FROM "*CORPORATE DISLOYALTY*" TO "*UNFAIR COMPETITION*"

Manlio d'Agostino Panebianco[1]

Abstract
The loss of control and "*abuse*" of know-how, knowledge, corporate and business secrets, information and data acquired by an employee, collaborator and/or partner (in particular, in cases of outsourcing) during the relationship, expose the each entity/organization - domestic and international - to "*Corporate Disloyalty*" and "*Unfair Competition*", generating different dangerous financial, economical, patrimonial and reputational effects, both in short and long term. The article aims to highlight the main features, focusing on different legal frameworks and circumstances, in order to create a synoptic framework, useful to face a complex organizational aspect, suggesting some possible mitigation measures, both from legal and organizational perspective.

Index: 1. Introduction **- 2.** Legal Framework **- 3.** Some Risk Indexes **- 4.** Accountability, *culpa in eligendo* and *in vigilando* **- 5.** An integrated mitigation strategy - References

[1] Lecturer of "Criminal Economy and Cybercrime" at SSML CIELS; Lecturer of "Economical Intelligence" at Master of Rome Tor Vergata University; Lecturer of "Data Processing" at the Business School of "Il Sole 24 Ore"; member of "B-ASC Bicocca Applied Statistics Center" Research Center of University of Milan Bicocca. With a special thank for the help in sources-research to Filippo Schesari and Andrea Brisotto.

1. Introduction.

Any kind of entity (organization, association or community) is constituted by employees, partners, collaborators, etc., who deliver a professional service against of a remuneration, "Human Capital" is the most important corporate asset (Dimartino A., Fischetti G., 2018)[2]: on the other hand, places the utmost trust in its employees, establishing relationships based on mutual loyalty. This relationship takes on both a relational and a legal aspect, which is expressed and declined in different phases (*ex ante*, *in itinere* and *ex post*), with different risk exposures.

In our modern society and the economy, there is a close and direct relationship between the "natural person" (in the role of employee, collaborator, partner, etc.) and corporate information/data, especially when the latter assumes the quality of "strategical" and "relevance".

The article aims to highlight the main features, focusing on different legal frameworks and circumstances, in order to create a synoptic framework, useful to face a complex organizational aspect, that generates different dangerous effects in relation to the different phase of the relationship. This can be possible, thanks to the raising awareness on this topic, also identifying some indicators that can help in identifying the main risk circumstances.

The starting and focal point is the evolution of the risk to which an entity is exposed, in terms of loss of control and "*abuse*" of know-how, knowledge, corporate and business secrets, information and data acquired by an employee, collaborator and/or partner (in particular, in cases of outsourcing), during the relationship.

So, in all organizations – domestic and international – non-quantifiable factors come into play: these includes all organizational risks (including *corporate disloyalty*), and so formal procedures and controls nearly always carry a risk a subversion by the "human factor" (O'Regan, 2014)[3].

As a matter of facts, the during the "job-relationship", whenever an

[2] Dimartino A., Fischetti G., *Il Dirompente valore del capitale Umano,* Secop Edizioni, 2018

[3] O'Regan, *International Auditing: Practical Resource Guide*, John Wiley & Sons, 2004

employee, collaborator and/or partner has access to “confidential” data, an entity has to deal with “*corporate disloyalty*” (in itinere), while this legal risk would change (*ex post*) into “*unfair competition*” just in the time the relationship (between the entity and former's employee, collaborator and/or partner) ends, since all information and knowledge acquired by the these and due to the loss of the Entity's control become a weak point, exposing to significant and relevant loss, both financial, economical and reputational.

As a matter of facts - present and former - employees, collaborators and partners could use some practices, processes and confidential information, to benefit a competitor: the only difference lays on the possibility and capability of the entity to mitigate and manage these kind of risk exposures.

As a result, the Human Capital (and the loyal relationship) is both the most important strength for an Entity, and eventually the most important threat: harmful behaviours had been always a risk for every kind of organization. Over the last years, due to technological innovations, this kind this risk exposure is increased (Hodge N., 2016)[4]: one of the main reason is that “Knowledge” and “Datas and Information” not only are the main drivers, but even since they are intangible assets with one of the higher added value.

This risky circumstance concerns particularly “knowledge workers”, i.e. those tasks and jobs characterized by temporary and precariousness, for which cases have been detected of people who deliberately accumulate information and knowledge (even of a confidential nature) with the desire to use them later, in the subsequent use: it is a sort of strategy that tends to transform the “trap of temporariness” into a “competitive advantage” (Armano E., 2012)[5].

In order to prevent and avoid these situations, the entity is called to take preventive measures, already before and since the establishment of job-relationship.

[4] Hodge N., “*The dangers within: employee disloyalty*”, IBA, 2016
[5] Armano E., “*Narrativity as a power of self-representation of invisible conditions: knowledge workers*”, in *M@gm@*, 2012

2. Legal Framework.

In order to frame the legal context, the analysis start from the European and Italian situation, although it can be generally considered as a reference point to be extended for other Countries (*infra* quoted).
Firstly, quoting the article 2104 of Italian Civil Code (concerning "Diligence of the employee"), the employee shall work with diligence required by the nature of his or her service, by the interest of the company and by the overriding personal interest; also he must also observe the provisions for the execution and for the discipline of work given by the entrepreneur and by the collaborators of this which depend hierarchically.

Then, for the following article 2105 (concerning "*Loyalty obligation*") «*the employee must not handle business, on his own behalf and/or on behalf of third parties, in competition with the entrepreneur, nor disclose information pertaining to the organization and production methods of the company, or make use of it in order to be able to bring to it injury*».

This last provision brings to three different aspects: the first one is the prohibition of competition, extended even out of the working hour; the duty of secrecy which covers all the information the employee becomes acknowledged because of the execution of his/her job, allowing him/her to use only in the workplace; finally, the prohibition of bringing out of the company the know-how.

Obviously since knowledge is intangible, and it derives from a process of stratification deriving from a previous[6] educational process, study, but which it is also fed by the development of expertise about the accomplishment of some tasks associated with a specific production process (Albino V. et al., 2001)[7], it is very important to correctly define the perimeter between the abuse of corporate information and individual knowledge. Therefore, the breach of law may take place with reference to specific production methods, for instance "*innovative process*": besides the definitions, doctrine and jurisprudence

[6] prior to the job-relationship

[7] Albino V., Garavelli A.C., Schiuma G., *A metric for measuring knowledge codification in organisation learning*, in *Technovation*, 2001

clarified and somehow expanded the obligations the employee shall observe.

Corporate Loyalty is a fundamental prerequisite, such that when it lacks, it is permitted to interrupt the working relationship[8].

In addition, it is appropriate to report that Article 622 of the Italian Criminal Code punishes the disclosure of a "*professional secret*" by a person that comes across it, especially if committed by a general manager, an administrator or an auditor (increasing the punishment).

In order to complete the previous analysis, it is appropriate to add that – in the Italian context - in the public fields, a worker must act even according to the principles of *integrity*, *correctness*, *good faith*, *proportionality*, *objectivity*, *transparency*[9], and a *disloyal behaviour* (regarding and concerning the disclosure of information and/or the use of *office secrets*) could - also and even - configure the conduct listed in article 326 of the Italian Criminal Code.

More over, since a "*personal data*" is comparable to a "*strategical asset*" that has its own intrinsic value and, it is undeniable as in the new digital dimension, how data has become one of the main source of value creation (d'Agostino Panebianco M., 2019)[10]: the correct data processing becomes essential to avoid those "data breaches", which can be declined not only in an accident, but in real disloyal behaviour.

As a matter of facts, a Data Breach can defined as «*the intentional or inadvertent exposure of confidential information to unauthorized parties*» (Cheng L. et al., 2017)[11], and it can be due by endogenous or exogenous causes, as well as intentional (in bad faith) or unintended (in good faith, mistake or negligence).

In addition to ICT technical aspects, it is important to highlight that "*personal data breach*" events concern directly legal aspects related to an

[8] Italian Supreme Court, Civ., Labour Section, April 11th 2019, judgment n. 10239
[9] See articles 6 to 12 of the Code of Conduct for Public Employees, pursuant to Presidential Decree 62/2013
[10] d'Agostino Panebianco M., "*Vivere nella Dimensione Digitale*", Themis Ed., 2019
[11] Cheng L., Liu F., Yao D., *Enterprise data breach: causes, challenges, prevention, and future directions*, in *Wire Data Mining and Knowledge Discovery*, 2017

high risk exposure to the rights and freedoms of the natural persons. As a matter of facts, the General Data Protection Regulation[12] (even so called GDPR) gives a specific definition (at article 4, point 12) of this event, focusing the perimeter to any «*breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed*», which compromise the 3 main principles of personal data treatment (confidentiality, integrity and availability), and as a result of which, the "Data Controller" is not able to guarantee compliance with the present legal framework, and according to Article 32 (Security of processing), Article 33 (Notification of a personal data breach to the supervisory authority) and Article 34 (Communication of a personal data breach to the data subject) a "Data Controller" must promptly take action to manage the emergency situation, declining the principle of accountability (article 24), in favor of the weaker party (data subject).

These violations, in fact, can expose the interested parties to various risks – from identity theft to material damage, with consequent financial losses, of confidentiality of personal data protected by professional secrecy - and with serious prejudice on the reputation and on the private sphere.

As a matter of facts, these can cause a there is a "*cause and effect connection*", which leads to direct responsibility, assumed firstly by whoever carries out a treatment: the Data Controller, and therefore in a pyramid scheme, the Manager, sub-manager and authorized parties (d'Agostino Panebianco M., 2019)[13]; moreover, these responsibilities do not begin exclusively when the violation is committed and verified[14], but arise already when data processing is planned (Cippitani R., 2019)[15] (recalling the *culpa in eligendo principle*, i.e. related to the choices made) and continuing during the

[12] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC

[13] d'Agostino Panebianco M., "*Vivere nella Dimensione Digitale*", Themis Ed., 2019

[14] European Union - Agency for Fundamental Rights, Council of Europe, Publications Office of the European Union, Manual on European Data Protection Law, Luxembourg, 2018

[15] Cippitani R., *Purposes of scientific research and exceptions to the discipline of personal data protection*, in *Cyberspace and Law*, vol. 20, n. 62, 2019

entire data-treatment (due to *culpa in vigilando principle*, i.e. of monitoring that all risk management and mitigation measures are put in place).

The European Legislator emphasized the need for a broader coordination in the "Data-Breach emergency management" amongst interested parties (National Data Protection Authority, Data Controller, Data-Subject, etc.), introducing - *in primis* - a "*notification obligation*"[16] and - in the most serious and dangerous cases - the one of direct "*communication to the interested parties*"[17].

The reasons of the quoted obligations can be explained by linking it to:

- both to the promotion and the increase of the culture of *personal data protection* and *Digital Awareness*, and the implementation of a better security data risks assessment, in order to adopt adequate measures to mitigate and manage harmful events;

- the sharing of risk management methods which allows - each for one own skills and scope - the adoption of those strategies and additional security measures, aimed to limit the effects and negative consequences[18];

- the disclosure on accidents (mainly to data-subjects) is not only a an essential element of crisis management obligation but, primarily, it can reduce and contain damages, since providing specific and accurate information to data-subjects (as highlighted by the Italian Data Protection Authority[19]), allow them to adopt on their own individual and additional security measures (Karyda M., Mitrou L., 2016)[20].

A last consideration regarding the regulatory framework of reference concerns Intellectual Property Law (IP), since the implementation of an

[16] Regulation (EU) 2016/679, art.33 "Notification of a violation of personal data to the supervisory authority"
[17] Regulation (EU) 2016/679, art.34 "Communication of a violation of personal data to the interested party"
[18] See also Council of Europe Convention on the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention No. 108), modernized as amended by CETS Protocol No. 223, adopted by the Committee of Ministers of the Council of Europe on 18 April 2018
[19] See Italian Data Protection Authority Newsletter of May 30th, 2019
[20] Karyda M., Mitrou L., *Data Breach Notification: Issues and Challenges for Security Management*, in *MCIS Proceedings*, 2016

"innovation" (both related to a product, a service and/or a process) that leads to the registration of a trademark and/or a patent is characterized by the "transformation" of an idea and/or a discovery, into a strategic corporate high added value asset, mainly based on reserved information.

«*The term "intellectual property" refers to a loose cluster of legal doctrines that regulate the uses of different sorts of ideas and insignia. The law of copyright protects various "original forms of expression," including novels, movies, musical compositions, and computer software programs. Patent law protects inventions and some kinds of discoveries. Trademark law protects words and symbols that identify for consumers the goods and services manufactured or supplied by particular persons or firms. Trade-secret law protects commercially valuable information (soft-drink formulas, confidential marketing strategies, etc.) that companies attempt to conceal from their competitors. The "right of publicity" protects celebrities' interests in their images and identities*» (Fisher W., 2001)[21].

The strategic importance of this argument is such that - for some years - the European Legislator has been regulating it through the adoption of some specific legislative measures: the most recent is the the Directive (EU) 2019/790[22] *on copyright and related rights in the Digital Single Market*, that follows the Regulation (EU) 2015/2424[23] *on the harmonization in the Internal Market of Trade Marks and Designs*, and the Directive (EU) 2015/2436[24] *to approximate the laws of the Member States relating to trade marks*[25].

[21] Fischer W., "*Theories of Intellectual Property*", Cambridge, 2001

[22] Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC

[23] Regulation (EU) 2015/2424 of the European Parliament and of the Council of 16 December 2015 amending Council Regulation (EC) No 207/2009 on the Community trade mark and Commission Regulation (EC) No 2868/95 implementing Council Regulation (EC) No 40/94 on the Community trade mark, and repealing Commission Regulation (EC) No 2869/95 on the fees payable to the Office for Harmonization in the Internal Market (Trade Marks and Designs)

[24] Directive (EU) 2015/2436 of the European Parliament and of the Council of 16 December 2015 to approximate the laws of the Member States relating to trade marks

[25] In Italy, both the Regulation (EU) 2015/2424 and the Directive (EU) 2015/2436 were implemented with Legislative Decree of 20 February 2019, n.15 (published in Italian Official Journal of March 8, 2019, No. 57), introducing - in particular - important changes to the art. 21 of the Italian Industrial Property Code (Legislative Decree f10 February 2005, n. 30).

For instance, in Italy, the reveal of the content about secret documents - that implies a damage to the "legitimate owner" - configures the behaviour described in the provision of article 621 (violation of industrial secret) of the Italian Criminal Code, considering as guilty as the quoted, all those third party who buys or has a financial advantage from that documents.
Moreover, article 623 of the Italian Criminal Code punishes whoever reveals any information about a discover, an industrial application or an invention that is meant to be secret with the scope of gaining a profit for himself/herself or for others.

«*The law of unfair competition is primarily comprised of torts that cause economic injury to a business through a deceptive or wrongful business practice. Unfair competition can be broken down into two broad categories: unfair competition (sometimes used to refer only to those torts that are meant to confuse consumers as to the source of the product, also known as deceptive trade practices) and unfair trade practices (comprises all other forms of unfair competition)*»[26].

So *Unfair Competition* can be put in place in different ways: firstly, having the specific knowledge and access to sensitive data (included the clients of the former entity/employer or those related to trade secrets), the former employee/partner can bring with him or her them to his/her own-run new business or to a competitor's company.

The Italian Civil Code states that the judge has the power to set any measure to inhibit the behaviour or the continuation of it and to erase the negative effects produced in the meanwhile. From a practical point of view, those measures are: the order of stopping the activity and the prohibition to start again a certain profession.

On the other hand, in Common Law, a fundamental rule is the duty not to engage in any *disloyal act* against the employer: this duty does not necessarily rely on a written contract. The employee shall act honestly, in a

[26] Unfair Competition, Legal Information Institute, www.law.cornell.edu

loyal manner and must comply to all his or her duties to the sole benefits of the employer. There are several elements to be taken into consideration when evaluating the breach of the duty of loyalty (Cavico F.J., et al., 2018)[27]. For sure, directly competing against the employer while working for him or her clearly violate the duty of loyalty. For example, in case of law Pure Power Boot Camp. inc., et al. vs. Warrior Fitness Boot Camp, llc, et al., the Court stated:

> *«Although an employee may, of course, make preparations to compete with his employer while still working for the employer, he or she may not do so at the employer's expense, and may not use the employer's resources, time, facilities, or confidential information; specifically, whether or not the employee has signed an agreement not-to-compete, the employee, while still employed by the employer, may not solicit clients of his employer, may not copy his employer's business records for his own use, may not charge expenses to his employer, which were incurred while acting on behalf of his own interest, and may not actively divert the employer's business for his own personal benefit or the benefit of others»*[28].

In addition to what already quoted, in Common Law, has been elaborated as component of the duty of loyalty "*the Corporate Opportunity Doctrine*" that affects the ability of starting a new autonomous business by a "*corporate fiduciary*": the most relevant feature of this regards "conflict of interests", since the interests of the two (or more) parties are not simply misaligned, but in deep contradiction (Talley E., Hashmall M.)[29]. Whenever a new business opportunity may appear, the employee/partner shall offer it firstly to the corporation he/she is addressing his/her professional service/competences, and only in case the Entity is not interested in it, the employee/partner can run that business on his/her own, and/or propose that

---

[27] Cavico F.J., Mujtaba B. G., Muffler S., *The duty of loyalty in the employment relationship: legal analysis and recommendations for employers and workers*, in *Journal of Legal, Ethical and Regulatory Issues*, 2018

[28] United States District Court, S.D. New York, Pure Power Boot Camp, Inc., et al. v. Warrior Fitness Boot Camp, LLC, et al., 813 F. Supp. 2d at 521, 2011

[29] Talley E., Hashmall M., *The Corporate Opportunity Doctrine*, in *U.S.C. Institute for Corporate Counsel*, 2001

opportunity to a different subject, even a competitor.

In United States legal system, the Courts elaborated a so called "*Doctrine of Inevitable Disclosure*" pointing out certain business information which the former employee can not disclose or use in his/her new job because they fall into the category of "*trade secret*". Those information must meet some specific requirements, like: the claimant must have legitimate access to such information; the former employee will unavoidably use those information during the performance of his o her new employment; the disclose of the information will cause an irreversible damage to the company.

It is therefore possible to summarize that the "*Doctrine of Inevitable Disclosure*" acts as a *non-disclosure agreement*, apart from the circumstance that is draft and performed by a judge. The court is not absolutely free of determine the content of such clause, but it must take into consideration certain elements such as: the degree of similarity between the new and previous employee's employment, the degree of trade secret's exposure toward the examined employee, the level of competition between the two arguing companies, the possible advantage the company gained from the knowledge of such a secret, the measures the former employer took in order to protect the secret (Harris J.O., 2000)[30].

3. Some Risk Indexes.

The lack of "security awareness" in various industries, according to a survey conducted by Ponemon Institute and Symantec (2013)[31], concerns the 41% of employees admit to send sensitive data from their professional email to their personal one. Moreover, the 37% declared they use file-sharing apps (such as Dropbox or Google Docs) without permission from the employer. In

[30] Harris J. O., *The Doctrine of Inevitable Disclosure: A Proposal to Balance Employer and Employee Interests*, in *Washington University Law Review*, 2000

[31] *What's Yours is Mine: How Employees are Putting Your Intellectual Property at Risk*, Ponemon Institute, Symantec, 2013

addiction, those data are hardly-ever cleaned up after the use, exposing in such fashion the data to a further risk. When employees change job, datas follow them. To be honest, most of the times, employees are not in bad-faith, but simply negligent: however, the 40% of them admits to use those information in their new job; and most of them do not know that this attitude expose the company and themselves to an additional risk.

Another kind of "*leak of knowledge and data*" is due to business organization models, choices and strategies, especially focusing on the relevant percentage of partnerships (and/or self-employed collaborators), outsourcing and employee turnover (i.e. separations and new hirings).
As a matter of facts, external collaborators are needed since their experience is wider (since it comes from different realities and situations) and – normally - the cost is proportional to the aims; but, on the other hand, since it is time limited and they access to some relevant and confidential information and data about their clients, they can expose to an higher risk of "corporate disloyalty" and "unfair competition".

A sensitive field regards Research and Development (R&D) investments, which have as goal and result (according to European Commission's survey[32]) the discover of new applications (compared to the present knowledge), an increase of expertise and of efficiency and effectiveness, in particular in referring to production process and new products. At the meantime, R&D investments expose to greater risks in terms of disloyalty because their output could be brought out of the business. So, the R&D growth rate can help to identify the most exposed sectors, such as: Aerospace & Defence; Automobiles & other transport; Chemicals; HealthCare industries; ICT producers and services. In addiction to the quoted, there is another sector seriously exposed to these risks: Banking financial services, insurances and pension funds. As a matter of facts, since the 2008 financial crisis, the financial system - all over the world – began a process of transformation mainly due to two main reasons: the need of costs-cut and the IT revolution. These changes led to a

[32] "*The EU Industrial R&D Investment Scoreboard*", European Commission, 2018

significant decrease and reorganization in the workforce (with a logical consequence of a reduction of the number of workers and branches) in order to maintain the level of profits.

4. Accountability, *culpa in eligendo* and *in vigilando*.

Any kind of violations (such as Data-Breach) or disloyal behaviour (even concerning unfair competition, in case of former employees or partners) is one of the most important risk exposure that each entity daily has to face and deal with, in particular those who work in an highly competitive sector such as "innovation", "high-tech" field and "high knowledge" companies (such as digital, pharmaceutical, healthcare, aerospace, etc.).

While the responsibilities recalled by the GDPR concerns "personal data" in favour to guarantees and rights of data-subjects, generally confidential data-management refers to a wider responsibility of all the stakeholders of the entity, since deriving loss may be huge. So there is a direct relationship between the organization responsibilities (and its effects) and the risks to which each one is exposed, in managing and processing information and data (not only personal ones).

Once again, it is appropriate to make a parallelism between the approach indicated by the GDPR and the more traditional legal principles.

While the European Regulation impose to adopt a model based on the "*principle of accountability*"[33] that cannot be interpreted as an only *ex ante* and/or static "*responsibility*" but, on the contrary, it is a dynamic and ongoing "*responsibility*", which primarily invests the Data Controller with a "*ripple effect*" on all other persons – both natural and/or other entities - involved in the treatment process, by adopting[34] appropriate behaviours, measures and

[33] Regulation (EU) 2016/679, Article 5 "Principles relating to processing of personal data"

[34] a Data-Controller is responsible for, and be able to demonstrate compliance with the principles of lawfulness, fairness and transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and

methods to protect the rights of the individual concerned, reducing its risk exposure (d'Agostino Panebianco M., 2019).

«*It is fundamental therefore to evaluate the consequences of such an unsuitable behaviour, but apparently without risks, can entail for the authorized parties that operate on personal information (but this, in truth, also applies to confidential non-personal data) and follow the instructions given by the employer, not accessing or trying in any way to access information for which one is not authorized, otherwise one might find oneself involved in unfortunate situations*» (Spedicato A., 2019)[35].

As declining the principle of Accountability in *personal-data-treament*, generally referring to confidential and/or sensitive data/information management - in the perspective of reduce the exposure to the risks of *Corporate Disloyalty* and *Unfair Competition* - any entity - at any stage, and for any deriving and arising actions (Karyda M., Mitrou L., 2016)[36] - is called to consider both the responsibilities related to each choice (correlated to the legal principle of *culpa in eligendo*), and to the constant attention to the effectiveness and efficiency of the risk mitigation measures planned, implemented and applied (correlated to the principle of *culpa in vigilando*).

5. An integrated mitigation strategy.

As already highlighted, *Corporate-Disloyalty* and *Unfair-Competition* can be considered both individually, and/or the timely and logical evolution of the first one into the second one.
So the mitigation strategy should begin at the early stage of hiring or contracting and continuing during the job relationship, as one complex and

confidentiality
[35] Spedicato A., *Italian Supreme Court: Whoever instigates the colleague to send confidential information to himself illegally accesses the computer system*, in www.consulenza.it, 2019
[36] Karyda M., Mitrou L., *Data Breach Notification: Issues and Challenges for Security Management*, in *MCIS Proceedings*, 2016

integrated one.

An interesting well known methodology in Human Resources field of "*skills and competences assessment*", that in this context should be considered as a best practice, with a different aim.

As a matter of facts, a proper *risk strategy* (focused on these objects) should consider - *ex ante* - a qualitative and quantitative evaluation[37] of the skills and the knowledge of the candidate/new employee, gained by his/her previous experience and/or education.

During the job-relationship (*in itinere*), both to monitor the risk exposure (quantitative) but also to get to know the value of "*company intangible heritage*", the entity should assess the "increase" of knowledge of individual employee or partner.

These first two activities allow, both to monitor the coherence of knowledge to the role; and, in case of perception and/or certainty of disloyal behaviours (*corporate disloyalty*), to promptly adopt correctional actions. Moreover, in all the cases of ending a job-relationship (planned or sudden), the entity is able to know what kind and quantity of information, data and knowledge a former employee/partner could bring outside and eventually (ab)use (*unfair competition*).

Considering that a *legal contract* should be considered as one of the measures to manage or mitigate risk, it is important to highlight that each article/point/clause of it, should derive directly by the results of previous risk assessment, both forecasting - priorly - the possible negative scenario and the "agreed" methodology to face it.

So, in addition, it is appropriate to include in the job contract (so, from the very early stage of the relationship) a "*non-disclosure clause*"[38], which restricts (during and after the job relationship) the use of data and information, by prohibiting a contracting party from divulging them (Beyer

[37] For instance, through structured materials such as tests or self-analysis sheets

[38] This solution can be adopted even by implementing a stand-alone Non-Disclosure Agreement

G.W., 2001)[39]. The intent is to restrict the use and disclosure of confidential information and data by the other party, that requires definition of what information is confidential, and how the other party will (and will not) be allowed to use them. *Non-disclosure clauses* or *agreements* are an aspect of contract law, in which is important to be explicit and to use specific and proper language (Grossman M., 2004)[40].

A similar agreement can be implemented and signed by the interested parties, only concerning the *ex post phase*, (i.e. beginning by the end of the job-relationship) when a former employee/partner is free to work for anybody, even with competitors.

In order to avoid those circumstances of *interest conflicts* or *unfair-competition*, it is appropriate to regulate (into a contract or a "*non-competition agreement*") the immediate period after the ending of the previous job-relationship, which it should meet two fundamental requirements: firstly, the restriction on competition must be reasonable, this means that such measure must be necessary to protect a legitimate interest of the employer. On the other hand, this Agreement must be supported by adequate consideration.

The needed features of this contract to limit the activity of the former employee/partners are: set limit of time; indicate the specific object of the restriction; the geographical limit of the agreement; the remuneration. In terms of duration, the law set a limit that varies depending on the job position the former employee had in the company. Usually, in the international context, for managers the agreement can not exceed 5 years, for all the others the limit is 3 years, and the activities that can be listed in the agreement, normally concern all the tasks typical of the specific field or industry, even considering all other possible forms (consultancy, board member, etc.).

Amongst all the possible mitigation measures (implementation of

[39] Beyer G.W., "*Modern Dictionary for the Legal Profession"*, William S. Hein & Co., Buffalo, 2001
[40] Grossman M., "*Technology Law: What Every Business (and Business-Minded Person) Needs to Know*", The Scarecrow Press, Inc., 2004

Security Policy, workforce education, Internal Auditing controls, Digital and Security Awareness programmes, limitation of the use of personal device on company's net, and/or use of personal email on the company computer, and/or the use of company's device for personal use, combination of strong-authentication with log-monitoring, etc.) it is worth to quote those tools which allow the *traceability of access to the data.*

A latter patented solution (called BioDIS[41]) can mark with a "biometric stamp" any kind of digital information, ensuring the traceability of documents, with a double effect: discouraging unfair actions, and laying the foundations for the creation of a possible evidence to be brought to trial.

References.

Albino V., Garavelli A.C., Schiuma G., *A metric for measuring knowledge codification in organisation learning*, in *Technovation*, 2001

Armano E., "*Narrativity as a power of self-representation of invisible conditions: knowledge workers*", in *M@gm@*, 2012

Bada M., Sasse A.M., Nurse J.R.C., *Cyber Security Awareness Campaigns: Why do they fail to change behaviour?*, International Conference on Cyber Security for Sustainable Society, 2015

Beyer G.W., "*Modern Dictionary for the Legal Profession*", William S. Hein & Co., Buffalo, 2001

Cavico F.J., Mujtaba B. G., Muffler S., *The duty of loyalty in the employment relationship: legal analysis and recommendations for employers and workers*, in *Journal of Legal, Ethical and Regulatory Issues*, 2018

Cheng L., Liu F., Yao D., *Enterprise data breach: causes, challenges, prevention, and future directions*, in *Wire Data Mining and Knowledge Discovery*, 2017

Cippitani R., *Purposes of scientific research and exceptions to the discipline of personal data protection*, in *Cyberspace and Law*, vol. 20, n. 62, 2019

d'Agostino Panebianco M., "*Vivere nella Dimensione Digitale*", Themis Ed.,

[41] See www.biobitlab.com

2019

d'Agostino M., Mariani P., Tuvo M., "Business Intelligence Handbook", Editrice Le Fonti, 2007

Dimartino A., Fischetti G., *Il Dirompente valore del capitale Umano,* Secop Edizioni, 2018

European Commission, "*The EU Industrial R&D Investment Scoreboard*",2018 https://publications.jrc.ec.europa.eu/repository/bitstream/JRC113807/eu_rd_scoreboard_2018_online.pdf

European Union - Agency for Fundamental Rights, Council of Europe, Publications Office of the European Union, Manual on European Data Protection Law, Luxembourg, 2018

Fischer W., "*Theories of Intellectual Property*", Cambridge, 2001

Grossman M., "*Technology Law: What Every Business (and Business-Minded Person) Needs to Know*", The Scarecrow Press, Inc., 2004

Harris J. O., *The Doctrine of Inevitable Disclosure: A Proposal to Balance Employer and Employee Interests*, in *Washington University Law Review*, 2000

Hodge N., "*The dangers within: employee disloyalty*", IBA, 2016

Karyda M., Mitrou L., *Data Breach Notification: Issues and Challenges for Security Management*, in *MCIS Proceedings*, 2016

Karyda M., Mitrou L., *Data Breach Notification: Issues and Challenges for Security Management*, in *MCIS Proceedings*, 2016

O'Regan, *International Auditing: Practical Resource Guide*, John Wiley & Sons, 2004

Ponemon Institute, Symantec, What's Yours is Mine: How Employees are Putting Your Intellectual Property at Risk, 2013

Spedicato A., *Italian Supreme Court: Whoever instigates the colleague to send confidential information to himself illegally accesses the computer system*, in www.consulenza.it/Contenuti/News/News/2667/cassazione-accede-abusivamente-al-sistema-inf, 11/01/2019

Talley E., Hashmall M., *The Corporate Opportunity Doctrine*, in *U.S.C. Institute for Corporate Counsel*, 2001

Legal Sources.

Code of Conduct for Public Employees, pursuant to Italian Presidential Decree 62/2013

Council of Europe Convention on the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention No. 108), modernized as amended by CETS Protocol No. 223, adopted by the Committee of Ministers of the Council of Europe on 18 April 2018

Directive (EU) 2015/2436 of the European Parliament and of the Council of 16 December 2015 to approximate the laws of the Member States relating to trade marks

Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC

Regulation (EU) 2015/2424 of the European Parliament and of the Council of 16 December 2015 amending Council Regulation (EC) No 207/2009 on the Community trade mark and Commission Regulation (EC) No 2868/95 implementing Council Regulation (EC) No 40/94 on the Community trade mark, and repealing Commission Regulation (EC) No 2869/95 on the fees payable to the Office for Harmonization in the Internal Market (Trade Marks and Designs)

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC

Other sources.

European Court of Justice. 27-9-2017, n.73

Italian Data Protection Authority Newsletter of May 30th, 2019

Italian Supreme Court, Civ., Labour Section, April 11th 2019, judgment n. 10239

Unfair Competition, Legal Information Institute, www.law.cornell.edu

United States District Court, S.D. New York, Pure Power Boot Camp, Inc., et al. v. Warrior Fitness Boot Camp, LLC, et al., 813 F. Supp. 2d at 521, 2011

www.biobitlab.com