PRIVACY AS PUBLIC GOOD: ADDRESSING THE COMMON INTEREST IN DATA PROTECTION

Haekal AL ASYARI *

ABSTRACT: *It is well accepted that all aspects of society has been affected by digitization. Issues of privacy and data protection has exceeded individual interests and constitutes major challenges in recent times. Due to the complex interrelations between state, businesses, and citizens, data protection has become a shared concern and responsibility. The protection of personal data that competes with collective interests of the society warrants a public good dilemma. Based on the study of Fairfield and Engel who has established privacy as a public good, this study will dwell on the further inquiry in the context of legal policy of data protection as a public good. It will discuss in more details on the concept of personal data protection laws between the public and private sphere. Using a normative methodology based on existing literatures, this article re-elaborates the understanding of privacy as public good. It explains further on the common interest shared in privacy and provides contextual example of data protection policy in the European Union. Lastly, it discusses the interrelations between actors of data protection and the shared interests between them.*

KEYWORDS: *privacy, public good, common interest, data protection,*
JEL CODE: *K24*

1. INTRODUCTION

The current normative frameworks that are generally adopted in regulating privacy focuses on empowering individuals.[1] This is reflected by the notion that one's personal

* Doctoral Candidate, Géza Marton Doctorol School of Legal Studies, University of Debrecen. Lecturer, International Law Department, Faculty of Law, Universitas Gadjah Mada.

[1] 'States' in this context refers to the majority of developed and developing states that adopts the western approach of self-regulatory regime such as the European Union. *See* Public International Law of Cyberspace, Kriangsak Kittichaisaree, Law, Governance and Technology Series, Vol.32, Springer, Switzerland, 2017, Roger Brownsword and Morag Goodwin, Law and the Technologies of Twenty-First Century: Text and Materials, Cambridge University Press, Cambridge, 2012, Chris Reed, Making Laws for Cyberspace, Oxford University Press, United Kingdom, 2012, ISBN 978-0-19-965761-2, Cybersecurity Policy in ASEAN Countries, Jirapon Sunkpho, Sarawut Ramjan, Chaiwat Ottamakorn, Information Institute Conferences, Las Vegas, 2018, (Conference Paper), Roger Brownsword, Morag Goodwin, Law and the Technoogies of the Twenty-First Century: Text and Materials, Cambridge University Press, Cambridge, 2012

data is theirs to protect and control. It also reflected in the general acceptance of data protection that is heavily inclined towards self-regulation (Stockmann, 2023). Whereby individuals can decide for themselves which data they share, with whom and for what purposes. This concept gives authority to individuals to determine how much privacy they wish to share with others.

However, an aspect of this concept that is often overlooked is that when a person accepts certain terms and conditions to be a part of a certain network; their acceptances will increase in data flows, as well as technical and economic complexity of the public (Schünemann and Baumann 2017). The contribution of accepting their data to be collected will affect the interest of other parties. This is seen by self-regulation of data protection which reflects the relationship between individual users towards public agencies or the state (Schünemann and Baumann 2017).

Metadata, content, and personal information that are collected by so called data controllers, to which then processed, analysed by data processors are turned for profit by companies by offering individualized services or to design more efficient system in sectors such as healthcare, public transportation, insurance, and many more (Schünemann and Baumann 2017). In this sense, it could be concluded that the interrelations between actors of data protection which are the state/government, businesses, and citizens all share a collective interest and the common good (Schünemann and Baumann 2017).

The extent to which one's 'privacy' could be exercised depends on the context that it is granted, and how much 'redistributive effects' that it produces (Bennett and Raab, 2006). Whether in terms of benefits, security, and risks that it shares not with just individuals, but also companies and even the state. Thus, data protection as an individual goal competes with the common interest of the society. Such common interests include public order, health, security, and ultimately the freedom of others. This becomes the primary reason of why privacy will always have its limitations.

In other words, there exists an individualism bias that exposes the social dimension of privacy (Post, 1989). Historically, individualism in the theory of privacy stems from the right to be left alone and manifested in an individual's control of their own data (Schünemann and Baumann 2017). In the modern notice and choice regime, this right does not apply in favour of individuals, but rather companies. Because people tend to not read what they agree to (Schünemann and Baumann 2017). In the rare case that they do, it could be agreed that protecting one's privacy is socially beneficial. But it does not mean that the protection of one's personal data guarantees the protection of others.

Today's self-regulatory approach at protecting privacy and data focus on empowering individuals. This leaves a gap when an individual is given an almost absolute power to control their data and is reckless with it. One source of risk that is created by one person affect the data and information of others. This is the nature of data processing whereby algorithm, information about one person is always related to another; whether it be a spouse, friend, colleagues who are exposed by big data collection (Schünemann and Baumann 2017). This inattentiveness towards privacy and personal data as public good covers the collective interest in the society.

This article will address the said common interest that is shared between actors of data protection. The first section of this article will elaborate, based on existing literatures on how privacy should be treated as a public good. It will explore the line the is shared by privacy between a public good and public bad. The next section will then discuss the

common interest in privacy, which then followed by an explanation on the relationship between privacy, data protection and cybersecurity. Such discussion will provide examples in the context of the European Union. The next part, which is the core of this article, discusses the common interest that is shared between actors when data protection is considered as public good. Lastly, privacy will be explained as to why it poses a political challenge.

2. PRIVACY AS PUBLIC GOOD

Despite the fact that privacy has existed long before the rule of law in nation states took place, it was not until the 19th – 20th century that the right to privacy was recognized in legal systems (Lukács, 2016). Warren's and Brandei's revelation for the right to privacy as a demand in the new society is a considerable landmark to understanding the principle underlying the rights (Warren and Brandeis, 1890). The claim that they both made is that such 'right to be let alone' was aimed to ensure a person to be protected against unwanted disclosure of private facts, thoughts, and emotions (Prosser, 1960). The position of 'individual' playing a central role in achieving the right to privacy is a pinpoint at highlighting the concept of 'individualism' that is substantially contained in the right to privacy.

This study supports Fairfield and Engel's view that predominant privacy theories creates individualism bias (Fairfield and Engel, 2015). While the right to privacy encompasses social dimensions, it lacks engagement with the social dilemma. The traditional right to privacy does not touch upon the spill over effects of information that is exposed or left unprotected by an individual. It merely focuses on the individual's control of information that originates from or bears on that individual exclusively (Fairfield and Engel, 2015). In other words, this traditional approach to privacy have not considered the fact that the data one person shares about another can form toxic pools of data pollution to which forms a public bad. In this sense, Fairfield and Engel's position on treating privacy as a social dilemma becomes a tool of conceptualizing privacy as public good.

Public good can be understood as a social benefit that risks not being produced because everyone can share in it equally, whether they contribute to or not (Fairfield and Engel, 2015). Some examples of public good includes clean air, drinkable water, safe environment, up to national defence. However, there exists a prejudice that it is against everyone's best interest to expand resources contributing to the production of the good; or otherwise known as social dilemma (Fairfield and Engel, 2015). When an information about one person affects others, it creates a source of risks that is immediate an palpable. For example, the information that we provide to hospitals that may include our personal data such as our name, gender and blood type. There are also other information that are linked towards others, for example mothers or family members name and house address. Another example is one's presence on social media such as Instagram, where the feature of 'tagging' others in a post that contains visual information about them, or patterns of online purchases that are personalized based on geographic locations. By algorithm, information about a spouse, colleague, and friends are exposed, and by revealing interests and disinterests algorithm can predict the behaviour of people which forms a basis for targeted behavioural advertising which creates a potential for abuse by data controllers or processors (Fairfield and Engel, 2015). These information that are accumulated across time

and sources could form toxic pools of data to which contributes to a social dilemma for governing privacy.

Because privacy is a kind of commons that requires some degree of social control to construct and preserve, it also constitutes as a public good. It serves the same social function and provide benefits similar to clean air and national defence (Schwartz, 2011). There is a collective value of privacy where its recognition has some features of a public good that has the interests of government and economy to which its protection is indispensable (Regan, 1995).

3. COMMON INTEREST IN PRIVACY

Privacy is a significant public interest that promotes free expression and a free media necessary for effective democracy, and thus it could sometimes conflict with other important public interests. In cases where breaching an individual's privacy is justified for an important public interest, privacy must give way. Therefore it is essential to have a clear process for balancing competing interests to ensure that new actions do not prioritize privacy over other critical public interests.[2]

Defining privacy boundaries in the digital space requires consideration of three different aspects (Egan, 2022). Firstly, one needs to analyse the boundaries that are currently established by legal regulations. Secondly, it is important to identify boundaries that have not yet been recognized by the law but should be. Lastly, there are practical boundaries that are enforced through technical measures like security software or human actions such as rejecting cookies. These practical boundaries are particularly significant because they directly impact an individual's level of privacy, regardless of the extent of their legal rights (Egan, 2022). Despite vocal opposition to interference with privacy boundaries, several scholars have pointed out that people's behaviour doesn't reflect a significant effort to safeguard these boundaries. In fact, many individuals willingly disclose personal information and openly share intimate details about their lives on the internet (Solove, 2009).

Regan's claim at addressing privacy for having a substantial public value is an ideal explanation to understanding the common interest shared in privacy (Regan, 1995). Approaching privacy as an individual right is a frail stance for privacy policy-making. When privacy is viewed as an individual right, policy-making requires balancing that right against other competing interests or rights (Regan, 1995). Typically, the competing interest is considered a societal interest, with the assumption that the individual has a stake in these interests. This approach puts privacy in a defensive position, with those claiming a privacy violation required to prove that the activity in question does indeed violate privacy and that the social benefit gained from the violation is less significant than the individual harm incurred (Regan, 1995).

Privacy is a shared value, as all individuals value some level of privacy and have common perceptions about privacy. Privacy is also a public value, as it is not only valuable to the individual and society as a whole, but also to the democratic political system (Regan, 1995). The public value of privacy arises not only from its role in protecting individuals

[2] Australian Law Reform Commission, Serious Invasions of Privacy in the Digital Era, ALRC Report 123, 2014, https://www.alrc.gov.au/wp-content/uploads/2019/08/fr123_9._balancing_privacy_with_other_interests.pdf

but also from its usefulness in restraining government power or the misuse of power (Solove, 2009).

4. DEMYSTIFYING THE RIGHTS BETWEEN PRIVACY AND DATA PROTECTION

The complex relationship between the right to privacy and personal data protection raises the question of whether each is a distinct right or whether they are complementary. This is clear from the scholarly discussion surrounding the position of the Right to Private Life and the Right to Personal Data in the EU's Charter of Fundamental Rights (Annelien, Bredenoord, Sloot, and Delden, 2017). Others argued that the right to data protection is an additional right to the right to privacy (Fuster, 2014).

The EU's perception of the right to privacy and the right to personal data protection as distinct rights has changed. The GDPR and CJEU case law both emphasise this. National laws on data protection are frequently referred to as "privacy laws" in traditional data protection instruments of the OECD, for instance.[3] While "data protection by design" and "data protection impact assessment" have replaced earlier "privacy-based" ideas.

Mostert et al., have addressed the differential aspects between the right to privacy and data protection for the context of big data health research (Annelien, Bredenoord, Sloot, and Delden, 2017). In order to understand the complexities of the two, it is perceived that individual rights were to be decoupled from privacy. While both rights guarantee individual rights, their scope and substance differ (Annelien, Bredenoord, Sloot, and Delden, 2017).

The right to data protection encompasses almost all types of personal data protection, regardless of whether the right to privacy is interfered (Kokott and Sobotta, 2013). The interference with the right to privacy is contingent on the nature and context of the particular processing. The right to privacy does not extend to the simple collection of personal information. Rather, it lies within the scope of the right to data protection because it constitutes protection of personal data.[4] Individual rights pertaining to the right to privacy are more context-dependent in nature. The link between the right to data protection and the right to privacy is when the collected data permit very precise conclusions to be drawn about the private lives of the person whose data has been retained, such as their habits of everyday life, permanent or temporary places of residence, daily or other movements, activities performed, social relationships, and the social environments.[5]

The right to privacy does not assure a general right of access to personal data by the data subject.[6] While the right to data protection explicitly guarantees such a right of access, regardless of any interference with the right to privacy, the right to access is not affected by the right to privacy. However, there is a trend towards the ECtHR recognising a general right to data based on the right to privacy, which creates a difficulty in differentiating the substantive protection provided by both rights (Annelien, Bredenoord, Sloot, and Delden, 2017).

---

[3] ECtHR, Khelili v. Switzerland, App no. 16188/07 (18 October 2011)
[4] CJEU, Case C-139/01, Österreichischer Rundfunk and Others, ECLI:EU:C:2003:294, para. 74 and 64
[5] CJEU, Case C-293/12, Digital Rights Ireland, ECLI:EU:C:2014, para 238.
[6] ECtHR, Gaskin v. United Kingdom, App no. 10454/83 (7 July 1989)

The right to data protection is a positive obligation, meaning that states are obligated to take steps to safeguard personal data. While the right to privacy is merely a negative obligation, authorities must refrain from arbitrarily invading the private affairs of individuals (Sloot, 2014). The right to data protection is more comprehensive and systematic than the right to privacy, which is more individualistic. The right to data protection is governed by explicit principles, objectives, and constraints. In addition to the technical aspect of data security protection, accountability of data processors is also required. Thus, the right to data protection transcends the notion of individuals asserting or enforcing their rights (Annelien, Bredenoord, Sloot, and Delden, 2017).

5. PRIVACY AND DATA PROTECTION IN THE EUROPEAN UNION

The rules of data protection have come a long way in the EU since 1970. When Germany adopted the first law concerning the use of personal information by public authorities,[7] Sweden then approved a law on processing of personal information three years later[8] followed by France in 1978.[9] These early examples of regulatory efforts for data protection all began over the concerns of computerization of public authorities and the collecting of information about individuals in centralized data banks. (Naef, 2021).

The development and materialization of personal data protection in the EU was a progressive process. The Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data of the EOCD and the Convention of the Protection of individuals with regard to Automatic Processing of Personal Data of the Council of Europe linked connected the dots of data protection and trade. While Directive 95/46/EC initiated the formal commitments to fundamental rights in the EU, producing the right to private life in the European Charter of Human Rights. The realization towards the importance of protecting fundamental human rights in relation to the changes in society, social progress and technological development became a strong reason for developing a substantial data protection framework in the EU (Naef, 2021).

The right to data protection in the EU are based on foundational values that are inherently individualist. We have established that privacy is one of them and it significantly overlaps (Naef, 2021). In addition to privacy, other values includes; informational self-determination which ensures a person's dignity, personal liberty and autonomy (Naef, 2021). Transparency which strive to bring balance between data subjects and data controllers. Democracy, where data protection rules foster the capacity of individuals to freely make their decisions and protect their political freedom(Naef, 2021).

According to the value of informational self-determination, the level of privacy is determined by the ability of individuals to decide which data they want to share, with whom and for what purpose. This sums up the position of data protection as an instrument of privacy protection. At this point in time, the current regime of data protection in Europe is largely based on the notion of 'user content' and control, or in other terms; self-regulation (Schonberger, 2013). In self-regulation, individuals consensually accept the

[7] Hessisches Datenschutzgesetz vom 7. Oktober 1970, Gesetz- und Verordnungsblatt für das Land Hessen Teil I, Nr. 41, 625 vom 12. Oktober 1970

[8] Datalag av. den 11 maj 1973, Svensk författningssamling 1973:289.

[9] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, Journal Officiel de la République Française, 227 du 7 janvier 1978.

terms that they wish to be a part of a vast community of network. This participation increases data flows and adds to the technical and economic complexity of data collection. When one's personal data are pooled with others, it is no longer a matter of individual consent on whether or not their data are connected to others.

The GDPR which was enacted in 2018, aims for harmonization, legal certainty, and tech-neutrality, ensuring long-term application to short and mid-term technological innovations (Felkner et.al., 2021). Personal data processing by controllers and processers which are established in the GDPR is irrespective of where the processing takes place and of their establishment. This rule is intended to cover a broader reach of the GDPR to include non-EU businesses and organizations processing the data of EU citizens, including the activities of behavioural monitoring provisions of goods and services.[10]

Personal data in the GDPR refers to any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. The approach that the GDPR has taken is focused on the concept of 'identifiable persons' and are by default to be controlled by those persons, even if the data do not implicate privacy or reputation.[11]

The GDPR specifies a number of justifications for processing personal data, each of which serves distinct purposes and interests. These includes individual consent, contractual obligation, legal obligation, protecting vital and public interest, as well as legitimate interest.[12] It is worthy to note the last two basis in which the GDPR detaches individual private interest in data processing. It is either when public authorities or organizations requires specific purposes such as public health, research, or the administration of justice, or when there is a legitimate reasons to override the data subjects' fundamental right to data protection legitimately.[13] These two grounds of processing personal data can be considered as an attempt to balance the relevant interests of data processors.

It is important to highlight that the GDPR recognises certain circumstances in which personal data may be processed for communal purposes without explicit consent. This provision does not indicate that the GDPR has strayed from its original goal of protecting privacy. Instead, it demonstrates that the protection of personal data is not restricted to the preservation of individual ownership and control over such data.

The GDPR recognises that there may be instances in which publicly available or accessible personal data may be processed for communal purposes. This could include instances in which data is utilised for purposes of public interest, research, or statistical analysis. The regulation recognises that the protection of personal data in these circumstances extends beyond the strict confines of private ownership and control. By permitting non-consensual processing for certain communal purposes, the GDPR recognises that the protection of personal data serves a larger societal interest. It

[10] GDPR Art. 3
[11] (GDPR art. 4)
[12] (GDPR art. 6).
[13] GDPR Hub, https://gdprhub.eu/Article_6_GDPR#(f)_legitimate_interest

emphasises that the regulation seeks to establish a balance between the protection of privacy rights and the facilitation of legitimate data uses for the common good. This strategy reinforces the notion that data protection encompasses public interest and the greater benefit in addition to individual control.

Thus, the GDPR's provision for the non-consensual processing of personal data for certain communal purposes does not undermine its primary purpose of protecting privacy. Instead, it emphasises that the regulation recognises the significance of striking a balance between privacy rights and communal interests, ensuring that personal data is protected even when it is publicly accessible and used for purposes that benefit the entire society.

The GDPR restricts the processing of special categories of personal data, which include data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data used to uniquely identify a natural person, and data relating to a natural person's health or sex life or sexual orientation. The general norm is that such data cannot be processed unless certain conditions are met. The explicit assent of the data subject is one of the most important requirements for processing special categories of personal data. Individuals must provide clear and unambiguous authorization for the processing of their sensitive data in order for explicit consent to apply. This ensures that individuals have complete knowledge and control over the disclosure and use of their sensitive information, allowing them to make informed decisions regarding its disclosure and use.

Explicit consent places a significant emphasis on individual autonomy and privacy, recognising the sensitive nature of the data involved. Individuals must actively and knowingly consent to the processing of their sensitive data, and organisations must explicitly communicate the purpose and scope of the data processing. By requiring explicit consent for the processing of special categories of personal data, the GDPR seeks to give individuals a high degree of control over their sensitive information. This measure protects against potential excesses or discriminatory practises that could result from the processing of sensitive data without the explicit knowledge and consent of the individuals involved.

6. PRIVACY AS PUBLIC GOOD: COMMON INTEREST IN DATA PROTECTION

The number of literatures pointing out the limitation of privacy and constraints of ‘individualism’ in data protection is adequate to state the existence of the inherent ‘public’ aspect in data protection rules (Regan, 1995) (Naef, 2021). Joshua and Christoph argued that there is a gap in law and policy whereby individuals are blinded from their own vulnerabilities which are caused by others who are careless with personal data. In this sense, the simple argument that is put forward is that one’s personal data is subject to the protection of others. By this logic, the protection of an individual’s personal data requires group cooperation and coordination. The failure of such coordination will result in the failure of privacy. This becomes the basis for addressing such gap by treating privacy as a public good.

For a data-driven society to succeed, it is important to ensure that data is properly protected and not misused by whomever has access to them. There are numerous ways in which data could be abused, ranging from setting higher insurance premiums based on an individual’s shopping history, to limiting user choices in creating information bubbles that

affect the entire society. When personal data is shared and collected by responsible data controllers, it could be utilized for benefits (for researches and public surveys) and increase economic welfare. However when it is abused, it could lead to massive human right violations and criminal offences (Lane, 2013). In other words, the pooling of personal data can create a public good with societal benefits occurring from big data (Lane, 2013).

In order to ensure the common interest in data protection, policy approaches must balance between ensuring necessary data readily available for the public good and safeguarding the privacy and rights of individuals (Lane, 2013). Citizens, businesses, and the state all share a collective interest in this respect. Baumann and Schünemann described this interrelations as "ménage à trois". The Regulation and self-regulation of data protection reflects the relationships of individual users or citizens towards public agencies of all sorts or the state.

In the first leg of this relationship, the concept of privacy is heavily associated with government control. Taking the classical origin of privacy (and data protection) as a liberal defensive law, it reserves the scope for public interest and the expectation of privacy. It places privacy as a fundamental right to protect individuals from the intrusive surveillance from the state.

The second leg of relationship concerns data as an important source of economic activity between users and service providers. Metadata, content, and personal information are gathered, processed and analysed by companies and businesses for profit in order to offer personalised services in sectors such as healthcare, public transportation and insurance. While this might contribute to growing the economy, there is a high risk of data abuse in surveillance and undermining informational self-determination (Schünemann and Baumann 2017).

Lastly, the relationship between state and businesses encompasses a dilemmatic and overlapping interest over data protection and surveillance. On the one hand, state and businesses tend to collaborate in terms of intelligence and criminal investigations concerning individuals' data. On the other, businesses also tend to uphold privacy claims of their users. Nevertheless, state remains a primary actor in regulating the relationship in this ménage à trois (Schünemann and Baumann 2017).

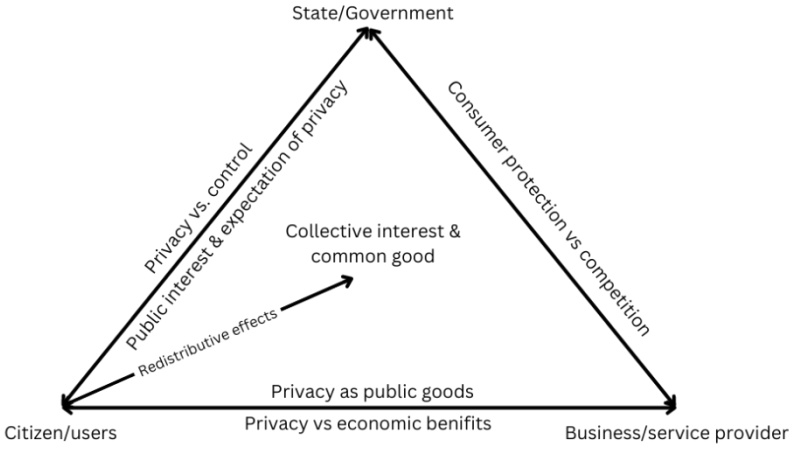

Figure 1. Interrelationship and interests in privacy data protection

Returning to the context of GDPR, the attempt at balancing data protection between private and collective interest could be seen by the rules exempting consent (Park, 2021). Data protection may consider personal data as a commodity or service made available to all members where individuals cannot be excluded from enjoying the benefits. This encompasses information that shared and used by all individuals; for example in the purpose of scientific research, public records, and statistics. This position also places personal data as non-excludable and non-rivalrous.

For personal data that involves personal information, such as name, addresses, social security number, health records and financial data, when they are consented to be processed it therefore becomes excludable. Individual possess a right to control and limit others from using it. Personal data belonging to an individual that has not been given to any data controller or has not been 'excluded' by way of their right to control, is still considered as a private good. But once such data is given consent to, collected, integrated, and processed, to become information that has benefit to the general public, this is when such data becomes public.

In Google Spain vs AEPD and Costeja, the CJEU highlights the balancing interest between data subject's right to personal data. The Court ruled that a search engine is considered a "controller" in relation to the "processing" of personal data, which occurs through its actions of locating, indexing, storing, and distributing said information. It was asserted that to ensure the safeguarding of privacy rights and personal data protection, search engine operators may be obligated to eliminate personal information that has been published by third-party websites. However, users' right to access personal information must be balanced depending on the nature of the information in question and its sensitivity for the data subject's private life and on the interest of the public in having that

information.[14] To this end, personal data that has been given consent to, disclosed publicly, by whichever lawful process, and is not defamatory, privacy infringing should always be considered public.

The loosening of ownership-like control on a subject's personal data is a manifestation of detaching personal data from the concepts of private good. When data protection exempts the consent requirement for the use of data for **'**communal' purposes of the society shifts its purpose to become a public good. Specifically, in the GDPR, data controllers may subject personal data to further processing if it is processed in a manner that is not incompatible with' the original purposes for which the data was collected, reflecting a broader scope of further processing beyond the original purpose (Park, 2021).

There exists an inherent benefit of personal data for community purposes (Park, 2021). This is particularly apparent in the aspect of 'further processing' under the GDPR.[15] So long as the processing for a new purpose or off-purpose processing is in a manner consistent with the original purpose (moderated by additional requirement of data minimization and pseudonymization), there is an intention that such data is afforded for non-consensual use in the interest of public such as scientific and historical research, as well as statistics. The balancing of social and individual interest in setting this scope is intended by legislators to give some flexibility on the concept of private ownership of personal data. The fact that further processing is for a different purpose does not necessarily mean that it is automatically incompatible and is determined on a case-to-case basis. This additional flexibility may be needed to allow for a change of scope or focus on situations where the expectations of society or data subject themselves have changed**.**

Thus, there is a limit to treating personal data protection as a private good. Fitting into the public goods context of non-rivalrous nature; so long as data is the result of interaction between you and another person who perceived you or your features, there is no right reason to why you should own data about yourself (Park, 2021). Data is created for transferability, making personal data to not only for keeping, but to also for sharing and receiving (Kerry and Morris, 2019).

7. CONCLUSION

The concept of privacy is multifaceted and encompasses both individual and societal interests. While individuals have the right to protect and control their personal data, there are inherent limitations due to the complex nature of data flows and the redistributive effects it produces. The social dimension of privacy highlights the need to balance individualism with the common interests of society, such as public order, health, security, and the freedom of others. Privacy is not only a shared value among individuals but also a public value that plays a crucial role in restraining government power and safeguarding democratic political systems.

The right to privacy and the right to data protection are closely intertwined but have distinct characteristics. The right to privacy is a negative obligation, requiring authorities to refrain from arbitrarily invading private affairs, while the right to data protection is a

[14] Judgment of the Court (Grand Chamber), 13 May 2014. Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González., para.81

[15] GDPR, Recital 50,

positive obligation that mandates states to safeguard personal data. The right to data protection goes beyond individual enforcement and includes principles, objectives, and constraints for comprehensive data security and accountability of data processors.

The General Data Protection Regulation (GDPR) recognizes the balance between privacy rights and communal interests by permitting non-consensual processing of personal data for certain communal purposes, such as public interest, research, or statistical analysis. This provision does not undermine the GDPR's primary purpose of protecting privacy but emphasizes the regulation's recognition of the larger societal interest in data protection. It strives to establish a balance between individual control and the facilitation of legitimate data uses for the common good.

To achieve an effective data protection policy, it is crucial to strike a balance between making necessary data available for the public good and safeguarding the privacy and rights of individuals. This requires a collaborative approach involving citizens, businesses, and the state, with the understanding that data protection serves the collective interest of society. By recognizing the interconnectedness of these stakeholders, regulations and self-regulation can reflect the relationships between individuals and public agencies, fostering a harmonious balance of private and public interests for data protection.

REFERENCES

Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era*, ALRC Report 123, 2014, https://www.alrc.gov.au/wp-content/uploads/2019/08/fr123_9._balancing_privacy_with_other_interests.pdf

Brownsword Roger and Goodwin Morag, *Law and the Technologies of Twenty-First Century: Text and Materials*, Cambridge University Press, Cambridge, 2012,

Brownsword Roger, Goodwin Morag, *Law, and the Technoogies of the Twenty-First Century: Text and Materials*, Cambridge University Press, Cambridge, 2012

C. J.Bennett, , & C. Raab, *The governance of privacy. Policy instruments in global perspective*. Cambridge: MIT Press. 2006

CJEU, Case C-139/01, Österreichischer Rundfunk and Others, ECLI:EU:C:2003:294, para. 74 and 64

CJEU, Case C-293/12, Digital Rights Ireland, ECLI:EU:C:2014:238.

Datalag av. den 11 maj 1973, Svensk författningssamling 1973:289.

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

ECtHR, Gaskin v. United Kingdom, App no. 10454/83 (7 July 1989)

ECtHR, Khelili v. Switzerland, App no. 16188/07 (18 October 2011),

Egan Mo, Privacy boundaries in digital space: an exercise in responsibilities, Information & Communications *Technology Law*, 31:3, 2022, DOI: 10.1080/13600834.2022.2097046

Felkner, Anna, Kadobayashi Youki, Janiszewski Marek, Fantin Stefano, Ruiz Francisco Jose, Adam, and Kozakiewicz Gregory Blanc. *Cybersecurity Research Analysis Report for Europe and Japan : Cybersecurity and Privacy Dialogue between Europe and Japan*. Cham, Switzerland: Springer, 2021

G.G. Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, Dordrecht: Springer, 2014, DOI:10.1007/978-3-319-05023-2.

Hessisches Datenschutzgesetz vom 7. Oktober 1970, Gesetz- und Verordnungsblatt für das Land Hessen Teil I, Nr. 41, 625 vom 12. Oktober 1970

Judgment of the Court (Grand Chamber), 13 May 2014. Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González., para.81

Kerry F. Cameron, & Morris B. John Jr., *Why Data Ownership is the Wrong Approach to Protecting Privacy*, BROOKINGS (June 26, 2019), https://www.brookings.edu/blog/techt ank/2019/06/26/why-data-ownership-is-the-wrong-approach-to-protecting-privacy/.

Kittichaisaree Kriangsak, Public International Law of Cyberspace, *Law, Governance and Technology Series*, Vol.32, Springer, Switzerland, 2017,

Kokott J. and Sobotta C., 'The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR', *International Data Privacy Law* 3(4), 2013,

Lane Julia, et. Al., *Privacy, Big Data, and the Public Good: frameworks for engagement*, Cambridge University Press, New York, 2014.

Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, Journal Officiel de la République Française, 227 du 7 janvier 1978.

Lukács Adrienn, *What is Privacy? The History and Definition of Privacy*, University of Szeged, 2016 https://publicatio.bibl.u-szeged.hu/10794/7/3188699.pdf

Mostert Menno, Bredenoord Annelien L., Sloot van der Bart, J.M Johannes. van Delden, From Privacy to Data Protection in the EU: Implications for Big Data Health Research, *European Journal of Health Law* Vol.24, 2017

Naef Tobias, *Data Protection without Data Protectionism*, Springer, Vol.28, European Yearbook of International Economic Law, 2021

Park S. Kyung, Data as Public Goods or Private Properties?: A Way Out of Conflict Between Data Protection and Free Speech, *6 UC Irvine Journal of International, Transnational, and Comparative Law*, Vol.77, 2021

Post C. Robert, *The Social Foundations of Privacy: Community and Self in the Common Law Tort*, Vol. 77 CALIF. L. REV. 957, 958, 1989

Reed Chris, *Making Laws for Cyberspace*, Oxford University Press, United Kingdom, 2012, ISBN 978-0-19-965761-2,

Regan Priscilla M., Legislating Privacy: *Technology, Social Values, and Public Policy*, Vol. 228, 231, 1995

S. D Warren,. L. D.,Brandeis, The Right to Privacy. *Harvard Law Review* Vol. 4, No. 5., 1890

Schünemann Wolf J, Baumann Max Otto, *Privacy, Data Protection and Cybersecurity in Europe*, Springer, 2017, ISBN 978-3-313-53634-7

Schwartz Paul M., *Regulating Governmental Data Mining in the United States and Germany: Constitutional Courts, the State, and New Technology*, 53 WM. & MARY L. REV. 351, 367–68 (2011).

Sloot van der B., 'Privacy as human flourishing: Could a shift towards virtue ethics strengthen privacy protection in the age of Big Data?', *Journal of Intellectual Property, Information Technology and Electronic Commerce Law* Vol.5 (3), 2014

Solove Daniel, Understanding Privacy, *Harvard University Press*, 2009,

Stockmann Daniela, *Tech companies and the public interest: the role of the state in governing social media platforms*, Information, Communication & Society, 26:1, 1-15, 2023, DOI: 10.1080/1369118X.2022.2032796

Sunkpho Jirapon, Ramjan Sarawut, Ottamakorn Chaiwat, Cybersecurity Policy in ASEAN Countries, *Information Institute Conferences*, Las Vegas, 2018

W.Prosser, Privacy. *California Law Review*, Vol. 48, No. 3. (1960) p. 384.; Warren, Brandeis 1890. p.193.