Comparative Law Review

2024 - Special Issue

Incontro di Studi dei Giovani Comparatisti

Le declinazioni della Giustizia

Università La Sapienza
Roma 2/3 febbraio 2023

ISSN:2983 - 8993

COMPARATIVE LAW REVIEW
The Comparative Law Review is a biannual journal published by the
I. A. C. L. under the auspices and the hosting of the University of Perugia Department of Law.

Office address and contact details:
Department of Law - University of Perugia
Via Pascoli, 33 - 06123 Perugia (PG) - Telephone 075.5852437
Email: complawreview@gmail.com

Comparative Law Review is registered at the Courthouse of Monza (Italy) - Nr. 1988 - May, 10th 2010.

COMPARATIVE
LAW
REVIEW
SPECIAL ISSUE VOL. 15/1

Le declinazioni della Giustizia

PERSONAL DATA'S PROTECTION IN THE USE OF PREDICTIVE JUSTICE SYSTEMS: EU VS U.S.

Ediola Terolli

TABLE OF CONTENTS

This research aims to analyze, through the lens of comparative law methodology, the legislative framework of the European Union and the United States on privacy and protection of personal data in the use of predictive justice systems.
The right to privacy was born in the U.S. and developed in the EU into the right to protection of personal data. Unlike the EU, the U.S. presents a fragmented regulatory framework in the field of privacy and data protection. Obviously, the protection of personal data in the use of predictive justice systems in EU and U.S. is based on a very different legal landscape and compliance challenges differ. Notwithstanding the differences, it is interesting to see the EU's General Data Protection Regulation (EU 2016/679) influence on the U.S. data privacy landscape – such as the California Consumer Privacy Act of 2018 and the importance of comparative data protection law in the field of predictive justice.

Keywords: personal data, predictive justice, comparative law, EU, U.S.

I. INTRODUCTION

The right to privacy was born in the United States of America as 'the right to be let alone' that reproduced the pattern of private property, 'my home my castle', excluding others' interference in one's private sphere[1], and developed in the European Union into a fundamental right to the protection of personal data.
The EU and U.S. have a different regulatory framework in the field of privacy and data protection – the latter being quite fragmented[2].
Despite the differences, it is interesting to see how the General Data Protection Regulation (EU 2016/679) has affected the U.S. data privacy landscape, such as the California Consumer Privacy Act of 2018[3], and the relevant developments related to the field of predictive justice.
Predictive justice is defined as the use of artificial intelligence, concretely machine learning and natural language processing technologies, for predicting outcomes of legal disputes. Machine learning algorithms aim at analyzing and creating links among different data and Natural Language Processing means the IT processing of human language.
As it has been explained in a study of the Council of Europe, a machine does not reproduce legal reasoning, it does not explain the meaning of the law or the behavior of judges, but it consists in a statistical or probabilistic approach. Given the impossibility of mechanically identifying all the causative factors of a decision, there remains the risk of confusing correlation and causality[4].
Robot judges who can decide on cases autonomously do not exist but there are systems that can assist judges and lawyers by quicky analyzing a large quantity of resources to unveil

[1] S.D. Warren, L.D. Brandeis, *The Right to Privacy*, in 4 *Harv. L. Rev.* 5, 1890, p. 193-220.
[2] L. Jolly, *Data Protection in the United States Overview*, Data Protection Global Guide, Thomson Reuters: Practical Law, 2019.
[3] C. Barett, *Are the EU GDPR and the California CCPA becoming the de facto global standards for data privacy and protection?*, 15 *SciTech Law.* 3, 2019.
[4] Council of Europe, *Artificial Intelligence and judicial systems: The so-called predictive justice*, 9 May 2018.

the potential outcome of a legal dispute. Even though, there is the risk of not looking beyond the algorithms when studying a case, or losing that singularity that characterizes a specific case, they are being tested. In France, Predictice and Case Law Analytics are start-ups that are operating in the field, having the capacity to analyze millions of court cases in seconds and offer possible results of a case. In the United States, a similar start-up, Lex Machina is being used for statistics regarding court decisions. Dentons and DLA Piper are also using such algorithms for internal assessments.
The scope of this research is privacy and data protection in the use of predictive justice in the EU and U.S., from data protection principles to data subjects' rights.
Compliance with the latest iterations of privacy and data protection legislation in EU or U.S. is key in using algorithms in predictive justice but how do they differ and what do they have in common?

II. Privacy and data protection in the European Union

Privacy and data protection in the European Union constitute two separate fundamental rights, the right to privacy is enshrined in art. 7 of the Charter of fundamental rights of the EU and the right to data protection in art. 8 of the Charter of fundamental rights of the EU and art. 16 par. 1 of the TFEU.
EU institutions must respect and guarantee these rights, as well as the Member States when implementing the EU law[5].
The right to privacy manifests itself in the 'negative' freedom not to have one's private life interfered with, while the right to personal data protection in the 'positive' freedom to exercise control over the processing and circulation of information concerning one's person[6].
The EU data protection framework includes another legal instrument: the ePrivacy Directive[7] and ePrivacy Regulation -proposal, that aims to provide a higher level of protection to users of electronic communications[8].
The EU data protection framework is complemented by Regulation 2016/679 (GDPR)[9], Directive 2016/680 (LED)[10]- applicable to data processing by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, Regulation 2018/1725 [11] - applicable to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data and Directive (EU) 2016/681 (PNR) – applicabile to the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime [12].
For the purposes of this research, we will focus on the GDPR.

---

[5] Article 51, Charter of Fundamental Rights of the EU.
[6] S. Rodotà, "*Il mondo nella rete. Quali i diritti, quali i vincoli*", *Dall'habeas corpus all'habeas data*, Roma, 2014, p. 31-32.
[7] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) available at:
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02002L0058-20091219.
[8] Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) available at
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017PC0010.
[9] Available at *https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679*.
[10] Available at *https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32016L0680*.
[11] Available at *https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32018R1725*.
[12] Available at *https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016L068*.

A. *The General Data Protection Regulation*

The Regulation (EU) 2016/679 [13] of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, better known as GDPR is a regulation of the European Union which became applicable on 25 May 2018[14].

Since its entry into force, the GDPR has repealed Directive 95/46/EC[15] and unified a patchwork of 28 different data protection laws of the Member States, bringing about a crucial and ambitious shift in the field of personal data protection.

The dispositions of Regulation (EU) 2016/679, unlike Directive 95/46/CE, are immediately applicable, without any necessary national legislative intermediation, except the few articles where explicit reference is made to it regarding specified cases and areas[16].

The GDPR compared to Directive 95/46/EC has an extraterritorial scope and determines whether processing falls within its geographical scope by considering the following factors: the location where personal data are processed and the location of the data subject[17]. The intention is to make the Regulation equally applicable to organisations inside and outside the EU when processing personal data of EU citizens. The extraterritorial scope of the GDPR currently makes comparative privacy and data protection law of great interest.

The Recitals of the Regulation itself state that the processing of personal data is at the service of mankind; the right to the protection of personal data is not an absolute prerogative but must be considered in the light of its social function and be balanced with other fundamental rights, in accordance with the principle of proportionality.

«Rapid technological developments and globalisation have brought new challenges for the protection of personal data»[18].

Under the regulation «personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors

---

[13] Published on the Official Journal of the EU on L 119/1, 04/05/2016.

[14] For an extensive analysis of the GDPR see: L. Bolognini, E. Pelino, C. Bistolfi (eds.), *Il Regolamento Privacy europeo. Commentario alla nuova disciplina sulla protezione dei dati personali*, Milano, 2016; F. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali. Il Regolamento europeo 2016/679*, II, Torino, 2016; M. Soffientini (ed.), *Privacy Protezione e trattamento dei dati,* Milano, 2016; M. G. Stanzione, *Il regolamento europeo sulla privacy: origini e ambito di applicazione*, in *Eur. dir. priv.*, 2016, p. 1249 ff.; S. Sica, V. D'Antonio e G.M. Riccio (eds.), *La nuova disciplina europea della privacy*, Padova, 2016; L. Califano e C. Colapietro (eds.), *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679*, Napoli, 2017; A. Ciccia Messina e N. Bernardi, *Privacy e regolamento europeo*, Milano, 2017; G. Finocchiaro, *Introduzione al Regolamento europeo sulla protezione dei dati*, in *Nuove leggi civ.*, 2017, p. 1 ff.; G. Finocchiaro (ed.), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Bologna, 2017; E. Calzolaio, *Il regolamento europeo sulla protezione dei dati personali: spunti ricostruttivi e profili problematici*, in *Nuovo dir. civ.*, 2017, p. 331 ff.; G. Cassano, V. Colarocco, G.B. Gallus. e F. P. Micozzi (eds.), *Il processo di adeguamento al GDPR. Aggiornato al D.lgs. 10 agosto 2018, n. 101*, Milano, 2018; G. Comandé e G. Malgieri (eds.), *Manuale per il trattamento dei dati personali*, Milano, 2018; E. Lucchini Guastalla, *Il nuovo regolamento europeo sul trattamento dei dati personali: i principi ispiratori*, in *Contr. impr.*, 2018, p. 106 ff.; V. Zeno-Zencovich, *Data protection in the Internet, in Annuario di diritto comparato e di studi legislativi*, 2018, p. 431 ff.; G.M. Riccio, G. Scorza, E. Belisario (eds.), *GDPR e normativa Privacy. Commentario*, Milano, 2018; V. Cuffaro, R. D'Orazi e V. Ricciuto (eds.), *I dati personali nel diritto europeo*, Torino, 2019; R. Panetta (ed.), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato. Commentario al Regolamento UE n. 2016/679 (GDPR) e al novellato d.lgs. n. 196/2003 (Codice Privacy)*, Milano, 2019; E. Tosi (ed.), *Privacy Digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, Milano, 2019; N. Zorzi Galgano (ed.), *Persona e mercato dei dati. Riflessioni sul GDPR*, Padova, 2019.

[15] The Directive 95/46/CE entered into force on 13/12/1995, with the scope of harmonising the EU data protection law given the precedent difficulties in the free flow of personal data between Member States. In that sense, G. Scarchillo, *Il trasferimento di dati verso gli Stati Uniti. Evoluzioni e prospettive di diritto comparato,* in *Responsabilità e diritti,* Jovene Editore, Napoli 2018, p. 12.

[16] In that sense, F. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali*, cit., p. 150.

[17] Art. 3, GDPR: "Territorial Scope".

[18] Recital 6 GDPR.

specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person»[19].
The scope of application of GDPR includes the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system. It does not include the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security [20].
The GDPR allows member states to introduce exemptions on issues including national and public security, judicial independence and civil law enforcement as deemed necessary and appropriate. Also, the GDPR allows member states to introduce limitations to specific contexts such as the balancing of data protection rights with freedom of information and expression[21] or archiving proposes[22].
In an increasingly data-driven world, the rules aim to protect all EU citizens from privacy and data breaches, while creating a clearer and more coherent framework for businesses[23].
The GDPR in Article 5[24] outlines the six data protection principles that organisations must respect when collecting, processing and storing personal data of EU residents:

1) Lawfulness, fairness and transparency

Personal data collection activities by organisations must comply with the law and must not hide anything from the data subjects. The principle of lawfulness must be read in correlation with the principle of strict legality enshrined in Article 52 of the Nice Charter[25]. The principle of fairness essentially concerns the relationship between the data controller / processor and the data subject[26]. As regards the principle of transparency, as recital 39 specifies, it must be transparent to natural persons how their data are collected, used, consulted or otherwise processed and the extent to which they are or will be processed [27].

2) Purpose limitation

The purpose for which personal data is collected must be precise and the data must be kept only as long as necessary to complete the purpose for which it was collected. The purposes of processing must be «specified, explicit and legitimate and not further processed in a manner that is incompatible with those purposes»[28].

3) Data minimisation

Only data that are necessary to achieve the purposes for which they are processed should be processed. Personal data must only be processed if the purpose of the processing cannot reasonably be achieved by other means (use of anonymised or pseudonymised data)[29]. In

[19] Art. 4 GDPR.
[20] Art. 1, par. 1 e Art. 2, par. 1 GDPR.
[21] Art. 85 GDPR.
[22] Art. 89 GDPR.
[23] K. Milt, *Protezione dei dati personali*, 2018, Note sintetiche sull'UE available at: http://www.europarl.europa.eu/RegData/etudes/fiches_techniques/2017/N54564/it.pdf
[24] Art. 5, GDPR.
[25] See F. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali*, cit., p. 241.
[26] *Ivi*, p. 267.
[27] G.M. Riccio, G. Scorza, E. Belisario (eds.), *GDPR e normativa Privacy. Commentario*, cit., p. 54.
[28] Recital 39, GDPR.
[29] Recital 39, GDPR.

the principle of minimisation provided by the GDPR, qualitative and quantitative aspects are combined [30].

4) Accuracy

Data subjects have the right to request that their inaccurate or incomplete data be erased or rectified[31]. The concept of accuracy is relational because it needs be assessed in close correlation with the purpose and use of the data [32].

5) Storage limitation

Personal data must be retained as long as they are necessary for the purposes for which they are collected, with further retention only permitted for archiving in the public interest, scientific or historical research or statistical purposes[33].

6) Integrity and confidentiality

Data must be processed in such a way as to ensure adequate security, including protection, by appropriate technical and organisational measures, against unauthorised or unlawful processing and against accidental loss, destruction or damage[34].
The person in charge for compliance to such principles is the data controller.

The key changes of the GDPR are as follows: increased territorial scope; enhanced data inventory requirements; increased penalties; appointment of a Data Protection Officer (DPO); broader obligations for data controllers; direct obligations for data controllers; more timely reporting of personal data breaches; the right to data portability; the right to erasure ('the right to be forgotten'); increased consent from the data subject[35].

III. PRIVACY AND DATA PROTECTION IN THE UNITES STATES

The United States' data protection framework is fragmented and lacks a single regulatory framework applicable to the private sector, unlike the European Union. As regards the public sector, the Privacy Act of 1974[36] regulates access, collection, processing, and disclosure of personal data by federal government activities. The Privacy Act imposes several obligations on federal governmental activities to protect the privacy of data subjects, such as, inter alia, notifying the data subject of the existence and nature of the file containing his or her personal data, as well as the possibility of modification. Yet, the effectiveness of the protection guaranteed by the Privacy Act is doubtful, as the statute provides numerous exceptions for information collected for national security purposes[37].
On the level of sources of law, at the constitutional level, the Fourth Amendment to the Constitution protects privacy and the protection of personal data, which does not, however,

[30] L. Bolognini, E. Pelino, C. Bistolfi (eds.), *Il Regolamento Privacy europeo. Commentario alla nuova disciplina sulla protezione dei dati personali*, cit., p. 107.
[31] Articles 16 and 17, GDPR.
[32] On this point, see F. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali. Il Regolamento europeo 2016/679*, cit., p. 200.
[33] The Court of Justice's case law on data retention has been built on the principle of storage limitation (Digital Rights Ireland, rendered in Joined Cases C-293/12 and C-594/12, on 8/4/2014 and Tele2 and Watson, rendered on 21/12/2016, in Joined Cases C 203/15 and C 698/15), to the point of annulling both national and European regulations (Dir. 2002/58/EC in part qua), which were deemed incompatible with these principles. See G.M. Riccio, G. Scorza, E. Belisario (eds.), *GDPR e normativa Privacy. Commentario*, cit., p. 60.
[34] Art. 5, par.1, lett. f), GDPR.
[35] *Ex multis*, see C. Russell, S. Fuller, *GDPR for Dummies, MetaCompliance Special Edition*, Chichester, 2017, p. 6.
[36] 5 U.S.C. § 552° (2000 & Supp. IV 2004), see *Overview of the Privacy Act of 1974*, *The United States Department of Justice*, available at https://www.justice.gov/opcl/overview-privacy-act-1974-2015-edition.
[37] Regarding the exepctions on the scope of application of the *Privacy Act*, see F. Bignami, *European versus American liberty: a comparative analysis of anti-terrorism data-mining*, in 48 *B.C. L. Rev.* 609, 2007, p. 631 ff.; F. Bignami, G. Resta, *Transatlantic Privacy Regulation: conflict and cooperation*, in 78 *Law & Contemp. Probs*, 2015, p. 237.

enshrine a general constitutional right to privacy[38], whereas the ordinary type of regulation in the US legal system includes federal and state legislation.
Moreover, in the jurisprudence of the U.S. courts, state or federal, there is no majority position in favour of a constitutional right to privacy[39]. This is also due to the so-called 'third party doctrine'[40] which denies Fourth Amendment protection to information and data that an individual voluntarily exposes to third parties, even from his or her home or office[41].
The Fourth Amendment to the United States Constitution enshrines the right of every individual to be secure in his or her person, dwelling, and effects, protecting him or her from unreasonable searches and seizures by government authorities[42]. Reasonableness is determined by balancing two interests, the intrusion on an individual's rights protected by the Fourth Amendment and the legitimate interest of government authority such as public safety[43].
The third-party doctrine[44] argues that an individual does not have a legitimate expectation of privacy with respect to information disclosed to third parties by him or her voluntarily[45]. The NSA's databases, belonging to this category of 'non-content information', do not fall within the scope of the Fourth Amendment[46].
The third-party doctrine, which has proven to be a tool for legitimising government surveillance activities by U.S. authorities, has been challenged in a recent U.S. Supreme Court ruling, in which Justice Sotomayor, in support of the decision stated that even if an individual protests the government's disclosure, without a warrant, of a list of all websites visited in the previous week, month, or year, he or she will only be able to obtain constitutional protection if Fourth Amendment jurisprudence stops treating secrecy as a prerequisite to privacy[47].

A. *Sectoral Federal Laws*
In the United States, there is no federal law regulating the collection and use of personal data. The U.S. privacy model, unlike the general framework of EU law, is a system of sectoral laws[48], federal and state laws[49], as well as numerous case law precedents[50]. In

[38] See C. M. Barrett, *FBI Internet Surveillance: The Need for a Natural Rights Application of the Fourth Amendment to Insure Internet Privacy*, 8 *Rich. J.L. & Tech* 16, 2002.
[39] On these aspects see F. Bignami, G. Resta, *Transatlantic Privacy Regulation: conflict and cooperation*, cit., p. 235-236.
[40] Common law doctrine elaborated by the U.S. courts.
[41] Katz v. United States, 389 U.S. 347, 351 (1967).
[42] Available at *https://www.archives.gov/founding-docs/bill-of-rights-transcript*.
[43] C. Barett, *Are the EU GDPR and the California CCPA becoming the de facto global standards for data privacy and protection?*, cit., pp. 24-29.
[44] Smith v. Maryland, 442 U.S. 735, 744 (1979). For a complete analysis of "*third party doctrine*", see R.M. Thompson II, *The Fourth Amendment Third-Party Doctrine, Congressional Research Service Report*, 2014. Available at *https://fas.org/sgp/crs/misc/R43586.pdf*.
[45] Smith v. Maryland, 442 U.S. 735, 743-44 (1979).
[46] See F. Bignami, *European versus American liberty: a comparative analysis of anti-terrorism data-mining*, cit., p. 624-625.
[47] On this topic see A. Schinelli, *Profili critici del trasferimento di dati personali UE-USA tra conflitti regolatori e reazioni politche*, in S. Bonavita (a cura di), *Società delle tecnologie esponenziali e General Data Protection Regulation: La circolazione internazionale dei dati personali*, Milano, 2019, p. 11-35.
[48] The relevant constitutional protection essentially passes through the decisions of the Washington Supreme Court.
[49] See G. Stevens, *Privacy Protections for Personal Information Online*, in *Congressional Research Service*, 2011.
[50] «In addition to the very narrow scope of data protected under federal statutes, court cases are also of limited benefit with respect of data privacy because of the conflicting interpretations of these sparse statutes», W. G. Voss, K. A. Houser, *Personal Data and the GDPR: Providing a Competitive Advantage for U.S. Companies*, in 56 *Am. Bus. Law J.* 2, 2019, p. 302.

addition, there are many guidelines developed by government agencies and industry groups that are regarded as 'best practices' and have components of accountability and sanctions that are increasingly being used as an instrument of control by legislators.

Some of the most important federal privacy laws include, but are not limited to, the following:

The Federal Trade Commission Act (FTC Act)[51] is a federal consumer protection law that prohibits unfair or deceptive practices and has been applied to offline and online privacy and data security policies. The FTC has introduced numerous enforcement actions against companies that do not comply with published privacy policies and for unauthorised disclosure of personal data. The FTC is also the primary enforcer of the Children's Online Privacy Protection Act (COPPA) (15 U.S.C. §§6501-6506), which applies to the online collection of children's information and the Self-Regulatory Principles for Behavioural Advertising.

The Financial Services Modernization Act (Gramm-Leach-Bliley Act)[52] regulates the collection, use and disclosure of financial information. It applies broadly to financial institutions such as banks, securities firms and insurance companies, and other businesses that provide financial services and products.

The Health Insurance Portability and Accountability Act (HIPAA)[53] regulates the medical information industry. It may apply to healthcare providers, data controllers, pharmacies and other entities that deal with medical information.

The Fair Credit Reporting Act[54] (and the Fair and Accurate Credit Transactions Act[55]), which amended the Fair Credit Reporting Act) applies to consumer reporting agencies, those that use consumer reports, and those that provide information on consumer reports.

The Electronic Communications Privacy Act[56] and the Computer Fraud and Abuse Act[57] regulate the interception of electronic communications and computer tampering, respectively.

In 2016, Congress enacted the Judicial Redress Act, giving citizens of some allied nations (notably, EU Member States) the right to seek redress in U.S. courts for privacy violations carried out in the exchange of information with law enforcement agencies.

B. *State privacy laws*

There are many laws at the state level regulating the collection and use of personal data, California being at the forefront, having adopted several privacy laws, some of which have far-reaching effects nationwide.

California was the first state to enact a security breach notification law[58]. The law requires a person or business that owns or licenses computer data that includes personal information to notify any breach of system security to all California residents whose unencrypted personal information was acquired by unauthorised persons.

Most early state laws on security breach notification mirrored California law and tended to be reactive, i.e., they set forth requirements for responding to a security breach, such as the Massachusetts Regulation[59], which prescribes in detail an extensive list of technical, physical, and administrative security aspects and protocols aimed at protecting personal information that companies must implement in their security architecture.

---

[51] 15 U.S.C. §§41-58.
[52] (GLB) 15 U.S.C. §§6801-6827.
[53] 42 U.S.C. §1301 et seq.
[54] 15 U.S.C. §1681.
[55] Pub. L. No. 108-159.
[56] 18 U.S.C. §2510.
[57] 18 U.S.C. §1030.
[58] California Civil Code §1798.82.
[59] 201 CMR 17.00.

On 28 June 2018, California passed the broadest of all privacy laws in the United States, the California Consumer Privacy Act of 2018 (effective in January 2020)[60]. The Act offers Californian consumers numerous new rights: the right to be informed about how personal information is collected and for what purpose;[61] the right to know with which third parties personal information is shared; the right to object to having one's personal information sold to third parties (right to opt-out)[62]; the right to request the deletion of one's data [63]; the prohibition to sell the data of children under 16 to third parties, unless consent is given (right to opt-in), which must be parental consent if the personal information is of a child under 13[64]; the right to take action against the company in case of a personal information breach[65]; the right to seek protection from the California Attorney General. The right to act against the company in case of a personal information breach will probably lead to high-level class actions in California[66].

A company that has suffered a data breach is obliged to notify the General Attorney within 30 days of the breach, under penalty of a penalty of USD 7,500 per breached record.

In November 2020, CCPA was amended by the Proposition 24, the CPRA that added additional privacy protections as of 1 January 2023: the right to correct inaccurate personal information that a business has about them and the right to limit the use and disclosure of sensitive personal information collected about them.[67]

With the introduction of these rights, the California Consumer Privacy Act 2018 bears similarities to the GDPR[68], although there are still vast differences[69]. Sometimes even referred to as 'the mini-GDPR'[70] The Californian framework protects individuals only as consumers residing in California (and not as citizens or users of a public service)[71].

Even at this level, the Californian regulation only binds for-profit organisations that: obtain revenues of at least USD 25 million per year; or process the personal information of at least 50,000 consumers, households or devices; or obtain at least 50 per cent of their profits from the sale of personal information[72] .

The compliance of local operators in cases where their business also concerns the personal data of EU citizens would be burdensome as they have to comply with California state law, U.S. federal law, and the EU Regulation (GDPR).

Other federal states such as Nevada, Maine and New York, Massachusetts and Connecticut are embracing the same trend of privacy protection and data sovereignty.

New York passed the Stop Hacks and Improve Electronic Data Security Act ('SHIELD Act')[73] and made amendments to the data breach notification law[74]. It represented a clear

---

[60] Official text available at: *https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375*.
[61] 1798.100; 1798.110.
[62] 1798.120.
[63] 1798.105.
[64] 1798.120. (d)
[65] 1798.150.
[66] L. Jolly, *Data Protection in the United States Overview*, cit.
[67] R. Bonta, Attorney General, *CPPA*, available at *https://oag.ca.gov/privacy/ccpa*.
[68] J. Tashea, *Leading the Way: Inspured by Europe's sweeping GDPR, California's new data privacy law could change how companies do business in the Golden State*, in 34 *ABA Jour.*, 2019, X. Becerra, *California's GDPR inspiration, Reactions*, London, 2019.
[69] C. Barett, *Are the EU GDPR and the California CCPA becoming the de facto global standards for data privacy and protection?*, cit., p. 24-29 and J. Tashea, *Leading the Way*, cit.
[70] C. Meyer, A. Pierce, *California Enacts Mini-GDPR Effective 1 January 2020*, in *JDsupra*, 2018.
[71] 1798.140 (g) del *California Consumer Privacy Act* 2018.
[72] 1798.140 (c) (A) (B) (C) del *California Consumer Privacy Act 2018*.
[73] Senate Bill S5575B, available at: *https://www.nysenate.gov/legislation/bills/2019/s5575*.
[74] On these aspects, J. Day, *New York Passes SHIELD Act Amending Data Breach Notification Law - The SHIELD Act significantly amends New York's data breach notification law and data protection requirements*, in *JDsupra*, 2019. Besides see M.M. Miner, A. Troyanovych, *The New York SHIELD Act: What's new under the state's breach law?*, in 33 *The Business Journal- Central New York, Syracuse* 48, 2 December 2019.

step forward in data protection but many politicians in New York wanted to take it a step further. This led to the drafting of the New York Data Privacy Act, very similar to the GDPR.

The New York Data Privacy Act has many similarities with the California Consumer Privacy Act, but goes even further, aiming to allow any citizen of the state the possibility of suing companies in the event of unlawful processing of personal data[75]. New York Data Privacy Act has passed Senate on 8 June 2023 – Senate Bill 365[76].

Residents of New York could boast strong control over their data, much more than in any other state in the U.S. Businesses, on the other hand, would have to put users' privacy before their profit.

Moreover, while the California law applies only to companies that generate more than $25 million in annual gross revenue, the New York law would apply to companies of any size. The New York Privacy Act would thus grant state citizens greater control and power over their personal data and force companies to prioritise privacy over profit. In short, the bill would force all technology companies to act as 'information fiduciaries', which would prevent them from using data in ways that harm consumers.

Like the CCPA, New York's privacy law would allow citizens to require companies to disclose the recipients with whom data is shared, and, where appropriate, to correct or delete it. Sharing data or selling it to third parties would therefore risk ending[77].

Alike the GDPR, companies will have to respond to general requests for information within 30 days (but unlike the GDPR, only for a 12-month reference period prior to the request). The obligation to report data breaches is clearly inspired by the GDPR.

Vermont has a law strictly focused on data brokers. Maine does not regulate data brokers but regulates Internet service providers. Illinois has a biometric data law that most other states do not. Twenty-five states and Puerto Rico have considered legislation focusing on various aspects of consumer data.

All 50 states, as well as the District of Columbia, Puerto Rico and the U.S. Virgin Islands have enacted laws requiring notification of security breaches involving personal information. All these laws are subject to change.

This complex and inconsistent regulatory environment risks the U.S. relinquishing its leading position in technology. The best solution would be a federal law that provides a consistent set of standards applicable online and offline.

A national privacy law would be stronger with unified and well-funded enforcement through the Federal Trade Commission. Federal oversight would allow all U.S. citizens to benefit from multiple privacy protections, including the option to delete their data, transparency in data collection, and portability of data between services[78].

IV. PREDICTIVE JUSTICE IN THE EUROPEAN UNION

The European Union 's regulatory approach to Artificial Intelligence includes in addition to the data protection framework that is analysed above and remains fully applicable, the newly enacted legislation – Data Services Act[79] and Data Markets Act[80], as well as the AI

[75] California law leaves enforcement to state attorney general.

[76] See New York State Assembly. Available at: *https://nyassembly.gov/leg/?default_fld=&leg_video=&bn=S00365&term=2023&Summary=Y&Actions=Y&Text=Y*.

[77] On these aspects see M. Valeri, *Privacy per lo Stato di New York vale più del profitto: nuova legge fa tremare i big del Web*, in *Cybersecurity360*, 13 June 2019.

[78] M. Beckerman, *Americans will pay a price for State privacy laws*, in *The New York Times*, 14 October 2019. Available at: *https://www.nytimes.com/2019/10/14/opinion/state-privacy-laws.html*.

[79] Regulation (EU) 2022/2065 of the European Parliament And of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) available at *https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32022R2065*.

[80] Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU)

Act[81] that was actively debated and adopted by the European Parliament on March 13, 2024.[82]

According to the European Commission, the aim of DSA and DMA is «to create a safer digital space in which the fundamental rights of all users of digital services are protected and to establish a level playing field to foster innovation, growth, and competitiveness, both in the European Single Market and globally»[83].

Whereas the AI Act is the first international comprehensive law on Artificial Intelligence to ensure better conditions for the development and use of this innovative technology.

Predictive justice is still in its experimental phase in the EU.

In France, two appeal courts - Douai and Rennes, in 2017, at the initiative of the Ministry of Justice, tested a predictive justice software called "Predictice" that aimed to make justice more scientific, logic and controllable by reducing the variability in court decisions in the name of the principle of equality of citizens before the law. Software reasoning biases were revealed that resulted in inappropriate outcomes «due to confusion between mere lexical occurrences of judicial reasoning and the causalities that had been decisive in the judges' reasoning»[84]. Judges concluded that there is no added value in using predictive justice in their activities[85].

In France, another start-up called Case Law Analytics uses Artificial intelligence to quantify of legal risk. The company models the judicial decision process to present you the whole decisions that would be made on a given file[86].

In Italy, some interesting projects of AI applications in the field of predictive justice are taking place. The first one, operational since November 2021, is promoted by the Court of Appeal and the Court of Brescia, in cooperation with the University of Brescia. For now, it only deals with 'Labour Law' and 'Business Law', already accessible on the website of the judicial offices. The aim of the project is to provide users and economic agents with data of certainty and predictability and, at the same time, to contain demand, disincentivising reckless litigation, as well as to promote the transparency of decisions, the circularity of jurisprudence between first and second instance and the overcoming of unconscious contrasts[87].

Another project is promoted by the Court of Appeal of Venice, in collaboration with Ca' Foscari University of Venice, *Unioncamere del Veneto* and Deloitte. The aim of the first phase, relating only to the subject of dismissals for just cause, was to digitalise all the decisions issued in the district during the three-year period 2019-2021, to make case law precedents knowable and decisions predictable, discouraging litigation with low probability of success[88].

2020/1828 (Digital Markets Act), available at *https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32022R1925*.

[81] Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain union legislative acts, 21/04/2021, available at *https://eur-lex.europa.eu/legal-content/en/txt/?uri=celex%3a52021pc0206*.

[82] European Parliament legislative resolution of 13 March 2024 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD)).

[83]European Commission, The Digital Services Act Package, *https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package*.

[84] European Commission for the Efficiency of Justice (CEPJ), Council of Europe, *European ethical Charter on the use of Artificial Intelligence in judicial systems and their environment*, 4 December 2018, p. 42.

[85] M. Par Jahera, C. Piret, *La justice predictive: de la revolution à la désillusion*, in *InterFrance*, 13 October 2017.

[86] Source: Case Law Analytics. Available at *https://www.caselawanalytics.com*.

[87] See C. Castelli, *Giustizia predittiva*, in *Quest. giust.*, 8 February 2022.

[88] A. Traversi, *Giustizia predittiva: Quale futuro?,* in Altalex, 15 March 2023.

Also in the tax sector, a project called 'Prodigit' has been financed, aimed at creating systems based on algorithms that can analyse laws, judgments, and doctrinal contributions to predict, with a sufficient degree of probability, the orientation of the decision of a judge on a given legal issue. It is envisaged that the computer, by analysing a large quantity of judgments, thanks to its capacity to learn, will become increasingly reliable, allowing the taxpayer, when the system is operational, to obtain an answer as to whether or not to file an appeal[89].

In the field of administrative justice, there have already been some ground-breaking decisions of the Council of State on the role of artificial intelligence in public administration decision-making that underly the advantages of the use of artificial intelligence, provided that the mechanism through which the robotized decision is realised is knowable and, consequently, can be reviewed by the judge[90].

Regarding criminal justice, in the Italian Code of Criminal Procedure, no expert opinions are allowed to establish the character or personality of the defendant (Article 220(2) of the Code of Criminal Procedure). Therefore, an Italian judge could hardly use a computer to establish whether there is a risk of a defendant reoffending[91].

In respect of international courts, researchers at UCL, the University of Sheffield and the University of Pennsylvania have done a study on 584 decisions of the European Court of Human Rights (ECtHR), by using a machine learning algorithm and the judicial decisions of ECtHR have been predicted to 79% accuracy, being the first to predict the outcomes of a major international court. This success rate is on the "facts" part, and it decreases to 62% on the application part of the Convention[92].

V. PREDICTIVE JUSTICE IN THE UNITED STATES

Artificial Intelligence is developing rapidly in the U.S., but «federal agencies are largely constrained to adapting existing U.S. law to AI systems». «The EU has passed, and is beginning to implement, the DSA and DMA. These acts have significant implications for AI in social media, E-commerce, and online platforms in general, while the U.S. does not appear yet prepared to legislate on these issues», authors suggest that the U.S. should work on a legal framework for online platforms and consider alignment with the EU's DSA and DMA as well as a framework similar to the AI Act [93].

In the U.S., at the federal and state levels, artificial intelligence – automated decision-making tools are frequently used in the criminal justice system to estimate the risk that a given defendant will commit a crime after release [94]. According to the Electronic Privacy Information Center risk assessment tools are being used by judges in pre-trial, sentencing, prison management and parole. Factors such as socioeconomic status, family background, neighborhood crime, employment status, stability and other factors are being used to predict individuals' criminal risk and classified as "low", "medium" or "high"[95].

One of the most widely used algorithms in the U.S. courts is the Correctional Offender Management Profiling for Alternative Sanctions – COMPAS that uses statistics to assess the risk of recidivism. It is based on the criminal history of the offender and 137 questions

[89] See A. Traversi, *Op. cit.*

[90] Cons. Stato, sec. VI, no. 2270/2019, Cons. Stato, sec. VI, no. 8472/2019, no. 8473/2019 and no. 8474/2019. On these decisions see: A.L. Rum, *Il provvedimento amministrativo adottato mediante algoritmo: il ruolo dell'intelligenza artificiale nel processo decisionale della P.A.*, 13 May 2021.

[91] See A. Traversi *Op. cit.* and G. Canzio, *Intelligenza artificiale e processo penale*, in G. Canzio, L. Luparia Donati (eds.), *Prova scientifica e processo penale*, II ed., Milano, 2022, p. 908.

[92] See A. Traversi *Op. Cit.*

[93] A. Engler, *The EU and U.S. diverge on AI regulation: A transatlantic comparison and steps to alignment*, in *Brookings*, 25/04/2023.

[94] J. Forward, *The Loomis Case: The Use of Propriety Algorithms at Sentencing*, in *State Bar Wis.*, 19 July 2017.

[95] Electronic Privacy Information Center, *Algorithms in the Criminal Justice System*, available at https://epic.org/algorithmic-transparency/crim-justice.

that the latter must answer to generate a risk score between 1 and 10. Based on this score, COMPAS classifies the risk of recidivism as low-risk (1 to 4), medium-risk (5 to 7), or high-risk (8 to 10). The result is then part of the defendant's PSI report supplied to the sentencing judge. As a result, a defendant's sentence is influenced to some degree – if not determined -by the COMPAS's recidivism risk assessment. [96]
The Wisconsin Supreme Court has highlighted the need of a cautious use of the COMPAS risk assessment in the case of Eric Loomis[97]. Although, it held that COMPAS is a proprietary instrument which mechanism can't be disclosed to the public. Also, it noted that it used publicly available data and information provided by the defendant and the court had based its decision only partly on the COMPAS assessment as other circumstances were taken into consideration as well in taking an individualised judgement[98].
Some studies consider the tool as biased against African Americans[99].
«Cognitive bias occurs because of distortion or change in perception from rational to irrational in making decisions and illogical interpretation in human thought. In other words, the wrong way of thinking makes us wrong in making a decision»[100].
Another predictive justice tool used in the United States is PredPol that is used for predictive policing. It predicts "crime hotspots" by using data related to crime type, date, and time[101].
There are many companies operating in the field of predictive justice such as Lex Machina, a company based in Silicon Valley, that provides legal analytics by combining data and software with individual attorney review. Its «Lexpressions® engine scans millions of pages of litigation information to create valuable insights on courts, judges, law firms, lawyers, and parties. This information has enabled legal professionals, for the first time, to anticipate the behaviors and outcomes that different legal strategies will produce»[102]. According to a lawyer and data scientist at Lex Machina, recently a user can build a list of cases according to any criteria and then look at and filter the analytics for that list of cases. Get information about judges regarding caseloads, timing, damages, remedies and even how they handle specific violations [103].
In the U.S. predictive justice applications are developing rapidly.

VI. Data protection in the use of predictive Justice EU vs U.S.

Predictive justice, the automated analysis of data, raises concerns for the data protection/privacy laws.
In the EU, GDPR guarantees the right to "meaningful information about the logic involved"[104] in automated decisions and AI applications in predictive justice should provide detailed reasoning. In addition, it guarantees the data subject "the right not to be subject to

[96] A. Lee Park, *Injustice Ex Machina: Predictive Algorithms in Criminal Sentencing,* in *UCLAReview.org*, 19 February 2019.
[97] Loomis was an African American convicted felon, arrested after an escape attempt driving a car previously involved in a firefight and found in possession of weapons, whom a Wisconsin judge sentenced to six years' imprisonment in 2016, based on the COMPAS algorithm's response that had defined him as a 'high risk of violence'.
[98] State v Loomis 881 N.W.2d 749 (Wis. 2016), sec 16., See H.-W. Liu, C.-F. Lin, Y.-J. Chen, *Beyond State v Loomis: Artificial Intelligence, Government Algorithmization, and Accountability*, in 27 *Int. J. Law Inf. Technol.* 2, 2019, p. 122-141.
[99] J. Angwin, et. al., *Machine Bias*, in *Propublica.org,* 23 May 2016; M. Gialuz, *Quando la giustizia penale incontra l'intelligenza artificiale: luci e ombre dei* risk assessment tools *tra Stati Uniti e Europa*, in *Dir. Pen. Cont.*, 2019, p. 5.
[100] D. Kahneman, *Thinking Fast and Slow*, Farrar, 2011.
[101] M. Degeling, B. Berendt, *What is wrong with Robocops as consultants? A technology-centric critique of predictive policing*, in 33 *AI & Soc.*, 2018, p. 347-356.
[102] A LexisNexis Company *https://lexmachina.com/about/*.
[103] R. Ambrogi, *Judge Analytics is the New Black*, in *Litigation and Research*, 23 July 2015.
[104] Article 13-15 GDPR.

a decision based only on automated processing, including profiling, which produces legal effects concerning him or her or similarly affects him or her"[105].

The right to information on the underlying logic of algorithms' decisions is enshrined in the GDPR, while in the U.S. courts are still reluctant to recognize it fully and weigh private interests – particularly the protection of intellectual property[106].

GDPR is a more comprehensive legal framework and offers a stronger protection of personal data even when it comes to predictive justice.

State laws, in U.S., that are introducing alike standards like the California Consumer Protection Act and New York Data Privacy Act, are raising the data privacy standards.

According to the Council of Europe, case law in open data is fuel for AI application as there is a growing tendency to make available data coming from public institutions – including courts' decisions in the form of freely downloadable databases as part of a global movement calling for transparency and accountability of public action [107].

In France, with the adoption of the 2016 law on "Digital Republic", all court decisions at all instances are disseminated in the form of open data for free and with respect for the privacy of the persons concerned. An analysis of the risk of reidentification of the persons concerned is done beforehand[108].

The Court of Justice of the European Union and the General Court when acting in their judicial capacity ensure that the principle of open courts and public information is balanced with the protection of personal data of natural persons mentioned in cases brought before it. They provide the data subject the possibility of requesting anonymity in the context of that case [109]. This is very important in case predictive justice tools would be used on its case-law.

It is interesting to see that in a resolution of the American Bar Association, that addresses ethical and legal issues related to the usage of artificial intelligence in the practice of law, it is recommended regarding privacy that: «Considering that AI could be used in monitoring people and making decisions about them based on their personal information, it is important that the courts and lawyers address the privacy impact in using the AI and to the extent that lawyers and law firms are subject to privacy laws, AI impact analysis may need to assess such usage's compliance with such laws, such as GDPR»[110].

VII. CONCLUSIVE REMARKS

The U.S. approach to privacy is part of the larger U.S. understanding of the appropriate regulatory approach to the digital economy[111]. The EU approach, on the other hand, seeks to balance the development of the digital economy with the protection of personal data as a fundamental right.

The U.S. data protection framework is fragmented and lacks a single legal framework - at the federal level - applicable to the private sector, unlike the European Union. As seen above, it consists of a system of federal and state laws, as well as numerous case law precedents.

The GDPR, which ensures the highest level of data protection globally, is affecting the global privacy and data protection landscape, including the United States.

The California Consumer Privacy Act 2018 bears similarities to the GDPR with regard to the new rights introduced (e.g. the right to be forgotten), although there are still vast

[105] Art. 22, par. 1, GDPR.
[106] CEPJ, Council of Europe, cit., p. 55.
[107] Council of Europe, Artificial Intelligence and judicial systems: The so-called predictive justice, 9 May 2018.
[108] Council of Europe, Artificial Intelligence and judicial systems: The so-called predictive justice, 9 May 2018.
[109] Court of Justice of the European Union, *https://curia.europa.eu/jcms/jcms/p1_2699100/en/*.
[110] American Bar Association, House of Delegates, Resolution, 12-13 August 2019.
[111] H. Farrell, A.L. Newman, *Of Privacy and Power. The Transatlantic Struggle over Freedom and Securty,* Princeton, 2019.

differences. Furthermore, the future New York Data Privacy Act, when adopted, will be very similar to the GDPR.
An eventual move towards harmonisation, if not standardisation, of privacy laws at the federal level seems inevitable considering the compliance costs that companies currently face[112].
It is interesting to note that European Commission adopted a new adequacy decision for the EU-U.S. Data Privacy Framework on 10 July 2023, after the invalidation of Privacy Shield in the Shrems II judgement of the Court of Justice of the European Union, that allows personal data to flow freely from the EU to companies in the United States that participate in the Data Privacy Framework[113].
Predictive justice algorithms need to comply with the applicable data privacy laws both in the EU and the U.S..
According to the GDPR standards', is important to assess the compatibility of the algorithms used in predictive justice with data protection principles such as the lawful, fair, and transparent processing of personal data, the purpose limitation, data minimization, accuracy, storage limitation, integrity, confidentiality, and accountability.
In addition, it is necessary to carry out a data protection impact assessment and implement data protection by design and by default at a very early stage when algorithms are used to assist judicial proceedings.
Moreover, the rights of the data subjects concerned shall be respected and protected, inter alia the right not to be subject to an automated decision, the right to have access to the data that are being processed, the right to object, the right to obtain information about the reasoning of the data processing carried by algorithms, the right to a legal remedy etc.
Also, important questions such as who the data controller and data processor are apply – as well- in predictive justice algorithms.
Predictive justice applications in the U.S. do not face all these challenges in every state, given the fragmented data privacy framework analysed above but it is promising to see that alike standards are being introduced in some states.
Predictive justice tools are built by private companies and their mechanism is kept confidential due to trade secrets; this poses a transparency problem that some authors call also "the black box" problem[114]. It could be resolved by a public-private partnership in building such mechanisms or if they would be completely developed by the public authorities' oversight.
In conclusion, research engines make links among doctrine, case law, laws and regulations could be helpful, but data should be of a good quality and algorithms should be transparent, non-biased, certified by an independent authority, always accessible by a judge for an

---

112 E. Goldman, *An Overview of the California Consumer Privacy Act*, in *Internet Law Cases & Materials*, 2019, p. 9. For a complete analysis see M. Humerick, *The Tortoise and the Hare of International Data Privacy Law: Can the United States Catch Up to Rising Global Standards?*, 27 *Cath. U. J. L. & Tech*., 2019 and N. O'Connor, *Reforming the U.S. Approach to Data Protection and Privacy*, in *Council on Foreign Rel*., 2018: «Most Western countries have already adopted comprehensive legal protections for personal data, but the United States-home to some of the most advanced, and largest, technology and data companies in the world-continues to lumber forward with a patch-work of sector-specific laws and regulations that fail to adequately protect data. U.S. citizens and companies suffer from this uneven approach-citizens because their data is not protected, and companies because they are saddled with contradictory and sometimes competing requirements».
112Even before the invalidation of *Privacy Shield* some were thinking of alternative mechanisms *Binding Corporate Rules*. In that sense, C. Stupp, *Companies Face Uncertainty Over Challanges to Trans-Atlantic Data Traansfers; EU's Privacy Shield and other legal tools could be upended in near-tearm court decisions*, in *WSJ*, 23 September 2019.
113 Commission Implementing Decision of 10.7.2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework, available at *https://commission.europa.eu/system/files/2023-07/Adequacy%20decision%20EU-US%20Data%20Privacy%20Framework_en.pdf*.
114 H.-W. Liu, C.-F. Lin, Y.-J. Chen, *Beyond State v Loomis*, cit., p 17.

adversarial debate – as the judge cannot exclude doubt a priori in the face of machines built to give certain answers[115], and in compliance with the rights of the data subjects and the applicable legislation that is trying to keep up with the pace of AI.

[115] G. Riccio, *Ragionando su intelligenza artificiale e processo penale*, in *Arch. Pen.*, 3, 2019, p. 10.