Hastings Science and Technology Law Journal

Volume 14
Number 1 *Winter 2023*

Article 7

Winter 2023

Reversing the Irreversible: Mitigating Legal Risks of Blockchain-Based Data Breach through Corporate Governance

Katayoon Beshkardana

Reversing the Irreversible: Mitigating Legal Risks of Blockchain-Based Data Breach through Corporate Governance

KATAYOON BESHKARDANA*

Abstract

The European General Data Protection Regulation (GDPR) embodies a set of enforceable data subject rights, data controller and processor obligations, and compliance requirements. The GDPR outreach is extraterritorial and impacts US blockchain-based businesses that collect and process personal data of individuals from the EU. Given the ambiguities of the law itself surrounding what is considered as personal data on blockchain, and who data controllers and processors are, this research examines the corporate governance response to the GDPR as a bottom-up solution for compliance. To secure the sustainability of the business models based on blockchain solutions there is an immediate need to revisit traditional agency theory of corporate governance. Modern theory of corporate governance must inevitably integrate Corporate Social Responsibility and Environmental, Social, and Governance standards into its policies and procedures to mitigate risks and hedge against breaches of data security and privacy.

* Assistant professor at Morgan State University, Earl G. Graves School of Business and Management. The author wishes to thank the Academy of Legal Studies in Business for receipt of the Gaylord Jentz scholarship award as part of the support for this research paper.

TABLE OF CONTENTS

I. Introduction

Corporate activities empowered with digital technologies have a growing power over individuals and accordingly been subject of broader scrutiny and debate for comprehensive regulation.[1] In the meantime, the behavior of tech companies in collecting, storing, and processing personal data for commercial purposes has been investigated by law enforcement authorities.[2] While violation cases were primarily revolved around algorithmic biases and machine learning systems (MLS) that discriminate against individuals, recent observations and ever-growing evidence suggest that blockchain has an

1. Several federal bills have been introduced to both the House and the Senate and are currently reviewed at the committees. One of the most prominent proposals that has gained bipartisan support is the American Data Privacy and Protection Act (ADPPA), H.R. 8152. The House Energy and Commerce Committee has voted for the bill to advance to the full House of Representatives. The bill introduces right to private action, preempts state laws with some exceptions and delegates the Federal Trade Commission (FTC) and state attorneys general for the enforcement of the Act. For the summary of the bill, *see* JONATHAN M. GAFFNEY ET AL., CONG. RSCH. SERV., LSB10776, OVERVIEW OF THE AMERICAN DATA PRIVACY AND PROTECTION ACT, H.R. 8152 (2022). Another bill, Data Protection Act, introduced in February 2020 (renewed in 2021) by Senator Kristen E. Gillibrand and is now being considered in the Senate Committee on Commerce, Science, and Transportation. This bill, if passed, establishes an independent federal Data Protection Agency (DPA) to regulate the collection, disclosure, processing, and misuse of individuals' personal data by a covered entity. For summary of the Act and related actions in the Senate, *see* Data Protection Act of 2021, S. 2134, 117th Cong. (2021). In addition, states that have introduced their own data protection laws include California (Consumer Privacy Act), Massachusetts (Data Protection Act), Arkansas, Colorado, Nevada, Texas, Rhode Island, Minnesota, Oregon, Maryland, Florida, Connecticut, Indiana, New Mexico, Utah, and Kansas. *See* Security.org Team, *47 States Have Weak or Nonexistent Consumer Data Privacy Laws*, SECURITY.ORG, https://www.security.org/resources/digital-privacy-legislation-by-state/ (last updated on Feb. 4, 2021). For a comparison of privacy bills at the Congress *see* JONATHAN M. GAFFNEY, CONG. RSCH. SERV., LSB10441, WATCHING THE WATCHERS: A COMPARISON OF PRIVACY BILLS IN THE 116TH CONGRESS (2020).

2. In July 2019, Facebook reached a $5 billion settlement with the U.S. Federal Trade Commission (FTC) for violating an agreement with the agency to protect user privacy. Clearview AI allegedly built a facial recognition database of over three billion photos scraped from the internet without any oversight. Volkswagen and Audi were hit by a data breach that exposed the contact information and, in some cases, personal details like driver license numbers, of more than three million customers in the United States and Canada. Consumer privacy complaints are piling up with allegations of unfair and discriminatory practices concerning data collection, marketing, cross-device tracking, consumer profiling, user tracking, and data disclosure to third parties. Some cases include Monroy v. Shutterfly, Inc., No. 16-C-10984, 2017 WL 4099846 (N.D. Ill. Sep. 15, 2017), Rivera v. Google, Inc., 366 F.Supp.3d 998 (N.D. Ill. 2018), McDonald v. Symphony Bronzeville Park LLC, No. 126511, 2022 WL 318649 (N.D. Ill. Feb. 3, 2022), Rosenbach v. Six Flags Entm't Corp., 129 N.E.3d 1197 (Ill. 2019). Sprint and Time Warner have both incurred multi-million-dollar fines for biased data from the FTC. *See* Harald Smith, *The Hidden Hands of Data Bias*, INFOWORLD (Apr. 19, 2018), https://www.infoworld.com/article/3269060/the-hidden-hand-of-data-bias.html. In 2019, National Fair Housing Alliance (NFHA) settled the first federal discriminatory lawsuit to deal with racial bias in Facebook AI-Driven advertising platform. S*ee Summary of Settlement Between Civil Rights Advocates and Facebook*, NAT'L FAIR HOUS. ALL., https://nationalfairhousing.org/wp-content/uploads/2019/03/3.18.2019-Joint-Statement-FINAL-1.pdf.

equally potential impact on an individual's personal data.[3] New technologies interact with each other and their combination and convergence create synergies that greatly increases their social impact.[4]

As the capacity of technology increases and the controllers of that technology explode in size, sophistication, and wealth, protection of personal data is becoming a major and expanding concern for many jurisdictions.[5] The broad corporate access to personal data of individuals has urged Europe to pass a comprehensive law known as General Data Protection Regulation (GDPR).[6] Coming into force in 2018, GDPR provides an enforceable regulatory framework for accountability of electronic data controllers and processors and gives power to European authorities to hold liable companies that breach the fundamental right of individuals to protection of their personal data, regardless of the technology used.[7] Accordingly, GDPR has a broad scope that includes violations of personal data using any technology such as big data, data analytics, MLS, blockchain, or AI. In addition, the GDPR is an overarching regulation with global outreach and extraterritorial impact on private entities as well as public authorities that process personal

3. *See generally* Michèle Finck, *Blockchain and the General Data Protection Regulation: Can Distributed Ledgers be Squared with European Data Protection Law*?, EUR. PARLIAMENTARY RSCH. SERV. (2019).

4. Mark Fenwick & Erik P.M. Vermeulen, *Technology and Corporate Governance: Blockchain, Crypto, and Artificial Intelligence* 1–26 (EURO. CORP. GOVERNANCE INST., Working Paper No. 424/2018, 2018). The authors characterize modern digital transformation by "amplification effects" as multiple technologies accelerate each other in contrast to previous technological revolutions that were simply sequential. For example, Blockchain may converge with Artificial Intelligence (AI) for automatization of business processes. Smart contracts embedded with AI models can execute transactions on blockchain, process payments, or stock purchases and resolve disputes. In the health sector, blockchain and AI converge enabling data integrity, transparency, patient tracking and consent management. In supply chains and financial services, the convergence of blockchain with AI facilitates tracking data, accelerating transactions, increasing visibility for intellectual properties, and enhancing security and privacy of data. *See Blockchain and Artificial Intelligence (AI)*, IBM, https://www.ibm.com/topics/blockchain-ai (last visited Feb. 23, 2022).

5. Coral Ingley & Philippa Wells, *GDPR: Governance Implications for Regimes Outside the EU*, 16 J. LEADERSHIP, ACCOUNTABILITY & ETHICS 27 (Apr. 15, 2019).

6. Regulation 2016/679, of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) [hereinafter GDPR].

7. Article 8 of the Charter of Fundamental Rights of the European Union (EU) provides that "everyone has the right to the protection of personal data. Such data must be processed fairly for specified purposes and based on the consent of the person concerned or some other legitimate basis laid down by the law. Everyone has the right of access to data which has been collected on them, and the right to have it rectified or removed based on legitimate grounds." *See* Charter of Fundamental Rights of the European Union, art. 8, 2000 O.J. (C 364) 1 [hereinafter Charter]. Personal data is information that relates to natural person, or can identify the individual, either by itself or together with other available information. Personal data can include the name, address, contact details, an identification number, IP address, CCTV footage, access cards, audio-visual or audio recordings of natural persons, biometrics, and location data. GDPR, *supra* note 6, at art. 4, § 1.

data.[8] It applies to all businesses and organizations established in the EU or outside the EU that offer goods or services, process personal data, or monitor the behavior of individuals in the EU regardless of where the actual processing of the data takes place.[9] Fines for noncompliance are assessed by the national Data Protection Authority (DPA) in each member state and subject to appeal in national courts.[10] In the first two years of the GDPR enforcement, DPAs issued 273 GDPR fines against companies for a range of violations.[11] Given their frequent use of personal data to conduct daily operations, United States (U.S.) firms have been the primary subject of the investigating authorities for data breaches and unlawful data processing.[12] Since coming into effect, many U.S. firms have attempted to comply with the GDPR, such as revising user terms of agreement and requesting explicit user consent. Yet,

8. For GDPR fines against local government and government agencies, *see* Brian Daigle & Mahnaz Khan, *The Changing Tides of Data Protection Regulation in Europe*, U.S. INT'L TRADE COMM'N, OFF. OF INDUS., Working Paper ID-079, 1, 4, 7, 29, 30, 32 (Feb. 2022), https://www.usitc.gov/publications/332/working_papers/changing_tides_of_gdpr_enforcement_trends_final-compliant_1.pdf. Although its scope is not limited to the private sector, the focus of much of the publicity and warnings has been on the impact of the GDPR for companies.

9. Article 3 GDPR provides that the GDPR applies to the processing of personal data where personal data processing occurs in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not. This implies that where a natural or legal person that qualifies as the data controller or data processor under the GDPR is established in the EU and processes personal data through blockchains or other means, the European data protection framework applies to such processing. The Regulation also applies where the personal data relates to data subjects that are based in the EU even where the data controller and data processor are not established in the Union, but they offer goods or services to data subjects based in the EU with or without payment. This could, for instance, be the case where operators of a blockchain make available their service to individuals in the Union. Where someone based outside of the EU uses blockchain to process personal data in the context of monitoring the behavior of EU-based individuals the Regulation equally applies. In sum, blockchains that are used to process personal data and have some link to the European Union are subject to GDPR requirements. *See* RACHEL F. FEFER & KRISTIN ARCHICK, CONG. RSCH. SERV., IF10896, EU DATA PROTECTION RULES AND U.S. IMPLICATIONS (2020).

10. GDPR, *supra* note 6, at art. 83; *see also* Ben Wolford, *What Are The GDPR Fines?*, GDPR.EU, https://gdpr.eu/fines/ (last visited July 25, 2022).

11. FEFER & ARCHICK, *supra* note 9.

12. Largest fines include U.S. multinational companies such as Google, Marriot, and PwC. Belgium Data protection Authority has fined Google €600,000 for not complying with the "right to be forgotten". In January 2019, French data authorities fined Google €50 million ($56 million USD) after finding Google's use of blanket consent forms and pre-ticked boxes as insufficient, invalid, and unclear consent under GDPR. In July 2019, the UK Information Commissioner's Office (ICO) issued a £99 million ($118 million USD) fine against Marriott after the company discovered an earlier data breach that compromised the passwords and credit cards records of 30 million EU residents. Greece fined U.S. consulting company PwC for failing to gain employee consent for the use of their personal data for analytics purposes. U.S. tech companies investigated, and levied fines, are Facebook, Amazon, Twitter, Instagram, WhatsApp, LinkedIn, Apple, Google, Quantcast, Verizon. *See* Brian Daigle & Mahnaz Khan, *One Year In: GDPR Fines and Investigations against U.S.-Based Firms*, U.S. INT'L TRADE COMM'N, Executive Briefings on Trade (Sept. 2019), https://www.usitc.gov/publications/332/executive_briefings/gdpr_enforcement.pdf.

they have voiced their concerns regarding high costs for compliance, legal uncertainties around imposed obligations, and limitations the law creates on technology development.[13] GDPR's compliance particularly impacts small and mid-sized enterprises (SMEs), creating a *de facto* trade barrier for those with less resources available.[14]

So far, the U.S. policy makers have not reacted to technology disruption the way Europeans did, signaling that current regulatory framework might be robust enough to deal with the effects of technological change on business models and corporations. The U.S. data protection and privacy laws are traditionally tailored to specific sectors of industry broadly leaving the cross-border data flows unrestricted.[15] Thus, instead of passing a comprehensive federal regulation, the authorities have reemphasized the role of agency regulation and oversight in dealing with distributed ledger technology (DLT) that impact market.[16] A quick look at the involvement of government agencies in screening, investigating, and charging blockchain activities confirms the American approach to apply current laws and regulations to DLTs by way of expansion and interpretation.[17] Corporate activities of companies that

13. For the list of companies that dropped out of EU market upon coming into force of the GDPR *see* Hanna Kuchler, *US Small Businesses Drop EU Customers Over New Data Rule*, FIN. TIMES (May 24, 2018), https://www.ft.com/content/3f079b6c-5ec8-11e8-9334-2218e7146b04. The Chicago Tribune, New York Daily News, and LA Times were among the first that temporarily closed their websites to European users. *See GDPR:US News Sites Unavailable to EU Users Under New Rules*, BBC NEWS (May 25, 2018), https://www.bbc.com/news/world-europe-44248448.

14. FEFER & ARCHICK, *supra* note 9.

15. FEFER & ARCHICK, *supra* note 9. The U.S. data protection and privacy laws consists of state and federal laws. Federal laws currently in force include: 1974 U.S. Privacy Act which outlines rights and restrictions regarding data held by US government agencies; 1996 Health Insurance Portability and Accountability Act (HIPAA) which regulates privacy and security in the healthcare industry; 1999 Gramm-Leach-Bliley Act (GLBA) which governs how consumers' non-public privacy information is collected and used in the financial industry; 2000 Children's Online Privacy Protection Act (COPPA) prohibits online companies from asking for Personal Identifiable Information (PII) from children 12-and-under unless there's verifiable parental consent; 2018 Clarifying Lawful Overseas Use of Data Act (CLOUD Act) that compels tech companies to respond to warrants issued by law enforcement agencies to obtain user data stored in the U.S. or in foreign countries. *See* STEPHEN P. MULLIGAN & CHRIS D. LINEBAUGH, CONG. RSCH. SERV., IF11207, DATA PROTECTION AND PRIVACY LAW: AN INTRODUCTION (2019).

16. Some U.S. policy makers favor regulation. *See supra* note 1.

17. To protect the least powerful participants in decentralized networks against false appearance of the market activity or price manipulation, SEC monitors and investigates cryptocurrency exchange and decentralized finance (DeFi). It recently investigated Coinbase over the launch of its new digital asset lending product called Lend. Lend would have allowed customers to earn an annual percentage yield starting at 4% by lending their holdings of a Stablecoin, USDCoin, to other users. The SEC considered Lend to involve a security and claimed that there were not enough investor protections in crypto finance yet. Cryptocurrencies and decentralized finance may evolve to threaten the financial system much the way credit default swaps did ahead of the 2007–08 financial crisis. *See SEC Charges Global Crypto Lending Platform and Top Executives in $2 Billion Fraud*, U.S. SEC. & EXCH. COMM'N (Sept. 1, 2021), https://www.sec.gov/news/press-release/2021-172; *see also* Dan Ennis, *Coinbase Scraps Crypto Lending Product Under Fire from*

utilize DLT are monitored and investigated by specialized agencies such as the Securities and Exchange Commission (SEC), Federal Trade Commission (FTC), Commodity Future Trading Commission (CFTC), Department of the Treasury, the Office of the Comptroller of the Currency (OCC), and the Financial Crimes Enforcement Network (FinCEN).[18] Areas of law such as sales, securities laws, anti-money laundering and counter financing terrorism (AML/CFT), and taxation impose certain obligations on companies that provide technology services.[19] Nevertheless, the general attitude is to leverage investment in the technology by granting innovators regulatory relief from state securities laws and money transmission statutes to improve local economies and public services.[20]

Diverging legal and policy trends explains why Europe passes the GDPR while the United States takes a '*watch and see'* stance when it comes to regulating blockchain.[21] The U.S. and the EU are important commercial

SEC, BANKING DIVE (Sept. 21, 2021), https://www.bankingdive.com/news/coinbase-scraps-crypto-lending-product-under-fire-from-sec/606920/. Coinbase is not the only crypto company whose interest-bearing accounts are under scrutiny. The SEC recently charged BlockFi for failing to register the sales of its crypto lending product. *See BlockFi Agrees to Pay $100 Million in Penalties and Pursue Registration of Its Crypto Lending Product*, U.S. SEC. & EXCH. COMM'N (Feb. 14, 2022), https://www.sec.gov/news/press-release/2022-26.

18. Joe Dewey, *Blockchain and Cryptocurrency Laws and Regulations 2022, USA*, GLOB. LEGAL INSIGHTS (Oct. 10, 2021), https://www.globallegalinsights.com/practice-areas/blockchain-laws-and-regulations/usa.

19. For example, companies are under obligation to run customer identification vetting process or IRS tax cryptos as property. *See id.*

20. For example, Wyoming has created crypto banks to legally allow businesses to hold digital assets. Oklahoma introduced a bill to allow crypto as an instrument of monetary value within the governmental agencies. Arizona has adopted a regulatory sandbox to monitor the development of new emerging industries including blockchain. The law grants regulatory relief and enables companies to test their innovative products for up to two years and 10,000 customers before needing to apply for formal license. Other states, such as Utah, Kentucky, Vermont, Nevada, Hawaii, and Wyoming have followed. *See id.*

21. Several European countries have already introduced legislative regimes to require companies and corporate enterprises to carry out mandatory human rights' due diligence. The best known and most far-reaching is the French Corporate Duty of Vigilance Law. *See* Loi 2017-399 du 27 mars 2017 relative au devoir de vigilance des sociétés mères et entreprises donneuses d'ordre [Law 2017-339 of March 27, 2017 on Relating to the Duty of Vigilance of Parent Companies and Ordering Companies], Journal Officiel de la République Française [J.O.] [Official Gazette of France], Mar. 28, 2017, p. 1. According to the law, the company must set out its approach to assessing and addressing human rights and environmental risks posed by its own activities, those companies which they control, and the activities of those suppliers or contractors with which they have an established commercial relationship. *See* UNITED NATIONS HUM. RTS. OFF. OF THE HIGH COMM'R , UN HUMAN RIGHTS "ISSUES PAPER" ON LEGISLATIVE PROPOSALS FOR MANDATORY HUMAN RIGHTS DUE DILIGENCE BY COMPANIES (June 2020), https://www.ohchr.org/sites/default/files/Documents/Issues/Business/MandatoryHR_Due_Diligence_Issues_Paper.pdf. Laws are products of political processes that reflect the relative power of various organized social groups. Different legal and political systems create different solutions to protect citizens and provide justice when their rights are violated. Civil law systems evolved in France, and later in Germany are "top down" where traditionally lawmakers provided laws that gave judges very little discretion and

partners with massive trade and investment volume that involves online communication and cross-border services, supply chains, research sharing, and supporting technological innovation.[22] They differ, however, in their approaches to data privacy and protection. Differences in the U.S. and EU legal regimes have created uncertainties for U.S. firms running transnational operations, especially after coming under the GDPR's authority.

Another area of tension between the GDPR and blockchain relates to the technology itself. Blockchains are known to be an append-only ledger purposefully designed to render the unilateral deletion and modification of data extraordinarily burdensome to secure data integrity and trust in the network.[23] The ledger's data is resilient as it is simultaneously stored on many computers called nodes so that even if one or several fail, the data goes unaffected. The irreversibility feature of the technology fundamentally contradicts with the GDPR's requirement that data be mutable to secure the right of individuals to rectify information on blockchain or to demand its erasure.[24] The right to erasure provides the data subject with control over personal data

preserved state power over the rights of individuals. Common law systems evolved "bottom up." In the United Kingdom, local courts would protect the rights of the gentry from infringement by the king. Later, merchants would use these same courts to enforce contracts and prevent the expropriation of their property. Culture, indexed by religious traditions and solidarity that generates trust in a population, also appears to affect such laws. *See* Neil Fligstein & Jennifer Choo, *Law and Corporate Governance*, 1 Ann. REV. L. & SOC. SCI. 61 (2005).

22. KRISTIN ARCHICK & RACHEL F. FEFER, CONG. RSCH. SERV., R46917, U.S.-EU PRIVACY SHIELD AND TRANSATLANTIC DATA FLOWS 5 (2021).

23. On blockchain, a hash function representing information as a string of characters and numbers, is a one-way cryptographic function, designed to be impossible to revert. Blocks are continuously added but never removed which explains the blockchain's append-only data structure. Where the relevant consensus-mechanism that is used is proof-of-work, to make any changes the majority of all connected nodes would have to verify again the legitimacy of every effected transaction backwards, unbuild the entire blockchain, block by block, and then rebuild it afterwards, with every such transaction step to be distributed block-wise to all existing nodes. *See* Finck, *supra* note 3, at 3, 75.

24. Article 16 secures the right of individuals to rectification and Article 17 secures their right to erasure of data. GDPR, *supra* note 6, at art. 16, 17. According to Article 17 of the GDPR, the data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; the data subject withdraws consent on which the processing is based or where there is no other legal ground for the processing. Private blockchains can support such requests through an alteration of the relevant transaction record by re-hashing subsequent blocks where this is facilitated by the respective technical and governance set-up. Rectifying data on public and/or permissionless blockchains is, however, much more difficult. This is not because it is strictly impossible from a technical perspective, as every single node can alter its own local copy of the ledger. All nodes could agree to fork to a new version of the blockchain in periodic intervals to reflect requests for erasure. This level of coordination, however, has been said to be difficult to achieve among potentially thousands of nodes. *See* Jean Bacon et al., *Blockchain Demystified: A Technical and Legal Introduction to Distributed and Centralised Ledger*s, 25 RICH. J.L. & TECH. 1, 76 (2018).

that directly or indirectly relates to them and in that sense is a fundamental right to secure data self-determination.[25] The blockchain characteristics create doubts as to whether the modification and erasure of data that is required by the GDPR can ever be implemented. Even if there would be a means of ensuring compliance from a technical perspective, it may be organizationally difficult to get all nodes to implement related changes on their own copy of the database, particularly in public and permissionless blockchains.

Inconsistencies between laws that regulate blockchain, on the one hand, and technical difficulties regarding effective implementation of GDPR right to rectification and erasure, on the other hand, triggers an alternative approach stemming from within the corporate enterprise to provide effective data protection and privacy. Ultimately, protection of individuals' personal data rests with an effective governance solution that safeguards and remedies data breach from within the corporate structure and enables coordination among DLT participants. The emerging decentralized and disintermediated world requires an immediate revisiting of existing corporate governance structure. Firms must go beyond accounting profits and complement their corporate governance (CG) model with corporate social responsibility (CSR). CSR can be viewed as an extension of firms' efforts, voluntary or induced, to foster effective CG, ensuring firms' sustainability via sound business practices that promote accountability and transparency not only to shareholders, but to broader stakeholders. Convergence of CG with CSR affects many types of corporate risks including regulatory, litigation, and reputational risks.[26]

Today, corporations try to distance themselves from the dominant narrative of the 1970's that the sole objective of the business is to increase profit.[27] Yet, corporate surveys suggest that issues related to human rights and CSR continue to be ranked at the bottom of board priorities.[28] It appears that decision-making at the boardrooms and C-Suites continues to be primarily based on maximizing profit for shareholders. The time has arrived to bridge this gap between CG and CSR for private subjects that are driven by

25. Finck, *supra* note 3, at 75.

26. Evidence suggests that firms with higher CSR ratings receive better settlements from prosecutors and have higher resulting market valuations. *See* Harrison G. Hong & Inessa Liskovich, *Crime, Punishment, and the Halo Effect of Corporate Social Responsibility*, NAT'L BUREAU ECON. RSCH., NBER Working Paper Series No. 21215 (May 2015). In addition, research has established that suppliers face a lower likelihood of environmental and social related lawsuits when their corporate customers have better CSR policies. *See see* Gillan, Koch, & Starks, *supra* note 26, at 9.

27. Milton Friedman, *The Social Responsibility of Business Is to Increase Its Profit,* N.Y. TIMES (Sept. 13, 1970), at 17, https://www.nytimes.com/1970/09/13/archives/a-friedman-doctrine-the-social-responsibility-of-business-is-to.html.

28. Lynn S. Paine, *Sustainability in the Boardroom*, 92 HARV. BUS. REV., 86–94 (2014).

profit and function on corporate power.[29] Business today inescapably needs to be sensitive towards fundamental rights of individuals, putting in place a socially sustainable governance framework. Companies must increase their transparency efforts, disclose information on their organization, purpose, activities, and sources of funding, and must accept accountability for their conduct.[30]

The GDPR is a mandatory legal regime to address data breach on digital platforms. Given its financial impact on firms, the law has created a ground for reform of CG and its convergence with CSR. Blockchain-based data breach can be effectively controlled through: 1) GDPR that transforms the role and accountability of the board and management in blockchain based businesses and compels compliance, 2) CSR as a voluntary soft means of human rights due diligence that impacts CG, and 3) technology itself that evolves governance from hierarchy to platforms and provides for decentralized flat governance. Human rights no more belong to public domain with primary responsibility beholding to states and extends to private sector.

The paper proceeds as follows. Section two will subsequently provide an overview of the GDPR as it relates to DLT and illustrates how GDPR regulates, administers, and adjudicates data breach occurring on blockchains. The GDPR acts as a catalyst for restructuring CG of blockchain based businesses. Section three will discuss the interrelation between business and human rights and convergence of CG with CSR. CSR and more recently Environmental, Social, and Governance (ESG) standards for socially responsible investment (SRI) have impacted the traditional agency theory of CG. Given that the impact of corporations on human rights have been recognized for quite some time, they are no longer considered as a mere conduit for financial performance. Accordingly, there is an immediate need to operationalize a human rights policy within the framework of CG to ensure corporate sustainability in the decentralized economy of the future. Section four will discuss the characteristics of blockchain technology and its impact on the CG of decentralized autonomous organizations (DAOs). Blockchain automates governance through smart contracts where all members of the network directly participate in decision makings, provides real time visibility of management activities, transactions and exchange of information, and a suitable environment for implementation of an effective CG converged with CSR/ESG metrics.

By mapping the GDPR regulatory landscape, the relationship and interdependence of CG and CSR, and peculiarities of the technology itself, the

29. PHILIP ALSTON, NON-STATE ACTORS AND HUMAN RIGHTS 19 (2005).

30. Eisuke Suzuki, *Non-State Actors in International Law in Policy Perspective*, in NON-STATE ACTORS IN INTERNATIONAL LAW (Math Noortmann, August Reinisch, & Cedric Ryngaert eds.) 33, 45 (2015).

paper ultimately concludes in section five that the old-world CG model needs to transform considering the profound disruption of business by DLTs. A sustainable CG model inevitably relies on a functioning human rights policy.

II. GDPR and Blockchain: Legal Framework and Regulatory Gap

Blockchains are a class of general-purpose ledger data management and distribution technology designed to achieve resilience through replication and maintained by a consensus algorithm often involving numerous parties.[31] Blockchains combine several technologies and function on a multilayered ecosystem often converging with Artificial Intelligence (AI) for automatization of business processes.[32] They are sequential databases of information secured by methods of cryptographic proof collecting, storing, and processing data in a decentralized manner. Blockchain records verified transactions among parties permanently. Data on blockchains can represent anything we believe and agree it represents, such as goods, services, entitlements, and assets.[33] The potential for a broad usage of the technology is appealing to various actors to achieve different objectives. In the private sector, blockchain enables various forms of digital money, mobile banking, tracking goods, and managing software licenses. It offers a new way of creating, exchanging, and tracking the ownership of financial assets on a peer-to-peer basis. Blockchains also have the potential to register and trade shares of corporate stock and accommodate debt securities and financial derivatives through autonomous execution of smart contracts.[34] The public sector uses the technology to protect critical infrastructure against cyberattacks or for digital identity, voting schemes, operational and budgetary transparency, and traceability of tax fraud.[35] Further applications may exist in government record-keeping of databases for land titles and vital statistics.[36] Thus, blockchain revolutionizes trade as an online chain of value circulation.

31. Finck, *supra* note 3, at 1. Nodes refers to computers that store a local version of the distributed ledger.

32. For example, smart contracts embedded with AI models can execute transactions on blockchain, process payments, or stock purchases and resolve disputes. In the health sector, the convergence of blockchain and AI enables data integrity, transparency, patient tracking and consent management. In supply chains and financial services, blockchain/AI ecosystem facilitate tracking data, accelerating transactions, and increasing visibility for intellectual properties. Blockchains themselves rely on the Internet to operate. *See* IBM, *supra* note 4.

33. Blockchain-based assets can have purely on-chain value (Bitcoin) or be the avatar of a real-world asset (Non-Fungible Tokens, NFTs). Finck, *supra* note 3, at 4.

34. David Yermack, *Corporate Governance and Blockchains*, 21 REV. FIN. 7, 1 (2017).

35. *Id.* at 6.

36. It has been said that blockchains create potential advantages in cost, speed, and data integrity. From stocks and bonds to luxury handbags, and works of art, recording ownership of variety

Technology is not without risks. Decentralization of authority might leave data vulnerable to sabotage where hackers could potentially crack the network and divert assets to themselves.[37] The alternative could be a permissioned blockchain, updated only by authorized participants, or a private blockchain, controlled by a central gatekeeper authority that might appear attractive for security reasons, both of which lack some of the appealing features of an open blockchain.[38] Blockchains are presently applied in a very

of assets on blockchain is being investigated by firms. Further studies suggest that governments can use blockchain for public records such as real estate and automobile titles, birth certificates, driver's licenses, and university degrees. Using blockchains to record stock ownership resolves the companies' inability to keep accurate and timely records of who owns their shares. Blockchains could provide unprecedented transparency to allow investors to identify the ownership positions of debt and equity investors and reduce the opportunity for rent-seeking (an economic concept that occurs when an entity seeks to gain added wealth without any reciprocal contribution of productivity, increasing one's share of existing wealth without creating new wealth) or corrupt behavior by regulators, exchanges, and companies. For shareholders, blockchains could offer lower costs of trading while permitting visible real-time observation of transfers of shares and ownership records. Managerial ownership could become much more transparent, with insider buying and selling detected by the market in real time, and manipulations such as the backdating of stock compensation becomes much more difficult, if not impossible, since blockchain participants are unable to "rewrite history" by changing their entries retroactively. Corporate shareholder voting could become more accurate. Blockchain can further be used for time-stamping the creation of intellectual property to fix property rights with the creator before it can be copied by others. *Id.* at 2–3.

37. The most basic problem for users of open blockchain would be an attack, in which one participant on the blockchain controlled enough mining power to force through a change in the software to benefit themselves at the expense of everyone else. Protecting against these types of attacks may emerge as a significant problem for open source blockchains. Even though Nakamoto's original paper (through which he introduced Bitcoin as the first digital money transacted on blockchain) raised concerns about the possibility of attacks against "honest nodes", it did not consider the possibility of collusion among miners, something recognized as a clear potential danger today. In 2016, a successful hack occurred against the Ethereum platform. In response, the sponsors of Ethereum erased their blockchain from the point of the hack forward by implementing a "hard fork," thereby negating the theft by the hacker. This action, which was supported by 85% of the Ethereum miners, rewrote the history of transactions, and introduced human intervention to negate the unanticipated consequences of a self-executing smart contract. *See id.* at 32–34.

38. In many of the prominent blockchain applications now under development such as the Australian Securities Exchange in Sydney and the Depository Trust Clearing Corp. in New York, the gatekeeper role is assumed by an established "trusted third party" whose actions are constrained by government regulators as well as reputational considerations. A blockchain organized by a powerful sponsor of this type is often referred to as a "private" blockchain, since access for customers requires consent of the gatekeeper. The party with authority to encode new transactions into a blockchain, who can be thought of as a sponsor or gatekeeper for the archive, holds enormous power that potentially poses great risks to individual blockchain participants. The gatekeeper can restrict entry into a market, assess monopolistic user fees, edit incoming data, treat some users preferentially, limit users' access to market data, and possibly share user data with outsiders, among other problems. Private blockchains with central gatekeeper authority concentrate operational risk in a single point of failure beating the entire purpose of the technology to eliminate third party intermediaries in financial transactions. Publishing the sequence of records in a public blockchain essentially crowd-sources the verification function classically played by auditors or bank inspectors, and it is an essential component of the open blockchain structure introduced by Nakamoto for Bitcoin. Nakamoto introduced a blockchain design for Bitcoin where transactions are publicly

narrow area of the economy due to the unknown potential risks, uncertainties regarding its practical future impact and regulatory frameworks, and potential technical limitations to deliver different outcomes.[39]

The European Union's GDPR is a comprehensive regulation on data protection and privacy that primarily seeks to protect fundamental rights of natural persons while ensuring data flows to strengthen Europe's Digital Single Market.[40] It establishes a detailed legislative framework that harmonizes data protection across the European Union.[41] GDPR enforcement lies principally with national data protection authorities (DPAs) according to where violations occur and where companies are headquartered.[42] GDPR applies to any company that processes personal data of EU residents, even if they are not physically located in the EU or process data on servers located outside the EU.[43]

In the European Union, the right to data protection enjoys the status and protections of a fundamental right.[44] Accordingly, individuals known as data subjects have a right to access, rectify, and erase their personal data from digital databases. Furthermore, GDPR identifies legitimate grounds for data processing and sets out rules for data retention, storage, and erasure. The European Parliament rendered a resolution in 2018 mandating blockchain-based applications to comply with the GDPR.[45] Yet, the law retains

announced with no gatekeeper controlling the addition of new blocks. Blockchain is supposed to be a "trust machine," since its algorithms report economic transactions with very high precision without any need for a trusted third party. *See The Great Chain of Being Sure About Things*, THE ECONOMIST (Oct. 31, 2015), https://www.economist.com/briefing/2015/10/31/the-great-chain-of-being-sure-about-things?utm_medium=cpc.adword.pd&utm_source=google&utm_campaign=a.22brand_pmax&utm_content=conversion.direct-response.anonymous&gclid=Cj0KCQjwof6WBhD4ARIsAOi65ahR1MSA48Hg_HzV; *see also* Yermack, *supra* note 34, at 7–8.

39. Current regulations majorly cover initial coin offering (ICOs), cryptocurrencies, know your client (KYC), and Anti-money-laundering (AML). *See* Dewey, *supra* note 18.

40. Finck, *supra* note 3, at 7.

41. GDPR applies to all residents across the EU, three European Economic Area (EEA) member states not part of the EU (Norway, Liechtenstein, and Iceland), and the United Kingdom until the country formally exited the EU. *See* Daigle & Khan, *supra* note 8, at 1.

42. *See* Daigle & Khan, *supra* note 8, at 1.

43. GDPR, *supra* note 6, at art. 3, "Territorial Scope," effective May 25, 2018.

44. Article 8 of the Charter of Fundamental Rights provides that everyone has the right to the protection of personal data concerning him or her. Consequently, personal data must be processed fairly for specified purposes and based on the consent of the person concerned or some other legitimate basis laid down by law. The Charter furthermore provides that everyone has a right to access personal data relating to them, including a right to have such data rectified. *See* Charter, *supra* note 7, at art. 8.

45. Proposition de Résolution déposée à la suite de la question avec demande de réponse orale [Motion for a Resolution on Distributed Ledger Technologies and Blockchains: Building Trust with Disintermediation], Eur. Parl. Doc. (RSP 2017/2772) (2018) at ¶ 33, https://www.europarl.europa.eu/doceo/document/TA-8-2018-0373_EN.html.

uncertainty regarding the way it applies several provisions to blockchain. This is, for instance, the case regarding the concept of anonymous data, the definition of the data controller, and the meaning of '*erasure'* under Article 17 of the GDPR. Below, some of these uncertainties are mapped.

According to the GDPR, personal data is defined as data that directly or indirectly relates to an identified or identifiable natural person.[46] 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."[47] While data stored on blockchains on its face might not seem like personal data due to encryption, hashing, and tokenization, these digital representations can be reversed and ultimately linked to personal data.[48] Blockchain is a "smart environment" that provides for perfect identifiability of information, datafication, and advances in data analytics with potentials for relating data to a person or person in purpose or effect.[49]

GDPR applies to the processing of personal data wholly or partly by automated or other means which form part of a filing system or are intended to form part of a filing system.[50] The initial addition of personal data to a distributed ledger, its continued storage, and further processing for any form of data analysis or reaching consensus on the network constitutes personal data processing.[51]

To secure personal data, GDPR introduces pseudonymization as the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information.[52] Pseudonymized data remains personal data but significantly reduces the link-ability of a dataset with the original identity of a data subject and minimizes risk of data breach. It is not, however, an ultimate safeguard that fully protects personal data. From a legal perspective, pseudonymous

46. GDPR, *supra* note 6, at art. 4, § 1.

47. *Id*. Information on blockchain qualifies as personal data regardless of it being related to one's private or public life. This justifies the broad scope of the GDPR that enforces data protection and not merely data privacy. *See* Article 29 Data Protection Working Party, *Opinion 04/2007 on the Concept of Personal Data* (Eur. Comm'n, Working Paper No. 136, 01248/07/EN, 2007), at 7.

48. Law enforcement officials and regulators can require corporate insiders to disclose their digital wallet identifications, or public keys, under penalty of law. Besides, hackers have shown in the past that they can rehash and decrypt data on blockchain through different methods and get to individuals' personal data. *See* Yermack, *supra* note 34 at 18, 28.

49. Finck, *supra* note 3, at 16.

50. GDPR, *supra* note 6, at art. 2, § 1.

51. *Id.* at art. 4, § 1.

52. *Id.* at art. 4, § 5.

data could be attributed to a natural person using additional information unless transformed to anonymous data.[53]

When data is not identifiable by all the means reasonably likely to be used and therefore not attributed to a natural person using additional information, it is no longer personal data.[54] The data is anonymous if: (i) it is not possible to single out and to isolate some or all records which identify an individual in the dataset, (ii) it is not possible to link records relating to an individual, and (iii) information concerning an individual cannot be inferred.[55] These criteria effectively rule out the existence of anonymous data as ultimately there will always be parties able to combine a dataset with additional information that may re-identify it.[56]

On blockchain, every user has a public key (a string of letters and numbers representing the user), comparable to an account number that is shared with others to enable transactions. In addition, each user holds a private key (also consisting of a string of letters and numbers), comparable to a password that must never be shared with others. Both keys have a mathematical relationship by virtue of which the private key can decrypt data that has been encrypted through the public key. A public key is data that is pseudonymized and can no longer be attributed to a specific data subject unless it is matched with additional information such as a name, an address, or other identifying information.[57] Pseudonymization disguises identities but it is not irreversible. Singling out, link-ability, and inference can link public keys to an identified or identifiable natural person. Where the public key serves to identify a natural person, the public key is personal data under the GDPR.[58]

---

53. *Id.* at Recital 26.

54. Recital 26 of the GDPR foresees that, considering the current state of the art, a 'reasonable' investment of time and financial resources should be considered to determine whether a specified natural person can be identified based on the underlying information. Given that blockchain records transactions perpetually no reasonable analysis can possibly assume that identification remains unlikely in the future.

55. GDPR, *supra* note 6, at Recital 26; *see also* Article 29 Working Party, *Opinion 05/2014 on Anonymization Techniques* (Eur. Comm'n, Working Paper No. WP 216, 0829/14/EN, 2014) 3, 11, 12. To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly.

56. Finck, *supra* note 3, at 25.

57. GDPR, *supra* note 6, at art. 4, § 5.

58. There are DLT use cases where public keys do not relate to natural persons. For example, where financial institutions are using a blockchain to settle end-of-day inter-bank payments for their own accounts public keys would relate to these institutions and not natural persons, meaning that they would not qualify as personal data that is subject to the GDPR. There are, however, ample examples where data subjects have been linked to public keys through the voluntary disclosure of their public key to receive funds, through illicit means, or where additional information is gathered in accordance with regulatory requirements, such as where crypto asset exchanges perform Know Your Customer (KYC) and anti-money laundering duties. Wallet services or exchanges may indeed

Distributed ledgers are often used for tracking of the assets. Transactional data indeed constitutes personal data where it directly or indirectly relates to an identified or identifiable natural person. Both public keys and transactional data can be used in encrypted form or hashed when put on the blockchain. Technical circles presume encryption and hashing anonymize data. Although encryption may significantly contribute to the confidentiality of personal data, it does not render personal data irreversibly anonymous.[59]

Hashing runs information through a mathematical formula or algorithm that provides a unique code of numbers and characters to represent the data. In hashing, the same input always deterministically yields the same output.[60] It is fairly easy to relate a hash to a data subject.[61] Mere use of a hash function will not automatically transform personal data into anonymous data.[62]

---

need to store parties' real-world identities to comply with anti-money laundering requirements. Besides, public keys may also reveal a pattern of transactions with publicly known addresses that could be used to single out an individual user such as through transaction graph analysis. Public keys can be traced back to IP addresses, aiding identification. Bitcoin blockchain encrypted data has been proven to allow for transactions to be traced back to users. Law enforcement agencies across the world have identified individuals through their public keys and forensic chain analysis techniques to identify suspected criminals. *See* Finck, *supra* note 3, at 27.

59. Article 29 Data Protection Working Party, *Opinion 05/2012 on Cloud Computing* (Eur. Comm'n, Working Paper No. WP 196, 01037/12/EN, 2012). It must be noted that there is a tension between anonymity in data protection law and other areas of regulation such as tax evasion or anti-terrorism legislation. The Finance Committee of the French *Assemblée Nationale* indeed suggested banning anonymous cryptocurrencies which rely on tools such as zero knowledge proofs as they facilitate fraudulent and illegal activity such as money laundering and terrorist financing. *See Rapport d'Information par la Commission des Finances, de l'Economie Générale et du Contrôle Budgétaire relative aux monnaies virtuelles* [Information Report by the Committee on Finance, General Economy, and Budgetary Control Relating to Virtual Currencies], Assemblée Nationale (Jan. 30, 2019), http://www.assemblee-nationale.fr/15/pdf/rap-info/i1624.pdf.

60. *See* Finck*, supra* note 3, at 29 ("A cryptographic hash is a mathematical function that is fed an input value which is transformed into an output value of fixed length.").

61. *See* Kevin Nisbet, *The False Allure of Hashing for Anonymization*, TELEPORT (Apr. 30, 2018), https://goteleport.com/blog/hashing-for-anonymization/ (explaining that the biggest limitation of hashing is that hackers have already created rainbow tables of all the possible combinations); *see also* Gunes Acar, *Four cents to deanonymize: Companies reverse hashed email addresses*, FREEDOM TO TINKER (Apr. 9, 2018), https://freedom-to-tinker.com/2018/04/09/four-cents-to-deanonymize-companies-reverse-hashed-email-addresses/ (explaining that it has been suggested that hashing existing email addresses globally would take about ten milli seconds and cost less than one hundredth of a U.S. dollar. As running an email address through the same hashing algorithm will always yield the same result, outputs can be guessed from known inputs. Thus, for hashing to be irreversible, the number of possible inputs must be sufficiently large and unpredictable to prevent all possible combinations. Considering the increasing power and decreasing cost of computing, this is hard to achieve); *see also* Ed Felten, *Does Hashing Make Data "Anonymous?"*, U.S. FED. TRADE COMM'N (Apr. 22, 2012), https://www.ftc.gov/news-events/blogs/tech-ftc/2012/04/does-hashing-make-data-anonymous (concluding that hashing is not an ultimate anonymization technique).

62. *See What to do now about tomorrow's code-cracking computers*, ECONOMIST (July 14, 2022), https://www.economist.com/leaders/2022/07/14/what-to-do-now-about-tomorrows-code-cracking-computers (explaining the National Institute of Standards Technology and computer

Under the GDPR, accountability rests with the controller of data. The data controller is "the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of personal data processing."[63] The data controller determines, respectively, the "why" and the "how" of data processing, what data to process and for how long, which third parties have access to the data, and when, and how data can be manipulated.[64] A factual analysis is needed to determine controllership, meaning where influence over the means and purposes of personal data processing is.[65]

To protect the rights of data subjects, the GDPR requires the controller of data to implement, in an effective manner, appropriate technical and organizational measures at the time of the determination of the means for processing and at the time of the processing itself, and to integrate the necessary safeguards into the processing.[66] To comply with GDPR, the controller must adopt internal policies and implement measures which meet the principles of data protection by design and by default.[67] Such measures consist of transparency in data processing, pseudonymization, data minimization, and

scientists' efforts to develop post-quantum cryptography (PQC) protocols to enable outpacing capabilities of quantum machines and quantum-enabled hackers in light of the current cryptographic protocol's vulnerability to quantum computing of the future that enables code-cracking).

63. GDPR, *supra* note 6, at art. 4, §7.

64. Where an entity decides to rely on a blockchain database, it has decided regarding the means of personal data processing, creating a strong indication that it qualifies as the data controller. A company that relies on a blockchain to manage its accounts and automate payments to its clients also determines the purposes for which it needs this technology to process personal data, and accordingly liable to comply with the GDPR.

65. *See* Case C-131/12 Google Spain v. Agencia Española de Protección de Datos (AEPD), ECLI:EU:C:2014:31, ¶ 34 (May 13, 2014) (emphasizing the need to ensure effective and complete data subject protection through a broad range of the concept of controller. Consequently, the Court qualified the operator of the Google search engine as a data controller, even though it did not exercise control over the personal data published on the web pages of third parties); *see also* Article 29 Working Party, *Opinion 10/2006 on the processing of data by the Society for Worldwide Interbank Financial Telecommunications* (WP128) 01935/06/EN (whereupon Article 29 argues that it was a controller as it exercised significant autonomy in data processing and had decided to establish a US-based data center to disclose data to US authorities. In cloud computing, cloud providers can be considered to determine the means of processing because they chose the software, hardware and data centers that are used.); *see also* Finck, *supra* note 3, at 43 (noting that comparably, the parties that operate a specific blockchain can be considered to influence the means of processing).

66. *See* GDPR, *supra* note 6, at art. 25, §1,2 (requiring that data processing integrates technical and organizational safeguards to protect the rights of data subjects from the outset. For example, GDPR requires pseudonymization as a key measure to ensure that personal data are de-identified (design), while data protection by default could be interpreted as ensuring that the least privileged level of access is the default setting for all users. GDPR requirement for data protection by design and by default suggests a complementary relationship between data security and privacy).

67. *Id.* at Recital 78.

enabling the data subject to monitor processing.[68] At the time personal data is collected, a data controller must reveal its own identity and contact details.[69] Data controllers may have insufficient control over the data and only see encrypted data. This results in a situation where many entities have legal responsibilities in relation to processing operations that they cannot control.

Personal data shall be processed lawfully, fairly, and in a transparent manner in relation to the data subject.[70] Personal data processing will be lawful where there is a legal ground that permits such processing.[71] Additionally, data subjects might willfully provide consent to data processing.[72] Data processing is also lawful where it is necessary for the performance of a contract to which the data subject is party or to take steps at the request of the data subject prior to entering a contract.[73] Processing may also occur where it is necessary for compliance with a legal obligation to which the controller is subject. For instance, personal data is regularly processed to comply with Know Your Customer (KYC) and AML/CFT requirements, which are indeed imposed by law.[74]

In addition, personal data must be collected for specified, explicit, and legitimate purposes.[75] Data collection and processing shall be limited to only what is necessary in relation to the purposes for which they are processed.[76] Inaccurate personal data must be reasonably erased or rectified without delay regarding the purposes for which they are processed.[77] Personal data must be

68. *See* Finck, *supra* note 3, at 32-35 (listing some of the methods used to fulfill data protection by design and by default are zero-knowledge proof, Stealth addresses, homomorphic encryption, state channels, ring signatures, adding noise to the data, chameleon hashes and editable blockchains, data minimization and storage limitation, and pruning).

69. *See* GDPR, *supra* note 6, at art. 13, §1 (explaining the identity and contact details of the controller, information regarding the purposes of processing, information regarding the recipients and categories of personal data, and whether the controller intends to transfer the data to a third country).

70. *See id.* at art. 5, § 1(a).

71. *See id.* at art. 6.

72. *Id*. at art. 4, § 11 (defining consent as "any freely given, specific, informed, and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her); *see id*. at art.7, § 3 (providing that consent can only be informed where the purpose of processing and the controller's identity are known to the data subject. The data subject, however, has the right to withdraw his or her consent at any time).

73. *Id.* at art. 6, § 1(b).

74. *Id.* at art. 6, § 1(c).

75. *Id.* at art. 5, § 1(b); *see* Finck, *supra* note 3, at 65-66 (considering the append-only nature of blockchain databases, once it is on the ledger, data remains stored and continues to be processed pursuant to the modalities of the used consensus algorithm. The storage and subsequent processing of such data could be potentially incompatible with the purpose limitation principle).

76. GDPR, *supra* note 6, at art. 5, § 1(c).

77. *Id.* at art. 5, § 1(d).

kept in a form which permits identification of data subjects for no longer than necessary for the purposes that the personal data are processed.[78] Furthermore, processing must ensure security, confidentiality, and integrity of personal data, including protection against unauthorized or unlawful processing, accidental loss, destruction or damage.[79]

It should be transparent to individuals that their personal data are collected, used, consulted, or processed.[80] The GDPR principle of transparency requires that "any information and communication relating to the processing of those personal data be easily accessible and easy to understand."[81] Data subjects must be aware of the risks involved in processing.[82] Where there are no channels of communication between the controller and data subjects, transparency requirements are violated.

The GDPR requires any inaccurate data be rectified or erased without delay.[83] This is in contrast with the append-only feature of blockchain where data can only be removed or altered in extraordinary circumstances. The replicated nature of data on distributed networks violates the data minimization requirement under the GDPR. The storage limitation requirement mandates that no obsolete data be retained.[84] Blockchains are set up in a manner that can hardly accommodate and comply with the law.

Data subjects enjoy explicit rights under the GDPR. The processing of personal data is only allowed where data subjects have given their explicit consent or where the information is necessary to meet other legal requirements.[85] Under the GDPR, data subjects have the right to know the reason why their personal data is being processed, who the personal data will be shared with, how long the personal data will be kept, and how to exercise applicable data protection rights. When data subjects receive their personal data after an access request, they have several additional data protection rights. If personal data is inaccurate, data subjects have the right to have the data corrected without undue delay. If personal data is incomplete, data subjects have the right to have the data completed. Furthermore, data subjects

78. *Id.* at art. 5, § 1(e).

79. *Id.* at art. 5, § 1(f).

80. *Id.* at Recital 39.

81. *Id.*

82. *Id.*

83. *Id.* at art. 5, § 1(d).

84. *Id.* at art. 5, § 1(e).

85. Article 4, § 11 of the GDPR requires that the data subject's consent be informed. GDPR, *supra* note 6, at art. 4, § 11. The Court held in *Bara* that "the requirement to inform the data subjects about the processing of their personal data is even more important since it triggers the data subjects' subsequent right to access to, and right to rectify, the data being processed and their right to object to the processing of those data.' *See* Case C-201/14 Smaranda Bara and Others v Presedintele Casei Nationale de Asigurtiri de Sinfitate and Others, 2015 ECLI:EU:C:2015:638, ¶ 33.

can ask for their data to be deleted altogether. Finally, data subjects have a right to make a complaint to the DPAs and petition for redress of grievances.

Data subjects primarily have a right to access their personal data.[86] This requires adequate governance mechanisms that enable effective communication and data management.[87] Following the right to access, data subjects have the right to obtain, without undue delay, the rectification of inaccurate personal data.[88] Blockchains are an append-only ledger designed to minimize the possibility of unilateral data deletion and modification to secure data integrity and trust in the network. Blockchains claim to be irreversible.[89] This feature of the technology fundamentally contradicts with the GDPR's requirement that data be mutable. Securing an effective implementation of the right to rectification on blockchain requires technical solutions, on one hand, and governance solutions, on the other, to enable coordination among the many participants.

Furthermore, the controller has the obligation to erase data without undue delay where: 1) personal data have been unlawfully processed, 2) data are no longer necessary in relation to the purposes for which they were collected and processed; 3) the data subject withdraws consent, or 4) there are no overriding legitimate grounds for the processing.[90] The right of data subjects to erasure is considered as a right to data self-determination. Nevertheless, deleting data from blockchain seems to beat the entire purpose of the technology which its distinguishing features are tamper-proof, append-only, irreversible, and immutable.[91] Even if the technology can provide a solution,

86. *Id.* at art. 15.

87. *See* Finck, *supra* note 3, at 72.

88. *See* GDPR, *supra* note 6, at art. 16.

89. Private blockchains can support such requests through an alteration of the relevant transaction record by re-hashing subsequent blocks where this is facilitated by the respective technical and governance set-up. Rectifying data on public and/or permissionless blockchains is, however, much more difficult, and individual actors are not able to comply with such requests. This is not because it is strictly impossible from a technical perspective to do so, much to the contrary as every single node can alter its own local copy of the ledger (provided that they can identify the relevant data to be rectified as this is far from evident where the relevant data is encrypted). However, even if all nodes, miners, and users were considered to in fact qualify as the data controllers liable to implement data subject rights, this would not necessarily provide effective protection for data subjects. This is so as even though all nodes could agree (through a contract or another form of agreement) to fork to a new version of the blockchain in periodic intervals to reflect requests for erasure. This level of coordination has been said to be difficult to achieve among potentially thousands of nodes. *See* Jean Bacon et al., *supra* note 24, at 77.

90. *See* GDPR, *supra* note 6, at art. 17.

91. On blockchain, hashing is a one-way cryptographic function that groups together multiple transactions in a single block and adds that block to the existing chain of blocks. *See* Finck, *supra* note 3, at 3. The blocks include a hash of all transactions contained in the block, a timestamp, and a hash of the previous block that creates the sequential chain of blocks. *See id.* The cryptographic function of hash chaining makes blockchains tamper-proof and increases transparency and accountability. *See id.* "Indeed, because of the hash linking one block to another, changes in one block

from a governance perspective, it would be organizationally difficult to get all the participants of the network to implement related changes on their own copy of the database.[92] Thus, there is an immediate need for innovative governance designs for blockchain.

The GDPR further provides data subjects with a right to obtain a restriction on processing, or object to the processing of personal data altogether.[93] Most importantly, data subjects have a right to human intervention under the GDPR. Individuals have the right not to be subject to a decision based solely on automated processing, including profiling.[94]

The GDPR ensures the right of all individuals to demand an explanation for any significant decisions made by machines at all levels (when data is obtained, when a decision is made, when an individual's consent is obtained, or when an individual requests information), and enables data subjects' recourse to human authorities, thereby mitigating the effect of data misuse. This includes provisions on individual notification and access rights specific to automated decision-making when information is collected directly from individuals or from third parties. The disclosure of information must be meaningful about the logic involved, as well as the significance and the

change the hash of that block, as well as of all subsequent blocks." *Id*. Because blocks are continuously added but never removed, a blockchain can be qualified as an append-only data structure. *See id.* at 6. Blockchain networks are resilient due to replication because data are simultaneously stored on many nodes so that even if one or several nodes fail, the data goes unaffected and there is no central point of failure at the hardware level. *See id.* at 3. Connected nodes use proof-of-work as the consensus-mechanism to verify transactions. *See id.* at 5. These characteristics of blockchain creates doubts as whether the modification and erasure of data that is required by the GDPR can ever be implemented.

92. One of the technical solutions suggested by the French Data Protection Authority (CNIL) is the destruction of the private key, which would have the effect of making data encrypted with a public key inaccessible. The CNIL has suggested that erasure could be obtained where the keyed hash function's secret key is deleted together with information from other systems where it was stored for processing. Other solutions are to design editable blockchains that are forgetful or use pruning, chameleon hashes and zero knowledge proofs. Some have indeed predicted that in the future there may be new automated technology that enables reversibility, such as corrective operation that can occur automatically using smart contracts. *See* Finck, *supra* note 3, at 76–77.

93. GDPR, *supra* note 6, at art. 18, 21. Article 21 GDPR provides a right to the data subject to object to any processing of personal data that directly or indirectly relates to them where such data is processed by the data controller. Where the data subject exercises that right, the data controller must stop processing this personal data unless it is in a position to demonstrate compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defense of legal claims. Compelling legitimate grounds for processing enables the data controller to reject data subject's request to exercise their right to a restriction of processing. The integrity of blockchain records may qualify as such a legitimate interest. While there must be a balance between the interests of the data controller and of the data subject, the European Court of Justice (ECJ) has previously established that the privacy of the data subject supersedes the interests of the company. *See* Case T-194/04 *Commission of the European Communities v Bavarian Lager*, 2007 EU:T:2007:334.

94. *Id.* at art. 22, § 1.

envisaged consequences of processing for the data subject. The GDPR due process safeguards includes human intervention with appropriate authority to change the decision. This systemic accountability involves both internal and external auditing. Compliance with GDPR requires a combination of measures including technology, human intervention, and internal processes.[95]

The GDPR is designed to secure a balance between data subjects' rights and data controllers' obligations in a context of unbalanced power-relations. Data protection enjoys the status of a fundamental right, yet, it is not an absolute right, and must instead be balanced against other fundamental rights based on proportionality principle. It should further be noted that not all GDPR provisions are relevant to all businesses. Based on the business activities and the industry needs, corporations can single out the most relevant GDPR provisions in setting internal governance policies for compliance. While this does not mean that they are released of any obligations under the law, such obligations must be balanced against competing and legitimate corporate interests.[96] These balancing interests between the rights of data subjects and obligations of data controllers are well reflected in several cases where the national courts reduced or thrown out entirely the fines imposed by DPAs.[97]

95. For example, to secure the rights of data subjects under GDPR, the right to access and correct data can be achieved through process, the right to erasure, objection to the processing of data and not to be subject of automated decision making and data portability can be achieved through technology and to be informed about how data about data subjects are collected, processed, and used human intervention is required. Communicating a breach to the DPA requires a strong process performed in conjunction with the corporate communications department to ensure consistency between the message communicated to affected natural persons after a breach and the notification to the DPA. Obligations of controllers to obtain meaningful consent from data subjects can be done through technology. Data protection impact assessment requires human intervention through appointment of data protection officer. Record of processing, data protection by design and default, ensuring security are fulfilled through technology. Data governance requirements of GDPR is achieved using technology, accompanied with strong internal policy and process and human roles and responsibilities. These require the board preparedness and responsiveness to modern issues surrounding data. The corporate conversation must be guided beyond mere mechanical regulatory compliance and operating model impacts. The corporate sensitivity towards the rights of the data subjects and business incentives such as the culture change around data can outweigh the regulatory requirements for GDPR compliance. *See* Guy Pearce, *Reporting on GDPR Compliance to the Board*, 1 ISACA J. 32 (Jan. 1, 2019) https://www.isaca.org/resources/isaca-journal/issues/2019/volume-1/reporting-on-gdpr-compliance-to-the-board.

96. Charter, *supra* note 7, at art. 52, § 1.

97. At least six large fines have been reduced either through court action or subsequent decisions by DPAs. In November 2020, a Bonn district court reduced a December 2019 €9.55 million fine issued against 1&1 Telecom GmbH to €900,000 for being unreasonably high. €18 million fine issued by Austria's DPA was tossed by an Austrian court for failing to link violations to a specific person and prove that person knew or did nothing to stop the violations. The United Kingdom's largest fines issued against Marriott in November 2018 and British Airways in July 2019 were both reduced by the UK Information Commissioner's Office in October 2021 from €112 million to €20.5

A. Concluding Observation

Blockchain is strongly linked and have an impact on fundamental right of individuals to protection of their personal data. This fundamental right is preserved through series of principles as explained above. To comply with the GDPR, both system design and blockchain governance matter.[98] The GDPR poses governance and risk management challenges for companies, large or small, operating either directly in the EU, or indirectly via organizations operating in the EU. These risks and challenges arise not only because of the potentially significant monetary costs of compliance but also the costs of any legal proceedings and damages to organizational reputation.[99] Considering the risks of violating rights of natural persons posed by the processing, the controller shall implement governance measures capable of ensuring respect, protect, and remedy for the principles of GDPR. This includes existence of efficient channels of communication between data subjects and data controllers. It further includes access to redress when violations occur. Where data processing is likely to result in a breach of fundamental rights, preventive measures such as Data Protection Impact Assessment (DPIA) need to be in place to determine the impact of processing on personal data.[100]

GDPR has created a liability framework for corporate board and management. It has potential implications for board composition, board accountability, and transparency.[101] Compliance with GDPR is directly linked to the board ability to anticipate and identify risks, allocate resources, enable transparent information flows, and review and adapt to change. The board mitigates risk of incurring financial penalties by ensuring compliance.[102] It is also the board's responsibility to mitigate the reputational risk caused by violation of the law. To protect personal data, board members need to actively be involved in certifying data protection, ensuring cybersecurity, and approving

million and €207 million to €22.1 million, respectively. Rather than basing fines on the economic value of the firm in violation, the courts emphasized the proportionality of fines to the violations. *See* Daigle & Khan, *supra* note 8 at 11–13.

98. Article 25 of the GDPR imposes an obligation on data controllers to implement technical and organizational measures capable of ensuring respect for the principles of European data protection law. GDPR, *supra* note 6, at art. 25. The European Court of Justice (ECJ) held in *Digital Rights Ireland* that the essence of Article 8 of the Charter of Fundamental Rights requires the adoption of technical and organizational measures that are able to ensure that personal data is given effective protection against any risk of abuse and against unlawful access and use. *See* Joined Cases C-293/12 & C-594/12 *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and K. . .rntner Landesregierung*, 2014 ECLI:EU:C:2014:238, §§ 40, 66–67.

99. Ingley & Wells, *supra* note 5, at 105–13.

100. GDPR, *supra* note 6, at art. 35, § 1.

101. Ingley & Wells, *supra* note 5, at 105–13.

102. The up to 4 percent of global revenue fine under the GDPR can endanger the survival of smaller businesses.

internal policies and actions. Directors must be responsive to how, when and where they store documents that contain data of individuals from the EU. They need to deal in specifics, rather than take an "overview" approach.[103] GDPR further impacts the c-suite and corporate management.[104]

Data protection and privacy requires board action while directors seem to largely lack technology governance skills to inform their decisions.[105] Directors must improve their understanding of the implications of the GDPR, the current adequacy of their corporate structures for ensuring data protection and privacy, as well as risk mitigation and prevention of data breaches. With the massive and ongoing emergence of DLTs that carry business activities there is an urgent need to revisit corporate governance. Failure to understand that business is not as usual for the broad and management will negatively impact the corporate performance. Corporate governance can provide both short-term solutions for risk management and long-term solutions for corporate resilience to ensure the future of unforeseen array of risks.[106] Companies must implement suitable measures, at the outset and as processing continues, to safeguard the data subjects' rights and legitimate interests.

The GDPR regulates corporate obligations with regards to the fundamental right of individuals to protection of their personal data, administers implementation of those obligations through its enforcement tracker, and adjudicates violations through DPAs. It has created a comprehensive self-contained legal regime that requires corporate governance adaptation and

103. Andrea Bonime-Blanc, *A Strategic Cyber-Roadmap for the Board*, HARV. L. SCH. F. ON CORP. GOVERNANCE & FIN. REG (*Jan. 12, 2017),* https://corpgov.law.harvard.edu/2017/01/12/a-strategic-cyber-roadmap-for-the-board/.

104. To give examples of how GDPR impacts the C-Suite, a Chief Executive Officer is accountable for reputation, compliance, and operational risks. A Chief Financial Officer is accountable for financial penalties. A Chief Information Officer is responsible for systems changes and IT governance, and the data portability. A Chief Data Officer is responsible for data changes and data governance meaning that under GDPR responsible for data rectification, completeness, and accuracy. A Chief Marketing Officer is responsible for consent by affirmative act establishing a freely given, specific, informed, and unambiguous data subject's agreement to the processing of their personal data. A Chief Operations Officer is responsible for the rights of the data subject not to be solely subject to automated decision making. A Chief Human Resources Officer is responsible for corporate code of conduct. *See* Pearce, *supra* note 95.

105. Surveys show that a considerable percentage of directors think that cybersecurity risk is "out of their hands." Cybersecurity expertise has not been a core strength sought in candidates for most director positions who mostly have finance, legal and business backgrounds. The percentage of companies with technology expertise on the board are slim while a high percentage of director consider technology expertise a key skill for new directors. PwC's 2016 *Annual Corporate Directors Survey* reported that 81 percent are at least moderately engaged with overseeing the risk of cyber-attacks. However, about one in five directors say their management teams don't sufficiently, or at all, provide the board with adequate security metrics. *See* Bonime-Blanc, *supra* note 103.

106. Ingley & Wells, *supra* note 5, at 111.

adjustments.[107] In this sense, GDPR is a law that compels companies to take proactive steps to address violations of data breach within the corporate structure.

Beyond the GDPR mandatory scope that imposes responsibilities on the board for data protection and privacy, the CG of blockchain based businesses is impacted by set of community standard soft laws known as CSR and ESG that require corporate boards to play an active role in setting policies to mitigate data breach. Accordingly, the next section discusses the interrelation between human rights and business, and the evolution of CG theory with CSR.

III. Human Rights and Business: Convergence of Corporate Governance with Corporate Social Responsibility

A. Human Rights and Business: An Overview

The impact of corporate activities on individual and citizens' rights is not a recent development. For decades, environmentalists, civil society activists, and policy makers have voiced their concern over harmful corporate activities that negatively impact people and the planet.[108] The end of the Cold

107. A self-contained regime is a system of '*lex specialis*' institutionalized through substantive rights and obligations accompanied by procedural rules that administers their implementation and an adjudicative body that settles the disputes.

108. The civil society advocacy groups have voiced their concerns surrounding irresponsible corporate activities and business entities' negative impact on labor, environment, and human rights for quite some time. In the United States, the consumer protection movements resulted in Federal Trade Commission (FTC) investigations leading to agency reform regarding automobile safety, water, and air pollution. The enactment of the Freedom of Information Act, Foreign Corrupt Practices Act, Clean Water Act, Consumer product Safety Act, and Whistleblower Protection Act are the result of these civil society movements. When the World Trade Organization—an inter-governmental organization regulating trade—was born in 1995, it led to public concerns that the adjudication arm of the organization, the Dispute Settlement Body, would decide from a purely economic perspective and ignore the local environmental and social values of the American people. The voice of environmentalists later echoed in the so-called "Battle of Seattle," which were protests held during the WTO Ministerial Conference in Seattle in 1999. *See* Clyde Summers, *The Battle in Seattle: Free Trade, Labor Rights, and Societal Values*, 22 U. PA. J. INT'L ECON. L. 61, 61–63 (2001). Ralph Nader, a well-known American political activist believed that the WTO would institutionalize a global economic and political structure that makes every government increasingly hostage to an unaccountable system of transnational governance designed to increase corporate profit with little attention to social and ecological considerations. His opinion is well described in his own words "[u]nder the WTO many decisions affecting people's daily lives are being shifted away from local and national governments and being placed increasingly in the hands of unelected trade bureaucrats sitting behind closed doors in Geneva, Switzerland. These bureaucrats are empowered to dictate whether people in California can pursue certain actions to prevent the destruction of their last virgin forests or determine if carcinogenic pesticides can be banned from their food, or whether the European countries have the right to ban the use of risky biotech materials in their food. Moreover, once the WTO's tribunals issue their rulings, there is no way to escape the consequences. Worldwide conformity or continued payment of fines is required. At stake is the

War and the triumph of a free market economy coincided with a more active role of private entities as a legitimate force for development and prosperity.[109] With this increasing activity came numerous scandals.[110] Unchecked private activities with impunity coupled with abuse of authority resulted in fiascos.[111] Corporations potentially impact human rights by employing child or forced labor, discriminatory recruitment policies, and damaging the environment. They can indirectly create an incentive to the government to violate human rights for business purposes or support authoritarian regimes by providing infrastructure, financial means, or international credibility. There is, however, a lack of collective will to agree upon a binding instrument for corporate human rights liability on international level.[112] Binding

very basis of democracy and accountable decision-making that is the necessary foundation of just distribution of wealth and adequate health, safety, human rights, and environmental protections. An erosion of democratic accountability, and the local, State, and national sovereignty that is its embodiment, has taken place over the past several decades." RALPH NADER, *Introduction in* THE WTO: FIVE YEARS OF REASONS TO RESIST CORPORATE GLOBALIZATION 6 (Greg Ruggiero ed., 1999).

109. ALSTON, *supra* note 29, at 7.

110. The Iraq war is one of the examples where the role security private contractors played in providing security and reconstruction services gave them a nickname of 'private for-profit militias.' They were taking over tasks normally delivered by public authorities, permitted to operate within a legal vacuum out of reach of U.S. or other international courts. *See* David Barstow, James Glanz, & Kate Zernike, *Security Companies: Shadow Soldiers in Iraq*, N.Y. TIMES (Apr. 19, 2004), https://www.nytimes.com/2004/04/19/world/security-companies-shadow-soldiers-in-iraq.html.

111. During the 1990s, the Shell Oil Company consortium partnered with state-owned Nigerian oil company and exploited oil reserves in Ogoniland with zero consideration of the health or environment of the local communities disposing toxic wastes into local waterways causing spills in proximity of villages that consequently caused several skin infections, respiratory ailments, and reproductive problems. Corporate activities infringing upon the rights of citizens raised voices for corporate accountability for human rights violations. *See* ALSTON, *supra* note 29, at 13.

112. Policy guidance frameworks such as the United Nations Conference on Trade and Development (UNCTAD) Investment policy Framework for Sustainable Development, International Institutde for Sustainable Development (IISD) model International Agreement on Investment for Sustainable development, and the Organisation for Economic Co-operation and Development's (OECD) effort to create a multilateral agreement on investment have been abandoned in the past due to lack of support. WTO's similar initiatives failed in 2004 due to concerns regarding undue restrictions the agreement would create regarding regulatory freedom of states. Despite being the crafter of the international legal order and the champion of international rule-based system, the United States itself has a long history of commitment to pragmatism over legalism in international law. *See generally*, JEFFREY L. DUNOFF, *Does the United States Support International Tribunals? The Case of the Multilateral Trade System* in THE SWORD AND THE SCALES: THE UNITED STATES AND INTERNATIONAL COURTS AND TRIBUNALS 336 (Cesare P. R. Romano ed., 2009). Deference to national over international authorities in making and enforcing policies has its roots in lack of direct accountability of international treaty regimes to American people. THOMAS M. FRANCK, *Can the United States Delegate Aspects of Sovereignty to International Regimes?*, *in* DELEGATING STATE POWERS: THE EFFECTS OF TREATY REGIMES ON DEMOCRACY AND SOVEREIGNTY 2–3 (Thomas M. Franck ed., 2000). The supramacy of the U.S. national policies over international law and reluctancy to join international legal regimes manifests itself in other areas of interantional law beyond corporate human rights liability. For example, domestic opposition to the international trade law regime has been evident during the Uruguay Round negotiations establishing the WTO. *See*

corporation with human rights obligations confronts legal, political, and business impediments. States are reluctant to form a collective will to regulate private practice as they enjoy having an open hand in treating them. Business entities themselves tend to perform better under less restrictive regulatory regimes where the rights and obligations are blurry and open to broader interpretation. Traditionally, the corporate structure has been associated with an inherent tendency to create a category of confidential or secret information which is held within the corporate person and is the object of "*executive privilege*" and by its nature is not open to public circulation but is subject to internal control.[113] Too much transparency at times conflicts with legitimate requirements of commercial confidentiality and trade secrets.

As a general principle, corporations are subject to laws of the jurisdiction in which they are registered or have their headquarters or major operations and place of business.[114] It is natural for national jurisdictions to regulate the behavior of corporations domestically. When it comes to transborder regulatory framework, the U.S. has been *avant-garde* in stipulating civil liability against private entities of any nationality (U.S. or foreign) through the

World Trade Organization (WTO) Dispute Settlement Review Commission Act: Hearing on S. 16 Before the S. Comm. on Fin., 104th Cong. (1995); *WTO Dispute Settlement Review Commission Act*, H.R. 1434, 104th Cong. (1995). The Administration at the time issued a Statement of Administration Action affirming that the decisions of the WTO DSB have no binding effect under the U.S. law and any changes to the U.S. law would remain at the sole discretion of the Congress. *See* Uruguay Round Agreements Act, H.R. Res. 5110, 103d Cong. (1994) (enacted). For later debates, *see* H.R. Rep. No. 106-672 (2d Sess. 2000) which includes a report from the U.S. House of Representatives Committee on Ways and Means on Withdrawing the Approval of the United States from the Agreement Establishing the World Trade Organization. This was similarly evident during the Congressional debates on creation of the International Trade Organization (ITO) that led to the decision of President Truman to abandon his efforts to seek Congressional approval of the ITO Charter in December 1950. William Diebold, a member of the Council on Foreign Relations and former member of the U.S. State Department's Commercial Policy Division, in an essay published in October 1952 explained that the Cold War and changes in world politics impacted the priorities in American foreign policy. In addition, American domestic politics (Republican gains in November 1950 elections) coupled with the opposition of the American businesses convinced President Truman not to seek approval of the International Trade Organization (ITO) Charter in the Congress. *See* WILLIAM DIEBOLD, *The End of the I.T.O.*, *in* 16 ESSAYS IN INT'L FIN. 3 (Princeton Univ. ed., 1952); *see also* Richard Toye, *Developing Multilateralism: The Havana Charter and the Fight for the International Trade Organization, 1947-1948*, 25 INT'L. HIST. REV. 282, 283 (2003); PETER VAN DEN BOSSCHE, THE LAW AND POLICY OF THE WORLD TRADE ORGANIZATION: TEXT, CASES AND MATERIALS 80–81 (2005). For President Truman's decision not to seek approval for the ITO Charter in Congress, *see Future Administration of GATT*, Announcement to the Press (Dec. 6, 1950), *in* 23 DEP'T ST. BULL., Dec. 1950, at 977.

113. H. PATRICK GLENN, *Transparency and Closure in* RESEARCH HANDBOOK ON TRANSPARENCY 17–18 (Padideh Ala'i & Robert G. Vaughn eds., 2014).

114. 28 U.S.C.A. § 1332 (c). In Hertz Corp. v. Friend, the Supreme Court determined that a "nerve center" test must be applied to determine the corporation's principal place of business. The "nerve center" of the corporation is a place where its officers direct, control, and coordinate the corporation's activities. *See* Hertz Corp. v. Friend, 559 U.S. 77 (2010).

Alien Tort Claims Act (ATCA) for breach of the law of nations.[115] The ATCA does not grant new rights to aliens, but simply opens the federal courts for adjudication of the rights already recognized internationally. To be actionable under the ATCA, a defendant's conduct must violate "well-established universally recognized norms."[116]

One of the seminal cases investigated by the U.S. courts under the premise of the ATCA is the case of *Presbyterian Church of Sudan v. Talisman Energy Inc*.[117] The court affirmed in this case that corporations, like any other private actor, can positively be found liable for violations of human rights.[118] This was a rather progressive decision since relevant precedents at the time supported a view that human rights obligations are solely imposed on states. The persuasive legal argument for the court rested on the notion that what is illegal for an individual should be equally illegal for a group of individuals who established themselves as a corporation and formed to make

115. The Alien Tort Claims Act, 28 U.S.C. § 1350.

116. Kadic v. Karadzic, 70 F.3d 232, 239 (2d Cir. 1995) (quoting Filartiga v. Pena-Irala, 630 F.2d 876, 888 (2d Cir. 1980)).

117. 453 F. Supp. 2d 633 (S.D.N.Y. 2006). Talisman Energy Inc. was a Canadian multinational oil and gas exploration and production company. In the late 90s, while the second Sudanese Civil War was underway, Talisman purchased Arakis Energy, a business heavily involved in the Sudan Oil industry through Greater Nile Petroleum Operating Company (GNPOC). The government of Sudan was at the time almost entirely reliant on oil revenues to finance the war, for which it was later accused of serious human rights violations, genocide, and forced displacement for oil exploration and exploitation. NGOs started a campaign for international divestment in Talisman shares and pushed the Canadian government to penalize the company for its collaboration with the Sudanese government in ethnic cleansing of civilians in southern Sudan surrounding oil concessions to facilitate exploration and extraction of oil. The Presbyterian Church sued the company in an American Court for genocide, alleging that Talisman assisted Sudanese government to bomb churches, attack villages and kill church leaders to clear way for access to oil. In an unprecedented decision, the U.S. District Court for Southern District of New York accepted to hear the case but later dismissed it due to lack of admissible evidence to support claims against Talisman Energy. This was an evident case of universal jurisdiction for domestic courts over a foreign private entity that has no minimum contact with the U.S. territory. Talisman moved to dismiss the case on several basis of lack of subject matter jurisdiction, lack of personal jurisdiction, lack of plaintiff' standing, forum *non conveniens*, international comity, act of state doctrine, political question doctrine, failure to join necessary and indispensable parties, and because equity does not require a useless act. The court, however, denied the motion to dismiss based on finding jurisdiction according to 28 U.S.C. § 1350. The Act states that "the district courts shall have original jurisdiction of any civil action by an alien for a tort only, committed in violation of the law of nations or a treaty of the United States." The court reasoned that the jurisdiction is definitive since the allegations of genocide, war crimes, torture, and enslavement violate universally recognized norms of international law. These types of acts, if proven true, would constitute behavior manifestly in violation of the most basic rules of international law and, indeed, of civilized conduct. Such acts violate peremptory norms, or *jus cogens*.

118. Presbyterian Church of Sudan v. Talisman Energy, Inc., 244 F. Supp. 2d 289 (S.D.N.Y. 2003).

a profit.[119] The ATCA, therefore, grants federal courts subject matter jurisdiction for certain torts occurred anywhere in the world.[120] In the American legal system, corporate liability can even extend to criminal liability.[121]

The ATCA extraterritorial jurisdiction has by no means gained general international praise or advocacy.[122] Historically, corporations were untouched by human rights obligations.[123] There have been efforts to recognize the human rights liability of corporations, yet the efforts have remained at the level of soft law and guiding principles.[124] Implementation of these

119. Jose E. Alvarez, *Are Corporations "Subjects" of International Law?*, 9 SANTA CLARA J. INT'L L. 1, 4 (2011).

120. Douglas M. Branson, *Holding Multinational Corporations Accountable? Achilles' Heels in Alien Tort Claims Act Litigation*, 9 SANTA CLARA J. INT'L L. 227 (2011).

121. David K. Millon, *The Ambiguous Significance of Corporate Personhood,* 2 STAN. AGORA ONLINE J. LEGAL. PERSP. 39 (2001); *see also* Alvarez, *supra* note 118. There is precedent in American courts that corporations are criminally liable for the acts of their directors, officers, and employees independent of the individuals who are liable for crimes they commit on behalf of or to further the interest of the corporation. Evidently, the consequence of crimes committed by corporations is not time in prison but rather it is sanctioned with fines, loss of license, and the like.

122. *Case Concerning the Arrest Warrant of 11 April 2000 (Democratic Republic of Congo v. Belgium)*, (2002) 41 ILM 536, Joint Separate Opinion of Judges Higgins, Kooijmans and Buergenthal, ¶ 48. Beyond ATCA, there are number of other U.S. laws such as the U.S. Foreign Corrupt Practices Act of 1977 to prohibit bribery of foreign governments by US corporations, Uyghur Act that aims to fight imports to the U.S. from human rights violators, report requirements on human rights and environmental compliance under the Securities laws.

123. The UN started its efforts in drafting a code of conduct for corporations back in the 1970s. *See Draft United Nations Code of Conduct on Transnational Corporations*, UN Doc. E/1983/17/Rev.1 (1983). In those years, the role of corporations was defined in relation to their impact on the new international economic order, and the sovereignty of the host States and securing foreign investment in developing contexts rather than human rights, social and environmental liabilities. *See* ALSTON, *supra* note 29, at 7.

124. The OECD Guidelines for Multinational Enterprises sets non-binding recommendations for responsible business conduct to respect human rights of those affected by their activities. The guidelines were first adopted in 1976 and later revised in 2000 and in 2011. The guidelines require corporations to respect human rights, avoid causing or contributing to adverse human rights impacts, address and seek ways to prevent or mitigate these impacts, have a policy commitment to respect human rights carry out human rights due diligence and provide for remedy, responsible supply chain management. The International Labor Organization's Tripartite Declaration of Principles Concerning Multinational Enterprises and Social Policy is a non-binding instrument adopted in 1977 amended in 2000 and 2006. Principles on employment, training, conditions of work and life are amongst many that workers, employers and governments are recommended to observe on a voluntary basis. The declaration doesn't have a compliant mechanism. Global Compact is a voluntary initiative based on CEO commitments to implement universal sustainability principles and to take steps to support UN Sustainable Development Goals (SDGs). With the support of business and other stakeholders, the UN Global Compact's governance framework was adopted by then UN Secretary-General in 2005, following a year-long international process led by then Special Advisor to the Secretary-General. That process included studying governance models of other cutting-edge global action and solution networks and holding focus groups with participants and stakeholders, including governments, local networks, and academics. The resulting governance framework distributes governance functions among several entities to engage participants and stakeholders at the global and local levels in making decisions and giving advice on the matters of greatest importance

guidelines is voluntary and dependent on internal corporate policy and procedures. It's been said that the effects of these guidelines are "commercial rather than legal."[125]

One such effort is the UN Guiding Principles on Business and Human Rights, developed by the Special Representative of the Secretary-General.[126] The objective of these guiding principles is to enhance standards of business and human rights to achieve tangible results for affected individuals and communities and contribute to a socially sustainable corporate activity.

According to the UN Guiding Principles, business enterprises must identify, prevent, mitigate, and remedy any adverse human rights impacts they cause or to which they contribute.[127] They should carry out human rights due diligence based on a human rights policy approved at the most senior level of the business enterprise and stipulate the enterprise's human rights expectations of personnel, business partners, and other parties directly linked to its operations, products, or services.[128] Human rights due diligence goes beyond simply identifying and managing material risks to the company itself, to include risks to right holders. The process should include assessing actual and potential human rights impacts, integrating, and acting upon the findings, tracking responses, and communicating how impacts are addressed. This involves internal as well as independent external human rights expertise and a meaningful consultation with potentially affected groups and other relevant stakeholders.[129] Where a business enterprise may contribute to an adverse human rights impact, it should take the necessary steps to cease or prevent its contribution and mitigate any remaining impact to the greatest extent possible.[130] Corporate remedy may include apologies, restitution,

to their role and participation in the UN Global Compact, and to reflect the initiative's public-private and multi-stakeholder character. The principles of the UN Global Compact are derived from the Universal Declaration of Human Rights, the International Labor Organization's Declaration on Fundamental Principles and Rights at Work, the Rio Declaration on Environment and Development, and the United Nations Convention Against Corruption.

125. Eric De Brabandere, *Human Rights and Transnational Corporations: The Limits of Direct Corporate Responsibility*, 4 HUM. RTS. & INT'L LEGAL DISCOURSE 66, 82 (2010).

126. John Ruggie, *Report of the Special Representative of the Secretary-General on the Issue of Human Rights and Transnational Corporations and other Business Enterprises to the Human Rights Council, The Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect, and Remedy" Framework*, United Nation General Assembly A/HRC/17/31 (Mar. 21, 2011), endorsed by HRC Resolution A/HRC/RES/17/4 (June 16, 2011).

127. *Id.* at 15–16.

128. *Id.* at 16-18.

129. Formal reporting is evolving from traditional annual reports and corporate responsibility and sustainability reports, to include online and integrated financial and non-financial reports. Business enterprises whose operations pose risks of severe human rights impacts should report formally on how they address them. These reports should be accessible to its intended audience and external stakeholders, including investors.

130. Ruggie, *supra* note 126, at 24.

rehabilitation, financial or non-financial compensation and punitive sanctions such as fines, as well as the prevention of harm through, for example, injunctions or guarantees of non-repetition.[131] An effective grievance mechanism is based on engagement and dialogue and consulting the stakeholder groups. A grievance mechanism can only serve its purpose if the people it is intended to serve know about it, trust it, and are able to use it.[132]

Following the adoption of the above guiding principles, the UN Human Rights Council established an open-ended intergovernmental working group with the mandate "to elaborate an international legally binding instrument to regulate, the activities of business enterprises in international human rights law."[133] The Working Group set the goal to promote and implement the guiding principles and launched an annual forum on business and human rights to strengthen dialogue and cooperation. Later, the United Nations High Commissioner for Human Rights (UNHCHR) released an Issue Paper on "Legislative Proposals for Mandatory Human Rights Due Diligence by Companies" in which the OHCHR summarized the policy and legislative choices for lawmakers to adopt a human rights due diligence regulation for companies.[134] Mandatory human rights due diligence regimes are considered as part of a "smart mix" of measures to effectively foster business respect for human rights and encourage companies to embed proper human rights risk management processes across their operations.[135]

In the traditional corporate law realm, the concept of due diligence is fundamental to the legal, commercial, or reputational risks to the business enterprise.[136] Human rights due diligence, on the other hand, changes the focus to risks to people. They can vary in terms of the legal obligations imposed, the scope of the obligations, the way the obligations are monitored and enforced, the sectors covered, and the human rights themes and risks targeted.[137] The GDPR is an example of a mandatory human rights' due

131. *Id.* at 27.

132. *Id.* at 34.

133. Human Rights Council Res. 26/9, U.N. Doc. A/HRC/Res/26/9 (June 26, 2014).

134. UNITED NATIONS HUM. RTS. OFF. OF THE HIGH COMM'R, *supra* note 21.

135. *Id.*

136. *See* Human Rights Council U.N. Doc. A/HRC/38/20/Add.2, ¶ 8 (June 1, 2018).

137. An example of mandatory human rights due diligence legislation is the French Corporate Duty of Vigilance Law. *See* Loi No. 2017-399, *supra* note 21. The law requires the company to set out its approach to assessing and addressing human rights and environmental risks posed by its own activities, those companies which they control, and the activities of those suppliers or contractors with which they have an established commercial relationship. The company's vigilance plan is required by the law to cover risk assessment and screening, a risk mitigation strategy, an "alert system" and a risk monitoring scheme to verify the effectiveness of measures taken. The company must include implementation of a vigilance plan in its annual report. Interested persons who have been harmed by corporate failures can recourse to judicial authorities to compel compliance and request financial compensation.

diligence regime with a narrow scope that focuses on the right of individuals to protection of personal data.

Stakeholder groups and civil society organizations support a binding approach to human rights due diligence due to continuing failures by companies to identify, mitigate, and address human rights risks effectively. Mandatory due diligence as a legal standard of care may provide harmonization, a level playing field, and increasing leverage in business relationships.[138] At the same time, there is an ongoing debate concerning the unintended consequences of legal interventions and possible disadvantages of over-regulation. Restrictive legal regimes are known to discourage innovation and proactive behavior by companies and encourage narrow, "check box" human rights due diligence processes.[139] Holding a balance between legislative flexibility and restrictiveness can be difficult to strike in practice when reconciling competing considerations.[140]

To be effective and practically enforceable, mandatory human rights due diligence must be considered with the size of the business enterprise, the risk of severe human rights impacts, and the nature and context of its operations.[141] The regime could not possibly cover all human rights since it is complex, costly, resource intensive, and overwhelming for corporate duty bearers. Corporations need to prioritize those rights with a potentially severe adverse impact in the context of the relevant business operation where a delayed or no response could cause irreparable harm. Overambitious regimes will lack credibility to drive changes in business behavior.

The growing number of guidelines and soft law instruments is an indicator of an ever-expanding public awareness and formation of a strong public opinion around corporate human rights liability.[142] The power of public opinion, exposure to campaigns against brands, and demands for responsible business creates market incentives for a corporate human rights policy. Businesses respect human rights to ensure predictability and preserve reputation. These guidelines, however, do not provide a clear roadmap regarding what company directors and officers are permitted, let alone required, to do regarding human rights.

---

138. *Study on Due Diligence Requirements Through the Supply Chain: Final Report*, EUR. COMM'N, 17 (2020) op.europa.eu/en/publication-detail/-/publication/8ba0a8fd-4c83-11ea-b8b7-01aa75ed71a1/language-en [hereinafter BIICL Study].

139. UNITED NATIONS HUM. RTS. OFF. OF THE HIGH COMM'R, *supra* note 21.

140. Human Rights Council U.N. Doc., *supra* note 135, at para. 17.

141. Ruggie, *supra* note 126, at 17–19.

142. *See, e.g.,* Nevsun Resources Ltd v. Araya, (2020) S.C.R. 5 (Can.) (holding that in a claim for damages against a Canadian mining company by three Eritreans, a narrow majority in the Canadian Supreme Court held that it is not "plain and obvious that corporations today enjoy a blanket exclusion from direct liability for violations of obligatory, definable, and universal norms of international law.").

The overwhelmingly expanding literature and demand from the civil society organizations to hold corporations liable for violations of human rights has further contributed to the development of metrics for corporate human rights policy. What follows is a discussion on how the traditional CG theory and practice revolutionizes beyond mandatory laws and voluntary guidelines and converges with CSR to mitigate legal risks.

B. The Evolution of CG from a Shareholder to a Stakeholder Model

Corporations usually have some sort of self-imposed code of conduct known as corporate governance that improves economic performance of business.[143] CG is defined as a set of policies, processes, and mechanisms that influence the control, direction, and evaluation of corporations, a structure through which the objectives of the company are set, and the means of attaining those objectives and monitoring performance are determined.[144] CG is traditionally concerned with the relationship between the board, management, and shareholders, and the alignment of their interests.[145] Debates about managerial accountability, board structure, and shareholder rights are CG matters. CG encompasses a wide range of activities, rules, processes, and procedures to ensure optimal use of resources and corporate strategies so that corporate objectives are achieved.[146] In essence, CG relates to profit maximization and protection of those who have provided capital to the firm.[147] It further protects minority shareholders from the actions of majority

143. Mirela-Oana Pintea, *The Relationship Between Corporate Governance and Corporate Social Responsibility*, 1 REV. OF ECON. STUD. & RSCH. VIRGIL MADGEARU 91, 91 (2015).

144. ORG. FOR ECON. COOP. AND DEV., *G20/OECD PRINCIPLES OF CORPORATE GOVERNANCE* (2015), https://www.oecd-ilibrary.org/docserver/9789264236882-en.pdf?expires=1668980375&id=id&accname=guest&checksum=60C7283D9072E662314174CC79F4629E. CG is "the system by which companies are directed and controlled." ADRIAN CADBURY, REPORT OF THE COMMITTEE ON THE FINANCIAL ASPECTS OF CORPORATE GOVERNANCE (1992).

145. Gerry H. Grant, *The Evolution of Corporate Governance and its Impact on Modern Corporate America*, 41 MGMT. DECISION 923, 923 (2003).

146. Investors require assurance that their contribution to financial capital will generate a return. CG makes these investments possible. Thus, CG consists of the whole set of legal, cultural, and institutional arrangements that determine what corporations can do, who controls them, how that control is exercised and how the risks and returns from the activities they undertake are allocated. Examining CG is essential in understanding the structures of power and channels of financial flows.

147. Andrea Beltratti, *The Complementarity Between Corporate Governance and Corporate Social Responsibility*, 30 INT'L ASS'N FOR THE STUDY OF INS. ECON.: THE GENEVA PAPERS, 373, 374 (2005). "Corporate governance deals with the ways in which suppliers of finance to corporations assure themselves of getting a return on their investment. How do the suppliers of finance get managers to return some of the profits to them? How do they make sure that managers do not steal the capital they supply or invest it in bad projects? How do suppliers of finance control managers?". *See* Andrei Shleifer & Robert W. Vishny, *A Survey of Corporate Governance*, 52 J. FIN., 737, 737 (1997).

shareholders who exploit their control power.[148] So long as business activity is conducted through the corporate form, CG defines the interrelationship between executives, directors, shareholders, and stakeholders.[149]

CG has both internal and external tools. For example, concentration of control rights in the hands of shareholders who have the incentive to monitor the managers, efficient mechanisms for the formation of the board of directors, renumeration structures for managers which are anchored to performance, are internal mechanisms of CG. The external means of CG include control of outside stakeholders, especially banks and financial institutions, and the takeover threat from other firms, which may impose discipline on the managers whenever they do not maximize the value of the company. Firms with strong internal and external governance are known to produce a higher return to shareholders by stimulating the proper and efficient use of corporate resources.[150]

The principal-agent relationship between managers and owners was originally formulated as an efficient way to address abuse of power by managers. The use of corporate form to do business during the 19th century in America grew great capital with dispersed ownership among thousands of shareholders.[151] Firms needed to raise sufficient money to produce products and take advantage of economies of scale. The managers who ran these firms lacked the capital to do so. On the other hand, there existed people with money who could be owners but lacked either the expertise or the interest to run the firm. To solve this problem, the principals (i.e., the investors) would give their money to agents (the managers) to make profits and assure those principals of maximum returns on their investments. This, however, created the possibility of conflict between investors and managers and the problem of monitoring those agents.[152] Managers, who were not investors, pursued less risky investments to stabilize firms, preserve their jobs, and produce bonuses for themselves.[153] They seek profit sufficient to keep the security

148. Beltratti, *supra* note 147, at 374.

149. Brian R. Cheffins, *The History of Corporate Governance.* OXFORD HANDBOOK OF CORPORATE GOVERNANCE 1, 23 (European Corporate Governance Institute Law Working Paper No. 184/2012), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1975404.

150. Pintea, *supra* note 143, at 96.

151. Gerald F. Davis, *New Directions in Corporate Governance*, 31 ANN. REV. SOC. 143, 144 (2005).

152. Harwell Wells, *The Birth of Corporate Governance*, 33 SEATTLE U. L. REV., 1247, 1251 (2010).

153. ROBIN MARRIS, THE ECONOMIC THEORY OF 'MANAGERIAL' CAPITALISM (1968); *see also* EDITH PENROSE, THE THEORY OF THE GROWTH OF THE FIRM (1959).

holders satisfied and pursue prestige and power.[154] Shareholders were powerless over managers who ran the firms.[155]

CG seemed to resolve the agency problems associated with the separation between owners and managers.[156] Accordingly, boards of directors were formed with a fiduciary duty to shareholders to monitor the managers. Managers' compensation was tied to firm performance thereby aligning their interest with the interests of owners. Disclosure laws required timely filing of operational and performance results to current and prospective investors. Under agency theory, the primary goal of corporate governance is to protect shareholders from managerial discretion. Corporate governance mechanisms, external and internal, attempt to reduce agency costs and guarantee an efficient decision-making process that maximizes the corporate wealth. To survive, corporations must demonstrate they fit the financial market by showing that they are oriented towards the shareholder value.[157]

Accordingly, corporate law and financial regulations have evolved to enhance shareholder value. They make it possible for minority shareholders who have little access to the internal workings of the firm to gain knowledge of how firms are doing financially. In essence, these laws specify rules on disclosures and governance of corporations. In exchange for being able to raise capital publicly, managers must make information available to the public and be governed by a board of directors.[158] CG is thus a "nexus of institutions defined by company law, financial market regulations, and labor law."[159] Laws are created to meet the functional needs of owners who prefer not to directly administer firms, and maximize their returns by lowering agency costs and increasing corporate value with laws of competition.[160]

According to the agency theory of CG, raising large sums of capital by separating ownership from control and ensuring that managers use capital wisely and minimize agency costs will result in economic prosperity precisely because the shareholder wealth is secured.[161] Pursuing goals other than

154. ADOLF BERLE & GARDINER MEANS, THE MODERN CORPORATION AND PRIVATE PROPERTY 122 (1932).

155. Davis, *supra* note 151.

156. BERLE & MEANS, *supra* note 154.

157. To create shareholder value has become managerial orthodoxy. Davis, *supra* note 151, at 149.

158. HENRY HANSMANN, THE OWNERSHIP OF ENTERPRISE (1996).

159. John W. Cioffi, *Governing Globalization?: The State, Law, and Structural Change in Corporate Governance*, 27 J.L. & SOC., 572, 574 (2000).

160. For example, corporate law prescribes that firms can incorporate in any state whether they have operations or not creating competition among state legislatures over incorporation fees through the legal product they provide. *See* Davis, *supra* note 151, at 146.

161. Fligstein & Choo, *supra* note 21, at 66.

shareholder wealth maximization through CG and ignoring agency costs results in underperformance and less profitable investments for owners.[162]

The literature supports that systems of CG across societies vary because they reflect national, political, social, and cultural contexts and continuously shape the laws that define CG.[163] Not all systems define CG through agency theory. The expansive view that institutions like law, trust, politics, and culture affect market outcomes has led scholars to conclude that systems of CG are more political and historical than mere efficient and pragmatic solutions to the functional needs of the owners of capital who seek to maximize profits for themselves.[164] In addition, the fact that many societies have experienced comparable economic growth without converging on a single form of CG suggests that there are many forms of best practices that allow for economic growth.[165] Agency problems of owners and managers and the need for firms to obtain capital are solved differently in different societies.[166]

In the U.S., the CG model is based on scattered financing by shareholders in a corporate structure directed by management teams under strict monitoring of the board of directors, where workers have no representation on the boards.[167] In this system of CG monitoring transparency, information flow, oversight and accountability is provided by outside directors, private entities such as external auditors, securities analysts, accountants, and government agencies such as the SEC.[168] Incentive compensation for managers, takeovers, and proxy fights also provide competitive market mechanisms designed to align management interests more closely to those of the shareholders.[169]

In the German model, dominant across continental Europe and Japan, banks, insurance companies or other financial institutions form the large bulk of stock shareholders, where these shareholders have extensive authority to

162. Michael C. Jensen, *Eclipse of the Public Corporation*, HARV. BUS. REV. (1989), https://hbr.org/1989/09/eclipse-of-the-public-corporation.

163. Fligstein & Choo, *supra* note 21, at 64.

164. *Id.*

165. For example, the common law system of the U.S. has led to strong protection of minority shareholder rights. These in turn, have reduced agency costs of monitoring and influence of majority shareholders, and opened capital markets to firms. *See* Fligstein & Choo, *supra* note 21, at 15.

166. War, revolution, invasion, colonialization, class struggle, and politics have been at the heart of how societies have come to structure their economies and the organization of their corporate governance institutions. Ethnic and religious differences also appear to account for why some governments work better, have more legitimacy, and produce more effective systems of corporate governance. *See id.* at 20.

167. Fligstein & Choo, *supra* note 21, at 70.

168. *Id.*

169. *Id*. at 16 (stating the U.S. model of shareholder capitalism is applied in Great Britain, Canada, Australia, and New Zealand).

internally monitor the daily operation of the firm.[170] In this ownership structure, the information flow is controlled and opaque. [171] Non-shareholder stakeholders such as organized labor influence the governance of corporate firms through worker representation on boards of directors.[172] Norms of shareholder capitalism do not automatically prevail over the claims of other corporate stakeholders.[173]

Where managers and owners have more power, CG institutions favor shareholders over stakeholders. Where workers have more power, as they do in many of the European countries, CG institutions tend to favor stakeholders. Different legal and political systems regulate CG differently. This explains why Europe takes a position to pass GDPR while U.S. takes a '*watch and see*' position in regulating blockchain.

The corporations are products in the financial market just like the actual products they create. The founders have an incentive to make products that people want to buy, the same way they have incentives to create the kind of firm, governance, and securities the customers in capital market want. While key mandates of corporations are profit maximization, managing costs and risks and maintaining security and privacy, the change in the dominant paradigm, diverse demands of customers from the market and overwhelmingly growth of literature on impact of business beyond shareholders and on broader stakeholders have linked CG with CSR and ESG.

1. CSR Impact on CG

The idea of corporate self-regulation and *laissez-faire* doctrine dominantly governed corporate behavior for a long time.[174] Corporations were considered to have no established moral obligations beyond their duties to uphold the interests of their shareholders and a sole objective to increase profit.[175] The efforts corporations made to improve their public image in relation to human rights were a matter of self-interest that did not reflect the existence or acceptance of a legally enforceable obligation. In contrast, their voluntary commitment to codes of conduct were seen to reduce their competitiveness and cause them financial harm.[176]

Accelerated social and economic transformations subject corporations to the continued need to change their business model, the mode of thinking,

170. Fligstein & Choo, *supra* note 21, at 70.

171. *Id*.

172. *Id*.

173. *Id*. at 16–17.

174. *See generally* Friedman, *supra* note 27.

175. Friedman, *supra* note 27.

176. Richard Falk, *Human Rights*, 141 FOREIGN POL'Y, 18, 20–22 (2004); *see also* ALSTON, *supra* note 29, at 22–23.

attitudes, and patterns of interaction with stakeholders. Corporations are challenged to meet through performance the values, interests, and expectations of society. There is a growing expectation from corporations to operate as good corporate citizens. This is mainly due to the growing social awareness of the influence corporations have on the lives of individuals. A surge in social, environmental, and governance related scandals, financial crisis and unethical behavior of managers, and executives have increasingly channeled discussions towards the interplay between CG and CSR.[177] This development means a considerable broadening of the notion of CG beyond accountability to suppliers of finance to a wider stakeholder and strengthening the integration of CG with CSR.

Companies are constructs of the communities in which they operate, and they depend on them. They must take into consideration the effects of their activities in a wider context, taking account of all categories of stakeholders including their shareholders, investors, customers, employees, suppliers, and the communities within which they operate.[178] The social responsibility of business is no longer limited only to increase profit.[179] In this sense, corporate sustainability is understood as the ability of companies to positively influence environmental, social, and economic development through their governance practices and market presence. Good corporate governance mitigates risk, improves performance, opens the way to efficient financial markets, and establishes an attractive investment climate, showing transparency and social responsibility. As a result, good corporate governance builds market confidence, encourages long-term investment flows, and

177. *See* Rashid Zaman et al., *Corporate Governance Meets Corporate Social Responsibility: Mapping the Interface*, 61 BUS. & SOC'Y 690, 691(2022) (describing examples such as the Volkswagen emissions scandal, the Global Financial Crisis, or the Deepwater BP oil spill).

178. *See* R. EDWARD FREEMAN, STRATEGIC MANAGEMENT: A STAKEHOLDER APPROACH 46 (1984) (defining stakeholders as "any group or individual who can affect or is affected by the achievement of the organization's objectives."); *see* Thomas Donaldson & Lee E. Preston, *The Stakeholder Theory of the Corporation: Concepts, Evidence, and Implications*, 20 ACAD. MGMT. REV., 65-91, 68 (1995) (stating that advocates of the stakeholder perspective consider "all persons or groups participate in an enterprise with legitimate interests to obtain benefits and there is no *prima facie* priority of one set of interests and benefits over another."); *see* Charles W. L. Hill & Thomas M. Jones, *Stakeholder-Agency Theory*, 29 J. MGMT. STUD.,131-154, 134 (1992) (explaining that a company emerges as a nexus of implicit and explicit contracts between various actors with interests that are not always compatible).

179. *See* Friedman, *supra* note 27, at 4 (asserting that the dominant corporate drive since 1970 is summed in Milton Friedman's essay "*The Social Responsibility of Business is to Increase Its Profits*" where he once stated, "There is one and only one social responsibility of business–to use its resources and engage in activities designed to increase its profits so long as it remains within the rules of the game, which is to say, engages in open and free competition without deception or fraud.").

"[has] a strong impact on reputation and brands, an increasingly important part of company value."[180]

According to agency theory, well-designed CG systems align managers' incentives with those of shareholders and enhance corporate financial performance (CFP).[181] The alternative CG theory, however, requires managers to serve their stakeholders.[182] A firm has relationships with a broad variety of stakeholders, including governments, competitors, consumer, environmental advocates, the media, and others.[183] CG, thus, encompasses the rights and responsibilities among the parties with a "*stake*" in the firm[184] as well as processes that affect both financial and nonfinancial outcomes.[185]

The CSR is "a model of extended CG whereby who runs a firm (entrepreneurs, directors, managers) . . . have fiduciary duties towards the owners . . . and all the firm's stakeholders."[186] In a socially responsible firm managers balance a multiplicity of interests. They strive to make a profit, obey the law, be ethical, and be a good corporate citizen. They are required to consider, manage, and balance the economic, social, and environmental impact of their activities. CSR encompasses policies and processes including disclosures that firms put in place to improve the social state and well-being of their stakeholders whether undertaken voluntarily or mandated by law.[187] CSR, *prima facie*, is in contrast with profit maximization because it suggests a set of actions, which is beneficial to some external stakeholders and may

180. *Who Cares Wins: Connecting Financial Markets to a Changing World*, GLOB. COMPACT (2004), https://www.ifc.org/wps/wcm/connect/de954acc-504f-4140-91dc-d46cf063b1ec/WhoCaresWins_2004.pdf?MOD=AJPERES&CVID=jqeE.mD.

181. *See generally* Michael C. Jensen & William H. Meckling, *Theory of Firm: Managerial Behavior, Agency Costs, and Capital Structure*, 3 J. FIN. ECON. 305 (1976); Lucian Bebchuk, Alma Cohen & Aleen Ferrell, *What Matters in Corporate Governance*?, 22 REV. OF FIN. STUD. 783 (2009).

182. Joan E. Rodriguez Ricart, Miguel Angel Rodriguez, & Pablo Sanchez, *Sustainability in the Boardroom: An Empirical Investigation of Dow Jones Sustainability World Index Leaders*, 5 CORP. GOVERNANCE 24 (2005); Heiko Spitzeck, *The Development of Governance Structures for Corporate Responsibility*, 9 CORP. GOVERNANCE 495 (2009).

183. FREEMAN, *supra* note 178.

184. MASAHIKO AOKI, INFORMATION, CORPORATE GOVERNANCE AND INSTITUTIONAL DIVERSITY: COMPETITIVENESS IN JAPAN, THE USA, AND THE TRANSITIONAL ECONOMIES 11 (2000).

185. Zaman et al., *supra* note 177, at 692.

186. Lorenzo Sacconi, *Corporate Social Responsibility (CSR) as a Model of "Extended" Corporate Governance: An Explanation Based on the Economic Theories of Social Contract*, *Reputation and Reciprocal Conformism*, 143 LIUC PAPERS IN ETHICS, LAW, & ECON. 6 (2004); Hoje Jo & Maretno A. Harjoto, *The Causal Effect of Corporate Governance on Corporate Social Responsibility*, 106 J. BUS. ETHICS 53, 54 (2012) (CSR "generally refers to serving people, communities, and the environment in ways that go above and beyond what is legally required.").

187. Zaman et al., *supra* note 177, at 692.

conflict with the interest of the shareholders. It is, however, argued that CSR policies and practices can yield business-related benefits.[188]

CG and CSR both relate to corporate management practices and there are synergies between the two. They aim to reduce risks associated with the company's activity through compliance with regulatory requirements, disclosure of all material information including financial information, and respects for norms of business and social responsibility. Previous research tended to treat CG and CSR distinctly oblivious of CSR impact on corporate governance and performance. This has been specifically a dominant trend in the field of finance, which has traditionally focused on the relationships between suppliers of capital and managers. Even though there are not enough studies to provide any definitive conclusions regarding causality between CG and CSR, some preliminary evidence shows that companies have started to incorporate CSR into their governance structure.[189] There is an increasing trend of forming CSR committees within the boards of directors indicating to the CG-CSR-CFP nexus.[190] Findings based on analysis of CSR reporting show that most corporations have a separate CG section in their CSR report or directly link CG and CSR issues.[191]

CG either follows the shareholder model, which puts the shareholder and its interests on focus, or the stakeholder model, where the company considers the impact of their actions on all stakeholders' groups.[192] From the

188. *Id.* at 712.

189. Ricart, Rodriguez, & Sanchez, *supra* note 171, at 24–41. Governance & Accountability Institute reported in 2018 that 86% of S&P 500 firms released sustainability or corporate responsibility reports compared with just under 20% in 2011. *See Navigating the Way to Sustainability, Flash report: 86% of S&P 500 Index® Companies Publish Sustainability / Responsibility Reports in 2018*, GOVERNANCE & ACCOUNTABILITY INST. INC., https://www.ga-institute.com/storage/press-releases/article/flash-report-86-of-sp-500-indexR-companies-publish-sustainability-responsibility-reports-in-20.html (last visited July 27, 2022).

190. Spitzeck, *supra* note 182.

191. Ans Kolk & Jonatan Pinkse, *The Integration of Corporate Governance in Corporate Social Responsibility Disclosures*, 17 CORP. SOC. RESPONSIB. & ENVIRON. MGMT. 15, 15 (2010). A large majority of the Fortune Global 250 engage in non-financial reporting. The logic behind this is that, with increasing size and profitability, firms become more visible and consequently feel more pressure to disclose information that may be of relevance to stakeholders. For example, firms' integration of climate change into their governance practices and strategic planning depends on the investor-related interest in obtaining more information about firms' practices and the pressure a firm receives from the investment community. This issue has become prominent at shareholder meetings in the U.S. with the rise of institutional investors concerned about the business implications of climate change in recent years. *See* Douglas G. Cogan, *Corporate Governance and Climate Change: Making the Connection*, CERES (2006), http://ww.w.rrojasdatabank.info/ceres06.pdf.

192. Agency theorists argue that CG mechanisms–such as board monitoring, top management incentive schemes, and firm ownership structures–should encourage the adoption of CSR activities only when they result in efficiency benefits for the firm. *See* Abagail McWilliams & Donald S. Siegel, *Profit Maximizing Corporate Social Responsibility*, 26 ACAD. OF MGMT REV. 504 (2001); *see also* Abagail McWilliams, Donald S. Siegel, & Patrick M. Wright, *Corporate Social*

stakeholder perspective, the main reason for firms to deal with stakeholders is that neglecting them could mean a loss of control of the strategic direction and performance. In fact, CSR may be considered a profit maximizing strategy by troubling other competitors who are not efficient enough to comply. From the shareholder perspective, investing more into human capital may well decrease profits. Indeed, if these objectives were achievable in the normal search for profit maximization, firms would have already embraced them. Managers pursuing CSR at the expense of profit maximization would behave unethically from the point of view of not respecting the contracts which they have signed with the owners of the firm, unless the socially responsible behavior was dictated by the owners themselves. Under these circumstances, any socially responsible action would imply a profit-decreasing choice on the part of the managers. If we accept the view that CSR is in contrast with profit maximization, then, managers who have been hired to maximize the value of the firm would behave unethically by being socially responsible. They would increase the welfare of some groups of stakeholders at the expense of the welfare of shareholders.[193]

It is true that CSR has costs for the firm as well as for financial investors of the firm. It is, however, conceivable that by communicating their role of social responsibility, firms may be able to extract more revenues from the pool of socially alert consumers who are willing to pay more for services which are certified to be produced in the context of a process which looks at social responsibility and is itself socially responsible. CSR also manages risks as one of the CG goals by minimizing the cases of bad behavior and their potentially negative consequences on the value of the firm.[194] Another positive effect of CSR is associated with improvements in branding of the corporation in the relevant market by constructing a special relationship with the stakeholders, especially clients and suppliers.[195] While it may be difficult to place a value on the reputation of the firm in terms of CSR, indirect evidence such as the reaction of stock market and decrease in share value of the

Responsibility: Strategic Implications, 43 J. MGMT STUD. 1 (2006). The rise of stakeholder logic in liberal market economies signals that scholarship has embraced that CG is not only about shareholder value maximization but also about the relationships among multiple stakeholders such as investors, employees, and society, and the impact of corporate actions on the wider community and environment.

193. Managers may decide that the firms behave in a socially responsible way at the expense of profits. Beltratti, *supra* note 147, at 378.

194. For example, ExxonMobil's CSR is positively related to the value of the firm from the point of view of minimizing future possible liabilities (legal risks and litigations) associated with lack of social responsibility. *Id.* at 380.

195. According to a 2009 McKinsey Survey, two-thirds of CFOs and three-quarters of investment professionals embraced the notion that corporate social responsibility adds to shareholder value. They believed that the value added is tied to promoting a good corporate image. Hong & Liskovich, *supra* note 26, at 1.

firm following news about illegal actions is associated with the damage to reputation.[196] Furthermore, empirical studies show that both CG and CSR are positively related to the market value of the firm.[197]

Scholars define the interrelation between CG and CSR in three different modes:

1) CG is a function of CSR, along with human capital, stakeholder capital and the environment. In this strand CSR subsumes responsible governance.[198]
2) CSR is a function of CG where CG systems, structures, and processes impact firms' CSR policies and practices. In this strand, board characteristics such as board diversity, board expertise, and board independence are positively associated with CSR.[199]
3) CG and CSR are a part of a Continuum.[200]

The interplay between CG and CSR varies among different national business systems.[201] For example, in "liberal market economies national institutions encourage individualism, workers and other actors are less organized and firms coordinate their activities through the market mechanism and hierarchies."[202] In such systems CG norms are guided by agency theory and shareholder value maximization. Greater reliance on stock markets translates into short-termism, interfirm relations are more competitive and at

196. CSR is inversely related to overall risk, for example, the risk of being involved in legal disputes about pollution, health damage, and regulation. *See* Marc Orlitzky, Frank L. Schmidt & Sara L. Rynes, *Corporate Social and Financial Performance: A Meta-Analysis*, 24 BUS. & SOC'Y 403 (2003).

197. Orlitzky *et al*. study the relationship between CSR and the financial performance of the firm and find a positive relation. Margolis and Walsh compare the results of 95 studies that globally consider 70 financial indicators and 11 social indicators. In all, 55 out of 95 find a positive relation and only four studies find a negative relation. *See* Beltratti, *supra* note 147, at 380–81.

198. Zaman et al., *supra* note 177, at 691.

199. Pamela Kent & Reza Monem, *What Drives TBL Reporting: Good Governance or Threat to Legitimacy*?, 18 AUSTRALIAN ACCT. REV. 297 (2008). The spread of global production chains has, on one hand, exacerbated social and environmental issues and, on the other hand, has weakened the government's regulatory capacity. This has created a market "for external monitoring of CG and CSR by transnational entities such as international NGOs, and other international institutions (e.g., UN) as well as elicit responses from corporations in the form of transnational private regulatory coalitions such as multi-stakeholder initiatives (MSIs), business-led private governance initiatives (BLIs) to adopt voluntary codes of conduct for governance and sustainability. To date, we have little knowledge on firm strategies around private regulations and initiatives and their impact on performance." *See* Zaman et al., *supra* note 177, at 728.

200. Pintea, *supra* note 143, at 104.

201. Gregory Jackson & Androniki Apostolakou, *Corporate Social Responsibility in Western Europe: An Institutional Mirror or Substitute*?, 94 J. OF BUS. ETHICS, 371–94 (2010).

202. Representatives of this cluster are United States, the United Kingdom, Australia, Canada, Ireland, and New Zealand. Zaman et al., *supra* note 177, at 694.

arm's length.[203] On the other hand, coordinated market economies emphasize collectivism, with heavy reliance on nonmarket forms of coordination.[204] They demonstrate greater dependence on credit-based financial systems which translates into long termism. Interfirm relations in these systems are collaborative in nature and unionization is accepted. The state has a greater role in organizing economic activities. Greater focus is on value maximization for multiple stakeholders, influencing how firms perceive both CG and CSR norms and behaviors.[205] In highly coordinated economies, states play a dominant role in the coordination of economic activities and regulation of markets, and there exists a high level of paternalistic authority. There is a general prevalence of insider-dominated governance structures.[206] European peripheral economies[207] exhibit a strong presence of industrial and craft unions, banking-led financial systems, and hierarchical decision-making at firm and national levels. Despite European institutions' pressure such as the European Commission for CSR, the liberal market economy cluster including the U.S. has an explicit CSR practice compared to Europe.[208] The voluntary nature of CSR practices often acts as a substitute for institutional pressures, and firms operating in those countries tend to adopt and disclose more on CSR practices [209] whereas in countries with stronger institutional pressures a stakeholder model is adopted by way of mandatory legal norms and structures.[210] CG and CSR interrelationship depends on various complex factors that may emanate from inside and outside the boundaries of the firm such as *internal* CG mechanisms (board composition, ownership, and managerial incentives) and *external* CG (the nature of the legal system, the market for corporate control, external auditing, monitoring by institutional

203. *Id.* The interrelationship between CG and CSR first became a hot topic in the United States when the Exxon Valdez oil spill disaster occurred in 1980s. The incident became the symbol of managerial self-interest, driving attention toward transparency on environmental reporting. *See* M. G. Bowen & F. C. Power, *The Moral Manager: Communicative Ethics and the Exxon Valdez Disaster*, 3 BUS. ETHICS Q., 97–116 (1993); *see also* Zaman et al., *supra* note 177, at 701.

204. In this cluster we have Austria, Belgium, Denmark, Finland, the Netherlands, Norway, Sweden, and Switzerland. *Id.* at 694.

205. *Id.*

206. Japan is in this category. *Id.*

207. France, Greece, Italy, Portugal, Spain, Czech Republic, Hungary, Poland, Romania, and Slovakia France, Greece, Italy, Portugal, Spain, Czech Republic, Hungary, Poland, Romania, and Slovakia. *Id.*

208. Dirk Matten & Jeremy Moon, *Implicit and Explicit CSR: A Conceptual Framework for a Comparative Understanding of Corporate Social Responsibility*, 33 ACAD. MGMT REV. 404 (2008); *see Zaman*, *supra* note 177, at 694, 701.

209. T. Jain, R.V. Aguilera & D. Jamali, *Corporate Stakeholder Orientation in an Emerging Country Context: A longitudinal Cross Industry Analysis*, 143 J. BUS. ETHICS, 701–19 (2017).

210. Gregory Jackson & Androniki Apostolakou, *Corporate Social Responsibility in Western Europe: An Institutional Mirror or Substitute*?, 94 J. OF BUS. ETHICS 371 (2010).

investors and security analysts, rating organizations, stakeholder activism, and the media).[211]

CG can be integrated with CSR depending on the national business systems.[212] The integration of CG with CSR also relates to the sector in which a firm operates. In sectors with high social and environmental impacts, increasing numbers of firms have CSR reporting while in other sectors, particularly the financial sector, had been delayed.[213] In addition to sector, country of origin has also been important for the way debates on CG and CSR develop.

Disclosing information on CSR issues not only is material to those stakeholders traditionally interested in the social and environmental impact of a firm, such as NGOs, advocacy groups, and policymakers, it increasingly extends to shareholders and investors and therefore becomes a matter relevant to CG.[214] Some scholars suggest that overinvestment in CSR is a waste of valuable resources and a potentially value-destroying proposition.[215] The growing importance of stakeholder theory has developed studies on the causal impact of CG on CSR as well as the causal impact of CSR on CG, and the effect of CSR on CFP.[216] The stakeholder theory advocates firms use CSR as an extension of effective CG mechanisms to resolve conflicts between managers and non-investing stakeholders that consequently enhance

211. Ruth V. Aguilera et al., *Connecting the Dots: Bringing External Corporate Governance into the Corporate Governance Puzzle*, 9 ACAD. OF MGMT. ANNALS 483, 484 (2015).

212. For instance, firms operating in CMEs, highly coordinated, and European peripheral economies focus on both internal and external CSR mechanisms (*i.e*., employee centric CSR and environmental CSR. In contrast, firms operating in LMEs, notably the United States, Australia, and New Zealand are more likely to single out external CSR as opposed to internal CSR. *See id.*

213. The recent history of the financial sector is a prime example of the importance of CSR and of the negative externalities, inflicted to the economy by failures in socially responsible behavior. Helping corporations to create offshore companies with the aim of hiding losses, arranging special trading operations between mutual funds and hedge funds to increase assets under management, selecting specific wealthy clients for the allocation of hot initial public offerings are examples of CSR failures. The financial sector has claimed no wrongdoing in most of these cases, however financial intermediaries failed to behave in a socially responsible way, neglecting the consequences for specific groups. The fact that most financial intermediaries decided to pay financial penalties to settle the accusations is probably the best example of what was stated in the introduction that societies are not willing to passively accept all the actions coming from the corporate sector. Society has an increasing number of tools to control the decisions of the corporate world.

214. CSR gives a competitive edge to firms in the market given the value relevance of social and environmental information. This inherently creates incentives for shareholders to be concerned with how the firm they are financially contributing to performs on CSR metrics.

215. These scholars argue that effective CG prevents overinvestment. *See* Amir Barnea & Amir Rubin, *Corporate Social Responsibility as a Conflict between Shareholders* 97 J. BUS. ETHICS 71 (2010).

216. *See generally* Maretno & Harjoto, *supra* note 186.

CFP.[217] Measurable markets in which firms operate are product market, capital market, and market for social responsibility, as urged by shareholders, government, NGOs, and social activists.[218] In consumer industries, it is likely that financial performance and social performance link and companies get a financial edge by behaving socially responsibly.[219] While managers conduct CSR to fulfill their moral, ethical, and social duties for their stakeholders, they are strategically achieving corporate goals for their shareholders. CSR increases the firm's reputation and strengthens relationships with core stakeholders.

2. Environmental, Social, and Governance (ESG) Impact on CG

ESG are a set of environmental, social and governance standards for company operations that impact a company's ability to create long-term values including safety issues and data security, board diversity and visibility, executive pay, and tax transparency.[220] The ESG social criteria examines how a company manages relationships with employees, suppliers, customers, and the communities where it operates. It covers equal opportunity policy, human rights policy such as whether the company has implemented any initiatives to ensure the protection of the rights of all people it works with, training policy, employee CSR training, health and safety policy, and fair remuneration policy. Corporate ESG strategies also relates to internal governance and how leadership qualities affect management choices.[221] Governance deals with a company's leadership, executive pay, audits, internal controls, and shareholder rights. ESG governance criteria consist of both stakeholder and shareholder management strategies and covers criteria such as independent directors, CEO duality, audit committee, board diversity, data security expert on board composition, executive compensation linked to ESG goals, business ethics, and guidelines for executives conduct.[222]

217. FREEMAN, *supra* note 178, at 234. Conventional corporate performance metrics are profit, growth, stability.

218. David P. Baron, Maretno Agus Harjoto, & Hoje Jo, *The Economics and Politics of Corporate Social Performance*, 13 BUS. & POL. 1 (2011).

219. *Id.*

220. ESG: How can you Unlock Value?, PwC, https://www.pwc.com/us/en/services/esg/esg-journey.html (last visited July 27, 2022).

221. Institutional owners have a direct channel to communicate their sustainability preferences to the management and the board. The board has a strong impact on shaping firm's CSR and sustainability performance specifically in firms with less concentrated institutional ownership. *See* PETER ILIEV & LUKAS ROTH, DO DIRECTORS DRIVE CORPORATE SUSTAINABILITY*?*, 1, 26 (2020), https://portal.northernfinanceassociation.org/viewp.php?n=2240017388.

222. ESG is predominantly engaged in environmental risks. A quick look at the World Bank Operational Policy 4.03 Performance Standards for Private Sector Activities shows that out of 8 standards 3 hardly touch on social risks *See Operational Policy 4.03, Performance Standards for*

In the business world, the awareness of ESG-related risks that were once considered as uncommon issues is becoming stronger than ever.[223] As global interest in ethical investment grows, ESG factors have increasing financial relevance. Investors have, in recent years, shown interest in putting their money where their values are. Socially responsible investors are increasingly applying non-financial factors and a broad range of behaviors and policies as part of their analysis process to identify material risks and growth opportunities. They seek to ensure the companies they fund are socially responsible, good corporate citizens and are led by accountable managers. Although institutional investors have a duty to maximize shareholder value, there is growing awareness that ESG ratings are an indicator of a company's long-term performance, including return and risk, as well as its ethical standing.[224]As a result, companies are increasingly offering financial products with ESG criteria.[225] ESG plays a crucial role as a proxy for sustainability performance and an enabler of the socially responsible investment market.[226] In addition to their social value, ESG criteria can help investors avoid crisis resulting from companies' risky or unethical operations.[227]

Private Sector Activities, WORLD BANK (May 2013), http://web.worldbank.org/archive/website01541/WEB/0__C-116.HTM. Within the context of the blockchain and new disruptive technologies more attention needs to be paid to social risks.

223. Guidance on ESG- related risks published by the Committee of Sponsoring Organizations of the Treadway Commission and the World Business Council for Sustainable Development (COSO-WBCSD, 2018). Investor interest in ESG/CSR is highlighted by the fact that in 2019 alone, 300 mutual funds with ESG mandates received a total of $20 billion in net flows, which was 4 times the 2018 total. *See* Greg Iacurci, *Money Moving into Environmental Funds Shatters Previous Record*, CNBC (June 14, 2020), https://www.cnbc.com/2020/01/14/esg-funds-see-record-inflows-in-2019.html.

224. *What is ESG*?, CGLYTICS, https://cglytics.com/what-is-esg/ (last visited July 27, 2022). Socially responsible investors have specific characteristics in terms of gender, education, and income. Studies regarding motivation suggest that both financial and nonfinancial motivations influence the investment decision based on an investor's tolerance toward the risk of lower financial returns. Corporate tendency to focus on financial concepts, particularly the financial performance of investment portfolios is a potential distraction. Investors, however, have raised concerns regarding the lack of a clear definition of when investments can be classified as socially responsible, the absence of standards for socially responsible investments, and the quality of available data on ESG ratings of companies. *See* Emma Avetisyan & Kai Hockerts, *The Consolidation of the ESG Rating Industry as an Enactment of Institutional Retrogression*, 26 BUS. STRAT. & ENV'T 316 (2017); *see also* Gunnar Friede, *Why Don't We See More Action? A Meta-Synthesis of the Investor Impediments to Integrate Environmental, Social, and Governance Factors*, 28 BUS. STRAT. & ENV'T 1260 (2019).

225. Financial services companies such as JPMorgan Chase, Wells Fargo, and Goldman Sachs have published annual reports that extensively review their ESG approaches and results.

226. Luluk Widyawati, *A Systematic Literature Review of Socially Responsible Investment and Environmental Social Governance Metrics*, 29 BUS. STRAT. & ENV'T. 619, 619 (2019).

227. BP's 2010 Gulf of Mexico oil spill and Volkswagen's emissions scandal negatively impacted companies' stock prices and cost them billions of dollars.

Boards of directors are the highest-level decision-making authority in a firm, the most visible and accountable senior leaders, and exercise considerable power over a firm's strategic direction, actions, and resource allocations. Boards of directors are unlikely to demonstrate the same decision-making patterns and therefore their attention to CSR/ESG is likely to differ from board to board. Surveys have found in the past that issues related to sustainability are consistently ranked at the bottom of board priorities.[228] Board composition plays an important role in understanding and adequately addressing the issues of CSR/ESG given that ignorance exposes the corporate enterprise to litigation and legal risks. Diversity on the board may help to improve boardroom dynamics and interaction in a unique way.

There is empirical evidence that shows voluntary CSR/ESG strategies together with an independent and diversified board composition enhance corporate efficiency, sustainability and financial performance including return on assets, and market value.[229] Companies that adopt a policy to implement CSR/ESG metrics enhance their corporate reputation and market value.[230] According to these studies, the market values a policy that focuses on creating an ideal corporate culture even if it generates little connection with efficiency and profitability.[231] The relationship between corporate

228. *See* Paine, *supra* note 28.

229. For social activities, firms that try to reduce demographic discrimination and offer training programs tend to outperform their peers. In terms of governance activities, independent directors play an important role in reducing agency costs and maximizing shareholder value, which lead to better financial performance. Including women on the board also has a strong positive relationship with financial performance. Researchers have also noted how gender impacts the way boardrooms operate. Diversity in workgroups is also known to influence constructive debate over differing viewpoints. *See* Jun Xie et al., *Do Environmental, Social, and Governance Activities Improve Corporate Financial Performance*?, 28 BUS. STRAT. & ENV'T. 286, 297–98 (2018).

230. According to a study by Friede et al., there have been more than 2000 published empirical academic studies in fields such as management, accounting, finance, and economics attempted to answer whether and how ESG/CSR relates to firm performance and value. The authors conduct a meta-analysis of this literature and conclude: "Roughly 90% of studies find a nonnegative ESG/CFP relation. More importantly, the large majority of studies reports positive findings." *See* Gunnar Friede et al., *ESG and Financial Performance: Aggregated Evidence from More than 2000 Empirical Studies*, 5 J. SUSTAIN. FIN. INV. 210 (2015). ESG/CSR activities could create value because they increase shareholder wealth by increasing cash flows. Customers want to buy from firms that have good reputations in corporate responsibility, employees are more productive when they work for such firms. ESG/CSR activities could create firm value through the channel of maximizing shareholder utility. For example, shareholders could value the environmental or social goods produced by high ESG/CSR profile firms in addition to the cash flows they produce. Under this alternative, shareholders receive more utility by owning responsible firms, even if the cash flows are the same as those of irresponsible firms. High valuations and better financial performance lead to higher ESG/CSR performance. *See* Gillan, Koch, & Starks, *supra* note 26, at 16.

231. *See* Xie et al., *supra* note 229, at 296.

efficiency and ESG disclosures is non-linear and broadly depends on CSR/ESG criteria that are realistic, measurable, and actionable.[232]

ESG and CSR can affect many types of risk, including systematic risk, regulatory risk, supply chain risk, product and technology risk, litigation risk, reputational risk, and physical risk.[233] Evidence shows that firms with higher CSR/ESG ratings receive more favorable settlements from prosecutors and have higher market valuations.[234] Strategic CSR/ESG creates value by improving corporate image.

IV. How Blockchain Impact CG: Mapping the Future

Digital technologies profoundly disrupt how companies are organized and governed. The decentralized autonomous organizations (DAOs) are based on a peer-to-peer, community-driven forms of corporate organization and governance.[235] In this model decisions are reached by a community of users in the absence of a centrally designated authority that makes and enforces those decisions. The DAO automates the governance using computer codes to manage various aspect of firm.[236] This *flat governance* structure is built with smart contracts that run on the blockchain platform.[237] DAO gives investors direct real-time control over decisions about how contributed funds would be distributed to projects.[238]

232. ESG metrics remain flawed and not well mapped due to a lack of transparency, consistency, and convergence.

See Widyawati, *supra* note 226, at 631–33.

233. For example, firms with high ESG/CSR strategies have a wider investor base and face lower litigation risk, ultimately leading to a lower cost of capital. For studies on CSR/ESG impact on risks *see* Gillan, Koch, & Starks, *supra* note 26, at 12.

234. Hong & Liskovich, *supra* note 26.

235. Essentially, a DAO is an organization controlled by token holders that operate on a blockchain through smart contracts. These token holders will replace board members and top management in making decisions for the organization. A DAO is an amalgamation of blockchains, smart contracts and stakeholders all working together interactively. The basic rules of governance are programmed into the blockchain at setup. All stakeholders involved with the DAO will possess tokens that represent a share in the DAO's performance similar to a share of an organization/firm. *See* Dulani Jayasuriya Daluwathumullagamage & Alexandra Sims, *Blockchain-Enabled Corporate Governance and Regulation*, 8 IN'L J. FIN. STUD. 1, 10 (2020).

236. Fenwick & Vermeulen, *supra* note 4, at 17.

237. A smart contract refers to a computer program code or protocol that automates the verification, execution and enforcement of certain terms and conditions of a "contractual" arrangement.

238. It must be noted that DAOs are not flawless. The crowdfunding campaigns of Initial Coin Offerings (ICO) revealed that flaws in the DAO code provides hackers with an opportunity to transfer funds to subsidiary accounts. Therefore, regulatory frameworks such as GDPR emphasizes human intervention and holds accountable data controllers and processors on blockchain to protect ultimate investors on such platforms. Technology failures are evidence that corporate governance issues cannot completely resolve through digital technologies.

Companies that operate as platforms leverage DLTs to facilitate economic exchange, transfer information and connect people. These new models of organization are inclusive and communal enabling multiple stakeholders to collaborate, and use their feedback to continuously improve their experience, engagement, and accountability in a company. The technology provides a suitable environment for implementation of an effective CG converged with CSR/ESG metrics.

Recent technological changes are disrupting the "old corporate world" of centralized authorities and hierarchies. The emerging new world is characterized by the *decentralization and disintermediation* of business organizations.[239] Blockchain facilitate community-driven dispersed forms of CG in which authoritative decisions are reached by a community of users in the absence of a centrally designated authority that makes and enforces those decisions.[240] Blockchains could dramatically affect the balance of power between directors, managers, and shareholders.[241] Centralized organizations generate trust through formal and informal hierarchies, procedures, and processes.[242] DAOs enabled with blockchain technology introduce a "flat-hierarchy" that aims to tackle shortcomings of centralized, heavily bureaucratic, and hierarchical organizations.[243] DAOs distribute organizational governance, authority, and decision-making among a holacracy of networked members rather than being vested in a management hierarchy.[244] The peer-to-peer connections, communications, interactions, and transactions automate trust and impact the meaning of leadership and management operation of the firms.[245]

CG could change in many ways under a blockchain regime. Blockchain crowdsources the function of auditing and verification by distributing each block of transactions to every member of the network. Thus, all company shareholders and other interested parties would be able to view the ownership of assets in real time and identify changes instantly as they occur.[246]

239. Fenwick & Vermeulen, *supra* note 4, at 5.

240. *Id.*

241. Yermack, *supra* note 34, at 3.

242. Fenwick & Vermeulen, *supra* note 4, at 8.

243. "Old world" organizations make decision-making slow, cumbersome, and costly. Decentralized alternatives offer a degree of independence that resonates with more and more people. *See id.* at 8-10.

244. *Id*. at 9.

245. In the new digital world, trust is placed in machines and algorithms empowered through smart contracts instead of institutional intermediaries. *Id.* at 11-12.

246. Those able to view the distributed ledger of share ownership would be able to identify the holders of individual shares and the counterparties of important transactions. For instance, if a manager sold shares of his own stock, will not only observe the sale but will also discern the selling manager's identity. Yermack, *supra* note 34, at 17–18.

Better transparency would significantly impact the profit opportunities, acquisition, and liquidation of ownership available to managers, institutional investors, and shareholders, among others. Investors would have more reliable information regarding the value of the companies.

Cheaper and faster trade execution and settlement on blockchain increases liquidity and facilitate easy entry and exit by shareholders.[247] Managers' trades would be transparent in real time deterring insider trading by the executives as a *de facto* compensation system.[248] Share transfers cannot be backdated or otherwise changed retroactively on blockchains as add-only databases in which entries are time-stamped and impossible to be rewritten.[249] Blockchain evolves corporate proxy voting system by allowing direct shareholder votes to be quickly and securely recorded and significantly diminishing inaccuracy in the outcome of corporate elections.[250] Company's accounting data, financial reporting, and the entire ledger are visible immediately to any shareholder, customer, lender, trade creditor, or other interested party. This increases trust in the integrity of the company's data, reduces opportunities for manipulating reported earnings, fraudulent conveyances and suspicious asset transfers, and conflicts of interests.[251]

The lower cost, greater liquidity, more accurate record-keeping, and transparency of ownership offered by blockchains significantly change the balance of power among managers, institutional investors, smaller shareholders, auditors, and other stakeholders involved in corporate governance.[252] Increased visibility and traceability increases accountability and

247. Sale of stock on the blockchain could be settled much more quickly and it would not require intermediaries. Indirect savings would emerge from the reduced need for firms to tie up assets in collateral as a form of bonding during the settlement process. *See id.* at 19.

248. *See id.* at 20.

249. Yermack, *supra* note 34, at 21.

250. For example, instead of designing a regulatory system to attempt to prevent empty voting, empty voting shares can be programmed on blockchain so that following the sale of a share, it is stripped of voting rights for a set period and no individual would be able to borrow a share and vote using that share. NASDAQ Talinn (Estonia) Stock Exchange announced a pilot program for blockchain voting in shareholder meetings for companies listed on the exchange in February 2016. *See id.* at 23.

251. Yermack, *supra* note 34, at 25–26.

252. Yermack, *supra* note 34, at 7. Delaware amended its corporation law in 2017, allowing companies to use blockchain technology to maintain their stock ledgers and other corporate records. In July 2018, the fourth largest stock exchange, the *Shanghai Stock Exchange* (*SSE*), released plans to introduce distributed ledger technologies, including blockchain, in securities transactions. *Nasdaq* successfully tested blockchain technology in a proxy voting experiment on its exchange in Estonia. The *Australian Stock Exchange* has started to develop distributed ledger technology solutions for clearing and settlement activities. The *Japan Exchange Group* collaborates with *IBM* in investigating blockchain solutions in low-liquidity assets. *See* Fenwick & Vermeulen, *supra* note 4, at 14; *see also* Yermack, *supra* note 34, at 28.

enables corporate board's efficient oversight and decision-making.[253] Beyond the corporate structure, blockchain can facilitate a form of novel organization without senior management or an organizational hierarchy. Smart contracts might end the need for bankers as directors to signal financial markets' creditworthiness in the composition of the board.[254] Automated processes might better select board members, be accurate in predicting future performance of directors and reducing the agency costs. With blockchain-enabled CG the "need for intermediaries such as brokers, banks and lawyers would be significantly reduced."[255] Traditional roles such as investors, executives, managers, and consumers will become blurred, and information asymmetries will become much less significant. Traditional models of CG will be less relevant considering uncertainties about risks, benefits, future directions, and social and ethical concerns. Given that for the foreseeable future, blockchain investments are expected to increase globally, this new environment for trade and transaction requires new CG design that is dynamic, responsive, experimental, and flexible in addressing potential harm to people.

V. Conclusion

Digital personal data is a "new asset class," a valuable resource, and currency of the digital world.[256] DLTs collect and process considerable amounts of personal data. In the fast-approaching era of quantum computers current encryption will not provide ultimate data security. Cryptographic protocols of today are vulnerable to quantum computing of the future that enables code cracking. Technology is doing its part to increase digital security by introducing post-quantum cryptography (PQC) protocols with outpacing capabilities of quantum machines and quantum-enabled hackers.[257] Mandatory regulations such as the GDPR contribute equally to protection against data breach and harm to individuals on digital platforms such as blockchain. In such an uncertain environment, governance structures of decentralized platform organizations need to be proactive in responding to potential threats to society.

New technologies are correcting the errors of our old-world centralized organizations with hierarchies and intermediaries. Blockchain allegedly

253. Daluwathumullagamage & Sims, *supra* note 235, at 17.

254. *Id.* at 10.

255. *Id.* at 14.

256. *Personal Data: The Emergence of a New Asset Class*, WORLD ECON. F. 5 (2011), https://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf.

257. *See* THE ECONOMIST, *supra* note 62; *see also How to Preserve Secrets in a Quantum Age*, THE ECONOMIST (July 13, 2022), https://www.economist.com/science-and-technology/2022/07/13/how-to-preserve-secrets-in-a-quantum-age.

corrects the errors of record keeping and creates resilience through replication by distributing data to a countless number of participants in public peer-to-peer networks (like the internet) or private and permissioned peer-to-peer networks (like an intranet).[258] Yet, in contrast to the old technology developments that were sequential, current technologies "amplify" each other and create synergies that greatly increase their social impact and effects.[259] Visionary managers and overambitious directors of digital firms see their business solutions as a mission to change the world, enhance democracy, freedom, and shared prosperity.[260] The private executives feel empowered to make global decisions as arbiters of right and wrong.[261] In the meantime, trusting business to do good all by itself free from liability and a monitoring, evaluation, and enforcement mechanism would be too unrealistic.[262]

Some commentators argue that CG will not be disrupted by new technologies and contend that existing legal and corporate structures sufficiently address the effects of new technologies on business models and organizations.[263] On the other hand, policy makers, regulators, and activists are concerned with the security of the new technologies, and their impact on different stakeholders. Legal intervention and possible over-regulation might have

258. Fenwick & Vermeulen, *supra* note 4, at 13.

259. *Id*. at 4–5. For example, *Amazon* offers an online retail platform through algorithm-driven recommendations and online customer ratings and reviews, creating a new type of consumer experience that is highly personalized *and* communal. *See id.* at 16. Another example is Blockchain that converge with Artificial Intelligence (AI) for automatization of business processes. For example, smart contracts embedded with AI models can execute transactions on blockchain, process payments, or stock purchases and resolve disputes. In the health sector, the convergence of blockchain and AI enables data integrity, transparency, patient tracking and consent management. In supply chains and financial services, it facilitates tracking data, accelerating transactions, increasing visibility for intellectual properties, and enhancing security and privacy of data. *See* IBM, *supra* note 4.

260. *Elon Musk is Taking Twitter's "Public Square" Private*, THE ECONOMIST (Apr. 30, 2022), https://www.economist.com/business/2022/04/30/elon-musk-is-taking-twitters-public-square-private.

261. The corporate executives of big tech companies are assuming roles to safeguard the future of civilization and trying to answer problems with automation. One of the examples of these Inflated ideas is Elon Musk when struck a deal to buy Twitter on April 25, 2022, promised to make online speech freer and to publish in the name of transparency Twitter's code including its recommendation algorithm, describing Twitter as "*de facto* public town square." On the other end, governments are tightening laws and passing regulations to protect individuals from potential risks. The European Union Digital Services Act requires services to strengthen and systematize content moderation. The GDPR is focused on data protection and privacy and algorithmic biases that discriminate.

262. While business ethics shape part of the reason why corporations withdrew from Russia in the recent war in Ukraine, a pragmatic motive was determinative, the very fact that the Russian market was not a major source of revenue for most firms. *Is Cancel Culture Coming to Free Trade?*, THE ECONOMIST (Apr. 2, 2022), https://www.economist.com/business/2022/04/02/is-cancel-culture-coming-to-free-trade.

263. Fenwick & Vermeulen, *supra* note 4, at 4.

a restrictive impact on innovation and proactive behavior of tech companies and those who utilize technology to provide products and services in a more efficient way and with lesser costs. There is, therefore, a continuous debate on how to strike a balance between legislative flexibility and restrictiveness regarding new technologies.[264]

The GDPR already puts in force a comprehensive data protection and privacy regulatory framework that impacts U.S. headquartered firms particularly in technology sector.[265] An analysis of the GDPR trends indicates that DPAs appear to be placing a greater emphasis on necessary measures controllers and processors must take to demonstrate that they have taken adequate precautions to protect personal data. This includes best practices such as pseudonymization and encryption of data, ensuring confidentiality and integrity of systems, restoring access to personal data following a data breach, and regular testing to ensure effectiveness. The GDPR obligations impact CG in a mandatory fashion. Legal and litigation risks increasingly draw the attention of the directors and executives to the need for data experts in the composition of boards. GDPR mandatory landscape has become a force for change from shareholder model of CG based on principal-agent dynamics to

264. The UN guiding principles on business and human rights and subsequently the issues paper on legislative proposals for mandatory human rights due diligence, while attempting to encourage companies to embed proper human rights risk management processes across their operations, might be considered as too burdensome for companies and unrealistic to enforced. *See* Ruggie, *supra* note 126, at 16–18. The Special Representative annexed the Guiding Principles to his final report to the Human Rights Council (A/HRC/17/31). The Human Rights Council endorsed the Guiding Principles in its resolution 17/4 of 16 June 2011. *See* UNITED NATIONS HUM. RTS. OFF. OF THE HIGH COMM'R , *supra* note 21.

265. The GDPR enforcers tend to issue fines against e-commerce/retail firms, digital service providers and technology firms mainly based in the United States with global platforms, and telecommunication firms. Firms that have faced a substantial level of regulatory scrutiny have typically been industries that heavily rely on customer data for operational purposes. These include the medical services sector, the energy services sector, and the banking sector. The GDPR authors released a short interim publication on GDPR fines analyzing enforcement trends after the GDPR had been implemented for one year, and subsequently released a second more lengthy report in June 2020 exploring GDPR fines issued between May 2018 and March 2020. Both publications showed that Western European countries such as the UK (before Brexit), France, and Germany appeared to be aggressive in imposing larger fines and initiating investigations, often against U.S. tech companies. GDPR enforcement trends against U.S.- headquartered firms, which represents more than 80 percent of the monetary value of all fines issued by DPAs during the subject period. Fines issued against the e-commerce/retail sector such as Amazon, H&M, Carrefour constitute more than 60 percent of the value of all fines issued by European DPAs. Examples of internet service providers being investigated or fined by DPAs are WhatsApp, Google, Meta, Twitter, TikTok. Amazon disclosed in a filing to the U.S. Securities and Exchange Commission (SEC) that it had received a fine of €746 million from the Luxembourg National Data Protection Commission in July 2021. Luxembourg's Amazon fine is the largest GDPR-related fine on record to date and represents nearly 60 percent of the total value of all fines issued by all EU DPAs during the entire May 2018–December 2021 period. *See* Daigle & Khan, *supra* note 8.

a poly-centric stakeholder model of CG with an emphasis on financial as well as non-financial performance of the firms.

Apart from the mandatory law, the CSR/ESG discourse and its interrelationship with CG has an increasingly impact on the corporate performance and pressures corporate enterprises to adopt a stakeholder policy within the structure of their CG. Given the growing market for socially responsible investment (SRI) that requires reporting on human rights policy of the firms, CSR/ESG associates positively with the market value and reputation of the firms and therefore, considered to impact the CFP.[266] Accordingly, CG is impacted by the voluntary CSR/ESG metrics that requires simultaneous measurement of economic viability, environmental integrity, and social responsiveness. Data protection and privacy in the context of firms that are heavily reliant on data collection and processing for their business activity is part of the human rights policy of the firm and requires attention of the board and executives in defining internal processes to protect private information. CG and CSR are complementary in shaping the objectives and the constraints faced by corporations. They can reinforce each other in the modern vision of the firm as an institution which does not disregard various relevant constituencies in its search for increases in value. CSR/ESG is a new tool to induce corporations to move beyond traditional CG mechanisms and towards an extended performance metrics. An effective CG would prevent illegal actions against stakeholders as well as legal but inappropriate actions that have negative consequences for the firm's value.[267]

Besides the old-world corporate structures that might use blockchain to run their business activities, the rise of DAOs empowered with blockchain data processing technology equally impacts CG. We live in a world that has long been dominated by centralized organizations characterized by formal and informal hierarchies. Companies are a typical example, with traditional hierarchies between shareholders, directors, managers, and employees. Today, however, digital technologies are disrupting this model of organizational design from hierarchies to platforms. Blockchain is digitalizing CG where a peer-to-peer, community-driven organization makes and enforces decisions in the absence of a centrally designated authority. The DAO's *flatter governance* structure automates management of various aspects of the firm. Blockchain is dramatically changing the balance of power between directors, managers, and shareholders and impact the meaning of leadership

266. This contrasts with the traditional CG theory that was of the view that CSR is nothing more than cynical corporate strategy with little economic implications and it comprises nothing more than some year-end reports about various initiatives that are not very costly.

267. There is a growing market for firms to screen out irresponsible companies from their indexes. These scores are correlated with the values of investors and CEOs. In sum, the preponderance of the evidence establishes the scoring system as an informative measure of a firm's genuine attempts to address the impact of their production on society.

and management operation of the firms. Greater transparency offered by blockchain would be an ultimate benefit that provides for an effective public control over corporations and efficiency of markets. Blockchain removes the traditional '*executive privilege*' over confidential and secret corporate information[268] as all corporate activities are visible in real-time on such platforms.

Yet, the decentralized finance (DeFi) removes the protection regime and screening process offered by the intermediaries in traditional finance. Accordingly, an average investor is more at risk of losing assets since it has less access to expert consultations and analysis of information to make informed decisions on investments. Transparency is not, after all, just about provision of data and information. The mere fact that the data is publicly available does not wipe out the liability of those who inflict damages on the members of the network. The Securities and Exchange Commission (SEC) has investigated the largest cryptocurrency exchange, Coinbase, over the launch of its digital asset lending product called Lend. Lend would have allowed customers to earn up to 4% annual profit by lending their Stablecoin, USDCoin, to other users. The SEC considered Lend to involve a security and due to lack of sufficient investor protection in crypto finance, requested Coinbase to stop launching the product. Cryptocurrencies and decentralized finance may evolve to threaten the financial system and create a financial crisis.[269] While transparency is primarily related to access to information, the essential goal it secures is to enable public scrutiny, provide the aggrieved with access to justice, and ensure accountability of those liable for violations of laws. This explains the underlying provisions of the Securities and Exchange Act and further SEC regulations on disclosure and compliance requirements including registration and reporting of beneficial owners of certain classes of securities.[270]

Blockchains have the potential to transform the future of the corporations to a digitized decentralized network of stakeholders and to facilitate a form of novel organization without senior management or an organizational hierarchy. Ultimately blockchains must rely on a governance process in which the users agree upon a set of requirements including provisions for dispute resolution, sanctions for violating the rules, and procedures for enforcement of penalties.

---

268. GLENN, *supra* note 113 at 17–18.

269. Ennis, *supra* note 17. Coinbase is not the only crypto company whose interest-bearing accounts were investigated by law enforcement authorities. State regulators have previously ordered BlockFi Lending LLC (BlockFi) to stop selling that type of account to state residents, on the grounds that the product represents an unregulated security. SEC recently charged BlockFi for failing to register the sales of its crypto lending product. U.S. SEC. & EXCH. COMM'N, *supra* note 18.

270. 15 U.S.C. § 78l; 15 U.S.C. §§ 78m(d)(g); 15 U.S.C. 78(p); 17 CFR §§ 240.13d-1, 13d- 3. The Securities and Exchange Act further prohibits trading for the purpose of giving the false appearance of market activity or to manipulate the price of a security (15 U.S.C. § 78(i)).

The CG of blockchain-based business entities is impacted by enforceable regulation such as the GDPR and voluntary CSR/ESG metrics to strike a balance between innovation and protection of data. Blockchain technology itself provides for a flat governance structure where all the members of the network directly participate in the organization's decision makings. Such enabling environment for stakeholders is seen to provide for a vigilant data security and to shield corporations against legal risks in the future.

Technology changes over time. The rules and principles of good governance remain the same as they go to the essence of democratic values, safeguard a free and functional market, and preserve the duty of all to protect, respect and remedy violations of individual rights and freedoms. In our polycentric world where new technologies are tremendously changing the public dynamics, market laws and regulations, CSR/ESG, and the technology together provide an effective oversight and maximize data protection and privacy to fulfill obligations towards the public at large. Democracy after all must fight both the public and private means of control. With the rise of new technologies, this challenge is extended.