UNDERSTANDING THE DYNAMICS OF THE RELATIONSHIP BETWEEN GENERAL DATA PROTECTION REGULATION AND ENVIRONMENT PROTECTION

Kuldeep Singh Panwar [*] ***& Jaishree Gaur*** [*]

[**Abstract**: *One of the main issues resulting from the expansion of the IT industry is energy usage. A tremendous quantity of energy in the form of power is consumed by the data hubs and internet infrastructure needed to maintain the global internet and all of the devices connected to it. With the industry expanding quickly and connected devices becoming more affordable and available in formerly impoverished regions of the world, consumption is only anticipated to increase. It is crucial to examine the energy consumption of the industrial sector and identify the components that might be reduced through efficient data protection regulation. Both the transmission and storage of personal and non-personal data cause environmental pollution and are significant consumers of energy and other resources. The generation of vast amounts of machine generated data, or non-personal data, as a result of companies selling data to advertisers results in billions of spam emails, calls per day, leads to significant energy waste in supporting these systems. Global adoption of adequate data governance and regulations will significantly reduce pollution, E-waste, and energy consumption. The equipment for storage and transmission is necessary, and its manufacture and upkeep demands additional resources like cooling energy and precious metals which causes potential harm to the environment. The modern problems require modern solutions which mean with the use of conventional solutions like renewable energy and sustainable development, there is a need to focus on the modern solutions for reducing e-waste. This paper will try to explain and analyze the relationship between the data governance and regulations under GDPR and the conservation of environment. Further this paper will also focus on the effect of different types of data production and its contribution to the environmental pollution.*]

Keywords: *Non-Personal Data, GDPR, Environment, e-waste, Data, Pollution*

[*] Associate Professor, H.O.D, Department of Law, Nagaland University, Lumami; Mob. No. 9414135915 Email id- kuldeepsingh.panwar@nagalanduniversity.ac.in

[*] Research Scholar, Department of Law, Nagaland University, Lumami; Mob. No. 8437333143 Email id- jaishree07gaur@gmail.com

I

Introduction

As the digital age has taken hold of the world and more of the world's population gains access to the internet, companies and other entities have found increasingly invasive methods of harvesting and exploiting their customers' data for monetary gain. Taking into account the exploitative nature of these practices, many governments have introduced or are planning to introduce regulations that protect their citizens' data from the clutches of companies and advertisers. These regulations have been shown to be highly effective in accomplishing the goal of protecting the data of citizens of cyberspace; however, there is a positive side effect of these regulations that accomplishes an even greater goal.

The effect of data protection regulations on the environment is a field that has not had much research. Since the implementation of the General Data Protection Regulation in the EU, its effects on the environment have come to light. From reducing energy usage to decreasing carbon emissions, the effects of the regulation have been numerous. The extent of the effect is worth exploring seriously as the presence of data and cyberspace become even greater parts of the human experience and the fields supporting this expansion get more power hungry and environmentally destructive. This paper aims to explore the dynamics of the relationship between the GDPR and the environment protection.

II

Understanding Personal and Non-Personal Data

The legal definition of personal data may be different from one jurisdiction to another, and different countries apply different rules governing personal data collection and usage.[1] Personal data, as defined by the UK Data Protection Act of 1984, is 'data consisting of information relating to a living individual who can be identified from that information (or from that information and other information in the data users' possession), including any expression of opinion about the individual but not any indication of the data user's

[1] Sarah Spiekermann *et al., The Challenges of Personal Data Markets and Privacy*, XXV Electronic Markets (2015).

intention with respect to that individual.'[2] Data is defined as information that has been captured in a way that enables it to be processed by machinery that is economically responsive to commands sent for that purpose. The identity of a natural person is limited to the expressed information, but not their mental status or even their preference, as long as it is kept in mind as abstract information with respect to that data subject. Therefore, that definition distinguishes between information based on a natural person's expression and explicitly excludes that of the indication of intention of an individual.

The term "personal data" currently refers to any information about a natural person that can be used to directly or indirectly identify that person, including but not limited to references to names, location data, identification numbers, online identifiers, or any other identity, whether physical, physiological, genetic, mental, economic, cultural, or social (Article 4 (1) of the GDPR). Given the legal definition of "personal data," "non-personal data" can be defined as "data that may refer to any information relating to a non-natural person when such information does not convey any identification of a natural person, whether directly or indirectly." Examples of such data[3] include statistical data, intellectual property assets (such as standard essential patents and trade secrets), security information, general confidential information of businesses, and so forth. Non-personal data also includes information or data that is anonymous, that is, information that does not relate to an identified or identifiable natural person, or personal information that has been made anonymous in a way that makes the data subject anonymous or impossible to identify. In other words, anonymization entails stripping data sets of all personal identification.

India is one of the few countries attempting to set the standard for non-personal data regulation. The recent report on the framework for non-personal data governance that was submitted by the Kris Gopalkrishna Committee is significant in this regard. The "Draft Report by the Committee of Experts on Non-Personal Data Governance Framework, Version 2" is a revised version of the original document. Initially, a report on the governance structure for non-personal data existed, but it required more explanations and consultations before it could be published. Report defined non-personal data in

[2] Data Protection Act 1984, *available at:* https://www.legislation.gov.uk/ukpga/1984/35/contents/enacted (last visited May 28, 2023).

[3] Michael R. Overly, OVERVIEW OF INFORMATION SECURITY AND COMPLIANCE: SEEING THE FOREST FOR THE TREES (2014).

paragraph 4[4] as "When the data is not 'personal data', or the data is without any personally identifiable information (PII), it is considered NPD."

Today's businesses in the European Union base a significant portion of their operations on "data flows," which are essential for contract regulation and the discovery of new business prospects across a variety of industries due to the rapid advancement and digitalization of technology.The "data economy" is being promoted and developed by the EU's Digital Single Market strategy, which really favors the free flow of both personal and non-personal data.[5]Two significant regulations serve as the cornerstones of this procedure:

- Personal data regulation (EU) 2016/679

- The Non-Personal Data Regulation (EU) 2018/1807

The first of them, often known as GDPR ("General Data Protection Regulation"), defines "personal data" as "any information relating to an identified or identifiable natural person" in an intentionally wide manner.[6]On the other hand, the non-personal data legislation defines non-personal data in opposition to how personal data is defined, stating that "non-personal data" is to be interpreted as "data other than personal data *(...)"*.[7] This specifically refers to information that was previously personal but was later made anonymous or information that does not initially refer to an identified or identifiable natural person.

III

Understanding GDPR

The General Data Protection Regulation, or GDPR, is an acronym, and its implementation marked a turning point for privacy protection in the new big data era. The European

[4] Ministry of Electronics and Information Technology, REPORT BY THE COMMITTEE OF EXPERTS ON NO-PERSONAL DATA GOVERNANCE FRAMEWORK (2020).

[5] *Personal Data and Non-Personal Data: Differences*, Lexology (Sep. 5, 2022) *available at:* *https://www.lexology.com/library/detail.aspx?g=db2e2c36-deab-4c3a-b7e9-8aee31f70faa* (last visited May 28, 2023).

[6] *What is Personal Data?* European Commission, *available at:* https://commission.europa.eu/law/law-topic/data-protection/reform/what-personal-data_en (last visited May 28, 2023).

[7] Michèle Finck, Frank Pallas, *They who must not be identified—distinguishing personal from non-personal data under the GDPR*, X International Data Privacy Law, 11-36 (2020).

Economic Area (EEA) single market now has a unified data protection regulatory framework that applies to all member states of the European Union (EU), plus Iceland, Lichtenstein, Norway, and Switzerland.[8]

A regulation in EU law governing data protection and privacy in the EU (European Union) and the European Economic Area (EEA) is known as the General Data Protection Regulation (GDPR). It received EU approval in April 2016 and went into effect on May 25, 2018. The GDPR replaces the UK's 1984 Data Protection Act and the EU's 1995 Data Protection Directive with new regulations that are more appropriate for the world that is dominated by technology today. The main goals of the GDPR are to give individuals control over their personal data and to streamline the regulatory framework for global trade by harmonizing EU regulations.[9] Because it is a regulation rather than a directive, every member state of the European Union must comply with it. There are 99 articles divided into 11 chapters. The organizations are required by the terms of GDPR to ensure that personal data is collected lawfully and in accordance with strict guidelines and those who collect and manage it are required to protect it from misuse and exploitation as well as to respect the rights of data owners - or face penalties for failing to do so. The GDPR also gives individuals additional rights to request the deletion of their personal data, provided there are no legitimate grounds for doing so (Right to Erasure). The GDPR strengthens enforcement and reporting requirements, and data breaches must be reported within 72 hours. If the GDPR regulations are broken, there might be a fine of up to 4% of global turnover or 20 million Euros, whichever is higher.[10]

Who Does the GDPR Apply to?

Any business operating within the European Union is subject to GDPR, as is any firm operating outside the EU that sells goods and services to consumers or companies within the EU. Consequently, GDPR has an international impact. The law applies to both processors and controllers, two different categories of data handlers.

[8] Rich Castagna, *General Data Protection Regulation (GDPR),* TechTarget, *available at:* https://www.techtarget.com/whatis/definition/General-Data-Protection-Regulation-GDPR (last visited May 28, 2023).

[9] *Id.*

[10] *Id.*

Controllers - A 'controller' is a person, public authority, agency, or any other body that chooses, on their own or in collaboration with others, the objectives and means of processing personal data.[11] Processor - A 'processor' is a person, public authority, agency, or any other entity that manages personal data on behalf of the controller. Controllers are required to ensure that any agreements with processors adhere to GDPR.[12] Personal data is defined under GDPR as names, email addresses, ID card numbers, and IP addresses, which are examples of personal data, which is information that can be used to identify a real individual. Additionally, it contains delicate personal information like genetic and biometric data, which can be used to identify a person uniquely.

GDPR Supervisory Authority

GDPR requires every member state to designate a supervisory authority. Each member state has established an independent public authority to oversee the GDPR's implementation and compliance.

Officer for Data Protection

According to GDPR regulations, some businesses are required to appoint Data Protection Officers (DPO). The appointed DPO (Data Protection Officer) must have a high level of expert knowledge of the laws, practices, and GDPR compliance. The controller and the processor ensure that the data protection officer is involved, properly and promptly, in all issues relating to the protection of personal data.

The advantages of GDPR are that the GDPR serves as a roadmap for achieving a greater level of data security. The Companies doing business in the EU or providing services to EU clients have improved their cyber security status in order to comply with the GDPR regulations. The GDPR gives the most weight to consumer consent; as a result, clients place their trust in businesses and share their data knowing that it is being done in a secure atmosphere.

But at the same time GDPR is disadvantageous because of the concerns regarding overregulation exist with regard to GDPR, as is typical of legislation. The fine for breaking the GDPR's rules is severe: 4% of the company's annual global turnover, or 20

[11] *What are 'Controllers' and 'Processors'?*, ICO., *available at:* https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/controllers-and-processors/controllers-and-processors/what-are-controllers-and-processors/ (last visited May 28, 2023).

[12] *Id.*

million Euros, whichever is higher. The GDPR adds a significant degree of complexity to online commerce. Regardless of turnover, every company must be compliant.

IV

India and GDPR

Online data protection in India is covered under the Information Technology Act, 2000 (IT Act) and IT Rules. While the GDPR and the IT Act both aim to manage and regulate the transfer of data for e-commerce, the GDPR is more concerned with protecting the rights of the citizens (of the EU), but this is lacking in Indian law.[13] Both stipulate that data collecting must be done lawfully and that it must be done solely for the stated purposes. The IT Act only applies to data collection and utilization (not processing), but GDPR also applies to data processing. The principles outlined in the GDPR which are absent in the IT Act are responsibility, fairness, openness, and protection from unauthorised processing of data. The GDPR grants Member States the power to establish unique processing standards and to specify five additional criteria for when processing is necessary. The IT Act does not make such demands. Prior to data collection, consent is required under both the IT Act and the GDPR, and consent providers have the right to revoke their consent at any time. In contrast to the IT Act, the GDPR defines consent, lays out requirements for children's consent, and requires the data controller to show proof of such consent. The rights to rectification, information, and the ability to revoke consent are covered under Section 43A of the IT Act, which generally corresponds to GDPR.[14]

Relationship Between Data and Environment

Energy consumption is one of the biggest concerns that is arising as a result of the growth of the IT field. The data centers and internet infrastructure required to maintain the global internet and all of the devices connected to it consume a staggering amount of energy in the form of electricity. In 2016 it took nearly 70 billion Kilowatt hours of electricity to run the internet.[15] With the rapid growth of the field as connected devices get cheaper and

[13] Tarun Khurana , Mudit Saxena & Upasna Rana, *India: GDPR Vis-À-Vis Indian Data Protection Laws,* Mondaq (Nov. 15, 2022) *available at-* https://www.mondaq.com/india/privacy-protection/1251008/gdpr-vis-%C3%A0-vis-indian-data-protection-laws (last visited May 28, 2023).

[14] Aditi Chaturvedi, *GDPR and India*, CIS-India (Oct. 17, 2017) *available at-*https://cis-india.org/internet-governance/files/gdpr-and-india (last visited May 28, 2023).

[15] Christopher Helman, *Berkeley Lab: It Takes 70 Billion Kilowatt Hours a Year To Run The Internet,*

more accessible in previously underdeveloped parts of the world, this consumption is only expected to rise. It is essential to see how the industry uses energy and which parts can be minimised by effective data protection regulation. The primary ways in which data uses energy is:

1. Electricity used by data centre equipment for its operation.

2. Electricity is used to cool the equipment.

3. Energy is used to create the infrastructure and equipment.

4. Transportation of the equipment and other resources.

5. Employees/technicians travel for maintenance.

In a voluntary project with 184 participants, including companies like IBM, BT, HP, Vodafone, and Unilever and organizations in the public sector like the United Nations, the European Commission published a code of conduct for data centres in 2008. The objective was to make data centres more energy-efficient while establishing minimal voluntary criteria that may later be used as the foundation for more stringent regulation. By 2020, it was projected that the energy used in data centers in Western Europe would increase by half, from 56 TWh to 104 TWh[16]. Electricity used by data centers in 2015 was 416.2 terawatt hours (2-3% of global energy consumption)[17]. Total energy consumption by data centers is estimated to reach 14% of global energy consumption by 2040. The rise of data-heavy processes such as video calling, cryptocurrency mining and user data farming will accelerate this increase in energy usage. Most of the energy used by data centres is made using environmentally destructive methods such as fossil fuels. Virginia's

Forbes (Jun. 28, 2016) *available at*-https://www.forbes.com/sites/christopherhelman/2016/06/28/how-much-electricity-does-it-take-to-run-the-internet/?sh=3f708af81fff (last visited May 28, 2023).

[16] *European Code of Conduct for Energy Efficiency in Data Centers*, European Commission, *available at:* https://joint-research-centre.ec.europa.eu/scientific-activities-z/energy-efficiency/energy-efficiency-products/code-conduct-ict/european-code-conduct-energy-efficiency-data-centres_en (last visited May 28, 2023).

[17] Tom Bawden, *Global warming: Data centres to consume three times as much energy in next decade, experts warn*, Independent (Jan. 23, 2016) *available at:* https://www.independent.co.uk/climate-change/news/global-warming-data-centres-to-consume-three-times-as-much-energy-in-next-decade-experts-warn-a6830086.html (last visited May 28, 2023).

"Data center alley", the site of 70% of the world's internet traffic (as of 2019) uses power from non-renewable energy sources.[18]

India relies heavily on coal and natural gas for its electricity production. This is especially true in the case of heavily industrialised states such as Maharashtra, which is home to most of India's data centers. Therefore, it becomes necessary to include this cost in energy production and pollution when addressing India's energy consumption and pollution goals and commitments. As part of COP26[19], India has promised to achieve "net zero emissions" by the year 2070 and to bring its carbon intensity down to 45% by the year 2030. The positive environmental effects of data protection regulations can help offset the rising carbon footprint of the IT sector in India and thereby help India achieve its carbon goals.

A significant portion of the energy consumed keeps storage and computing equipment cool. Equipment such as servers and hard drives, which store data and house crucial digital infrastructure, are extremely sensitive to temperature. High temperatures may affect the functions of these devices by either hindering performance or causing damage to them. These devices also generate waste heat during their functioning, which accelerates their decline in performance. Data centers often use systems that use water or chemical coolants to cool their server racks. Water is piped around the center to absorb the waste heat, and then the hot water is expelled. This heated water is often piped into nearby water bodies, which can be harmful to the local ecosystems that are adapted to a particular temperature. Furthermore, chemical coolants are often toxic (CFC). HVAC systems for cooling server rooms can account for as much as 50% of the energy consumed in a data centre's daily operation[20]. There has been a push to move all data centres to areas with colder climates to decrease the need for overall cooling. However, this introduces inefficiencies in transportation and maintenance. This is impossible in countries like India, where the climate fluctuates throughout the year, and the IT hubs are located in hot climates such as Mumbai, Bangalore and Delhi.

[18] Gary Cook & Elizabeth Jardim, *Clicking Clean Virginia: The Dirty Energy Powering Data Center Alley*, Greenpeace Reports (Feb. 13, 2019) *available at:* https://www.greenpeace.org/usa/fighting-climate-chaos/click-clean/ (last visited May 28, 2023).

[19] Shashank Mehta, *COP26 and Commitment of India*, XXVI ENVIS RP: Geodiversity and Impact on Environment 12 (2022).

[20] M. Dayarathna, *et al.*, *Data Center Energy Consumption Modeling: A Survey*, XVIII IEEE Communications Surveys & Tutorials 732-794 (2016).

Devices such as hard drives and servers use precious metals like gold. The mining of these resources requires energy and causes carbon emissions. Furthermore mining of these materials often cause environmental destruction to the areas surrounding the mines in the form of deforestation, soil contamination and water contamination.

A big problem that is being faced following the explosion in popularity of devices is E-waste generation. E-waste is generated as equipment fails. In India the E-waste generated in this manner would be regulated under the E-Waste (Management) Rules, 2016[21]. Equipment used in digital infrastructure that is constantly being used to maintain and store data has the potential to fail even more than consumer devices due to their increased and constant usage. A large amount of E-waste is generated in this manner. Components like batteries use toxic and dangerous material like lithium (flammable). The disposal of potentially toxic and dangerous materials found in batteries would also come under the E-Waste (Management) Rules, 2016. Some data centers are located in colder regions to decrease cooling requirements. However these are often in harder to reach places. This means an increase in the carbon footprint of technicians that have to travel to and from these data centers. There is also increased energy usage and emissions from building and maintaining large data center facilities. This includes on-site power back-up generators, transportation of supplies, and heating and cooling the buildings in general.

To make sure that no data is lost and to ensure that data is available at a moment's notice across the globe, there are multiple instances of the same data stored in different locations for redundancy. There may even be multiple instances of data stored in the same data center or even the same storage rack. This effectively doubles the energy used by the same data. The Climate Neutral Data Center Pact[22] is an agreement between major players in the data sector in the EU to become climate neutral by 2030. This is to be done by adopting clean energy providers, more efficient processes, better management and using renewable energy. There is also research that is being done to make data centers greener[23].There have been talks to adopt the features of this agreement and other research into a comprehensive policy under the GDPR.

[21] CPCB | CENTRAL POLLUTION CONTROL BOARD, *available at*: https://cpcb.nic.in/e-waste/ (last visited May 28, 2023).

[22] *The Green Deal needs Green Infrastructure,* Climate Neutral Data Centre Pact, *available at:* https://www.climateneutraldatacentre.net/ (last visited May 28, 2023).

[23] Jin, Xibo *et al., Green Data Centers: A Survey, Perspectives, and Future Directions,* I arXiv (2016). *available at:* http://arxiv.org/abs/1608.00687 (last visited May 28, 2023).

V

Role of GDPR in Environment Protection

Following the GDPR coming into effect, some websites are noted to load faster. Ads and data trackers made up 91% of the size of a website in some cases.[24] Not using trackers and targeted ads can reduce the time taken to load a website, data stored in website servers, and energy required to send and receive data from users, leading to an overall reduction in energy consumption and emissions.

There has been a drastic reduction in marketing emails as advertisers do not have access to this data and, therefore, cannot send emails to bulk email lists. The number of emails sent for advertising was reduced by as much as 1.2 billion per day.[25] This has led to a reduction of 360 tonnes of CO2 emissions per day. (Average CO2 emission per email (75kb average size) is 0.3g[26] | 0.3*1.2 billion emails = 360 tonnes of CO2). 1.2 billion emails at 75kb per email is about 90 terabytes of data stored on email servers, transferred across the internet and displayed on user devices. This leads to energy consumption, the need for more storage (resulting in more mining for metals and other resources for storage devices), and more CO2 and other pollutants from data centers.

The GDPR has resulted in reduced carbon emissions and reduced energy consumption in the EU. However, the environmental benefits of data privacy laws will be multiplied when applied on a global scale. According to a study conducted by McAfee and ICF international, there are an estimated 62 trillion spam emails sent every year, consuming close to 33 billion kilowatt-hours(KWh).[27] These emails are sent in bulk to email lists

[24] Nik Froehlich, *The Truth in User Privacy and Targeted Ads*, Forbes (Feb. 24, 2022) *available at:* https://www.forbes.com/sites/forbestechcouncil/2022/02/24/the-truth-in-user-privacy-and-targeted-ads/?sh=59db7236355e (last visited May 28, 2023).

[25] Timothy Libert, *et al.*, *Changes in Third-Party Content on European News Websites after GDPR*, Factsheet (2018). *available at: https://reutersinstitute.politics.ox.ac.uk/sites/default/files/2018-08/Changes%20in%20Third-Party%20Content%20on%20European%20News%20Websites%20after%20GDPR_0_0.pdf* (last visited May 28, 2023).

[26] Deborah Chu, *What's the carbon footprint of an email?*, Pawprint eco companion, *available at:* https://www.pawprint.eco/eco-blog/carbon-footprint-email#:~:text=The%20average%20carbon%20footprint%20of%20an%20email%20is%200.3g%20CO2e.&text=The%20numbers%20go%20up%2C%20however,an%20attachment%20(50g%20CO2e) (last visited May 28, 2023).

[27] Ariel Schwartz, *what's the Carbon Footprint of Spam? Enough to Power 2.4 Million Homes*, Fast Company (Apr. 15, 2009) *available at:* https://www.fastcompany.com/1269134/whats-carbon-footprint-spam-enough-power-24-million-homes (last visited May 28, 2023).

compiled from user data sold by companies to advertisers and scammers. The annual global energy required for creating, sending, receiving, storing, and viewing spam is more than 33 billion KWh, comparable to four huge new coal power plants. ICF estimates spam-related emissions for all email users at 17 million metric tonnes of CO2, or 0.2% of global emissions.

Spam emails account for close to 80% of all emails sent globally. National data protection regulations are essential to reduce the number of emails that can be farmed by companies and sold to advertisers. Such a reduction is monumental in reducing the carbon footprint as well as the energy consumption by the process of sending spam emails. Reduction in spam is only one of the benefits of data privacy regulations. As observed in the EU, better regulation of website trackers will lead to less data heavy websites. Trackers are pieces of code that observe user activity that are embedded in websites in order to learn about a user and then use that information to serve specifically targeted advertisements to that user. There can be multiple trackers on a website which leads to larger websites that take up more space on a server and takes more time to load and more energy to maintain and view.

As of October 2021, India is the 5th most spammed country in the world with an average of 7.97 billion spam emails sent per day[28]. This amounts to approximately 2391 tonnes of CO2 emissions per day. India is also 4th in the world when it comes to spam calls.[29] These spammers get information about emails and phone numbers from companies that sell this user data to them for advertising purposes. The low technology literacy in India leads to users more voluntarily giving up their user data when asked by companies. The users are unaware of how their data is used for advertising and spamming. Considering the right to privacy that India holds to high regard this is unacceptable.

The way to reduce this is by implementing data privacy regulations that protect user data and limit the data that companies can collect. Similar provisions to the GDPR, such as limiting data to only that needed for the company to provide their services and only using that data for their stated purpose, will go a long way in combating this spam problem. The proposed Digital Personal Data Protection Bill, 2022 is a step forward for India.

[28] Jyothiikaa Moorthy, *23 Email Spam Statistics to Know in 2023*, Mailmodo (Aug. 8, 2023) *available at:* https://www.mailmodo.com/guides/email-spam-statistics/ (last visited Nov 20, 2023).

[29] Hema Seth, *India Among the top 10 countries affected by spam calls in 2020: Truecaller*, The Hindu Business Line (Dec. 8, 2020) *available at:* https://www.thehindubusinessline.com/info-tech/india-among-the-top-10-countries-affected-by-spam-calls-in-2020-truecaller/article33280228.ece (last visited May 28, 2023).

However, the provisions and effectiveness of this bill and the environmental effects of this regulation remain to be seen. however, since it is based on and will emulate the GDPR it is likely that there will be similar environmental benefits. The benefits may be more than the GDPR since India uses more non-renewable energy sources for its IT sector. It will also be beneficial for India's poor infrastructure for E-waste management. In 2019 and 2020, only 22.7% of the E-waste generated in India was collected, recycled or disposed of[30]. The rest of the E-waste remains in landfills and water bodies. The harmful pollutants in components like hard drives contaminate soil and water bodies. Reduction in E-waste brought about by data privacy regulations will alleviate the stress on India's E-waste management infrastructure.

VI

Conclusion

The importance of data protection regulation has increased in the modern day. Companies and advertisers seek to gain from misusing their customers' data without consequence. Therefore, governments need to take steps to minimize the data that can be collected from their citizens that may not be aware of the way these companies are using their data. As demonstrated by the GDPR, these regulations are adequate for their intended purpose, but they also have the useful side-effect of helping the environment. Data storage and transmission is a large consumer of energy and other resources and polluting in nature. Companies selling data to advertisers leads to billions of spam emails and calls each day resulting in a huge wastage of energy required in the processes behind these systems. Applying the same standards for data privacy on a global scale would result in massive improvement in pollution, E-waste and energy savings. This is set to improve as technology advances and the amount of data created increases drastically in the future. Storage and transmissions require equipment whose creation and maintenance consume even more resources in the form of precious metals and cooling energy. This equipment becomes an E-waste problem once it ends. In a country like India, which has a massive spam and E-waste problem and is highly dependent on non-renewable, polluting sources of electricity, the decrease in data storage and data

[30] *78% of e-waste not disposed off by the government: Report*, Construction World (May 8, 2022) *available at:* *https://www.constructionworld.in/urban-infrastructure/wastewater-and-sewage-treatment/78--of-e-waste-not-disposed-off-by-the-government--report/34204* (last visited May 28, 2023).

processing resulting from data protection regulation can be a huge boon. The proposed Digital Personal Data Protection Bill is a step in the right direction for data protection in India as well as making the field of data collection, storage and transmission less environmentally destructive. The best way forward is for an environmental perspective to be considered by the framers of this bill and for limits on collection and storage to be developed to further environmental goals. It is therefore becoming obvious that data protection regulation is the need of the hour for both the right to privacy and the offset of the environmental damage being caused by the ever-expanding information technology industry.