Algorithmic Security: Issues and Policy Outlook

Marialuisa Gambini*

Abstract

The subject of the paper is security in the field of intelligent robotics and algorithms. As there is currently no already existing legal framework, this paper takes as its point of departure an examination of regulatory solutions and application experience gained in the areas of information society services and automated processing of personal data, marked by the steady introduction of an articulated set of obligations with regard to security and controls incumbent on the protagonists of technological innovation. From a policy standpoint, the paper proposes the adoption of a similar approach informed by the principles of prevention and precaution while ensuring that constitutional values and the protection of the human person always remain a priority.

I. Issues

The new digital economy[1] is marked by the spread of algorithmic processing of data, which is of key importance in three main contexts.

Firstly, in the provision of information society services: think, for example, of algorithmic data processing underlying search engine services or the automated computational analysis of information in digital format underlying online content sharing services.

The second context concerns the applications of new forms of artificial intelligence and robotic technology, more or less autonomous, in the processes of the production of goods and supply of services. This is a sector in constant growth and has assumed a significant social function, which is more visible when robotics and artificial intelligence (AI) affect constitutionally protected rights such as, for example, the right to life and health of individuals (think of the development of healthcare robots, cases of use of surgical robots and the spread of self-driving cars, which will lead to a reduction in the number of accidents and increased road traffic safety). But it is also a feature of applications that affect the functioning of government or developed for industrial use, if one considers just the impact on

* Full Professor of Private Law, 'G. D'Annunzio' University of Chieti-Pescara.

[1] Data is the resource of the new digital economy: see 'The world's most valuable resource is no longer oil, but data' *The Economist* (2017). In doctrine, for all, see, V. Ricciuto, 'La patrimonializzazione dei dati personali. Contract and market in the reconstruction of the phenomenon', in V. Cuffaro et al eds, *I dati personali nel diritto europeo* (Torino: Giappichelli, 2019), 23.

administration and working conditions.

Finally, technological innovation implies and implements continuous algorithmic processing of personal data that now permeate the lives of individuals: car robots that record data that allow one to reconstruct the behaviour of users, robot-assistants that detect the emotions of the elderly, children or patients and digital home assistants that listen to our most intimate conversations.

In this articulated scenario there comes a need to minimise the social (and hence not only economic) costs of the damage stemming from the algorithmic processing of data, adopting policies of prevention and security and that empower the persons involved. The relevance of the question is all the more evident when one reflects on the fact that it transcends the dimension of the economic interests tied to the algorithmic processing of data to extend to values more closely connected to the freedoms and fundamental rights of the person that can be harmed, such as the security of individuals, their health, private life and the protection of personal data, integrity, dignity, self-determination and non-discrimination.

From the perspective described just now of key importance is the issue of security obligations and controls on algorithmic data processing, internal to the system so to speak, ie incumbent on the actors involved in the process of technological innovation and informed by the principles of prevention and precaution.[2] In other words, obligations and controls are aimed at reducing the risks associated with algorithmic data processing and the dangers (not always foreseeable) of damage that can flow therefrom for the fundamental rights and freedoms of individuals, irrepressible in a society inspired by increasingly intense safeguards in terms of solidarity and personalism.[3]

[2] As is well known, the principle of prevention operates in the case of a concrete and imminent danger (in this case, for the rights and freedoms of the interested parties, consequent to the processing of personal data) and translates, among other things, into the obligation to adopt the security and caution measures necessary to avoid the occurrence of the damage. The precautionary principle, on the other hand, originates from the acquired awareness that scientific knowledge is not able to determine with certainty the harmful consequences and risks connected to the exercise of certain activities (for example, consider a processing of personal data in which a new technology is used on a large scale). The doctrine has revealed how the rule of precaution is already inherent in the private discipline of civil liability, being now identified, from time to time, in the discipline of damage from dangerous activities as per Art 2050 Civil Code (U. Izzo, *La precauzione nella responsabilità civile: analisi di un concetto sul tema del danno da contagio per via trasfusionale* (Padova: CEDAM, 2007), 642; F. Santonastaso, 'Principio di «precauzione» e responsabilità d'impresa: rischio tecnologico e attività pericolosa «per sua natura». Prime riflessioni su un tema di ricerca' *Contratto e impresa/Europa*, 21 (2001)); now in the institution of culpability, understood, in particular, as qualified fault in relation to the conditions and capacity of the person acting as agent (C. Castronovo, 'Sentieri di responsabilità civile europea' *Europa e diritto privato*, 787 (2008). More generally, see the observations of E. Del Prato, 'Il principio di precauzione nel diritto privato: spunti' *Rassegna di diritto civile*, 634 (2009); L. Rossano, 'Principio di precauzione e attività d'impresa' *Rivista critica del diritto privato*, 65 (2016)).

[3] On this point, see, for all, P. Perlingieri, *Il diritto civile nella legalità costituzionale secondo il sistema italo-comunitario delle fonti* (Napoli: Edizioni Scientifiche Italiane, 3rd ed, 2006), 433; Id, *La personalità umana nell'ordinamento giuridico* (Camerino-Napoli: Edizioni Scientifiche Italiane, 1972), 133; Id, *La persona e i suoi diritti. Problemi del diritto civile* (Napoli: Edizioni

The study of the subject will start from a brief examination of the current Italian-European regulatory framework, in the specific sectors of the provision of information society services and automated processing of personal data which are – at present – those among the three mentioned above to have received express consideration by lawmakers. In those contexts, the attention paid to the particular impact of new technologies and their damaging potential has led to the creation of a solid network of internal controls, ie entrusted, respectively, to Internet service providers and those who engage in processing (data controllers and – in some limited cases – data processors). With regard to the still unregulated area of the artificial intelligence systems, it will be intended, subsequently, to verify, in a perspective *de iure condendo*, the practicability of an analogous approach inspired by the principles of prevention and precaution, always assuming as priority the constitutional values and the protection of the human person.

II. Controls and Security in Electronic Commerce Law

In Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, transposed in Italy with decreto legislativo 9 April 2003 no 70, the issue of security and internal controls is only marginally addressed and is connected to that of the civil liability of Internet service providers. In fact, the rules clearly exempt service providers from a general obligation to monitor the information which they transmit or store on the network and from a general obligation to actively seeks facts or circumstances indicating the presence of illegal activities (Arts 15 of Directive 2000/31/EC – Art 17 of decreto legislativo no 70/2003),[4] as such obligations are considered as imposing

Scientifiche Italiane, 2005); F. Parente, 'La persona e l'assetto delle tutele costituzionali', in P. Perlingieri ed, *Trattato di diritto civile del Consiglio Nazionale del Notariato* (Napoli: Edizioni Scientifiche Italiane, 2012), 14; according to Corte di Cassazione 16 October 2007 no 21748, *Diritto di famiglia e delle persone*, I, 107 (2008), with commentary by F. Gazzoni, 'Sancho Panza in Cassazione (come si riscrive la norma dell'eutanasia, in spregio al principio di divisione dei poteri)', the personalistic principle 'animates our Constitution, which sees in the human person an ethical value in itself, prohibits any exploitation of the same for any purpose heteronomous and absorbing, conceives the solidarity and social intervention in function of the person and his development and not vice versa, and looks to the limit of "respect for the human person" '; P. Perlingieri and P. Femia, 'Nozioni introduttive e principi fondamentali', in P. Perlingieri ed, *Manuale di diritto civile* (Napoli: Edizioni Scientifiche Italiane, 2017), 14, 18, recognize that the hierarchy of values does not contain the a priori solution of any possible conflict of interest, but it is certain that 'a balance that damages health to the benefit of the wealth of others is incorrect, because the situations of the person prevail over those of the heritage'.

[4] Art 15(1) of Directive 2000/31/EC (No general obligation to monitor) provides that: '1. Member States shall not impose a general obligation on providers, when providing the services covered by Arts 12, 13 and 14, to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity. 2. Member States may establish obligations for information society service providers promptly to inform the competent public authorities of alleged illegal activities undertaken or information provided by recipients of their service or obligations to communicate to the competent authorities, at their

an unrealistic burden from a technical and legal standpoint. This position was also formally confirmed recently by Directive 2019/790/EU on copyright and related rights in the single digital market, which specifies that the obligations imposed by the new legislation on providers of online content sharing services do not entail any general obligation to monitor the information stored.

The special rules on the civil liability of Internet service providers (Arts 12-14 of Directive 2000/31/EC – Arts 14-16 of decreto legislativo no 70/2003) are based on the principle of negligence[5] and call the various providers to account for the failure to comply with the duty of care[6] incumbent on the them as professional operators. A duty that is shaped and calibrated by law on the basis of the activity carried out (*mere conduit,*[7] *caching*[8] and *hosting*).[9] This has resulted in stringent

request, information enabling the identification of recipients of their service with whom they have storage agreements'.

[5] For a subjective type of connection criterion, the first commentators expressed as follows: among others, G. Ponzanelli, 'Verso un diritto uniforme per la responsabilità degli internet service providers' *Danno e responsabilità*, 10 (2002); V. Zeno-Zencovich, 'Profili attivi e passivi della responsabilità dell'utente in Internet', in A. Palazzo and U. Ruffolo eds, *La tutela del navigatore in Internet* (Milano: Giuffrè, 2002), 195 ,140; G.M. Riccio, *La responsabilità civile degli internet providers* (Torino: Giappichelli, 2002), 57; Id, 'La responsabilità civile degli Internet Providers alla luce della direttiva n. 2000/31/CE', in S. Sica and P. Stanzione eds, *Commercio elettronico e categorie civilistiche* (Milano: Giappichelli, 2002), 391; G. Giacobbe, 'La responsabilità civile per l'uso di Internet', in V. Ricciuto and N. Zorzi eds, *Il contratto telematico* (Padova: CEDAM, 2002), 222; F. Signorelli, 'Profili di responsabilità del provider nell'e-commerce', in V. Franceschelli ed, *Commercio elettronico* (Milano: Giuffrè, 2001), 570, 571; M. Astone, 'La responsabilità del prestatore di servizi della società di informazione nella direttiva 2000/31/CE' *Europa e diritto privato*, 446 (2002); A. Piazza, 'La responsabilità civile dell'Internet Provider' *Contratto e impresa*, 147 (2004). They speak of specific fault of the intermediary and that is of fault for violation of the law R. Bocchini, *La responsabilità civile degli intermediari del commercio elettronico. Contributo allo studio dell'illecito plurisoggettivo permanente* (Napoli: Edizioni Scientifiche Italiane, 2003), 13, 14; F. Di Ciommo, 'La responsabilità civile in Internet: prove di governo dell'anarchia tecnocratica' *Responsabilità civile*, 562 (2006); Id, *Evoluzione tecnologica e regole di responsabilità civile* (Napoli: Edizioni Scientifiche Italiane, 2003), 294, 295; L. Bugiolacchi, 'La responsabilità dell'host provider alla luce del d.lgs. n. 70/2003: esegesi di una disciplina "dimezzata"' *Responsabilità civile e previdenza*, 193 (2005). For the reference to the concept of professional negligence with particular regard to the provider's non-contractual liability, see M. Franzoni, 'Fatti illeciti. Art 2043, 2056-2059', in F. Galgano ed, *Commentario* al *codice civile Scialoja-Branca* (Bologna-Roma: Zanichelli, 2004), 169; M. Gambini, *Le responsabilità civili dell'Internet service provider* (Napoli: Edizioni Scientifiche Italiane, 2006), 333.

[6] For the extensive application of Art 1176 of the Civil Code also in matters of non-contractual offences: see L. Mengoni, 'Obbligazioni "di risultato" e obbligazioni "di mezzi" Studio critico' *Rivista di diritto commerciale*, I, 205 (1954); L. Corsaro, 'Colpa e responsabilità civile: l'evoluzione del sistema italiano' *Rassegna di diritto civile*, 298 (2000); A. Ravazzoni, 'Diligenza' *Enciclopedia giuridica Treccani* (Roma: Treccani, 1989), XI, 1; M. Bussani, *La colpa soggettiva. Modelli di valutazione della condotta nella responsabilità extracontrattuale* (Padova: CEDAM, 1991).

[7] Art 12 of Directive 2000/31/EC (Responsibility in the activity of simple transport –Mere conduit): '1. Where an information society service is provided that consists of the transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network, Member States shall ensure that the service provider is not liable for the information transmitted, on condition that the provider:

(a) does not initiate the transmission;

obligations to take action and cooperate with the courts or administrative supervisory authorities in tackling offences committed on the network.

These obligations imply a limited form of monitoring by the Internet operators on the information transmitted or stored, which are referred exclusively to the phase following the commission of the offences, ie when a violation is ascertained or at least presumed. This was stated in the first Supreme Court judgment in

(b) does not select the receiver of the transmission; and

(c) does not select or modify the information contained in the transmission.

2. The acts of transmission and of provision of access referred to in paragraph 1 include the automatic, intermediate and transient storage of the information transmitted in so far as this takes place for the sole purpose of carrying out the transmission in the communication network, and provided that the information is not stored for any period longer than is reasonably necessary for the transmission.

3. This Article shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement'. On the differences between the liability regime of the e-commerce directive for access providers and hosting providers, see European Court of Justice 15 September 2016, C-484/2014, *Repertorio del Foro italiano,* 2016, under voice *Unione europea*, no 1441).

[8] Art 13 of Directive 2000/31/EC (Responsibility for temporary storage activities – Caching): '1. Where an information society service is provided that consists of the transmission in a communication network of information provided by a recipient of the service, Member States shall ensure that the service provider is not liable for the automatic, intermediate and temporary storage of that information, performed for the sole purpose of making more efficient the information's onward transmission to other recipients of the service upon their request, on condition that:

(a) the provider does not modify the information;

(b) the provider complies with conditions on access to the information;

(c) the provider complies with rules regarding the updating of the information, specified in a manner widely recognised and used by industry;

(d) the provider does not interfere with the lawful use of technology, widely recognised and used by industry, to obtain data on the use of the information; and

(e) the provider acts expeditiously to remove or to disable access to the information it has stored upon obtaining actual knowledge of the fact that the information at the initial source of the transmission has been removed from the network, or access to it has been disabled, or that a court or an administrative authority has ordered such removal or disablement.

2. This Article shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement'.

[9] Art 14 of Directive 2000/31/EC (Responsibility for information storage activities – Hosting): '1. Where an information society service is provided that consists of the storage of information provided by a recipient of the service, Member States shall ensure that the service provider is not liable for the information stored at the request of a recipient of the service, on condition that:

(a) the provider does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent; or

(b) the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information.

2. Paragraph 1 shall not apply when the recipient of the service is acting under the authority or the control of the provider.

3. This Article shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement, nor does it affect the possibility for Member States of establishing procedures governing the removal or disabling of access to information'.

Italy[10] on the liability of hosting providers.

Since 2000 the rightholders of infringed rights have encountered practical difficulties in making Internet service providers liable for infringements carried out through the new services offered to users on the Internet.[11] That situation and the necessity to give an adequate response to the requirement for greater security of the Internet advocated by civil society have given rise in various respects to a need to bring forward the protection against online offences to a time preceding actual commission of those offences. This naturally implies more monitoring of the contents present on the web.

In response to this need, the most recent legislative and case law developments – at domestic and European level[12] – would seem to tend towards entrusting Internet service providers with broad prevention and monitoring functions, requiring them to adopt new filtering measures and specific obligations to block, remove and disable access to illegal information in order to prevent or end its further circulation.

III. Security of Internet Services: a) Online Content Filtering

From this perspective, it is a matter of verifying the feasibility and reasonable limits of general filtering and blocking obligations incumbent on Internet service providers, whereby it would be expected that the providers – normally involved when a violation is ascertained or at least presumed – would take action at a stage prior to the infringement itself, ie not only to put an end to it but also to prevent its actual commission in the future. The issue is of key importance and not easy to resolve.

[10] Corte di Cassazione 19 March 2019 no 7708, *Foro italiano*, I, 2045 (2019), with commentary by F. Di Ciommo, 'Oltre la direttiva 2000/31/Cee, o forse no. La responsabilità dei provider di Internet nell'incerta giurisprudenza europea', which considers the concept of 'active hosting provider' to be a port of call now established at Community level: (European Court of Justice 7 August 2018, Case C-521/17, *Cooperatieve Vereniging SNB-REACT UA* v *Deepak Mehta*, *Diritto* e *giustizia*, 2018; European Court of Justice 14 June 2017, Case C-610/15, Stichting Brein, *Repertorio del Foro italiano*, 2017, voce *Unione europea*, no 1247); European Court of Justice 11 September 2014, Case C-291/13, *Sotiris* v *Papasavvas*, available pluris-cedam.utetgiuridica.it; Europan Court of Justice 12 July 2011, Case C-324/09, *L'Oreal* v Ebay International, in *Annali italiani del diritto d'autore* (Milano: Giuffrè, 2011), 480; European Court of Justice 23 March 2010, Case C-236/08-C-238/08, GOOGLE France, *Foro italiano*, IV, 458 (2010).

[11] The reference is to the huge digital platforms constantly fed by materials uploaded by users and therefore qualified as UGC – User Generated Content, including for example Google video and YouTube, but also the same social networks); the services of indexing, cataloguing, selecting and organizing information carried out by search engines, which are also commercially exploited for the placement of advertising messages or for connecting to content that responds to searches made by the user, and the spread of new technologies for sharing online and cloud services provided by online intermediaries, which significantly change the way of access and use of content.

[12] On which see, *infra* and para 4.

As regards filtering obligations,[13] the main legal obstacle to their general applicability is Art 15 of the e-commerce directive, which as stated above prohibits the imposition on intermediary service providers of measures which constitute an obligation to actively and generally monitor the information transmitted or stored.

Neither can any support for imposing generalised filtering obligations on Internet service providers be gleaned from the fact that the most recent specific legislation[14] on combating the sexual exploitation of children and child pornography, including on the Internet, and on online gambling and betting has imposed on intermediary service providers an obligation to adopt appropriate filtering tools (in addition to a series of information obligations). Leaving aside the fact that those provisions cover just some specific sectors, they are postulated on definite and objective parameters in the shape of a legal prohibition on the sexual exploitation of minors and unauthorised gambling, which facilitate the detection of violations committed. Definite and objective parameters that on the other hand are lacking with regard to other types of violations such as, for example, those relating to intellectual property rights. In addition to being capable of referring across the board to every product or service offered on the web, infringements of that type require an assessment whose boundaries are uncertain and variable boundaries. Furthermore, there is a need to proceed each time to compare the product or service against those protected by the intellectual property rights of others and to separate infringements from lawful uses associated with, for example, exercise of the right of criticism,[15] and from cases of works in the public domain or made available to the public by their author.[16]

Moreover, leaving aside the technical difficulty of adopting effective and flawless filtering systems (given the fact that it is impossible to monitor all existing servers, to monitor systematically all content and to safely distinguish between lawful and unlawful material), the European Court of Justice has repeatedly pointed

[13] On filtering systems, see F. Merla, 'Attività di "filtraggio" dei contenuti on-line, diritti di privativa e libertà di impresa' *Diritto e informatica*, 462, 475 (2012); V. Raggi, 'Brevi note sull'attività di filtraggio dei contenuti informativi veicolati in rete' *Diritto e informatica*, 292, 293 (2011); G. Finocchiaro, 'Filtering e responsabilità del provider' *Annali italiani del diritto d'autore, della cultura e dello spettacolo* (Milano: Giuffrè, 2010), 340; F. Di Ciommo, 'Programmi-filtro e criteri di imputazione/esonero della responsabilità on-line. A proposito della sentenza Google/Vivi Down' *Diritto e informatica*, 829 (2010).

[14] See legge 6 February 2006 no 38, containing 'Provisions on the fight against the sexual exploitation of children and child pornography, including via the Internet'; and legge 23 December 2005 no 266 ('2006 Finance Law', on online gambling and betting and the related implementing ministerial decree (decreto ministeriale 7 febbraio 2006 of Italian Economy and Finance Ministry-AAMS), in particular, Arts 3 and 4.

[15] On the difficulties encountered by the service provider called upon to assess the lawfulness/illicitty of the content submitted by users, see, lastly, Tribunale di Roma ordinanza 1 February 2019, *Foro italiano*, I, 2065 (2019), which excluded the filtering role of the caching provider, which manages an automatic service (Google My Business) consisting in the creation of a card on the activity of a professional.

[16] As you can read in the remittance ordinances Tribunale Amministrativo Regionale Lazio-Roma ordinanza 26 September 2014 no 10016 and no 10020, both in www.federalismi.it.

out that such systems involve complex and costly burdens to the detriment of the freedom to conduct a business of intermediary service providers. Worth citing in this regard are the *Sabam* cases, where a copyright collection society representing authors, composers and publishers of musical works was pitted against an access and a hosting provider respectively.[17] The Court has also highlighted that, from a legal point of view, these filtering technologies can affect the right to secrecy in communications and the protection of personal data of users as well as violate users' freedom of information since they are not able to adequately distinguish between illegal content and legal content. Furthermore, it has been sanctioned the incompatibility of preventive filtering systems against copyright infringement on the Internet with the principle that there is no general monitoring obligation to monitor. In other words, systems which apply without distinction to all users and without time limits at the sole expense of the service provider (access or hosting). In so doing the Court offers a useful interpretation of the principles of proportionality, reasonableness and appropriateness,[18] which must inform any measures to prevent infringements of intellectual property rights, having regard to Art 3 of Directive 2004/48/EC.

However, in addition to the business advantage of enjoying greater 'credibility' among users for Internet service providers that undertake some form of filtering of content and/or users, it is arguable that providers, in particular hosting providers who in the conduct of their business fail to adopt generally used and currently technically feasible filtering systems, should be held liable for a failure to comply with the duty of care[19] incumbent on them as professional operators. The rules governing the civil liability of Internet service providers can be considered as underpinned by the overriding principle that in situations that are potentially harmful to users, the operator is required to take steps to prevent the occurrence (and/or continuation) of the harmful event. This because he is the only person

[17] See European Court of Justice 16 February 2012, Case C-360/10, *Netlog NV* v *Sabam* and European Court of Justice 24 November 2011, Case C-70/10, *Scarlet Extended SA* v *Sabam*, *Foro italiano,* IV, 297 (2012), with commentary by M. Granieri, 'La fine è nota: diritto d'autore, evoluzionismo giuridico e i meccanismi spontanei di aggiustamento del mercato'; in argomento anche G. Colangelo, 'Internet e sistemi di filtraggio tra enforcement del diritto d'autore e tutela dei diritti fondamentali: un commento ai casi Scarlet e Netlog' *Nuova giurisprudenza civile commentata*, II, 580 (2012).

[18] With regard to the principle of proportionality, which has become part of our system mainly through the elaboration by the European Court of Justice, see P. Perlingieri, *Il diritto civile* n 3 above, 379. On the selective and guiding function of the principle of reasonableness in the balancing of interests operations, see P. Femia, *Interessi e conflitti culturali nell'autonomia privata e nella responsabilità civile* (Napoli: Edizioni Scientifiche Italiane, 1996), 158, 516; for a reconstruction of the balancing technique according to reasonableness, see G. Perlingieri, *Profili applicativi della ragionevolezza nel diritto civile* (Napoli: Edizioni Scientifiche Italiane, 2015), 102.

[19] For a reference to average or professional diligence with specific regard to the filtering obligations of Internet service providers, see the observations di A. Musso, 'La proprietà intellettuale nel futuro della responsabilità sulla rete: un regime speciale?' *Diritto e informatica*, 800 (2010).

able to take appropriate action or in any case the one best placed to do so.[20]

Of note in this regard is the recent directive on copyright protection in the digital market, Art 17 of which provides that providers of online content sharing services are to be held liable if, in the absence of the authorisations provided for, they fail to demonstrate that they have made the best efforts in accordance with high industry standards of professional diligence to ensure that their services do not contain works and other specific material protected by copyright uploaded by users. One would suppose *inter alia* that this can be pursued through the adoption of filtering measures identified and specifically calibrated in the light of the principles of proportionality and reasonableness.

From this standpoint one can therefore only welcome the voluntary initiatives, increasingly taken by online platforms, in the form of the advance adoption or provision to users of content filtering systems to increase the level of security of their services.[21]

However, at the same time, one must agree with the recent statement in Commission Communication COM(2017)555 of 28 September 2017 that – after noting that

> 'in the light of technological progress in information processing and artificial intelligence, the use of automatic detection and filtering technologies is becoming an even more important tool in the fight against illegal content online'

– has rightly ruled out 'that this may in itself imply by contrast losing the benefit of the liability exemption' enshrined in the legislation on electronic commerce.[22] Arguing to the contrary would give rise to the paradoxical situation in which the adoption of a filtering system, instead of demonstrating the care exercised by the hosting provider, would on the contrary entail liability for having interfered with the contents. That could encourage hosting providers not to equip themselves with any tool to monitor or filter the contents that they store and, consequently, not to invest in the research and development of safe systems out of the fear that

[20] For the general configurability of such liability on the part of the person who fails to perform an activity that is not risky for him and not binding enough to avoid damage to third parties, cf P. Trimarchi, 'Illecito (diritto privato)' *Enciclopedia del diritto* (Milano: Giuffrè, 1970), XX, 100. It bases its redefinition, in a functional key, of the civil responsibility on the recall to the imperative duties of solidarity of which to the Art 2 Italian Constitution, S. Rodotà, *Il problema della responsabilità civile* (Milano: Giuffrè, 1964), 89. For a fair balance between social solidarity and individual freedom, see L. Bigliazzi Geri, U. Breccia, F.D. Busnelli and U. Natoli, *Diritto civile*, III, *Obbligazioni e contratti* (Torino: Giappichelli, 1989), 705.

[21] On voluntary practices, see M.L. Montagnani, *Internet, contenuti illeciti e responsabilità degli intermediari* (Milano: Giuffrè, 2018), 159.

[22] *Contra* Tribunale di Roma 16 December 2009, Annali italiani del diritto d'autore, della cultura e dello spettacolo (Milano: Giuffrè, 2010), 1372.

> 'they will be blamed for their active participation in the offence and will therefore be charged with full legal liability for the damage caused'.[23]

Thereby sacrificing of the general need for prevention and security on the Internet.

IV. *Continued*. b) Blocking Systems

The use of systems for blocking intermediated content and/or websites, particularly in the area of copyright protection in the digital marketplace,[24] is increasingly gaining ground in our legal system (national and European), both at the legislative and caselaw level, although it is not easy to place it within the broader framework of protecting the other interests involved falling outside the realm of intellectual property law itself.[25] In fact, the threats that can be posed by those systems to online freedom and the ease with which they can be abused are all too evident whenever, due to their wide pervasive effect, they go beyond the purpose that they are intended for and end up preventing access to or

[23] So, textually, F. Di Ciommo, 'Programmi-filtro' n 13 above, 829, to the detriment of the general requirements of prevention and security on the Internet. See also, Tribunale di Roma 13 December 2011, *Diritto e informatica*, 462 (2012), with commentary by F. Merla, 'Attività di "filtraggio" ' n 13 above, 475.

[24] On intellectual property in the information society, see M.L. Montagnani, *Il diritto d'autore nell'era digitale. La distribuzione online delle opere dell'ingegno* (Milano: Giuffrè, 2012); V. Allotti, 'Il diritto d'autore di fronte alle nuove tecnologie' *Rivista di diritto commerciale*, I, 817 (1996); A. Fragola, 'Sui (non facili) rapporti tra Internet e diritto d'autore' *Il diritto di autore*, 12 (1999); M. Fabiani, 'Diritto d'autore e accesso a Internet' *Rivista di diritto commerciale*, 267 (2001); S. Ercolani, 'Il diritto d'autore: la legge italiana e le linee di evoluzione nella società dell'informazione' *Rivista di diritto commerciale*, I, 19 (2001); P.A.E. Frassi, 'Riflessioni sul diritto d'autore. Problemi e prospettive nel mondo digitale' *Rivista di diritto industriale*, 370 (2002); P. Autieri, 'Il paradigma tradizionale del diritto d'autore e le nuove tecnologie', in M. Borghi and M.L. Montagnani eds, *Proprietà digitale. Diritto d'autore, nuove tecnologie e* digital rights management (Milano: Giuffrè, 2006), 23; S. Lavagnini, 'La proprietà intellettuale in Internet' *Annali italiani del diritto d'autore*, 220 (2009); D. Mula, 'La responsabilità e gli obblighi degli Internet provider per violazione del diritto d'autore' *Rivista di diritto industriale*, 252 (2010); N. Bottero, 'Le nuove prerogative d'autore nell'era di Internet' *Giurisprudenza italiana*, 1953 (2011); M. Ricolfi, 'Diritto della proprietà intellettuale e WEB 2.0' *Giurisprudenza italiana*, 1943, 1944 (2011). On the crisis of the traditional system of copyright protection as a result of the generalised ease of dissemination and reproduction of protected works, see M. Libertini, 'Contraffazione e pirateria' *Annali italiani del diritto d'autore*, 215 (2007); V. Zeno-Zencovich, 'Diritto d'autore e libertà di espressione: una relazione ambigua' *Annali italiani del diritto d'autore,* 152 (2005); A. Musso, n 19 above, 797; M. Gambini, 'Diritti di proprietà intellettuale in Rete: criticità e prospettive degli strumenti di tutela nei confronti dei prestatori di servizi Internet' *Rassegna di diritto civile*, 135 (2016).

[25] A. Bertoni and M.L. Montagnini, 'Il ruolo degli intermediari internet tra tutela del diritto d'autore e valorizzazione della creatività in rete' *Giurisprudenza commerciale*, I, 451, 1452 (2013) highlights that these inhibitory means, in addition to clashing with fundamental rights, such as freedom of expression and confidentiality of users and economic initiative of operators, 'do not even appear to be able to implement concepts proper to the discipline of copyright such as private use and fair use'.

circulation of content, including lawful material, that has nothing to do with the alleged infringement.

For some time now in Italy the courts, even if with little success in practice, have intervened – for the most part through measures taken in interim proceedings and hence with only summary reasons given – by ordering, depending on the case, the disabling of access links as well as the seizure and blocking from time to time of content, websites, IP addresses and domain names.[26]

On several occasions the European Court of Justice has ruled in favour of the possibility for rightholders to obtain injunctive relief against Internet service providers aimed at blocking intermediated content and/or sites, in order not only to remove infringements of intellectual property rights already committed but also to prevent new infringements from being committed.[27]

The core issue is compliance with the principles of proportionality, appropriateness and reasonableness of the blocking remedies to protect the rights of inventors and creators *vis-à-vis* the other fundamental rights at stake: the provider's own freedom to conduct a business, freedom of expression and information, and Internet users' right to the protection of their personal data.

In that regard the Court of Justice has recognised the lawfulness, in principle, of an injunction (provided that it is issued by a court) prohibiting the service provider from granting its subscribers access to a website which posts online material protected by copyright without the consent of the rightholders. This is, however, subject to the condition that such an injunction does not specify the measures to be taken in practice to prevent or at least, make it difficult and discourage unauthorised access to the protected material but leaves it up to the supplier to decide what to do and allow the latter to escape liability by demonstrating that it has taken all reasonable measures, which in any event do not unnecessarily deprive users of the possibility of lawful access to the

[26] Tribunale di Teramo ordinanza 11 December 1997, *Rivista di diritto privato*, 637 (1998), with commentary by M. De Mari, *Diffusione di notizie lesive tramite Internet: profili di responsabilità e legge applicabile*; Pretura di Vicenza 23 June 1998, *Diritto e informatica,* 821 (1998); Tribunale di Verona 18 December 2000, *Foro italiano,* I, 2032 (2001) with commentary by F. Di Ciommo, 'Dispute sui domain names, fatti illeciti compiuti via Internet ed inadeguatezza del criterio del locus commissi delicti'; Corte di Cassazione 29 September 2009 no 49437, *Diritto e informatica*, 437 (2010), with commentary by F. Merla, 'Diffusione abusiva di opere in Internet e sequestro preventivo del sito web: il caso «the Pirate Bay»'; Tribunale di Roma 16 December 2009 n 22 above; Tribunale di Roma 11 February 2010, *Diritto e informatica*, 273 (2010), with commentary by L. Guidibaldi, 'YouTube e la diffusione di opere protette dal diritto d'autore: ancora sulla responsabilità dei providers tra hoster attivi, conoscenza dell'illecito e obbligo di sorveglianza'; Tribunale di Roma 22 March 2011, *Diritto e informatica*, 532 (2011); Tribunale di Roma 20 October 2011, *Guida al diritto*, 5, 2 (2013). *Contra*, Tribunale di Milano 3 June 2006, *Diritto dell'internet*, 557 (2006), with commentary of G. Dalia, 'Quando lo streaming di calcio non è illegale'; Tribunale di Roma 11 July 2011, *Rivista di diritto industriale*, II, 19 (2012).

[27] European Court of Justice 12 July 2011, Case C-324/09, available at tinyurl.com/y9v5lfvd (last visited 7 July 2020); European Court of Justice 27 March 2014, Case C-314/12, *UPC Telekabel* v *Constantin Film*, *Foro italiano*, IV, 363 (2014), with commentary of G. Dorè, 'In tema di diritti d'autore', on which see, *infra*, in the text.

information available. In this way, the Court offers domestic courts – called upon to make a considerable interpretative effort in determining the content of the specific injunctions to be issued in the individual case – the interpretative key to the correct implementation of the principles of proportionality, appropriateness and reasonableness to which the blocking remedies designed to protect intellectual property protection in the digital field must be subject. Additionally, the Court has set the degree of professional care that the service provider is called upon to exercise in furtherance of the injunction issued against it. In short, the latter has the power to adopt the measures that best suit its resources and abilities and that are strictly justified in the light of the objective pursued, without however unnecessarily and unjustifiably sacrificing the other two conflicting fundamental freedoms: the provider's own freedom to conduct a business and Internet users' freedom of expression and information, which must be guaranteed to the maximum.

On the regulatory level Art 17 of the recent Directive 2019/790/EU calls on online content-sharing service providers to cooperate with rightholders to avoid that their services include works and other copyright-protected material uploaded by users of those services, in the absence of the required authorisations, expressly providing that such cooperation may lead to the disabling of access or removal of content. It provides that the providers will be held liable if they fail to demonstrate that they have made their best efforts in accordance with high industry standards of professional diligence to ensure that works and other specific materials for which they have received the relevant and necessary information from rightholders are not available. In any event the providers will be liable if they do not prove that they acted expeditiously, upon receiving a sufficiently substantiated notice from the rightholders, to disable access to, or to remove from their websites, the notified works or other subject matter, and made best efforts to prevent their future uploads.

Moreover, Italian lawmakers – exercising the discretion granted to individual legal systems by Arts 12 to 14 of the directive on electronic commerce – had already provided in Arts 14, para 3, 15, para 2 and 16, para 3 of decreto legislativo no 70/2003 that

> 'a court or administrative authority with supervisory functions may require, including as a matter of urgency, that the provider ... prevent or terminate the infringements committed'.[28]

[28] With regard to the exemption from liability of intermediary service providers provided for in Directive 2000/31/EC, recital 45 states that such limitations should leave 'without prejudice to the possibility of inhibitory actions' which 'may, in particular, be orders from courts or administrative authorities requiring an infringement to be brought to an end or prevented, including by removing or disabling access to unlawful information'. In doctrine, see U. Ruffolo, 'Nuove tecnologie: questioni antiche e nuove tutele', in A. Palazzo and U. Ruffolo eds, *La tutela del navigatore in Internet* n 5 above, 286.

Therefore, injured parties are afforded the opportunity to obtain injunctions against network operators even though the latter could well not be held liable for the harmful conduct of users where the conditions exempting them from liability under the aforementioned legislation are fulfilled.[29] This is because they are in the best position not only to put an end to the infringements already committed by users through the Internet services provided to them but also to prevent new infringements (in terms of preventive action and advance safeguards).[30]

V. Security of Data and Systems in Automated Processing of Personal Data

Moving on to the automated processing of personal data, EU law (in the shape of Regulation (EU) 2016/679/EU – General Data Protection Regulation, hereinafter the 'Regulation') addresses the harm that may result from the processing of personal data in violation of regulatory provisions, primarily in terms of prevention by providing for the allocation of the related risks and only as an alternative in terms of remedying the harm caused. The model of protection adopted is based on the principle of liability[31] of those who are involved in the processing of personal data in connection with a commercial or professional activity,[32] principally the data controller and to a limited extent the data processor.

[29] As recital 40 of Directive 2000/31/EC recognises, it is in the interest of all parties active in the provision of information society services – and therefore also of Internet service providers, by virtue of their technical and economic position – to establish and implement rapid and reliable systems capable of removing unlawful information and disabling access to it and in the interest of all concerned, to develop and make effective use of 'technical protection and identification systems and technical monitoring tools made possible by digital technology, within the limits set by Directives 97/46/EC and 97/66/EC', on the subject of confidentiality. For the connection of the provisions of the regulation of electronic commerce with the regulations (national and European) on copyright and with the code of industrial property that, in the digital field, identify the Internet service providers – whose services are used by third parties to violate an intellectual or industrial property right – as possible addressees of injunctions, it is allowed to refer to M. Gambini, 'Diritti di proprietà intellettuale' n 24 above, 169.

[30] However, they express doubts about the effectiveness of copyright protection in the information society, P. Sirena, 'L'efficienza dei rimedi civilistici a tutela del diritto d'autore: prospettive di una ridefinizione sistematica' *Annali italiani del diritto d'autore*, 527 (2003); A. Musso, 'La proprietà intellettuale' n 19 above, 815.

[31] On the principle of accountability, see G. Finocchiaro, Privacy *e protezione dei dati personali. Disciplina e strumenti operativi* (Bologna: Zanichelli, 2012), 289; Id, 'Introduzione al regolamento europeo sulla protezione dei dati' *Nuove leggi civili commentate*, 10 (2017); C. Bistolfi, 'Le obbligazioni di compliance in materia di protezione dei dati personali', in L. Bolognini et al eds, *Il regolamento privacy europeo, Commentario alla nuova disciplina sulla protezione dei dati personali* (Milano: Giuffrè, 2016), 321; see also F. Di Ciommo, 'Civiltà tecnologica, mercato e insicurezza: la responsabilità del diritto' *Rivista critica di diritto privato*, 590 (2010); M. D'Ambrosio, *Progresso tecnologico, "responsabilizzazione" dell'impresa ed educazione dell'utente* (Napoli: Edizioni Scientifiche Italiane, 2017), 17. See also European Commission opinion 3/2010 WP-173 of 13 July 2010, available at tinyurl.com/yb2xdfz2 (last visited 10July 2020).

[32] Art 2, para 2, letter c) of the Regulation expressly excludes from its scope processing

The risks that arise from automated processing and the costs of mitigating, as a preventive measure, harm to the fundamental rights and freedoms of the individual are transferred to those persons.

This dual approach consisting of making those who process data accountable to the maximum and at the same time emphasising prevention of possible harm encompasses a number of precise obligations as to security[33] and controls under EU law, incumbent mainly on the data controller, in order to safeguard the rights of data subjects and the free movement of data.[34] The Regulation significantly extends the scope of those obligations and specifies the professional diligence that those involved in the processing of data must display so as to ensure the protection of the rights and freedoms of individuals and the full attainment of the purposes pursued by the law.[35]

The security rules are set out initially in Art 24 of the Regulation, which requires the data controller to implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with the provisions of the Regulation.

Art 25 of the Regulation, building upon what is stated in Art 24 and in implementation of the principle of data protection by design, extends that data controller's obligation to the initial design phase, requiring the integration of the measures themselves into the very structure of the computerised service it is intended to achieve. In addition, the data controller is required to adopt suitable default settings to limit processing to necessary data only, reducing the storage time and access by third parties, according to the principle of privacy by default. This, depending on the security of personal data and systems used in processing.[36]

operations carried out in the exercise of activities which are exclusively personal or domestic in nature and therefore have no connection with the commercial or professional activity pursued by the person concerned (see recital 18 of the Regulation).

[33] V.F. Bravo, 'L'«architettura» del trattamento e la sicurezza dei dati e dei sistemi', in V. Cuffaro et al eds, *I dati personali nel diritto europeo* (Torino: Giappichelli, 2019), 775.

[34] The combination of the two objectives – one of a non-asset nature: the protection of individuals with regard to the processing of personal data; and the other, more markedly mercantile: the free movement of personal data – already set out in Directive 95/46/EC – is an unavoidable feature of the new rules (see Art 1 of the Regulation, on the subject matter and purpose of the new legislative intervention). In this respect, see G. Finocchiaro, 'Quadro d'insieme sul regolamento europeo sulla protezione dei dati personali', in G. Finocchiaro ed, *Il nuovo regolamento europeo sulla privacy e sulla protezione dei dati personali* (Bologna: Zanichelli, 2017), 1; V. Ricciuto, 'La patrimonializzazione dei dati personali. Contratto e mercato nella ricostruzione del fenomeno', in V. Cuffaro et al eds, *I dati personali* n 33 above, 23.

[35] V.F. Bravo, n 33 above, 785, on the use of security regulations to protect the market, also in the light of Directive 2016/1148/EU (Networking and Information Security Directive, NIS Directive), implemented by decreto legislativo 18 May 2018 no 65, which, in Art 14, imposes on digital service providers the obligation to adopt technical and organizational measures adequate and proportionate to the management of risks relating to the security of the network and information systems they use in the context of the supply of services in the online market; to the online search engine, to cloud computing services.

[36] Cf F. Piraino, 'Il Regolamento generale sulla protezione dei dati personali e i diritti dell'interessato' *Nuova giurisprudenza civile commentata*, 388 (2017).

The foregoing obligations can be viewed in the wider context of the more general security obligation enshrined in Art 32 of the Regulation: in order to ensure a level of security appropriate to the risk to the rights and freedoms of individuals, the data controller is obliged to select and adopt appropriate technical and organisational measures, in order to prevent loss, destruction and accidental or illegal disclosure or access to the personal data processed. The Regulation itself indicates certain technical and organisational security measures, for example, in Art 32(1) where (in subpara a)) pseudonymisation and encryption are mentioned and likewise (in subpara b)) confidentiality, integrity, availability and resilience of processing systems and services. However, on the whole, European lawmakers have chosen not to set out a list of typical measures to be implemented.

Moreover, there is no longer any reference in the Regulation to minimum security measures, unlike in decreto legislativo 30 June 2003 no 196 (Data Protection Code), replaced by a reference to the appropriateness of the measures themselves. This is an indicator of the clear choice made by EU law to avoid a situation where the measures in concrete terms adopted must meet predetermined canons and correspond to a predefined list. By contrast measures are concretely identified and modulated in accordance with the principles of proportionality and reasonableness.

Additionally, the Regulation imposes an analogous security obligation also on the persons in charge of the activities carried out on behalf of the data controller in cases where the organisational measures adopted envisage such an appointment. With reference to the security measures, therefore, the responsibilities can be divided between the data controller and the data processor.

Once the technical and organisational security measures to be adopted have been established, the data controller is obliged to review and update them, if necessary in response to the increasingly pressing demands of technological development, and to test, verify and regularly evaluate their effectiveness (recital 74 of the Regulation) with particular regard to the security measures adopted (Art 32(d) of the Regulation itself). In this context, the Regulation (Art 28(3)(h)) provides that the data controller may carry out audits, including inspections, either itself or on through another person, since those activities are in fact the only ones that the data controller may delegate.

Furthermore, when the type of processing is likely to result in a high risk for the rights and freedoms of natural persons, as happens in the case in question due to the use of new technologies, Art 35 of the Regulation requires the data controller to undertake a prior assessment of the impact of processing on data protection.[37] It must indicate the nature, object, context and purpose of processing (subparas a) and b)); the identification and assessment of risks (subpara c)); all the measures envisaged to deal with the identified risk, including the security

[37] On which see R. Torino, 'La valutazione d'impatto (Data Protetion Impact Assesment)', in V. Cuffaro et al eds, *I dati personali nel diritto europeo* n 33 above, 855.

measures (technical and organisational) to be implemented; and it must meet the requirements of the Regulation and demonstrate its compliance therewith (subpara d)). The impact assessment is identified by the law as a fundamental tool available to the data controller to enable it to assess the necessity, proportionality and risks of the processing and to proceed to devise appropriate measures and adequate safeguards for the data subjects.[38]

If the impact assessment shows a high risk for the rights and freedoms of natural persons, in the absence of the adoption of appropriate measures to mitigate it, the data controller is required, before processing, to consult the supervisory authority in advance, pursuant to Art 36(1) of the Regulation.

All the activities described above must then be properly formalised since the data controller (and, where obliged, the data processor) is required not only to comply with the provisions of the Regulation but must also be able to demonstrate, in a documented manner – hence retaining the relevant evidence – the conformity of the processing carried out with the Regulation itself (Arts 24(1), 32(3) and 35(7)(d) of the Regulation), including the effectiveness of the measures adopted (according to recital 74 of the Regulation).

Finally, with a view as aforesaid to making the data controller more accountable in relation to the security of the processing and the protection of the fundamental rights and freedoms of data subjects, it should be noted that Art 17(2) of the Regulation imposes a further obligation on the data controller that first makes personal data public: the latter must take reasonable measures, including technical one, to inform third parties, who are processing the same personal data further that the data subject has requested the erasure of any links to the personal data in question, or copy or replication thereof.

Overall, the system of controls devised by EU law through the establishment of technical, organisational and security measures to be implemented by the data controller (and to a limited extent also the data processor) reveals a strong focus on the profile of the analysis and management of risks related[39] to the automated processing of personal data, which embodies the principles of prevention and precaution. The nature of the activity carried out and the means used entail, in fact, an intrinsic damaging potential since they create a not-always-foreseeable risk of harm to the rights and freedoms of natural persons that can be avoided or at least curbed, precisely, by adopting appropriate preventive and precautionary measures.

The concept of appropriateness embraced by Arts 24, 25 and 32 of the Regulation – interpreted in the light of the extension by EU law of the duty of

[38] On which see the Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is 'likely to result in a high risk' for the purposes of Regulation 2016/679, adopted in April 2017 by Art 29 Working Group, available at tinyurl.com/mhprzt5 (last visited 7 July 2020).

[39] V.A. Mantelero, 'Responsabilità e rischio nel Regolamento UE n. 2016/679' *Nuova giurisprudenza civile commentata*, 144 (2017).

care incumbent on those involved in the processing – makes it *per se* insufficient that the technical and organisational security measures actually adopted will ensure compliance with the requirements of the laws and regulations on the subject, and hence binding on all operators in a given sector and in relation to all personal data processing carried out in that area. In fact, those measures must be strengthened further (on a voluntary basis) in order to ensure maximum practical effectiveness (see, for example, recital 74 of the Regulation) and must be devised and modulated in practice by the data controller (and possibly also the data processor) on the basis of an assessment of what is best in terms of available technology and implementation costs (see for example, recital 84 of the Regulation) and having regard to proportionality and reasonableness. Those measures must be implemented on a case-by-case basis, taking into account the nature, context, scope and purpose of the single processing and the various and likely risks to the rights and freedoms of natural persons (see recitals 74, 83 and 84 of the Regulation).

An interpretative reading of this type seems moreover to be even more justified today in the light of the principle of liability on which the new protection of personal data is based. That principle requires that the data controller be given an incentive not only to refrain from processing of a type that is detrimental to the rights of data subjects but also to take preventive and precautionary measures aimed at averting the risks and avoiding the damage that may stem from the very processing of data. Without prejudice to the obligation to demonstrate that the processing is performed in accordance with law (Arts 24(1), 32(3) and 35(7)(d) of the Regulation), including as regards the effectiveness of the measures adopted.

Leaving aside for the moment the substantial administrative fines and penalties under Arts 83 and 84 of the Regulation that flow from a failure to adopt the aforementioned technical and organisational security measures, infringement of the relevant implementing measures that the professional operator could and/or should have taken in the knowledge of the risks and dangers involved – which (although not always foreseeable) are typologically connected with its activity – entails aggravated liability on grounds of presumed negligence of the data controller and (to a limited extent) the data processor. Consequently, the latter are obliged to pay compensation in respect of the damage (material and non-material) suffered by the data subject in accordance with Art 82 of the Regulation.[40] This paves the way – from the perspective of this work – to an evaluation of the diligence exhibited by the data controller (and to a limited extent by the data processor) in implementing the system of controls and security measures required by the legislation.

[40] For the examination of liability and compensation in the processing of personal data, M. Gambini, *Principio di responsabilità e tutela aquiliana dei dati personali* (Napoli: Edizioni Scientifiche Italiane, 2018).

VI. The Security of Artificial Intelligence Systems

In addition to the matters previously considered and somehow already 'known', these past years we have been witnessing the full flourishing of the 'Internet of Things' and the growth of the area of service robotics, which exploit intelligent devices able to communicate with each other or interface with humans, to collect data, analyse and process data autonomously and interactively (consider, for example, self-driving vehicles and robots used in the medical field or in healthcare services), increasingly based on deep learning algorithms regulating self-learning and programmed to decide autonomously the conduct to be adopted.

There is also the rapid spread of big data, systems that are based on huge amounts of digital data, collected through the Internet and from the many technological devices in common use. Those data are often analysed and processed in a way unknown to the data subjects, ie through employing secret algorithms, increasingly used to make decisions, engage in profiling or predictive analysis and that mark a radical change in services related to information.

It follows from these phenomena that the daily life of individuals is permeated by a continuous flow of data (including personal data) that can result in forms of illicit algorithmic manipulation thereof arising out of the fact that the source data used in algorithmic processing may be incorrect, inaccurate or incomplete. This is even more worryingly, since the algorithms are created by human decision-makers who, already at the design stage, can influence the analysis and distort the processing, leading to results that are detrimental to individual rights and freedoms.

The spread of algorithmic processing not only means the loss of control over personal data[41] but it can also affect other aspects which, by overcoming the problem of confidentiality, affect human dignity, freedom, autonomy, personal development and individuals' health and safety and involve clear risks of stigmatisation and discrimination of individuals.[42] Think, for example, of the scope of algorithmic decisions that prevent a person from entering a country, benefitting from a subsidy or even obtaining an essential service.

Therefore, in the 'algorithm society' there is an urgent need to implement appropriate mechanisms to protect privacy and more in general to safeguard the rights and freedoms of the individuals against unlawful algorithmic data processing. In particular, for the purposes of our analysis here of the security of data and algorithmic systems, it is necessary to establish the measures required to minimise risks, prevent dangers and avoid damage associated with the use of

[41] On the privacy in the age of the Internet of Things and big data: F. Giovannella, 'Le persone e le cose: la tutela dei dati personali nell'ambito dell'*Internet of Things*', in V. Cuffaro et al eds, *I dati personali* n 33 above; A. Mantelero, *La privacy all'epoca dei big data*, ibid, 1181.

[42] S. Rodotà, *Il mondo della rete. Quali i diritti, quali i vincoli* (Roma-Bari: Laterza, 2014), 37. According to the aforementioned 'Ethical Guidelines on AI', the principles of respect for freedom and autonomy of human beings must be defended and guaranteed also in the development and then in the use of artificial intelligence systems.

robotics and AI to build the 'architecture' of their processing.

Since there are no existing rules already in place it is necessary to ascertain, including from a policy perspective, the approach that it would be best to adopt in the regulation of security in the field of intelligent robotics and algorithms, possibly referring to regulatory solutions and application experience gained in the areas of technological innovation, verifying their transponibility to new scenarios while still prioritising constitutional values and the protection of human beings.

As we have seen, the models proposed by EU and national law in the sectors examined for the provision of information society services and automated personal data processing are marked by the progressive transition to a concept based mainly on internal controls, ie entrusted to professional operators, aimed at increasing the security of algorithmic systems, minimising risks, preventing dangers and avoiding harmful events. One must take note of the progressive introduction (through legislation and caselaw) of an articulated series of obligations in relation to security and controls incumbent on the protagonists of technological innovation. Such obligations operate as internal limits to the business that those protagonists conduct and end up shaping it to take account of the needs of protection to be achieved: protection of the rights and freedoms of the natural persons but also safeguarding of the market for new technologies.

Now, in order to guarantee the security of the 'algorithm society', it is desirable to adopt an analogous approach, inspired by the principles of prevention and precaution, which – to an even more incisive extent – focuses attention on the provision for an articulated system of controls incumbent on those responsible for the design, programming and implementation of the algorithms, aimed at reducing the risks and avoiding damaging events for the rights and freedoms of individuals in the first place, failing which compensation would be due. The foregoing with a view to ensuring maximum accountability for the design and development phases of algorithmic applications.

However, the overlapping of roles and responsibilities of many of the actors involved in the whole process of the conception, development, dissemination and use of complex and varied forms of AI makes it necessary to encourage all of the actors in question to minimise risks at the very outset before tackling the possible adverse consequences of their work.[43]

This issue is particularly relevant with reference to deep learning algorithms that regulate self-learning and are programmed to decide autonomously the conduct to be adopted. In this regard, however, the European Parliament Resolution of 16 February 2017 with Recommendations to the Commission on

[43] In addition to what will be said in the text regarding the creators and developers of algorithmic systems – consider the producers of goods and service providers who incorporate and implement algorithms, better equipped to affect the level of risk associated with the use of their goods and services. And the user community is called upon to pay a high level of attention to the use of different IA applications, for example, to update and monitor the software and to avoid its anomalous use.

Civil Law Rules on Robotics[44] reiterates the key point – already embraced by in Art 22 of the Regulation dealing with automated individual decision-making, including profiling –[45] that is it vital to respect the principle of the supervised autonomy of intelligent robots. In fact, it is provided that the possibility for human control must be integrated in the algorithmic processes, thus confirming the central role played by the person who supervises the activity of the algorithm and even before that its very programming. Today one cannot maintain that also systems endowed with the capacity of self-learning and decision-making autonomy can be programmed and operate independently of choices, criteria and algorithms set by man. That is consistent with the 'Ethics Guidelines for Trustworthy AI' presented on 9 April 2019 at Digital Day 2019 by the high-level group of experts appointed by the European Commission,[46] according to which AI systems must adhere to principles of human-centric design and development and leave significant scope for human choice, ie ensuring human oversight of operational processes in AI systems.

Therefore, in the field of robotics and AI one can only hope that the expected steps taken by hetero and self-regulation aimed at ensuring the security of the algorithms that underlie and govern them will translate into the establishment of a set of obligations as to conduct imposed on operators. Marking an increase in the standard of professional diligence required in the performance of their activities, those obligations will ensure the adoption of all security measures (technical and organisational) and controls in practice suitable to minimise risks, prevent dangers and avoid damage by algorithmic data processing.

With regard to their contents, these obligations should, first of all, provide for the adoption of privacy by design and privacy by default functionality, ie technical and organisational measures suited to guaranteeing compliance with

[44] Available at tinyurl.com/y8z4vamw (last visited 7 July 2020).

[45] Art 22 of the Rules of Procedure – Automated decision-making process concerning natural persons, including profiling – : '1. The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

Paragraph 1 shall not apply if the decision:

is necessary for entering into, or performance of, a contract between the data subject and a data controller;

is authorized by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or

is based on the data subject's explicit consent.

3. In the cases referred to in points (a) and (c) of paragraph 2, the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.

Decisions referred to in paragraph 2 shall not be based on special categories of personal data referred to in Art 9(1), unless point (a) or (g) of Art 9(2) applies and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place'.

[46] Available at tinyurl.com/y8ph3aka (last visited 7 July 2020).

the regulatory principles in force governing the personal data processing involved; and this from the initial phase of the design of the algorithms and subsequently by default too.

In addition, algorithm designers and developers should be required to establish a complex network of system security protection obligations, aimed not only at ensuring but also at demonstrating the correct implementation of appropriate and effective technical and organisational measures: consider, for example, the risks to human health and life stemming from the possibility of deactivation or deletion of the memory of cyber-physical systems integrated in the human body.

Algorithmic data processing should be preceded by rigorous impact assessment and early risk analysis, which should guide the selection and implementation of risk management measures as they are identified.

These activities should moreover be carried out on a continuous basis, ensuring that the measures taken are strengthened as a result of new technological developments or events that have demonstrated their inadequacy. Periodic maintenance, revision and updating obligations should therefore be imposed on the algorithms and the software into which they are incorporated, taking into account both the speed of progress in this area and the need to monitor over time the evolution of the learning of smart robots.

Furthermore, there should be an obligation to adopt monitoring and compliance procedures on algorithmic applications, in order to increase their compliance and prevent the violation of ethical and regulatory principles in force.

Further preventive protection tools should also include the construction of forms of control based on the maximum transparency of algorithmic systems. In this direction, it is worth citing a very recent judgment of the Italian Council of State,[47] which held an automated decision-making process adopted by a public authority would be lawful only if the associated

> 'algorithm is built in a manner that embodies a reinforcement of the principle of transparency, which also implies that it is fully knowable'

– both for citizens and for the courts – in every aspect:

> 'its authors, the procedure used for its elaboration, the decision mechanism, including the priorities assigned in the evaluation and decision-making procedure and the data entered and selected as relevant because that very same logic and reasonableness of the robotised administrative decision, or rather the 'rule' that governs the algorithm, must be 'readable' and comprehensible'.

Finally, the configurability of further controls on algorithms aimed at gaining

[47] Consiglio di Stato 8 April 2019 no 2270, *Guida al diritto*, 19, 16 (2019).

the trust of users could be evaluated, which could force the creators and developers of such technologies, for example, to adopt mechanisms for certifying the quality of the algorithms or to adopt specific guarantees of reliability, with effects on a reputational level. This is also confirmed by the 'Ethical Guidelines for Trustworthy AI' recently adopted by the European Commission's high-level expert group.

We are still a long way from translating these guidelines into a system of governance of internal controls that is required by law and which operators are called upon to comply with.

It is therefore hoped, first of all, that there will be an increase in intervention by non-authoritative sources of standardisation, providing for an increase in the level of professional diligence of those who design and develop algorithms and software and a valuing of the expertise required in the performance of their activities: technical rules, sector guidelines and protocols, codes of ethics and conduct, security standards, capable of constantly adapting to technological changes. This trend is confirmed by the 'Charter on Robotics', the 'Code of Ethical Conduct for Robotics Engineers' and the 'Licence for Designers', annexed to the European Parliament's resolution of 16 February 2017; and the recent 'Ethical Guidelines on Trustworthy AI'.

However, soft law does not appear to be sufficient since its effectiveness depends, as is well known, on voluntary adherence by operators, which cannot be taken for granted in the new technologies sector, where – as we have seen – there are many different players. It is therefore necessary that authoritative rules be laid down by national and supranational lawmakers that supplement those taken by competent authorities or technical bodies, as reflected in the proposal to establish a European Agency for Robotics and Artificial Intelligence referred to in the aforementioned Resolution.

In a desirable composite regulatory framework deriving from the interaction and combination of rules from different sources,[48] the obligations as to security and controls imposed on operators who design and develop algorithms will serve as parameters to inform their conduct regarding technological innovation. These obligations will encourage (by guiding) the adoption of virtuous models of behaviour and strategies as regards prevention and precautionary measures and that will act as an incentive for security and controls in connection with the algorithmic data processing that they perform and for promoting the constant improvement of new technologies (for the benefit of the community).

These obligations, if fulfilled, will play an active role in protecting the rights and freedoms of individuals against threats to which algorithmic data processing

[48] On the problem of the identification of the source – negotiated or authoritative – of the discipline of the telematic reality, see G. Alpa, 'Le "fonti" del diritto civile: policentrismo normativo e controllo sociale', in G. Alpa et al eds, *Il diritto civile oggi. Compiti scientifici e didattici del civilista, Atti del 1° Convegno Nazionale S.I.S.Di.C., Capri 7-9 aprile 2005* (Napoli: Edizioni Scientifiche Italiane, 2006), 107. According to C. Rossello, *Commercio elettronico. La* governance *di Internet, tra diritto statuale, autodisciplina,* soft law *e* lex mercatoria (Milano: Giuffrè, 2006), 21.

may expose them. This, in addition to, or rather, before being used by the courts as parameters to evaluate *a posteriori* the lawfulness/unlawfulness of the processing carried out. In this regard, it is desirable that the 'centre of gravity' so to speak of algorithmic liability should[49] be more about prevention rather than cure, ie shift the focus from compensation to that of actually avoiding harm being caused by robotics and AI in the first place.[50] Moreover, the ethical guidelines on AI referred to above seem to express such an orientation, placing damage prevention among the four fundamental ethical principles that should inspire and permeate any future application of AI, at least in Europe, where it is stated that 'AI systems and the environments in which they operate must be safe and secure' and technically robust and it should be ensured that they are not open to malicious use. The guidelines further warn as follows:

> 'Particular attention must also be paid to situations where AI systems can cause or exacerbate adverse impacts due to asymmetries of power or information, such as between employers and employees, businesses and consumers or governments and citizens. Preventing harm also entails consideration of the natural environment and all living beings'.

[49] However, there is no doubt that, at the current stage of development of the various algorithmic applications, the fear of damage is still high. So much so that the policy statements expressed in the European context, in particular, in the Parliament Resolution of February 2017, still focus on civil liability, making it a common denominator for all the issues dealt with. On the subject, which acquires particular importance with regard to deep learning algorithms, see U. Ruffolo, 'Per i fondamenti di un diritto della robotica *self-learning*, dalla *machinery* produttiva all'auto *driverless*: verso una "responsabilità da algoritmo"?', in U. Ruffolo ed, *Intelligenza artificiale e responsabilità* (Milano: Giuffrè, 2017), 1; A. Amidei, 'Robotica intelligente e responsabilità: profili e prospettive evolutive del quadro normativo europeo', ibid, 63; E. Palmerini, 'Robotica e diritto: suggestioni, intersezioni, sviluppi a margine di una ricerca europea' *Responsabilità civile e previdenza*, 1816 (2016).

[50] On the multi-functional character of the institute of civil liability, see P. Perlingeri, 'La responsabilità civile tra indennizzo e risarcimento' *Rassegna di diritto civile*, 1061 (2004); Id, 'Le funzioni della responsabilità civile' *Rassegna di diritto civile*, 115 (2011) and confirmed by recent jurisprudential developments (Corte di Cassazione-Sezioni unite 5 July 2017 no 16601, *La Nuova Procedura Civile*, 4 (2017)). For a teleological-functional reading of the rules on civil liability, see, *ex multis*, likewise, S. Rodotà, *Il problema della responsabilità civile* n 7 above; G. Calabresi, *Costo degli incidenti stradali e responsabilità civile. Analisi economico-giuridica*, in A. De Vita et al eds (Milano: Giuffrè, 1975); P. Trimarchi, *Rischio e responsabilità oggettiva* (Milano: Giuffrè, 1961); G. Ponzanelli, *La responsabilità civile. Profili di diritto comparato* (Bologna: Zanichelli, 1992).