Knowledge of the Law in the Big Data Age
G. Peruginelli and S. Faro (Eds.)

doi:10.3233/FAIA190005

Entropy in Digital Information and the Enforcement of Law: Towards a Unification of Remedies?

Giorgio GIANNONE CODIGLIONE
Università degli Studi di Salerno (Italy)

Abstract. The Chapter aims to examine the legal remedies – both judicial and non-judicial – available in the area of electronic communication, adopting as the main comparison parameter the problem of the legal status of digital information. The infocentric structure of today's society on the one hand does not allow for the advance identification of a clear and generalized correspondence between a subjective legal situation and digital information; on the other hand, protection mechanisms tend to converge both from a classification and a technical profile. In other words, the consolidated subjective right vs. remedy model – understood as a system of subjective situations that are pre-established by the law from which owners derive their faculty or powers and which puts the obligation to do (or also not do) in the hands of individuals or the rest of the community, and alongside which a range of protection instruments can be found that can be invoked before the courts in the case of violations (*ubi jus*, *ibi remedium*) – is often diminished and becomes more typically an action-reaction model. In a multi-subject context marked by a post-industrial, cognitive economic model, it is possible that at the operational level the administration of one type of remedy implies a different consequence for all the other subjects involved in the information flow. While respecting the diversity of the experiences analysed, the regulatory trend seems to be that of the parcelling up of behavioral standards in a preventive and collaborative key.

Keywords. theory of information, economic analysis of law, defamation, data protection, intellectual property, consumer protection, tort law, remedies

1. Introduction

Tackling the subject of enforcement of the law on the Internet leads us firstly to highlight three fundamental differences between the online and offline perspective:

1. As we all know, a person connects to the Internet through one or more terminals with the general expectation of anonymity (protected or unprotected) [1]; [2]; [3]; [4]; [5]; [6]; [7]; [8]; [9].
2. The access to the Internet and its services generates a legal connection of inter-dependence with the network and service providers and produces a constant flow of data, characterised by the endless possibilities of using in terms of replicability, modifications and ubiquity.
3. Data that transits over the Internet can identify the agent, but also the action: the creation of a technical ecosystem that produces and feeds itself with digital in-

formation makes the person as a 'complex information entity' [10], that acts ever more often through digital inputs, establishing a two-way relationship of production and sustenance.

In other words, data represents the most innovative form of social subject ever created by man [11]; [12]; [13], that condenses (also simultaneously) the functions of identification and actions, just as it does those of prescriptive, sanctionatory or reparatory functions of a norm or a binding legal decision [14]; [15].

The 'polisemic' nature of the legal meanings and the effects attributed to online data, where this is not associated with a continuous and compliant flow of information, brings up the problem of entropy as developed in thermodynamics, recalled by Norbert Wiener [16], the father of cybernetics and later used in many areas of the modern theories on information, even though this needs to be contextualised within the particular system of the Internet.

Physicists define entropy as the measure of disorder in a system, hence the more ordered and structured the system is, the less entropy (and the more information) there is and vice versa. In a wider sense, the concept of entropy associates disorder and uncertainty inherent in the natural state[1].

The Internet, understood as a decentralised communication system that encourages technical and human interaction through the communication of data packages from one point to another[2] [17]; [18]; [19], represents in theory an exceptional tool to counter the phenomena of entropy, but at the same time unveils new risks of degeneration typical of technology as the maximum expression of man's will for power [20]; [21]; [22]; [23]. According to Wiener, in fact, the main tool to control entropy is that of feedback, i.e. the human approach to act bearing in mind that which he has done before, thereby repairing any mistakes made[3].

On the Internet, this remedial function is in theory encouraged by the ease with which it is possible to communicate between different parties[4], but at the same time it suffers from the multiplier effect generated by the simultaneous and immediate circulation of non-compliant data, making it much more difficult to correct and modify the erroneous information within the system before they can have an effect[5].

Understanding these essential aspects of human actions on the Internet in more depth leads to a silent, but revolutionary, paradigm shift in the techniques of protection of the fundamental rights, requiring a holistic and multilevel approach, paying attention to verify how the attribution of a particular 'legal statute' to digital information can influence the different levels of the technological ecosystem [24].

2. Techniques of Protection of Online Reputation

Here I will try to outline two regulatory tendencies that are emerging – above all in Europe – and that concern three key areas of ICT Law: online defamation, data protection and copyright.

As is well-known, information (be it either digital or analogical) is considered as a 'good' [25]; [26]; [27]; [28]; [29]; [30]; [31], in the sense that it undergoes a process of 'cataloguing' in order to assign an owner and attribute a legal 'value' to it (which could also correspond in various measure also, ex ante or ex post, to an economic value) as well as the predisposition of a certain protection regime, consisting, for example, of the

fixing of certain rules of conduct and the guarantee of the effectiveness of those remedies. Every definition of a certain 'good' has three functions: recognise the owner, attribute a value, act either before and/or after as a protection.

In the area of digital information on the Internet, due to the reasons outlined previously, such functions often seem to be limited, above all regarding the preventative definition in the legal system of the relative areas of protection [32].

Reputation is an information 'good' that, despite being recognised *a priori* by the legal system, is often evaluated in a negative sense, in that it is identified as such every time is harmed.

The creation and the posting of false, inexact, or misleading data regarding a natural or legal person by third parties on the Web, is one of the crucial issues of the first thirty years of the history of the Internet. The infinite replication and the ease with which harmful and defamatory content is circulated has led legislators, judges (and also ISPs) to apply two different protection methods, that in general can be defined following the distinction established by Calabresi and Melamed between *property rules* and *liability rules*, but with the particularity that I will try to explain now.

Property rules refer to the rules that protect in an absolute and exclusive way – for example through a prohibition or an order – the owner of a good from any form of interference from third parties, except in cases in which the parties decide voluntarily to cede that good to a third party in exchange for payment [33].

In our case, reputation is a subjective situation (but also a fundamental right of the individual) that must not be harmed in any way by other members, except in the context of the balancing of other rights and fundamental freedoms such as that of the freedom of expression.

The prohibition to offend or unjustifiably harm the image of another person, once violated, is evaluated and sanctioned with the removal of the harmful content, the order not to repeat this form of conduct and the payment of a sum of money to compensate the victim for the damage suffered. In the latter case, therefore, where the legislation retains it difficult (or uneconomical) to enact (and to enforce) a property rule (hence in the presence of high transaction costs), it can cumulatively, or alternatively, sanction the transgressor by imposing the *liability rule*, defined by Calabresi and Melamed as a remedy to compensate the victim in cases where it is impossible or uneconomical for the person doing the harm and the person harmed to find an agreement for the transfer of the good.

On the so-called Web 2.0, the protection framework can be summarised as follows: given that the user must be able to operate freely on the Internet, in the case of content created and circulated on platforms managed by third parties, it is the provider that is required to act – on the input of the judicial authority or by the individual who has been harmed – to supply the identification data of the author of the unlawful content and/or remove the harmful information, or also to respond for the eventual failure to remove this content in a timely manner [34].

In other words, the system is based on the general activation of the property rule connected to the degree of collaboration of the provider (supply of the data regarding the author of the conduct, timely removal of the content). In essence, due to the difficulty in tracing the author of the damage, which is linked to the protection of the legitimate expectation of privacy of the user, the protection regime was characterised by the minimum goal of the removal of the content, to which is linked the eventual activation of the liabil-

ity rule – such as sanctions for the failure (or incorrect) fulfilment of a supervision duty given to the provider and consistent with the *ex post* protection of the rights of the users.

The framework described, proposed in the Electronic Commerce Directive 2000/31/EC and outlined in a more liberal way in the *U.S. Common Decency Act of 1996*, in the last decade has had to face the problem of the implementation of systems of social interaction that are entirely based (not only because of how they function, but also their economic sustainability) on the incentive for users to produce and share data.

The user is in fact encouraged to become an integral part of the system and this leads to the difficulty in controlling the flow of information and erasing harmful content in a definitive manner. This is a problem that is added to that already described of the identification of the true author of the conduct.

A recent judicial trend has strengthened the rule of the direct responsibility of the user, that places on the person who created and circulated the harmful content not only the duty to remove it, but also to act in order to prevent any form of replication or diffusion of the information.

The *Störerhaftung* rule, connected to an interpretation of § 1004 BGB (regarding the actions taken to remove the content that violates copyright or to inhibit its continuation) is aimed at all those who have either directly (*unmittelbarer Störer*) or even as an intermediary or indirectly (*mittelbarer Störer*) caused an unauthorised invasion into the judicial sphere of another[6], confirming a rule of responsibility that is particularly sensitive to the causal relationship of the harmful conduct, also in the presence of the extreme fragmentation induced by the presence of the user in the technical-informational ecosystem.

The *Störerhaftung* is set out as a property rule that is extended by case law also to the categories of the Individual - *Immaterialgüter rechte* and is applied if the 'interferer': a) contributed to the illegal activity in a causal and inappropriate manner; b) had the legal and practical possibility to prevent the violation; c) violated the reasonable duty of supervision or control over such illegal conduct for prevention purposes. In general, the violation of these rules does not lead to a sentence for compensation damages, but at most the payment of legal costs for any notification of cease and desist orders[7].

The responsibility linked to the possible circulation of content by third parties is partially given also to the person who initiated the communication: they must in fact take all adequate, proportionate and not excessively costly measures – with the cooperation of other users (who are in turn obliged to do as *Täter*, i.e. direct disturbers) – in order for the harmful content to be removed entirely from the Internet.

As for the rules regarding the duty of the ISP, a new direct policy tendency seems to be emerging, confirmed – as we will see – by some adaptations of case law[8].

Following the principle of neutrality confirmed in Article 15(1) of the Directive 2000/31/EC, providers do not have an overall duty to supervise the information that they transmit or store, or any obligation to actively look for facts and circumstances that indicate the presence of unlawful activity. This assumption, that has been reiterated many times by the EU Court of Justice and that became one of the key turning points in the evolutionary judicial interpretation of the e-commerce directive [35], finds a new interpretation in the recent position announced by the EU Commission[9].

According to the Commission, the heterogeneity of the regulatory approaches implemented over the years by the Member States, differentiated on the basis of the procedure and often dedicated to specific types of unlawful information, gives rise to a fragmented and ineffective framework.

From this standpoint, EU strategy begins with the promotion of voluntary measures (such as the *Code of Conduct to combat illegal forms of online hate speech*[10]) and others focused on the fight against specific crimes (such as child pornography or terrorism[11]), until reaching the provision of a dual channel of measures that strengthen the level of diligence required from hosting providers.

In terms of prevention, a discussion is underway on the adoption of effective proactive voluntary measures, aimed at identifying and removing illicit contents in order to reduce the risk of serious damage, without however the need for the provider to move outside the regime of applicability of the safe harbour regime referred to in Article 14, Directive 2000/31/EC[12].

In subsequent interventions, the Commission calls for the implementation of easily accessible and understandable mechanisms for the gathering of motivated and precise reports, which also guarantee the timely and effective removal or disabling of access to illegal content following reports from users[13].

3. The EU's Data Protection Strategy and Its Influence on the Evolution of ICT Law

The picture described so far foresees, therefore, the existence of a legal relationship – corresponding to different forms of supervision duty – between the user and the information introduced and circulated by them on a web platform. This tendency, interpreted backwards, reallocates the property rule in a greater measure to the author (or the co-authors) of the damage, framing the intervention rules and the responsibilities of the provider as a form of secondary regime, that is in turn split into prevention and reparation duties.

Also in the area of the protection of personal data, the regulatory tendencies seem to follow this new viewpoint, strictly linked to the parcelization of conduct with the creation of a qualified relationship between information and those involved in the processing activity.

The fundamental right to data protection is understood as a subjective legal situation that ascribes abstractly the 'belonging' to natural person of all the data that is directly or indirectly attributable to them. In the absence of consent and/or of a justifying cause, the processing of any information concerning an identified or identifiable natural person is illicit and leads to consequences for the parties who are involved in the processing to varying degrees (the controller, the joint controller, the processor, those authorised to process data).

Given the fundamental role that the circulation of data plays in the Internet environment and more generally in today society, Convention no. 101/1981 of the Council of Europe and Directive 95/46/EC (first) and General Data Protection Regulation 679/2016 (GDPR), followed in 2018 by the CoE's 'Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data' (after), established the evolution of the right to data protection on one hand as a right to the control and to the information of the data subject (*Recht auf informationelle selbstbestimmung*), and on the other hand, as an obligation for compliant processing for controllers and processors, establishing precautionary conduct and introducing a harsh administrative sanctions regime that in turn compensates for the mitigation of the criminal and civil sanctions regime.

In other words, the parties that undertake a processing activity[14] must adhere to strict rules in order not to suffer – amongst the other sanctions – the possible imposition of a liability rule. The accountability principle introduced by GDPR consists in the duty to enact (and provide proof) organisational activities (e.g. impact assessment, pseudonymisation, privacy by default and by design) and preventive or specific redress remedies such as the modification, rectification and erasure of data, the limitation of processing or the opposition and the provision of personal data in an interoperable format (the so-called right to portability) [36]; [37]; [38].

The online 'right to be forgotten' is a clear example of the parcelization of the duties of care and also of the complementary position attributed to pecuniary compensation rules: following the jurisprudential adaptation undertaken by the CJEU with the *Google Spain* case[15], Article 17 of the GDPR affirms the autonomy of the processing carried out by web-pages with respect to the activity of search engines, establishing the right of the data subject to request directly to the data controllers respectively to evaluate respectively the possible deindexing or erasure of the information deemed inaccurate or processed in an unlawful manner. An analysis of the case law on the issue (in France, Italy and Spain) shows that failure to properly comply with the screening of the requests does not necessarily lead to the obligation to pay damages, a measure that in most cases is limited to the refunding of legal and procedural costs[16].

As a remedy, paragraph 2 of the aforementioned Article 17 reformulates the rule proposed by the BGH on the issue of the protection of reputation: the data controller who made public the personal data considered illicit, must – "*taking into account the technology available and the costs of implementation*" – inform any other data controllers who are processing the same data of the request of the party concerned to delete any link, copy or reproduction of this[17]. If, for example, the editor of an online newspaper is obliged to delete some personal data contained in an article published in the past, they have the duty to inform also the other parties that supply further diffusion or links to that news story (as well as the search engines).

This trend should be read in the context of the interpretation of the concept of 'controller', 'joint controller' and 'processor' in a flexible and dynamic way not necessarily to the business figure of the ISP: these concepts can in fact be progressively extended for example to the user who manages a social profile not for mere domestic purposes, as established by recital no. 18 of the GDPR and confirmed by the CJEU in the recent case of *Wirtschaftsakademie Schleswig-Holstein* regarding the administration of a fan page[18].

4. Enforcing Digital Copyright and the Role of Internet Service Provider: From Reparation to Prevention?

Coming to digital copyright – understood as a right with a monopolistic-ownership matrix, having as its subject some particular forms of human creativity (such as literary works, musical works, but also databases) – it embodies the contrast par excellence between having the exclusive right over or having access to knowledge (and therefore the right to freely benefit from the information flow promoted by the Internet) [39]; [40]; [41].

Having lost the tangibility of the media used by intermediaries (such as publishers, producers, distributors), to 'capture' the intellectual work and facilitate the autho-

rized circulation after the payment of a price by the users, digital copyright is constantly searching for a new structure that is capable of making the requirement to effective protect copyright holders without limiting the incentive goal that is generally recognized in the free circulation of creative works.

In this sense, on a level of taxonomy, case law and doctrine have for a decade ensured the transit of copyright from the dominical dimension to that of so-called compensation fees. However, this does not solve the problem of the effectiveness of the remedies that protect the patrimonial and non-patrimonial assets of the authors encapsulated in the digital information, through techniques aimed at controlling their circulation (think for example of the DRM, an expression of a property rule that is a fundamental part of the conformation technique), or through the prior identification of the subject to whom to allocate at least the 'price' of unauthorized use, where it is not 'protected' by the safe harbour of fair use.

In this framework, a new and interesting interpretation of the material has been given by a set of judgments of the CJEU.

In *GS Media vs. Sanoma*[19], the publication and updating of hyperlinks, repeated also following the removal of protected content by the source websites, was deemed to be an unauthorized act of communication to the public, as it was carried out for profit (e.g. related to the publication of advertising banners) and for this reason "*with full knowledge of the fact that the work is protected and that the copyright holder may not have authorized the publication on the Internet*"[20]. The mere fact that the sole activity of providing a connection to protected works published without authorization is undertaken by a party who performs a business activity, includes a presumption of knowledge of the unlawfulness of such contents.

Together with the "*unavoidable role of the user*" and the "*intentional nature of his/her intervention*", the reference to the "*profit-making purpose*", introduced for the first time in the Premier League decision[21] – and indeed absent in Article 3(1), Directive 2001/29/EC – is used by the Court as a further parameter for an 'individualized assessment' of the EU concept of 'communication to the public', ensuring a fair balancing of the public interest in access to information, recognized to the activity of creating links to third-party websites carried out by private individuals who are not working to obtain any profit. In fact, in the case of non-profit entities, the Court introduces a general regime of unawareness of the possible illegality of the content to which the link refers. This rule no longer applies once the user has received notice about this, in a manner similar to the provisions on the exemption from liability of the hosting provider in the e-commerce directive.

The presumption of the unlawfulness of linking related to the requirement of the awareness of the person who posts it, as well as the lucrative nature of the communication, has found confirmation in the *Stichting Brein I* case: the marketing of portable multimedia players equipped with a software capable of opening web links to pages in which protected works were made available without the authorization of the copyright holders, was deemed an act of unauthorized communication to the public, which did not meet the requirements of the exception on temporary reproduction referred to in Article 5(1), Directive 2001/29/EC, read in conjunction with Article 5(5)[22].

This trend has found confirmation in *Stichting Brein II*[23] (the so-called *Pirate Bay* case), in which the CJEU judged as an unauthorized 'communication to the public' the conduct of a web platform, which by indexing metadata related to protected works (so-

called torrents) and the provision of a search engine allowed users to locate such works and share them over a network (*peer-to-peer*).

When interpreted together, the aforementioned decisions lead to a confirmation of a presumption of the responsibility of the provider who, for the pursuit of a profit, allows searching, location and sharing of protected works. In this case, the notion of profit is in any case implicitly linked to the fact that the provider offers a service that is addressed – entirely or in part – to the aggregation and provision of content uploaded by users (and in any case traceable to another physical address, represented by a website or even by the PC connected to the sharing network) and aimed at aware communicating to the public *en masse*, protected works.

The formulation of a general presumption of the knowledge of the unlawfulness of the contents in relation to the provider of links who acts for profit mainly, paves the way for the affirmation of a preventive duty of control placed also on generalist search engine [42].

To this, therefore, a parameter of imputation of semi-objective character should be applied, in some way comparable to that in force in the area of protection of personal data, given that the provider should be exempt from this only once this presumption has been confuted, by proving they "adopted all the appropriate measures to avoid the damage".

This direction is also confirmed by the recent approval by the European Parliament – albeit with some modifications – of the *Proposal for a Directive on copyright in the digital single market*[24], which in Article 13 foresees, for the 'new' category of online content sharing providers[25], the obligation to conclude licensing agreements with the owners of the rights of the works uploaded[26].

The proposal applies the obligation to negotiate licenses and to adopt content protection measures to a broad category of subjects, identifying in the "information society service providers one of the main purposes of which is to store and give access to the public or to stream significant amounts of copyright protected content uploaded/made available by its users, and that optimise content, and promote for profit making purposes, including amongst others displaying, tagging, curating, sequencing, the uploaded works or other subject-matter, irrespective of the means used, and therefore act in an active way".

In this way the provider – defined in the law in the category of the so-called 'active hosts' established through the interpretation of recital no. 42 of the Directive 2000/31/EC – is encouraged to act in a precautionary way to check and if necessary to remove the contents uploaded by users in order to avoid incurring liability. In other words, the proposal introduces a further supervision duty for the majority of Web 2.0 providers, who could thus be called on directly to respond to the failure (or incorrect) fulfilment of this obligation.

This supervision duty goes alongside that foreseen by the e-commerce directive, which, on the contrary, defines a regime of the general lack of responsibility of the provider, as long as they respect the precise rules of conduct (and timely intervention) in cases where they are notified of a violation [43].

The above mentioned proposal, now being examined by the Council, seems nevertheless to strengthen the idea of establishing an obligation of advance collaboration and negotiation of the rights of reproduction and/or communication to the public of protected works with the copyright holders or the assignees, linked to which is the implementation of systems to verify information uploaded and made accessible on platforms. This, in a

certain sense leaves a complementary role to remedies in a specific and subsequent form such as injunctive measures or notice and take down procedures[27].

This legal policy option underpins a different classification of service providers from a legal-economical point of view: the rules of provider responsibility (or lack of) introduced between the end of the last century and the beginning of the new millennium are based on the need to incentivize the growth of information society services [44]; [45]; [46]; [47].

In this context, the construction of the new EU copyright seems to be based on the awareness of the existence of entrepreneurial positions (often a form of monopoly) that reach across different sectors of the culture industry previously managed exclusively by the traditional media, with the consequent imposition of 'costs' – in the case of copyright in the form of preventive obligations for the control and/or payment of fair remuneration – aimed at redistributing in part the wealth produced by the activity of intermediation and aggregation of contents, as well as allocating more efficiently the 'anonymous harm' resulting from the inherent difficulty on the Internet of attributing the responsibility of the illegal conduct directly to the true author.

It should also be noted that the interpretative trends described (especially in *GS Media* case, but also with reference to Article 13 of the Proposal) here consolidate the emergence of the hybrid figure of the so-called prosumer, obliterating the theories that see the user as a mere (non-paying) exploiter of data flows and leaving space to a vision that takes into due consideration the economic value of the inputs produced and supplied to providers from each access to or by surfing the Internet[28].

5. The Intersection Between the Personal and the Economic Dimension of Data

The profile analysed before is worthy of further consideration, before coming to some brief conclusions.

The Web 2.0 user does not play a solely passive role as a user of the services and content offered by providers, but is induced to implement data assets that circulates on the Internet primarily through the non-pecuniary exchange represented by their personal data, captured by the providers both on the open platforms (for example with cookies) and on closed ones, subject to a registration process which has a para-contractual nature.

Confirmation of this point emerges from the contribution of the legal formants of some Member States[29] and also from some legislative proposals that tend to evaluate some types of personal (and non personal) data produced by users as a form of payment[30]. In this way, we would recognize an exquisitely consumeristic scope of protection for a basic level of legal relations hitherto inadequately highlighted since masked behind the paradigm of free services[31].

This tendency – aimed at protecting the user's freedom of access to information also as an incentive to a 'participatory exploitation' of services [48] – seems to be implicitly confirmed by the results of the *GS Media* case, in which the user's position with respect to a violation of the copyright that occurred through the posting of a link to a third content is firstly protected by a presumption of not-awarness.

Instead, concerning the phase for calculating the possible sum of money due for compensation purposes – which is an essential step for assessing the concrete scope of a liability rule, it seems appropriate to outline three different trends, which are interrelated:

a) the importance and the topical nature of the specific redress remedy as a complementary measure to compensation, "where this is wholly or partially possible" (as envisaged for example in Italy by Article 2058 of the Civil Code)[32];
b) given the inherent nature of the process of data circulation, Tort liability is understood primarily as a tool for parcelling and controlling the duties of care on the Internet among all the subjects involved in various ways in the flow of information[33];
c) taking into consideration what is stated in *a*) and *b*) above, the phase of the computation of the sum due as compensation is closely linked to the importance of compliance with and prompt activation of the remedial measures, in accordance with the principle of non-excessive burdens for the debtor. The remaining sum must then be calculated in relation to variable parameters, for example depending on the type of information that is the subject of the harm and the nature of the damage suffered: whilst, on the one hand, the criterion of the 'price of consent' appears progressively to extend from IP rights to other spheres which by tradition are defined as highly personal [49]; [50], such as the right to personal identity and digital privacy, on the other hand the liquidation of non-pecuniary loss seems to preserve its deterrent-sanctioning dimension, balanced by a more rigorous system of evidence on the injured party.

6. Concluding Remarks

Coming to the first (and partial) conclusions, the relationship between digital information and the user on the Internet is distinguished by the particular degree of complexity, moving it away from the traditional models.

From the first point of view, all the parties (be they legal, physical persons or else robots – even though currently not assigned with their own personality by the legal system[34], have the ability/duty to come into contact with the data according to a principle of 'digital solidarity'[35], ensuring that the flow of information is constant and that it is promptly corrected either as a precautionary or as a subsequent measure depending on supervision standards that vary according to the degree of proximity.

The owner of the right does not have an exclusive hold over the 'good' (whether it is the subject of a copyright or a right of the personality which is consolidated in their digital identity [51]; [52]; [53]), but releases this good into the information flow reserving for him/herself the right to observe the compliant use and the recognition of a flat-rate compensation fee that 'perceives' and 'spends' in the context of the permanence of the technical-informational ecosystem in either a contractual manner (e.g. through signing up for social media services and access to content available on this) or in an Aquilian manner (constituting harmful conduct).

The distinction between property rules and liability rules seems finally to fade, merging into a single remedial system. The elements collected so far propose in fact the image of a 'weakened' property rule in terms of scope and effectiveness (the remedy operate on a material level of the conduct and on the availability of unlawful data, but do not favour a negotiation based on the real value that the holder attributes to the right that is violated) and 'disguised' by a liability rule that by nature and entity is basically pre-established.

If we want to go further, the progressive 'codification' of online interactions (think e.g. of the advent of the blockchain technology) could open up the scenario of a definitive

reduction in the para-contractual logic of relationships, especially in the cases in which they constitute pecuniary loss. The violation of the duties of supervision divided *pro quota* among the parties involved in the information flow may in fact lead, in a future of digital relations, to the automatic transfer of a sum of money (therefore connected to strict or aggravated liability), understood as an indemnity that integrates the effectiveness of remedies able to interrupt and eliminate the harm.

Given the progressive osmosis between private enforcement and judicial system, the notion of 'harm' appears ultimately to be represented as the phenomenon of the initial or repeated circulation of inaccurate or unauthorized information, in some way merging the specific redress functions (aimed at the fulfillment of subjective situations or to prevent the violation, almost entirely delegated to the intervention of providers and users) with those of a compensatory form (aimed at removing and repairing 'harm'). This scenario could for example obliterate one important goal attributed to Tort Law, that is the deterrence function [54]; [55] and more in general imposes a radical reflection on the consequences of the 'datafication', in the perspective of the progressive automation of all type of relationship (e.g.: human-human, human-machine, machine-machine, human-robot etc.).

Endnotes

[1]According to Wiener [16], p. 28, 40: "As we have said, nature's statistical tendency to disorder, the tendency for entropy to increase in isolated systems, is expressed in the second law of thermodynamics. We as human beings, are not isolated systems. (...) As entropy increases, the universe, and all closed systems in the universe, tend naturally to deteriorate and lose their distinctiveness, to move from the least to the most probable state, from a state of organization and differentiation in which distinctions and forms exist, to a state of chaos and sameness. In Gibbs' universe order is least probable, chaos most probable. But while the universe as a whole, tends to run down, there are local enclaves of whose direction seems opposed to that of the universe at large and in which there is a limited and temporary tendency for organization to increase. Life finds its home in these enclaves. It is with this point of view at its core that the new science of Cybernetics began its development".

[2]According to [19]: "In a system that includes communications, one usually draws a modular boundary around the communication subsystem and defines a firm interface between it and the rest of the system. When doing so, it becomes apparent that there is a list of functions each of which might be implemented in any of several ways: by the communication subsystem, by its client, as a joint venture, or perhaps redundantly, each doing its own version. In reasoning about this choice, the requirements of the application provide the basis for a class of arguments, which go as follows: The function in question can completely and correctly be implemented only with the knowledge and help of the application standing at the end points of the communication system".

[3]See [16], p. 26: "It is my thesis that the physical functioning of the living individual and the operation of some of the newer communication machines are precisely parallel in their analogous attempts to control entropy through feedback. Both of them have sensory receptors as one stage in their cycle of operation: that is, in both of them there exists a special apparatus for collecting information from the outer world at low energy levels, and for making it available in the operation of the individual or of the machine. In both cases these external messages are not taken neat, but through the internal transforming powers of the apparatus, whether it be alive or dead. The information is then turned into a new form available for the further stages of performance. In both the animal and the machine this performance is made to be effective on the outer world. In both of them, their performed action on the outer world, and not merely their intended action, is reported back to the central regulatory apparatus. This complex of behavior is ignored by the average man, and in particular does not play the role that it should in our habitual analysis of society; for just as individual physical responses may be seen from this point of view, so may the organic responses of society itself. I do not mean that the sociologist is unaware of the existence and complex nature of communications in society, but until recently he has tended to overlook the extent to which they are the cement which binds its fabric together".

[4] *Ibidem*, p. 31: "Just as entropy is a measure of disorganization, the information carried by a set of messages is a measure of organization. In fact, it is possible to interpret the information carried by a message as essentially the negative of its entropy, and the negative logarithm of its probability. That is, the more probable the message, the less information it gives. Cliches, for example, are less illuminating than great poems".

[5] According to [12], p. 130: "*Nous venons de dire que la Technique produit au profit de l'homme des compensations aux inconvénients, qu'elle se produit pour elle-même des facilitations, et peut changer de caractère (décentralisation) cependant, il apparaît de plus en plus que ce système ne possède actuellement pas une des caractéristiques considérées généralement comme essentielle pour un système: le feedback, la rétroaction c'est-à-dire, rappelons-le d'un mot, ce mécanisme qui intervient lors- qu'un ensemble, un système en mouvement commet une erreur dans son fonctionnement, pour rectifier cette erreur mais en agissant à la source, à l'origine du mouvement. Il n'y a pas 'réparation' de l'erreur commise, il y a reprise du mouvement à son origine en modifiant une donnée du système. Le feedback n'existe pas seulement dans les systèmes mécaniques, artificiels, mais aussi dans les systèmes biologiques ou écologiques. Il implique un contrôle des résultats suivi d'une rectification du processus lorsque les résultats contrôlés sont nocifs ou insatisfaisants. Ainsi le système technique ne tend pas à se modifier lui même lorsqu'il développe des encombrements, des nuisances, etc., il est livré à une croissance pure, dès lors ce système provoque un accroissement des irrationalités, et d'autre part, il est d'une lourdeur et d'une viscosité considérable: lorsque l'on constate des désordres et des irrationalités, cela n'entraîne rien que des processus compensatoires. Le système continue à évoluer dans sa propre ligne*".

[6] BGH, 28 July 2015 - VI ZR 340/14. *Il Diritto dell'informazione e dell'informatica*, 2, 2016, 292, translation and comments by G. Eramo Puoti. On this matter, see also [56]; [57].

[7] See e.g. BGH, 12 May 2010 - I ZR 121/08, in *MIR*, 6, 2010; for further remarks [58]; [59]; [60].

[8] See e.g. the contribution of the European Court of Human Rights: ECtHR, Application no. 64569/09, Judgement 16 June 2015, *Delfi AS v. Estonia*; ECtHR, Application no. 22947/13, Judgement 2 May 2016, *Magyar Tartalomszolgáltatók Egyesülete and Index.hu Zrt v. Hungary*.

[9] EU Commission, *Tackling Illegal Content Online. Towards an Enhanced Responsibility of Online Platforms*, 28-09-2017, COM(2017) 555 final; Commission Recommendation (EU) 2018/334 of 1 March 2018 on measures to effectively tackle illegal content online, in OJ L 63/50. 6.3.2018.

[10] In 2016, four of the leading Web 2.0 service providers (Facebook, Twitter, YouTube and Microsoft, to which Instagram was added) in fact signed the Code of Conduct on countering illegal online hate speech, promoted by the Commission and non-governmental bodies, implementing measures for receiving and screening reports on contents non-compliant with the Framework Decision 2008/913/JHA of 28 November 2008, on combating certain forms and expressions of racism and xenophobia through the use of criminal law. In almost two years of implementation of the Code, the providers have intervened in the majority of cases removing the contents deemed unlawful under the Framework Decision and/or the laws of the Member States within 24 hours (about 70% of the reported contents).

[11] This reference is above all to Directive 2011/93/EU on the removal of child pornography websites or to Directive 2017/541 concerning the online contents that constitute incitement to carrying out crimes of terrorism.

[12] Commission Recommendation (EU) 2018/334 of 1 March 2018 on measures to effectively tackle illegal content online, cit., recitals no. 25 and 26: "In addition to notice-and-action mechanisms, proportionate and specific proactive measures taken voluntarily by hosting service providers, including by using automated means in certain cases, can also be an important element in tackling illegal content online, without prejudice to Article 15(1) of Directive 2000/31/EC. In connection to such proactive measures, account should be taken of the situation of hosting service providers which, because of their size or the scale on which they operate, have only limited resources and expertise and of the need for effective and appropriate safeguards accompanying such measures. It can, in particular, be appropriate to take such proactive measures where the illegal character of the content has already been established or where the type of content is such that contextualisation is not essential. It can also depend on the nature, scale and purpose of the envisaged measures, the type of content at issue, on whether the content has been notified by law enforcement authorities or Europol and on whether action had already been taken in respect of the content because it is considered to be illegal content. With regard to child sexual abuse material in particular, hosting service providers should take proactive measures to detect and prevent the dissemination of such material, in line with the commitments undertaken in the context of the Global Alliance against Child Sexual Abuse Online". These preventive obligations are therefore placed within the scope of applicability of Recital no. 48, Directive 2000/31/EC, being able to affect the safe harbor of the provider in the event of failure to intervene. On the one hand, in fact, the Commission excludes that by adopting these measures, the provider can be automatically be placed alongside the active hosting providers. (EU Commission, *Tackling Illegal Content Online*, cit., 12: "the mere fact that an online platform takes certain

measures relating to the provision of its services in a general manner does not necessarily mean that it plays an active role in respect of the individual content items it stores and that the online platform cannot benefit from the liability exemption for that reason"). On the other hand, it states that the platform, once aware of the illegality of the content during the course of preventive control activities, could lose its immunity if it does not act promptly to remove or disable access to illicit information (*Ibidem*, 13: "It follows that proactive measures taken by an online platform to detect and remove illegal content may result in that platform obtaining knowledge or awareness of illegal activities or illegal information, which could thus lead to the loss of the liability exemption in accordance with point (a) of Article 14(1) of the E-Commerce Directive. However, in such cases the online platform continues to have the possibility to act expeditiously to remove or to disable access to the information in question upon obtaining such knowledge or awareness. Where it does so, the online platform continues to benefit from the liability exemption pursuant to point (b) of Article 14(1). Therefore, concerns related to losing the benefit of the liability exemption should not deter or preclude the application of the effective proactive voluntary measures that this Communication seeks to encourage").

[13]EU Commission, *Tackling Illegal Content Online*, cit., 8: "Given that fast removal of illegal material is often essential in order to limit wider dissemination and harm, online platforms should also be able to take swift decisions as regards possible actions with respect to illegal content online without being required to do so on the basis of a court order or administrative decision, especially where a law enforcement authority identifies and informs them of allegedly illegal content. At the same time, online platforms should put in place adequate safeguards when giving effect to their responsibilities in this regard, in order to guarantee users' right of effective remedy".

[14]According to Article 4, no. 2) of GDPR, 'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction".

[15]CJEU, grand chamber, 13 May 2014, C-131/12, *Google Spain, Google Inc. v. AEPD, Costeja González.*

[16]See TGI Paris, 24 November and 19 December 2014, Marie-France M. v. Google France e Google Inc. *Il Diritto dell'informazione e dell'informatica*, 2015, 532; Trib. Roma, 3 December 2015, X v. Google Inc., *ivi*, 2016, 266; Sala de lo Contencioso-administrativo de la Audiencia Nacional, 29 December 2014, no. ric. 725/2010, 18 persone v. Google Spain e Google Inc., www.poderjudicial.es.

[17]Similarly, Article 19 GDPR on 'Notification obligation regarding rectification or erasure of personal data or restriction of processing' states that: "The controller shall communicate any rectification or erasure of personal data or restriction of processing carried out in accordance with Article 16, Article 17(1) and Article 18 to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The controller shall inform the data subject about those recipients if the data subject requests it".

[18]CJEU, grand chamber, 5 June 2018, C-210/16, *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v. Wirtschaftsakademie Schleswig-Holstein GmbH*, paras. 33-43: "(...) Moreover, other entities such as Facebook partners or even third parties 'may use cookies on the Facebook services to provide services [directly to that social network] and the businesses that advertise on Facebook'. That processing of personal data is intended in particular to enable Facebook to improve its system of advertising transmitted via its network, and to enable the fan page administrator to obtain statistics produced by Facebook from the visits to the page, for the purposes of managing the promotion of its activity, making it aware, for example, of the profile of the visitors who like its fan page or use its applications, so that it can offer them more relevant content and develop functionalities likely to be of more interest to them. While the mere fact of making use of a social network such as Facebook does not make a Facebook user a controller jointly responsible for the processing of personal data by that network, it must be stated, on the other hand, that the administrator of a fan page hosted on Facebook, by creating such a page, gives Facebook the opportunity to place cookies on the computer or other device of a person visiting its fan page, whether or not that person has a Facebook account. (...) In those circumstances, the administrator of a fan page hosted on Facebook, such as Wirtschaftsakademie, must be regarded as taking part, by its definition of parameters depending in particular on its target audience and the objectives of managing and promoting its activities, in the determination of the purposes and means of processing the personal data of the visitors to its fan page. The administrator must therefore be categorised, in the present case, as a controller responsible for that processing within the European Union, jointly with Facebook Ireland, within the meaning of Article 2(d) of Directive 95/46. (...) In those circumstances, the recognition of joint responsibility of the operator of the social network and the administrator of a fan page hosted on that network in relation to the process-

ing of the personal data of visitors to that page contributes to ensuring more complete protection of the rights of persons visiting a fan page, in accordance with the requirements of Directive 95/46. However, it should be pointed out (. . .) that the existence of joint responsibility does not necessarily imply equal responsibility of the various operators involved in the processing of personal data. On the contrary, those operators may be involved at different stages of that processing of personal data and to different degrees, so that the level of responsibility of each of them must be assessed with regard to all the relevant circumstances of the particular case".

[19]CJEU, 8 September 2016, C-160/15, *GS Media BV v. Sanoma Media Netherlands BV, Playboy Enterprises International Inc., Britt Geertruida Dekker*, in particular paras. 45 and 54.

[20]CJEU, C-160/15, cit., par. 50.

[21]CJEU, grand chamber, 4 October 2011, C-429/08, C-403/08 and C-429/08, *Football Association Premier League Ltd. and others*.

[22]CJEU, 26 April 2017, C-527/15, *Stichting Brein v. Jack Frederik Wullems*.

[23]CJEU, 14 June 2017, C-610/15, *Stichting Brein v. Ziggo BV, XS4ALL Internet BV, (Stichting Brein II)*.

[24]COM(2016) 593 final.

[25]See Recital no. 37a: "Certain information society services, as part of their normal use, are designed to give access to the public to copyright protected content or other subject-matter uploaded by their users. The definition of an online content sharing service provider under this Directive shall cover information society service providers one of the main purposes of which is to store and give access to the public or to stream significant amounts of copyright protected content uploaded / made available by its users, and that optimise content, and promote for profit making purposes, including amongst others displaying, tagging, curating, sequencing, the uploaded works or other subject-matter, irrespective of the means used therefor, and therefore act in an active way. As a consequence, they cannot benefit from the liability exemption provided for in Article 14 of Directive 2000/31/EC. The definition of online content sharing service providers under this Directive does not cover microenterprises and small sized enterprises within the meaning of Title I of the Annex to Commission Recommendation 2003/361/EC and service providers that act in a non- commercial purpose capacity such as online encyclopaedia, and providers of other subject-matter are used as well as their possibilities to get an appropriate remuneration for it, since some user uploaded content services do not enter into licensing agreements on the basis that they claim to be covered by the 'safe-harbour' exemption set out in Directive 2000/31/EC".

[26]Article 13, on the 'Use of protected content by online content sharing service providers storing and giving access to large amounts of works and other subject-matter uploaded by their users': "Without prejudice to Article 3(1) and (2) of Directive 2001/29/EC, online content sharing service providers perform an act of communication to the public. They shall therefore conclude fair and appropriate licensing agreements with right holders".

[27]See *Commission Staff Working Document Impact Assessment on the Modernisation of EU Copyright Rules*, cit., 147: "The above obligations will be without prejudice to liability regimes applicable to copyright infringements and the application of Article 14 ECD. In particular, with regard to services that are covered by Article 14 ECD, the obligation to put in place content identification technologies would not take away the safe harbour provided that the conditions of Article 14 are fulfilled. The notice and takedown regime will continue to apply for hosting service providers covered by Article 14 with respect to content not covered by agreements or in cases where the content is not properly identified". For a first opinion on the matter see [61].

[28]The spread of the social networks and the advent of other types of platforms that help the users in their search for websites, goods or other services – the quality of which is dependent on their collaborative nature – must be linked to a phenomenon of concentration of market power (which, in short, distinguishes every 'cycle' in the history of mass communication means), posing a series of problems of political and regulatory nature: on this matter see [62]; [63]; [64]; [65]; [66]; [67]; [68].

[29]See e.g. Italian Antitrust Authority, 12 May 2017, cases no. PS10601 and CV154, WhatsApp. *Il Diritto dell'informazione e dell'informatica*, 2, 2017, 390; KG Berlin, 8 April 2016, in *Multimedia und Recht*, 2016, 601.

[30]See the *Proposal for a Directive of the European Parliament and of the Council on certain aspects concerning contracts for the supply of digital content*, COM(2015) 634 final. On this matter see [69]; [70]; [71]; [72]; [73].

[31]Should the aforementioned draft law enter into force, it appears that would in any case be applied in a subsidiary or supplementary way, always within the respect for the general principles for the protection of personal data, such as those regarding the revocability of the consent of the data subject: see e.g. Recital no. 11, Directive 2011/83/UE on consumer rights: "This Directive should be without prejudice to Union provisions relating to specific sectors, such as medicinal products for human use, medical devices, privacy and electronic

communications, patients' rights in crossborder healthcare, food labelling and the internal market for electricity and natural gas".

[32]"The injured party can demand specific redress when this is wholly or partially possible. The court, however, can order that the redress be made only by providing an equivalent, if specific redress would prove to be excessively onerous for the debtor". On the matter see [74]; [75]; [76]; [77].

[33]On the goals of effective prevention connected to Tort Law system see [78].

[34]Frosini [79], p. 111, considers a robot endowed with artificial intelligence as a moral subject, in conflict between inner consciousness (characteristic of man born from ζωή) and outer consciousness (technical upgrading of the first). See also [80]; [81]; [82]; [83].

[35]Following this reasoning, we could add also a different definition of the cooperative approach to this inclusive sense of digital solidarity, stemming from the right to access and communicate online. In other words, to the concept of 'computer freedom' identified first by Vittorio Frosini [84], we can add the notion of 'online' or 'digital' solidarity, by which the transit of legal information from one area of the Internet to another leads to an increase in the overall value of the system and therefore of its functioning and the beneficial effects that it can have on society. On the concept of solidarity in the changed technological and social model, see [85], p. 115, in which this inclusive nature is highlighted in the context of the advent of new relational goods and the redistribution of power; in argument see also [86].

References

[1] Branscomb, A. W. (1995). Anonymity, Autonomy, and Accountability: Challenges to the First Amendment in Cyberspaces. *The Yale Law Journal, 104*(7), 1639-1679.

[2] Nicoll, C., Prins, J. E. J. & van Dellen, M. J. M. (Eds.) (2003). *Digital Anonymity and the Law*. TMC Asser Press, xiv+307.

[3] Posner, R. A. (2008). Privacy, Surveillance, and Law. *University of Chicago Law Review, 75*, 245.

[4] Krausova, A. (2008). Identification in Cyberspace. *Masaryk University Journal of Law and Technology, 2*, 83.

[5] Choi, B. H. (2012). The anonymous internet. *Maryland Law Review, 72*, 501.

[6] Zeno-Zencovich, V. (2014). Anonymous Speech on the Internet. In Koltay, A. (Ed.). *Media Freedom and Regulation in the New Media World*, 103-116.

[7] Finocchiaro, G. (2010). Anonimato. *Digesto delle Discipline Privatistiche–Sezione Civile. Aggiornamento*. UTET, 12-20.

[8] Codiglione, G. G. (2013). Indirizzo IP, Reti Wi-Fi e responsabilità per illeciti commessi da terzi. *Il Diritto dell'informazione e dell'informatica, 29*(1), 107-143.

[9] Resta, G. (2014). Anonimato, responsabilità, identificazione: prospettive di diritto comparato. *Il Diritto dell'informazione e dell'informatica, 30*(2), 171-205.

[10] Floridi, L. (2014). *The Fourth Revolution: How the Infosphere Is Reshaping Human Reality*. Oxford University Press.

[11] Baudrillard, J. (1968). *Les système des objects*. Denoël-Gonthier.

[12] Ellul, J. (1977). *Le Système technicien*. Calmann-Lévy, 138.

[13] Ferraris, M. (2014). *Documentalità: perché è necessario lasciar tracce*. Laterza.

[14] Lessig, L. (2006). *Code: version 2.0*. New York.

[15] Glenn, H. P. (2014). *Legal Traditions of the World: Sustainable Diversity in Law*. Oxford University Press.

[16] Wiener, N. (1954). *The Human Use of Human Beings: Cybernetics and Society*. Anchor.

[17] Licklider, J. C. R. (1963). *Memorandum for Members and Affiliates of the Intergalactic Computer Network*, April 23.

[18] Baran, P. (1964). On Distributed Communications Networks. *IEEE Transactions on Communications Systems, 12*(1), 1-9.

[19] Saltzer, J. H., Reed, D. P. & Clark, D. D. (1984). End-to-end Arguments in System Design. *Technology, 100*, 0661.

[20] Nef, J. U. (1958). *Cultural Foundations of Industrial Civilization*. CUP Archive.

[21] Ellul, J. (1954). *La technique ou l'enjeu du siècle*. Armand Colin.

[22] Irti, N. (2013). *L'uso giuridico della natura*. Laterza.

[23] Irti, N. (2014). *Nichilismo giuridico*. Laterza.

[24] Rodotà, S. (2018). *Vivere la democrazia*, Laterza, 17.
[25] Samuelson, P. A. (1954). The Pure Theory of Public Expenditure. *The Review of Economics and Statistics*, 387-389.
[26] Arrow, K. J. (1962). Economic Welfare and The Allocation of Resources for Invention. *The Rate and Direction of Inventive Activity*. Princeton University Press and NBER.
[27] Stiglitz, J. E. (2002). Information and the Change in the Paradigm in Economics. *American Economic Review, 92*(3), 460-501.
[28] Zeno-Zencovich, V. (1993). Informazione (profili civilistici). *Digesto delle Discipline Privatistiche*. UTET, 420.
[29] Pardolesi, R. & Motti, C. (1991). L'informazione come bene. In De Nova, G., Inzitari, B., Tremonti, G. & Visentini, G. (Eds.). *Dalle res alle new properties*. Giuffrè, 37.
[30] Giannone Codiglione, G. (2015). Libertà d'impresa, concorrenza e neutralità della rete nel mercato transnazionale dei dati personali. *Il Diritto dell'informazione e dell'informatica*, 905.
[31] Zeno-Zencovich, V. & Giannone Codiglione, G. (2016). Ten Legal Perspectives on the "Big Data Revolution". *Concorrenza e mercato, 23*, 29-57.
[32] Lipari, N. (2013). *Le categorie del diritto civile*. Giuffrè, 125.
[33] Calabresi, G. & Melamed, A. D. (1972). Property Rules, Liability Rules, and Inalienability: One View of the Cathedral. *Harvard Law Review, 85*, 1089-1128.
[34] Sica, S. & Giannone Codiglione, G. (Eds.) (2018). *Security and Hate Speech. Personal Safety and Data Security in the Age of Social Media*. Il Mulino.
[35] Sartor, G. (2017). *Providers Liability: From the eCommerce Directive to the Future*.
[36] Resta, G. (2007). Identità personale ed identità digitale. *Il Diritto dell'informazione e dell'informatica, 3*, 511 ff.
[37] Di Majo, A. (1999). Il trattamento dei dati personali tra diritto sostanziale e modelli di tutela. In Cuffaro, V., Ricciuto, V. & Zeno-Zencovich, V. (Eds.). *Trattamento dei dati e tutela della persona*. Giuffrè, 225.
[38] Sica, S., D'Antonio, V. & Riccio, G. M. (Eds.) (2016). *La nuova disciplina europea della privacy*. Cedam, 55.
[39] Ghidini, G. (2018). *Rethinking Intellectual Property: Balancing Conflicts of Interest in the Constitutional Paradigm*. Edward Elgar Publishing.
[40] Moscati, L. (2017). Sfide tecnologiche e diritto d'autore tra riferimenti storici e direttive europee. *Rivista italiana di scienze giuridiche*, 443.
[41] Giannone Codiglione, G. (2017). *Opere dell'ingegno e modelli di tutela. Regole proprietarie e soluzioni convenzionali*. Giappichelli.
[42] Giannone Codiglione, G. (2017). I motori di ricerca. *Annali italiani del diritto d'autore, della cultura e dello spettacolo*, 395.
[43] Riccio, G. M. & Giannone Codiglione, G. (2018). Ancillary Copyright and Liability of Intermediaries in the EU Directive Proposal on Copyright. *Comparazione e diritto civile*.
[44] Yen, A. C. (1999). Internet Service Provider Liability for Subscriber Copyright Infringement, Enterprise Libility, and the First Amendment. *Georgetown Law Journal, 88*, 1833.
[45] Scruers, M. (2002). The History and Economics of ISP Liability for Third Party Content. *Virginia Law Review, 88*, 205.
[46] Landes, W. & Lichtman, D. (2003). Indirect Liability for Copyright Infringement: An Economic Perspective. *J.M. Olin Law & Economics Working Paper no. 179 (2nd series)*. Chicago.
[47] Riccio, G. M. (2002). *La responsabilità civile degli internet providers*. Giappichelli.
[48] Lanier, J. (2014). *Who Owns the Future?* Simon and Schuster.
[49] Mezzanotte, F. (2017). Access to Data: The Role of Consent and the Licensing Scheme. In Lohsse, S., Schulze, R. & Staudenmayer, D. (Eds.). *Trading Data in the Digital Economy: Legal Concepts and Tools*. Nomos, 159-187.
[50] Bergé, J. S., Grumbach, S. & Zeno-Zencovich, V. (2018). The 'Datasphere', Data Flows beyond Control, and the Challenges for Law and Governance. *European Journal of Comparative Law and Governance, 5*(2), 144-178.
[51] Zeno-Zencovich, V. (1993). Identità personale. *Digesto delle Discipline Privatistiche*. UTET, 294.
[52] Finocchiaro, G. (2010). Identità personale (diritto alla). *Digesto delle Discipline Privatistiche*. UTET, 721.
[53] Resta, G. (2011). The New Frontiers of Personality Rights and the Problem of Commodification: European and Comparative Perspectives. *Tulane European and Civil Law Forum, 26*, 33.

[54] Calabresi, G. (1970). *The Costs of Accidents: A Legal and Economic Analysis*. Yale University Press.
[55] Ponzanelli, G. (1992). *La responsabilità civile. Profili di diritto comparato*. Il Mulino.
[56] Peifer, K. N. (2016). Beseitigungsansprüche im digitalen Äußerungsrecht-Ausweitung der Pflichten des Erstverbreiters. *Neue Juristische Wochenschrift*, 23-25.
[57] Spindler, G. (2012). Persönlichkeitsschutz im Internet-Anforderungen und Grenzen einer Regulierung. In Gutachten, F. (Ed.). *Ständige deputation des Deutschen Juristentages Verhandlungen des 69*. Beck.
[58] Hartmann, A. (2009). *Unterlassungsansprüche im Internet: Störerhaftung für nutzergenerierte Inhalte*. Beck, Vol. 75.
[59] Neuhaus, S. (2011). *Sekundäre Haftung im Lauterkeits-und Immaterialgüterrecht: dogmatische Grundlagen und Leitlinien zur Ermittlung von Prüfungspflichten*. Mohr Siebeck, Vol. 50.
[60] Leistner, M. (2012). Common Principles of Secondary Liability? *Common Principles of European Intellectual Property Law*, 117-146.
[61] Angelopoulos, C. (2017). *On Online Platforms and the Commission's New Proposal for a Directive on Copyright in the Digital Single Market*, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2947800.
[62] Wu, T. (2010). *The Master Switch: The Rise and Fall of Information Empires*. Vintage.
[63] Gorz, A. (2003). *L'immatériel: connaissance, valeur et capital*. Ed. Galilée.
[64] Cairncross, F. (1997). *The Death of Distance: How the Communications Evolution Will Change Our Lives*. Harvard Business School Press.
[65] Ryan, J. (2010). *A History of the Internet and the Digital Future*. Reaktion Books.
[66] Rifkin, J. (2014). *The Zero Marginal Cost Society: The Internet of Things, the Collaborative Commons, and the Eclipse of Capitalism*. Macmillan.
[67] Zeno-Zencovich, V. & Mezzanotte, F. (2008). Le reti della conoscenza: dall'economia al diritto. *Il Diritto dell'informazione e dell'informatica*, 2, 141.
[68] De Franceschi, A. & Lehmann, M. (2015). Data As Tradeable Commodity and New Measures for Their Protection. *Italian Law Journal*, 1, 51.
[69] Resta, G. & Zeno-Zencovich, V. (2018). Volontà e consenso nella fruizione dei servizi in rete. *Rivista trimestrale di diritto e procedura civile*, 2, 411.
[70] Langhanke, C. & Schmidt-Kessel, M. (2015). Consumer Data as Consideration. *Journal of European Consumer and Market Law, 4*(6), 218-223.
[71] Twigg-Flesner, C. (2016). Disruptive Technology – Disruptive Law? In De Franceschi, A. (Ed.). *European Contract Law and the Digital Single Market*. Intersentia, 21, 40.
[72] Metzger, A. (2017). Data As Counter-Performance: What Rights and Duties for Parties Have. *Journal of Intellectual Property, Information Technology and Electronic Commerce Law, 8*, 2.
[73] Zeno-Zencovich, V. (1993). Profili negoziali degli attributi della personalità. *Il Diritto dell'informazione e dell'informatica*, 3, 545.
[74] Salvi, C. (2005). *La responsabilità civile*. Giuffrè, 250.
[75] Di Majo, A. (2003). *Problemi e metodi del diritto civile. 3. La tutela civile dei diritti*. Giuffrè, 261.
[76] Marella, M. R. (2000). *La riparazione del danno in forma specifica*. Cedam.
[77] Stoll, H. (1972). Consequences of Liability: Remedies. In Tunc, A. (Ed.). *International Encyclopedia of Comparative Law*, Vol. XI.
[78] Monateri, P. G. (2013). La natura del 'politico' e il 'problema' della responsabilità civile. In Alpa, G. & Roppo, V. (Eds.). *La vocazione civile del giurista: saggi dedicati a Stefano Rodotà*. Laterza, 243.
[79] Frosini, V. (1968). *Cibernetica diritto e società*. Edizioni di comunità, 111.
[80] Solum, L. B. (1991). Legal Personhood for Artificial Intelligences. *The North Carolina Law Review, 70*, 1231.
[81] Teubner, G. (2007). *Rights of Non-humans? Electronic Agents and Animals As New Actors in Politics and Law*. Max Weber Lecture No. 4.
[82] Rodotà, S. (2012). *Il diritto di avere diritti*. Laterza, 312, 341.
[83] Sartor, G. (2009). Cognitive Automata and the Law: Electronic Contracting and the Intentionality of Software Agents. *Artificial Intelligence and Law, 17*(4), 253.
[84] Frosini, V. (1984). 1984: L'informatica nella società contemporanea. *Informatica e diritto*, 3, 7-15.
[85] Rodotà, S. (2014). *Solidarietà*. Laterza, 115.
[86] Sunstein, C. R. & Ullmann-Margalit, E. (2001). Solidarity Goods. *Journal of Political Philosophy, 9*(2), 129-149.