified in the preamble to the EU Regulation – is not absolute and must be balanced against the employer's prerogatives.

The European approach to privacy therefore continues to be quite different from that of the US, according to which, with the exception of some piecemeal legislation adopted by certain states,[8] workers do not have any expectation of privacy. The arguments put forward by Matthew Finkin, proposing a substantial change in American legislation also on the basis of the European models such as the German one,[9] can be likened to kicking down an open door with reference to the European context.

The trans-Atlantic divide on this matter has been described in terms of a clash between the European safeguarding of dignity and the American priority for liberty, which prevents the US from imposing privacy constraints on entrepreneurs.[10] However, the EU Regulation also takes employer freedom into consideration to a significant extent, e.g. widely exempting them, while pursuing a 'legitimate interest'[11] (an expression which unquestionably includes the employer's interests), from the rule according to which the processing of personal data is only lawful with the consent of the data subject.[12]

It is nonetheless true that a profound gap remains between the two sides of the Atlantic on this issue (with the UK, as always, in the middle). The idea that the employees' freedom to express their personality in the workplace, for which the guarantee of a certain degree of privacy is indispensable, is also worth safeguarding, continues to be largely extraneous to the mainstream American culture, despite minority opinions drawing attention to the additional challenges posed by new technologies.[13] In this sense a contradiction emerges with the well-known

---

8 *See* M. W. Finkin, R. Krause & H. Takeuchi-Okuno, *Employee Autonomy, Privacy, and Dignity Under Technological Oversight*, in *Comparative Labour Law* 164–165 (M. W. Finkin & G. Mundlak eds, Cheltenham UK – Northampton MA, Edward Elgar Publishing 2017).

9 *See* M. W. Finkin, *Some Further Thoughts on the Usefulness of Comparativeness in the Law of Employee Privacy*, 14 Emp Rts. & Emp. Pol'y J. 11 (2010). *See also* M. W. Finkin, *Privacy: Its Constitution and Vicissitudes – A Half Century on*, 18 Can. Lab. & Emp. L.J. 349 (2015).

10 *See* Finkin, *Some Further Thoughts*, *supra* n. 9, especially 41 ff. The incommensurability of the American and European conception of privacy is classically argued by J. Q. Whitman, *Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 Yale L.J. 1151 (2004), whose arguments are extensively discussed and critiqued by Finkin.

11 *See* the EU Regulation, in Art. 6(1), according to which the consent rule does not apply when 'processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child'.

12 This exemption does not apply, however, to the processing of so-called 'sensitive data'.

13 In Finkin's footsteps, *see* L. Evans, *Monitoring Technology in the American Workplace: Would Adopting English Privacy Standards Better Balance Employee Privacy and Productivity?*, 95 Cal. L. Rev. 1115 (2007).

American sensitivity to anti-discriminatory protection, as it is evident that privacy is the first barrier to discrimination, as well as 'a necessary precondition for individual autonomy and human flourishing'.[14]

3 INVESTIGATIONS OF EMPLOYEES THROUGH SOCIAL NETWORKS

Once it has been established that in the European perspective the employee has a legitimate, though not absolute, expectation of privacy, the analysis must become more concrete in order to identify the main legal techniques in the European systems aimed at protecting this right, with a special focus on employee activity on social media.

The general premise is that since the Aristotelian unity of space, time and action traditionally characterizing subordinate work has been broken down by the advent of teleworking (which also denotes a particular form of subordinate work, such as smart work), both the spatial and temporal elements of the employment relationship have become progressively less important, though they are obviously not obsolete. This leads us to identify the lowest common denominator of the relationship in terms of the *circulation of information* which is naturally inherent to the drafting, conclusion and execution of the employment contract, in proportion to the intensity of the contact between the two parties.

Naturally, the disclosure of reciprocal information is always partial, as the conduct of both parties tends to be opportunistic or at least strategic. They usually try to find out as much as possible about the other party and to disclose as little as possible about themselves. The resulting asymmetry of information[15] has been widely examined in the economic literature, though usually without considering that what is particular about the employment relationship is that this asymmetry occurs in a situation which is already characterized by an inequality of power between the parties. Moreover, especially on the part of the employer, the novelty is that technology has triggered an 'inexorable drive' to know more and more about their employees, in order to reduce, as far as possible, 'the zone of the unknown'.[16] More information entails even greater power, but can legislation resist this 'inexorable drive'?

The relevant regulations are contained in privacy law, as well as in additional provisions that take account of the asymmetry of power (and not just the asymmetry of information, as in the economists' point of view) inherent in the employment relationship. These regulations are aimed at increasing the overall impact of

---

[14] *See* Mantouvalou, *supra* n. 4, at 921.

[15] For one of the earlier definitions of 'asymmetric information', *see* L. Philips, *The Economics of Imperfect Information* 2 (Cambridge, CUP 1988).

[16] *See* Finkin, *Privacy: Its Constitution and Vicissitudes*, *supra* n. 9, at 362.

protection in a logic of complementarity between privacy and the labour law perspective.

Let us take an example from Italian labour law. The premise is that Article 8 (1) of the GDPR (as well as the previous Directive) provides for reinforced protection of so-called 'sensitive data', that is:

> data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

The processing of these data is basically prohibited, except in specific circumstances that do not interest us here. The rule of consent by the data subject, which normally amounts to authorization of the processing of data, can be limited here, in that a Member State may establish that the basic prohibition cannot be lifted by the data subject. This is the case of the Italian provision referred to above, that dates back long before the topic of privacy gained great attention, i.e., Article 8, Act no. 300/1970, which establishes that:

> It is forbidden for the employer, both for the hiring process and throughout the employment relationship, to conduct investigations, also indirectly, of the political and religious opinions or the trade union affiliations of the employee, or of facts that are not relevant for the evaluation of his/her occupational capacity.

This article aimed, first of all, at providing an *ante litteram* (and in this case absolute) protection of workers' privacy by preventing the employer from accessing the sensitive information of the kind considered. In addition, Article 8 was meant 'to facilitate the free manifestation of the employee's personality' without fear of any consequences.[17] In this anti-domination view, the provision was clearly linked to anti-discriminatory protection.

However, Article 8 went beyond these goals: by means of the ban on any investigation of facts 'not relevant for evaluating the worker's occupational capacity', it pursued the even more ambitious goal of depersonalization of the employment relationship.

The basic idea was clear, but it must be noted that this was back in 1970. The worker made his/her labour and time available to the employer, and was paid for this, which exhausted the contractual exchange. As a result, not just the worker's political or religious opinions, ethnic origin, sexual preferences and so on, but also the rest of his/her life had to remain beyond the employer's knowledge and

[17] *See* A. Topo & O. Razzolini, *The Boundaries of the Employer's Power to Control Employees in the ICT Era*, 39 Comp. Lab. L. & Pol'y J. 101 (2018), s. 5.

evaluation, as though everything regarding the worker's personal life outside the workplace was to remain hidden, in a logic aimed at preventing employer abuse.[18]

In other words, as the legislator was aware of the unbridgeable gap of power between the employer and the employee, it was held that the only way to defend the employee was by building a barrier of *negative freedom* within a relationship nonetheless based on the legalized interference by one party with the other one.

One problem with provisions such as these, however, has always been that they are largely ineffective in terms of the employer's conduct during selection and recruitment procedures. This is due not only to the fact that any misconduct on the part of the employer (such as asking a female applicant if she intends to get married and/or get pregnant in the near future) normally takes place without witnesses (except when the interview is recorded, in which case the recording can be accepted as evidence by the courts), but also to the obvious fact that the employer does not need to provide reasons for rejecting a job application.

This leads us to address the widespread practice of carrying out searches on the open web, including social network pages that are not subject to privacy restrictions, in order to gather information about job applicants with a view to profiling their personality. Some of the most advanced HR firms are now already using sophisticated apps and algorithms to sort through job applications and pick the best candidates.

A growing number of jobseekers are encouraging this trend, as they try to give a boost to their careers through the web, in some cases to the point of becoming semi-professional bloggers.[19] Some social networks, such as LinkedIn, are expressly devoted to facilitating new professional contacts: the candidates' profiles are crucial in this respect.

It is also important to bear in mind that the concept of 'occupational skill' is intrinsically evolving, as growing importance is given to 'soft skills' which include all those attributes, linked to the employee's personality, that enable someone to interact effectively and harmoniously with other people. This practice is often encouraged as it allows for a more comprehensive appraisal of the worker's personality, which could be the premise for more complete individual self-realization at work. However, it also entails risks, as it leads employers to look for a wider range of data than strictly occupational

[18] For a case in which a violation of Art. 8 was detected when an employer had been storing all the employees' emails and connections to internet in the workplace as a preventive measure, claiming that all the stored information could be useful in order to identify employees responsible for any misconduct, *see* the Italian Court of Cassation, Labour Section, 19 Sept. 2016, no. 18302.

[19] This practice is considered as counter-productive, however, by some minority opinions: *see* C. Newport, *Quit Social Media. Your Career May Depend on It*, www.nytimes.com/2016/11/20 (accessed Nov. 20 2016).

information, thus eroding or even suppressing the boundaries between the private and occupational spheres.

Even Public Employment Services have been affected by these methods, at least those that seek to improve the efficacy of their employability policies, the importance of which is widely recognized, both at a European (under the flexicurity flag)[20] and a global[21] level. The effective profiling of jobseekers is, in fact, the premise for calibrating activation measures. In this light, a provision such as the above-mentioned Article 8 cannot prevent these practices since the concept of 'relevant' information is evolving, and in actual fact, because this information is often at everyone's disposal on the open web.[22]

Moreover, in certain cases, employers do not carry out an investigation but personal information about a worker is spontaneously provided by a third party, such as another employee. This may take place by reposting comments and pictures from a different social network, account or discussion board.

That said, undoubtedly the processing of such data falls under the scope of the more flexible privacy regulations. This will require employers and HR professionals, as well as employment agencies, headhunters and so on, to state the legal basis for data processing, retention periods, the data subject's right of complaint, and information about individual rights under the GDPR.

However, the impact of this regulation must not be overstated. On the basis of the GDPR, for example, employers should only be allowed 'to collect and process personal data relating to job applicants to the extent that the collection of such data is necessary and relevant to the performance of the job which is being applied for'.[23] As already noted, the conception of what is relevant to the job is becoming broader and broader, not to mention the fact that most of this processing occurs before any face-to-face contact between the parties has taken place, giving the impression that the vast majority of this microprocessing will continue to elude privacy protection.

What is easier to answer is the question as to whether the employer is entitled to ask for the employee's username or password to access his/her personal social media accounts. This is a matter of debate also in the US, where, according to common law, and in the absence of legislation, the request must be considered legitimate, meaning that the applicant who fails to communicate his/her username or password would not be hired and, if already employed, could be dismissed.

---

[20] *See*, most recently, the Fourth European Pillar of Social Rights, concerning the necessity to give 'active support to employment'.

[21] *See*, for one of the first International Labour Organization statements about the importance of employability, the Human Resources Development Recommendation, no. 195/2004.

[22] This is, instead, the opinion of Topo & Razzolini, *supra* n. 17, s. 5.

[23] *See* the Opinion of the Working Party set up under Art. 29 of the EU Directive, an independent advisory body on data protection and privacy.

However, since 2012, several states have passed legislation to prohibit employers from making such requests.[24]

In Germany, even though no specific regulations exist on this matter, it is commonly acknowledged, by virtue of the Federal Data Protection Act, that 'there cannot exist a duty of the applicant to disclose his/her password because this would inevitably lead to the unveiling of personal data beyond employment-related purposes'.[25] The Italian regulations are clearer in this regard, as they state that requesting access to an employee's personal account violates the above-mentioned Article 8, 'because it may reveal more than what is necessary for specifically detecting whether the employee is fit for the job position'.[26]

The same conclusion could be reached, both for Germany and Italy, also on the basis of the GDPR, but with the difference that the GDPR gives relevance to the consent of the data subject, who could therefore be 'forced' to disclose the password. Instead, on the basis of a more rigorous provision such as the Italian Article 8, the employee's consent would have no relevance, though this provision might be violated de facto, due to the worker's dependence on the job.

4 THE EMPLOYER'S CONTROL OVER EMPLOYEE ACCESS TO THE INTERNET AND SOCIAL MEDIA

Employees frequently access the internet during working hours for a variety of reasons, such as taking a break, contacting partners or friends, planning holidays, booking restaurants, purchasing flights, and even visiting pornographic websites. The use of social media is only one of the many reasons for access. Employees access the internet either using their own devices, such as smartphones, or the computer assigned to them by the employer. In both cases the work activity is interrupted, which may be tolerated by the employer, within certain limits, or not tolerated at all, depending on the policy adopted by the firm. Especially in cases in which they suspect abuse, employers often react by subjecting their employees to intensive monitoring potentially capable of ensuring the full traceability of their operations.

Here again the trans-Atlantic divide is evident, as in the US model the employer's power of monitoring, through video surveillance systems, geolocation technology and other computerized systems, is virtually unlimited, apart from sporadic constraints laid down in the legislation of certain states.[27] Instead, the European regulation has proposed essentially two models over the years that have

[24] *See* Finkin, Krause & Takeuchi-Okuno, *supra* n. 8, at 182–85.
[25] *Ibid*., at 185–86.
[26] *See* Topo & Razzolini, *supra* n. 17, s. 5.
[27] *See* Finkin, Krause & Takeuchi-Okuno, *supra* n. 8, at 188–89.

ended up overlapping with each other to a certain extent.[28] On the one hand, the traditional approach is based on the prohibition of *direct* control of workers via remote monitoring, and on the other, on the possibility of *indirect* control, justified on productive or organizational grounds, provided it is authorized either by the workers' representative, through a collective agreement at plant level (as in the case of Germany, where this is a matter of co-determination, and in Italy), or by an administrative body (as in the case of Italy).

However, this model raises a number of problems. First, the conceptual distinction between direct and indirect monitoring has always been spurious (productive or organizational reasons are often a fig leaf for deliberate monitoring of employees) and it is increasingly untenable with regard to IT, which potentially allows for full traceability of all the employee's operations. Second, it may be the case that the authorization by the trade unions is given simply in exchange for concessions from the employer, without having an effective impact on the way the monitoring is carried out.

The other model, the relevance of which has been increasing over the years due to the development of a culture of privacy, is centred on privacy protection rules, since they also act as a constraint on the employer's power of control, as the gathering of personal data by means of remote monitoring is recognized as a form of data processing, and is therefore subject to privacy regulations. However, these regulations must in turn take account of the fact that they apply to an environment which is characterized by legitimate prerogatives of one party over the other.

In this respect, the privacy regulation proposes a sort of exchange. On the one hand, it basically exempts the installation of IT systems that indirectly allow the monitoring of employees from the need to obtain the individual worker's consent, to the extent that such an installation is justified by the employer's 'legitimate interest' of a productive, organizational or technical nature.

On the other hand, the principles and rules governing privacy are a restraint on the employer's power of monitoring, which is not prevented but subjected to the proportionality criteria. The relevance of the *proportionality principle* in this respect is stressed in various European legislations, such as the French one.[29] However, the proportionality test is currently applied also by other legal systems.[30]

With specific reference to the GDPR, proportionality is broken down into additional, more specific principles. As far as employee access to the internet and

---

[28] For an analysis of this regulation from an Italian perspective, *see* Ingrao, *supra* n. 2; Topo & Razzolini, *supra* n. 17.

[29] *See* the Code du travail, Art. L. 1121-1.

[30] *See* G. Davidov, *A Purposive Approach to Labour Law* 184–87 (Oxford, OUP 2016), with examples taken from Canada, Israel, and UK (where proportionality has been brought into the analysis by means of the above-mentioned Art. 8 of the European Convention on Human Rights).

social media is concerned, the principle of '*lawfulness, fairness and transparency*' requires the employer to adopt a fairness and transparency policy that gives workers adequate information on how their data are processed, and how they can be subject to inspections. Then the principle of '*purpose limitation*' requires the specifying of the purposes of data processing and limits the processing to the pursuit of those purposes. At the same time, the principle of '*data minimization*' requires employers to adopt preventive measures before checking workers (e.g. installing software blocking access to sites that are extraneous to work activity), to mitigate the intensity of monitoring, which must not be continuous or pervasive, and anonymize the data as far as possible (as allowed by specific software), where necessary with the exception of cases in which significant anomalies in worker performance emerge. The actual circumstances of each case must also be taken into account: e.g. in the event of specific reasons for suspecting a certain worker, the proportionality principle should lead to acceptance of more intrusive monitoring, at least temporarily.

This regulation allows an employee who has been dismissed for disciplinary reasons on the basis of information gathered by means of remote monitoring to challenge the dismissal before a court by alleging that the evidence of his/her misconduct was unlawfully collected, and, therefore, not admissible in the proceedings.[31]

By way of example, this position was expressly laid down by the recent Italian reform of the rules concerning remote monitoring of employees,[32] which established that data collected via remote monitoring can be used 'for all purposes inherent to the employment relationship' (including disciplinary purposes, but also the evaluation of worker performance) provided that the workers have been adequately informed about the firm's policy on the use of electronic devices and that data collection has been carried out in compliance with the privacy regulations.

The importance of adopting a transparency policy, by virtue of which the worker is required to be informed in advance on how to use the firm's equipment and about the possibility of monitoring, was also stressed by the ECtHR in the interpretation of above-mentioned Article 8 of the European Convention of Human Rights. This particular case was referred to the Court by Mr Barbulescu, who was employed as a sales engineer at the Bucharest office of a Romanian

[31] In this respect, the conclusion reached by the Italian Court of Cassation, Labour Section, 15 June 2017, no. 14682, according to which the data concerning the time and amount of the employee's connections to internet during working time does not constitute personal data, so that the employer's non-compliance with the duty of prior information was not considered relevant, seems to be oversimplified.

[32] *See* the Legislative Decree no. 151/2015, which I analysed in R. Del Punta, *La nuova disciplina dei controlli a distanza sul lavoro*, Riv. it. dir. lav. 77, I (2016).

company. At his employer's request, in order to respond to customer enquiries, he set up an instant messaging account using Yahoo Messenger, an online chat service offering real-time text transmission over the internet. The employee had been informed of the prohibition on using the computer for personal reasons, but not explicitly about the possibility of monitoring by the employer.

In 2007, Mr Barbulescu was summoned by his employer to explain why, during a certain week, his internet activity had been much greater than that of his colleagues. At that stage, he had not been informed about whether the monitoring of his communications also concerned the content. Consequently, the employee told the employer that he had used Yahoo Messenger for work-related purposes only. Unfortunately, this was not true, as the company was well aware right from the start. As a result, the firm terminated his employment contract and the employee challenged the dismissal before the Romanian court, but unsuccessfully. The judgment was then brought before the ECtHR, based on the alleged violation of Mr Barbulescu's right to privacy.

The Court's reasoning was tormented. In the first stages the Chamber held that there had been no violation, in the specific circumstances, of Article 8 of the Convention.[33] This decision was overturned, albeit with a significant dissenting opinion, by the Grand Chamber[34] which essentially reproached the Romanian Court of Appeal for neglecting a number of elements that should have been taken into consideration in order to evaluate whether a fair balance had been struck between the two interests at stake. In other words, according to the ECtHR, the Court of Appeal

> failed to determine whether the applicant had received prior notice from his employer of the possibility that his communications on Yahoo Messenger might be monitored; nor did they consider the fact that he had not been informed about the nature or extent of this monitoring, or the degree of intrusion into his private life and correspondence. In addition, they failed to determine, firstly, the specific reasons justifying the introduction of the monitoring measures; secondly, whether the employer could have used measures entailing less intrusion into the applicant's private life and correspondence; and thirdly, whether the communications might have been assessed without his knowledge.[35]

These are, substantially, the same principles underlying the GDPR. This allows us to speak of a common European approach, by virtue of which the potential contradiction between the employer's power of monitoring, inherent in the condition of subordination, and the employee's expectation of privacy in the workplace, is handled, although not entirely resolved, by means of a number of principles which can be summarized by the idea that monitoring must be carried

[33] *See* ECtHR, IV Section, 12 Jan. 2016, *Barbulescu v. Romania*.
[34] *See* ECtHR, Grand Chamber, 5 Sept. 2017, *Barbulescu v. Romania*.
[35] *See Ibid*.

out both transparently and proportionally, taking into account all the specific circumstances.

However, transparency cannot mean that the employee needs to be informed prior to any particular monitoring action, as it is obvious that this would make it useless, giving the employee time to conceal at least the most evident proof of his/her misconduct (even though electronic evidence can usually be recovered by the server). Transparency must basically be intended in terms of prior knowledge of the possibility of monitoring, even if not continuous or intrusive.

In the end, the essential action that firms are required to carry out under the law in force is to draw up a privacy policy that ensures in an approximate manner that they are able to deal at least with the most serious acts of misconduct by the employees, while also preventing the employer from resorting to massive and continuous monitoring of the workforce.

This compromise seems to be the best possible solution in view of the balancing of the two interests, both legitimate, that are at stake, and each of which must give up its original claim to be absolute. However, the intrinsic uncertainty of the regulation, which is mostly (and inevitably) based on open principles rather than on precise prescriptions, is still a problem. It is never easy to clearly establish in advance, for either party, the boundary between what is allowed and what is forbidden, e.g. the point beyond which monitoring becomes excessive and intrusive with regard to the privacy of the other party. This is an argument in favour of a second-level regulation with more specific guidelines and prescriptions, such as those issued by data protection authorities.

It is hard to say whether this is a sufficient barrier for avoiding the degeneration of management control into a Big Brother or, even more classically, a Panopticon scenario, which has become a matter of concern even for *The Economist*, a champion of free enterprise, leading it to invoke transparent monitoring ('tracking the trackers') inspired by 'a strong dose of humanity', also considering that 'a more productive workforce is a prize worth having, but not if it shackles and dehumanises employees'.[36]

Finally, I would like to address a highly unusual case, that has to do with Facebook but shows how the monitoring of the employee's use of social media does not necessarily focus on the use of the employer's device. In this case an imaginative form of monitoring was devised to collect evidence that the employee frequently abandoned the workstation to chat on Facebook, thus leaving a dangerous press-machine unsupervised. The employer asked the HR manager to set up a fake female profile to induce the employee to chat using his own device during

[36] *See* the leader *Workplace of the Future*, The Economist, 31 Mar. 2018.

work time. The employee fell into the trap and once the evidence was collected (added to which, the press-machine jammed while the chatting was taking place), he was dismissed for just cause.

The Italian Court of Cassation argued that the evidence of misconduct had been lawfully collected by the employer, in that it was aimed at protecting the company's property.[37] As for the fact that the misconduct had not only been discovered but induced by an *agent provocateur*, purposely set up by the employer, the Court, unbelievably, did not detect any violation of the good faith principle.

5 FIRED FOR FACEBOOK

It has been argued that the social media environment is some kind of 'inter-reality' or hybrid reality, deriving from the merging and interaction of the digital and real world.[38] However, it may be the case that the real world takes its revenge in the very tangible form of a letter of dismissal for disciplinary reasons. Cases of employees fired because of their use of Facebook or other social media have become widespread worldwide, causing various reactions among the public and giving rise to delicate issues. These actually involve two situations, which must be addressed separately, due to their different legal implications.

The easier cases concern 'cyberslacking', in which the employee is alleged to have used the internet for personal reasons during working time (irrespective of whether it was with personal or company devices). This practice, that has been made easier with the advent of broadband internet connections, is estimated to have a high cost for employers in terms of lost productivity, additional security costs, and staff replacement. These situations often end up in dismissal on disciplinary grounds, thus giving rise to two distinct issues. The first one, which concerns the lawfulness of the data processing, has already been dealt with.[39] The second one concerns whether a breach of contract has occurred, and its seriousness.

In these circumstances, there is usually some form of violation of contractual duties. However, it may be the case that the firm has a policy of tolerating short work breaks. What is intriguing is the case of employees engaged in 'smart working', with regard to whom there is a need to ascertain whether the time lost on the internet was justified by their right to be disconnected with the employer after

---

[37] *See* Court of Cassation, Labour Section, 27 May 2015, no. 10955.

[38] *See* J. van Kokswijk, *Hum@n, Telecoms & Internet as Interface to Inter-Reality* (Hoogwoud, Berboek 2003); G. Riva, *I social network*, Bologna, Il Mulino, 2016, 106ff.

[39] *See* s. 4.

their work time, which has been upheld, albeit in various forms and still experimentally, by both French and Italian legislations.[40]

In this connection, it is more important to assess the seriousness of the breach, which depends on the criteria adopted in the different legal systems for defining the justified reason for dismissal. In this case, too, the guiding principle is that of *proportionality*, which involves all the facts of the case (duration and reiteration of the abuse, contents and transparency of the firm's policy, any tolerated bad practices) that have to be taken into account to establish whether the measure of dismissal was proportionate to the employee's infringement. The kind of websites visited, which may include social media, should not be relevant in this perspective, as long that they have nothing to do with the job. One example is the case of a French employee who tweeted during working time using the firm's smartphone, and the judge ruled that dismissal was unfair because four tweets a day can be tolerated by the employer as each of them takes only about one minute.[41]

The other and far more delicate problem concerns employees who are dismissed because of opinions or other expressions (through texts, videos, pictures) openly shared with a virtual community on the social media. I am mainly referring to the case of opinions posted on social media without any privacy settings. However, even if the opinion is shared with a limited number of friends but has nevertheless circulated on the web, it could still be relevant.

The most common situation concerns public criticism of the employer expressed by employees, often in vulgar terms. In principle, these cases do not entail a different approach from the one adopted in evaluating other situations, not related to social media, in which the worker makes a criticism in an open letter or speaking before a wide audience.[42]

On the one hand, the employee's freedom of expression is at stake, which cannot be suppressed in consideration of the duty of loyalty to the employer which is inherent to subordination. However, the right of criticism must be exercised – again – in respect of *proportionality*, which entails taking account of circumstances such as the truthfulness or the plausibility of the comments made, the context in which the opinions have been expressed (e.g. a union dispute can allow for more vehement criticism), the size of the audience (in our case a virtual

---

[40] As for France, *see* the Loi Travail no. 2016–1988; for Italy, with specific regard to smart workers, Art. 19, para. 1, Law no. 81/2017. For a conceptual analysis from a Spanish perspective, *see* F. Alemán Páez, *El derecho de desconexiòn digital, Trabajo y Derecho*, no. 30, 12 (June 2017). A provision pushing employers to consult prevention and protection committees and eventually draft agreements with them on the use of digital work tools, including disconnection, has been introduced in Belgium, by an Act of 26 Mar. 2018, although unlike the French provision it does not entail a right to disconnect.

[41] *See* M. Degeorges, *Tweeter au travail est-il passible de licenciement?*, www.LesEchos,fr (6 Mar. 2016).

[42] As in the case examined by the Italian Court of Cassation, Labour Section, 29 Nov. 2016, no. 24260.

community), and the offensive nature of the expressions used[43] (not necessarily in terms of the wording).[44] In order to establish that these shifting boundaries have been overcome, it is not strictly necessary for the employee to be guilty of defamation.

An Italian Court also considered how quickly the employee removed the comments from the internet in order to reduce their offensive impact.[45] As a matter of principle, there should be more tolerance with regard to a mere 'Like' posted by the employee, as it seems paradoxical that the termination of an employment relationship can depend on a gesture that may have been purely emotional, and almost subconscious. In other words, the natural 'liquidity' of the information circulating on the web should be taken into consideration.

Nonetheless, a delicate Italian case shows how a 'Like' on Facebook can also become a reason for dismissal. An Italian prison guard had posted a 'Like' to a comment stressing that too many suicides were taking place in that prison. The Court ruled that the employee had been lawfully dismissed as the opinion thus expressed could damage the prison's reputation.[46] It is hard to say how fair this judgment was: from the outside it seems that instead of focusing just on the reputational damage, the ruling could have taken into greater consideration the plausibility or otherwise of the charges.

A short tweet may also damage the employer's reputation, and as such, justify a disciplinary dismissal.[47] An intermediate situation occurs when offensive expressions are not addressed to the employer but instead to a colleague, regardless of whether it is during working time or outside work (provided, however, that they are not linked to strictly private reasons). If the offence is serious, to the point of constituting harassment, of course it may be a fair reason for dismissal, *a fortiori* in consideration of the harm indirectly caused to the organization.[48]

A link between a certain expression (in this case not in the wording) and employment may also be connected to special circumstances. An Italian Court

---

43 For an Italian case in which several employees used disparaging expressions towards the employer that were repeated outside the workplace, *see* Court of Cassation, Labour Section, 31 Jan. 2017, no. 2499. Instead, according to the Tribunal of Busto Arsizio 20 Feb. 2018, telling the employer he is a 'bastard' does not overstep the boundaries of legitimate criticism.

44 *See* Cour d'appel de Reims, Chambre sociale, Arret du 16 novembre 2016, Rép. gen. no. 15/03197, which regarded as fair the dismissal of an employee who had published a provocative video on Facebook where he and several colleagues had adhesive tape over their mouths and their hands tied.

45 *See* Tribunal of Milan, 1 Aug. 2014.

46 *See* TAR of Lombardia, III Section, 3 Mar. 2016 no. 246, also commented on by Topo & Razzolini, *supra* n. 17, s. 6.

47 *See* Tribunal of Milan, 29 Nov. 2017.

48 Such as *Joseph v. TeleTech UK Ltd* (2012) NIIT/00704_11IT, in which an employee has been fairly dismissed due to the posting on Facebook of a sex-related and offensive comments towards a female colleague. On this decision, *see* the favourable opinion of M. Pearson, *Offensive Expressions and the Workplace*, 43 ILJ 429 (2014).

upheld as fair the dismissal of an employee who posted a photo of himself online posing with guns, thus causing concern about safety in the workplace.[49] In this respect, the Court also took into account the fact that an act of violence had been committed in the firm by the dismissed employee's brother only a few days before.

In other cases, employees have been dismissed because of their private behaviour (personal habits and choices, general opinions on matters of public debate), as revealed by the employees themselves or by third persons on social media. In dealing with this topic, and in particular, the delicate cases of two men who had been dismissed for conduct relating to their sexual life (engaging in homosexual acts in the toilet of a café in the first case, and the performing of shows in hedonist and fetish clubs as well as managing a company selling products connected with extreme sex, in the second), Virginia Mantouvalou convincingly elaborated on the updating of the concept of privacy.[50]

In particular, she criticized the decision of the UK court in the first case mentioned above, according to which an activity occurring in a public place (such as a café) cannot constitute elements of the employee's private life. She argued, instead, that everything the employee does outside the workplace and working time must basically be considered as private, even when occurring in a public place. Her conclusion, inspired by the application of the republican concept of freedom from domination to the employment relationship, is that 'off-duty conduct may lead to lawful termination of employment only if there is a clear and present impact or a high likelihood of such impact on business interests; a speculative and marginal danger does not suffice'.[51]

I agree with these conclusions, which closely correspond with the arguments currently deployed by European courts in the interpretation of the notion of justified reason for dismissal. However, I doubt that the concept of privacy can have sufficient reach in this respect, essentially because privacy has to do with the control of personal information, so that it has little influence, unless it is overburdened, on the ways in which such information is evaluated from other perspectives once voluntarily disclosed, as is the case of an employee who is active on social media.

In other words, even if one believes, in accordance with the European approach, that privacy at work exists and must represent an initial limitation to the employer's power of intrusion in the employees' lives, both at and outside work, it must be acknowledged that in those situations in which privacy is de

---

[49] *See* Tribunal of Bergamo, 24 Dec. 2015.

[50] *See* Mantouvalou, *supra* n. 4, at 912. The conclusion of the *Pay v. UK* case, with an ECtHR decision, has been further commented by H. Collins & V. Mantouvalou, *Private Life and Dismissal*, 38 ILJ 133 (2009).

[51] *See* Mantouvalou, *supra* n. 4, at 912.

facto overcome in one way or the other, a second and even stronger frontier must be built up, which directly concerns the boundaries of subordination and the employer's managerial power with respect to the worker's personal freedom, which would be curtailed in the case that an employee could be dismissed for exercising it.

My view is quite radical in this regard. Compliance with patterns of moral behaviour favoured by the employer for some reason (often due to fear of reputational damage), or generally accepted at least according to mainstream opinion, cannot be basically considered as an employee's contractual duty. Otherwise, the employment relationship would internalize an ethical finalization contrary to the categorical imperative that labour law has raised in the course of its evolution, regarding respect for the worker's individual sphere as such.

This does not rule out the possibility of cases in which private conduct could justify dismissal, though they need to be marginalized as exceptional, due to the priority granted to the value of personal freedom, in other words, as I would say in a Capability Approach perspective, the personal capability of being or doing whatever one wishes to be or do.

Particular attention must be paid, of course, to those cases in which the employee's essential qualities or choices are at stake and come under the category of anti-discrimination protection (even though some of these cases must be differently evaluated in ideologically orientated organizations, such as political parties or religious institutions, where the boundaries of what is permitted to the employer are somewhat more extensive).

However, the area governed by anti-discrimination legislation does not cover all cases where the employee's personal freedom is at stake. The freedom to choose how to dress or the freedom not to wear make-up – to mention a case discussed by Finkin,[52] though not related to social media – may be as important as the freedom to express political opinions or sexual preferences.

I am not so concerned about the moralistic obsessions of some individual employer, as by the large companies' codes of conduct and practices inspired by the unwritten law of political correctness, that give me cause for concern in excessive cases. One of these excessive cases occurs, in my opinion, when the values rightly protected by anti-discriminatory legislation are paradoxically used to place disproportionate restrictions on the freedom of opinion and speech, especially in matters of public debate which are by their very nature controversial.

This can happen, for example, when employees are dismissed for having publicly expressed opinions on social media or elsewhere that are not in line

---

[52] *See* Finkin, *Some Further Thoughts*, *supra* n. 9, at 13 ff.

with mainstream views, on the pretext that they could cause damage to the employer.

A case brought before the UK High Court is interesting in this respect. A manager posted a link on his Facebook wall to a news article about gay marriage, criticizing the fact that 'people who have no faith and don't believe in Christ would want to get hitched in church as the Bible is quite specific that marriage is for men and women'. Due to these comments, the manager was demoted to a non-managerial position with a 40% reduction in pay, as a result of an alleged breach of the Equal Opportunities policy and possible damage to the reputation of the employer, the Stafford Housing Trust. The conclusion of the High Court leaves me with some doubt,[53] even though it sensibly ruled out that the manager's 'moderate expression of his particular views about gay marriage in church on his personal Facebook wall at a weekend out of working hours, could sensibly lead any reasonable reader to think the worst of the Trust … '. This was a sufficient argument for justifying the conclusion that the manager had been unlawfully demoted. However, it is significant that the Court failed to base its reasoning on the intrinsic value of freedom of expression as well, which must come first and can only be limited in exceptional circumstances or in the case of evident excesses. What would have happened, in other words, if the same opinion had been expressed by the manager in a less 'moderate', albeit respectful, manner?

In short, we must not think that freedom of expression is acceptable and must only be defended when the expressions of opinion are to our liking, or correspond with what we believe a reasonable and liberal-minded person should think. This would amount to drawing illiberal and even discriminatory consequences from anti-discriminatory legislation.

However, I am aware that these options raise delicate and sometimes even tragic dilemmas. While the excesses of political correctness and social conformism have been outlined above, in my view giving rise to serious concern, the complexity of this issue must nevertheless be acknowledged.

The fact is that the evolutionary trend of the most advanced societies, and global society to a certain extent, in combination with the growing use and importance of the internet, has brought about a dramatic increase in the degree of *social control*. This has fuelled a widespread circulation of standards of 'good thinking and practice', which may have a positive influence on the policies of important social actors, like global enterprises. This may lead them to align

---

[53] *See Smith v. Trafford Housing Trust*, (2012) EWHC 3221 (Ch). On this decision, *see* Pearson, *supra* n. 48.

themselves with ethical values such as women's rights or the struggle against racism.

It is clear, however, that this can leave more exposed to social reactions all those who, for one reason or another, do not respect these standards and wish to express dissenting or provocative views on the web. If these people are employees, it may be the case that they end up being dismissed. A difficult balance thus needs to be struck between the increased social control of the internet era (which is not necessarily the same as a democratic control) and the safeguarding of the fundamental (though often disturbing) freedom of expression. This is anything but an easy task.

6 CONCLUSIONS

In the scenario outlined above, the old anthropological image of the 'silent worker', whose personality remained hidden to the employer, except for the limited familiarity that could derive from working in the same environment, has become increasingly obsolete. The astonishing success of social media has exponentially multiplied the amount of information about employees which comes into the employer's possession often (but not necessarily) as a result of deliberate investigation.

This trend is virtually impossible to reverse, since it is fuelled both by employers, who look forward to obtaining the greatest possible amount of information about their potential or current employees, and by employees, who see their social identity as an expansion of their personality and thus as a way of improving their self-fulfilment.

Apart from the question as to whether this is true or not, that is, if both personal and social identity are able to overlap so harmoniously, which is not a given, employees often simply do not consider the fact that while their social media activities may enable them to improve their career prospects or realize themselves more completely, in the meantime they become much more exposed to the employer's evaluation and reactions, in a word, to the employer's power. The enhancement of individual capabilities of expression, which social media would seem to promote, could result, paradoxically, in a worsening of the employee's condition of subordination.

In certain contexts, the employees could even become afraid to express their opinion on matters of public debate, as was the case decades ago, without any connection to employment, just because they do not correspond to the dictates of conformism.

In order to prevent or at least counterbalance these pathologies, a dual line of defence must be defined, on the one hand based on a strong concept of privacy

according to the European approach, and on the other, on the restatement of the priority of the freedom of expression in the broadest possible sense.

I have argued that such rights must be kept conceptually separate, although they are closely interrelated and can both be justified, in the context of the employment relationship, on the basis of the value of freedom as non-domination,[54] as they are aimed at reducing the arbitrary nature of the employer's power over the employee. The capability approach can also be evoked, since we are speaking of how wide the areas of substantial freedom can be within the employment relationship.[55] However, the key challenge, or rather fine-tuning exercise, is the balancing with the employer's prerogatives, in relation to which the proportionality principle, as noted with regard to the various aspects of this topic, can play an essential role, although its application in specific situations is likely to be problematic and controversial.

Nevertheless, a policy orientation should be clear on the basis of the priority of the values of the worker's dignity and freedom. In these conditions, and in a spirit of *mutual respect* between the parties, with employers learning to accept that employees are not military personnel taking order or candidates for brainwashing, and employees not abusing their new-found freedom, the penetration of social media into the workplace could result in a reduction of the democratic deficit that is inherent in subordinate employment and end up being positive on the whole.

It is to be hoped that this is not just wishful thinking. In any case, labour law should defend the values outlined above as it would be paradoxical if its protections were bypassed, in the 'magnificent and progressive destiny'[56] of the post-Social Media era, by a new social paternalism left to the discretion (and often the hypocrisy) of employers fundamentally worried about the commercial success of their business. In conclusion, to answer the question in the title of this article, important values and rights are at stake.

---

54 On the relevance of the non-domination theory for labour law, *see* D. Cabrelli & R. Zahn, *Theories of Domination and Labour Law: An Alternative Conception for Intervention?* 33 Int'l J. Comp. Lab. L. & Indus. Rel. 339 (2017).

55 For rich insights into the capability perspective, *see The Capability Approach to Labour Law* (B. Langille ed., Oxford, OUP forthcoming).

56 From Giacomo Leopardi, *La ginestra*, 1836. The Italian poet's ironic words, which were directed against his contemporaries' faith in progress, can be taken as a warning not to lose control of technologies designed to benefit human beings.