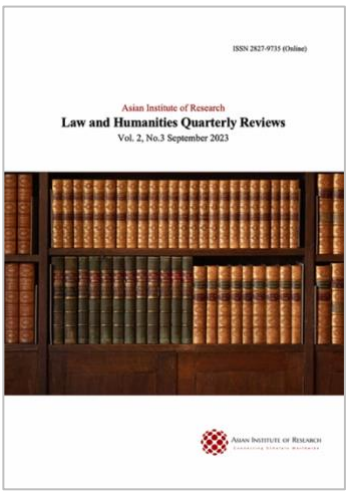


Law and Humanities Quarterly Reviews

Blandino, P. (2023). Blockchain, Legal Interpretation, and Contextuality as Tools to Establish Privacy and Fundamental Rights Protection Amid Geopolitical and Legal Uncertainty. *Law and Humanities Quarterly Reviews*, 2(4), 179-184.

ISSN 2827-9735

DOI: 10.31014/aior.1996.02.04.95

The online version of this article can be found at:
https://www.asianinstituteofresearch.org/

Published by:
The Asian Institute of Research

The Asian Institute of Research Law and Humanities Quarterly Reviews is a peer-reviewed International Journal of the Asian Institute of Research. The journal covers scholarly articles in the interdisciplinary fields of law and humanities, including constitutional and administrative law, criminal law, civil law, international law, linguistics, history, literature, performing art, philosophy, religion, visual arts, anthropology, culture, and ethics studies. The Law and Humanities Quarterly Reviews is an Open Access Journal that can be accessed and downloaded online for free. Thus, ensuring high visibility and increase of citations for all research articles published. The journal aims to facilitate scholarly work on recent theoretical and practical aspects of law.

ASIAN INSTITUTE OF RESEARCH
Connecting Scholars Worldwide

The Asian Institute of Research
Law and Humanities Quarterly Reviews
Vol.2, No.4, 2023: 179-184
ISSN 2827-9735

DOI: 10.31014/aior.1996.02.04.95

Blockchain, Legal Interpretation, and Contextuality as Tools to Establish Privacy and Fundamental Rights Protection Amid Geopolitical and Legal Uncertainty

Pierangelo Blandino[1]

[1] Ph.D. Candidate, Law, Technology and Design Thinking Research Group, University of Lapland – School of Law. Yliopistonkatu 8, 96300 Rovaniemi | m. +39 331 447 834. Email: pblandin@ulapland.fi

Abstract
This summary explores the degree of rights' protection when it comes to States forms of surveillance under a concise legal comparative outline. Given today's interdependence put into being first by Global Governance patterns and then by exchange on platforms, attention will be drawn to the Chinese Personal Information Protection Law (PIPL), American Clarifying Lawful Overseas Use of Data Act (Cloud Act) and the EU General Data Protection Regulation (GDPR), along with the recently adopted Data Privacy Framework (DPF). At a second stage, new possible techniques are considered to properly tackle these unprecedented changes that challenge traditional legal patterns.

Keywords: Blockchain, Legal Interpretation, Contextuality, Privacy, Fundamental Rights Protection

1. A comparative outline on (formal) limits to State surveillance

In the light of contemporary events regarding Ukraine and Taiwan, new forms of nationalism have emerged in the form of so-called techno-nationalism. Namely, it consists of «the emergence of a techno-nationalist vision that marries the praise of national scientific genius with greater state involvement in the financing of R&D and in the protection of the nation's scientific and technological heritage» (Le Grand Continent, 2022).

At a normative level, this prerogative can be observed in the prospective interpretative outcomes of existing pieces of legislation concerning surveillance over data. This estimate comes from US Government's National Security Strategy report issued on October 2022 (§Securing Cyberspace)[1].

[1] «Our societies, and the critical infrastructure that supports them, from power to pipelines, is increasingly digital and vulnerable to disruption or destruction via cyber-attacks. Such attacks have been used by countries, such as Russia, to undermine countries' ability to deliver services to citizens and coerce populations. We are working closely with allies and partners, such as the Quad, to define standards for critical infrastructure to rapidly improve our cyber resilience, and building collective capabilities to rapidly respond to attacks. In the face of disruptive cyber attacks from criminals, we have launched innovative partnerships, to expand law enforcement cooperation, deny sanctuary to cyber criminals and counter illicit use of cryptocurrency to launder the proceeds of cybercrime. As an open society, the United States has a clear interest in strengthening norms that mitigate cyber threats and enhance stability in cyberspace. We aim to deter cyber attacks from state and non state actors and will respond decisively with all appropriate tools of national power to hostile acts in cyberspace, including those that disrupt or degrade vital national functions or critical infrastructure. We will continue to promote adherence to the UN General Assembly-endorsed framework of responsible state behavior in cyberspace, which recognizes that international law applies online, just as it does offline».

In this respect, a classification based on the formal limits to State surveillance within the above-mentioned legal instruments can be fruitful to ascertain the underlying global degree of discontinuity in this sensitive subject matter. Methodologically, Richard's definition of privacy, understood as «the degree to which human information is neither known nor used» (Richards, 2021) conveys the idea of privacy as a bundle of prerogatives, including, but not limited to forms of outer interference. In that regard, it is possible to relate privacy as the basic building block for *habeas data* identifiable as right to (data) freedom (cf. Gstrein, & Beaulieu 2022; Risse (2023) [2]

Firstly, a centripetal regulatory technique can be noted in Chinese PIPL as per the residual element of art. 13's list[3] of conditions enabling personal information handling. Secondly, US Cloud Act does allow unilateral access, concretely neglecting the fundamental rights of non-US persons. From a European angle, these fundamental rights are the right to privacy, the right to data protection, and the right to an effective remedy and a fair trial[4].

Prior to the European Commission's adoption of the EU-U.S. Data Privacy Framework (DPF hereinafter) on 10th July 2023, Cloud Act opposed GDPR not allowing the disclosure of data without international mutual legal assistance[5] since it expressively omits this possibility[6]. Thirdly, GDPR places in between in light of its nature protecting civil liberties while also adding the principle of legitimate interest to data processing. Practically, it should be remarked that actors (i.e. companies) can potentially be faulty if they establish their legal strategy on one of these bodies of rules alone. Below, a comparative tab visually renders the above discussed traits pertaining to these instruments.

[2] As per Gstrein, & Beaulieu (2022) «We have already stressed that privacy should not be understood as an isolated concept, but rather as a proxy for the relationship between the individual and society. In this sense, the meaning of privacy evolves along the vectors of time, space and culture. While Cannataci argues that culture can be sub-divided in fields such as economic and technological development (Cannataci, 2016, pp. 8–10), the importance of political processes should not be underestimated. Few concepts relating to privacy and the control of information flows demonstrate this as clearly as habeas data, since its emergence is closely tied to the political history of countries in Latin America throughout the twentieth century (Gonzalez, 2015, p. 649). The expression 'habeas data' is derived from the more prominent legal principle 'habeas corpus', which is Latin for 'you should have the body'. In common law jurisdictions, this legal notion—or 'writ'—describes the requirement to bring a prisoner or detainee physically before the court to decide whether detention is lawful. In analogy, habeas data require public authorities to provide all personal data relating to a certain case or allegation to ensure that a person is aware of the basis of the accusations they are confronted with (Parraguez Kobek & Caldera, 2016, p. 114)».

3 Article 13:

Personal information handlers may only handle personal information where they conform to one of the following circumstances:

1. Obtaining individuals' consent;
2. Where necessary to conclude or fulfill a contract in which the individual is an interested party, or where necessary to conduct human resources management according to lawfully formulated labor rules and structures and lawfully concluded collective contract;
3. Where necessary to fulfill statutory duties and responsibilities or statutory obligations;
4. Where necessary to respond to sudden public health incidents or protect natural persons' lives and health, or the security of their property, under emergency conditions;
5. Handling personal information within a reasonable scope to implement news reporting, public opinion supervision, and other such activities for the public interest;
6. When handling personal information disclosed by persons themselves or otherwise already lawfully disclosed, within a reasonable scope in accordance with the provisions of this Law.
7. **Other circumstances** provided in laws and administrative regulations. [emphasis added]

https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/

[4] These rights are enshrined in articles 7, 8 and 47 of the Charter of Fundamental Rights of the European Union. For more details, https://policyreview.info/articles/analysis/mitigating-risk-us-surveillance-public-sector-services-cloud

[5] Through legal agreements.

[6] Additionally, «in 2020, the CJEU invalidated Privacy Shield in a decision known as Schrems II, in which the European Union was principally concerned with U.S. regulations enabling certain signals intelligence activities. The decision referenced Section 702 of the U.S. Foreign Intelligence Surveillance Act, which allows the U.S. government to compel communication service providers to assist in the surveillance of foreign persons outside the country, and U.S. Executive Order 12333, which denotes when intelligence agencies can engage in foreign intelligence surveillance abroad. Schrems II outlined two necessary benchmarks for the transatlantic data flows to be in compliance with EU law: U.S. surveillance activities should be limited to what is necessary and proportional and should be subject to judicial redress».

Source: https://www.csis.org/analysis/cloud-act-and-transatlantic-trust

Legal instrument	(Formal) limits to State surveillance	Remarks
GDPR	None	Limits set by ECJ
Cloud Act	Reasonable foreseeability	Insufficient check and balances when it comes to access of personal data stored overseas
PIPL	None	Cf. PIPL art. 13

Nonetheless, the DPF is partially bridging these normative gaps when it comes to data exchange and forms of State surveillance in EU and US space[7]. Although the US intelligence service can access data coming from the EU for security purposes, the access must be limited to what is strictly necessary and proportionate. Moreover, Europeans will also have access to the Data Protection Review Court (DPRC).

Hence, the individuation of new strategies is deemed necessary to protect the value of privacy, traceable back to the limit on the power of governments and companies and to the respect for individuals (Solove, 2020). Formally, it should not be excluded the virtual possibility for international agreements. Nonetheless, this approach alone does not suffice per se in the light of contemporary geopolitical contingencies. Additionally, a similar trend can be witnessed when it comes to international private law and blockchain[8].

2. Conclusions and viable strategies

«There can be no question of interpreting code. Code does not have a meaning; it has an effect. The only question can be whether the code fits with any natural language term of statement that preceded or accompany it» (H. Beale) (2021). In the remainder of the paper, attention will be drawn to viable alternatives to mitigate current global regulatory volatility. Additionally, It should be remarked that there are no technical limits having one's data accessed by governments' security agencies (Hildén, 2021).

In doing so, reference is made to the combined action of permissioned blockchain technology[9] and legal interpretation to increase contextuality with a double purpose. Firstly, this suggested approach would temper algorithmic determinism. Secondly, State sovereignty would not be hampered by blockchain as a form of outer agency adding, and therefore being susceptible to overlap with Statehood when it comes to international agreements formation.

[7] No transfer to the United States can be legitimised based on the Decision on the DPF without the inclusion of the US company receiving the data in the list kept by the FTC. The DPF is, in fact, based on a self-certification mechanism, and only once all the obligations imposed by the Decision have been fulfilled by the company interested in joining the DPF, can transfers to that company be made, without the need to implement additional data protection measures. Furthermore, we must not forget that, regardless of the mechanism used for the transfer, stipulating a contract with the recipient of the data, located in the United States, is in any case mandatory pursuant to the GDPR (cf. GDPR's Art. 28).

[8] Overall, international private law provisions and categories are currently found inconsistent with today's legal thinking since they do not correspond to smart contracts matters and practical needs. Specifically, PRIMA Model and the Factual PRIMA as of the Hague Convention presuppose the existence of intermediaries not existing as such in the blockchain (de Vauplane, 2019). Moreover, the criteria of *lex rei sitae* can be difficultly met considering the aterritorial nature of the internet and thus, leaving room to the problem of mobility in private international law.
Analogously, at a sentencing level, clarity is still missed. Although the landmark Singaporean Court's *Quoine* decision ([2020] SGCA(I) 02) establishes guidelines and principles, it does not explicitly answer whether the automated nature of platforms can give rise to legal obligations. In concrete, the decision confirms an English case law's precedent (*Thornton v Shoe Lane Parking* [1971] 2 QB 163) holding that data inputs in a piece of software represent an offer.

[9] «Permissioned blockchains are blockchains that are closed (i.e., not publicly accessible) or have an access control layer. This additional layer of security means that the blockchain can only be accessed by users with permissions» (Oracle, 2022).
The big difference with the past is that this ledger isn't stored in one place, it's distributed across several hundreds or even thousands of computers around the world. No one person or entity can control the data, which makes it transparent.
The data forms blocks that are encrypted into a continuous chain using complex mathematical algorithms. Once updated, the ledger cannot be altered or tampered with, only added to, and it is updated for everyone in the network at the same time» (BBC,2017).
From another angle, blockchain can be understood as the conjunction of «two of the central legal devices of modernity: the ledger and the contract» (Maurer, Du Pont, 2015).
Therefore, it is possible to grasp how this technology empirically enables the overcoming of territorial- physical limits. Specifically, the ductility of the blockchain allows it to be applied in the most diverse areas, making it a general-purpose technology on a par with the Internet and electricity (Skolnikoff, 1993).

In short, blockchain is «a distributed database that maintains a continuously growing list of ordered records, called blocks». These blocks «are linked using cryptography. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data. A blockchain is a decentralized, distributed and public digital ledger that is used to record transactions across many computers so that the record cannot be altered retroactively without the alteration of all subsequent blocks and the consensus of the network» [10] .

Added to the above, smart contracts, as pieces of software automatically running on the blockchain, can enhance States cooperation[11] by reducing uncertainty[12]. Given the flexible nature of tokens[13] susceptible of representing «almost anything: a unit of virtual currency, an asset, physical object, or any other abstract entity» (Gervais, 2018), «the paradox of erasing the need for trust» (Rantala, 2017) emerges. Concretely, «untrusted members can interact verifiably with each other without the need for a trusted authority» (Casino, Dasaklis, & Patsakis, 2019). Interestingly, Reid Hoffman's vivid expression «trustless-trust» (Werbach, 2009) conveys this state of affairs. More precisely, «on a blockchain network nothing is assumed to be trustworthy [...] except the output of the network itself» (Ibidem). For the sake of this study, it should be remarked that States can therefore refrain from ascertaining the consistency of their peers' (i.e. other States') actions given that blockchain constitutes an immutable record of transactions[14].

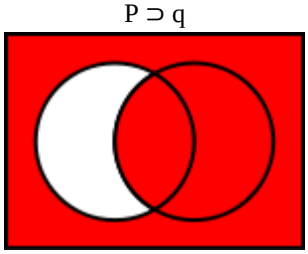
However, smart contracts are irrespective of possible contextual (i.e. factual) changes and human input remains essential to link actual development with that of blockchain. The following example illustrates these possible discrepancies. Let us consider, for instance, the case of a debtor who does not pay the sum of money to the creditors stipulated in the judgment. In many jurisdictions, the creditor may proceed in such a case with execution on the debtor's assets. In this case, the competent court will usually order the debtor's employer to start deducting a certain amount from the debtor's salary to satisfy the creditor. This possibility is not, however, unlimited, as it is intended to ensure that the debtor maintains a minimum subsistence level. Obviously, the rationale behind this rule is the need to balance the creditor's right to obtain the money with the need to preserve the debtor's basic needs and rights. Similarly, a landlord seeking to evict the tenant would not be able to achieve this result with immediate effect: this is true even where there are legitimate grounds for eviction. National tenancy law requires that the tenant be given a minimum amount of notice in order to balance the landlord's right to regain possession of the house with the tenant's need to find an alternative solution for his accommodation. Therefore, the enforcement procedures established by state law require a certain period of time not only because instantaneous coercion (Lessig, 1999 and 2006) is not practically feasible, but also and especially in order to balance the opposing interests of the parties (Colber, 2018). In contrast, the blockchain network does not - by its very nature - envisage either the presence of the judge (interpreter), the balancing of the interests at stake, or (to give just one example) respect for human rights (Fairfield, 2014; Wright, & De Filippi, 2015). And with respect to the two aforementioned examples, the smart contract could make an automatic deduction (Garcia-Teruel, 2020) from the wages of the defaulting tenant and might be able to recover his money efficiently, without the need to rely on state-mediated procedures that impose an expected rate of return. In the case of eviction, the use of automatic locks managed through blockchain technologies can make it immediately impossible for the tenant to gain access to the house once the landlord activates the eviction through software scripts.

[10] Synopsis, https://www.synopsys.com/glossary/what-is-blockchain.html#:~:text=A%20blockchain%20is%20%E2%80%9Ca%20distributed,a%20timestamp%2C%20and%20transaction%20data.
[11] Without posing questions on Art. 2, §4 of UN Charter asserting that States shall refrain from threatening the territorial integrity of any State. In contrast, the blockchain's a-territorial feature would allow to bridge these gaps.
[12] More properly, we should «qualify the 'smart contract' as a 'synecdoche': conceptually speaking, the smart contract does not correspond to the agreement, but presupposes it and constitutes a written translation of it (in computer code language) (Allen and Widdison (1996) (Cannarsa et al. Eds, 2019)). Smart contracts will be referred to as the source of the obligations between the parties, but these obligations arise from a will previously formed, which is received and formalized with the smart contract» (De Caria, 2020). In this respect, we are witnessing for the first time ever to non-anthropocentric conducts, whose effects become unpredictable for the definition of forms of legal liabilities (Adorno, 1951). In turn, these unprecedented features pose severe challenges to the core of legal sets of rules and institutions while considering the animus, as the pillar for legal reflections. In brief, blockchain networks, as well as AI, put into being forms of *agere sine intelligere* (Floridi, 2020 and 2022). Therefore, the notion and the sense of trust is eroded because «it consists of substituting the information that one does not have with other information that supports confidence in the action (Duranti and Rodgers, 2012).
[13] As per the blockchain ecosystem, a token is an asset that is digitally transferable between two people. For further details, s. Coinhouse, https://www.coinhouse.com/learn/blockchain-technology/what-is-a-token/#:~:text=In%20the%20Blockchain%20ecosystem%2C%20any,have%20different%20classification%20and%20uses
[14] Thus, States should overcome the initial burden of disclosing part of their actions to benefit from this technology.

In that regard, legal interpretation results as a connecting factor since jurists verify the correspondence of facts against their representation over the blockchain. In that regard, «the key to this issue lies in interpretation's dualistic nature, i.e. that it has both a backward-looking conserving aspect and a forwardlooking creative one. This dualism would seem to indicate that in interpret ing the law, judges both seek to capture and be faithful to the content of the law as it currently exists, and to supple ment, modify, or bring out something new in the law, in the course of reasoning from the content of the law to a dec ision in a particular case» (Dickson, 2008).

Similarly, the same pattern can be extended to contemporary challenges when it comes to Code, State law, and international law agreements. As per the above-mentioned impossibility of interpreting code (Beale, 2021), semiotics can work as a conceptual framework to bridge the existing gap between law (i.e. natural language) and code (i.e. artificial language). The scope of this proposition is to establish *contextual consistency* between (uninterpretable code) and natural language-based legal narratives. Specifically, the argument can be based on the semantic version of the *material conditional* as per the below formula and its graphic equivalent – where *p* individuates code, while *q* legal narratives.

$P \supset q$



Source: Wikipedia

Hence, *p* (code) materially implies *q* (legal narratives)

This condition establishes the possibility of setting the aforementioned test to verify whether code contains, and therefore implies legal narratives. To put it differently, this enables us to prove whether there is a relation, though partia,l between code's effects and the legal discourse. More properly, this correlation can allow the interpreter (e.g. a judge) to ascertain the existence of legal institutions, or at least the elements pertaining to them. In sum, the interpreter can verify the code's coherence before legal facets[15].

Funding: Not applicable.

Conflict of Interest: The authors declare no conflict of interest.

Informed Consent Statement/Ethics Approval: Not applicable.

References

Casino, F., Dasaklis, T. K., & Patsakis, C. (2019). A systematic literature review of blockchain-based applications: Current status, classification and open issues. Telematics and Informatics, 36, 55-81. https://doi.org/10.1016/j.tele.2018.11.006

Colber, A. J. (2018). Not-So-Smart Blockchain Contracts and Artificial Responsibility. Stanford Technology Law Review, 21(2), 198.

15 This process is irrespective of a legal smart legal contract's formation in line with the classification below:
(1) Natural language contract with automated performance.
(2) Hybrid contract.
(3) Solely code contract.

De Vauplane, H. (2018). Blockchain and intermediated securities. NIPR. https://www.kramerlevin.com/a/web/37847/1804-NIPR-Vauplane-Hubert-de-Blockchain-and-intermediated-securi.pdf

Dickson, J. (2008). Interpretation and coherence in legal reasoning. Stanford: Encyclopaedia of Philosophy.

Fairfield, J. A. T. (2014). Smart Contracts, Bitcoin Bots, and Consumer Protection. 71 WASH. & LEE L. REV. ONLINE 36. https://scholarlycommons.law.wlu.edu/wlulr-online/vol71/iss2/3. Garcia-Teruel, R. M. (2020). Legal Challenges and Opportunities of Blockchain Technology In The Real Estate Sector. Journal of Property, Planning and Environmental Law: Volume 12 Issue 2, 2020. Available at SSRN: https://ssrn.com/abstract=4304743.

Gervais, D. (2018). Blockchain and smart contracts: the missing link in copyright licensing. International Journal of Law and Information Technology, 314. https://www.ivir.nl/publicaties/download/IJLIT_2018.pdf

Gstrein, O., & Beaulieu, A. (2022). How to protect privacy in a datafied society? A presentation of multiple legal and conceptual approaches. Philos. Technol. 35(3). https://doi.org/10.1007/s13347-022-00497-4

Hildén, J. (2021). Mitigating the risk of US surveillance for public sector services in the cloud. Communication Rights in the Age of Digital Disruption, University of Helsinki, Finland. PUBLISHED ON: 30 Sep 2021. DOI: 10.14763/2021.3.1578

Le Grand Continent (VV.AA.). (2022). État, puissance et technologie : le techno-nationalisme à Washington, , https://legrandcontinent.eu/fr/2022/04/21/etat-puissance-et-technologie-le-techno-nationalisme-a-washington/

Title English translation: State, power and technology: techno-nationalism in Washington

Lessig, L. (1999). Code and Other Laws of Cyberspace. Harper Collins.

Lessig, L. (2006). Code: Version 2.0. Soho Books.

Maurer, W., & DuPont, Q. (2015). Ledgers and Law in the Blockchain. MIT Press. https://escholarship.org/uc/item/6k65w4h3

National Security Strategy report, §Securing Cyberspace, p. 34 https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf

Oracle (VV.AA.). (2022). Permissioned Blockchain https://developer.oracle.com/learn/technical-articles/permissioned-blockchain#:~:text=Permissioned%20blockchains%20are%20blockchains%20that,accessed%20by%20users%20with%20permissions

Rantala, J. (2017). Blockchain as a Medium for Transindividual Collective, quoting K. O'Hara, 'Smart Contracts – Dumb Idea'. IEEE Internet Computing, 21(2), 97–101. https://www.researchgate.net/publication/337634161_Blockchain_as_a_medium_for_transindividual_collective

Richards, N. (2021). Why Privacy Matters (Chapter one). Oxford University Press. Chapter one.

Risse, M. (2023). Political Theory of the Digital Age: Where Artificial Intelligence Might Take Us. Cambridge University Press.

Sklolnikoff, E. (1993). The Elusive Transformation. Princeton University Press.

Solove, D. J. (2020). The Myth of the Privacy Paradox. GW Law Faculty Publications

(VV. AA). (2021). Smart legal contracts Advice to Government, UK, 88.

Werbach, K. (2009). The blockchain and the new architecture of trust. MIT Press

Wright, A., & De Filippi, P. (2015). Decentralized Blockchain Technology and the Rise of Lex Cryptographia. Available at SSRN: https://ssrn.com/abstract=2580664 or http://dx.doi.org/10.2139/ssrn.2580664.