Raimondas Andrijauskas
Law School, Mykolas Romeris University

I.5. PRIVACY-FRIENDLY PERSONAL DATA PROCESSING AND SUSTAINABILITY: IS THERE MUTUAL SUPPORT?

The link between sustainable development and data

The modern industrial economic model, started over a century ago, developed in a world far different from the one we live in today. There were few people and plentiful resources. This resulted in the one-way, linear, highly productive "take–make–waste" system (Hedstrom 2018, p. 3). Economic globalization even intensified this "take resources out of the earth–make things–throw them away" flow by improving the efficiency of general production and global consumption. The pursuit of acquiring more physical goods drives modern economies, but this also means greater environmental degradation and the depletion of natural resources (Portney 2015, p. 86).

The idea of environmentally friendly economic growth first attracted widespread attention in the 1970s, when a number of international development programs were criticized for using their extensive financial resources to inadvertently promote environmental degradation under the guise of economic development in developing countries (Portney 2015, p. 22). Increased concerns from non-governmental organizations stressing the necessity of protecting the global environment finally materialized into the ambitious idea of sustainability that was internationally acknowledged in the work of the United Nations' (UN) World Commission on Environment and Development (WCED). In the report, sustainable development was defined as economic development activity that "meets the needs of the present without compromising the ability of future generations to meet their own needs" (WCED 1987, p. 39).

Sustainable development could be interpreted from the material point of view as overarching interests deriving from production–consumption systems. According to the UN (2016), by 2050 three Earths will be required to sustain our current lifestyles. This means that the fundamental transformation of humanity's development model is necessary: not only should production processes, products and services be re-evaluated, but also patterns of consumption and access to goods and services. Changes are required, in which the needs of persons are fulfilled but consumption patterns and lifestyles based on the consumption of far fewer resources are developed (Ceschin and Gaziulusoy 2020, p. 7). There is a need to urgently move towards socio-technical systems that are capable

of operating within the limits of our planet while ensuring that this move follows ethical and just pathways.

Sustainability requires many challenges to be solved, including the development of tools to evaluate the efficiency and impact of measures taken to achieve sustainable development goals (SDGs). The rapid pace of technological advancements and digitalization in recent decades is often considered a promising long-term solution for sustainable development (Portney 2015, p. 199). This approach was strengthened in 2014, when the UN Secretary-General's Independent Expert Advisory Group on the Data Revolution for Sustainable Development (IEAG) issued the report "Mobilising the data revolution for sustainable development" (IEAG 2014, pp. 4–5), encouraging the use of innovative data analysis technologies while monitoring and achieving SDGs. Increasing data collection, more advanced data processing techniques, and the availability of cloud computing services have been presented as solutions to societal challenges, as data are considered a resource for societal improvement and growth and a means by which to promote societal wellbeing and shared values. The potential of processing large amounts of data has been seen as ground-breaking in many domains – from healthcare (Chen 2019, pp. 18–19) to transportation (Rowland and Porter 2021, p. 31; Cottrill and Derrible 2015, p. 61), from reducing hunger (Belaud *et al.* 2019) to fighting climate change (Bibri 2021, pp. 36–37). This allows data to be referred to as the "New Oil" (Marr 2018).

Despite all of the benefits that the data revolution could propose for society's sustainable development, some scientists also draw attention to the negligence towards risks for the achievement of SDGs, which are threatened by the environmental footprint of the data revolution (Lucivero 2020, p. 1010). In the context of environmental research, it is acknowledged that information and communication technologies (ICT) used for data processing have a huge footprint, featuring the high consumption of non-renewable energy, waste production, and CO_2 emissions (Pohl *et al.* 2019; Williams 2011). Data volume is rapidly increasing: in 2012, it was estimated that from 2005 to 2020 the digital universe would grow by a factor of 300, from 130 to 40,000 exabytes (Gantz and Reinsel 2012, p. 1). Today, it is forecast that by 2025 the Global Datasphere (the term used to define the summation of all data that is generated – whether created, captured, or replicated – from three primary locations where digitization is happening and where digital content is created: the core – traditional and cloud datacentres; the edge – enterprise-hardened infrastructure like cell towers and branch offices; and the endpoints – PCs, smart phones, and IoT devices) will grow even further, to 175 zettabytes (Reinsel *et al.* 2018, p. 3). Although data analysis initiatives are continuously supported and well-funded – assuming that a larger amount of data enables better analysis and improved knowledge – this also means that the more data, the bigger its footprint, as it usually needs non-renewable energy and limited resources to function (Lucivero 2020).

Increased demands to process data and initiatives to use more advanced data analysis techniques for the well-being of society have not only received criticism from a number of environmental scientists (Berkhout and Hertin 2004; Williams 2011), but also several scholars who have addressed a series of ethical concerns. These scholars include Tamar Sharon (2016), who raised critical attention to the new power asymmetries based on access to data and control over technological infrastructures, and Danah Boyd and Kate Crawford (2012), who analyzed concerns about the inequalities in accessing data. As the data (both the information that is passively generated as by-products of people's everyday use of technologies and the information people willingly communicate about

themselves on the web) used for data analysis originate from various heterogeneous sources such as people, machines, or sensors (De Prato and Simon 2015, p. 16), analytical techniques applied to very large data sets make it technically possible to "re-identify" a person a large percentage of the time: using 15 months of mobile phone records for 1.5 million callers, researchers showed that three or four data points were enough to uniquely identify users approximately 95% of the time (Montjoye *et al.* 2013, p. 1). As illustrated by a report produced for the second Obama administration (Podesta et al. 2014, pp. 51–54) and used in briefings of the European Parliament (Davies 2016, p. 4), the use of this personal data can lead to surveillance, unwanted disclosure of private information, and discriminatory profiling. Uncertainty and the widespread public perception that there are significant risks to the protection of natural persons may constitute obstacles to achieving SDGs that are driven by data analysis technologies. These include the need to address a scientific problem that will be analyzed in this paper: whether sustainability values, for which data and data analysis technologies are used, and human rights to privacy and personal data protection values are coherent or in conflict. Could these values be mutually supportive?

This paper aims to analyze national and international legal documents that regulate privacy and personal data protection, define the main legal principles relating to the processing of personal data, and evaluate interconnections between those principles and sustainable development values. To achieve this goal, three steps will be taken: first, a comparative analysis of national and international legal documents related to privacy and personal data protection will be conducted; next, the formulation of the main principles relating to personal data processing will be examined, along with the context in which this occurs; finally, how the implementation of these principles may impact SDGs, for the achievement of which advanced data analysis is highly supported, will be assessed. This will allow for a conclusion as to whether sustainability values and human rights to privacy and personal data protection could be mutually supportive.

National and international regulations in the field of privacy and personal data protection

Perhaps not even S. D. Warren and L. D. Brandeis themselves could imagine how their article, published in 1890, could have impacted the world in the proceeding centuries. Their arguments justifying the existence of an independent right to privacy, understood as the right to be left alone (Warren and Brandeis 1890), were a background for other scholars to further develop the concept of the right to privacy that consists of three aspects: (1) physical (associated with a space in which a person can be left alone); (2) informational (the ability to control access to information about oneself); and (3) self-determination (the ability to make free decisions about one's own behavior) (Golding and Edmundson 2005, p. 272).

The first time the right to privacy appeared in international human rights law was in Article 12 of the Universal Declaration of Human Rights (UDHR) as one of the fundamental human rights. Soon after the UDHR was adopted, this right was also established in Europe – in Article 8 of the European Convention on Human Rights (ECHR). It is easy to observe that the UDHR and the

ECHR were adopted well before the rise of the internet and the rapid development of ICT that resulted in the explosion of the collection and use of data and the transformation of the way humans live. Increased computational power and sophisticated data analysis techniques make surprising findings, inventions, and innovations possible that improve quality of life, but at the same time they present new threats to the right to respect for private life. Responding to the need for specific regulation limiting the collection and use of personal information, the concept known as *informational privacy* (in legal literature detailed as the right to "informational self-determination" (de Terwangne 2014, p. 121)) was introduced, which is understood as: (a) protection of the person from disturbing information and the disclosure of inaccurate facts about them (Prosser 1971, pp. 802–815); (b) the ability to decide when, how and to what extent personal information may be disclosed to others (Westin 1967, p. 7); (c) a state where others do not have and do not know information about a person who is not public (Parent 1983, p. 269); and (d) the legitimate interest of the person and the real possibility of controlling the information relating to them (DeCew 1997, p. 53). The concept of informational privacy was the main inspiration behind elaborating special legal instruments that provide personal data protection.

While developing informational privacy frameworks, two different approaches were formed. According to European Union Agency for Fundamental Rights and the Council of Europe (EUAFRCOE 2018, p.18), by the end of the 1980s, several European countries (Sweden, France, Germany, the United Kingdom, etc.) decided to adopt separate laws on personal data protection. This perspective was based on a view that personal data protection is a fundamental human right that generally involves top-down regulation, and the imposition of common rules limiting the use of data or requiring the consent of the person for that use (Podesta *et al.* 2014, p. 17). In contrary to them, the United States (U.S.), because of its constitutional structure emphasizing negative liberties instead of positive liberties, addressed personal data issues through ad hoc, sector-by-sector solutions (Murray 1997, p. 970). These sector-specific laws create privacy safeguards that apply only to specific types of entities and data (Boyne 2018, p. 299) when it is determined that the particular industry would benefit from oversight, e.g., The 1970 Fair Credit Reporting Act, The 1996 Health Insurance Portability and Accountability Act, The Children's Online Privacy Protection Act of 1998, etc.

As more and more countries began to regulate 'informational privacy' and the processing of personal data in their national laws, the limits of national measures when protecting individuals in cross-border data flows soon became apparent. It did not take long before the Council of Europe drafted a Convention for the protection of individuals with regard to the automatic processing of personal data (Convention 108) in 1981. Convention 108 is binding for those states that have legally ratified it and applies to all data processing activities carried out by private and public entities, including by the judiciary and law enforcement authorities. It aims to protect individuals against abuses that may arise when processing personal data, and seeks to regulate the transborder flows of personal data. It should be noted that Convention 108 is open for acceptance even by third countries who do not belong to the Council of Europe, so Convention 108 has the potential to serve as the universal standard promoting personal data protection at the global level (EUAFRCOE 2018, p. 26).

Although all European Union (EU) member states participate in the Council of Europe as contracting counterparts and have ratified Convention 108, the EU is a unique organization at the global level, and is sometimes even defined as "a compelling experiment in political organization

beyond the nation-state" (Pollack 2005, p. 357). As such, its approach to personal data protection warrants more thorough examination. First, it should be explained that the uniqueness of the EU manifests in the sense that it has developed a complete and coherent system of judicial protection such that the rights derived from EU law can be enforced in court, in contrast to other international organizations where such enforceability is often non-existent (Lenaerts *et al.* 2014, p. 1). In essence, this means that sufficient legal remedies and well-defined procedures exist that allow the enforcement of the rights enshrined in EU law and the assurance of judicial review of the implementation of EU legal acts. As the EU legal system consists of primary and secondary law (the treaties that have been ratified by all EU member states form primary EU law; the regulations, directives, decisions, recommendations, and opinions that come from the principles and objectives of the treaties are known as secondary EU law), an understanding of privacy and personal data protection in primary law is needed because of its impact on secondary law. Originally, the European Economic Community was intended to be a regional organization focused on economic integration with a view to creating a single market, so the first treaties of the European Communities did not provide for a separate catalogue of human rights or any additional mechanisms for their protection (EUAFRCOE 2018, p. 27). When cases came alleging human rights violations in areas within the scope of the European Communities law, it was recognized that its policies could have an impact on human rights. This understanding was a stimulus to drafting the Charter of Fundamental Rights of the European Union (Charter), announced in 2000, which became legally binding as EU primary law when the Treaty of Lisbon, amending the Treaty of the European Union and the Treaty establishing the European Community, came into force on 1 December 2009.

The Treaty of Lisbon brought major changes in the legal structure of the EU, including the elevation of the Charter to constitutional status (Kuner *et al.* 2020, p. 3). The Charter provides the whole range of civil, political, economic and social rights of every EU citizen. These rights not only include guarantees to respect private and family life, but also enshrine the right to the protection of personal data, explicitly raising the level of this protection to that of a fundamental right. Such changes in primary EU law not only separated the right to personal data protection from the right to respect private and family life, but also developed it into qualitative new data protection law and granted the European Union the competence to adopt legislation in the field of data protection (EUAFRCOE 2018, p. 28). This led to further initiatives to modernize previous European Union data protection legislation in attempts to make it fit for the protection of fundamental rights in the context of the challenges that are posed by increased digitalization and the usage of data analysis techniques. In this vein, Regulation (EU) 2016/679 (GDPR) on the protection of natural persons with regard to the processing of personal data and on the free movement of such data was adopted, and Directive 95/46/EC was repealed. Directly applicable in the EU member states, the GDPR provides a single set of data protection rules and creates consistent application throughout the EU, serving as a legal certainty not only for the private and public sector that process personal data, but also for individuals that benefit from the protection it grants when their personal data is processed. The GDPR is even recognized as a global milestone for privacy policy (Lee and Hess 2021, p. 2) and is regarded as "a distillation and comprehensive update of the EU's goals in protecting the rights and freedoms of the people who live within it" (IT Governance Privacy Team 2020, p. 13).

Legal principles relating to the processing of personal data

As was introduced before, it is hard to deny that advanced data collection and innovative data analysis techniques could directly impact the well-being of society and contribute to the achievement of SDGs. While data collection and its further processing is highly promoted (IEAG 2014, pp. 4–5), several scholars (Boyd and Crawford 2012, pp. 673–675; Sharon 2016) and privacy policy makers (Davies 2016, p. 4; Podesta et al. 2014, pp. 51–54) still raise concerns relating to informational privacy. This means that it is essential to understand the default rules of behavior that are expected to be complied with even when personal data is supposed to be processed for the interests of general society, including sustainable development. From the legal theory point of view, the expected behavior could be exposed by analyzing legal principles, as they are basic norms that represent the general consensus of the basic understandings of society (Daci 2010, p. 111). Therefore, this section will analyze the principles relating to informational privacy when personal data is processed. For this analysis, Convention 108 (as not all protocols amending Convention 108 entered into force, in this paper Convention 108 will be analyzed with those amendments that are applicable) is selected, which still remains the only legally binding international instrument in the field of data protection, along with legal documents from the United States and the European Union because of their impact on data processing practice around the world.

Convention for the protection of individuals with regard to automatic processing of personal data (Convention 108)

Chapter II of Convention 108 is dedicated to the "basic principles for data protection." This chapter consists of 8 articles (from Article 4 to Article 11), but only Article 5 contains basic requirements of behavior when processing personal data, which in this article are attributed to the "quality of data." Other articles of this Chapter describe: (1) duties and obligations of the contracting parties when implementing Convention 108 provisions to their national laws (Article 4, 9, 10 and 11); (2) categories of data (defined as "sensitive data") that deserve greater protection because of their link to increased risk of harm for the individual (Article 6); (3) safety obligations requiring the implementation of adequate measures for the protection of personal data (Article 7); and (4) safeguards that have to be enabled for data subjects when their personal data are processed (these safeguards enshrine individuals' rights in data processing activities) (Article 8).

Article 5 of Convention 108 provides five main legal requirements that have to be observed while personal data undergoes automatic processing: obtained and processed fairly and lawfully; stored for specified and legitimate purposes; adequate, relevant and not excessive; accurate and kept up to date; and entailing permission for identification of the data subjects for no longer than is required.

The relevant regulation in the U.S.

As mentioned in Section 1 of this paper, the U.S. follows a sectoral approach to informational privacy protection. Instead of all-encompassing federal legislation that ensures the privacy and protection of personal data, legislation at the federal level primarily protects data within sector-specific contexts (Boyne 2018, p. 299). The first legislation relating to informational privacy in the U.S. was enacted in 1970 – The Fair Credit Reporting Act. Until now, this aimed to promote accuracy, fairness, and privacy protection with regard to the information assembled by consumer reporting agencies for use in credit and insurance reports, employee background checks, and tenant screenings (Podesta *et al.* 2014, p. 18). Even the approaches of sector-based informational privacy protection laws require general considerations about requirements that have to be introduced to provide basic protection for handling personal data by various data analysis techniques. In this regard, the Secretary's Advisory Committee on Automated Data Systems of the U.S. Department of Health, Education, and Welfare analyzed the harmful consequences that might result from automated personal data systems and recommended to the government the enacting of a Code of Fair Information Practices (The U.S. Department of Health, Education, and Welfare 1973, p. 50) that is based on five basic principles. Serving as certain safeguards for the use of information, these are known as the Fair Information Practice Principles or FIPPs.

Even though the FIPPs were successfully instantiated in many sectoral laws, in 2012 the White House observed that this framework lacks both a clear statement of the basic privacy principles that apply and a sustained commitment of all stakeholders to addressing consumer data privacy issues (The White House 2012). Considering this, the Administration introduced the Consumer Privacy Bill of Rights and called for Congress to adopt legal acts that implement the Consumer Privacy Bill of Rights to private sectors that are not subject to existing data privacy laws. The Consumer Privacy Bill of Rights reflects the FIPPs and supplements them by holding that consumers have a right to: 1) individual control; 2) transparency; 3) respect for context; 4) security; 5) access and accuracy; 6) focused collection; and 7) accountability.

In the Consumer Privacy Bill of Rights, the enshrined consumer rights clearly present default rules of behavior that have to be complied with by the private sector when the personal data of a consumer is processed. In essence, they are considered legal principles relating to the processing of personal data.

The legal framework in the EU

In the EU, the right to personal data protection constitutes a fundamental human right, and with the Treaty of Lisbon the EU has a specific legal basis for data protection legislation in Article 16 of the Treaty on the Functioning of the European Union. This grants the European Parliament the rights to oversight of and participation in data protection policy-making (Kuner *et al.* 2020, p. 3). With these developments, debates on the need to modernize European Union data protection rules began, and the long legislative process of negotiations between the European Parliament and the Council of the European Union finished in 2016 when the GDPR was adopted. The GDPR

is directly applicable in the EU member states, which are also obliged to update their existing national data protection laws to fully align with the regulation.

In the GDPR, default rules of behavior that are expected to be complied with when personal data is processed are enshrined in Article 5 as "Principles relating to processing of personal data." This article encompasses seven basic legal principles that have to be applied to the processing of personal data wholly or partly by automated means, and to the processing of personal data other than by automated means, which form part of a filing system or are intended to form part of a filing system: 1) lawfulness, fairness and transparency; 2) purpose limitation; 3) data minimization; 4) accuracy; 5) storage limitation; 6) integrity and confidentiality (or security); and 7) accountability.

When comparing Convention 108 in the U.S. to the principles providing the protection of personal data in the EU legal framework, it should be noted that the GDPR does not make fundamental changes in the field of personal data protection (de Terwangne 2020, p. 311) and the principles laid down in Convention 108 (based on the FIPPs) have proven to be sound in their application (Kotschy 2014, p. 277). The main difference can be seen in the enforcement mechanisms of these principles: while Convention 108 is legally binding for contracting parties, to what extent the principles are endorsed still depends on the country's national law. In the U.S., the implementation of principles relating to personal data processing depends on the adoption of sector-based laws; in the EU, the GDPR is directly applicable, and judicial remedies exist to enforce its application.

The implementation of principles relating to personal data processing

From international organizations (IEAG 2014, pp. 4–5) to researchers (Belaud *et al.* 2019; Bibri 2021, pp. 36–37; Chen 2019, pp. 18–19), it is encouraged to use innovative data analysis technologies while monitoring and achieving SDGs. Although data analysis initiatives are continuously supported and highly demanded, the human rights to privacy and personal data protection values raise concerns about the risks that could be posed by unprecedented data processing that could be linked to an individual person and could lead to surveillance, the unwanted disclosure of private information, and discriminatory profiling (Montjoye *et al.* 2013, p. 1; Davies 2016, p. 4; Podesta *et al.* 2014, pp. 51–54). This section will consider how sustainability values and human rights to privacy and personal data protection impact each other, and whether they could be mutually supportive while implementing principles relating to personal data processing.

The implementation of principles relating to personal data processing in the entire system of data processing activities is usually defined as *privacy-friendly* data processing. This term encompasses the commitment to ensuring privacy and personal data protection during the whole life cycle of data processing. Privacy-friendly personal data processing, in the context of sustainable development, means that privacy and personal data protection are highly valued, and the achievement of SDGs respects these values – even if this means that some sustainability initiatives should be

abandoned or modified because of their inadequate intrusion into an individual's informational privacy field (with a negative impact on sustainable development).

One of the most basic principles relating to personal data processing that is laid down in legal documents is the requirement to process personal data lawfully, fairly and in a transparent manner. In this context, lawfully means that personal data processing respects all applicable legal requirements (de Terwangne 2020, p. 314). Fairness implies that personal data processing operations must not be performed in secret, and that data subjects should be aware of potential risks. This is more like the requirement to process personal data in an ethical manner (EUAFRCOE 2018, p. 119). The transparency of personal data processing is explained as the obligation to provide clear information to the data subject about processing: what personal data is collected, why this data is needed, how it will be used, when it will be deleted, and whether and for what purposes it may be shared with third parties (The White House 2012, p. 47). In essence, this means that each initiative to enable data and innovative data analysis techniques for the achievement of SDGs should be carefully assessed in terms of whether there is legal ground for such a form of processing and what information was provided to the data subject in relation to the intended personal data processing. As these requirements can be easily implemented, they should not be obstacles when seeking sustainable development.

The principle of "purpose limitation" (or "respect for context") has long been regarded as the backbone of personal data protection and is connected with transparency, predictability and user control (EUAFRCOE 2018, p. 122). This principle has two aspects: 1) "purpose specification," requiring personal data to be collected for specified, explicit and legitimate purposes; and 2) "compatible use," prohibiting further processing of personal data in a manner that is incompatible for those purposes (de Terwangne 2020, p. 315). These two aspects are linked to the data subject's expectation that personal data is processed in ways that are known to them. This requires the definition of the specific purposes for which personal data is processed before the start of its collection. In the context of sustainable development, this principle means that data collected for a specific purpose linked to sustainable development cannot automatically be used for other related initiatives because of the obligation to evaluate compliance with the requirements of purpose specification and compatibility. If this evaluation shows incompatibility with the initial purposes, then personal data that has already been processed shall not be used for that particular initiative related to sustainable development, and a new data processing system has to be established. From the sustainable development point of view, this could be criticized because of the possible duplication of data that could lead to a larger environmental footprint (Lucivero 2020, pp. 1013–1016).

In the field of sustainable development, it is recognized that high-quality data used to create information that can track progress, monitor the use of resources, and evaluate the impacts of policy and programmes on different groups is a key ingredient in creating more mutually accountable and participatory structures to monitor the achievement of goals (IEAG 2014, p.20). The quality of data can be elevated if the data protection principles of "data minimization" and "accuracy" are implemented in data processing systems. The principle of "data minimization" means that "personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed" (Article 5 (1) (c) of the GDPR); in other words, there are limits on personal data that is collected. These limits are defined taking into account the purpose

for which data is collected and the requirement of grounding the data that is needed to achieve set goals. The requirement that personal data be accurate is mostly linked to the risk of adverse consequences to individuals if the data is inaccurate. This principle also requires that reasonable steps be taken to keep the data up to date and rectify inaccurate data – or, if that is not possible, erase it. Accordingly, the implementation of these principles can be significant for sustainability for two reasons: 1) it allows for the reasonable expectation that the data collected will be of a high quality and suitable for sustainability goals (via the assessment of whether this data is necessary for the purposes that they are collected and the accuracy check); and 2) because irrelevant data will not be collected, it reduces the burden on information and computing technologies and saves their manufacturing and maintenance resources, which is essential when talking about sustainable development (Williams 2011).

The "storage limitation" principle in personal data protection implies the prohibition of storing personal data in a form which permits the identification of individuals beyond the time necessary to achieve processing purposes. The data must be erased or anonymized when those purposes have been served. Time limits for erasure or for a periodic review should be established, but these limits only apply to data kept in a form which permits the identification of data subjects. The incorporation of this data protection principle into data analysis systems in general could define the exact end of the data life cycle and serve as a tool to monitor its application. It can also serve as a commitment to discard excessive data that is of no added value and uses limited resources.

The principle of "integrity and confidentiality" or "security" defines the requirement to ensure appropriate organizational and technical security measures to protect an individual's data against accidental, unauthorized or unlawful access, use, modification, disclosure, loss, destruction or damage. Depending on the specific circumstances of each individual case, appropriate technical and organizational measures could include different elements – for example, pseudonymisation and encryption of personal data and/or the regular assessment of the effectiveness of the measures to ensure that data processing is secure (Article 32 (1) of the GDPR). As this principle mostly relates to how to establish a secure, risk-based data management system within organizations, from the sustainable development point of view the implementation of this principle could be beneficial to ensure the quality of data. It also provides assurance that data used for sustainable development or measuring the achievement of its goals has not been modified, lost, destroyed or damaged.

The last principle relating to personal data processing is "accountability." This is more of a general rule stating that the data controller is responsible for compliance with all the previous principles. This principle is understood as an active demonstration that measures which would guarantee that data protection rules are adhered to in the context of processing operations are established, and those measures are documented. As "accountability" is more related to the distribution of responsibilities and the active demonstration of actions taken to protect personal data, it has no direct link to sustainable development.

Conclusions

Data collection and storage covering the entire life cycle of a person or device were important and ground-breaking developments in many domains. The potential of processing large amounts of data for monitoring and achieving SDGs has been presented as a solution to societal challenges, and data are considered a resource for societal improvement and growth and a means by which to promote societal well-being. This approach soon received criticism not only from a number of environmental scientists, but also from various researchers and policy-makers who addressed a series of privacy and personal data protection concerns. This led to the question of whether sustainability values, for which data and data analysis technologies are used, and human rights to privacy and personal data protection are coherent or in conflict – could these values be mutually supportive? Legal analysis shows that to preserve the human rights to privacy and personal data protection there are rules of behavior that have to be complied with – legal principles relating to personal data processing – when personal data is processed. The application of these principles encompasses a commitment to ensuring privacy and personal data protection, and can impact data processing activities during the whole life cycle of data. As such, sustainability, which is highly supported by increased demands to process data for the wellbeing of society, can be directly affected by the implementation of legal principles relating to personal data processing. While some of these principles can be considered neutral in terms of how they relate to sustainable development (e.g., the "lawfulness, fairness and transparency" principle, or the "accountability" principle), other principles – such as "data minimization," "accuracy," "storage limitation" and "integrity and confidentiality" – can be supportive to sustainable development. This is because they serve as prerequisites to the use of high-quality data to measure the achievement of SDGs ("data minimization," "accuracy," "storage limitation" and "integrity and confidentiality") or to reduce the burden on ITC and save on manufacturing and maintenance resources – an essential factor when thinking about sustainable development ("data minimization," "accuracy," "storage limitation"). The principle of "purpose limitation" can be criticized from the sustainable development point of view because of the possible duplication of data that could lead to a larger environmental footprint. The exact impact of the implementation of these principles in the data processing systems used for sustainable development could be an important topic for future research.

References

BELAUD, J.-P., N. PRIOUX, C. VIALLE & C. SABLAYROLLES, 2019. Big Data for Agri-food 4.0: Application to Sustainability Management for By-products Supply Chain. *Computers in Industry*, 111, 41–50. https://doi.org/10.1016/j.compind.2019.06.006.

BERKHOUT, F., & J. HERTIN, 2004. De-materialising and Re-materialising: Digital Technologies and the Environment. *Futures*, 36 (8), 903–920. https://doi.org/10.1016/j.futures.2004.01.003.

BIBRI, S.E., 2021. Data-driven Smart Eco-cities and Sustainable Integrated Districts: A Best-evidence Synthesis Approach to an Extensive Literature Review. *European Journal of Futures Research*, 9 (1), 1–43. https://doi.org/10.1186/s40309-021-00181-4.

BOYD, D., & K. CRAWFORD, 2012. Critical Questions for Big Data. *Information, Communication & Society*, 15 (5), 662–679. https://doi.org/10.1080/1369118X.2012.678878.

BOYNE, S.M., 2018. Data Protection in the United States. *The American Journal of Comparative Law*, 66, 299–343. https://doi.org/10.1093/ajcl/avy016.

CESCHIN, F., & İ. GAZIULUSOY, 2020. *Design for Sustainability: A Multi-level Framework from Products to Socio-technical Systems*. Abingdon, Oxon: Routledge (Routledge Focus on Environment and Sustainability). Available from: https://search-ebscohost-com.skaitykla.mruni.eu/login.aspx?direct=true&db=e001mww&AN=2144374&site=ehost-live [Accessed 13 April 2022]. https://doi.org/10.4324/9780429456510.

CHEN, W., 2019. An Overview: The Past, Present and Future of Digital Health. In: A. Liu, A.(A). Farzindar & M. Gong, eds. *Transforming Healthcare with Big Data and AI*. Charlotte, NC: Information Age Publishing, Inc. Available from: https://search-ebscohost-com.skaitykla.mruni.eu/login.aspx?direct=true&db=e000xww&AN=2296107&site=ehost-live [Accessed 13 April 2022].

COTTRILL, C.D., & S. DERRIBLE, 2015. Leveraging Big Data for the Development of Transport Sustainability Indicators. *Journal of Urban Technology*, 22 (1), 45–64. https://doi.org/10.1080/10630732.2014.942094.

DACI, J., 2010. Legal Principles, Legal Values and Legal Norms: Are They the Same or Different? *Academicus International Scientific Journal*, MMX, 109–115. https://doi.org/10.7336/academicus.2010.02.11.

DAVIES, R., 2016. *Big Data and Data Analytics: The Potential for Innovation and Growth*. European Parliament, Members' Research Service. Available from: https://www.europarl.europa.eu/RegData/etudes/BRIE/2016/589801/EPRS_BRI(2016)589801_EN.pdf [Accessed 13 April 2022].

DE PRATO, G., & J.P. SIMON, 2015. The Next Wave: "Big Data"? *Communications & Strategies*, 97, 15–39.

DE TERWANGNE, C., 2014. The Work of Revision of the Council of Europe Convention 108 for the Protection of Individuals as Regards the Automatic Processing of Personal Data. *International Review of Law, Computers & Technology*, 28 (2), 118–130. https://doi.org/10.1080/13600869.2013.801588.

DE TERWANGNE, C., 2020. Chapter II: Principles (Article 5–11). In: C. Kuner, L.A. Bygrave, C. Docksey & L. Drechsler, eds. *The EU General Data Protection Regulation (GDPR): A Commentary*. New York: Oxford University Press, 309–320.

DECEW, J.W., 1997. *In Pursuit of Privacy: Law, Ethics, and the Rise of Technology*. Ithaca, NY: Cornell University Press. https://doi.org/10.7591/9781501721243.

EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS AND COUNCIL OF EUROPE (EUAFRCOE), 2018. *Handbook on European Data Protection Law: 2018 Edition*. Luxembourg: Publications Office of the European Union. Available from: https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_en.pdf [Accessed 13 April 2022].

GANTZ, J., & D. REINSEL, 2012. *The Digital Universe in 2020: Big Data, Bigger Digital Shadows, and Biggest Growth in the Far East* [online]. IDC iVIEW. Available from: https://www.cs.princeton.edu/courses/archive/spring13/cos598C/idc-the-digital-universe-in-2020.pdf [Accessed 13 April 2022].

GOLDING, M.P., & W.A. EDMUNDSON, eds. 2005. *The Blackwell Guide to the Philosophy of Law and Legal Theory*. Malden: Blackwell Publishing. https://doi.org/10.1002/9780470690116.

HEDSTROM, G.S., 2018. *Sustainability: What It Is and How to Measure It*. Boston: De Gruyter. Available from: https://search-ebscohost-com.skaitykla.mruni.eu/login.aspx?direct=true&db=e000xww&AN=1927033&site=ehost-live [Accessed 13 April 2022]. https://doi.org/10.1515/9781547400423.

INDEPENDENT EXPERT ADVISORY GROUP ON A DATA REVOLUTION FOR SUSTAINABLE DEVELOPMENT (IEAG), 2014. *Mobilising the Data Revolution for Sustainable Development*. Available from: https://www.undatarevolution.org/wp-content/uploads/2014/11/A-World-That-Counts.pdf [Accessed 13 April 2022].

IT GOVERNANCE PRIVACY TEAM, 2020. *EU General Data Protection Regulation (GDPR) – An Implementation and Compliance Guide, Fourth Edition*. Ely, Cambridgeshire: ITGP. Available from: https://search-ebscohost-com.skaitykla.mruni.eu/login.aspx?direct=true&db=e000xww&AN=2641163&site=ehost-live [Accessed 13 April 2022]. https://doi.org/10.2307/j.ctv17f12pc.

KOTSCHY, W., 2014. The Proposal for a New General Data Protection Regulation – Problems Solved? *International Data Privacy Law*, 4 (4), 274–281. https://doi.org/10.1093/idpl/ipu022.

KUNER, C., L.A. BYGRAVE & C. DOCKSEY, 2020. Background and Evolution of the EU General Data Protection Regulation (GDPR). In: C. Kuner, L.A. Bygrave, C. Docksey & L. Drechsler, eds. *The EU General Data Protection Regulation (GDPR): A Commentary*. New York: Oxford University Press, 1–47. https://doi.org/10.1093/oso/9780198826491.001.0001.

LEE, D., & D.J. HESS, 2021. Data Privacy and Residential Smart Meters: Comparative Analysis and Harmonization Potential. *Utilities Policy*, 70, 101188. https://doi.org/10.1016/j.jup.2021.101188.

LENAERTS, K., I. MASELIS, K. GUTMAN & J.T. NOWAK, 2014. *EU Procedural Law*. Oxford: OUP Oxford.

LUCIVERO, F., 2020. Big Data, Big Waste? A Reflection on the Environmental Sustainability of Big Data Initiatives. *Science & Engineering Ethics*, 26 (2), 1009–1030. https://doi.org/10.1007/s11948-019-00171-7.

MARR, B., 2018. *Here's Why Data Is Not the New Oil* [online]. *Forbes*, March 5. Available from: https://www.forbes.com/sites/bernardmarr/2018/03/05/heres-why-data-is-not-the-new-oil/?sh=25e4643d3aa9 [Accessed 13 April 2022].

MONTJOYE, Y.-A.D., C.A. HIDALGO, M. VERLEYSEN & V.D. BLONDEL, 2013. Unique in the Crowd: The Privacy Bounds of Human Mobility. *Scientific Reports*, 3, 1376. https://doi.org/10.1038/srep01376.

MURRAY, P.J., 1997. The Adequacy Standard Under Directive 95/46/EC: Does U.S. Data Protection Meet This Standard? *Fordham International Law Journal*, 21 (3), 932–1018.

PARENT, W.A., 1983. Privacy, Morality and the Law. *Philosophy & Public Affairs*, 12(4), 269–288.

PODESTA, J., P. PRITZKER, E.J. MONIZ, J. HOLDREN & J. ZIENTS, 2014. *Big Data: Seizing Opportunities, Preserving Values*. Washington: Executive Office of the President. Available from: https://obamawhitehouse.archives.gov/sites/default/files/docs/big_data_privacy_report_5.1.14_final_print.pdf [Accessed 13 April 2022].

POHL, J., L.M. HILTY & M. FINKBEINERD, 2019. How LCA Contributes to the Environmental Assessment of Higher Order Effects of ICT Application: A Review of Different Approaches. *Journal of Cleaner Production*, 219, 698–712. https://doi.org/10.1016/j.jclepro.2019.02.018.

POLLACK, M.A., 2005. THEORIZING THE EUROPEAN UNION: International Organization, Domestic Polity, or Experiment in New Governance? *Annual Review of Political Science*, 8 (1), 357–398. https://doi.org/10.1146/annurev.polisci.8.082103.104858.

PORTNEY, K.E., 2015. *Sustainability*. Cambridge, Massachusetts: The MIT Press.

PROSSER, W.L., 1971. *Handbook of the Law of Torts*. St. Paul: West Publishing.

REINSEL, D., J. GANTZ & J. RYDNING, 2018. *Data Age 2025: The Digitization of the World from Edge to Core* [online]. Available from: https://www.seagate.com/files/www-content/our-story/trends/files/idc-seagate-dataage-whitepaper.pdf [Accessed 13 April 2022].

ROWLAND, Z., & K. PORTER, 2021. Autonomous Vehicle Driving Algorithms, Deep Learning-based Sensing Technologies, and Big Geospatial Data Analytics in Smart Sustainable Intelligent Transportation Systems. *Contemporary Readings in Law and Social Justice*, 13 (2), 23–36. https://doi.org/10.22381/CRLSJ13220212.

SHARON, T., 2016. The Googlization of Health Research: From Disruptive Innovation to Disruptive Ethics. *Personalized Medicine*, 13 (6), 563–574. https://doi.org/10.2217/pme-2016-0057.

THE U.S. DEPARTMENT OF HEALTH, EDUCATION, AND WELFARE, 1973. *Records, Computers, and the Rights of Citizens*. Washington D.C.: DHEW. Available from: https://www.justice.gov/opcl/docs/rec-com-rights.pdf [Accessed 13 April 2022].

THE WHITE HOUSE, 2012. *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*. Washington: The White House. Available from: https://obamawhitehouse.archives.gov/sites/default/files/privacy-final.pdf [Accessed 13 April 2022].

UNITED NATIONS, 2016. *Sustainable Development Goal 12: Ensure Sustainable Consumption and Production Patterns* [online]. Available from: https://www.un.org/sustainabledevelopment/sustainable-consumption-production/ [Accessed 13 April 2022].

WARREN, S.D., & L.D. BRANDEIS, 1890. The Right to Privacy. *Harvard Law Review*, 4 (5), 193–220. https://doi.org/10.2307/1321160.

WORLD COMMISSION ON ENVIRONMENT AND DEVELOPMENT (WCED), 1987. *Our Common Future: Report of the World Commission on Environment and Development*. Available from: http://www.un-documents.net/our-common-future.pdf [Accessed 13 April 2022].

WESTIN, A.F., 1967. *Privacy and Freedom*. New York: Atheneum.

WILLIAMS, E., 2011. Environmental Effects of Information and Communications Technologies. *Nature*, 479, 354–358. https://doi.org/10.1038/nature10682.