Data ethics and law are twins

3

DATA ETHICS AND LAW ARE TWINS

Pavan Duggal, India[130]

3.1 Introduction

Today, we are in a very interesting age of evolution as far as the internet and the electronic ecosystem is concerned. Internet has been with us for the last many decades. Internet has come to occupy a central lifeline in our day-to-day lives and we are all dependent on the internet.

As a natural corollary, we are all dealing, handling or processing data in the electronic form. We have all become global authors, global transmitters and global broadcasters of data. In fact, we are constantly generating data. World over, there is a new phenomenon. The world popula-

---

[130] Dr. Pavan Duggal, Advocate at the Supreme Court of India, Honorary Chancellor Cyberlaw University, President Cyberlaws.net, Chairman of the International Commission on Cybersecurity Law, Member of the International Board of Globethics. He has been acknowledged as one of the top four Cyber lawyers in the world. Contact: pavan@pavanduggal.com. More at www.pavanduggal.com.

tion at large is undergoing a Great Data Vomiting Revolution where people are not just generating data but are vomiting data about their personal, professional and social lives, without even thinking about the legal ramifications for the same.

Data is all around us. No wonder, data has become the new oil of the new data economy. It is this new oil, which is of massive significance because this data tends to get monetized. More and more data stakeholders are interested about collecting and monetizing data today than at any point of time in history earlier.

Therefore, data ethics assume massive significance. Data has become the precious raw material of this century. Hence, law has to come up with appropriate legal frameworks to deal with legally valid and sound approaches of dealing with data. More significantly, ethical principles have also evolved as to how data needs to be handled.

It is in this context that data ethics has become extremely significant in our lives. For the various definitions of data ethics we refer to the introduction of this book. Data ethics as a discipline has got a direct intrinsic connection with law.

3.2 Intrinsic Connection between Data Ethics and Law

There is intrinsic connection between data ethics and law, because data ethics provides basic logical and ethical principles on the basis of which data needs to be dealt, handled or processed with. These very logical and ethical principles often find themselves reflected in legal provisions under the law.

Therefore, law has got an intrinsic connection with data ethics. As more and more countries are today generating new laws on data, the principles of data ethics are getting enshrined in the said laws. In addition, more new principles on data ethics are evolving with the passage of time.

It is but natural to expect that principles of data ethics must be reflected in the evolving legal frameworks. No wonder, the interplay between law and data ethics thus becomes far more important and crucial.

In fact, it can easily be said that these two fields are interdependent on each other. It is the foundation of ethical principles in data economy provided by data ethics that becomes the raw material for the lawmakers to come up with new legal frameworks.

Similarly, the legal frameworks get far more meaning, topicality and relevance if they reflect and incorporate therein the foundational ethical principles pertaining to data. In fact, most of the people believe that data needs to be dealt, handled and processed with in an ethical manner. This becomes all the more significant since data invariably has got elements of personal privacy and also data privacy intrinsic therein. Most of the people today have an intrinsic expectation of privacy.

3.3 Ethical Principles for Using Data

Right now, experts agree on the following *ethical principles for using data:*

1. Privacy customer identity and data should remain private.
2. Shared private information should always remain private.
3. Customers should exercise a transparent view of how the data is being sold or utilized.
4. There should be no interference between big data and human will.
5. Big data should not institutionalize prejudicial biases.
6. As part of Consumer Relations, having excellent data ethics is a brilliant business decision.
7. Legality – Data management becomes a legal concern in some aspects as well. Thus, one needs to comply with the given regulations.
8. Implementing Data Ethics – If you opt to stay in business for a couple of years, it is a must to manage your data ethically. The manner

of protecting your people's data greatly depends on your company's needs. Whatever you gather, you should always be transparent.[131]

3.4 Interplay between Data Ethics and Law

In such a scenario, I find that the interplay between data ethics and law continues to keep on growing with the passage of time.

However, we need to understand that time has also taught us one thing which is that technology moves at a very rapid pace. Technology is invariably growing at such cutting-edge pace that it is leaving behind legal developments and law. In fact, it is often said that the law is almost ten steps behind the advent of technology. The massive speed of technological developments have actually now sparked our imagination.

Newly emerging technologies are evolving which are continuing to dazzle not just the technological ecosystem but also users, whether it is Artificial Intelligence, Blockchains, Internet of Things (IoT), Quantum Computing or the Metaverse. These newly emerging technological paradigms are continuing to amaze us. Also, the massive speed with which such developments in technology are evolving, is actually making us gasp for breath.

While the newly emerging technologies and their constructive usages are evolving, the cyber criminals are not far behind. They are increasingly coming up with new ways of misusing the said technologies to the detriment of people at large. Therefore, enabling technology legislation is the answer to the massive speed of technological developments.

Technology legislations across the world are taking the manifestation of cyber legal frameworks. Cyberlaw is a discipline that deals with the legal, policy and regulatory issues pertaining to technologies including the internet, cyberspace and the World Wide Web. Most of the countries, till today, have relied upon the UNCITRAL Model Law on Electronic

[131] Analytics Insight. 2021. Ethical Principles for Using Data. https://www.analyticsinsight.net/ethical-principles-for-using-data/

Commerce which has been ratified by the United Nations General Assembly for the member nations to come up with their own respective national laws on cyber legal affairs.

As a result, most of the countries have come up with their national cyber laws. In addition, the advent of newly emerging technological paradigms has effectively meant that countries have started coming up with more dedicated legal frameworks on these newly emerging technologies. Data protection and privacy have become an important thrust point for majority of countries. Therefore, beginning with the General Data Protection Regulations (GDPR) of the European Union, one finds that countries are increasingly coming up with new laws on data protection.

3.5 Advent of Emerging Technology and Data Ethics

Further, the advent of newly emerging technologies like cyber security is propelling countries to come up with their own distinctive national laws on cyber security. Various countries are in the process of not just coming up with new laws on cyber security but also updating their current laws so as to make them topical and relevant in the context of growing cyber security breaches.

The coming of Internet of Things (IoT) has actually meant that countries need to wake up to the need for protecting cyber security in the Internet of Things (IoT) paradigm. Therefore, countries have started coming up with their new legal frameworks on Internet of Things (IoT). These include legislations like the US Federal Internet of Things (IoT) Cybersecurity Improvement Act 2020. The European Union is now coming up with the new draft Cyber Resilience Act and also new draft legislation on Artificial Intelligence.

The advent of Artificial Intelligence is also propelling countries to start exploring ways of how they can come up with new legal frameworks so as to deal with Artificial Intelligence as a paradigm.

In these newly emerging technologies and their legal regulation, there is an intrinsic role of ethical values. This is so because new technology legislations, which are coming up to regulate technology, must have ethical foundations and principles as an integral bedrock of the same.

This assumes even more significance because ethical principles and ethical values need to be incorporated as an integral part of data economy age. In this data economy age where everybody is dealing with data, it becomes imperative that the world must rely on ethical approaches to dealing with data.

3.6 Golden Age of Cybercrime and Increasing Cyber Security Breaches

Much more needs to be done in this particular regard. Data ethics therefore assumes far more significance in the context of legal frameworks. This assumes even more significance given yet another unique challenge that the emergence of technology has brought forward, which is growing cybercrimes and cyber security breaches.

Already with the advent of Covid-19, we have begun to see the coming and emergence of the Golden Age of Cybercrimes. This Golden Age of Cybercrime is going to be with us for many decades. Hence, the focus has to be on how to come up with ethical responses to deal with such growing cybercrimes including phishing, identity theft and online financial frauds.

Over the last few years, the world has been increasing cyber security breaches. These breaches are beginning to become of immense significance and challenge as far as all digital stakeholders are concerned.

These cyber security breaches ultimately are targeting data resident on computer systems and networks and its illegal and unauthorised monetization. These growing cyber security breaches and their impact be-

comes evident when one looks at the facts and figures pertaining to the same.

1. During the third quarter of 2022, approximately 15 million data records were exposed worldwide through data breaches. This figure had increased by 37 percent compared to the previous quarter.[132]
2. Between March 2021 and March 2022, the average cost of a data breach in the healthcare sector amounted to over 10 million U.S. dollars, up from 9.23 U.S. dollars between May 2020 and March 2021. The financial industry ranked second, with 5.97 U.S. dollars per breach on average. The global average cost of a data breach in the measured period was 4.35 million U.S. dollars. Data breaches in the public sector ranked last, costing an average of 2.07 million U.S. dollars during the measured period.[133]
3. An average of 4,800 websites a month are compromised with formjacking code[134]
4. By stealing 10 credit cards per website, cybercriminals earn up to $2.2 million through formjacking attacks[135].
5. The average total cost of a data breach was more than $1 million higher when working remote was a factor in causing the breach, compared to breaches in which working remote was not a factor[136].
6. Cyber scams increased by 400 percent in the month of March 2020, making COVID-19 the largest-ever security threat. [137]

---

[132] Statista. 2022. Number of data records exposed worldwide from 1st quarter 2020 to 3rd quarter 2022, https://www.statista.com/statistics/1307426/number-of-data-breaches-worldwide/

[133] Statista. 2022. Average cost of a data breach worldwide from May 2020 to March 2022, by industry, https://www.statista.com/statistics/387861/cost-data-breach-by-industry/

[134] Symantec, 2019 Internet Security Threat Report, Executive Summary, ISTR Vol 24.

[135] Ibid.

[136] IBM. 2022. Reports. Cost of a data breach 2022, https://www.ibm.com/reports/data-breach.

A perusal of the aforesaid facts and figures of cyber security breaches thus clearly shows that they will have an extremely detrimental impact upon the data economy. Hence, the adoption of data ethics and related legal principles becomes far more relevant in the context of not just data economy but data economy stakeholders at large. Therefore, ethical values need to be an integral part of legal response and regulation mechanism, so as to deal with data in the data economy age.

Therefore, ethical principles and ethical values which form integral part of data ethics need to be an integral part of the legal response mechanism to emerging technology laws. But when one looks at the prevailing international approaches, one finds that countries and state actors tend to adopt a dual approach.

3.7 Dual Approaches on Data Ethics and Law by Countries

In the context of data ethics and law vis-à-vis their national legislations, countries often incorporate data ethical principles as an integral component thereof. This assumes more significance because countries want their national citizens to comply with the ethical principles and therefore data ethics principles often find reflection in the national laws.

However, when one looks at the international scenario, countries tend to behave differently. In today's scenario, where countries are engaging in both covert and overt activities, countries do not really want any naming and shaming phenomenon in cyberspace or also in international paradigm.

Therefore, countries then often tend to drag their feet and not respond effectively in the direction of ethical regulation of cyberspace at the international scenario. That is the reason why there is no international Cyberlaw or cyber security law in place.

---

[137] Sobers, Rob. 2022. 89 Must-Know Data Breach Statistics [2022], Varonis. https://www.varonis.com/blog/data-breach-statistics.

We need to understand that there is a need for incorporating data ethics in the legal principles and legal frameworks, both at the national level as also at the international level, because ultimately dealing with data in an ethical manner becomes a foundation for the further robust growth of the data economy.

3.8 Increasing Cyber Attacks and Data Ethics

However, there is yet another new trend on the horizon which is beginning to threaten data ethics and law which is growing cyber attacks. Cyber attacks are now being launched in by both state and non-state actors for the purposes of breaching the cyber security of computer systems and networks located in other jurisdictions and data that is resident therein. This becomes even more apparent when one looks at the numbers in this regard.

1. Malware increased by 358 percent in 2020.[138]
2. Ransomware attacks rose by 435 percent in 2020 compared to 2019.[139]
3. On average, a company falls victim to a ransomware attack every 11 seconds.[140]
4. 57 percent of organizations see weekly or daily phishing attempts.[141]
5. 65 percent of cybercriminal groups used spear-phishing as the primary infection vector.[142]

---

[138] Help Net Security. 2021. Malware increased by 358% in 2020, https://www.helpnetsecurity.com/2021/02/17/malware-2020/.

[139] Ibid.

[140] Morgan, Steve. 2020. Cybercrime To Cost The World $10.5 Trillion Annually By 2025. Cybercrime Magazine. https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/.

[141] Business Email Compromise Report. 2021. Cybersecurity Insiders. https://info.greathorn.com/hubfs/Reports/2021-Business-Email-Compromise-Report-GreatHorn.pdf.

6. Phishing attacks account for more than 80 percent of reported security incidents.[143]
1. $17,700 is lost every minute due to a phishing attack.[144]
2. By 2023, the total number of DDoS attacks worldwide will be 15.4 million.[145]
3. Attacks on IoT devices tripled in the first half of 2019.[146]
4. IoT devices experience an average of 5,200 attacks per month.[147]

As of now, at this particular moment, there is no dedicated international agreement on how to deal with the growing cyber attacks. There is Tallinn Manual 1.0 and Tallinn Manual 2.0, which have basically relied upon ethical principles of how countries need to adopt norms of behaviour in cyberspace. But that at best are only academic works and have not yet gained substantial traction across the world.

In this kind of a scenario, there is an urgent and immediate need that countries need to synergise the speed of technological legislations and ethical values. The speed of technological legislation effectively should be embellished with appropriate data ethical values which are enshrined in emerging principles of data ethics.

This is the need of the hour and it has to be appropriately adhered to. In fact, when one looks at the international scenario, one finds that there is a need to evolve appropriate important guidelines and principles for the digital stakeholders on how they can actually follow the principles of

---

[142] Broadcom. https://www.broadcom.com/support/security-center.

[143] Carlson, Brian. 2021. Top cybersecurity statistics, trends, and facts, CSO, https://www.csoonline.com/article/3634869/top-cybersecurity-statistics-trends-and-facts.html.

[144] Ibid.

[145] CISCO. 2019. Annual internet report, white paper. https://www.cisco.com

[146] Carlson, Brian. 2021. Top cybersecurity statistics, trends, and facts, op. cit.

[147] Sobers, Rob. 2022. 166 Cybersecurity Statistics and Trends [updated 2022] https://www.varonis.com/blog/cybersecurity-statistics

data ethics and law as they deal with the various emerging challenges of the data economy.

The ultimate future growth of data economy is dependent on how quickly in a resilient manner the principles of data ethics get incorporated in legal frameworks and how the said ethical principles are appropriately and effectively implemented through instruments of law. That is the focussed thrust and direction that countries need to move in.

3.9 Darknet and Data Ethics

There is also a need for countries to realize yet another big danger that is emerging on the horizon. The emergence of darknet has today brought in distinctive new paradigms. Darknet is the deep, dark underbelly of the internet where the intrinsic architecture of the darknet and the TOR network actually promises complete anonymity to all stakeholders. Complete anonymity breaths contempt in the form of growing cybercrimes.

Therefore, cybercrime is the dominant economic model as far as the darknet is concerned. Darknet is the complete antithesis of data ethics and law. In fact, darknet is used as a launching pad for committing various cybercrimes and cyber attacks on all stakeholders of the data economy as also the superficial net. However, while all kinds of unethical activities take place on darknet, it is also unique and important to appreciate that the darknet is also the embodiment of ethical values because even in that anonymous space, even for doing illegal and criminal activities, the stakeholders are adhering to certain ethical values. Though there are anonymous stakeholders, they have come up with appropriate indigenous approaches so as to uphold ethical values. So if a deviant actor does not perform the promised contracted deliverables on the darknet, he is blacklisted by the entire darknet community.

Hence, even in a place where criminal activities are launched in complete contravention of data ethics, there are still principles of data

ethics that are being followed by the respective stakeholders in the darknet economy. The challenges of the darknet have to be kept in mind more so, from the context of data ethics and law as today countries across the world are still struggling to come up with appropriate new effective regulatory frameworks so as to deal with the darknet. The darknet today presents immense challenges for the emerging data economy because more and more attacks on data economy are originating on the darknet.

3.10 Growing Data Economy Age, Data Ethics, Law and the Future

The growing data economy age is going to be the evolving future. In this context, the relationship of data ethics and law in the context of data economy assumes far more significance. In fact, more and more ethical principles, as are enshrined in the emerging discipline of data ethics, need to be incorporated in legal frameworks so that these newly embellished legal frameworks can then help support the further growth of the data economy at large.

The future is the future of data and the future lies in the manner of how data is going to be continuously getting evolved and monetized. This becomes further manifested in the following facts and figures pertaining to the projected growth of data in the data economy age.

1. Already, it has been estimated that poor data quality costs the US economy up to $3.1 trillion yearly.
2. In 2020, every person generated 1.7 megabytes in just a second.
3. Internet users generate about 2.5 quintillion bytes of data each day.
4. Predictions estimate the world will generate 181 zettabytes of data by 2025.
5. 80-90% of the data we generate today is unstructured.
6. The market of Big Data analytics in banking is set to reach $62.10 billion by 2025.

7. Big data in healthcare could be worth $71.6 billion by 2027.
8. Data interactions went up by 5000% between 2010 and 2020.

A perusal of the aforesaid facts and figures thus clearly tell us that data is now the new DNA that is connecting all stakeholders in the digital ecosystem. This data needs to be appropriately protected. The data economy age will only continue to consolidate in case if ethical principles are abided to and adhered to by data stakeholders when they deal, handle or process data.

3.11 Conclusion

Hence, the principles of data ethics and law, when joined together, can play a very important and cogent role in the further evolution of data economy as a whole.

To conclude, one can specifically state that data economy age is representing a new chapter in our lives. Data ethics as a discipline is continuing to evolve and stipulate new principles and foundations for the ethical use of data in the electronic ecosystem.

These ethical principles need to be well enshrined in the legal frameworks and laws across the world so that they can become potent combination in the direction of more effective and minimal enablement and regulation of the data economy age.

Together, with data ethics and law joining hands, they can provide a very potent constructive and positive direction in which the data economy has to ultimately evolve in the coming times.

It will be really interesting to see how the interplay between data ethics and law will continue to evolve with the passage of time and would have an impact upon the data economy in the coming times.