Privacy in Financial Information Networks: Directions for the Development of Legal Privacy-Enhancing Financial Technologies

Ferrari, V.

DOI
10.1007/978-3-030-52535-4_17

Publication date
2020

Document Version
Final published version

Published in
Blockchain and Applications

Privacy in Financial Information Networks: Directions for the Development of Legal Privacy-Enhancing Financial Technologies

Valeria Ferrari(✉)

University of Amsterdam, Nieuwe Achtergracht 166,
1018 WV Amsterdam, The Netherlands
v.ferrari@uva.nl

Abstract. In light of the strategic role of financial information for law enforcement, the protection of privacy regarding financial data must be balanced with the advantages of automated mechanisms for the monitoring and recording of financial activities. The growing availability of financial data and the global dimension of financial networks, however, impose to carefully examine practices concerning the management of financial data, checking them against the core rules and principles of data protection. This paper steers this effort providing a framework for understanding privacy in the financial context; moreover, it overviews the relevant legal frameworks affecting the management of financial information and assesses concrete industry practices to expose some compelling privacy issues. The study suggests that further research is needed to establish (1) whether current practices in the financial industry determine a lack of legal protection with regard to users' privacy; (2) whether it is desirable to develop technological solutions that allow a greater degree of anonymity for digital financial transactions; and, if so, (3) which is the most suitable governance/legal and institutional framework for anonymous digital transactions.

Keywords: Financial privacy · Cryptocurrencies · FinTech · GDPR

1 Introduction

In the past decades, two major tendencies have emerged that urge to bring the issue on financial privacy in the spotlight. The first one is the digitalization of money and commerce, which have exponentially expanded the production and availability of financial data. In 2019, countries like Sweden and the Netherlands have registered a higher total amount of digital transactions than cash-based ones, showing a tendency towards substituting cash even in daily small-size payments. The second tendency is the reconfiguration of the incentives underlying the provision of financial services around data exploitation.

New tools for data collection and processing and possibilities of intersecting financial data with additional information about users' online activities situate financial informational within the logics of contemporary information economy. Financial intermediaries are subject to sector-specific provisions that – pursuing the objectives of

J. Prieto et al. (Eds.): BLOCKCHAIN 2020, AISC 1238, pp. 157–160, 2020.
https://doi.org/10.1007/978-3-030-52535-4_17

transparency, prevention of illegal activities and tax avoidance – mandate data collection, data retention and reporting obligations regarding individuals' transactions in order to enable efficient enforcement. These rules and the goals they pursue seem to overrun privacy considerations; however, the present paper argues that ongoing development of a the financial industry – characterized by data-intensive business models and global reach of financial intermediaries - impose to re-define the meaning of privacy in this particular context, checking the practices and the policies that govern financial information against the core principles of data protection.

2 Methodology

This paper addresses issues of financial privacy scrutinizing (a) the incentives for information gathering and the power imbalances created by data flows; and (b) the transparency and fairness of automated data processing and algorithm-based decision-making. The study provides an overview of legal instruments that affect the governance of financial data: Anti-Money Laundering (AML) and Counter-Terrorist Financing (CTF) policies on one side, and privacy legislation - i.e. the GDPR[1] and the Law Enforcement Directive[2] - on the other. In this context, the technological means that are or can be deployed to achieve the legal objectives are presented. Finally, the study discusses practices in the management of financial data that raise privacy issues and/or expose conflicts between law enforcement priorities and privacy legal protections.

3 Preliminary Findings

3.1 (Conflicting) Legal Frameworks Governing the Flows of Financial Data

Regulatory and governance frameworks at the international and European level ensure that financial institutions and firms cooperate with law enforcement agencies providing access to financial databases. The coordinating guidelines of the FAFT (Financial Action Task Force) and the Common Reporting Standards (CRS) by the OECD (Organization for Economic Co-operation and Development) set out global standards for the collection and exchange of financial information in the fight against money laundering, tax evasion and other financial crimes. At the EU level, the 5th Anti-Money Laundering Directive[3] the and other legal instruments[4] mandate that financial intermediaries have in place automated systems for customer identification, transactions monitoring and reporting. These compliance processes imply massive data collection, long data retention periods and the use of algorithmic decision-making systems for consumers' profiling and red flagging. While the regime of surveillance over financial

[1] Regulation (EU) 2016/679 (General Data Protection Regulation).

[2] Directive (EU) 2016/680.

[3] Directive (EU) 2015/849.

[4] E.g. Directive (EU) 2015/2366, Directive 2006/24/EC, etc.

flows has been strengthen in the aftermath of the 2008 financial crisis, the adoption of the GDPR has, in the EU, introduced principles and priorities for the government of business data that are diametrical opposite to those set out by AML and CTF rules. Financial institutions, therefore, are expected to enforce legal requirements and policy goals that are uneasy to incorporate within the same technological and governance structure.

In the meantime, solutions based on distributed ledger technologies have been proposed to address both the problems of financial transparency and privacy, following a different logic: not by enhancing the responsibility of the intermediary to enforce the legal objective, but eliminating vulnerabilities in the system by decentralizing its governance.

3.2 Privacy Issues in Financial Information Networks

Both the GDPR and the Police Directive create exceptions to privacy protection regimes when data is collected and analyzed for crime prevention, investigation and other legitimate law enforcement necessities. However, the boundaries of such limitations are not well defined: industry and law enforcement practices must be continually checked against the principles and standards set out by the European privacy frameworks. The Article 29 Data Protection Working Party (WP29) stresses, in various documents, that the core principles of data protection - including the principle of purpose limitation and data minimization - must be applied to data acquired and stored for law enforcement purposes.[5] This is not an easy task: the global dimension and the technological development of financial information networks make the EU legal instruments insufficient to prevent questionable practices of both financial firms and pubic authorities that affect European citizens' data.

Problems arise from the dual purpose of the personal data collected by financial intermediaries in the context of their AML/CTF procedures. Financial institutions collect and process massive consumers data on the basis of their legal obligations to do so, but it's hard to prevent such data to be used for consumer purposes as well - e.g. to provide personalized services, for targeted advertainment and credit scoring. For the latter, they share data with third parties, including insurance companies, marketing firms and social media platforms.[6] The dual purpose of the processing hampers the enforceability of individuals' rights as granted by the GDPR. The rights to data portability and erasure established by the GDPR for data collected for commercial purposes, for example, are not granted in case of data collected in the context of AML and law enforcement procedures.

Another, interrelated, aspect that affects the enforcement of European privacy policies is the cross-national nature of financial services and the underlying data flows.

[5] See, for instance, Article 29 Data Protection Working Party, "Opinion on some key issues of the Law Enforcement Directive (EU 2016/680), available at: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610178.

[6] This is stated in some banks' and payment providers' privacy policies; some banks, for instance, share data with Facebook for the service of Facebook Custom Audience, used for targeted marketing. .

Data protection rules established for firms and public authorities in the EU do not always have equivalents in the US. A staggering difference is, for instance, the data retention limitation: US companies can retain consumers data for up to 80 years. Moreover, while in the EU firms are bound by the principle of purpose limitation, in the US the commercial use of data collected for enforcement purposes is not prohibited. The impact of these differences in terms of privacy, surveillance and geopolitical power imbalances becomes glaring if one considers the global pervasiveness of the US financial service industry.

Finally, the high volume of data processing involved in AML procedures obliges financial firms to deploy automated or semi-automated systems for data collection and analysis and algorithm-based consumers profiling. Again, these practices are specifically addressed by the GDPR, but are not comprehensively targeted by US law. The WP29 has underlined how profiling, even when deployed in the context of law enforcement activities, must respect data protection principles and be grounded on a legal basis specified by national law.[7] Moreover, while the GDPR qualifies AML as legitimate grounds for automatic processing, the regulation guarantees nonetheless the individual's right to challenge the outcome of such processing. Once again, however, the expansion of data availability (including the possibility to link financial data with other types of personal data), the increasing complexity of algorithmic systems and and the global dimension of information networks challenge the effectiveness of European legal safeguards.

References

1. Campbell-Verduyn, M.: Bitcoin, crypto-coins, and global anti-money laundering governance. Crime, Law and Social Change, vol. 69 (2018)
2. Chaum, D.: Achieving Electronic Privacy. Scientific American, New York (1992)
3. Cohen, J.E.: What Privacy Is For. Harvard Law Review, vol. 126 (2013)
4. Frasher, M.: Multinational banking and conflicts among us-euaml/ctf compliance &privacy law: operational & political views in context. Swift Institute Working Paper No. 2014-008 (2016)
5. Gurses, S., Hoboken, J.: Privacy After the Agile Turn. Cambridge Handbook of Consumer Privacy, Cambridge (2018)
6. Jentzsch, N.: Financila privacy: An International Comparison of Credit Reporting Systems. Springer, Heidelberg (2007)
7. Lloyd, I.: Privacy, anonymity and the Internet. Electron. J. Comparat. Law **13**, 1 (2009)
8. Stan, S.: Financial Privacy in a Cashless Society (2019). SSRN: https://ssrn.com/abstract=3367610 or http://dx.doi.org/10.2139/ssrn.3367610
9. Swire, P.P.: Financial Privacy and the Theory of High-Tech Government Surveillance, Washington University Law Review, vol. 77 (1999)
10. Kleiman, M.N.: Privacy vs computerised Law Enforcement, Northwestern University Law Review, vol. 86 (1992). http://www.springer.com/lncs. Accessed 21 Nov 2016

[7] Article 29 Data Protection Working Party, "Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679", available at: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053.