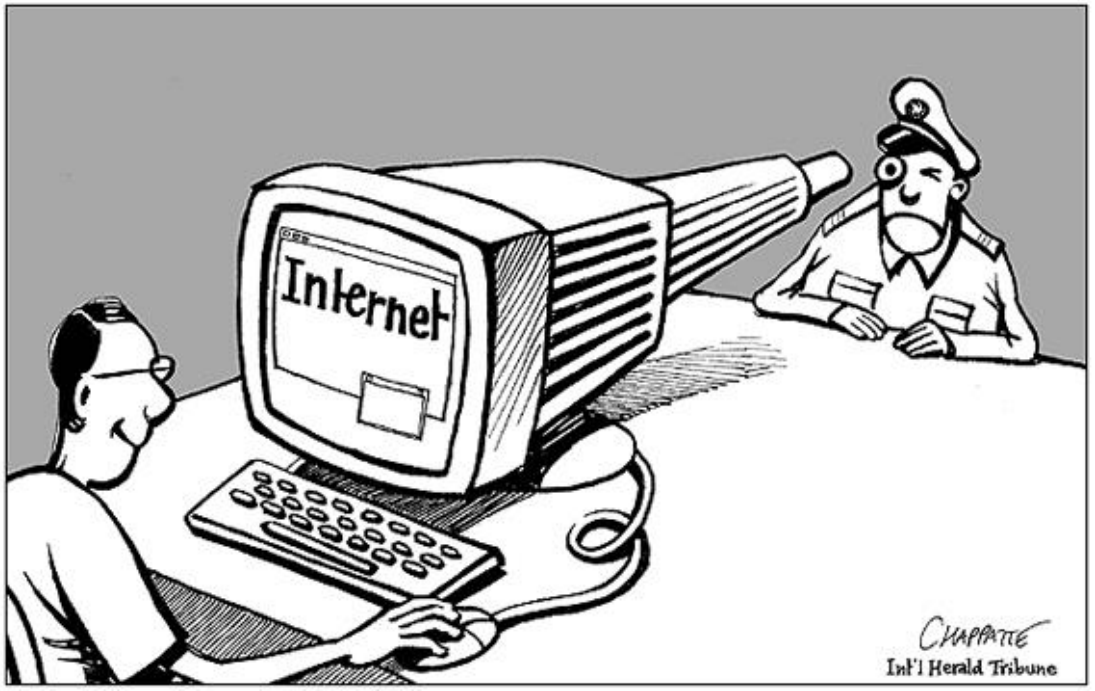
European Working Group on Labour Law

The right to privacy in employment

Italian Report

University of Cassino and Southern Lazio



Gianluca Minotti
Ilaria Purificato
Vanessa Tiseo
Ilaria Tomassi

European Student Seminar – Frankfurt (Oder)
Tuesday 21 - Friday 24 March 2017

Questions for National Reports

Introduction, general remarks and sources of law

1. "Right to privacy": Is a right to privacy recognized in your system of law (apart from art. 8 ECHR and art. 7 and 8 of the Charter of Fundamental Rights of the European Union [CFR]), i.e. in the constitution, in statutes, in national case law? If there is no explicit recognition of such a right, how are elements of it protected in your legal system? What has the role of the right to privacy in art. 8 ECHR and art. 7, 8 EU-CFR been in your domestic legislation and case law?

Surveillance at work:

2. In what cases and in which form is surveillance of employees at work legal and in which cases/forms is it prohibited? Please consider: (secret) video and audio taping, monitoring of computer and email activities, GPS tracking, personal searches etc. What are the relevant sources of law?
3. Data protection relating to health: In which cases (if at all) may the employer ask employees (or applicants) to reveal information relating to his/her health or submit to medical tests? What are the relevant sources of law?
4. What is the role of collective representation bodies in regard of secret or open surveillance measures? Is the works council's prior approval necessary?
5. Do executive and/or independents authorities occupied with data protection (= authorities which uphold the laws protecting personal data) exist and what is their role in this context? Can such authorities impose sanctions for non-compliance with data protection legislation? Is it a (criminal) offense to collect or process data in violation of the applicable protective provisions?
6. Optional: Is it – generally speaking – legally possible to use material (video, photos, testimonies) obtained through illegal (covert) surveillance measures for dismissals? Is such material admissible as evidence in court especially in claims against dismissals?

Whistleblowing:

7. In which cases – if at all – are whistleblowers protected against dismissal in your country?

Social media in the working relation:

8. Are the (legal) consequences of postings over social media about the employer, superiors, colleagues, workplace conditions and so on an issue in your country? If yes, can such postings lead to a dismissal and / or slander claims?

Table of contents

7.2 The legal grounds for the protection of whistleblowers

7.3 The specific rules protecting civil servants

7.4 The protection of employees within the private sector: main crucial points

7.5 The balancing performed by case law between the employees' right to information and right of criticism, on one side, and the employer's right to secrecy and personality rights, on the other side: protected behaviours

7.6 Protections for the whistleblower in case of dismissal or mobbing

8. Social media in the working relation

1. The right to privacy in Italy: legal framework

1.1 Constitution

The Italian Constitution (promulgated on 27 December 1947) contains no express guarantee of the right to privacy.

Anyway, the existence of this right may be derived, according to the doctrine and the case law, from the systematic interpretation of other relevant provisions of the Constitution such as:

a) **art. 13**, according to which "*Personal liberty is inviolable. No form of detention, inspection or personal search nor any other restriction on personal freedom is admitted, except by a reasoned warrant issued by a judicial authority, and only in the cases and the manner provided for by law. In exceptional cases of necessity and urgency, strictly defined by the law, law-enforcement authorities may adopt temporary measures that must be communicated to the judicial authorities within forty-eight hours. Should such measures not be confirmed by the judicial authorities within the next forty-eight hours, they are revoked and become null and void. All acts of physical or moral violence against individuals subject in any way to limitations of freedom shall be punished. The law establishes the maximum period of preventive detention*".

b) **art. 14** which provides that: "*The home is inviolable. Inspections, searches or seizures may not be carried out except in the cases and in the manner set out by law and in accordance with the guarantees prescribed for the safeguard of personal freedom. Controls and inspections for reasons of public health and safety or for economic and taxation purposes are regulated by special laws*".

c) **art. 15** under which "*The freedom and confidentiality of correspondence and of every other form of communication is inviolable. Restrictions thereto may be imposed only by a reasoned warrant issued by a judicial authority with the guarantees established by law*".

d) **art. 21, par. 1**, under which: "*All persons have the right to express freely their ideas by word, in writing and by all other means of communication*".

Moreover, the right to privacy has followed a fate similar to other "new" rights and found constitutional protection through an anchor to the principles contained in articles 2 and 3 of the Constitution.

Art. 2: "*The Republic recognises and guarantees the inviolable rights of the person, as an individual and in the social groups where human personality is expressed. The Republic expects that the fundamental duties of political, economic and social solidarity be fulfilled*".

Art. 3: "*All citizens have equal social dignity and are equal before the law, without distinction of sex, race, language, religion, political opinion, personal and social conditions. It is the duty of the Republic to remove those obstacles of an economic and social nature which really limiting the*

freedom and equality of citizens impede the full development of the human person and the effective participation of all workers in the political, economic and social organization of the country".

1.2 The fundamental role of case law before the explicit normative recognition

In the absence of a specific legal regulation, the right to privacy was first recognized by the courts. After World War II, the courts were forced to take affirmative steps toward the protection of a person's private life in order to answer the challenges of technological evolution.

From the 1950s until the first half of the 1970s, there was a clear contrast between the decisions of the Courts of first instance and those of Appeal: the former recognized the right to privacy, while the latter refused to acknowledge it. An example of this contrast can be found in the well-known *Caruso* case (Rome Court, 14.09.1953).

Caruso was a famous opera singer; after his death, his heirs asked the Court of Rome to protect his private life by barring the disclosure of certain indiscretions that would have harmed his privacy and memory.

The Rome Court rendered an innovative decision, recognizing the existence of a right to privacy, which implied the prohibition of intruding into someone's private sphere.

Nonetheless, the Court of Appeal of Rome (ruling of 17.05.1955) and then the Court of Cassation (22.12.1956, n. 4487) reversed the decision rendered by the Tribunal, stating that the simple desire for privacy alone could not be protected by the law.

It was only in the seventies that the Constitutional Court (ruling no. 38 of 12.4.1973) and the Court of Cassation (ruling no. 2129 of 27.05.1975) finally acknowledged the existence of the right to privacy, stating that "*a general right to privacy is deemed to exist in our legal system, a right protecting strictly personal and domestic situations [from disclosure] if not justified by preeminent public interests*".

This case opened the way for a series of decisions confirming the right to privacy.

There were no landmark cases; rather, the courts, with their intense activity, built a path that, decision after decision, led to the adoption of the first legal measures.

As affirmed by the afore mentioned Court of Cassation, the regulation of the areas of protection of the privacy of the subject, even if not expressly mentioned in the constitutional dispositions, has its first referent in the complex of the principles obtainable from articles 2 and 3 of the Fundamental Paper.

The right to privacy, as a right of the personality, allows, in fact, to individualize the correlative juridical base directly anchoring to art. 2 of the Constitution, provision of prescriptive and not programmatic character (see also Court of Cassation, ruling no. 5658 of 1998).

The reference to art. 2 is also relevant from the point of view of the recognition and guarantee of fundamental human rights, for the bond that is establishes between people and social groups, to the express terms of the mandatory duties of economic solidarity, political and social nature.
Articles 2 and 3 express the personalist principle that individualizes a priority of value of the human person in the hierarchy of the juridical values.
Articles 2 and 3 of the Constitution affirm, therefore, the inviolability of the right to privacy that, being part of the core of the fundamental principles, is not subject to constitutional review: such a review would result, in fact, in a rupture of the established order.
The right to privacy is described by the doctrine as the right to hold secrets aspects, behaviours, actions, related to the intimate sphere of the person, preventing that such information is divulged without the authorization of the interested subject.
Besides the "negative" aspect of the right as non-interference, privacy has also a "dynamic" aspect because the subject has the power to control the dissemination of his/her data, by intervening against conducts of disruption or aggression.

1.3 Statutory provisions

1.3.1 Act No. 675/1996 - Data Protection Authority

The first law dealing specifically with the issue of data protection was enacted in 1996 (Act No. 675) in order to implement EU Directive 95/46 on Data Protection.
Act No. 675/1996 instituted the “Garante per la Protezione dei Dati Personali” (Data Protection Authority) in order to ensure lawful data processing and the respect of people’s fundamental rights.
The Garante is an independent and autonomous collegiate body whose nature, composition and functions will be examined *infra* in paragraph 5.

1.3.2 Personal Data Protection Code (Legislative Decree No. 196 of 2003)

Act No. 675/1996 was then repealed and replaced in 2003 by the “*Codice in Materia di Protezione dei Dati Personali*” (Personal Data Protection Code - Legislative Decree No. 196 of 30.06.2003), which implements both EU Directive 95/46 on Data Protection and Directive 2002/58 on Privacy and Electronic Communications.
The Code expressly recognizes that "*everyone has the right to protection of the personal data concerning them*" (art. 1) and is aimed at ensuring that personal data are processed by respecting

data subjects' rights, fundamental freedoms and dignity, particularly with regard to confidentiality, personal identity and the right to personal data protection (art. 2, par. 1).

According to art. 2, par. 1, the processing of personal data shall be regulated by affording a high level of protection for the rights and freedoms referred to in paragraph 1 in compliance with the principles of simplification, harmonisation and effectiveness of the mechanisms by which data subjects can exercise such rights and data controllers can fulfil the relevant obligations.

The Code brings together all the various laws, codes and regulations relating to data protection since 1996.

There are three key guiding principles behind the code, which are outlined in section 2:

1. Simplification
2. Harmonisation
3. Effectiveness

The code is divided into three parts.

The first part sets out the general data protection principles that apply to all organisations.

Part two of the code provides additional measures that will need to be undertaken by organisations in certain areas, for example, healthcare, telecommunications, banking and finance, or human resources.

Part three relates to sanctions and remedies.

It is expected that the second part of the code will be developed further through the introduction of sectoral codes of practice.

Scope - The code applies to all processing within the State and its territories. It will also affect outside organisations that make use of equipment located within Italy, which could include e.g. PCs and other computer-based systems (see Section 5 of the Code). If an organisation outside the EU is processing data on Italian territory, it must appoint a representative in Italy for the application of Italian rules (this will be necessary for notifying with the Garante, if notification is due, and providing data subjects with information notices).

Main Features of the Data Protection Code

Notification - One of the key targets for simplification was the notification process, which was made more straightforward compared to the 1996 Act in line with the EU Data Protection Directive - which allows the notification process to be simplified in cases where data processing does not adversely affect the rights and freedoms of data subjects (see Article 18(2) of the directive). Under the Italian code, organisations are only required to notify the Garante when processing higher-risk categories of data. These include, in particular, genetic and biometric data, data processed for the purpose of analysing or profiling individuals, and credit-related information

(see Section 37 of the code for additional details). This approach is also aimed at making the process more transparent and understandable for individuals.

Data minimisation - Section 3 of the code introduces the element of data minimisation into Italian data protection. The code encourages organisations to make use of non-personal data whenever possible.

Data subjects' rights/Decision taking - The code aims to strengthen individuals' data protection rights, allowing them to exercise their rights and instigate proceedings more easily. In an effort to simplify the complaints process, the Garante has published a complaints form on its website. The Garante can also order businesses to abide by compliance requirements set out in its decisions. When responding to investigations, businesses now have 15 days to comply, compared to the previous 5-day timeframe. The turnaround for dealing with complaints has been raised to 60 days (previously it was 30 days); this period was found to be suitable in order for the Garante to work effectively and the parties to prepare their pleadings appropriately.

International Data Transfers - The data protection Code has incorporated and, to some extent, updated the previous rules on data transfers (data transfers are addressed in Sections 42-45 of the Code). Whereas previously businesses had to notify the Garante of their intention to transfer data outside the EU, under the new system companies will only have to provide notification in cases in which the transfer of data could prejudice data subjects' rights (see the Notification section). Additionally, the new system does not require organisations to resubmit notifications each year The rules for legitimising transfers to non-EU countries can be found in Section 43 of the Code and include consent, meeting contractual obligations, public interest requirements, safeguarding life/health, investigations by defence counsel, use of publicly available data, processing for statistical/historical purposes. Additional provisions for legitimising transfers are laid out in Section 44 of the Code and include transfers to countries deemed adequate by the European Commission, the adoption of contractual safeguards, and the use of binding corporate rules. Data subjects are entitled to lodge claims in Italy for non-compliance with the said contractual/corporate safeguards.

Main Features in Respect of Specific Processing Operations

Human Resources Data - The code has fully implemented Article 8 (b) of the EU directive which applies to the processing of data. Organisations processing sensitive data that wish to find an alternative to the somewhat unreliable issues of employee consent, can look at the exemptions laid out in Section 26 of the code. For example, Section 26 (4d) allows the processing of sensitive data without consent if necessary to meet obligations under employment law.

Health data - Processing is allowed with the data subject's consent (which must be provided in writing) and the Garante's authorisation if the data controller is a private body. As for public bodies, processing is allowed if it is provided for in laws/regulations; however, the latter must set out the specific processing operations and purposes in detail, otherwise the relevant public bodies must specify them via ad-hoc regulatory instruments. The data subject's consent is not required, in principle, whilst the Garante's authorisation is necessary except for the processing by health care professionals that is indispensable with a view to the data subject's health and/or bodily integrity. The Garante's authorisation has been granted in the form of an instrument applying to several entities and/or processing operations, i.e. as a "General Authorisation for the Processing of Sensitive Data" by various categories of data controller (see Legislation section). It should be recalled that specific provisions are laid down in the DP Code to regulate the processing of medical data in the health care sector (Sections 75-94). In particular, health care professionals and public health care bodies may process medical data (the Code refers to "data suitable for disclosing health") with the data subject's consent and without the Garante's authorisation if the processing concerns data and operations that are indispensable with a view to the data subject's health and/or bodily integrity; conversely, they may process medical data without the data subject's consent but with the Garante's authorisation if the processing is indispensable to safeguard public health.

Electronic Communications Data - The Code has implemented the provisions contained in the E-Communications privacy directive 2002/58/EC as well as in the data retention directive (2006/24/EC) (see Title 10, Part 2 of the Code). One of the main principles is on electronic marketing which requires organisations to obtain prior consent before sending electronic marketing to consumers (see Section 130). This applies to all forms of e-marketing, including e-mail, fax, SMS/MMS etc.. Specific provisions were added to regulate telemarketing. There is also a ban on sending e-marketing from anonymous addresses - this is a breach of the data protection code as the data controller has withheld its identity. As for data retention, communications service providers (CSPs) are permitted to retain traffic data for only a six-month period in order to deal with disputes over billing and subscriber services (section 123(2)). CSPs are also required to retain traffic data for longer in connection with law enforcement purposes; the retention periods are currently set at twenty-four months (telephone traffic data) and twelve months (electronic communications traffic data), irrespective of the given offence at issue (in pursuance of directive 2006/24/EC) (see section 132). Following ratification of Council of Europe's Cybercrime Convention (via Act no. 48/2008, which amended Section 132 of the DP Code), police authorities were enabled, under specific circumstances, to order IT and/or Internet service providers and operators to retain and protect Internet traffic data - except for contents data- for no longer than

ninety days, in order to carry out pre-trial investigations or else with a view to the detection and suppression of specific offences. The order issued by police authorities must be notified to and validated by the competent public prosecutor.

Main Features as to Compliance and Enforcement

Complaints - Data subjects can settle disputes either through the courts or by lodging a complaint with the Garante in case they have been prevented from exercising access/erasure/rectification/updating rights (as per Section 7 of the code). Organisations have 30 15 days to respond and can appeal to the Garante for more time. The Garante will then have 60 days to consider the request (see above "Data Subjects' Rights/Decision Taking").

Inspections - The Garante's inspection powers are laid out in Section 158 of the code. When investigating organisations, the Garante can request information and documents, although these requests are not legally binding. However, if there is no cooperation, and the organisations refuses access to its systems, the Garante can apply for a judicial order to carry out an investigation.

When carrying out formal inspections, the Garante can demand copies of manual records and databases, which may be passed onto the judicial authorities. A report of the outcome is then published.

Codes of Conduct

Legislative decree 196/2003 has enhanced the importance of codes of conduct and professional practice in respect of the protection of personal data.

In particular, it provides for their adoption in several, highly significant sectors such as processing of data via the Internet and/or in the employment context, for purposes of direct marketing, by private credit reference agencies, or in connection with video surveillance activities. The main principle in this connection is that compliance with the provisions set forth in the relevant code of conduct is a prerequisite for the processing operations to be lawful - see section 12(3). Adoption of the codes of conduct takes place following the impulse given by the Italian DPA with the involvement of the relevant industry sector; a specific procedure is envisaged and the final instrument is to be published in Italy's Official Journal (the official collection of legal and regulatory instruments).

The codes adopted so far in the various sectors are:

- Code of Practice Applying to the Processing of Personal Data Performed with a View to Defence Investigations;
- Code of conduct and professional practice applying to information systems managed by private entities with regard to consumer credit, reliability, and timeliness of payments;

- Code of conduct and professional practice applying to processing of personal data for statistical and scientific purposes;
- Code of conduct and professional practice applying to the processing of personal data for statistical and scientific research purposes within the framework of the national statistical system;
- Code of conduct and professional practice Regarding the processing of personal data for historical purposes;
- Code of Practice Concerning the Processing of Personal Data in the Exercise of Journalistic Activities;
- Code of Ethics and Conduct in Processing Personal Data for Business Information Purposes.

Guidelines concerning employment context

The Garante has adopted several guidelines specifically regarding **the employment context** such as:

1) Guiding Principles Applying to the Processing of Employees' Personal Data for the Purpose of Managing Employment Relations in the Private Sector (23 November 2006);
2) Guidelines applying to the Use of E-Mails and the Internet (1 March 2007);
3) Guiding Principles on the Processing of Employees' Personal Data in the Public Sector (14 June 2007)
4) Vehicle Geo-Location and Employer-Employee Relations (4 October 2011).

2. Surveillance at work

2.1 Foreword and sources of law

The power of control constitutes an indisputable component of the employer's directive power.

The matter of controls at work is regulated by the Workers' Statute (Act No. 300/1970 - Articles. 2-6) and further restrictions of the power of control were introduced by the aforesaid Personal Data Protection Code (Legislative Decree No. 196/2003).

Legislative Decree No. 151/2015 has recently modified article 4 of the Workers' Statute concerning the control at a distance of employees with audio-visual instruments and other machinery.

The entire regulation is aimed at finding the fair balance between the right of the employer to control that the work is performed in accordance with its directives and those of the workers not to see violated their privacy, personal dignity, freedom of expression and communication.

2.2 Article 2 of the Workers' Statute: controls carried out by private police

Art. 2 of Act No. 300 of 1970 prohibits using security guards -fairly frequent in the past- inside firms for reasons other than the protection of private property, in particular for the purpose of controlling workers' activities.

The aim of this provision is to prevent that the presence of the private police in the workplace may result in an intimidating and degrading environment, detrimental to the dignity and freedom of workers.

Consequently, these security guards are forbidden in principle from entering work premises and from denouncing violations of the employees' duties (not related to private property).

The violation of this disposition is sanctioned under criminal law with a fine ranging between 154 and 1.549 Euros or with incarceration for a period of 15 days to 1 year, unless the violation falls within the criminal code and is punishable by criminal sanctions.

In the more serious cases, both sanctions (fine and incarceration) can be imposed against the employer.

Furthermore, the judge may increase the fine up to 7.745 Euros if, taking into account the employer's means, the maximum fine of 1.549 Euros is not effective.

The court can order publication of the sentence as an additional sanction.

2.3 Article 3 of the Workers' Statute: the supervisory personnel

According to Art. 3 of Act No. 300 of 1970 "*The names and specific tasks of the personnel responsible for the supervision of the work activities must be communicated to the workers concerned*".

Article 3 seeks to balance two needs: avoiding hidden controls since they would be unfair and offensive to the dignity of the worker; allowing the employer to verify the exact fulfilment of the job performance.

In the absence of specific indications, it is believed that communication imposed by art. 3 can take place by any appropriate means to achieve its purpose.

2.4 Article 4 of the Workers' Statute: limits to the power of control at a distance of employees with audio-visual instruments and other machinery

Legislative decree No. 151/2015 has rewritten the text of article 4 of Act No. 300 of 1970. This provision regulates remote controls or, to be more accurate, the limits to the employer's controls made through audio-visual instruments or other machinery including digital and electronic tools.

Art. 4 aims to balance the needs of the employer, who aspires both to control the proper fulfilment of the work performance and to protect the corporate heritage, and the right to privacy of the

worker, which is an expression of the fundamental rights of the individual.

The new wording of article 4 of the Workers' Statute is the following:

"*1. If the audio-visual devices and other instruments can control at a distance the employees' activity, they will be only used for organizational, productive and safety reasons and for the need to protect the corporate heritage. The installation needs a prior collective agreement with trade unions or, in case the enterprises have productive units located in different provinces of the same region or in different regions, such agreement shall be concluded with the most representative unions at national level. In the absence of such agreement, the authorization by labour inspectorate in territorial headquarters it is necessary or, alternatively, the authorization by labour inspectorate in headquarters for enterprises with productive units located in different territorial areas of competence…*".

2. The provision under paragraph 1 shall not apply to instruments used by the workers to fulfil their job performance and to instruments used by the employer for recording access and attendance at work.

3. On condition that an adequate knowledge of methods of use and procedures for checks is given to the employee and in compliance of Legislative Decree No. 196/2003, the information collected pursuant to paragraphs 1 and 2 may be used for all purposes relating to the employment relationship".

The first paragraph of article 4 provides, as seen, the possibility of using "*audio-visual devices and other instruments which can control at a distance the employees' activity*" where the term "*at a distance*" is referred both to a spatial extension (control carried out in a place far away from the place where the employee works) and temporal extension (control carried out in a different moment from the time of the performance) of the control.

However, the provision sets out strict limits:

- first of all, the employer is allowed to install the instruments only if organizational, productive and safety reasons occur or in case of need to protect the corporate heritage.

-second, the installation of these instruments has to be preceded from a collective agreement concluded between the employer and RSA or RSU. In case the enterprises have productive units located in different provinces or regions, the agreement may be concluded at national level, and, if the enterprise is lacking any agreement, it is essential to obtain an administrative license from the labour inspector.

2.4.1 Labour instruments

The aforesaid limits do not extend to paragraph 2 of article 4. Indeed, paragraph 2 provides that

the control through instruments used by the workers to fulfil their job performance and through instruments used by the employer to record access and attendance at work can be carried out without the limits fixed by paragraph 1 because the collection of information takes place, in this case, while the worker is using the tool.

However, an active role of the employee is necessary in the use of the instrument.

Therefore, to be considered a "labour instrument", the tool must be used by the worker to perform her/his duties.

For these reasons, it is not possible to give a general definition of "labour instruments": they are an heterogeneous category and it all depends on the way the employer decides to qualify the instruments which will be used by the workers to perform their duties.

As a consequence, the same tool may be qualified as a labour instrument or as a control instrument depending on how the task is performed and how the employer's power is exercised.

2.4.2 IT instruments

IT tools deserve a particular attention because their use is widespread in the workplace nowadays.

It is essential to distinguish between hardware (*id est* the PC, the tablet, the smartphone) and the software which is installed on them.

When the employee uses these applications, they produce a particular type of information (called log) which is captured by the employer.

Usually there are hundreds of applications in one digital network and they interact with each other.

In order to configure the case referred to in the second paragraph of art. 4, the log has to be produced by the software used by the worker to perform her/his tasks and not by another application created to this purpose by the employer.

It is also essential to previously inform the employee about the functioning of the tools.

Thus, the worker is able to know which application produces log and how it will be used by the employer.

2.4.3 Instruments used for recording access and attendance at work

The reference to the "*instruments for recording access and attendance at work*" allow the employer to decide how to use these tools without necessarily having to restrict them to the recording of the start and end of the activity. Indeed, they can include movements of the worker during working hours. Moreover, it is generally accepted that the "access" is not restricted to the physical environment but is extended to digital methods of access to informatic networks.

2.4.4. Rules on processing employees' personal data: previous information

The use of the information obtained, both in case of paragraph 1 and in case of paragraph 2, is dependent on an adequate knowledge, by the employee, of "*methods of use and procedures for checks*" (art. 4, par. 3). Therefore, surveillance carried out without any employee's knowledge is considered unlawful because the employer has a burden to inform, clearly and in detail, employees about the proper use of the available instruments of control and about how and to what extent the checks are carried out.

Such purpose can be reached, for example, with the use of clear internal rules which are supported by an appropriate (written) information.

2.4.5 Reference to the Personal Data Protection Code and to Data Protection Authority's guiding principles

The use of the information obtained through the controls is also dependent on the respect of the provisions contained in the Personal Data Protection Code (art. 4, par. 3).

Such reference to Legislative Decree No. 196/2003 is complementary to article 4 of Act 300/1970.

As a consequence, the controls must be carried out in accordance with the general principles of necessity, fairness and relevance contained in the Code.

The Garante has also adopted several guidelines which have to be respected by the employer in the following matters.

2.4.6 E-Mails and Internet.

The Guidelines Applying to the Use of E-Mails and the Internet in the Employment Context (1 March 2007) instruct private and public employers to take several measures required in order to safeguard data subjects, consisting in the obligation to specify the usage arrangements employees are to comply with in respect of email and the Internet – whereby they shall have to clearly specify how the tools they make available should be used as well as whether, to what extent and in what manner controls are carried out.

According to the Guidelines, the employers have to take the following measures:

a. adopting and publicizing internal guidelines;

b. adopting organisational measures, in particular to

- carefully assess the impact on employees' rights;
- specify in advance which employees are allowed to use email and access the Internet, also by category/class;
- specify the location of workstations so as to reduce the risk of misuse.

c. adopting technological measures, which include in particular, but are not limited to, the following:

I. as for use of the Internet:

- specifying which websites (by category) are considered to be related/unrelated to work performance;
- configuring systems and/or using filters to prevent certain operations from being performed;
- processing data in anonymous format and/or in such a manner as to prevent users from being mmediately identified, by suitably aggregating the data in question;
- retaining the data for no longer than is necessary to achieve organisational, production and/or security purposes;
- providing for a layered approach to controls;

II. as for email services:

- making available email accounts to be shared by several employees, possibly along with individual accounts;
- making available an ad-hoc account to be used by an employee for private purposes;
- making available specific user-friendly functions to allow automatically sending out-of-office reply messages whenever it is known in advance that an employee will be absent from work, whereby such messages should provide details for contacting another employee and/or department at the company/body in question;
- where it is necessary to access the contents of email messages on account of pressing requirements related to work, and the relevant employee is absent from work unexpectedly and/or for a prolonged period, allowing the data subject (i.e. the employee in question) to entrust another employee (trusted party) with checking the contents of his/her email messages and forwarding such messages as are considered to be work-relevant to the employer (data controller). The data controller should keep specific records of these activities and the employee concerned should be informed thereof as soon as possible;
- including a disclaimer in email messages to clarify, where appropriate, that they are not to be regarded as confidential and/or personal in nature, specifying whether the replies may be accessed by third parties in the sender's organisation;
- providing for a layered approach to controls;

Moreover, the Guidelines prohibit private and public employers from processing personal data by means of hardware and software systems with a view to the distance monitoring of employees, in particular by means of the following:

a. the systematic scanning and recording of email messages and/or the respective external data apart from what is technically necessary to provide email services;

b. the reproduction and systematic storage of the web pages visited by employees;

c. keystroke pattern analysis and recording devices;

d. hidden monitoring/analysis of laptops entrusted to individual employees.

2.4.7 Vehicle geo-location

The Guidelines on Vehicle Geo-Location and Employer-Employee Relations (4 October 2011) require that public and private employers relying on location and positioning systems installed on board vehicles to meet organizational, production and/or occupational safety requirements:

a. Ensure, as a necessary measure, that vehicle location is not monitored continuously by the data controller in compliance with the data minimization principle, and that this is only done if it proves necessary in order to achieve the purposes legitimately pursued by the data controller;

b. Ensure, as a necessary measure, that the retention periods applying to the various data categories to be processed are proportionate to the individual purposes that are to be achieved, in compliance with the principle whereby the data must be relevant and not excessive;

c. Ensure, as a necessary measure, that any entities providing vehicle location and positioning transmission services are appointed as data processors in pursuance of the DP Code and receive such instructions as are necessary with regard to the lawful use of the data they collect, which must only serve the purposes set out in the location services agreement, by also determining the data categories to be processed and the relevant retention mechanisms and periods;

d. Ensure, as an appropriate measure, that a simplified information notice model is relied upon such as the one contained in Annex 1 hereto, to be used under the terms set out in the premises, in order to notify data subjects of the processing operations performed via the vehicle location system(s).

2.4.8 Use of the information collected by the employer

The information collected by the employer respecting the above described rules may be used for all purposes relating to the employment relationship and, consequently, also for disciplinary purposes.

2.4.9 Defensive controls

Particular attention has to be paid to the s.c. defensive controls. They are controls, carried out in various ways by employer, that are meant to preserve company's asset and/or to prohibit unlawful behaviours. On the contrary, they are not carried out to verify the exact fulfilment of the job performance.

For such checks, the law requires the agreement with the trade unions or the administrative authorization only when "*it is also possible a remote control of worker's activity*". Case law has often intevened on this matter.

For example, the judgment of Court of Cassation n 22662/2016 has decided on a lawful dismissal for misconduct noticed to an employee, who had stolen an envelope containing money from physiotherapeutic company's safe. The conduct was proved by a record of a camera installed in order to control the safe and not to checks the employees' activities.

Court of Cassation has consequently stated this principle of law: "*if the installation of control systems and devices for preserving the corporate heritage does not implies the possibility of a remote control of work activities and if it respects the dignity and the privacy of employees, it will not be subject to the limits set out in article 4 paragraph 2 of the Workers' Statute*"

2.5 Personal searches

Art. 6 of the Workers' Statute regulates personal searches providing that "*The personal searches on the worker are forbidden except in the cases in which they are necessary for company assets' protection, in relation to work tools' or raw materials' or products' quality.*

In such cases, personal searches are permitted only if they are performed at the exit of the workplaces, provided that the employees' dignity and privacy are safeguarded and that they are carried out with the application of automatic selection systems related to the community or to groups of workers.

The hypotheses in which the personal searches can be carried out, as well as, subject to the conditions specified in the second paragraph of this article, the detailed rules governing such searches must be agreed by the employer with the company union representatives or, failing that, with the internal commission. In the absence of agreement, on an employer's request, the Labour Inspectorate provides...".

According to the predominant case law (Court of Cassation n. 14197/2012; n. 12197/1999; n. 1461/1988) art. 6 of the Workers' Statute should only apply to physical inspections, given that the disposition literally regards only "*personal visits*".

In particular, according to the mentioned rulings (also confirmed by the merit case-law: Potenza's Court of Appeal May 2, 2015 n. 102; Alba's Court April 30, 2009) searches (for example) on the accessories (bags, pockets, etc..) can be carried out without the procedural constraints referred to in the aforesaid art. 6.

The Constitutional Court (judgment June 25 of 1980, n. 99) stated that these controls don't conflict with the Constitution's provisions that protect personal freedom (articles 2, 3, 13) because they require, in any case, the consent of the person concerned.

In case of unjustified employee's refusal to undergo to the personal searches, however, he or she may be subject to a disciplinary procedure (Cass. November 19 of 1984, n. 5902).

It is important to underline that these searches, according to the first paragraph of art. 6, are considered as an "*extrema ratio*" a mean to be used only if it is not possible to carry out alternative technical controls legally enforceable (such as the metal detectors, the banning of bags in working areas, etc.).

Moreover, personal searches can only be performed "*at workplaces' exit*" (art. 6, paragraph 2) and respecting the worker's dignity and privacy (for example a search carried out by a controller of the same sex of the worker); in order to avoid any discrimination, the choice of the workers to be searched has to be made with "*the application of automatic sorting systems related to the community or related to workers' group*", where "*automatic selection*" means a selection without discretion of management or supervisory staff.

The hypotheses in which personal searches can be carried out and the rules governing such searches must be agreed by employer with r.s.a. or with r.s.u., and, failing an agreement with them, "*provides the Labour Inspectorate on the employer's request*" (art. 6, paragraph 3 workers' statute).

Under art. 38 of the Workers' Statute, the violation of this disposition is sanctioned penally with a fine ranging between 154 and 1.549 Euros or with incarceration for a period of 15 days to 1 year, unless the violation falls within the criminal code and is punishable by criminal sanctions (for example kidnapping). In the more serious cases, both sanctions (fine and incarceration) can be imposed against the employer. Furthermore, the judge may increase the fine up to 7.745 Euros if, taking into account the employer's means, the maximum fine of 1.549 Euros is not effective. The court can order publication of the sentence as an additional sanction.

3. Data protection relating to health

3.1 Article 5 of the Workers' Statute: checks on physical fitness and illness of the employees

Article 5 of the Workers' Statute prevents the employer from directly checking (id est through doctors of his own choice, suspected of being partial) the physical fitness and the illness of his employees.

Check on absences due to illness or work accidents can only be made through the inspection services of the relevant social security institutions, which are obliged to carry out them when requested by an employer.

This principle is held applicable also to medical checks previous to hiring.

As regards checks on physical ability, Italian legislation gives the employer the opportunity to carry out these controls in certain cases (for instance to verify the healing after a re-entry for infirmity) and reserving such controls exclusively to public entities and specialised public institutes.

These checks are made with a dual purpose: on one side, the protection of the employer's interest to the exact fulfilment of the job performance, that only a physically fit employee is able to ensure; on the other side, the protection of the employee's safety and health constitutionally guaranteed and provided for by article 2087 of the Civil Code as an employer's obligation.

As mentioned above, our legal system provides the possibility, for the employer, to carry out pre-contractual medical examinations which were, for a long time, in the middle of an extensive debate between doctrine and case law, about their being subject or not to the discipline of art. 5 of the Workers' Statute.

This debate has been overcome in the light of a systematic consideration of the Statutory regulation, which does not admit any discrimination between workers who aspire recruitment and workers already hired, recognizing, therefore, a broad interpretation of the provision.

Furthermore, Article 39 of Legislative Decree n.81/2008 regulates the hypothesis in which the employer may appoint a competent doctor to whom entrusts "*compulsory health surveillance*": to said doctor is entrusted task to carrying out periodic and preventive examinations aimed to assess employee's physical ability about specific tasks, but also and above all, only under conditions specified by law.

Under art. 5 of the Workers' Statute, the performing of the controls on the absence determined by illness is reserved, as we have seen, to "inspection services of competent social security institutes". In case of illness, a doctor draws up an electronic certificate, which will be sent to INPS (within 48 hours) and communicates to employee the transmitted certificate protocol number. The employee, then, has the obligation to communicate promptly to the employer the absence period; then INPS will send certificate, received by doctor, to the employer within a maximum of 48 hours. Only the prognosis certificate and not the diagnosis will be sent to employer, in order to

safeguard the employee's privacy and with the only exception of the case in which the worker is affected by infectious disease. In some cases, it is in the employee's interest, who want to take advantage from special favourable rules laid down by the legal system, to reveal to the employer the suffering from diseases such as, for example, tuberculosis or cancer, given that the implementation of this special rules cannot disregard the disease knowledge by employer.

It is evident that in the employment relationship there are many interests related to the binomial health – privacy, such as the employee's interest to preserve secret information about his health so that employer cannot use them in a discriminatory manner, but this information, at the same time, is useful to ensure that the employer directs the worker to compatible tasks with his or her health condition. About infectious diseases, it should be noted that article 5 and 6 of Act No. 135/1990 protect employees anonymity when they are affected by HIV.

Sick employees have to remain at their domicile in time bands of availability (from 9 am to 1 pm and from 3 pm to 6 pm) being at disposal for eventual medical checks, unless there is a justifiable reason to absence. If sick employee is not available without a justifiable reason, he or she loses the economic treatment provided for by law. Another burden on sick employee is to allow visit performing: refusal would be disciplinary offense.

In case of employee's illness for accident at work, controls mentioned above cannot be carried out except by I.n.a.i.l. (National Institute for Insurance against Accident at Work); moreover, legislation about availability at certain times does not find application.

In case of violation of art. 5, the employer is sanctioned under criminal law according to the above examined art. 38 of the Workers' Statute.

4. The role of collective representation bodies in regard of surveillance measures

As it has been previously highlighted, the RSU (or RSA) role is relevant, as well as provided for by paragraph 2 of art. 4 of the Workers' Statute: an agreement between trade unions and the employer is, in fact, necessary in order to use "*audiovisual system and tools from which also derives the possibility of remote employee's monitoring*". It is relevant because, failing such an agreement, an authorization by Territorial Labour Direction or Labour Ministry is required.

These agreements (or, possibly, permissions) play an important role in checking legality and correctness in using these instruments in order to protect the employees' rights.

5. The role of the Italian Data Protection Authority (Garante per la protezione dei dati personali)

The Italian Data Protection Authority (Garante per la protezione dei dati personali) is an independent authority set up, pursuant to Article 8 of the Charter of Fundamental Rights of the

European Union, to protect fundamental rights and freedoms in connection with the processing of personal data, and to ensure respect for individuals' dignity.

The Data Protection Authority was set up in 1997, when the former Data Protection Act (Act No. 675/1996) came into force, and its composition and functions are currently provided for by the Legislative Decree No. 196/2003 (Personal Data Protection Code).

The Garante is an independent and autonomous collegiate body composed of four members, two of whom are elected by the Chamber of Deputies and two by the Senate from among "*persons ensuring independence and with proven experience in the field of law or computer science*".

The elected members hold office for seven years, and the appointment cannot be renewed. Under penalty of losing office, they cannot carry out professional or advisory activities, manage or be employed by public or private entities, or hold elective offices.

The tasks of the Garante are described in article 154 of the Personal Data Protection Code and include the following:

• supervising compliance with the provisions protecting private life;

• handling claims, reports and complaints lodged by citizens;

• banning or blocking processing operations that are liable to cause serious harm to individuals; • checking, also on citizens' behalf, into the processing operations performed by police and intelligence services;

• carrying out on-the-spot inspections to also access databases directly;

• reporting to judicial authorities on serious infringements;

• raising public awareness of privacy legislation;

• fostering the adoption of codes of practice for various industry sectors;

• granting general authorisations to enable the processing of certain data categories;

• participating in Community and international activities, with particular regard to the work of joint supervisory authorities as per the relevant international conventions (Schengen, Europol, Customs Information System).

Furthermore, the Garante draws Parliament's and the Government's attention to the need for regulatory measures in the data protection sector and renders mandatory opinions on regulatory instruments and administrative measures drafted by public administrative bodies.

The authority submits an annual report to Parliament describing its activities.

5.1 Administrtative and criminal sanctions

Violations of the Personal Data Protection Code are punishable with heavy sanctions that, according to the nature of the infringement, may be either administrative or criminal.

Administrative sanctions

Under Sections from 161 to 166 of the Code, the breach of the provisions protecting personal data shall be punished by a fine, directly applied by the Garante, consisting in the payment of a sum of money ranging, according to the type of violation, between six thousand and three hundred thousand Euro.

The amount of the fines may be increased up to four times if it is found to be ineffective on account of the offender's economic status.

Criminal sanctions

Under Section 167 of the Code (Unlawful Data Processing):

1. any person who, with a view to gain for himself or another or with intent to cause harm to another, processes personal data in breach of Sections 18, 19, 23, 123, 126 and 130 or else of the provision made further to Section 129 shall be punished, if harm is caused, by imprisonment for between six and eighteen months or, if the offence consists in data communication or dissemination, by imprisonment for between six and twenty-four months, unless the offence is more serious.

2. any person who, with a view to gain for himself or another or with intent to cause harm to another, processes personal data in breach of Sections 17, 20, 21, 22(8) and (11), 25, 26, 27, and 45 shall be punished by imprisonment for between one and three years if harm is caused, unless the offence is more serious.

Under Section 170 of the Code (Failure to Comply with Provisions Issued by the Garante), whoever fails to comply with a provision issued by the Garante, in breach of the relevant obligations, shall be punished by imprisonment for between three months and two years.

6. Use of material obtained through illegal surveillance measures for dismissals and as evidence in claims against dismissals

In the Italian legal system, material derived from unlawful surveillance measures cannot be used neither for dismissal nor as evidence in claims against dismissal.

7. Whistleblowing in Italy

7.1 The significance of whistleblowing in the Italian legal system

Whistleblowing is not significant at all in the Italian legal system. There are only a few – about a few dozen – decisions published dealing with the issue and there is little literature on the subject-matter.

The reason for the poor attention paid to whistleblowing mirrors the poor spread of the phenomenon throughout the social reality and also depends on the fact that there are no specific rules in Italy for the protection of whistleblowers.

7.2 The legal grounds for the protection of whistleblowers

Even though there is no law of general application whatsoever for the protection of whistleblowers, nonetheless, case law in any event finds effective protection instruments in the legal system, first, against dismissal, but also more in general against retaliatory and discriminatory acts, and mobbing put in place by the employer or by the colleagues to whom the complaint relates.

Solely recently, within the framework of wider rules aimed at repressing corruption and illegality within the public sector, has a specific rule for the protection of whistleblowers who are civil servants been introduced.

7.3 The specific rules protecting civil servants

Art. 54 *bis* of Legislative Decree No. 165/20015 sets forth that the civil servant, who reports to the Courts or to the "Corte dei Conti" (the administrative authority in charge of controlling the administrative and accounting compliance by the public entities) or to his/her senior manager unlawful behaviours of which he/she has become aware in light of his/her employment, shall in no way be subject to disciplinary penalties, nor may he/she be dismissed, and in no way may he/she undergo any discriminatory measure, either direct or indirect, having an impact on the work conditions for reasons directly or indirectly linked with the complaint. Should any such measures be adopted, the party concerned and the trade unions shall report the foregoing to the Public Service Department for all necessary measures.

The whistleblower who reports false facts or facts not committed by the person to whom the complaint relates shall not be subject to this type of protection, thus becoming criminally liable for the slander or defamation offences, or civilly liable by any such way for unfair damage.

As we shall see in detail hereunder, the rule limits itself to expressly stating – for the specific public service sector – principles which may already be retrieved from the legal system as a whole and which are also valid for employees within the private sector. Indeed, the code of silence – that is the obligation to keep quiet about unlawful acts, which are significant from a criminal, administrative or disciplinary standpoint, put in place by the employer or by senior managers and by colleagues, and attributable to the employer – does not fall within the scope of the obligations of employees.

All things being like this, it is clear that the complaint made by the employee as to unlawful behaviours held in the company does not amount to any breach of the contractual obligations and, precisely for this reason, he/she is not liable to any repressive measure taken by the employer (disciplinary penalty, dismissal or any other unfavourable measure which, precisely in light of the aim connoting same, exactly takes the shape of a discriminatory measure).

Art. 54 *bis* of Legislative Decree No. 165/2001 adds to the general principle just mentioned above specific provisions for the protection of the secrecy of the whistleblower's identity, both throughout the disciplinary procedure and in accessing the relevant administrative records, such as not to expose him/her to the greatest possible extent to any retaliation whatsoever by the persons to whom the complaint relates.

From the former standpoint, the aforesaid art. 54 *bis* sets forth that – during the disciplinary procedure issued against who has committed the unlawful act –, in no way shall the whistleblower's identity be revealed without his/her consent. An exception to the above would be the case in which the formal disciplinary notice is totally or partially grounded on the whistleblower's complaint and the knowledge of the latter's identity is of the essence for exercising the right to defence.

From the latter standpoint, then, the whistleblower's complaint is not subject to the access foreseen in general for administrative records.

The provision thus overcomes the firm stance of administrative case law, pursuant to which each single party needs to be able to precisely take cognisance of the contents and of the authors of complaints and reports.

Art. 54 *bis* of Legislative Decree No. 165/2001 – despite having been greeted by law scholars, since it brings about the first protection specifically aimed at whistleblowers – has been deemed inadequate from different standpoints.

First of all, it has been pointed out that the rule does not specify the different ways and procedures in which employees may bring the relevant complaint.

It has then been stressed that the guarantee as to the secrecy of the whistleblower's identity is totally relative, since it is aimed at inevitably jeopardising when the reported behaviours have criminal significance and thus need be reported to the Public Prosecutor's Office. Finally, some have complained about the fact that the provision does not change – as it should have done in order to strengthen the protection of whistleblowers – the customary allocation of the burden of proof, especially, in so far as discriminatory dismissal is concerned.

7.4 The protection of employees within the private sector: main crucial points

As already stated, there are no specific provisions protecting whistleblowers who are employed by private employers. It is case law which – by arguing based on the principles and rules governing the employment relations – in any event ensures a protection for the employee bringing the complaint.

It needs be stressed that, up to now, case law has exclusively focused on whistleblowers who are employees. Therefore, and first of all, we shall give an account of the problems and solutions formulated in this respect.

Nonetheless, similar problems may be raised for self-employed workers, in particular, for any self-employed worker carrying out a personal activity.

The first issue that case law has had to solve concerns the mutual boundaries between the right to information and the right of criticism, on one side and, on the other side, the right to secrecy set forth by law in respect of business facts and information, and the personality rights granted to the employer by the Constitution.

Indeed, in interpreting case law, both the extent and the contents of the right to information and of the right of criticism – amounting to a variation of the principle of free expression of ideas, in general granted to all citizens by the Constitution and confirmed by the law in favour of employees – result from the balancing with the employer's right to the employees' loyalty, inclusive of a right to the secrecy of all business information and, moreover – as we shall see hereunder – with the employer's personality rights – to dignity, reputation, image –, which penetrate the employment agreement either pursuant to the general obligations of fairness and good faith in the performance of the agreement, or pursuant to the general principle of prohibition of any abuse of right.

The consequence is that, should the right to information and the right of criticism be exercised by exceeding the limits fixed by any such balancing, the employee shall be in default and shall expose himself/herself to the employer's lawful reactions (dismissal, disciplinary penalties).

Besides such fundamental issue, it is worth mentioning other issues pertaining, more in particular, to the ways through which the complaint may be brought.

First of all, we need to ask ourselves whether the employer needs to identify internal procedures for allowing the employee's complaint and whether the employee then necessarily needs to use them.

In this respect, it is worth taking into consideration the provisions set forth by Legislative Decree No. 231/2001 – aimed at guaranteeing the legality and transparency of the public authorities, and at preventing and repressing corruption – which, in foreseeing the administrative liability of legal entities for the very first time, for a series of specifically indicated criminal offences, lays an

obligation upon any entity willing to be exempted from any such liability to adopt organisational models aimed at preventing the perpetration thereof.

Secondly, we need to discuss the ways in which the employer may use the complaint received.

In this respect, there are problems arising from the relevant data protection rules (Legislative Decree No. 196/2003), which foresee that the employer may solely process the personal data provided that certain conditions are met.

Finally, there are issues arising in connection with the protection which may be called for by the whistleblower, which shall be dealt with in paragraph 7.6 hereunder.

7.5 The balancing performed by case law between the employees' right to information and right of criticism, on one side, and the employer's right to secrecy and personality rights, on the other side: protected behaviours

The Italian legal system lays a loyalty obligation upon employees, which expressly includes the obligation to secrecy, that is the obligation not to "*disclose information concerning the company's organisation and production methods*" (art. 2105 of the Civil Code). Should that obligation be breached, the employee shall be in default and shall thus be liable to disciplinary penalties up to reaching dismissal in the most serious cases (for justified subjective grounds or for just cause).

But which is exactly the content of the obligation to secrecy?

May it include a prohibition to disclose further information with respect to those specifically provided for under the law provision (information 'concerning the organisation and production') but, in any event, fit to cause damage to the company's reputation and image, thus damaging market competitiveness (it is sufficient, for instance, to think of any information concerning the company's financial trend)? And still: may said prohibition, should it be understood in the broad sense, go so far as to include any internal information of the company, including the irregularities and even the unlawful behaviours put in place within the company (such as the breach of safety at work rules, tax rules, anticorruption rules, and anti-mafia rules)?

In so far as the extent of the loyalty obligation is concerned and, for the purposes hereof, as regards the boundaries of the obligation to secrecy, there is a conflict between law scholars and case law: law

scholars deem that the obligation to secrecy needs be understood in a restrictive sense, since instrumental to protect the company's goodwill and, therefore, as provided for under the rule, solely with respect to the information "concerning the organisation and production" whilst case law, instead, tends to widen the content thereof, also including the disclosure of further information within the respective scope, in any event, provided that related to the running of the

business and fit to damage the image and reputation, also on the market (See Court of Piacenza, 6 June 2007. See also Cass. 6 May 1998, No. 4952)

In some cases, case law reaches the same result, that is of widening of the loyalty obligation (and of the obligation to secrecy) – thus understood as a general loyal behaviour obligation –, by enhancing the clauses of fairness and good faith in the performance of the agreement (Articles 1175 and 1375 of the Civil Code).

In any event, also in case law, it is undisputed that the obligation to secrecy laying upon employees does not entail a general code of silence: the fiduciary relation linking employees with the respective

employer – the expression of which is the loyalty obligation – "*concerns the employer's reliance on the employee's capacity to fulfil the work obligation and not on his/her capacity to share secrets which are not instrumental to the company's productive and/or commercial needs*" (Cass. 14 March 2013, No. 6501).

Indeed, the obligation to secrecy aims at solely protecting the entrepreneur's lawful activities, "*it being certainly not possible to request employees to fulfil any such obligations (...) even when [the entrepreneur] is willing to pursue unlawful interests*" (thus Cass. 16 January 2001, No. 519, which faces a case in which the whistleblower had reported to the Court the behaviour of the employer, who had tried to evade the tax authorities by concealing the sales of the manufactured goods).

Therefore, employees may certainly – and in some cases must– report the behaviours put in place in the company by the employer or ascribable thereto, which amount or may amount to criminal unlawful acts (for instance, corruption), administrative unlawful facts (for instance, breach of tax regulations), or civil unlawful acts (it is sufficient to think, for instance, of mobbing).

But case law goes beyond.

It is a shared opinion that the employee's complaint does not need to be solely limited to the specific unlawful acts, but may also have as purpose facts or behaviours which are just irregular or even perfectly lawful (such as, for instance, investment policies or any choices of manufacturing decentralisation or delocalisation), and may also include critical assessments and opinions of the whistleblower.

From a more in-depth view, it emerges – and this is the aspect of greatest interest – that the focal point of judicial control, regardless of the purpose of the complaint and of the employee putting it in place, is not the compliance with the obligation to secrecy which, even if it is often cross-referenced, fades into the background.

Instead, the Judges directly balance the employee's right to information and right of criticism set forth by the Constitution, on one side and, on the other side, the likewise constitutional personality rights

of the employer (dignity, reputation, image) to the respective ideal and economic extent. In order to do so the Judges check, in particular, whether the right to information and the right of criticism have been exercised in compliance with certain limits: limits of content (the principle of substantive restraint), formal or procedural limits (principle of formal restraint), and finalistic limits (principle of the pursued interest).

Only provided that these limits are complied with will the right to information and the right of criticism be lawfully exercised, thus a breach on the employee's side would not take shape.

Therefore, such limits have to be analysed separately.

In so far as the limits of content are concerned (principle of substantive restraint), firm case law requests that the complaint has as purpose true facts or, at least, facts which the whistleblower deems true, without any wilful misconduct or gross negligence (the so-called putative truth). Therefore, the employee must control, to the extent possible in light of the role held in the company, the truthfulness of the reported facts, thus being under the obligation to refrain from falsely accusing someone of the facts that he/she knows are not true.

Nonetheless, the employee is entitled - as long as acting in good faith - to report facts to the Court in order to assess the criminal relevance thereof.

Instead, when the complaint does not have as purpose facts, but opinions or judgments, there are no problems of truthfulness or untruthfulness whatsoever. The judgments (which are obviously relevant

herein if negative) may always be expressed, even if they inevitably turn out to damage the public image of the person to whom the complaint relates.

In so far as the formal or modal limits are concerned (principle of formal restraint), case law requests that all expressions and tones be proportionate and instrumental to the aims of the communication, and such as not to gratuitously damage the employer's image. Therefore, in no way will the communication go too far as to become an insult or indulge in rude or obnoxious approaches, or in expressions which are gratuitously aimed at causing contempt and disrepute (thus Court of Rome, 26 October 2009 but see, more recently, Cass. 14 May 2012, No. 7471). Quite the opposite, it shall be marked by fairness, civility and moderation of the expressions and by the balance of tones (See Cass. 6 May 1998, No. 4952).

The line of reasoning followed by case law does not change in its baseline, regardless of the communication means chosen and the context in which it takes place. This does not mean that the

Judges do not take into consideration the peculiarity of the communication instrument (newspaper article, television interview, leaflet, satirical cartoon) and, therefore, the expressive codes featuring same and the context in which the communication takes place (for instance, the complaint brought by a trade union representative in the context of a harsh collective confrontation).

With special respect to satire, the use of symbolic and paradoxical language, the recourse to strong and exaggerated images, aimed at making fun of facts and situations, are permitted (see Magistrates' Court of Bergamo, ruling of 29 September 1997).

Lastly, in so far as the finalistic limits are concerned (principle of the pursued interest), case law deems that, through the complaint, the whistleblower may lawfully pursue both an own individual interest (such as, for instance, the exercise of the right to defence pursuant to the Constitution, or the right to protect his/her own job), as well as a collective and trade union interest (for instance, the protection of employment levels within the company, or safety in the workplace), or a public and general interest (for instance, salubrity of the environment, transport safety, the repression of criminal phenomena such as mafia infiltration).

Nonetheless, it needs be stressed that, pursuant to the leading stance, the significance given under the legal system to the final interest pursued - be it a collective or general interest - leads to mitigate the strictness of the substantive and formal limits just discussed, thus reverberating on the balancing judgment between the employee's right to information and right of criticism, and the employer's personality rights.

In short, the assessment of the final interest at which the complaint is aimed leads to read the employee's right to information and right of criticism in a broader way.

Case law gives special significance to this aspect with respect to the complaints brought by a trade union representative, by stressing that, in this case, the latter acts on equal terms and not on subordinate terms with respect to the employer, since his/her complaint is at the same time the free expression of ideas and the expression of trade union freedom.

Similar remarks may be raised for the workers' representative for safety, who is in charge of protecting the right to the health of workers in the workplace.

Instead, the event in which the whistleblower's complaint is merely aimed at damaging the employer goes beyond the scope of the right to information and of the right of criticism. In any such event, there would be abuse: the right is no longer exercised for spreading information and for forming a critical awareness by the public as to the company's operations, but solely in order to damage the personality and cause financial damage thereto.

7.6 Protections for the whistleblower in case of dismissal or mobbing

The whistleblower is protected both against dismissal and discriminatory acts, and against mobbing. But once again, upon failure of an *ad hoc* law, it is necessary to have recourse to the general rules set

forth for employees.

The dismissal of the whistleblower who has lawfully exercised the right to information and the right of criticism – also after the so-called "Monti's reform" (Act No. 92/2012) and the Renzi's "*Jobs Act*" (in particular Legislative Decree No. 23/2015), which have mitigated in general the protection against dismissal in the Italian legal system – is subject to the most incisive protection, namely, the so-called "real strong protection": the dismissal is null and void, and the employee is entitled to be reinstated in his/her former position and to receive an indemnity proportionate to the last actual global retribution from the date of dismissal until that of the effective reinstatement.

The current legislation provides that the so-called "real strong protection" shall apply, regardless of the number of employees of the employer, in the most serious cases of pathology of the dismissal and, in particular, to discriminatory dismissals, to dismissals for unlawful reasons, and to null and void dismissals in the other cases provided for by law.

Well then, the dismissal of the whistleblower who has lawfully exercised his/her own right of criticism and who is thus dismissed for said reason amounts without doubt to a case of retaliatory dismissal, a case in point which Italian case law (and now also the law: cfr. art. 28, par. 6, and 55-*ter*, par. 6, of Legislative Decree No. 150/2011, which expressly trace the retaliatory acts to cases of discrimination) constantly traces back to discriminatory dismissals or to dismissals for unlawful reasons (see Cass. 11 October 2012, No. 17329; Court of Milan, 27 December 2012).

Therefore, the so-called "real strong protection" needs be applied herein.

The same result may be reached even if we follow the most restrictive theories of interpretation, which try to limit the scope of application of the so-called "real strong protection" to the greatest possible extent. Indeed, pursuant to these different readings, the so called "real strong protection" would solely be positively foreseen for the events in which a "loathsome" dismissal is taken into consideration, namely, a dismissal in breach of a fundamental right of the employee. It is clear that any such event would arise in the case under analysis, since the dismissal opposes the whistleblower's lawful exercise of the right to information and of the right of criticism, an expression of the employee's fundamental right under the Constitution to the free expression of ideas.

The dismissal of the whistleblower who lawfully exercises any such right is thus protected in the Italian legal system to the greatest extent.

Some problems arise, instead, in connection with the allocation of the burden of proof.

Pursuant to firm case law, the burden of proof of the discrimination or of the illegal grounds (including the retaliatory grounds), as well as the existence of a cause of nullity in the dismissal shall rest on the employee (amongst the most recent decisions, see Cass. 26 March 2012, No. 4797).

Truly, said assumption should be discussed in light of the fact that, for discriminations in general, the legal system now foresees a partial reversal of the burden of proof (see hereunder).

In any event, it needs be stressed that the employee's burden of proof is actually partially mitigated by the incisive preliminary investigation powers granted to the Judges within employment proceedings, by the power vested thereto to have recourse to simple assumptions for the purposes of the relevant judgment (which need be serious, precise and concordant105) and by the fact that, pursuant to law, the employer has the burden of proof of the just cause or of the justified subjective or objective grounds, which are in any event necessary for the lawfulness of the dismissal. The consequence is that, should the employer not be able to prove the existence of the reason grounding the termination and should there be circumstantial evidence in favour of a retaliation event (for instance, the time proximity of the dismissal with respect to the employer's declarations), the Judge may rule declaring the nullity of the dismissal, thus applying the so-called "real strong protection".

A similar line of reasoning needs be followed in connection with any discriminatory acts put in place by the employer during performance of the employment (disciplinary measures, acts exercising the so-called *ius variandi*, *etc.*), namely, acts which are not based on organisational needs, but amount to retaliation with respect to the lawful exercise of the right of criticism. The general rules in the matter of discriminations apply herein, pursuant to which the discriminatory acts are null and void (Art. 15 of the Workers' Statute) and, therefore, having no effects whatsoever and the employee shall be entitled to property and non-property damages.

The burden of proof of discriminations – in compliance with Directive 2006/54/CE – is partially reversed herein by the law (see art. 28, par. 5, of Legislative Decree No. 150/2011 for discriminations in general; see arts. 37, paragraphs 3, 4, and 38, of Legislative Decree No. 198/2006, for sexual discrimination). It is sufficient that the employee provides "*factual elements, also of statistical nature, from which the existence of discriminatory acts, understandings or behaviours may be assumed*", since "*the defendant has the burden of proving the non-existence of the discrimination*" (Art. 28, paragraph 4, of Legislative Decree No. 150/2011. Instead, as regards sexual discrimination, art. 40 of Legislative Decree No. 198/2006 requests that the employee provides "*precise and concordant*" factual elements). Therefore, if the employee

provides circumstantial evidence which is even less consistent than that requested in the matter of simple assumptions, the burden of proving the lack of discrimination is transferred to the employer.

Finally, the whistleblower may appeal to the protection against mobbing.

Mobbing is not governed under the Italian legal system, however, pursuant to case law, it is in any event repressed pursuant to the rule laying the security obligation upon the employer and, namely, the obligation to protect the health and dignity of the respective employees (art. 2087 of the Civil Code). The security obligation provision therefore implies, first, that it is forbidden for the employer to directly hold mobbing behaviours and, second, that the employer is under the obligation to prevent those behaviours from being put in place by the employee's colleagues.

Pursuant to case law, mobbing is a complex case in point, which takes shape when the employer or a colleague of the victim puts in place a series of legal acts (de-skilling, for instance) and/or material behaviours (insults and physical aggressions, for instance), extended in time or repeated, the purpose of which is that of striking the employee in his/her dignity, often in order to induce him/her to resign.

Therefore, should the whistleblower undergo mobbing, the latter may seize the Judge by complaining about the breach of the security obligation and request the employer be ordered to perform, namely, to end the mobbing, as well as to order the compensation for the relevant property and non-property damages.

In the event of mobbing, the employee shall have the burden of proving the existence of the employment relation, as well as of any and all incurred detrimental effects, whilst the employer shall have the burden of proving to have fulfilled the security obligation.

The only relevant case for the purposes herein which may be worth taking into consideration, in which the Italian legal system acknowledges that collective parties have the capacity to sue, is composed of the procedure for repressing the anti-trade union behaviour It is foreseen that the local bodies of the national trade union associations be entitled to bring an action should the employer hold behaviours aimed at limiting trade union activities (art. 28 of the Wokers' Statute). The case in point may arise with respect to whistleblowing in the event in which the employee is a trade unionist exercising the respective right to information and right of criticism for the protection, for instance, of the employees' health or job.

8. Social media in the working relation

The consequences of posting over social media about the employer, superiors, colleagues and workplace conditions is a quite recurrent issue in Italy.

In the absence of a specific regulation, however, the Courts make reference to the general provisions regarding the loyalty obligation contained in art. 2105 of the Civil Code, so we can here recall all the comments made in the paragraph concerning the whistleblowing.

Anyway, we have to stress that recently case law has been quite prolific on this subject matter.

The Court of Appeal of Turin (ruling No. 164 of 17.7.2014), for example, has declared as lawful the dismissal of an employee that had repeatedly posted on Facebook sexist comments of absolute gravity, using a particularly defamatory language, regarding some of his colleagues.

With respect to the principle of proportionality between the violation and the disciplinary sanction (Art. 2106 of the Civil Code), the Court of Appeal has taken in great account the circumstance for which the post had not been published in the so-called “closed groups” or with a visibility limited to the “friends”. On the contrary, the post had been published on the public profile of the worker, thus visible to all the users of the social network.

Also Parma Labour Court, with ruling of 16.05.2016, has declared as lawful the dismissal of the vice-head unit of a great fruit and vegetables company, which had, through a public post, defamed his own employer, accusing him to have manifested the will of sending to work the employees even on Sundays. The Court has, in this case, placed emphasis, as an aggravating circumstance, on the position of responsibility covered by the employee.

The use of the social networks lies outside from the regulation contained in article 4 of the Worker's Statute that limits the installation of audio-visual devices and other instruments that can control at a distance the employees’ activity.

The employer is allowed, therefore, to sign up on the socials network used by his own employees and to access to the contents published by them accepting the “friendship” or entering a closed group. Nevertheless, the employer must observe the duty of good faith towards his employees. Such duty is violated, for example, when the employer uses the so-called “fake profiles”, hiding his own identity in order to access anonymously to the contents published by his workers or to contact them in order to know their opinions. Furthermore, this behavior is held a criminal offence under article 494 of the Penal Code that punishes the crime of “impersonation”. Moreover, if the employer monitors the employees in violation of Legislative Decree No. 169/2003 or of the Garante’s Guidelines, he commits illegal data processing and he is punishable by administrative and penal sanctions.