Autonomous Systems and the Law

Edited by
Nikita Aggarwal
Horst Eidenmüller
Luca Enriquez
Jennifer Payne
Kristin van Zwieten

2019
Preface

Nikita Aggarwal, Horst Eidenmüller, Luca Enriques, Jennifer Payne, Kristin van Zwieteren

Recent advances in artificial intelligence research stand to significantly transform the law: both the way we practice law, and the way law performs its societal functions.

A defining feature of this transformation is the increased ‘autonomy’ of computerized systems, and their ability to automate or mechanize tasks previously performed by humans. Increasingly autonomous, data-driven systems create new challenges for law and policy. These include: how should (semi-)autonomous systems be regulated to capture the benefits of automation and provide adequate space for innovation, whilst still protecting consumers and investors? How should data protection and privacy laws control the use of personal data in such systems? How should liability be attributed or distributed where a (semi-)autonomous agent causes harm or loss? How does legal education and training need to change to equip the lawyers of tomorrow with the skills needed to manage increasingly automated legal processes? And, how should autonomous systems be designed so as to maximise their resilience to cyberattacks?

Against this backdrop, the academic editors of the Oxford Business Law Blog selected ‘The Law of Autonomous Systems and the Automation of Law’ as the theme of its 2018 annual conference. The conference took place on 8 March 2018 at St Hugh’s College, University of Oxford. It was organized around roundtable discussions, on the following themes: (i) Smart Contracts and Dispute Resolution; (ii) FinTech and LegalTech; (iii) Data Control and Cybersecurity. Conference participants were asked to present their ideas on a topic relating to one of the roundtable themes and, following the conference, to submit a blog post for a special series of the Oxford Business Law Blog.

For this book publication on ‘Autonomous Systems and the Law’, the authors substantially revised, extended and updated their contributions. Making them available in one volume will, we hope, facilitate the international discussion on one of the most fascinating and important policy debates of our times.

---

1 See https://www.law.ox.ac.uk/business-law-blog.
# Table of Contents

Preface .................................................................................................................. V
Author Biographies ................................................................................................ IX

**Part A. Smart Contracts and Dispute Resolution** .............................................. 1
  I. Smart Contracting: Simple, Digital, Automated *(Kai Jacob)* ....................... 3
  II. Toward a Consumer Contract Law for an Algorithmic Age *(Lauren Henry Schols)* .................................................................................................................. 9
  III. Smart Consumer Contracts: The End of Civil Procedure? *(Martin Fries)* .... 13
  IV. Micro-Justice and New Law: ‘Swarm Arbitration’ as a Means of Dispute Resolution in Blockchain-Based Smart Contracts *(Andreas Heczek)* ........... 17
  V. How to Resolve Smart Contract Disputes: Smart Arbitration as a Solution *(Mateja Durovec)* ............................................................................................. 23
  VI. Defining Smart Contracts: The Search for Workable Legal Categories *(Riccardo de Caria)* .................................................................................................. 27

**Part B. FinTech and LegalTech** ......................................................................... 35
  VII. Machine Learning, Big Data and the Regulation of Consumer Credit Markets: The Case of Algorithmic Credit Scoring *(Nikita Aggarwal)* .............. 37
  VIII. Regulating Robotic Conduct: On ESMA’s New Guidelines and Beyond *(Florian Möslin)* ................................................................................................. 45
  IX. Consumer Finance 3.0: Behavioural Insights, Big Data and Digital Technologies *(Geneviève Kelleringer)* ................................................................. 51
  X. The Day After Tomorrow of Banking: On FinTech, Data Control and Consumer Empowerment *(Oscar Borgogno and Cristina Poncele)* ..................... 55
  XI. Innovation without Authorisation? The Regulatory Black Box of Cryptocurrencies in China *(Mimi Zou)* ................................................................. 61
  XII. Paving the Way for Legal Artificial Intelligence: A Common Dataset for Case Outcome Predictions *(Ludwig Bull and Felix Steffek)* .................... 67

**Part C. Data Control and Cybersecurity** .......................................................... 73
  XIII. Machine Performance and Human Failure *(Horst Eidenmüller)* .......... 75
  XIV. Cities as Corporations? The Privatisation of Cities and the Automation of Local Law *(Sofía Ramchandani)* ......................................................... 81
  XV. Blockchains and the Right to be Forgotten *(Michele Frick)* .................... 87
  XVI. Automated Decisions Based on Profiling: Information, Explanation or Justification – That is the Question! *(Lukke Meerd and Martijn Storm)* .... 91
  XVII. Biometric Data Matching Risks and the Rise of Self-Sovereign Identity *(Alan Morrison)* ................................................................. 99

Index .................................................................................................................... 105
Author Biographies

Nikita Aggarwal is a PhD candidate at the Faculty of Law, University of Oxford, and a Research Associate at the Oxford Internet Institute. Her research focuses on the interaction of law and emerging technologies, with a particular interest in the regulatory challenges arising from Big Data and machine learning. Prior to this, she was an attorney in the legal department of the International Monetary Fund, where she advised on financial and fiscal law reform and worked extensively on initiatives to reform the legal and policy frameworks for sovereign debt restructuring. She previously practiced as a solicitor with Clifford Chance LLP, where she specialized in EU financial regulation and sovereign debt restructuring. She earned her LLB (Hons) from the London School of Economics and Political Science.

Oscar Borgogno is a PhD candidate at the Law Department of the University of Turin, and a research fellow at the Tilburg Institute of Law and Technology of the University of Tilburg. His research agenda focuses on competition law, FinTech, data portability and payments services markets. He is currently also working on smart contract and blockchain capabilities to enforce the rights of weaker parties. He received the ‘Donato Menichella’ Scholarship 2018/2019 granted by the central bank of Italy.

Ludwig Bull is the CTO at CourtQuant, the premier litigation risk assessment platform for litigation funders and insurers in the UK. He has a background in computer science as well as law (Cantab). Originally from Germany, Ludwig has spent most of his life abroad. He is a marathon runner and practices martial arts.

Dr Riccardo de Caria is an Assistant Professor of Comparative Public Law at the University of Torino. He earned a PhD in public law from the University of Torino, and a Master of Laws (LLM) from the London School of Economics and Political Science. He has published many articles in national and international law reviews, and a book on lobbying regulation. He has also been dealing extensively with financial regulation. Recently, he has started working on the legal framework for blockchain, bitcoin, and smart contracts. He teaches Public Law and Economics at the University of Torino and has taught the same subject at the University of Aosta.

Dr Mateja Durovic is a Lecturer in Contract and Commercial Law at King’s College London. Prior to this, he was an Assistant Professor (2015-2017) at the School of Law, City University of Hong Kong. He holds PhD and LLM degrees from the European University Institute, Italy (EUI), an LLM degree from the University of Cambridge, UK, and an LLB degree from the University of Belgrade, Serbia. Dr Durovic was a Post-Doc Research Associate at the EUI (2014-2015), Visiting Scholar at Stanford Law School, USA (2011), and at the Max Planck Institute of Private International and Comparative Law, Hamburg, Germany (2010). He has worked for the Legal Service of the European Commission, as well as being a consultant for the European Commission, The European Consumer Organisation (BEUC) and the United Nations. His work has been published in leading law journals (European Review of Private Law, European Review of Contract Law, Journal of Consumer Policy).

Dr Horst Eidenmüller is the Freshfields Professor of Commercial Law (Statutory Chair) at the University of Oxford and a Professorial Fellow of St Hugh’s College, Oxford, since 2015. Eidenmüller was born in Munich, Germany. He obtained an LLM at Cambridge University (1989) and a PhD from Munich University (1994) after working for McKinsey & Co. in the 1990s. After his Habilitation in 1998, he was a law professor at the University of Münster from 1999 until 2003. From 2003 to 2014, he held the Chair for Private Law, German, European and International Company Law at Munich University. Eidenmüller’s main research areas are contract law, company and bankruptcy law, and alternative dispute resolution. He is known for his economic and empirical analysis of important problems in these fields. Eidenmüller has held
visiting positions at major other universities such as Cambridge (2007), Harvard (2011) and Stanford (2014). From 2008 to 2009, he was a Fellow of the Institute for Advanced Study in Berlin. Eidenmüller is a Research Associate of the European Corporate Governance Institute (since 2009) and a Member of the Berlin-Brandenburg Academy of Sciences and Humanities (since 2008).

Dr Michèle Finck is a Senior Research Fellow at the Max Planck Institute for Innovation and Competition and a Lecturer in EU Law at Keble College, University of Oxford. Her research focuses on case law and judicial change from the perspective of EU law. She has particular expertise in AI, Big Data, platforms and blockchains, as well as data (protection) law.

Dr Martin Fries is a private lecturer (Privatdozent) at the University of Munich (LMU). His research focuses on various topics around civil law, commercial law, conflict of laws, legal ethics, and legal technology. Martin regularly serves as a mediator in commercial and inheritance disputes.

Dr Andreas Hacke studied law at the universities of Heidelberg, Leiden, Bonn and Münster (PhD). Since 2003 he has worked as a lawyer, arbitrator, mediator and academic. He regularly acts as an arbitrator, mediator and neutral expert to resolve complex national and international commercial and investment disputes. Further, he represents and advises corporate clients on all commercial and corporate matters. His special interest lies in designing tailor-made dispute resolution procedures to help resolve commercial and investment disputes. His academic work (both in research and in teaching) focuses on negotiation skills and on all forms of dispute resolution (litigation, arbitration, mediation and other forms of ADR). Andreas is Visiting Lecturer at the University of Oxford, teaching on the BCL/MJur courses on International Commercial Arbitration and on Commercial Negotiation and Mediation.

Dr Geneviève Hellingringer is a Law Professor at ESSEC Business School, Institute of European and Comparative Law, Lecturer in Law at Oxford University and ECGI Research Member. Geneviève is an executive editor of the Oxford Journal of Finanical Regulation (OUP).

Kai Jacob, a lawyer by education, joined SAP in 2008 and has headed the Global Contract Management Services team since 2011. In 2015, he was promoted to Global VP, assuming additional responsibility for Legal Information Management, aiming to support the legal digital transformation of the legal function. Kai joined the IACCM (International Association of Contract and Commercial Management) in 2004, became a member of its Board of Directors in 2012, and since January 2016 has been serving as Chairman of the Board. Kai is a regular speaker at conferences and has engaged in various round-tables, boards and initiatives in support of his vision of LIQUID LEGAL. In June 2018, Kai was appointed Chairperson of the newly founded Liquid Legal Institute e.V.

Alan Morrison is a Senior Research Fellow and Technology Editor for PwC. A 17-year veteran of PwC’s think tanks in Silicon Valley, Alan identifies emerging technologies on the cusp of adoption, analyzes how they are being used by large enterprises, and assesses their near-term business impact on behalf of PwC’s clients. Before PwC, Alan worked as a semiconductor market analyst, a retail site location analyst, a contract administrator for the Office of Naval Research at Stanford, and, on active military duty, as a US Navy Intelligence analyst. Alan has also served as a University Lecturer at the Faculty of Law, University of Cambridge, and a Senior Fellow of Newnham College. He serves as Co-Director of the Centre for Corporate and Commercial Law and as Deputy Director of the LLM programme.

Lokke Moerel is Professor of Global ICT Law at Tilburg University (The Netherlands) and Senior Of Counsel with Morrison & Foerster (Berlin). Her work with large U.S. tech giants on their strategic privacy and ethical issues has made her an expert on Big Data and artificial intelligence. Lokke is a member of the Dutch Cyber Security Council (the advisory body of the Dutch cabinet on cybersecurity). In 2016, Ms. Moerel was appointed to be the co-author of the annual public advice to the Dutch government on behalf of the Dutch Lawyers Society (NVM) on the Dutch Supreme Court on Big Data and the Internet of Things. In 2018, Lokke received the International Law Office Client Choice Award for Best Tech Lawyer Germany.

Dr Florian Millein is Professor of Law at Philips-Universität Marburg and co-director of its newly founded Institute for Law and Regulation of Digitalisation. He previously held positions at the Universities of Bremen and St. Gallen. Florian graduated from Ludwig-Maximilians-University of Munich in 1998, after having received the degree 'Licence en droit' from the University of Paris in 1996. He also holds a degree in business administration. In 1999, he was awarded a Master of Laws (LLM) from the University of London. Florian was a Jean-Monnet-Fellow at the European University Institute (Italy, 2007), and has been invited as a visiting fellow by the Universities of Sydney and Melbourne (Australia, 2011), as well as by the Universities of Berkeley and Stanford (United States, 2014). He has published various books, articles, comments on corporate law, contract governance, finance, and default rules, in addition to numerous articles in German and European law reviews.

Dr Cristina Poncio is a Professor of Comparative Private Law in the Law Department of the University of Turin, and a member of the PhD in Law, Person and Market board. She is also the Director of the Masters in International Trade Law of the ICT-ILO, the University of Turin and UNECE. In her career, Cristina has obtained an 'EFEMarie Curie Fellowship' of the European Commission at the Université Panthéon-Assas, a 'Max Weber Fellowship' of the European University Institute and a 'Lagrange Project Fellowship'. Before pursuing an academic career, Cristina was a trainee and associate at Allen & Overy. She is currently working on the interaction between contract law and technology in an international and comparative perspective.

Dr Sofia Ranchordas is a Professor of European and Comparative Public Law at the Faculty of Law of the University of Groningen and a Rosalind Franklin Fellow. She is also an Affiliated Fellow, and a former Resident Fellow, of the Information Society Project at Yale Law School. She has published a number of international peer-reviewed articles in international journals, book chapters, and well-ranked US law reviews. Her publications address the regulation of disruptive technologies, digital platforms, and the legal implications of data-driven regulation. She is the recipient of prestigious national and international grants (Knight Foundation, Independent Social Research Foundation, Dutch Science Foundation, Dutch Royal Academy of Sciences). She has advised the European Commission (DG GROW) and the Dutch Ministry of Interior on the regulation of disruptive technologies and is a regular invited speaker at international conferences.

Lauren Henry Scholz is an Assistant Professor at Florida State University College of Law. Before coming to FSU, she was a fellow at the Project on the Foundations of Private Law and the Berkman Klein Center for Internet & Society, both at Harvard Law School. She was also a fellow at Yale Law School's Information Society Project. Before entering academia, Scholz was a law clerk for the American Civil Liberties Union of Massachusetts and the Center for Democracy and Technology. Her research interests include contracts, torts, commercial law, information privacy and intellectual property. She is a Member of the Board of the Journal of Corporate Law Studies, the Cambridge Yearbook of European Legal Studies and other academic journals. She has also been an expert for the European Commission, the European Parliament, the World Bank, the OECD, national governments, courts,
Author Biographies

parliaments and science foundations. He studied in Cambridge (LLM), Heidelberg (PhD, undergraduate) and Hamburg (Habilitation, court clerkship).

Marijn Storm is an associate with Morrison & Foerster. His practice focuses on the intersection of data protection, information technology and intellectual property law. Resident in Morrison & Foerster’s Brussels office, he has advised leading EU-headquartered companies and semi-governmental organizations on a range of their most pressing privacy and data security challenges. Marijn has provided extensive advice to clients on the implementation of data breach notification requirements, and in the context of security breaches, has assisted with notification to both regulatory authorities and data subjects. Marijn regularly authors Privacy + Data Security client alerts and presents at seminars on topics ranging from GDPR compliance and breach notification to cloud computing and 3-D printing.

Dr Mimi Zou is the inaugural Fangda Career Development Fellow in Chinese Commercial Law at the University of Oxford. Dr Zou obtained her Doctor of Philosophy in Law and Bachelor of Civil Law (Distinction) degrees from St John’s College and Christ Church College, Oxford. She also graduated with first class honours degrees in Law, Economics, and Social Sciences (University Medal) from the University of Sydney. Prior to her appointment at Oxford, Dr Zou was an Edwards Fellow at Columbia Law School, Assistant Professor at the Chinese University of Hong Kong, and Senior Researcher at Utrecht University. Dr Zou is a qualified solicitor in England and Wales and lawyer in New South Wales (Australia). Alongside academia, she has worked and served as a consultant to law firms, international organisations, government departments, tech and financial institutions in Asia-Pacific and Europe for over 15 years.

PART A

SMART CONTRACTS AND DISPUTE RESOLUTION
Part B. FinTech and LegalTech

the gap with Big Data. Big Data is indeed another key to understanding consumer behaviour. Businesses have started to exploit Big Data to improve customer relationship management and, above all, to increase their profits.

The power of Big Data and associated predictive analytics could also be used to improve the efficiency of consumer law. While heterogeneity among consumers often means that regulations are over- and under-inclusive, the rise of Big Data has significantly decreased the costs associated with creating and administering personalized legal rules tailored to specific individual profiles or circumstances.¹⁶

As to disclosures, one possibility would be for salient messages to focus on overdraft or above-plan charges for consumers who have a lower degree of will-power and who are therefore likely to consume more than planned. By contrast, disclosures could focus on the core deal for consumers who are more likely to remain within the limits of the agreed-upon deal. Whether this will be effective, or desirable, is currently an open question.

Regarding default rules, such as caps on overdraft charges, their stickiness could be increased for customers whose profile indicates that they have a low credit score and are more likely to need overdrafts and might be the primary target of banks’ effort to have them opt out; other profiles could enjoy lower interest rates in exchange for an easier opt-out from the default. Even some mandatory protective rules (e.g., usury thresholds), which limit options for consumers, could be applied according to the individual consumer’s degree of rationality. Again, this raises questions both of practicality and policy.

In short, the combination of behavioural economics and Big Data analysis opens up the possibility of tailoring the regulation of market behaviour to more empirically valid characteristics, and to personalise it. This exciting prospect also opens up major questions, relating in particular to how privacy can be ensured and how justice can be achieved.


X. The Day After Tomorrow of Banking: On FinTech, Data Control and Consumer Empowerment

Christina Ponzibò and Oscar Borgogno

1. Setting the Scene

The increasing pace of innovation in technology used for financial and banking services (FinTech) both raises alarm bells and brings high expectations. On the one hand, traditional banking players fear serious losses in terms of eroded market power, reduced customer loyalty and disintermediation of direct consumer relationships. Traditional players are concerned about the impact that FinTech’s promise of ‘unbanking’ will have on their core functions (settling payments, collecting savings, providing credit and sharing risk).¹ On the other hand, the arrival of new, non-traditional players raises hopes of increased levels of competition within financial markets. For a long time, the retail-banking sector has been affected by lock-in problems, low elasticity of demand, abuse of market power by incumbents and high barriers to entry.² As a result, large, longer-established banks have been able to not only maintain high and stable market shares, but also engage in product-tying practices to the detriment of new market entrants and consumer welfare.

It is worth pointing out that this challenge is presented not only by start-ups, but also by technology ‘giants’. Over the years, companies like Apple, Google, Uber, Facebook and Alipay have gathered huge digital datasets as well as increased their Big Data analytics skills in exploiting consumer data and offering tailored services. It is just a matter of time before they start systematically providing financial and banking services to customers along with their core offerings.³ New FinTech services are based on the innovative use of financial data, such as insights into personal expenses, budgeting, comparison tools and tailored financial planning. Therefore, service providers need access to accounts data to implement their business. For their part,

Part B. FinTech and LegalTech

traditional banking players have always kept a strict and exclusive control over this information in order to consolidate their market power.4

To help FinTech achieve its pro-competitive potential, policy makers and financial regulators are now setting new regulatory frameworks and pursuing new supervisory approaches. The regulatory landscape that is relevant for FinTech in the EU includes Regulation (EU) No 679/2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (‘GDPR’), which came into force on 25 May 2018, and the sectoral Directive (EU) No 2366/2015 on payment services in the internal market (‘PSD2’), which came into force on 13 January 2018.6

2. From Ownership to ‘Control’ of Consumer Data: The Purpose of Competition Policy

One of the core innovations brought by the GDPR is the right to data portability. Pursuant to Article 20 of the Regulation, each person has the right to obtain a copy of all their personal data in a machine-readable, commonly used and structured format in order to share them, for instance, with a new data controller.

Despite the collocation within the GDPR, data portability has little to do with the right to data protection stated under Article 8 of the EU Charter of Fundamental Rights.7 In particular, we would stress that the concept of ‘data portability’ is not a matter of data protection but rather of competition policy.8 By allowing individuals to move their data from one controller to another, the EU legislator aims to boost competition among data-enabled service providers.

Further, data regulation challenges traditional concepts of civil law: like other information-related goods, data can be reproduced and transferred at almost zero marginal cost. In this respect, data portability has been shaped as a specific form of control over data, rather than a property ownership right. Thus, the right to data portability under the GDPR cannot be identified with a property rights-like regime. Sufficient to say that property entails the right to exclude anyone, which is not provided by the GDPR (nor the PSD2, examined below). Similarly, the right to erasure under the GDPR (Article 17) cannot be seen as a proprietary tool, due to its extremely limited (and highly contested) applicability.9

In this context, PSD2 represents a fundamental piece of legislation aimed at promoting competition by empowering consumers to exploit their own data within the Internal Market. Some of the changes concerning data regulation enacted by the Directive are far-reaching and are worth investigating from a competition policy perspective. Under the so-called Access to Account rule (XS2A) introduced by PSD2, providers of payment initiation services (PISs) and account information services (AISs) have free access to a user’s account data, on the condition that it is accessible online, and the customer gives his explicit consent.10 PISs are services based on orders to initiate a payment, at the user’s request, directed to another account service provider (such as a bank). These services contribute towards the opening up of the retail payment market by lowering transaction costs and facilitating online payments, both for businesses and consumers. This development opens the door to widespread use of mobile and internet payments, which is fueling the current trend of e-commerce growth.

AISs are services aimed at providing consolidated information about one or more payment accounts held by the user with another payment service provider. This means that firms providing customers with payment accounts will give access to their account data and operations to third parties, such as the new FinTech players. Under this new legal framework, banks are expected to both execute payment orders given by users through providers of PISs, and provide account information to providers of AISs for free, and on an equal footing with their own services.

Thus, consumers will exercise a specific form of control over their data. Here the question is whether such a notion of ‘control’ will represent a valid substitute for traditional ownership rights in protecting consumer rights and interests, especially concerning privacy.

As suggested above, by introducing the XS2A rule, PSD2 marked a crucial step towards the opening of retail payment markets for authorized newcomers, which from now on will have the right to request account information without any previous agreements with banks. Thus, the EU aims to promote competition within retail payment markets to the benefit of customers by giving them greater bargaining power and control over their financial data.

3. Disentangling Data Portability and the Access to Account rule

It is worth evaluating the XS2A rule as an important contribution to the overall data governance regime in the EU and, more specifically, as a sector specific form of data portability limited to account data. PSD2 pre-empted

---


9 See B Koops (n 8).

10 Art 66 PSD2 (n 6).
Part B. FinTech and LegalTech

the entry into force of the GDPR by a few months and now provides a useful reference point for the implementation of data portability under the GDPR.

Of course, account data is clearly personal data according to the GDPR's broad definition ('any information relating to an identified or identifiable natural person'), so it is necessary to clarify how the two regimes should be coordinated. In fact, the Article 29 Working Party (WP29), which is a group formed by representatives of EU national supervisory authorities aimed at providing the Commission with independent advice on data protection matters, tried to reduce legal uncertainty by publishing specific guidelines on applying data portability rights. The WP29 also made it clear that the PSD2 sectoral legislation overrides the GDPR whenever data subjects' requests aim specifically at providing access to bank account history to third party service providers.

Therefore, when it comes to accounts data, the PSD2 X2A rule will take priority over the GDPR data portability regime. However, banks have been collecting huge quantities of data relating to their customers for years, as part of their business and regulatory duties, which exceed the material scope of X2A obligations (for example, relating to creditworthiness, commercial profiling, know-your-customer and anti-money laundering compliance, just to mention a few). Hence, it is clear that when customers ask to port their data, they will need to make a choice between what a regulator requires and what a customer requests. Consequently, attention should be paid when establishing transparency mechanisms to help customers navigate this scenario. Otherwise, the fragile pro-competitive goal pursued by EU legislators could be jeopardized.

4. Looking ahead

As discussed, data governance regimes enshrined by the EU legislator in the GDPR and PSD2, even if substantially different, introduce data portability as an emerging concept within EU law, which is likely to play a central role in the data-driven economy. Nonetheless, the process is far from complete: interoperability and portability need to be made effective, which is exactly where they risk remaining a dead letter. The PSD2 implementation process is at a more advanced stage compared to GDPR data portability. In particular, PSD2 required the European Banking Authority (EBA) to develop five sets of guidelines and six drafts of Regulatory Technical Standards (RTS) aimed at ensuring workable interoperability and implementation of the X2A rule, among other aspects.

After a complex drafting process, characterized by a heated debate with the European Commission, the EBA released the technical standards, which were later amended and published by the European Commission in November 2017. In order to comply with the X2A rule, banks can now set dedicated interfaces to transmit account data to third party service providers. Should the interface prove ineffective or excessively dysfunctional, FinTech companies have direct access to customers' accounts as a fall-back remedy. The difficult task of ensuring the proper functioning of this mechanism is left to the EBA and national authorities across the Internal Market.

Many players and scholars believe that Application Programming Interfaces (APIs) are the most reliable technologies for implementing the X2A rule. However, there is no consensus regarding who should define the APIs or, even more importantly, whether to standardize their creation. A likely negative consequence of a top-down approach to API standards would be reduced innovation. In fact, firms will prefer to provide services that are compliant with the chosen APIs, disregarding further potential innovations based on different interfaces. The pace of innovation could slow down, together with the ability of market players to operate freely and follow their entrepreneurial instincts.

However, despite several complex technicalities implied by effective implementation of data portability rules, Article 20(1) of the GDPR merely states a general requirement for the format of transmitted data, which need to be 'structured, commonly used and machine readable'.

Unsurprisingly, the WP29 advisory group suggested the adoption of APIs to implement data portability. So, it is likely that standardization will continue to play a substantial role in ensuring the consistent implementation of data portability regimes. Therefore, the major challenge which policymakers should focus on is whether and how to reach consistent 'data interoperability' between heterogeneous players across the industries, or allow undertakings to develop their own data portability environments autonomously and let the market pick the winners.

5. Conclusion

To conclude, it is clear that data portability is going to play a key role in the discussion concerning a suitable data governance regime for the future digital economy. In particular, we put forward that data portability relates to competition policy rather than to data protection. Further, the point we make in this contribution is that the EU legislator is not tackling the matter consistently. On the one hand, it has introduced a general right to data portability into an already complex data protection eco-system, raising the expectations for data protection authorities in managing this competition policy task: a task that could be carried out more effectively by competition authorities. On the other hand, it recognized the need to intervene with sector-specific solutions such as

---

11 Art 4 GDPR (n 5).
13 For a first overview on the point, see I Graef, M Husovec, N Purtova (n 7).
14 On this complex process, see, e.g., D Milanesi (n 2).
the XS2A rule, which is aimed at strengthening competition by empowering consumers to have more control over their data.

As we are witnessing, the standardization process under PSD2 shows how difficult it can be to reach a viable and effective outcome for market players. In this respect, the implementation of data portability rights under the GDPR is likely to be even more complex and troublesome, given the multifarious interests at stake across the range of existing industries covered by the general scope of the GDPR.

We believe, therefore, that regulators and policy makers would do better to design rules tailored to the specific needs of each industry, instead of adopting holistic and overly broad approaches.

XI. Innovation without Authorisation?
The Regulatory Black Box of Cryptocurrencies in China

Mimi Zou

Among the more controversial FinTech innovations in recent years has been the rise of cryptocurrencies, such as Bitcoin and Ethereum, on the back of ever-expanding possibilities offered by distributed ledger technology, such as blockchain. Peer-to-peer transactions involving cryptocurrencies operate on a decentralised, distributed ledger which does not require any intermediaries, such as banks or money transmitters. As the value of Bitcoin skyrocketed in 2017, Initial Coin Offerings (ICOs) also became a popular financing method for start-ups. ICOs entail the offering of digital coins or tokens, usually denominated in a cryptocurrency, to investors in return for cash. The tokens give investors a prescribed interest in the start-up, which in principle should gain value with the success of the business venture (sometimes the tokens can be used to purchase the product itself).

Growing popularity in the use and trading of cryptocurrencies, especially among speculators, and the lack of clarity on how they fit into existing regulatory frameworks, has attracted significant attention of late from regulators around the world. In China, the country with the largest cryptocurrencies exchanges, regulators issued a complete ban on exchanges and ICOs in September 2017. Nevertheless, some have viewed this ban as 'temporary' until the government figures out alternative regulatory measures, which could include the issuance of an official digital currency by the Chinese central bank, the People’s Bank of China (PBoC), and/or a government-run and controlled exchange.

In this contribution, the regulation of cryptocurrency in China is described as a ‘black box’, whereby the outside observer has no knowledge of the process through which the inputs enter the system and the outputs emerge at the other end. The opaqueness of such a system can widen the scope for regulatory arbitrage and give rise to ‘innovation without authorisation’. There has been a reported growth of cryptocurrency trading and ICO activities that involve the use of foreign platforms and other strategies to circumvent the ban. At the same time, regulators have shown considerable enthusiasm for

---

1 Circular of the People’s Bank of China, the Office of the Central Leading Group for Cyberspace Affairs, the Ministry of Industry and Information Technology, the State Administration for Industry and Commerce, the China Banking Regulatory Commission, the China Securities Regulatory Commission and the China Insurance Regulatory Commission on Preventing the Financing Risks of Initial Coin Offerings, issued on 4 September 2017 (‘2017 Circular’).
# Index

## A
- Algorithm(s), Algorithmic
  - Algorithmic Accountability 10, 82, 85, Chapter XVI
  - Algorithmic Auditing 42, 95
  - Algorithmic Contract II
  - Algorithmic Credit Scoring Chapter VII
  - Algorithmic Decision-Making 42–43, 45, 49, 81, Chapters II and XVI
  - Algorithmic Exploitation 11, 40–41
  - Algorithmic Testing 42, 48, 97
- Bias 40, 42, 70, 92–93, 97–98
- Black Box (algorithm, testing) 9, 95–97
- Consensus (algorithm) 29, 87, 89
- Fairness Chapter XVI
- White Box (algorithm, testing) 97–98

AI, See "Artificial Intelligence"

API, See "Application Programming Interface"

Application Programming Interface 59

Arbitration, See "Dispute Resolution"

Artificial Intelligence 6–7, 28; Chapters VII, VIII, XII, XIII, XVI
- Artificial Neural Networks 39, 68–71, 94
- Deep Learning 7, 39, 48, 94
- Explainable AI (XAI) 43, Chapter XVI
- Machine Learning Chapters VII and XIII, 9, 11, 45, 77, 93, 95
- Training Data 39, 68, 94, 98

Automated Decision-making. See "Algorithm (Algorithmic Decision-Making)"

## B

Behavioural Economics, Behavioural

Science 40, 54, 82, 85

Big Data 11, 20; Chapters VII, IX, X, XIV, XVI

Biometrics, Biometric

Data 40, 11, 15

Blockchain Chapters IV and XV, 3–5, 16, 23–26, 27–32, 61, 63, 81, 101–103
- Consensus (algorithm), See "Algorithm (Consensus)"
- Encryption 89, 100–101, 103
- Forking 89
- Hash (-ing) 88–90
- Immutability, See "Tamperproof (Tamper Resistance)"
- Key (public, private) 88–89, 101
- Off-Chain 88, 90, 102
- Oracle 5
- Mining/Miners 89
- Tamperproof (Tamper Resistance) 29, 88–90, 101

## C
- Competition Law/Policy 55–60
- Consumer
  - Consumer Contracts Chapters II, III, 25, 53–54, 84
  - Consumer Finance, Consumer Financial
    Law Chapter VII, IX
- Contract Law (General) Chapters II–VI, (See also "Consumer Contracts")
- Defences 11, 21, 32
- Credit Scoring Chapter VII, 49
- Cybersecurity, See Generally Part C

**DAO**, See "Decentralized Autonomous Organization"

Data
- Alternative Data 39, 43
- Data Protection, See "EU General Data Protection Regulation"
- Financial Data 39, 41, 45, 55, 57
- Legal Data 8, Chapter XII
- Personal Data Chapters VII, X, XIV, XV, XVI, XVII, 77

Decentralized Autonomous Organization (DAO) 4

Digital Currency(ies) 29, 33, 61, 63
- Virtual Currency 33, 62
- Cryptocurrency Chapter X, 3–4, 88–89, 101–102, 18
- Bitcoin, See "Cryptocurrency"
- Ethereum 3–5, 62
- Tokens (Digital) 3, 61–62, 90

Digital Literacy 82, 85

Discrimination
- Unlawful, Wrongful Discrimination 58, 83; Chapters VII, IX, XVI
- Disparate Impact 11, 40, 93, 98
- Behavioural Discrimination 38, 40, 41
- Dispute Resolution Chapters III, IV, V, XII
- Distributed Ledger Technology, See "Blockchain"
- DLT, See "Distributed Ledger Technology"

**E**
- EBA, See "European Banking Authority"
- ECI, See "European Court of Justice"
- Encryption, See "Blockchain (Encryption)"
- ESMA, See "European Securities Markets Authority"
- EU General Data Protection Regulation
  - Anonymization 94–95
  - Data Portability 41, 56–60, 101
Index

L
Legal Personality, Legal Personhood 47-48, 77
Legal Process Outsourcing 5
LegalTech Chapters I, III, XII
Liability Chapter XIII
- Duty of Care, See "Standard of Care"
- Standard of Care 41, 47, 77-79
- Strict Liability 10, Chapter XIII
Litigation, See "Dispute Resolution"

M
Medical Diagnosis Chapter XIII

P
Personalized Law, Personalization 12, 20, 40, 42, Chapter IX
Predictive Analytics, See "Big Data"
Privacy 51, 54, 57, 77-78, 84, 89, 93-96, 99-101, (See also "Fundamental Rights")
Profiling, See "Discrimination"
PSD2, See "Second EU Payment Services Directive"

R
Regulatory Sandbox 42, 61-65
Robo-advice 45-50

S
Second EU Payment Services Directive 41, 55-60
Self-driving Cars, See "Autonomous Vehicles"
Self-sovereign Identity 102
(Semi-) Autonomous Vehicles 76
Smart Cities 81-85
Smart Contract(s), See Generally Part A

F
FCA, See "UK Financial Conduct Authority"
Financial Conduct Authority, UK, 37, 40-42, 53, 59, 63
FinTech, See Generally Part B (Chapters VII-XI)
Fundamental Rights 10, 21, 56, 76, 78-79

G
GDPR, See "EU General Data Protection Regulation"

H
Hacker, Hacking 4, 21, 101-103
High Frequency Trading (HFT) 9
Human Rights, See "Fundamental Rights"

I
ICO, See "Initial Coin Offering"
Initial Coin Offering 61
Intellectual Property (Law) 30-31
Internet of Things 15, 77, 81, 99
IoT, See "Internet of Things"