European Legal Studies Institute Osnabrück
Research Paper Series

No. 20-02

Christoph Busch

Algorithmic Regulation and (Im)Perfect Enforcement in the Personalized Economy

January 2020

The Research Paper Series is edited by Christoph Busch, Oliver Dörr, Thomas Groß, Hans Schulte-Nölke, Fryderyk Zoll and provides access to research by scholars of the European Legal Studies Institute Osnabrück.
All papers in this series can be accessed at: elsi.uni-osnabrueck.de

Algorithmic Regulation
and (Im)Perfect Enforcement in the Personalized Economy

Christoph Busch[*]

Working Paper Version (January 2020)

Final Version to be published in: Christoph Busch and Alberto De Franceschi (eds.)
Algorithmic Regulation and Personalized Law, C.H.Beck Nomos Hart, 2021

Technological advances in data collection and information processing make it possible to tailor legal norms to specific individuals and achieve an unprecedented degree of regulatory precision. However, the benefits of such a "personalized law" must not be confounded with the false promise of "perfect enforcement". To the contrary, the enforcement of personalized law might be even more challenging and complex than the enforcement of impersonal and uniform rules. Starting from this premise, the first part of this Essay explores how algorithmic personalization of legal rules could be operationalized for tailoring disclosures on digital marketplaces, mitigating discrimination in the sharing economy and optimizing the flow of traffic in smart cities. The second part of the Essay looks into an aspect of personalized law that has so far been rather under-researched: a transition towards personalized law involves not only changes in the design of legal rules, but also necessitates modifications regarding compliance monitoring and enforcement. It is argued that personalized law can be conceptualized as a form of algorithmic regulation or governance-by-data. Therefore, the implementation of personalized law requires setting up a regulatory framework for ensuring algorithmic accountability. In a broader perspective, this Essay aims to create a link between the scholarly debate on algorithmic decision-making and automated legal enforcement and the emerging debate on personalized law.

[*] Professor of Law at the University of Osnabrück, Germany. I am grateful to the participants of the Yale Information Society Project Spring Conference on "(Im)Perfect Enforcement" (Yale Law School, April 2019) and the conference "AI Policy and Law" organized by the Chinese Academy of Social Sciences (Hangzhou, October 2019) for their very helpful comments.

Introduction

In recent years, a small but growing body of literature on personalized law has started to explore whether technological advances in data collection and data science could be used to tailor legal norms to specific individuals.[1] In this perspective, the use of big data and artificial intelligence could redefine the optimal complexity of legal rules and refine their content to a hitherto unachievable level of granularity. Personalized legal rules could thus consider actor heterogeneity to a degree impersonal laws are unable to do. As a result, regulatory errors stemming from over- and under-inclusive norms based on coarse-grained typifications could be reduced. Moreover, legal categories could be designed in a more precise and granular way taking into account insights from behavioral science.

Against this backdrop, this Essay aims to make two contributions: The first part of the Essay explains how algorithmic personalization of legal rules could be operationalized on the basis of user profiles for tailoring disclosures, mitigating discrimination in the sharing economy and optimizing the flow of traffic in smart cities. The second part of the Essay looks into an aspect of personalized law that has so far been rather under-researched: a transition towards personalized law involves not only changes in the design of legal rules, but also necessitates modifications regarding compliance monitoring and enforcement. It is argued that personalized law can be conceptualized as a form of algorithmic regulation or governance-by-data. Considering that personalized law builds on algorithmic processes and data analytics, the implementation of personalized law requires setting up a regulatory framework for

[1] See, for example, Ariel Porat and Lior J. Strahilevitz, *Personalizing Default Rules and Disclosure with Big Data* 112 Mich L Rev 1417 (2014); Omri Ben Shahar and Ariel Porat, *Personalizing Negligence Law* 91 NYU L Rev 627 (2016); Cass Sunstein *Choosing not to Choose: Understanding the Value of Choice* (Oxford 2015), 157–73; Christoph Busch, *The Future of Pre-contractual Information Duties: From Behavioural Insights to Big Data*, in Christian Twigg-Flesner, ed, *Research Handbook on EU Consumer and Contract Law* (Edward Elgar 2016) 221; Anthony J. Casey and Anthony Niblett, *The Death of Rules and Standards* 92 Indiana Law Journal 1401 (2017); Philipp Hacker, *Personalizing EU Private Law: From Disclosures to Nudges and Mandates* 25 European Review of Private Law 651 (2017); Christoph Busch and Alberto De Franceschi, *Granular Legal Norms: Big Data and the Personalization of Private Law* in Vanessa Mak et al, eds, *Research Handbook in Data Science and Law* 408 (Cheltenham 2018); Philipp Hacker, The Ambivalence of Algorithms: Gauging the Legitimacy of Personalized Law in Mor Bakhoum et al, eds, Personal Data in Competition, Consumer Protection and Intellectual Property Law, 85 (Heidelberg 2018); Omri Ben-Shahar and Ariel Porat, *Personalizing Mandatory Rules in Contract Law*, 86 U Chi L Rev 255 (2019); Christoph Busch, *Implementing Personalized Law: Personalized Disclosures in Consumer Law and Data Privacy Law*, 86 U Chi L Rev 309 (2019).

ensuring algorithmic accountability. Thus, in a broader perspective, this Essay aims to create a link between the scholarly debate on algorithmic decision-making and automated legal enforcement and the emerging debate on personalized law.

The Essay proceeds as follows: Part I sets the stage by very briefly introducing the broader societal context of personalized law as a form of algorithmic regulation. Part II introduces the concept of personalized law and discusses three use cases relating to digital marketplaces and smart cities. It also analyses the relationship between personalized law and personalization techniques applied by firms. Part III explains why personalized law can be described as a form of algorithmic regulation and argues for setting up a governance framework for ensuring accountability under a system of personalized law.

I. Big Data and the Crisis of Generalities

As the digital transformation expands into more and more areas of life, new data-driven business models are being developed at a rapid pace which are based on algorithms and data analytics.[2] The spectrum ranges from personalized advertising to telematics-based insurance and personalized medicine. In other areas, artificial intelligence is used for building "prediction machines"[3] which are utilized for a broad range of purposes from predictive maintenance of aircraft engines to predictive policing.[4] A common feature of the new technologies is that they are fuelled by the availability of granular data about individuals, objects and locations as well as significant advances in data-processing capacity.

These developments go hand in hand with a pervasive trend towards personalisation – some would even say "hyper-individualisation" – which, according to some observers, will result in a fundamental change in the relationship between the individual and society. The ubiquitous quantification and datafication of individuals and their social relations leads to a dissolution of collective categories, such as "citizen" and "consumer" and shifts the focus towards quantifiable differences between individuals. In the emerging "society of

[2] See, for example, Viktor Mayer-Schönberger and Kenneth Cukier, *Big Data: A Revolution That Will Transform How We Live Work and Think* (Boston 2013); Shaun B. Spencer, *Privacy and Predictive Analytics in E-Commerce*, 45 New England L Rev 101 (2015).

[3] Ajay Agrawal, Joshua Gans and Avi Goldfarb, *Prediction Machines: The Simple Economics of Artificial Intelligence* (Boston 2018).

[4] See, for example, Andrew Guthrie Ferguson, *Policing Predicitive Policing*, 94 Wash U L Rev 1109 (2017); Andrew D. Selbst, *Disparate Impact in Big Data Policing*, 52 Ga L Rev 109 (2017)

singularities"[5] the individual is no longer considered as a representative of a certain social group defined by general criteria based on an average model,[6] but rather as a singular and solitary being defined by a cloud of data points. According to some observers this shift from generality to singularity is a symptom of a more fundamental "crisis of generalities" caused by the advent of big data.[7]

Recently, research on the legal implications of big data and artificial intelligence has been gathering momentum. So far, the focus primarily lies on analysing the potential dangers for privacy and autonomy, and on elaborating a regulatory framework for the collection and processing of personal data and new data-driven business models.[8] However, the digital transformation may require a more fundamental recalibration of the relationship between individuality and legal norms. Adjustments will be necessary along two axes: One the one hand, it is necessary to define limits for the novel personalization techniques that enable firms to target individuals at a level of granularity that was unimaginable only a few years ago. On the other hand, the new technologies can be utilized for tailoring legal rules to small segments of the population or even individuals. So far, the scholarly discourses about the two aspects of law and personalization have been somewhat detached from each other, but it seems that they are two sides of the same coin.

II. Making Laws for the Personalized Economy

A. Granular Legal Norms: The Demise of Typifications?

Starting from this very brief diagnosis of social change, the proponents of personalized law argue that the rise of the data-driven society could change the way how legal rules are being designed.[9] Usually, legal norms formulate impersonal and abstract rules that are

[5] Andreas Reckwitz, *Die Gesellschaft der Singularitäten* (Berlin 2017). An English translation of this lucid analysis of the "crisis of generalities" will be published as Reckwitz, *The Society of Singularities* (Cambridge 2019).

[6] See also Todd Rose, *The End of Average* (New York 2016).

[7] See Reckwitz, *Die Gesellschaft der Singularitäten* at 24 (cited in note 5).

[8] See, for example, Ryan Calo, *Digital Market Manipulation*, 82 Geo. Wash. L. Rev. 995 (2014); Gerhard Wagner and Horst Eidenmüller, *Down by Algorithms? Siphoning Rents, Exploiting Biases, and Shaping Preferences: Regulating the Dark Side of Personalized Transactions*, 86 U Chi L Rev 581 (2019); Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (London 2019).

[9] This section draws on Busch, 86 Chi L Rev at 313-14 (cited in note 1) and Busch and De Franceschi, *Granular Legal Norms* at 410-13 (cited in note 1).

supposed to cover a large number of individual cases: To legislate means to generalize.[10] A tool for generalizing commonly used by the legislator are so-called "typifications". These are normative models that divide the infinite variations of the social world into certain categories that create meaningful order.[11] Through the use of typifications, situations which are on closer inspection heterogeneous are typified as being homogeneous. A classic example for legal typification is the determination of legal capacity by reference to age in order to avoid making difficult inquiries into the actual cognitive faculty and maturity of a person.[12] The rules on legal capacity do not take into account the actual maturity of judgment of an individual, but schematically define age limits. Similarly, the disclosure rules of consumer law do not take into consideration the informational needs of the individual consumer. Instead they are based on the model of the average consumer.[13] The same is true for liability rules in contract and tort law where a generalized objective standard is used. The normative model which is usually applied in this context is the reasonable person test referring to the "normal, reasonable person of average competence".[14] However, the rather crude one-size-fits-all design of legal norms based on typifications suffers from a certain degree of imprecision. The underlying typifications represent only a blurred picture of reality and ignore what *Oliver Wendell Holmes* called the "personal equation" of the individuals.[15] In mathematical terms, typifications only offer an approximate value.[16] They are heuristic approximations that simplify the problems caused by the infinite complexity of the real world. However, the use of legal approximations

[10] See Paul Kirchhof, *Allgemeiner Gleichheitssatz*, in Josef Isensee and Paul Kirchhof, eds, *Handbuch des Staatsrechts der Bundesrepublik Deutschland*, VIII, 697, 773 (Heidelberg 3d ed 2010); see also Hans Kelsen, *Allgemeine Staatslehre*, 231-32 (Berlin 1925).

[11] See Michael D. Barber, *Social Typifications and the Elusive Other: The Place of Sociology of Knowledge in Alfred Schutz's Phenomenology* (Lewisburg 1989) (on the use of typifications in sociology).

[12] Rudolf von Jhering, *Der Geist des römischen Rechts auf den verschiedenen Stufen seiner Entwicklung*, Part 1, Vol. 1, Leipzig 1854, 53-4; see also Duncan Kennedy, *Form and Substance in Private Law Adjudication* 89 Harvard Law Review 1685 at 1688-89 (1976).

[13] CJEU, Case C-210/96 – Gut Springenheide and Rudolf Tusky [1998] ECR I-4657, para 31; see generally Fabian Klinck and Karl Riesenhuber, eds, *Verbraucherleitbilder* (Berlin 2015).

[14] See, for example, § 276(2) of the German Civil Code; Hein Kötz and Gerhard Wagner, *Deliktsrecht* at 114 (13th ed Munich 2013); see also Mayo Moran, *Rethinking the Reasonable Person: An Egalitarian Reconstruction of the Objective Standard* (Oxford 2003). The legislative method of typification has been expressed very clearly by Oliver Wendell Holmes, *The Common Law* at 108 (London 1881): "The standards of the law are standards of general application. The law takes no account of the infinite varieties of temperament, intellect, and education which make the internal character of a given act so different in different men."

[15] Oliver Wendell Holmes, *The Common Law* at 108 (cited in note 14).

[16] One could argue that the reasonable man standard is an 'aspirational norm' which does not necessarily reflect reality, but provides an incentive to strive for a higher level of care. On aspirational norms, see Martin S. Flaherty, *Rights, Reality and Utopia*, 72 Fordham Law Review, 1789, 1791 (2003).

leads to regulatory errors and inequities and cause potential losses of efficiency resulting from the over- and under-inclusiveness of the normative models. The imprecisions resulting from typifications are only partially mitigated by applying group-specific standards and, in exceptional cases, typified adjustments. In hard cases, the inequities caused by coarse-grained typifications are compensated through general clauses.[17]

From an economic point of view, typifications can be conceptualized as means for reducing complexity costs.[18] The more complex a legal norm is, the more difficult and thus costlier is rule drafting, ex ante compliance and ex post adjudication. Thus, in the past a higher degree of individual fairness can only be achieved at the price of less legal certainty or higher complexity costs. In this model, complexity costs are directly linked to the limited capacity of human information-processing. Thus, one could argue that the optimal complexity of legal rules – and the granularity of the entire legal system – is limited by the bounded capacity of human-information processing. From this perspective, one could conceptualize the widespread use of typifications as the answer to an information problem and a concession to the imperfections of a legal system administered by humans. If this is true, we might be heading for the "demise of typifications". In the near future, big data, super-human information-processing capabilities and artificial intelligence could redefine the optimal complexity of legal rules and refine their content to a hitherto unachievable level of granularity. In such a scenario, personalized or "granular" legal rules could take into account actor heterogeneity to a degree impersonal laws are unable to do. As a result of granularization, regulatory errors stemming from over- and under-inclusive norms based on coarse-grained typifications could be reduced. In particular, legal categories could be designed in a more precise and granular way taking into account insights from behavioural science and the available data about individual actors. For example, it has been suggested that personalized disclosures could replace standardized information in consumer law and data privacy law[19]. Similarly, in a world of "quantified selves" rules on negligence could be tailored

[17] Marietta Auer, *Materialisierung, Flexibilisierung, Richterfreiheit* at 140 (Tübingen 2005); see also Frederick Schauer, *The Convergence of Rules and Standards*, 2003 N Z L Rev 303 at 308-09

[18] See, generally, Louis Kaplow, *A Model of the Optimal Complexity of Legal Rules* 11 Journal of Law, Economics & Organization 150 (1995).

[19] See Busch, 86 Chi L Rev at 319-24 (cited in note 1).

to the "personal equation" of individual actors.[20] Some even envisage personalized default rules in family and inheritance law.[21]

B. Use Cases of Personalized Law

The following section will briefly discuss three use cases that illustrate how personalized law could be applied in digital marketplaces and smart cities. The first example relates to personalized disclosures, which have become a favorite topic among those interested in personalized law.[22] The second example illustrates how personalization techniques could be used as a tool for mitigating discrimination in online marketplaces. Finally, the third example shows how personalized norms could be embedded into the regulatory environment of smart cities.

1. Personalized Disclosures on Digital Marketplaces

One field of application, which lends itself well to the use of personalized law, are mandatory disclosures.[23] Through personalized disclosures, it could be possible to provide consumers with information that is tailored to their situations, personalities, demographic characteristics and cognitive capabilities. The provision of such behaviorally informed (personalized) information instead of standardized (impersonal) information could reduce the amount of information to be provided and, at the same time, increase the relevance of a disclosure for the individual recipient of the information. Under such a model, data on consumers' purchasing habits and other patterns of past behavior could be used for reducing both the quantity problem of information overload and the quality problem of information mismatch that is associated with the one-fits-all approach to disclosure.[24]

---

[20] Ben-Shahar and Porat, 91 NYU L Rev 627 (cited in note 1).

[21] Porat and Strahilevitz, 112 Michigan Law Review 1417 (cited in note 1); see also Busch and De Franceschi, *Granular Legal Norms* at 420-21 (cited in note 1)

[22] See, for example, Porat and Strahilevitz, 112 Mich L Rev 1417 (cited in note 1); Busch, *The Future of Pre-contractual Information Duties* 221 (cited in note 1); Hacker, 25 European Review of Private Law 651 (cited in note 1)

[23] This section draws on Busch, 86 Chi L Rev at 316-17 (cited in note 1).

[24] For a critical analysis of impersonal disclosure mandates see, for example, Omri Ben-Shahar and Carl E. Schneider, *More Than You Wanted to Know: The Failure of Mandated Disclosure* (Princeton 2014); see also Busch, *The Future of Pre-contractual Information Duties* 221 (cited in note 1).

A famous and often cited example that illustrates this use case is the retailer Target, who used data mining to identify pregnant women among its customers.[25] Target's data miners observed that pregnant women were likely to buy certain nutritional supplements in their first trimester, unscented lotion in their second trimester, and hand sanitizer close to their due dates.[26] Knowing that the birth of a child is a watershed moment in the customer relationship, when shopping behaviors are open to change and new brand loyalties are likely to emerge, Target used the information to send personalized advertising and coupons to the pregnant women.[27] From a regulatory perspective, one could consider whether a retailer who has obtained such insights through data analytics should be obliged to use this information to provide consumers with targeted health warnings.[28] For example, a customer with a high "pregnancy prediction score" could be confronted with a specific warning message if she buys alcoholic beverages or raw cheese in an online shop.

Maybe this example seems a little bit creepy and overly paternalistic. This could indeed be the case. Let me be clear: I am not saying that the law *should* require online retailers to identify pregnant customers and confront them with unwanted warnings. What I am saying is that the law *could* do this on the basis of data analytics. This is a regulatory option that was not available a few years ago. Therefore, it has to be decided in which cases it is appropriate to use the new type of data-driven disclosure mandates and where to draw a line. This is of course a policy question that may be subject to conflicting points of view.

2. De-biasing Customer Ratings in the Sharing Economy

The second example of algorithmic personalization relates to the design of online reputation systems which are a common feature in the so-called sharing economy.[29] In

[25] See Charles Duhigg, *How Companies Learn Your Secrets* (NY Times Magazine, Feb 16, 2012), archived at http://perma.cc/8VGY-D93F.

[26] Id.

[27] Id.

[28] See Busch, *The Future of Pre-contractual Information Duties* at 234 (cited in note 1).

[29] See, for example, Steven Tadelis, *Reputation and Feedback Systems in Online Platform Markets*, 8 Annual Review of Economics 321 (2016); Sofia Ranchordas, *Online Reputation and the Regulation of Information Asymmetries in the Platform Economy*, 5 Critical Analysis of Law 127 (2018); see also Christoph Busch, *Crowdsourcing Consumer Confidence: How to Regulate Online Rating and Review Systems in the Collaborative Economy, in Alberto De Franceschi, ed, European Contract Law and the Digital Single Market*, (Cambridge 2016).

particular, ridesharing platforms, such as Lyft and Uber, are using reputation systems that allow customers to rate the work performance of drivers. After the service is rendered, customers are prompted to rate the service provider. These systems facilitate the semi-automated management of large, disaggregated and non-traditional workforces by outsourcing performance evaluations to customers.[30] However, recent research indicates that rating systems can be a vehicle for workplace discrimination if customer's biases creep into the evaluation for drivers.[31] This is particularly problematic where work-related decisions by platform operators are based on customer ratings. For example, it has been reported that Uber deactivitates drivers' accounts if their average rating falls below 4.6 out of 5.[32] Under anti-discrimination laws, employers are legally prohibited from making employment decisions based on protected characteristics of workers. However, reliance on potentially biased costumer ratings to make material determinations may actually lead to a disparate impact in employment outcomes.[33]

A number of regulatory interventions have been proposed for reducing the impact of biased rankings, such as raising awareness through establishing baseline statistics, reducing information available to raters or resituating the use of ratings within organizational structures.[34] Another, more technological approach would involve statistical pattern recognition and automated correction of biased ratings. In such a model, the rating behavior of customers would be scrutinized in order to detect patterns that indicate bias. For example,

---

[30] It is a matter of controversy whether drivers working for ridesharing platforms can be categorized as employees. However, this question can be left open for the purposes of our analysis. See generally Jeremias Prassl and Martin Risak, *Uber, Taskrabbit and Co: Platforms as Employers? Rethinking the Legal Analysis of Crowdwork*, 37 Comp Lab L Pol J 619 (2016).

[31] Alex Rosenblat, Karen E.C. Levy, Solon Barocas, and Tim Hwang, *Discriminating Tastes: Uber's Customer Ratings as Vehicles for Workplace Discrimination*, 9 Policy and Internet 256 (2017); Rossana Ducato, Miriam Kullmann, and Marco Rocca, *Customer Ratings as a Vector for Discrimination in Employment Relations? Pathways and Pitfalls for Legal Remedies* (2018), available at https://ssrn.com/abstract=3141156; see also Benjamin Edelman, Michael Luca, and Dan Svirsky, *Racial Discrimination in the Sharing Economy: Evidence from a Field Experiment*, 9 American Economic Journal: Applied Economics 1 (2017) (studying racial discrimination on Airbnb); see also Raymond Fisman and Michael Luca, *Fixing Discrimination in Online Marketplaces*, 94 Harvard Business Review 88 (2016).

[32] Prassl and Risak, 37 Comp Lab L Pol J at 638 (cited in note 30).

[33] Rosenblat, et al, 9 Policy and Internet 256 (cited in note 31); see also Miriam Kullmann, Platform Work, Algorithmic Decision-Making, and EU Gender Equality Law, 34 International Journal of Comparative Labour Law and Industrial Relations, 1 at 11 (2018).

[34] See, for example, Chrysanthos Dellarocas, *Immunizing Online Reputation Reporting Systems Against Unfair Ratings and Discriminatory Behavior*, Proceedings of the 2nd ACM Conference on Electronic Commerce. New York: ACM, 150–7 (2000) (suggesting a controlled anonymity scheme and cluster filtering); see also Rosenblat, et al, 9 Policy and Internet 269-74 (cited in note 31).

as suggested by *Rosenblat et al.* ratings could be checked for significant "statistical disparities between ratings assigned by a particular rater to workers inside and outside a protected group, according to matched comparisons based on other observable attributes".[35] If evidence of bias is found, the biased ratings provided could be assigned lower weight or corrected by a personalized "de-biasing factor" in order to ensure that the biased ratings will not influence the aggregate rating of the platform worker.[36] The example also shows the limits of algorithmic personalization as a regulatory instrument. Since, in practice, the implementation of such a model may be complicated by a lack of sufficient data that would allow a reliable detection of discriminatory rating patterns.[37]

Such a personalized de-biasing scheme could be implemented at various levels and does not necessarily require a public regulator to introduce such a system. Instead, one could imagine the implementation of a personalized de-biasing scheme by means private ordering.[38] It would be no surprise if some platform operators themselves take the initiative to introduce personalized de-biasing as part of their corporate non-discrimination policy. In fact, in the recent literature, platforms have been rightfully described as "the new governors"[39] reflecting that many platform operators are quite active regulating communications and activities of platform users.[40] Secondly, a requirement to implement a personalized de-biasing system could be included into an industry standard such as the recently adopted ISO 2018:20488 for online reviews.[41] In fact, the new ISO standard already contains a provision according to which the platform operator "should use dedicated IT programs for analysis within the computer systems used to moderate content for the purpose of verifying its appropriate, relevant and

---

[35] See also Rosenblat, et al, 9 Policy and Internet 269-74 (cited in note 31).

[36] See also Fisman and Luca, 94 Harvard Business Review 88 (cited in note 31) (suggesting that Uber could underweight ratings from those passengers, who have revealed themselves to be discriminatory, when calculating overall feedback scores).

[37] See also Rosenblat, et al, 9 Policy and Internet at 271 (cited in note 31).

[38] See, generally, Verstein, Privatizing Personalized Law, 86 U Chi L Rev 551 (2019) (discussing in which scenarios personalized lawmaking could be facilitated by non-state actors).

[39] Kate Klonick, *The New Governors: The People, Rules, and Processes Governing Online Speech*, 131 Harv L Rev 1598 (2018);

[40] See, generally, Michèle Finck, *Digital co-regulation: designing a supranational legal framework for the platform economy*, 43 Eur L Rev 47 (2018); see also Christoph Busch, *Self-Regulation and Regulatory Intermediation in the Platform Economy*, in Marta Cantero Gamito and Hans-Wolfgang Micklitz, eds, *The Role of the EU in Transnational Legal Ordering: Standards, Contracts and Codes* (Cheltenham 2019) (forthcoming), available at https://ssrn.com/abstract=3309293.

[41] ISO 20488:2018 (Online consumer reviews – principles and requirements for their collection, moderation and publication).

impartial character by automated means".[42] While this provision does not yet explicitly require the use of any automated de-biasing system, the implementation of a personalized de-biasing mechanism would probably be in compliance with the ISO standard.

3. Personalized Traffic Rules in the Smart City

Another use case of personalized algorithmic regulation could be the deployment of personalized traffic rules in smart cities.[43] The management and control of traffic flows through Advanced Traffic Management Systems (ATMS) is at the very core of research on data-driven urbanism. While most of the current literature focuses on the use of aggregate data of traffic streams, one could also consider the use of algorithmic personalization to implement a more granular regulatory policy. Indeed, such technologies are already being piloted in some cities. For example, in the Netherlands the city of Tilburg has recently been testing a new app called "Crosswalk" that alters crossing times at traffic lights based on the individual mobility needs of pedestrians.[44] A sensor in the traffic lights constantly scans the pavement in its vicinity and if it recognizes a pedestrian with the app installed on her smartphone, it adjusts the green-light time. The app comes pre-installed with one of four time settings, depending on the user's level of mobility, to minimise delays to other traffic. It is easy to conceive applications that apply similar technology for other applications. Dynniq, the Dutch company, that has developed the "Crosswalk" app is also developing an app for cyclists called "CrossCycle" which will sense when bikes are approaching a junction and change the lights sooner. Another version of the app shall detect visually impaired pedestrians and individually activate the ticking sounds that tell them whether the light is red or green. In the same vein, preferential parking permits could be issued to individuals based on relevant

[42] ISO 20488:2018, Section 6.5.3 (emphasis added)

[43] There is little consensus regarding the definition of "smart city". For an overview of the literature, see, for example, Vito Albino, Umberto Berardi, and Rosa Maria Dangelico, *Smart Cities: Definitions, Dimensions, Performance, and Initiatives* 22 Journal of Urban Technology 3 (2015); Andrea Caragliu, Chiara Del Bo, and Peter Nijkamp, *Smart Cities in Europe* 18 Journal of Urban Technology 65 (2014); see also Rob Kichin, Tracey P. Lauriault, and Gavin McArdle, eds, *Data and the City* (New York 2018).

[44] Gordon Darroch, *The slow lane: Dutch app allows elderly to 'hack' traffic lights* (The Guardian, July 12, 2017), https://www.theguardian.com/cities/2017/jul/12/dutch-app-elderly-hack-pedestrian-crossings; see also *The pros and cons of placebo buttons* (The Economist, January 26, 2019), https://www.economist.com/science-and-technology/2019/01/26/the-pros-and-cons-of-placebo-buttons.

temporary or permanent health conditions or family circumstances (for example, driving young children).[45]

A common feature of the examples cited here is that they involve tailored norms which are embedded in the digital infrastructure or the "regulatory environment"[46] of smart cities and are applied in real time.[47] This shows that the prospect of algorithmic personalization is closely linked to the development of Internet of Things (IoT) infrastructure. At the same time, it is important to note, that the above cited examples do not necessarily involve "technological management"[48] in the sense that traffic commands are superseded by technological traffic control, that would leave no autonomous choice for citizens.

C. Fighting Fire with Fire: Adverse Targeting meets Personalized Law

While the use cases of personalized law discussed above are still at an experimental phase or merely hypotheticals, businesses are using big data and artificial intelligence already today for personalizing their interactions with customers. In the emerging "personalized economy", sellers are using big data and sophisticated algorithms to tailor their commercial advertising, products, and prices with the aim of targeting individual consumers. While the welfare effects of first-degree price discrimination and the need for regulatory action against personalized pricing are a matter of controversial debate,[49] there is little doubt that the law should set limits to the use of personalization tools that systematically target and exploit idiosyncratic vulnerabilities of individual consumers.[50] It is less clear, however, which regulatory instruments should be used and where to draw the line between "smart" personalization techniques that are still acceptable and those that require regulatory action.

Consider, for example, that businesses with access to social media data can use information harvested from Facebook posts for individually targeting consumers in specific

---

[45] See Niva Elkin-Koren and Michal Gal, *The Chilling Effect of Governance-by-data on Innovation*, 86 U Chi L Rev 401 (2019); see also Casey and Niblett, 92 Indiana L. J. 1401 (cited in note 1).

[46] Roger Brownsword, *In the Year 2061: From Law to Technological Management*, 7 Law, Innovation and Technology 1 (2015).

[47] See generally Rob Kitchin, *The Realtime City? Big Data and Smart Urbanism*, 79 GeoJournal 114 (2014).

[48] Brownsword, 7 Law, Innovation and Technology at (cited in note 46)

[49] See, for example, Oren Bar-Gill, *Algorithmic Price Discrimination When Demand Is a Function of Both Preferences and (Mis)perceptions*, 86 U Chi L Rev 217 (2019); Marc Bourreau and Alexandre de Streel, The *Regulation of Personalized Pricing in the Digital ERA*, OECD Note, DAF/COMP/WD(2018)150.

[50] Calo, 82 Geo. Wash. L. Rev. 995 at 1010 (cite in note 8); Wagner and Eidenmüller, 86 U Chi L Rev 581 (cited in note 8).

life situations. Thus, advertising for online dating services could be displayed to users who have just changed their relationship status from "in a relationship" to "single" or "it's complicated". While this may be considered an acceptable way of targeting consumers, big data and artificial intelligence can be utilized for more problematic practices. As *Ryan Calo* underlines, "trouble arises when firms start looking at the consumer behavior dataset to identify consumer vulnerabilities".[51]

Indeed, new technologies allow businesses to exploit informational asymmetries and consumer biases in novel ways and open the door to the darker side of personalization in algorithmic marketplaces.[52] Recent research shows that the psychological characteristics of consumers can be quite accurately predicted from their "digital footprints", such as Facebook likes, Tweets, or Instagram posts.[53] For example, a recent study demonstrated that machine learning tools using color analysis, metadata components, and algorithmic face detection can make it possible to identify markers of depression in Instagram posts.[54] These results could provide new avenues for early screening and detection of mental illness. However, they could also enable businesses to exploit the vulnerabilities for adverse targeting and manipulative marketing techniques. Thus, individual customers could be addressed in their weakest moments.

Existing contract law rules and doctrines, such as unconscionability, undue influence, misrepresentation and duress may provide some minimum protection for consumers in extreme cases.[55] But they fail in cases where businesses use more subtle techniques to target psychologically instable consumers.[56] Another option for regulatory action would be to

---

[51] Calo, 82 Geo. Wash. L. Rev. 995 at 1010 (cited in note 8).

[52] Wagner and Eidenmüller, 86 U Chi L Rev 581 (cited in note 8); Philipp Hacker, *The Ambivalence of Algorithms* at 88-92 (cited in note 1); Natali Helberger, *Profiling and Targeting Consumers in the Internet of Things: A New Challenge for Consumer Law*, in Reiner Schulze and Dirk Staudenmayer, eds, *Digital Revolution: Challenges for Contract Law in Practice* (Baden-Baden 2016) 135, 151-52.

[53] David Stillwell, et al, *Psychological targeting as an effective approach to digital mass persuasion*, Proceedings of the National Academy of Sciences of the United States of America, 114 (48), 12714 (2017).

[54] Andrew G. Reece and Christopher M. Danforth, *Instagram photo reveal predictive markers of depression*, 6 EPJ Data Science 15 (2017).

[55] Wagner and Eidenmüller, 86 U Chi L Rev 581 (cited in note 8).

[56] But see Helleringer, *Profiling and Targeting Consumers in the Internet of Thing*s at 153-60 (suggesting that unfair commercial practices law might offer more flexible solutions); see also Przemysław Pałka, Agnieszka Jabłonowska, Hans-W. Micklitz, and Giovanni Sartor, *Before Machines Consume the Consumers*, EUI Department of Law Research Paper No. 2018/12, 6.

address the foundation of exploitative algorithmic techniques: big data. As adverse targeting is fueled by big data, this digital manipulation could be curbed by limiting sellers' access to information about consumers. But, as *Oren Bar-Gill* argues in the context of personalized pricing, attacking the big data foundation "runs the risk of throwing the baby out with the bathwater. Given the benefits that personalization provides, cutting the flow of information might be a net loss for consumers."[57]

A different solution has recently been proposed by *Gerhard Wagner* and *Horst Eidenmüller*, who suggest that consumers whose choices have been influenced by big data and artificial intelligence tools should be granted a special right to withdraw from the transaction.[58] They argue that such a remedy would be a justifiable extension of existing withdrawal rights under European Union (EU) law, which address exogenous and endogenous distortions of preferences. Generally speaking, in the EU mandatory rights of withdrawal exist for three types of scenarios: (1) distance contracts, for example, contracts concluded by phone or on the Internet; (2) off-premises contracts, for example, contracts concluded at the consumer's home or at her place of work; and (3) certain types of contracts that the legislator considers to be particularly complex, for example, insurance contracts and the sale of timeshares.[59]

The proposal by *Wagner* and *Eidenmüller* essentially means taking the existing withdrawal rights, which are based on coarse-grained typifications of contracting situations or contract types that typically raise issues of impaired consumer choice as a starting point and transforming them into more tailored instruments of consumer protection. However, as a start, it is not entirely clear whether the new withdrawal right shall apply in all cases where business utilize big data and artificial intelligence tools to influence consumers or only in the more problematic cases where particular vulnerabilities are exploited. The first case would almost certainly translate into a massive and undesired proliferation of withdrawal rights as the use of big data and artificial intelligence becomes common practice among businesses.

---

[57] Oren Bar-Gill, 86 U Chi L Rev 217 (cited in note 49).

[58] Wagner and Eidenmüller, 86 U Chi L Rev 581 (cited in note 8).

[59] See generally Jonathon Watson, *Withdrawal Rights* in Christian Twigg-Flesner, ed, *Research Handbook on EU Consumer and Contract Law* 241 (Cheltenham 2016); Christian Twigg-Flesner, Reiner Schulze, and Jonathon Watson, *Protecting Rational Choice: Information and the Right of Withdrawal* in Geraint Howells, Iain Ramsay, and Thomas Wilhelmsson, eds, Handbook of Research on International Consumer Law 111 (Cheltenham 2018); for a critical analysis see Horst Eidenmüller, *Why Withdrawal Rights?* 7 European Review of Contract Law 1 (2011); see also Omri Ben-Shahar and Eric Posner, *The Right to Withdraw in Contract Law*, 40 J Legal Stud 115 (2011).

The second case, which appears more plausible, would probably raise enforcement problems which will be addressed in Part III of this Essay.

III. Governance of Algorithms for Personalized Law

The remainder of this Essay explains why personalized part can be conceptualized as a form of algorithmic regulation and identifies some key elements of a governance framework for personalized law regimes. It is argued that it will be necessary to take privacy seriously, preserve autonomy and ensure the quality of data and the accuracy of the statistical model on which a personalized norm is built. In addition, a transition towards personalized law will require setting up an appropriate framework of compliance monitoring and algorithmic auditing.

A. Personalized Law as Algorithmic Regulation

The use cases of personalized law analyzed in Part II of this Essay show that personalized law is typically based on algorithmic processes. It can therefore be described as a form of algorithmic regulation.[60] As *Brauneis* and *Goodman* explain, an algorithmic process typically involves "(1) the construction of a model to achieve some goal, based on analysis of collected historical data; (2) the coding of an algorithm that implements this model; (3) collection of data about subjects to provide inputs for the algorithm; (4) application of the prescribed algorithmic operations on the input data; and (5) outputs in the form of predictions or recommendations based on the chain of data analysis."[61]

[60] See generally Karen Yeung, *Algorithmic Regulation: A criticial Interrogation*, 12 Regulation & Governance 505 (2018) (defining algorithmic regulation as "decisionmaking systems that regulate a domain of activity in order to manage risk or alter behavior through continual computational generation of knowledge from data emitted and directly collected (in real time on a continuous basis) from numerous dynamic components pertaining to the regulated environment in order to identify and, if necessary, automatically refine (or prompt refinement of) the system's operations to attain a prespecified goal"); see also Tim O'Reilly, *Open Data and Algorithmic Regulation*, in Brett Goldstein B and Lauren Dyson, eds, *Beyond Transparency: Open Data and the Future of Civic Innovation* (San Francisco 2013) 289.

[61] Robert Brauneis and Ellen P. Goodman, *Algorithmic Transparency for the Smart City*, 20 Yale J L & Tech 103 (2018) at 113-4; see also Tal Zarsky, *Transparent Predictions*, 2013 U. Ill. L. Rev. 1503, 1517-20; Tarleton Gillespie, *The Relevance of Algorithms,* in Tarleton Gillespie et al., eds, *Media Technologies: Essays on Communication, Materiality, and Society* 167 (2014); Joshua A. Kroll et al., *Accountable Algorithms*, 165 U Pa L Rev 633, 640 (2017).

In the example of personalized disclosures discussed above,[62] these five elements of an algorithmic process are present: (1) The personalized health warnings would be based on model that builds on correlations between particular purchasing patterns and pregnancy that have been observed in historical data. (2) On the basis of these correlations, an algorithm is coded that implements this model. In the example, the algorithm was developed by Target for the purpose of personalized advertising. The same algorithm could be repurposed for delivering personalized health warnings. (3) In order to identify customers that need a specific health warning, the purchasing history of individual customers is recorded. This data serves as input for the algorithm. (4) The algorithm is applied on the customer data; and (5) outputs a "pregnancy prediction score". On the basis of this score, it is decided whether a personalized health warning is displayed or not.

While this system seems not overly complex, the implementation of personalized law can even be simpler. As illustrated by the example of the "Crosswalk" app in Tilburg,[63] the application of personalized law does not necessarily require any complex analysis of input data. In this example, the personalization is made possible simply by real time communication technology that enables direct interaction between traffic lights and the apps installed on the smartphones of individual pedestrians.

B. Privacy and Choice

Personalized law is built on user profiling. Therefore, it is obvious that this regulatory model raises privacy concerns.[64] One could even ask whether the classic conflict between legal certainty and individual fairness, which personalized law purportedly is meant to solve,[65] is just replaced by a new conflict between individual fairness and *privacy*.

From a privacy perspective, within the EU a system of personalized law would have to comply with Article 8(1) of the Charter of Fundamental Rights of the European Union (CFR) and Article 16(1) Treaty on the Functioning of the European Union (TFEU) which both guarantee the protection of privacy. At the level of secondary legislation, these fundamental principles are mainly implemented by the General Data Protection Regulation (GDPR). Therefore, a system of personalized law introduced in the EU would have to be in line with

[62] See text accompanying notes 23-28.

[63] See text accompanying notes 43-48.

[64] This section draws on Busch, 86 Chi L Rev at 326 (cited in note 1).

[65] See text accompanying note 18.

the principles laid down by the GDPR. First, the GDPR would require the enactment of a law sanctioning the collection and data for the purpose of personalization.[66] Second, it is important to note that under the GDPR customer profiling is not prohibited as such. However, Article 22(1) GDPR gives every natural person the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.[67] This provision is subject to several exceptions spelled out in Article 22(2) GDPR. In particular, Article 22(2)(c) GDPR allows measures based on profiling if the processing of data is based on the data subject's explicit consent.[68]

In line with the principle *volenti non fit iniuria*, which is the foundation of Article 22(2)(c) GDPR, some applications of personalized law could be designed as an *opt-in model*.[69] This regulatory technique would probably be most suitable for personalized disclosures. Under an opt-in regime the consumer would have the right to choose between impersonal and personalized information. As a consequence, the degree of personalization of the information provided to the individual consumer would depend on her preference for privacy. This approach would reflect actor heterogeneity and take into consideration that different consumers may have different attitudes to privacy. If a consumer prefers the benefits of personalized law, she must accept customer profiling. If, however, a consumer is not willing to accept the processing of personal data for the purpose of customer profiling, she voluntarily forgoes the benefits of personalized law. In other use cases, such the automated de-biasing of customer ratings, it may be justified to apply personalization schemes irrespective of the data subject's explicit consent.

---

[66] See Article 6(3) GDPR and Recital 45 of the GDPR.

[67] On the scope of Article 22 GDPR see Sandra Wachter, Brent Mittelstadt, and Luciano Floridi, *Why a Right to Explanation of Automated Decision-Making Does not Exist in the General Data Protection Regulation*, 7 International Data Privacy Law 76 (2017); see also Lilian Edwards and Michael Veale, *Slave to the Algorithm? Why a "Right to an Explanation" is Probably Not the Remedy You Are Looking For*, 16 Duke Law and Technology Review 18 (2017).

[68] For these cases, Art. 22(3) GDPR requires the data controller "shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests". This can be interpreted to the effect that the GDPR requires the implementation of discrimination-aware profiling techniques, see Michael Veale and Lilian Edwards, Clarity, surprises, and further questions in the Article 29 Working Party draft guidance on automated decision-making and profiling, 34 Computer Law & Security Review 398, 403 (2018).

[69] Busch, *The Future of Pre-Contractual Information Duties* at 237-8 (cited in note 1).

C. Quality of Data and Models

Considering that personalized law is a form of governance-by-data, the quality of any relevant training data as well as the quality of the input data on which the prescribed algorithmic operations are applied is of key importance. The use of polluted or partial data could lead to inaccurate profiling of individuals and thus distort the application of personalized norms.[70] As profiling is based on statistical techniques, it is vulnerable to the problem of false positives and false negatives. As a result, an individual could be treated as part of a segment to which she does not in fact belong (false positive or type I error) or treat her as a person who does not belong to a category to which she in fact does (false negative or type II error).[71] The impact of such errors is very much context-dependent. In the case of personalized health warnings, the costs of a type I error are relatively modest, if a warning message about alcoholic beverages is displayed to a customer who was wrongly identified as "probably pregnant". By contrast, both type I and type II errors would have a distorting impact on online reputation systems in the case of automated de-biasing of customer ratings. The risk of erroneous classifications is particularly high if only little relevant data is available. Therefore, the implementation of personalized law regimes could be made conditional on a certain minimum amount of available data that allows sufficiently reliable inferences.

The reliability of personalized law not only depends on the quantity and quality of the data that is used for training and input, but also on the accuracy of the underlying model. The standard of accuracy (i.e. the strength of the empirical correlations) that is required may vary from case to case depending on the intrusiveness of the norm. For personalized rules concerning issues of health and safety a higher standard of accuracy (i.e. a lower misclassification rate) will be required than for information duties of lesser importance.

D. Compliance Monitoring and Algorithmic Auditing

Finally, a transition from coarse-grained typifications to highly-granular personalized law has also consequences on the level of compliance and enforcement.[72] Monitoring compliance with uniform rules such as standardized information duties is, as a general rule,

---

[70] Elkin-Koren and Gal, 86 U Chi L Rev 401 (cited in note 45); see also Anthony Casey and Anthony Niblett, *A Framework for the New Personalization of Law*, 86 U Chi L Rev (2018) (forthcoming).

[71] Mireille Hildebrandt and Bert-Jaap Koops, *The Challenges of Ambient Law and Legal Protection in the Profiling Era*, 73 Modern Law Review , 433-4 (2010).

[72] This section draws on Busch, 86 Chi L Rev at 328-30 (cited in note 1).

rather simple. Enforcement authorities such as the FTC in the United States or other market participants in countries with a system of decentralized enforcement of consumer law (for example, Germany) only have to verify whether the information provided by a trader complies with the list of disclosure items defined by the law. Compliance is even simpler if the law requires the use of certain standard forms for informing consumers, such as the Standard European Consumer Credit Information (SECCI)[73] or the European Standard Information Sheet for Mortgage Credit (ESIS).[74]

In contrast, monitoring compliance with personalized information duties is more complex. In the above-mentioned example of personalized health warnings based on a "pregnancy prediction score",[75] the question whether an online retailer has to display a personalized warning message depends on the data available to the company about the customer's purchasing history. Similarly, the automated de-biasing of customer ratings depends on correctly identifying patterns of discrimination in the rating history. Consequently, compliance monitoring in these cases would involve testing whether the business used the data which was available and has made the right inferences on the basis of the data set.

Similarly, the idea of personalized withdrawal rights as a remedy against adverse targeting, although appealing at first view, raises difficult enforcement problems. While many European consumers have a general knowledge about the existence of withdrawal rights in case distance contracts and off-premises contracts, the applicable rules will be less obvious if they depend on "stealth infringements"[76], i.e. the use of exploitative marketing techniques that are specifically targeted at an individual consumer. In other words, a consumer will almost certainly be unaware that her choice has been influenced by targeted sales techniques that exploit her idiosyncratic vulnerabilities and that the law therefore grants her a special right of withdrawal. Therefore, the consumer will not be aware of her withdrawal right if a rogue trader does not provide her with the legally required information about the withdrawal right. Monitoring whether a business that utilizes algorithmic targeting techniques complies with the duty to inform the most vulnerable consumers about their personalized withdrawal

[73] See Annex II of Directive 2008/48/EC of the European Parliament and of the Council of 23 April 2008 on credit agreements for consumers, OJ L 133/66 (2008)

[74] See Annex II of Directive 2014/17/EU of the European Parliament and of the Council of 4 February 2014 on agreements for consumers relating to residential immovable property, OJ L 60/34 (2014).

[75] See text accompanying notes ###

[76] Pałka et al, *Before Machines Consume the Consumers* at 5 (cited in note 56).

rights, would require that an enforcement authority opens the seller's "black box" and checks whether he has sensitive information about individual vulnerabilities.

From a market control perspective, the implementation of personalized will considerably increase the complexity of the "compliance landscape" and may lead to an "atomization" of market practices. Therefore, it is much more difficult and maybe even impossible for private actors such as consumer organizations to monitor whether a business complies with the applicable rules. As a consequence, effective enforcement of personalized law most probably requires some form of public enforcement. From a practical perspective, compliance monitoring would also require that the enforcement authority performs regular algorithm audits in order to ensure that the personalization algorithms perform as provided by the law (for example, use the right criteria for generating personalized disclosures). Such audits would also have to cover the data pools that are used for profiling customers in order to assess the validity of data and to ensure that the data is unbiased.

Conclusion

Technological advances in data collection and data science could be used to tailor legal norms to specific individuals. Thus, regulatory errors resulting from the over- and under-inclusiveness of coarse-grained legal rules can be reduced and the level of regulatory precision can be increased. Personalized law could even be used as in instrument for limiting the adverse impact of personalization techniques utilized by firms for targeting particular vulnerabilities of individual consumers. However, as a form of algorithmic regulation or governance-by-data, personalized law is itself vulnerable to the limitations of algorithmic processes. The precision of personalized law very much depends on the quality and quantity of data which fuels the personalization machine and the accuracy of the underlying model. Therefore, personalized law offers not a blueprint for "perfect enforcement"[77] but is subject to the imperfections that are inherent in algorithmic regulation. Therefore, it is necessary that a transition to personalized law is combined with an effective regulatory framework ensuring good governance of algorithms for personalized law.

[77] Jonathan Zittrain, *Perfect Enforcement on Tomorrow's Internet* in Roger Brownsword and Karen Yeung, eds, Regulating Technologies: Legal Futures, Regulatory Frames and Technological Fixes, 125 (Oxford 2008).