THEMIS 2018
Semi-Final C - *European Civil Procedure*

The New Deal of E.U. Privacy Law: Legal Remedies and Jurisdiction

TEAM ITALY 1

Participants:
Giovanna Piazzalunga
Matthias Viggiano
Giulia Volpe

***Coach*:**
Angelo Gaglioti

Abstract

This paper deals with the issues of legal remedies and jurisdiction within the European Union (E.U.) in the matter of Privacy Law. To this end, an introductory section explains the notions of Privacy (§1) and specific features of Torts related to the breach of personal data (§§ 2-3). Through the analysis of the most pertinent doctrine and case-law, and taking into account the most recent ECJ decisions, the paper will depict three main legal remedies (rectification, removal, compensation for damages) and the issues of jurisdictions involved herein (§ 4). The writers propose to use the regime of legal costs for proceedings as an antidote to possible abuse of process as to the choice of the competent judge and assess the distribution of legal remedies between judicial and administrative Authorities, according to their truly nature – i.e. specific or compensatory remedies (§ 5). Furthermore, the subject of coordination between judicial and administrative enforcement of privacy law will be addressed (§6), even with reference to the recent E.U. Regulation on Data Protection (§ 7). Throughout the text some remarks on the extension of concepts and remedies from Consumer Law to Privacy Law, together with its consequences in point of jurisdiction will be drawn. The Authors intend to point out that a coherent pattern of rules on jurisdiction is vital to ensure that E.U. Privacy laws be in line with E.U. general principles and human rights, as enshrined in the ECHR, with specific reference to the right of defense.

Table of contents

1. What is *privacy*?

Central matter of our days are the worries about *privacy* and *personal data protection*: these are two crucial concepts of contemporary life with which every man, not only lawyers, has to face daily, even if sometimes many people do not realize the risks and damages related with them.

Starting with privacy, one idea has to be immediately fixed: there is much confusion about the word "*privacy*". A first definition[1] describes privacy as the right of people to conceal information about themselves that others might use to their disadvantage: but this description confuses privacy with secrecy, while the two concepts must be separated, as explained hereinafter.

Another famous explanation, even if ancient because it runs back to the end of the XIX century, portrays privacy as the "*right to be alone*"[2]: this phrase enlightens the heart of the concept, its core meaning; at the same time, it's important to notice that privacy is, nowadays, something more.

Indeed, as a prominent scholar[3] noted, **four different states of privacy can be constructed**: *solitude*, *intimacy*, *anonymity*, and *reserve*. The first one is the oldest idea of privacy, and it's related to a physically existing space separated from other persons: in other words, the domicile protection. The second is wider and includes all situations where two or more people create a secret in a group so to excludes the rest of the world from this knowledge: just think about the protection of the family, taken as a social group, where differences are settled in the house. The third is an individual desire to hide personal identity: for instance, the right to publish a book anonymously. Finally, the last one is the erection of walls (not only physically) against unwanted intrusion.

As this brief introduction points out there is no universally accepted definition of privacy: that is why, in this paper, **we will use the word *privacy* referring to the right not to be disturbed both in physically and in virtual spaces**. This means that privacy incorporates also rights already recognized under different names[4].

For instance, the right not to be disturbed in his own body is the well-known *habeas corpus*, whose spatial projection is domicile. In other words, privacy is a particular declination of freedom: in the same way, it has exact borders[5].

These circumstances can be proved, by observing the legal instruments designed to protect people's privacy. They are shaped similarly to other civil rights: indeed, ***privacy is a civil right*** (e.g., as set by art. 8 of the *European Convention on Human Rights and Fundamental Freedoms* (hereinafter *"ECHR"*), or art. 7 of the *Charter of fundamental rights of the European Union,* which ensure a

[1] See POSNER, *The economics of justice*, 1983.
[2] See WARREN and BRANDEIS, *The Right to Privacy*, 1890.
[3] See WESTIN, *Privacy and Freedom*, 1967.
[4] For instance, the *European Court of Human Rights* (hereinafter "ECtHR") protects privacy as to four different interests: private life; family life; home; correspondence. For more in details, see ECtHR, 27 October 1994, Application n. 18535/91, where the primary State's obligation is of the classic negative kind, like other freedoms.
[5] E.g. General Court, 3 December 2015, T-343/13, p. 47.

strong protection of all already mentioned privacy states).

However, what has really to be pointed out, is the way privacy protection spreads over the previous already known liberties. In fact, especially the fourth feature of privacy (i.e. the defense against unwanted – virtual – intrusions) has enormously grown through the latest years: the reason of this increase is related to the rise of more powerful tools facilitating virtual intrusions.

Until here, the existing freedoms, granted by the traditional civil rights, had not the power to avoid this so-called interests-harming behavior[6]: therefore, a brand-new instrument had to be shaped so as to defend this specific aspect of personal liberty. In fact, the object itself to protect wasn't correctly identified. Only in the last years, the legislative experience has managed to find which "*thing*" was to defend: *personal data*, as enshrined, for instance, in art. 8 of the *Charter of fundamental rights of the European Union*[7].

For the sake of a better understanding of this profile, it is necessary to explain what *personal data* really are, and why it has been necessary to create this legal category.

2. What is *data protection*?

According to art. 4 of E.U. Reg. 679/2016, personal data are "*any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*".

In other words, **every information** (represented as a word, a sign, or a picture, etc.) **that may lead to identify a man or a woman**.

Since the very beginning of this reasoning, it has immediately to be set out that, from the start of mankind's civilization, the identification of a person through name, day and place of birth, family memberships, etc., has been a very important concern for public powers: people must know, for example, with whom they make business, or who caused them losses. Nowadays, this identification need is addressed in nearly all countries in various ways: every person is inscribed in some public registers, owns an ID-card and a passport, etc. Alternately, people can individualize another person through his personal aspect or features. In both cases, as long as the process of identification occurs only between few persons, no great problem could rise[8]. Tricky issues, however, can spring out

[6] In the Civil law systems, the first attempts go back to the Seventies, when Germany, France and Italy introduced criminal laws to punish those who committed unwanted intrusions in other people's lives.

[7] Protection of personal data: "*1. Everyone has the right to the protection of personal data concerning him or her. 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. 3. Compliance with these rules shall be subject to control by an independent authority*".

[8] Even the usage of false name can be overcome quite easily.

when one subject starts collecting and filing huge amount of data and, even worse, when he uses such information. Therefore, the questions come really simply: how should privates acquire, manage, store and use personal data? And for which purposes?

The first problem seems to be possibly solved quite easily: no one can violate other people's personal data, unless the so-called "*data subject*" gives his or her consent(art. 6of E.U. Reg. 679/2016). This construction connects with the definition of *privacy* given by Posner[9], making personal data the object of a secret.

However, it appears to be not so: some personal data can be managed even without consent; just like for other civil rights, in specific conditions, public authorities can compress their protection while pursuing general superior interests, like criminal justice investigation[10]. At the same time the conduct of voluntarily publishing some personal data does not automatically imply that the subject refuses personal data protection[11].

Focusing on "*consent*", it is worth noting that "*consent*" is usually the most powerful instrument for a natural person to protect his or her privacy: data processing – and its limits – are fixed by the scope of consent, which makes aware (or, at least, should make aware) the data owner about data disclosure and the faculties afforded to the "*controller*" over personal data.

This is the real turning point of the questions about privacy protection: how can one be sure that the controller respects the extent and scope of the given consent? How can we prove that controller misused personal data? Consequently, which reaction can one undertake against a violation, especially to prevent any further violation? Finally, as to huge, corporate subjects processing billions of data units (e.g. telephonic, banking or insurance companies)[12], how should they store and use all such collected data, in particular in their relationships with national public authorities?

Such complications have become even more relevant today, because personal data are of information, which can easily be processed, stored and spread through computers and the Internet, making it nearly impossible to block and to confine them in a certain place ("*ubiquitas*").

3. How can *personal data* be violated and misused?

The ways privacy and personal data can be breached are different. One might summarize them using the concepts shown in some well-known legal researches, such as those led by Prossner and Solove.

---

[9] Look at previous § 1 of this paper, in particular at footnote nr. 1.

[10] See "*whereas"* nr. 4. of E.U. Reg. 679/2016. Also the ECtHR, 25 June 1997, Application n. 20605/92, explains that any interference by a public authority must be in accordance with the law (rule of law); ECJ, 27 September 2017, C-73/16.

[11] This statement represents a vital issue for privacy law and personal data protection; it will dealt with in the following §§ of this paper.

[12] Nowadays journalists publish news and inquiries about the improper use of personal data: just think about *Cambridge Analytica (for instance, see: https://www.thetimes.co.uk/article/cambridge-analytica-how-the-scandal-unfolded-3mspj5mkr)*, or the so called *Datagate (for instance, see: https://www.huffingtonpost.it/2013/06/19/datagate-wikileaks-pentagon-papers_n_3464126.html).*

As said before, personal data cannot in principle be processed without the consent of the person concerned by them: unauthorized usage of data is illegal and should be punished even by criminal legislation, or at least it must lead to pecuniary compensation for the damage incurred. This conduct constitutes the so-called ***personal data breach***[13].

Another matter is avoiding that personal data, once violated, could be partaken to third persons: this issue is even much more complex, because, using the Internet, information can be instantaneously diffused worldwide, while removing such information from the entire web is practically impossible. This is the so-called **information dissemination**, which is not necessarily linked with unconsented personal data processing: in fact, also the breach of confidentiality is an example of it[14].

However, these are not the only relevant violations of privacy: while invasions of privacy hinder the right of individuals to keep personal secrets (e.g. stealing the PIN-code of a debt-card), there are more insidious forms of intrusion, such as in the case of collecting data so as to influence individual choices. Such intrusions, also known as **decisional interference**, can described as "*an injection in someways into the personal decision-making process of another person, perhaps to influence that person's private decisions but, in any case, doing so in a way that disrupts the private personal thoughts that a person has*"[15].

Such reasoning shows why nowadays there is so great concern about privacy: providing that in previous times no tool could so widely and rapidly collect huge amounts of information, potentially influencing individual and social decision-making processes.

Indeed, the gathering of information is typical of non-democratic states, where the establishment takes control over all political opponents (this is what has been called **surveillance**)[16].

In contemporary liberal western societies, data collection, even if not related with some physically identified person, enables to create a sort of anonymous clone, whose decision-making process can be studied and directed in a way or in another: this is in practice what happens when we make a search on the internet[17]. However, even more dramatically, also the voting process can be influenced by such information collection, as in the disputed case of political elections for the Presidency of the United States of America in 2016[18]. What has to be pointed out in this paper, is the fact that this occurs not only when collection of private data is *per se* illegal, but also (and mostly) by rough collection of personal information that everybody daily shares via social medias.

In other words, *privacy* is not only just a legislative matter of concern, but also a cultural and

[13] See PROSSNER, *Privacy*, 1960. The way the violation is qualified by national authorities is basically the same: indeed, it is a non-contractual obligation, hence a *tort* (for further details, see § 4.1).

[14] See PROSSNER, *Privacy*, 1960, and SOLOVE, *Understanding Privacy*, 2008. Of course, the breach of confidentiality consisting in the revelation of a secret to a third friend has (nearly) always limited impact to in their lives. Not so in case of spreading the same secret in the internet: such behaviors can lead a fragile person directly to suicide.

[15] SOLOVE, *Understanding Privacy*, 2008.

[16] See the critical meditations of WESTIN, *Privacy and Freedom*, 1968.

[17] This is what happens with the so-called *cookies* on the internet, which track, record and store information given to a search engine, so as to "*personalize*" the instrument according to our preferences.

[18] Since a public investigation is still on going, we will not focus on this issue any longer.

democratic issue: if we refuse today to protect our freedom, our right to privacy, then we are heading for dictatorship. The only way to avoid this risk is to gather the care of our own privacy: everybody has to understand immediately the risks of managing with too much frivolousness his own personal identity and information. Only in a second time one might ask for protection of his own personal data by public authorities, which sometimes, are our first *headsman* (as some recent cases, such as NSA scandal, have apparently revealed)[19].

Anyway, European Union has adopted, as already mentioned above, a quite tough legislation to protect people's privacy and avoid events similar to those newly happened in the U.S.A. (and already cited in this paper).

4. Judicial data protection: general framework, distinctive features and new challenges.

The qualification of the rights connected to privacy violations, as deriving from a non-contractual obligation, and more precisely from a *tort*, by the ECtHR is the basis for the subsequent protection from the judicial point of view and, more specifically, for the procedural one. As a matter of fact, procedural law being essentially instrumental to the satisfaction of substantive rights, it has to be considered that European procedural law is no exception to that principle, so that it is highly recommended for the interpreter to read European rules from the perspective of enhancing the substantive legal positions of everyone, considering both groups and individuals and, in the latter case, referring to natural as well to the juridical persons.

Disputes related to infringements of privacy and rights related to personality share the common framework of E.U. procedural rules dedicated to non-contractual obligation (tort, delict or quasi-delict), which can be ideally divided into two areas of rules: rules of jurisdiction; rules on remedial techniques. Furthermore, these rules need to be interpreted taking into consideration the distinctive features of disputes involving privacy. We specifically refer to the *ubiquitas* of the network, which poses several questions about jurisdiction; the intimacy of right to the person, which implies a different aim of protection, compared to the one accorded to other non-material goods (such as in intellectual property) or to other weak parties (such as in consumer law).

Finally, the continuous technological improvement urges for some sorts of solutions in an increasing way. This is true in particular whereas the rights of personality are claimed for or offended by a juridical person, considered the increasing number of companies dealing with huge amounts of personal data for business reason (so-called *Big data protection*), or by an abusive use of new technology (i.e. mass-storage with clouds and profiling). This is a very crucial point, in order to avoid an abusive use of new technologies, hence preserving the advantages of the new technological conquests.

[19]See also the last case, which the ECJ will soon decide, filed at C-623/17, about the transmission of personal data to national agencies.

4.1. Special jurisdiction in matters relating to torts, delicts or quasi-delicts.

If your court case has **an international or cross-border dimension**, you have to find out the competent judge. The answer to this question might have some significant consequences. If you have to litigate abroad, you may have to face additional inconveniences and costs, for example because of the necessity to translate your statements, to instruct a lawyer in the Member State where proceedings take place or to travel so as to assist to court hearings. Applying to the wrong court, a dispute over the question of jurisdiction implies the risk of a considerable delay in the proceedings or even of a dismissal of your case because of lack of jurisdiction. This could also lead to the circumstance in which two or even more Member States Courts declare their jurisdiction, thus creating a high risk of multiple proceedings and conflicting decisions, which could hardly be enforced.

The main framework for E.U. judicial cooperation in jurisdictional civil matters is Regulation nr. 1215/2012. It aims at finding a practical solution to the issues here above, delineating a number of *criteria* helping civil parties, involved in a dispute characterized by cross-border elements within the E.U., to easily identify the member State and the subsequent Court having jurisdiction, in order to avoid multiple proceedings and to reach faster court settlements. **The main principle** of the Regulation system is the predictability of the competent court: in order to ensure a high protection of the right of defense, the (juridical or natural) person who is sued must know in advance the competent Court, through objective criteria. The Regulation establishes the general rule that the Member State having jurisdiction is the Member State where the defendant is domiciled. Nevertheless, the principle of the most predictable court must be mitigated with the principle of effective protection of the right concerned. That is why Recital 15 of the 1215/2012 Regulation states that, in addition to the defendant's domicile, there should be alternative grounds of jurisdiction based on a *close connection* between the court and the action or in order to facilitate the sound administration of justice, especially as to proximity of the judge to the evidence. The application of the connecting factor leads, as a practical result, to the shift of jurisdiction from the forum of defendant's domicile to the forum of the claimant (*forum actoris*).

The existence of a *close connection* should equally grants legal certainty and avoid the possibility of the defendant being sued in a court of a Member State, which he could not reasonably have foreseen. Hence Article 7 of this Regulation, which forms part of Section 2, headed '*Special jurisdiction'*, of Chapter II, provides in paragraph 2 that: '*A person domiciled in a Member State may be sued in another Member State: … (2) in matters relating to tort, delict or quasi-delict, in the courts for the place where the harmful event occurred or may occur*.' It should be noted that Article 7(2) sets out that, in matters relating to tort, delict or quasi-delict, a person domiciled in a Member State may be sued in another Member State in whose territory the harmful event occurred or may occur. It is established case-law that the rule of special jurisdiction in matters relating to tort,

delict or quasi-delict must be interpreted independently, by reference to the scheme and purpose of the regulation of which it forms part[20].This rule of special jurisdiction is based on the existence of a particularly close connecting factor between the dispute and the courts of the place where the harmful event occurred or may occur, which justifies the attribution of jurisdiction for reasons relating to the sound administration of justice and the efficacious conduct of proceedings. In matters relating to tort, delict or quasi-delict, the courts of the place where the harmful event occurred or may occur are usually the most appropriate to try the case, in particular on the grounds of proximity and ease of evidence. It is also appropriate, when interpreting Article 7(2) of Regulation Nr. 1215/2012, to bear in mind Recital 16 of this regulation, stating that the existence of a **close connection between the court and the action should ensure legal certainty and avoid the possibility of the defendant being sued in a court of a Member State which he could not reasonably have foreseen**, which is important, in particular, in disputes concerning non-contractual obligations arising out of violations of privacy and rights relating to personality, including defamation. According to settled case-law of the Court, the expression '*place where the harmful event occurred or may occur'* is intended to cover **both the place where the damage occurred and the place of the event giving rise to it**, since each of them could, depending on the circumstances, be particularly helpful in relation to the evidence and the conduct of the proceedings[21].

4.2. Judicial remedies in case of violations of privacy and other rights relating to human persona.

Applying the above depicted general rules to data protection field, the question of law to be solved by the Courts was, more precisely: on the basis of which connecting factors is it possible to allow the data protection authorities or the National Court of a Member State to apply their national law on data protection, being the law of the data subject's domicile (*forum actoris*) with regard to a data controller whose main establishment is located in another Member State or, even, in a Third country?

Actually, in three different cases, *Google Spain, Weltimmo and Amazon*[22], the data controller disputed that the processing of data was "*carried out in the context of an establishment of the controller on the territory of the Member State*" whose law was claimed (by the data subject being domiciled in that MS) to be applicable, arguing that the data processing was undertaken abroad, the tasks of the local establishment being of a different nature than data processing. According to the ECJ[23], the processing of personal data is carried out in the context of the activities of an

[20]See, to that effect, judgment of 25 October 2011, eDate Advertising and Others, C-509/09 and C-161/10, EU:C:2011:685, paragraph 38).
[21]Judgment of 25 October 2011, eDate Advertising and Others, C-509/09 and C-161/10, EU:C:2011:685, paragraph 41, and the case-law cited therein.
[22]That is, cases nn. C-131/12 (Google Spain), C-230/14 (Weltimmo), C-230/14 (Amazon).
[23] I.e., hereinafter, the "*Court of Justice of the European Union*".

establishment of the controller on the territory of a Member State, when the controller exercises, through stable arrangements in the territory of a Member State where the data subject is domiciled, a real and effective activity — even a minimal one — in the context of which that processing is carried out. In order to ascertain whether that is the case, the referring court may, in particular, take account of the fact that:

1) the operator of a search engine sets up in this Member State a branch or subsidiary which is intended to promote and sell advertising space offered by that engine and which orientates its activity towards the inhabitants of that Member State (Google Spain);
2) (i) the activity of the controller in respect of that processing, in the context of which that processing takes place, consists of the running of property dealing websites concerning properties situated in the territory of that Member State and written in that Member State's language and that it is, as a consequence, mainly or entirely directed at that Member State, and (ii) that that controller has a representative in that Member State, who is responsible for recovering the debts resulting from that activity and for representing the controller in the administrative and judicial proceedings relating to the processing of the data concerned (Weltimmo);
3) but an establishment cannot exist in a Member State merely because the undertaking's website is accessible there (Amazon).

In the recent case C-194/16, Svensk Handel, the ECJ has newly faced the problem of effective procedural data protection, referring to both jurisdiction and remedies. The case stems out from a litigation between an Estonian company and an employee of the same both taking action against a Swedish firm having published in internet a blacklist including the plaintiff company as committing fraud. The claim had as an object **the three main remedies in the field of data protection**, that is to say the; **rectification** of the false information published; the **removal of harmful comments** which were published as a consequence (right to *oblivion*), and the **monetary compensation for patrimonial and non-patrimonial damage**. The plaintiff chose to sue the defendant before the Estonian Court according to art 7 of 1215/2012 regulation, particularly choosing the court of the member state where the damage was inflicted. The Estonian Court of first instance had declined jurisdiction, stating that no damage could be located in the Estonian territory since the available false info was published in Swedish language and the harm was actually language-related so that the clients of the plaintiff company could hardly know it, so that no economic loss could be suffered in Estonia. The plaintiff appealed the decision to the Court of second instance, which referred a preliminary ruling to the ECJ asking for two different questions of law:

'(1) Is Article 7(2) of [Regulation No 1215/2012] to be interpreted as meaning that a person who alleges that his rights have been infringed by the publication of incorrect information concerning him on the internet and by the failure to remove comments relating to him can bring an action for

rectification of the incorrect information and removal of the harmful comments before the courts of any Member State in which the information on the internet is or was accessible, in respect of the harm sustained in that Member State?

(2) Is Article 7(2) of [Regulation No 1215/2012] to be interpreted as meaning that a legal person which alleges that its rights have been infringed by the publication of incorrect information concerning it on the internet and by the failure to remove comments relating to that person can, in respect of the entire harm that it has sustained, bring proceedings for rectification of the information, for an injunction for removal of the comments and for damages for the pecuniary loss caused by publication of the incorrect information on the internet before the courts of the State in which that legal person has its centre of interests?

(3) If the second question is answered in the affirmative: is Article 7(2) of [Regulation No 1215/2012] to be interpreted as meaning that: – it is to be assumed that a legal person has its centre of interests in the Member State in which it has its seat, and accordingly that the place where the harmful event occurred is in that Member State, or – in ascertaining a legal person's centre of interests, and accordingly the place where the harmful event occurred, regard must be had to all of the circumstances, such as its seat and fixed place of business, the location of its customers and the way and means in which its transactions are concluded?

As to the second and the third questions, which the ECJ assumed to examine as first, the ECJ stated that the legal person can take action to obtain the rectification of false information and the removal of comments against its reputation before the same court where it decides to take action for the entire harm sustained. The ECJ underlines that, this court coinciding with the one where the damage occurred, it is however not necessarily the court of its statutory seat, because the Regulation needs to be interpreted aiming at granting the most effective protection of the right of self-reputation, thus leaving chance to the claimant to prove that the center of its interest is actually differently located, i.e. in the place where its main economic activities regularly takes place.

As to the first question of law, the ECJ clarifies that, if the plaintiff can choose to take **action for damages compensation before the courts of the several Member States where a portion of the damage has occurred,** rather than before the one court related to the center of its interests, **there is no symmetry between this remedial technique and the protection got through the rectification and the removal of harmful comments**. Actually, the *ubiquitas* of the network - which features this kind of disputes - makes it impossible to split the *specific* remedies (that is the remedies of *rectification* and *removal*) before different Member States' Courts, as it can happen instead for *monetary compensation* (for an in depth analysis, see par. *5.2 "Claim-splitting as a form of "abuse of process": the Italian point of view*). On the contrary, it implies the concentration of these remedies before the only Member State's court where the main center of interests lies, which is the same where the whole economic compensation can be asked for.

4.3.Extending contractual remedies: consumer procedural rights applied to data protection.

In *data protection* field, no specific rule was in principle posed to derogate the general rule of defendant's domicile jurisdiction (*actor sequitur forum rei*). Differently from Consumer Law, where the clear presence of a weaker party had prompted the E.U. legislator to establish the more favorable *criterion* of the *forum actoris*, **in the sector of data protection** the rule of law for jurisdiction is the result of thoroughly construction by **ECJ, establishing by case-law the *forum actoris* rule in a number of cases through the balance of proportionality and predictability**, also by extending to data protection issues the protection granted to consumers by contract.

Particularly, in Amazon case[24], the ECJ considered the data subject as a consumer, thus applying the specific rule of *forum actoris* and extending to him the *ex officio* powers of the Court in order to declare null and void some abusive clauses. This construction, on the other way, shall be limited, due to the need to balance effectiveness and proportionality of the remedies.

In case Schrems 2[25], the ECJ has stated that the *forum actoris* for the data subject, who is also a consumer, is justified by its weaker position as a singular *vis-à-vis* to a company; *viceversa*, in case the plaintiff is leading a class-action, this natural disparity lacks, so the general rule of the forum of defendant shall come into force again. It is interesting to remark that the chance for the data subject, who is victim of his personal data breach, to lead a class-action is possible only by considering him as a consumer in a contractual relationship since, originally, no collective remedy was offered for compensation of the rights connected to privacy.

5. Damage Claim-splitting and relevant risks.

After having explained - in the previous § - the most relevant ECJ case-law on jurisdiction in data protection sector, in this § we will focus on the legal issues of jurisdiction arising from claim-splitting, whenever an action for damages compensation is activated by the victim of personal data breach.

5.1. Introduction

As already explained above, especially in § 4.2, the ECJ judgment on case C-194/16, Svensk Handel, states that the possibility to bring an action before the courts of the Member State in which the center of its interests is based, is **just an alternative** for the victim of privacy violations carried out through the internet.

More specifically, due to paragraph 31, read in conjunction with paragraph 32 of the said statement, it seems that a natural or a legal person which alleges the infringement of personality rights by

[24]See Judgment of the court (Third Chamber), 28 July 2016, Verein für Konsumenteninformation v. Amazon EU Sàrl, C-230/14 (Amazon).

[25]See Maximilian Schrems v. Facebook Ireland Limited, Case C-498/16.

means of data content placed online, have **two options:**

(i) to bring **one** single action for the whole damages before a single court (which must be identified, as above said, in the court of the Member State in which the center of its interests is based);

(ii) to bring **more** actions for damages, each before the courts of any Member State in which the victim has suffered an injury to its reputation: in this case any court requested has jurisdiction solely in respect of the harm caused in the relevant Member State[26].

Such principle had already been settled in a previous pronounce by the ECJ in order to give content to the criteria of the "*place where the harmful event occurred*" (see above § 4.1.) in the case of a victim of libel by a newspaper article distributed in several Member States. The ECJ had grounded its position on the following considerations: "*The place where the damage occurred is the place where the event giving rise to the damage, entailing tortious, delictual or quasi-delictual liability, produced its harmful effects upon the victim. In the case of an international libel through the press, the injury caused by a defamatory publication to the honour, reputation and good name of a natural or legal person occurs in* ***the places where the publication is distributed, when the victim is known in those places***"*"*[27]

In this respect, it has to be pointed out that, as explicitly acknowledged by the same ECJ, the said possibility may lead to "***admittedly disadvantages to having different court ruling on various aspect of the same dispute***"[28]. Such disadvantages may consist in remarkable risks and very harmful consequences with reference to privacy violations carried out through the internet, given that online contents are often spread to a wide range of public and are not usually limited to a specific geographic area (as already pointed out above, in § 3). Therefore, if the victim has an international reputation, '*the place where the damage occurred*' may – in theory – coincide with a

[26]ECJ, judgment of 17.10.2017, C-194/16, paragraphs 31 and 32:
"*In that regard, the Court has held, in relation to actions seeking compensation for non-material damage allegedly caused by a defamatory article published in the printed press, that the victim may bring an action for damages against the publisher before the courts of each Member State in which the publication was distributed and where the victim claims to have suffered injury to his reputation, which have jurisdiction to rule solely in respect of the harm caused in the Member State of the court seised (judgment of 7 March 1995, Shevill and Others, C-68/93, EU:C:1995:61, paragraph 33)".*
"*In the specific context of the internet, the Court has, nonetheless, ruled, in a case relating to a natural person, that, in the event of an alleged infringement of personality rights by means of content placed online on a website, the person who considers that his rights have been infringed must have the option of bringing an action for damages, in respect of all the harm caused, before the courts of the Member State in which the center of his interests is based (judgment of 25 October 2011, eDate Advertising and Others, C-509/09 and C-161/10, EU:C:2011:685, paragraph 52)*".

[27] ECJ, judgment of 7 March 1995, Shevill and Others, C-68/93, paragraphs 28 and 29. In the following paragraph 33, the ECJ has established that: *In light of the foregoing, the answer to the first, second, third and sixth questions referred by the House of Lords must be that, on a proper construction of the expression "place where the harmful event occurred" in Article 5(3) of the Convention, the victim of a libel by a newspaper article distributed in several Contracting States may bring an action for damages against the publisher either before the courts of the Contracting State of the place where the publisher of the defamatory publication is established, which have jurisdiction to award damages for all the harm caused by the defamation, or before the courts of each Contracting State in which the publication was distributed and where the victim claims to have suffered injury to his reputation, which have jurisdiction to rule solely in respect of the harm caused in the State of the court seised*".

[28] ECJ, judgment 7 March 1995 (case C-68/93), paragraph 32.

great number of Member States.

In the light of the foregoing, the **option** given to the victim, to sue the damaging party before the courts of any Member States in which the allegedly defamatory content is detected, seems to open the door to some malicious and arbitrary judiciary actions, consisting of an unreasonable splitting of the damage claim, in order to harass the defendant, forcing him to bear multiple costs.

5.2. Claim-splitting as a form of "*abuse of process*": the Italian point of view.

Italian Supreme Court ("*Corte di Cassazione*", hereinafter: "ISC") in 2007[29], with an innovative pronounce of its *United Sections*[30] ("*Sezioni Unite*"), has qualified the arbitrary splitting of a damage-claim into several minor actions as a kind of "***abuse of process***". The principle of "*abuse of process*" has been conceived by the case-law as a specific type of "*abuse of rights*".

5.2.1. The general principle of the prohibition of "*abuse of right*" in EU law and in ECJ case-law.

The principle of the prohibition of "*abuse of right*" finds its first recognition in Article 17 of ECHR, dated 1950, headed "*Prohibition of abuse of rights*"[31].I n addition, the ECJ case-law has gradually recognized such principle[32]. The said rule, therefore, represents the **balance between the strict application of the rule of law and the true spirit of that rule.** In this respect, a landmark case is *Emsland-Starke*[33], in which the ECJ pointed out that "*this general legal principle of abuse of rights exists in almost all the Member States and has already been applied in the case-law of the Court of Justice, although the Court has not expressly recognized it as a general principle of Community law*" (par. 38). As a consequence, "*By virtue of the legal principle of abuse of rights in force in Community law, financial advantages are not to be granted or, in some cases, are to be withdrawn retrospectively if it is shown that the commercial operations at issue were for the purpose of obtaining an advantage* ***which is incompatible with the objectives of the applicable Community rules*** *in that the conditions for obtaining that advantage were created artificially*" (par. 43)[34].

[29] ISC, United Sections, 15 November 2007, n. 23726.

[30] ISC sits in the special composition of "*Sezioni Unite*" especially in cases that urge the solution of contrasts among the case-law of several Italian judicial authorities, due to the fact that, in principle, in Italian legal system the common-law principle of "*stare decisis*" does not apply.

[31] It provides that: "*Nothing in this Convention may be interpreted as implying for any State, group or person any right to engage in any activity or perform any act aimed at the destruction of any of the rights and freedoms set forth herein or at their limitation to a greater extent than is provided for in the Convention*".

[32] So as to adjust the application of a rule of law on the basis of other values, such as good faith, fairness and substantial justice, in all those cases in which, despite the formal observance of the conditions of the rule, the concrete legal outcome appears to be against the objective of that rule.

[33] ECJ, judgment 14 December 2000, case C-110/99: (the case at hand was about a German company that exported potato-based products to Switzerland, for which it received an export refund on the basis of the Regulation 2730/79. Immediately after their release, the products were transported back to Germany, unaltered and by the same means of transport, and were there released for home use. The ECJ emphasized that the aim of the EU Regulations cannot be to cover abuses on the part of trader).

[34] With its well-known pronounce "Halifax", the ECJ clarified that in E.U. VAT (i.e. value added tax) a finding of abuse is triggered when obtaining a VAT advantage is the sole or the principal aim of the transaction. The court also

Trying the case *Kofoed* the ECJ finally referred to the prohibition of *abuse of right* as a general principle of E.U. law[35]. Such principle is now explicitly set forth also in the *Charter of Fundamental Rights of E.U.*, dated 2000, whose Art. 54 is headed "*Prohibition of abuse of rights*"[36].

5.2.2. The "*abuse of process*" as a particular form of "*abuse of rights".*

The so-called "*abuse of process*" has been recognized by the case-law[37] and legal writings[38] as a specific kind of "*abuse of rights",* which occurs whenever the judiciary action is not (or not only) filed with the aim of obtaining justice, but (also) with the aim of harming the counterpart. Such principle is considered as **a balance between the right to take legal proceedings and the right to a fair trial** (provided for by Art. 6 of ECHR). This specific concept has been constructed mostly in Common law States, but it has also gained great importance in Italian case-law, with particular reference to the splitting of legal claims for damages[39].

5.2.3. Claim-splitting in Italian case-law.

The constant jurisprudence of the ISC explicitly prevents an injured party from bringing more than one action, each for a single part of suffered damages, if such damages arise from a single cause of action and there is not any objective reason to split the same. Such behavior would be, in fact, considered as a form of "*abuse of process*". The *ratio* of this rule consists in the need to avoid that the bringing of not necessary actions becomes unjustifiably vexatious and oppressive for the defendant.

---

indicated that artificially splitting supplies into separate supplies by separate taxable persons can be taken as evidence of abuse of rights.

[35] ECJ, judgment of 5 July 2007, case C-321/05, *Hans Markus Kofoed v. Skatteministeriet*, paragraph 38. According to such principle: "*individuals must not improperly or fraudulently take advantage of provisions of Union law. The application of Union legislation cannot be extended to cover abusive practices, that is to say, transactions carried out not in the context of normal commercial operations, but solely for the purpose of wrongfully obtaining advantages provided for by Community law*".

[36] Art. 54 sets out that: "*Nothing in this Charter shall be interpreted as implying any right to engage in any activity or to perform any act aimed at the destruction of any of the rights and freedoms recognized in this Charter or at their limitation to a greater extent than is provided for herein*".

[37] See, e.g., the decision of Italian "*Consiglio di Stato*" (i.e. the highest Court for claims against public administrations), Section III, 13 April 2015, n. 1855.

[38] See, e.g., D. ANDERSON, *Abuse of rights*, 2006, *Judicial Review*, vol. 11 n. 4, 348, 350; G. VERDE, *L'abuso del diritto e l'abuso del processo (dopo la lettura del recente libro di Tropea)*, *Riv. Dir. Proc.*, 2015; K. POLONSKAYA, *Abuse of Rights: Should the Investor-State Tribunals Extend the Application of the Doctrine?*, 2014; E. de BRABANDERE, '*Good Faith', 'Abuse of Process' and the Initiation of Investment Treaty Claims, Journal of International Dispute Settlement*, Vol. 3, n. 3, pp. 1-28, 2012.

[39] The principle has been recognized also in UK: for example, the House of Lords in Johnson v Gore Wood has stated that: "*an important purpose of the rule is to protect a defendant against the harassment necessarily involved in repeated actions concerning the same subject matter*". In *Port of Melbourne Authority v Anshun Pty Ltd*, it was established that: "*…where a given matter becomes the subject of litigation in, and of adjudication by, a Court of competent jurisdiction, the Court requires the parties to that litigation to bring forward their whole case, and will not (except under special circumstances) permit the same parties to open the same subject of litigation in respect of a matter which might have been brought forward as part of the subject in contest, but which was not brought forward, only because they have, from negligence, inadvertence, or even accident, omitted part of their case*". It is widely accepted that it is an abuse to bring two or more sets of proceedings in respect of the same subject matter. This can in fact amount to harassment of the defendant in order to make it fight the same battle more than once with the consequent multiplication of costs, time and stress.

More specifically, the ISC, with the sentence no. 23726/2007 issued by its *Unified Sections*, stated that a creditor of a certain amount of money, owed under a single obligation, is not allowed to split the credit into many judicial requests, since such a division of the content of the obligation, operated by the creditor, aggravating the debtor's position, contrasts not only with the principle of correctness and good faith, which must underlie the relationship between the parties during the judicial proceedings, but also with the principle of a fair trial, set forth by Article 6 of ECHR. Therefore, parceling the judicial request for the purpose of satisfying the credit claims is an abuse of the judicial instruments that the legal system offers the parties.

Such general principle, established in the context of contractual obligations, has been then extended to torts, considering an *abuse of process* to separate, for example, the claim for material damages from the claim for compensation of the suffered injuries[40].

It has to be pointed out that **the rule is not based on the principle of *res judicata***, since it applies to different claims concerning different parts of damages (even if arising from the same cause of action), and not, therefore, to the "same claim".

With regard to the consequences of the breach of the said principle, the ISC has clarified since 2008 that the request put forward in a second time, without any objective reason, must be considered as '*non-actionable*'[41].

After all, said conclusion appears to be an excessive sanction, considering that it affects the right to take legal proceedings for (part of) suffered damages, in the absence of an explicit legal provision in this respect. For this reason, a minority opinion has deemed more coherent to the constitutional and European fundamental rights that the sanction may only be the burden of judicial costs, even if the party (who abused of the process) turns out to be the winner[42].

5.2.4. A critical and suggested point of view.

As above said (see above, especially §§ 4.2 and 5.1), a victim of privacy torts may bring actions in any Member State in which the infringement has produced its effects, for the sole part of damage occurred in that State.

This rule turns out to be a sort of claim-splitting, with the same harmful consequences for the defendant as the ones examined in the previous sub-paragraphs. Such consequences can be even worse if we consider that the splitting of the damage claim occurs among different States, so that the defendant is not only bound to bear multiple costs and the pressure of several actions with reference to the same event, but it has to defend himself before the courts of different States, with different legal procedures, languages, etc.

This is why **we deem it appropriate that the possibility, granted to the victim of privacy torts,**

[40] ISC, Section III, 22 December 2011, n. 28286.
[41] ISC, Section III, 11 June 2008, n. 15476; ICS, Unified Sections 16 February 2017, n. 4090 and ISC, Section III, 17 January 2017, n. 929.
[42] E.g. ISC, Section I, 3 May 2010, n. 10634.

to bring as many actions as the Countries in which the privacy infringement has produced its effects, should be reconsidered under the light of the theory of the "*abuse of process*", elaborated by the Italian case-law. It seems in fact, to us, more coherent with the EU general principles to allow the damaged party just to bring one single action for the entire amount of damages before the court of a single Member State (the one where the victim's center of interest is based).

The *equilibrium* should be better reached with reference to the burden of judicial costs. In effect, **a party claiming for damages which decides, without any reasonable ground, to split up its claim, still acts on the ground of its right to obtain compensation for the suffered losses**. This right, however, is wrongly exercised, turning out in an *abuse of process*, since it forces the defendant and the legal system to an useless waste of costs and time. Therefore, the most proper sanction seems to be that **the claimant should bear the superfluous costs generated through its (mis-)conduct**. On the contrary, a sanction affecting (*per se*) the right to claim for a part of damages seems to be in contrast with the fundamental right to an effective remedy, set forth by Article 47 the *Charter of Fundamental Rights of E.U.*[43] and by Article 13 of ECHR[44].

6. Cooperation between judicial and administrative Authorities: the key for integrated enforcement.

After having dealt with the questions of jurisdiction arising from E.U. privacy tort-law, in this § we will focus on the need of integration of the judicial and legal techniques, with some implications as to the way we propose to conceive and allocate the legal remedies in favor of any data breach victim[45]. The nature of tort obligation in privacy violations implies the need of a jurisdiction based on the proximity to the source of evidence; the high technological implications arising from most of the infringements create an emphasized bifurcation between *specific* remedies and the *compensatory* one. Actually, the formers often require specific knowledge to be applied and are better prevented in order to achieve the best possible protection; the latter, on the other ground, implies several legal questions in point of causal *nexus* and liable subject, which are better to be solved in the field of jurisdiction.

That is why, though E.U. law expressly grants judicial data protection, the field has known the

[43] Article 47 of the Charter of Fundamental Rights of European Union: *"Everyone whose rights and freedoms guaranteed by the law of the Union are violated has the right to an effective remedy before a tribunal in compliance with the conditions laid down in this Article. Everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal previously established by law. Everyone shall have the possibility of being advised, defended and represented. Legal aid shall be made available to those who lack sufficient resources in so far as such aid is necessary to ensure effective access to justice*".

[44] Article 13 of ECHR: "*Everyone whose rights and freedoms as set forth in this Convention are violated shall have an effective remedy before a national authority notwithstanding that the violation has been committed by persons acting in an official capacity*".

[45] In Italian recent ISC case-law on the role and the border between the two enforcement powers, it has been stated that the administrative decision cannot bind the related judicial proceeding concerning damages as a *res iudicata* (ISC, decision n. 1315/2017); nor the *lis pendens* before the *Data protection Authority* can automatically drive to a dismissal of judicial action (ISC decision n. 17408/2012).

development of national administrative authorities with high level of impartiality and technical expertise. It is possible to affirm that the special features of jurisdiction in privacy violations are defined by its relationship with Administrative Authorities. It is has been discussed if this *phenomenon* is to be read as an obstacle to graduated access to jurisdiction for the Member States. In Puskar[46], ECJ stated that E.U. law does not forbid graduated jurisdiction when it is imposed by reasons of *general interest*. Anyway, it must be considered that some written Constitutions of the Member States could formally be an impediment to this option[47].

As to the connection between judicial and administrative powers, currently, even if Authorities are cut out of vertical political control and are characterized by a high level of impartiality, they do not offer the same level of *neutrality* and *independence* as well as those granted by the right of defense typical of Courts' proceedings. As a result, across the E.U., administrative enforcement for privacy breaches, in point of *specific* remedies, should not exclude Judicial review.

Furthermore, even if administrative protection proves to be quite effective due to *ex officio* powers of the Authorities, particularly as for the *specific* remedies of *rectification* and *removal*, the subsequent judicial control is characterized by its large scope, far from being merely formal, and the proof settled in administrative procedure is persuasive, though not binding for the judge[48], considered the nature of fundamental rights of the legal positions involved[49].

The presence of two different patterns of enforcement, the judicial and the administrative one, has the advantage of virtually offering a very exhausting scheme of protection. On the other ground, it has the cons of possible lack of coordination resulting in longer and less efficient law enforcement of privacy, particularly because **E.U. law did not originally set forth a true right to be heard before administrative authorities, with a *vulnus* to the right of defense.**

Finally, it must be considered that, in the last years, the developed case-law and the new challenges linked to fast technological progress, with its declinations in everyday life of E.U. citizens and institutions, have made it clear that only a general reform might correct the lack of coherence and the weaknesses of the system.

[46]See Judgment of the Court (Second Chamber) of 27 September 2017, Peter Puškár v Finančné riaditeľstvo Slovenskej republiky, Kriminálny úrad finančnej správy, Case C-73/16.

[47]For example, artt. 24-113 of Italian Constitution state that judicial enforcement is always granted on administrative decisions affecting substantive rights; Italian case-law has stated that graduated access to jurisdiction can be allowed only if it is finalized to higher general interests, to be verified after an extremely rigorous check, which has often led to declarations of unconstitutionality of the rule (see, e.g., Italian Constitutional Court decisions, nn. 233/1996, 56/1995, 132/1998).

[48]For instance, in the decision of the Tribunal of Milan n. 10374/2016, the court, providing for the judicial review of the decision of the national supervisory authority, quashed the decision affirming that the balancing exercise between the public interest in the news (re-)published by an online blog, and the right to personal identity (enshrining the right to oblivion) was not correctly assessed by the national supervisory authority. In this case, then, the tribunal addressed in detail the proofs (i.e. the pieces of news published online) in order provide its own evaluation on whether the personal data of the claimant could be qualified as pertinent, complete and updated.

[49]See Tribunal of Milan, n. 5022/2017: the court confirmed the decision of Data Protection Authority and condemned a telephone operator (Telecom) for contacting about 2 million former customers who explicitly denied or did not consent to be contacted for commercial offers.

6.1 Overview of the architecture of remedies: some critical aspects.

As already explained, the architecture of E.U. data protection has faced some critical aspects urging for changes, in order to grant the effective enforcement of fundamental rights linked to *human persona.* As to jurisdiction, the lack of a specific rule stating *forum actoris* for the data subject has required an elaborated interpretation of the general rule of connecting factors in tort obligation, with a careful balance of the opposing principle of effectiveness (mainly affecting the claimant) and proportionality (manly affecting the defendant). As a consequence, ECJ and National courts have tried to grant the weaker position of data subject standing before big data companies, extending the contractual remedies posed for consumer protection, with though some difficulties and limitations due to the different *ratio* of the two systems. It should be considered that questions of jurisdiction might arise between E.U. and Third States too[50]. Furthermore, the need of coordination between judicial and administrative enforcement has known some limitations due to the lack of more specific rules about procedural guarantees before the Authorities, particularly as to the right to be heard.

It seems to us that the administrative authorities are better entrusted with *specific* remedies (i.e. *removal* and *rectification*), which do of course imply difficult balances between privacy and public interest (as in the case of request for the removal of harmful information concerning the so called right to *oblivion*), making more difficult the enforcement of data protection by such Authorities[51]. Hence, a shared approach to the issues arising from technologies is highly recommended[52]. Finally**, the restoration** before courts for damage involves new issues concerning the identification of the liable subject in big data companies and cloud technology. This is particularly relevant if we consider that the standard of the proof is extremely strict, since liability can be dismissed only by demonstrating complete diligence or lack of any causal *nexus*. In addition, some specific Consumer Law remedies might be successfully transplanted to data protection field, through specific rules of adjustment. It seems clear that only a general reform could provide for an effective, highly integrated system of enforcement in the field of data protection.

7. The New Deal of Data Protection.

The need of a general reform of E.U. data protection law has finally been satisfied by the issuing of Reg. nr.679/2016 (hereinafter "GDPR"). Its provisions aim at granting an updated, highly integrated

[50] The recent case-law has actually known the problem to extend E.U. jurisdiction to big data companies having statutory seats in third states, manipulating personal data without the level of protection of fundamental rights granted in E.U. and nevertheless claiming jurisdiction in their countries.

[51] The effectiveness of specific remedies in the field of data protection is strictly linked to the fast updating of technologies.

[52]For example, data available to big data companies processing metadata; protection of mass storage security in cloud technology, or, furthermore data subject profiling in electoral campaigns. In these cases, by the way, enhancing the preventive phase dealt by authorities could definitely be a key point of the system. See A. BIASOTTI, *Il Nuovo Regolamento Europeo sulla protezione dei dati*", EPC, III Edit.

system of protection, dealing with the most critical aspects of data protection law.

As to the object of this paper, it is worth noting that, whereas the former set of rules did not include any **specific rules on the jurisdiction**, article Article 79 (2) of the GDPR (and its Recital 145) faces the question[53]. The GDPR thus creates a specific rule on jurisdiction in favor of the data subject, who may bring his claim before the courts of the Member State of his own habitual residence. **This rule of favor is quite similar to the one laid down by Regulation Brussels I / Brussels I bis in favor of consumers.** Article 79 (2) is to be read in the light of Recital 147 of the Preamble of the GDPR[54]. This E.U. Regulation also makes law the important case-law involving big data companies, imposing them the compliance to E.U. privacy law when European citizens' data are processed and identifying the jurisdiction within the E.U. even outside the State of their statutory seat, in force of the connecting factor of the injured center of interests[55].

As for the *specific* remedies, the GDPR seems to correct some partial lack of coordination between administrative and judicial authorities. The administrative enforcement still appears to have better chance as to *rectification*, *suspension* or *removal* of unlawfully collected data. Nevertheless, the judicial protection takes place as a second step in order to review - to large extent - the administrative decisions. The balance is built, on the one hand, by making evidence collected in the administrative process persuasive but not binding and, on the other hand, by making the process before Authorities nearer to a *due process of law*[56], particularly by stating a precise right to be heard before privacy Authorities as a requirement for the lawfulness of their fines and/or injunctions[57]. Finally, the GDPR achieves to give an answer to the most difficult questions arising in the field of

[53] "*Proceedings against a controller or a processor shall be brought before the courts of the Member State where the controller or processor has an establishment. Alternatively, such proceedings may be brought before the courts of the Member State where the data subject has his or her habitual residence, unless the controller or processor is a public authority of a Member State acting in the exercise of its public powers."*

[54] "*Where specific rules on jurisdiction are contained in this Regulation, in particular as regards proceedings seeking a judicial remedy including compensation, against a controller or processor, general jurisdiction rules such as those of Regulation (EU) No 1215/2012 of the European Parliament and of the Council (13) should not prejudice the application of such specific rules*".

[55] At the same time, the consideration about different level of protection of privacy between E.U. and USA has put the basis for a reform of *Safe Harbor*, now overturned by the so-called *Privacy Shield*, imposing higher level of protection and supervision by USA government authorities when E.U. citizen data are processed.

[56] It should be noted that, in accordance to the regime provided by the previous Directive 95/46, the same procedural guarantees were not binding and they resulted, for instance, in the denial to the obligation to provide an oral hearing before the national supervisory authority. For instance, in Ireland, in case Martin v. Data Protection Commissioner [2016] IEHC 479, the High Court affirmed that the Data Protection Commissioner, in case of refusal to further investigate the facts with a complaint procedure, was not empowered to hold an oral hearing under the Data Protection Directive 95/46/EC or the Data Protection Acts 1988 and 2003 (the Acts). However, the High court affirms that consequently to the appeal against the decision of the Data Protection Commissioner, the claimant will exercise his right to be heard before a court. Differently, in Scotland, in the case of a procedure to recover medical records related to an individual, which was the complainer in a different case of domestic abuse, the Outer House of the Court of Session affirmed that the right to privacy and medical confidentiality, interpreted in the light of Article 8 ECHR entitles, complainers to be heard and have legal representation in the procedure.

[57] In particular, recital (129) GDPR affirms that "…*The powers of supervisory authorities should be exercised in accordance with appropriate procedural safeguards set out in Union and Member State law, impartially, fairly and within a reasonable time. In particular each measure should be appropriate, necessary and proportionate in view of ensuring compliance with this Regulation, taking into account the circumstances of each individual case, respect the right of every person to be heard before any individual measure which would affect him or her adversely is taken and avoid superfluous costs and excessive inconveniences for the persons concerned*".

compensatory protection, which stays the kind of remedy to be efficiently granted only through jurisdiction. For what concerns the identification of the responsible subject in big data companies, it openly states a collective liability between the Data Controller and the Data processor, with the structure of joint and several liability and a subsequent action of claim-back (GDPR art. 82). It also follows the path opened by ECJ case-law by importing some remedial techniques originally belonging to Consumer Law, adapting them to data protection, such as the use of class action: article 80 of GDPR now provides for the faculty of representation of data subjects by a no-profit body, representation or association before courts, thus introducing a kind of collective redress.

For such reasons, as a **conclusive remark**, we point out that it may prove to be particularly interesting to assess the possible future consequences of the introduction of such GDPR provisions in the field of *Jurisdiction*. As a matter of fact, since **the weaker position of data subject is now mitigated by class action**, **the ECJ,** and subsequently the national courts, **could implement the orientation of Schrems case** and, as a result, find more appropriate to settle jurisdiction according to the *forum* of defendant rather than to the *forum actoris*, balancing *effectiveness* and *proportionality* in the view of the best protection possible of the right of defense.