University of Zurich[UZH]

Zurich Open Repository and Archive
University of Zurich
University Library
Strickhofstrasse 39
CH-8057 Zurich
www.zora.uzh.ch

Year: 2018

Die Regulierung der prädiktiven Analytik: eine juristisch-verhaltenswissenschaftliche Skizze

Hermstrüwer, Yoan

Posted at the Zurich Open Repository and Archive, University of Zurich
ZORA URL: https://doi.org/10.5167/uzh-257945
Book Section
Published Version

Originally published at:
Hermstrüwer, Yoan (2018). Die Regulierung der prädiktiven Analytik: eine juristisch-verhaltenswissenschaftliche Skizze. In: Hoffmann-Riem, Wolfgang. Big Data – Regulative Herausforderungen. Baden-Baden: Nomos, 99-116.

Die Regulierung der prädiktiven Analytik: eine juristisch-verhaltenswissenschaftliche Skizze

Yoan Hermstrüwer

Die prädiktive Analytik als Sammelbegriff für unterschiedliche statistische Datenauswertungstechniken zur Vorhersage von Ereignissen schafft nicht nur Chancen.[1] Sie birgt auch Risiken, die die Entscheidungs- und Verhaltensfreiheit der Nutzerinnen und Nutzer auf die Probe stellen. Ein zentrales Instrument zum Umgang mit diesen Risiken ist das präventive Verbot mit Erlaubnisvorbehalt (Art. 6 Abs. 1 Datenschutz-Grundverordnung [DSGVO], § 4 Abs. 1 Bundesdatenschutzgesetz [BDSG]), das der klassischen Idee vom Datenschutz als Vorfeldschutz Rechnung trägt.[2] Danach ist die Verarbeitung personenbezogener Daten nur auf Grundlage einer gesetzlichen Ermächtigungsnorm oder einer freiwilligen und informierten Einwilligung zulässig. Flankiert wird dieses Verbot durch Regelungen zu *privacy by default* (Erwägungsgrund 78, Art. 25 Abs. 2 DSGVO), Informationspflichten (Art. 13, 14 DSGVO) und eine Reihe individueller Kontrollrechte.

In jüngerer Zeit sind diese Regelungsinstrumente und die impliziten Risikoannahmen des Datenschutzrechts wiederholt mit der Begründung kritisiert worden, hierdurch werde paternalistischer Bevormundung durch harte und weiche Eingriffe Vorschub geleistet.[3] Anders als harter Paternalismus zielt weicher bzw. libertärer Paternalismus mithilfe von sanften

---

1 Näher zum Begriff der prädiktiven Analytik Gandomi, A. & Haider, M. (2015). Beyond the hype: Big data concepts, methods, and analytics. *International Journal of Information Management, 35,* 137; Hoffmann-Riem, W. (2017, i.d.B.). Rechtliche Rahmenbedingungen und regulative Herausforderungen von Big Data.

2 Aus der jüngeren Literatur Hoffmann-Riem, W. (2017). Verhaltenssteuerung durch Algorithmen. *Archiv des öffentlichen Rechts, 142,* 1, 21–23; Paal, B. & Hennemann, M. (2017). Big Data im Recht. *Neue Juristische Wochenschrift,* 1697, 1700; Klar, M. & Kühling, J. (2016). Privatheit und Datenschutz in der EU und den USA – Kollision zweier Welten? *Archiv des öffentlichen Rechts, 141,* 165, 173–175.

3 Härting, N. (16. Dezember 2015). Datenschutzgrundverordnung als Instrument der Bevormundung: Trilog erfolgreich, Einwilligung tot. *Legal Tribune Online.* Abgerufen von http://www.lto.de//recht/hintergruende/h/datenschutzgrund-vo-dsgvo-krit

Anstößen (*Nudging*) darauf ab, die Nutzerinnen und Nutzer besserzustellen, ohne ihre Entscheidungsfreiheit durch Zwang oder eine signifikante Veränderung von Anreizen zu beeinträchtigen.[4]

Doch wie gerechtfertigt ist diese Paternalismuskritik eigentlich? In diesem Beitrag soll die These aufgestellt werden, dass die Warnung vor einem paternalistischen Datenschutzrecht und einer Infantilisierung der Bürgerinnen und Bürger ebenso kurz greift wie ein Hayeksches Vertrauen auf die selbstheilenden Kräfte des digitalen Marktes oder der schlichte Verweis auf den Rechtsstaat. Denn die Gewährleistung freier und informierter Entscheidungen über den Umgang mit personenbezogenen Daten und von Verhaltensfreiheit – dem eigentlichen Schutzgut des Rechts auf informationelle Selbstbestimmung – ist zu einem kollektiven Regelungsproblem geworden, das der Markt ohne Marktdesign und der Staat ohne empirisch fundierte Regeln kaum bewältigen können. Dieses Problem weist strukturelle Ähnlichkeiten mit öffentlichen Gütern auf, etwa der Umwelt oder der Stabilität des Finanzsystems. Die Verarbeitung von Big Data birgt aber auch die Gefahr von Informationsasymmetrien oder von Schädigungen anderer (negative Externalitäten).

Soweit Big Data auf Grundlage einer individuellen Entscheidung zur Datenpreisgabe – einer Einwilligung – verarbeitet werden, betrifft diese Entscheidung nämlich nicht allein den Einzelnen selbst. Vielmehr versagen in Situationen der individuellen Datenpreisgabe bisweilen ganze Märkte. Ein solches Marktversagen droht nach klassischer Auffassung nicht nur bei Monopolen, sondern auch bei öffentlichen Gütern, Informationsasymmetrien oder negativen Externalitäten. Die Korrektur von Marktversagen lässt sich als Gemeinwohlbelang definieren, der staatliche Eingriffe rechtfertigen kann; zumindest liegt eine Gemeinwohldefinition inso-

---

ik/; Kapsner, A. & Sandfuchs, B. (2015). Nudging as a Threat to Privacy. *Review of Philosophy and Psychology, 6,* 455 ff.; Krönke, C. (2016). Datenpaternalismus. Staatliche Interventionen im Online-Datenverkehr zwischen Privaten, dargestellt am Beispiel der Datenschutz-Grundverordnung. *Der Staat, 55,* 319, 325–330; Bull, H. P. (2017). Fehlentwicklungen im Datenschutz am Beispiel der Videoüberwachung. *JuristenZeitung,* 797, 800.

4 Thaler, R. H. & Sunstein, C. R. (2003). Libertarian Paternalism. *American Economic Review, 93,* 175, 175; Sunstein, C. R. & Thaler, R. H. (2003). Libertarian Paternalism Is Not an Oxymoron. *University of Chicago Law Review, 70,* 1159 ff.; für eine differenzierte Neufassung des *Nudging*-Konzepts Sunstein, C. R. (2016). The Ethics of Choice Architecture. In A. Kemmerer et al. (Hrsg.), *Choice Architecture in Democracies* (S. 21 ff.). Nomos: Baden-Baden.

weit näher als bei einem bloßen Schutz vor sich selbst. Der Verweis auf die beschränkte Rationalität der Nutzerinnen und Nutzer und eine durch Rationalitätsdefizite bedingte Fehlfunktion von Märkten (*behavioral market failure*) ist insofern regelmäßig entbehrlich. Soweit bereits ein Marktversagen im klassischen Sinne festgestellt werden kann, sind auch die Schwellen der Eingriffsrechtfertigung geringer als bei beschränkt rationalem Verhalten und einer ins Auge gefassten (paternalistischen) Bewältigung von Rationalitätsdefiziten.

Deutlich wird dieses Zusammenwirken zwischen Zieldefinition und Eingriffsrechtfertigung am Beispiel von *Opt-in*-Standardeinstellungen (Erwägungsgrund 78, Art. 25 Abs. 2 DSGVO). Solche Standardeinstellungen können an die verhaltensökonomisch begründbare und empirisch nachgewiesene Entscheidungsträgheit (*status quo bias*) anknüpfen. Sie führen dazu, dass weniger Nutzerinnen und Nutzer sie betreffende Daten preisgeben – so wie *Opt-in*-Organspenderegelungen die Zahl der Organspenden im Vergleich zu einer *Opt-out*-Organspenderegelung verringern.[5] Dass sich eine Regelung mit einer verhaltensökonomischen Einsicht in Einklang bringen lässt, erlaubt jedoch nicht den Rückschluss auf den paternalistischen Charakter der Regelung. Eine Gleichsetzung von Verhaltensökonomik und libertärem Paternalismus trägt nicht, und zwar schon deshalb nicht, weil die Verhaltensökonomik der positiven Analyse dient, während es sich bei libertär-paternalistischem *Nudging* um ein normatives Konzept handelt. Vor allem aber können sowohl die Regelungsziele – die gesetzgeberisch geronnene Intention – als auch die Regelungswirkungen verhaltenswissenschaftlich informierter Regeln ganz andere sein als diejenigen, die in der *Nudging*-Diskussion und der verhaltensökonomischen Forschung zu Gebote stehen.

So lassen sich *Opt-in*-Standardeinstellungen nicht nur als Instrumente zum Schutz der Nutzerinnen und Nutzer vor einer selbstgefährdenden Datenpreisgabe oder mit der Vorsorge gegen beschränkt rationale Trägheit – der Tendenz zum Nichtwidersprechen gegen eine grundsätzlich erlaubte Datenverarbeitung – rechtfertigen. Vielmehr können *Opt-in*-Standardeinstellungen auch eine Verringerung von Informationsasymmetrien bezwecken. Solche Standardeinstellungen schaffen nämlich einen Anreiz für Diensteanbieter, die Nutzerinnen und Nutzer besser über die Datenverar-

---

5 Dazu Johnson, E. J. & Goldstein, D. (2003). Do Defaults Save Lives? *Science, 302,* 1338 ff.; Johnson, E. J., Bellman, S. & Lohse, G. L. (2002). Defaults, Framing, and Privacy: Why Opting In-Opting Out. *Marketing Letters, 13,* 5 ff.

beitungsmodalitäten aufzuklären (*penalty defaults*).[6] Da die Diensteanbieter genau wissen, wie Daten verarbeitet werden und insoweit einen Informationsvorsprung gegenüber den Nutzerinnen und Nutzern haben, wird die Nichteinbringung relevanter Informationen in den Markt „pönalisiert" und ein Gemeinwohlbelang gefördert.

Vor diesem Hintergrund erweisen sich die Paternalismuskritik, aber auch der Verweis auf die Vermachtung der Datenverarbeiter als verkürzt, zumal sich die Einhegung staatlicher oder privater Datenmacht kaum in handhabbare und angemessene Regelungsinstrumente übersetzen lässt. Not tut vielmehr eine präzise Analyse der konkreten Regelungsprobleme, die möglichst in empirisch fundiertem Wissen über das Nutzerverhalten und die strategischen Reaktionen der Datenverarbeiter auf bestimmte Regulierungsinstrumente wurzelt.

1. Regelungsprobleme

1.1 Begründungsdefizite

Prädiktive Analytik – mit denkbaren Anwendungen etwa in den Bereichen der künstlichen Intelligenz, des Data-Minings oder Machine-Learnings – beruht auf der Durchsuchung sehr großer Datensätze (Big Data) nach statistischen Regelmäßigkeiten, um hieraus mithilfe ökonometrischer Modelle bestimmte Ereignisse mit einer bestimmten Wahrscheinlichkeit vorherzusagen.[7] So verlassen sich Kreditkartenunternehmen darauf, dass die

---

6 Ayres, I. & Gertner, R. (1989). Filling Gaps in Incomplete Contracts: An Economic Theory of Default Rules. *Yale Law Journal, 99,* 87, 94; Ayres, I. (2012). Regulating Opt-Out: An Economic Theory of Altering Rules. *Yale Law Journal, 121,* 2032, 2087; krit. Maskin, E. (2005). On the Rationale for Penalty Defaults. *Florida State University Law Review, 33,* 557 ff.

7 Martini, M. (2014). Big Data als Herausforderung für den Persönlichkeitsschutz und das Datenschutzrecht. *Deutsches Verwaltungsblatt,* 1481 ff.; Cohen, J. E. (2013). What Privacy Is For? *Harvard Law Review, 126*, 1904, 1920; Diebold, F. X. (2012). A Personal Perspective on the Origin(s) and Development of "Big Data": The Phenomenon, the Term, and the Discipline. *Working Paper,* 1 ff.; für eine Anwendung auf die Prognose des Beschuldigtenverhaltens im Rahmen von Entscheidungen über die Untersuchungshaft Kleinberg, J., Lakkaraju, H., Leskovec, J., Ludwig, J. & Mullainathan, S. (2017). Human Decisions and Machine Predictions. *National Bureau of Economic Research Working Paper 23180,* 1 ff.

Käufer von Filzpads für Stuhlbeine erheblich kreditwürdiger sind.[8] Die Auswertung von Facebook-Likes, Browsing-Daten oder Konsuminformationen ermöglicht genaue Vorhersagen über ethnische Zugehörigkeit, parteipolitische Einstellung, Religion, Suchtstoffkonsum, sexuelle Orientierung, Extraversion, Intelligenz oder emotionale Stabilität auf Grundlage hiervon völlig losgelöster Daten.[9]

Anders als die empirische Sozialforschung ist die prädiktive Analytik losgelöst von einem Verstehensprozess, der die Wirkrichtung einer bestimmten erklärenden (unabhängigen) Variable auf eine bestimmte zu erklärende (abhängige) Variable und einen theoretisch begründbaren Kausalzusammenhang zu identifizieren versucht.[10] Ziel ist es vielmehr, irgendwie geartete statistisch signifikante Korrelationen zu finden, um hierauf basierend Entscheidungen treffen zu können.[11]

Prädiktive Analytik entbehrt folglich einer individuell nachvollziehbaren Begründungsleistung; ihre innere Rechtfertigung speist sich allein aus dem Verweis auf das Vorhandensein einer immensen Datenmasse. Dadurch werden die klassischen Instrumente des Diskurses stumpfer, das Ringen um Tatsachenargumente und der Angriff von Entscheidungen mithilfe von Alternativhypothesen werden den Betroffenen erschwert. Prädiktive Analytik nagt an der rechtsstaatlichen Vorstellung eines Prozesses mit fair verteilten Begründungslasten und Angriffsmöglichkeiten.

Der schlichte Verweis auf datengenerierte Vorhersagen zeitigt einerseits Gefährdungen des rechtlichen Gehörs in öffentlichen Rechtsverhältnissen (Art. 103 Abs. 1 Grundgesetz [GG]). So ist etwa unklar, inwiefern algorithmenbasierte Verwaltungsakte einer Begründung bedürfen (§ 39 Abs. 1 Verwaltungsverfahrensgesetz [VwVfG]) oder eine Anwendung von Ausnahmeregeln (§ 39 Abs. 2 Nr. 3 VwVfG) in Betracht kommt. Andererseits haben die Nutzerinnen und Nutzer aber auch in Privatrechtsverhältnissen ein Interesse daran, dass Entscheidungen – etwa seitens einer Versiche-

---

8 Strahilevitz, L. J. (2013). Toward a Positive Theory of Privacy Law. *Harvard Law Review, 126,* 2010, 2021.

9 Kosinski, M., Stillwell, D. & Graepel, T. (2013). Private traits and attributes are predictable from digital records of human behavior. *Proceedings of the National Academy of Sciences, 110,* 5802, 5803.

10 Grundlegend Mayer-Schönberger, V. & Cukier, K. (2013). *Big Data: A Revolution That Will Transform How We Live, Work and Think.* Boston: Houghton Mifflin Harcourt, S. 50 ff.

11 Kerr, I. & Earle, J. (2013). Prediction, Preemption, Presumption: How Big Data Threatens Big Picture Privacy. *Stanford Law Review Online, 66,* 65 ff.

rung – nachvollziehbar begründet werden, entweder um diese Entscheidung angreifen oder das individuelle Verhalten anpassen zu können. Automatisierte Einzelentscheidungen bringen damit eine Umwucht in das tradierte System der Entscheidungsbegründung und drohen den Rechtsschutz zu erschweren.

1.2 Kontrollverluste

Die prädiktive Analytik zeitigt durch ihre Zukunftsorientierung aber auch Verluste individueller Kontrolle über den Prozess der Informationsgenerierung.

Erstens besteht zum Zeitpunkt der Einwilligung fundamentale Unsicherheit darüber, welche Informationen durch Datenaggregation überhaupt erzeugt werden können. Letztlich tragen die Nutzerinnen und Nutzer durch eine Datenpreisgabe zur Generierung von Informationen bei, die es zum Zeitpunkt der Einwilligung noch gar nicht gibt. Da sich die Aussagekraft aggregierter Informationen nicht im Voraus bestimmen lässt, ist die Einwilligung zur Legitimation der Verarbeitung von aggregationsgenerierten Informationen denkbar ungeeignet. Das Gebot der Zweckbindung (Art. 6 Abs. 1a i.V.m. Art. 5 Abs. 1b DSGVO) entfaltet kaum noch entscheidungssteuernde Wirkung. Denn zum Zeitpunkt der Datenerhebung stehen die Zwecke der späteren Datenverarbeitung noch nicht fest. Diese Form der Datenverarbeitung geht mit erheblichen Informationsdefiziten auf Seiten der Nutzerinnen und Nutzer einher; die Einwilligung erfolgt mithin nahezu unter Unwissenheit bzw. „ins Blaue hinein".

Zweitens trägt die Einwilligung zunehmend Züge einer irreversiblen Entscheidung. Dies liegt insbesondere daran, dass sich selbst anonymisierte Datensätze zunehmend mithilfe personenbezogener Hintergrundinformationen deanonymisieren lassen.[12] Dies ist auch auf die zunehmende Menge an Datensätzen mit *Long-Tail*-Verteilungen zurückzuführen, also Datensätze mit vielen Datenpunkten, die ungewöhnlich weit vom Modus (also dem häufigsten Wert) einer Verteilung entfernt und damit relativ sel-

12 Narayanan, A. & Shmatikov, V. (2008). Robust De-Anonymization of Large Sparse Datasets. *Proceedings of the 2008 Symposium on Security and Privacy,* 111 ff.

ten sind.[13] Die Verarbeitung von Big Data führt mithin dazu, dass die Wahrscheinlichkeit der Personenbeziehbarkeit gen 1 steigt.[14]

Drittens lassen sich die Wirkungen von Informationen über die Zeit kaum kontrollieren. So gewährt das neue europäische Datenschutzrecht zwar ein Widerrufsrecht (Art. 7 Abs. 3 DSGVO), ein Widerspruchsrecht gegen Profiling (Art. 21 Abs. 2 DSGVO) und ein Recht auf Vergessenwerden (Art. 17 Abs. 1 DSGVO). Allerdings lässt sich das aus der Datenaggregation gewonnene personenbezogene Wissen kaum durch eine Löschung des Individualdatums beseitigen, zumal die Löschung eines Individualdatums angesichts der großen Anzahl unabhängiger Beobachtungen im Aggregatdatensatz die Vorhersagekraft des Datensatzes nahezu unberührt ließe.[15] Im Übrigen werden Aggregatdaten oft eher bestimmten, durch bekannte Merkmale kategorisierten oder typisierten Gruppen zugeordnet, ohne dass es auf eine unmittelbare Individualisierung ankäme. Das Phänomen der indirekten Identifikation durch sog. Aussondern (*singling out*) unterfällt deshalb nunmehr auch dem Anwendungsbereich des europäischen Datenschutzrechts (Erwägungsgrund 26 DSGVO), wobei die Wahrscheinlichkeit einer Nutzung von Mitteln zur Identifikation einschließlich Kosten und Zeitaufwand zu berücksichtigen sind.

1.3 Soziale Dilemmata

Die Vorstellung, der Schutz von Privatheit sei durch eine individuelle Ausübung des Rechts auf informationelle Selbstbestimmung steuerbar, ist auch aus anderen Gründen kritisch zu hinterfragen. Denn die prädiktive Analytik geht mit kollektiven Entscheidungsproblemen einher, die die

---

13 Zur kommerziellen Nutzung von *Long-Tail*-Verteilungen Brynjolfsson, E., Hu, Y. J. & Smith, M. D. (2003). Consumer Surplus in the Digital Economy: Estimating the Value of Increased Product Variety at Online Booksellers. *Management Science, 49,* 1580 ff.

14 Ohm, P. (2010). Broken Premises of Privacy: Responding to the Surprising Failure of Anonymization. *UCLA Law Review, 57,* 1701, 1749–1750; Crawford, K. & Schultz, J. (2014). Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms. *Boston College Law Review, 55,* 93, 94.

15 Spiecker gen. Döhmann, I. (2014). Steuerung im Datenschutzrecht – Ein Recht auf Vergessen wider Vollzugsdefzite und Typisierung? *Kritische Vierteljahresschrift für Gesetzgebung und Rechtswissenschaft,* 28, 38–39.

Nutzerinnen und Nutzer durch individuelle Freiheitsbetätigung kaum bewältigen können.

Aus der Einwilligung lassen sich zunehmend korrelationsgetriebene Aussagen über Gruppen oder andere Personen generieren.[16] Über den sozialen Graphen – die Vernetzung mit bestimmten Personen – lassen sich aus einer Einwilligung immer öfter auch Informationen über Personen erzeugen, die diese Information über sich selbst gar nicht preisgegeben haben oder preisgeben wollten, etwa die sexuelle Orientierung.[17] Die individuelle Preisgabe personenbezogener Daten entfaltet in vernetzten Umgebungen – etwa sozialen Netzwerken – damit zunehmend drittbelastende Wirkung und verursacht negative Externalitäten für die Privatsphäre anderer.

Die Einwilligung lässt sich damit als Entscheidung in einem sozialen Dilemma oder Gefangenendilemma charakterisieren.[18] In diesem Modell möchten Menschen selbst über die Preisgabe von Informationen über sich selbst entscheiden. Individuell betrachtet ist eine Preisgabe von Informationen über sich selbst rational, sofern der Nutzen der Einwilligung deren Kosten überwiegt. Der Nutzen einer Person ist dabei höher, wenn nur sie Informationen über sich selbst preisgibt, andere Nutzerinnen und Nutzer aber keine Informationen über sich preisgeben, eine Einwilligung also verweigern. Denn wenn auch andere Nutzerinnen und Nutzer einwilligen, können mittels Datenaggregation über die Person auch Informationen generiert werden, die sie gerade nicht preisgeben wollte. In dieser Situation besteht ein Anreiz, auf den Selbstschutzmaßnahmen anderer – etwa der

16 von Lewinski, K. (2014), *Die Matrix des Datenschutzes*. Tübingen: Mohr Siebeck, S. 56.

17 MacCarthy, M. (2011). New Directions in Privacy: Disclosure, Unfairness and Externalities. *I/S: A Journal of Law and Policy for the Information Society, 6,* 425 ff.; Jernigan, C. & Mistree, B. F. T. (2009). Gaydar: Faceboook friendships expose sexual orientation. *First Monday, 14*. Abgerufen von http://www.firstmonday.dk/ojs/index.php/fm/article/view/2611/2302..

18 Dazu ausführlich Hermstrüwer, Y. (2016). *Informationelle Selbstgefährdung*. Tübingen: Mohr Siebeck, S. 165–169; Fairfeld, J. & Engel, C. (2015). Privacy as a Public Good. *Duke Law Journal, 65,* 385, 397; mit einer anderen Definition des sozialen Dilemmas, aber einer im Ergebnis ähnlichen Kritik am Einwilligungsmodell Sunstein, C. R. (2015). *Choosing Not to Choose.* Oxford: Oxford University Press, S. 30; ähnlich Tene, O. & Polonetsky, J. (2013). Big Data for All: Privacy and User Control in the Age of Analytics. *Northwestern Journal of Technology & Intellectual Property, 11,* 239, 261–262.

Einwilligungsverweigerung – trittbrettzufahren.[19] Sofern alle Nutzerinnen und Nutzer diesem Anreiz folgen und sich rational verhalten, werden sie eine Einwilligung erteilen. Die Einwilligung ist spieltheoretisch die dominante Strategie. Dies führt allerdings dazu, dass in der Gesellschaft ein Maß an Privatheit produziert wird, das unterhalb des sozialen Optimums liegt.

Aus normativer Sicht deutet dies auf ein „liberales Datenschutzparadoxon" hin:[20] Die Rechtsordnung kann entweder die individuelle Einwilligungsfreiheit oder aber ein optimales Maß an Privatheit für die Gesellschaft sicherstellen, nicht aber beides zugleich. Ferner zeigt diese Analyse: Beschränkungen der Preisgabe oder Nutzung personenbezogener Daten müssen nicht zwingend paternalistischen Zwecken – dem Schutz vor sich selbst – dienen;[21] sie lassen sich auch mit der Bewältigung eines sozialen Dilemmas und damit eines Gemeinwohlbelangs begründen. Von dieser Warte lässt sich auch ein staatliches *Nudging* weniger als libertär-paternalistischer denn als gemeinwohlorientierter Eingriff konzeptionalisieren.

1.4 Diskriminierung und Erosionseffekte

Die prädiktive Analytik ist mit Sortierungs- und Selektionsprozessen verbunden, die Gewinner und Verlierer hervorbringen. Gerade in sog. Prinzipal-Agenten-Beziehungen, in denen der Prinzipal (beispielsweise eine Versicherung) bestimmte Eigenschaften des Agenten (beispielsweise des Versicherungsnehmers) nicht beobachten kann, erweist sich die ökonometrische Klassifikation als lukrativ und effizient.[22] Das Problem liegt dabei

---

19 Dazu allgemein Nalebuff, B. (1998). Prisoners' Dilemma. In P. K. Newman (Hrsg.), *The New Palgrave Dictionary of Economics and the Law* (Bd. 3, S. 89 ff.). New York: Palgrave Macmillan; Tuck, R. (2008). *Free Riding.* Cambridge: Harvard University Press, S. 19–29.

20 In Anlehnung an Sen, A. (1970). The Impossibility of a Paretian Liberal. *Journal of Political Economy, 78,* 152 ff.

21 Dazu ausführlicher Hermstrüwer, Y. (2017). Contracting Around Privacy: The (Behavioral) Law and Economics of Consent and Big Data. *Journal of Intellectual Property, Information Technology and Electronic Commerce Law, 8,* 9, 24–26.

22 Grundlegend Milgrom, P. R. (1981). Good News and Bad News: Representation Theorems and Applications. *Bell Journal of Economics, 12,* 380 ff.; Grossman, S. J. (1981). The Informational Role of Warranties and Private Disclosure About Product Quality. *Journal of Law and Economics, 24,* 461 ff.; Fishman, M. J. & Hagerty, K. M. (2003). Mandatory Versus Voluntary Disclosure in Markets with

nicht nur darin, dass aus Datensätzen auch unzutreffende Vorhersagen (falsch-positive oder falsch-negative) generiert werden können.[23]

Zum einen lassen sich mithilfe prädiktiver Analytik auch Informationen erzeugen, die mit verbotenen Unterscheidungsmerkmalen – etwa den in Art. 3 Abs. 3 GG und § 1 Allgemeines Gleichbehandlungsgesetz (AGG) genannten – signifikant korrelieren (Proxy-Variablen).[24] Dies birgt die Gefahr, dass Ungleichbehandlungen nur mittelbar und zufällig an verbotene Unterscheidungsmerkmale anknüpfen, bestehende Differenzierungsverbote unterlaufen und bestimmte soziale Gruppen systematisch anders behandelt werden.[25] Diese Gefahr ist besonders hoch, wenn Datensätze selbst aus verzerrten oder diskriminierenden Stichproben bestehen (*bias*), da Diskriminierungstendenzen dann verfestigt werden (*garbage in, garbage out*).

Zum anderen schaffen Diensteanbieter zunehmend Anreizsysteme zur Preisgabe personenbezogener Daten, indem monetäre Vergünstigungen als Gegenleistung für die Einwilligung gewährt werden.[26] Die Vorstellung, Privatheit realisiere sich durch die Verweigerung einer Einwilligung[27] oder gar durch die individuelle Preisgabe zur Erlangung eines geldwerten Vorteils[28], greift zu kurz. Denn diese Anreizsysteme können die Einwilligungsfreiheit von Personen mit negativ bewerteten Eigenschaften spürbar beschränken. Diese Beschränkungen werden nicht allein durch den mone-

---

Informed and Uninformed Customers. *Journal of Law, Economics, and Organization, 19,* 45 ff.; anwendungsbezogen Barocas, S. & Selbst, A. D. (2016). Big Data's Disparate Impact. *California Law Review, 104,* 671 ff.

23 Zum Problem unzureichender Datenqualität Hoeren, T. (2017). Big data and the legal framework for data quality. *International Journal of Law and Information Technology, 25,* 26, 31–37.

24 Crawford, K. & Schultz, J. (Fn. 14), 99–101; Hildebrandt, M. (2008). Profiles and Correlatable Humans. In N. Stehr & B. Weiler (Hrsg.), *Who Owns Knowledge? Knowledge and the Law* (S. 265, 269–271). New Brunswick: Routledge.

25 Barocas, S. & Selbst, A. D. (Fn. 22), 677–693; Crawford, K. & Schultz, J. (Fn. 14), 99–101.

26 S. den Vorschlag für eine Richtlinie des europäischen Parlaments und des Rates über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte, COM (2015) 634 final; ferner Metzger, A. (2016). Dienst gegen Daten: Ein synallagmatischer Vertrag. *Archiv für die civilistische Praxis, 216,* 817 ff.

27 Mayer-Schönberger, V. (2009). *Delete: The Virtue of Forgetting in the Digital Age*. Princeton: Princeton University Press, S. 128–134.

28 In diese Richtung wohl Klement, J. H. (2017). Öffentliches Interesse an Privatheit. *JuristenZeitung,* 161, 168.

tären Anreiz verursacht, den die Diensteanbieter setzen; sie werden durch strategischen Druck vermittelt, den die Nutzerinnen und Nutzer selbst erzeugen.

Doch wie kommt es zu diesem strategischen Einwilligungsdruck? Geldwerte Vorteile oder Vergünstigungen werden in der Regel für positiv bewertete Eigenschaften (beispielsweise sportliche Betätigung) gewährt.[29] In einem Pool von Personen mit unterschiedlichen Eigenschaften führt dies zunächst dazu, dass die Person mit den besten Eigenschaften den stärksten Einwilligungsanreiz hat. Gibt diese Person die sie betreffenden Informationen preis, schrumpft der Pool der durch Privatheit geschützten Personen. Die Person mit den zweitbesten Eigenschaften hat nunmehr den stärksten Einwilligungsanreiz. Nach der Logik sog. *Signaling*-Spiele wird sie einwilligen, um einen negativen Rückschluss auf ihre Eigenschaften zu vermeiden.[30] Dieser Erosionsprozess (*unraveling*) kann sich theoretisch fortsetzen, bis alle Personen eingewilligt haben.[31] Ähnlich wie in dem bereits erörterten sozialen Dilemma zeitigt die individuelle Einwilligung auch hier drittbelastende Wirkung, weil sie den Einwilligungsdruck für andere erhöht.

Dieser Erosionsprozess lässt sich empirisch belegen; er mündet jedoch nicht stets in einen vollständigen Verlust von Privatheit.[32] Zum einen können Diensteanbieter Schwellenwerte für Eigenschaften festlegen, für die keine Vergünstigung gewährt wird. Zum anderen können soziale Präferenzen den Erosionsprozess abmildern. Denn ein starker Datenschutz hat umverteilende Wirkung: Da Ungleichbehandlungen durch Diensteanbieter mangels Information ausgeschlossen sind, werden Personen mit negativ bewerteten Eigenschaften von Personen mit positiven Eigenschaften quersubventioniert. Personen mit ausgeprägten sozialen Präferenzen werden

---

29 Peppet, S. R. (2011). Unraveling Privacy: The Personal Prospectus and the Threat of a Full-Disclosure Future. *Northwestern University Law Review, 105,* 1153 ff.

30 Stigler, G. J. (1980). An Introduction to Privacy in Economics and Politics. *Journal of Legal Studies, 9,* 623 ff. Das Modell beruht auf der impliziten Annahme, dass der Datenverarbeiter Monopolist ist bzw. am Markt keine datenschutzfreundlichen Alternativen angeboten werden.

31 Baird, D. G., Gertner, R. & Picker, R. C. (1994). *Game Theory and the Law*. Cambridge: Harvard University Press, S. 90.

32 Benndorf, V., Kübler, D. & Normann, H.-T. (2015). Privacy concerns, voluntary disclosure of information, and unraveling: An experiment. *European Economic Review, 75,* 43, 51–52.

daher tendenziell auch ein höheres Datenschutzniveau befürworten und eine Einwilligung verweigern.

Auf eine solche prosoziale Haltung kann und muss die Rechtsordnung sich nicht verlassen, insbesondere dann, wenn Umverteilungsbelange nicht durch andere Instrumente berücksichtigt werden (beispielsweise im Steuersystem oder in den sozialen Sicherungssystemen). Zu berücksichtigen ist allerdings, dass eine einseitige Nutzung prädiktiver Testergebnisse durch die Nutzerinnen und Nutzer ohne Verifikationsmöglichkeit für die Diensteanbieter – etwa eine private Versicherung – die Gefahr adverser Selektion birgt: Kann die Versicherung mangels überprüfbarer Informationen nicht zwischen guten und schlechten Risiken unterscheiden, werden die guten Risiken aufgrund der stetig steigenden Versicherungsprämien vom Markt verdrängt.[33] Äußerstenfalls kommt es zum Zusammenbruch des Versicherungsmarktes.[34]

Diese Analyse zeigt, dass Beschränkungen der Einwilligungsfreiheit und Datennutzungsverbote sich nicht allein mit paternalistischen Zwecken, sondern auch mit dem Ziel des Schutzes anderer begründen lassen, dabei aber das Risiko eines Marktversagens berücksichtigen müssen.

1.5 Regelungsdesign und Abschreckungseffekte

Problematisch ist schließlich, inwiefern die Verarbeitung von Big Data Einschüchterungs- und Abschreckungseffekte (*chilling effects*) verursachen kann. Das Bundesverfassungsgericht (BVerfG) verweist (anders als etwa der *US Supreme Court*)[35] in nahezu allen Entscheidungen zum Datenschutz darauf, dass Unsicherheit über das Ob und Wie der Datenverarbeitung einen grundrechtsgefährdenden Druck zu Verhaltensanpassungen erzeugen kann.[36] Diese Abschreckungshypothese betrifft entsprechend der

33 Dazu Akerlof, G. A. (1970). The Market for "Lemons": Quality Uncertainty and the Market Mechanism. *Quarterly Journal of Economics, 84,* 488 ff.

34 Rothschild, M. & Stiglitz, J. E. (1976). Equilibrium in Competitive Insurance Markets: An Essay on the Economics of Imperfect Information. *Quarterly Journal of Economics, 90,* 629 ff.

35 Vgl. *Laird v. Tatum,* 408 U.S. 1, 15 (1972); *Clapper v. Amnesty International,* 133 S. Ct. 1138, 1152, 2013.

36 Vgl. nur Entscheidungen des Bundesverfassungsgerichts (BVerfGE) 115, 320 (342) – Rasterfahndung; BVerfGE 120, 274 (311 ff.) – Online-Durchsuchung; BVerfGE 120, 378 (430) – Automatische Kennzeichenerfassung; für eine umfas-

Abwehrfunktion der Grundrechte nur die staatliche Datenverarbeitung. Dabei liegt die empirische Fundierung der Abschreckungshypothese nicht auf der Hand.[37] Gleichwohl ist je nach Kontext – Generalisierungen sind kaum möglich – eine konkrete Abschreckungsgefahr oder sogar eine tasächliche Verhaltensanpassung anzunehmen.[38] Empirische Befunde aus der jüngeren Zeit deuten etwa darauf hin, dass die Suche nach sensiblen Begriffen auf Wikipedia nach der Enthüllung umfassender staatlicher Überwachung durch den US-Nachrichtendienst *National Security Agency* (NSA) merklich zurückging.[39] Dies deutet darauf hin, dass nicht nur unerlaubtes, sondern auch erlaubtes oder gar erwünschtes Verhalten einem Abschreckungseffekt ausgesetzt sein kann.

Auch im Bereich der privaten Datenverarbeitung können solche Abschreckungseffekte eintreten, freilich ohne dass sich damit eine unmittelbare Grundrechtsgefährdung begründen ließe. So kann etwa das konkrete Design von Datenerhebungsregeln im privaten Bereich Abschreckungseffekten Vorschub leisten – und zwar unabhängig von einem drohenden staatlichen Eingriff. Empirische Evidenz deutet darauf hin, dass die sichtbare und aufmerksamkeitsaktivierende Gestaltung von Einwilligungsoptionen in erster Linie die Orientierung an sozialen Normen und die Konformität des Verhaltens steigert, nicht aber das Einwilligungsverhalten der Nutzerinnen und Nutzer beeinflusst.[40]

Der letztgenannte Befund ist zum einen für die Interpretation des sog. Paradoxons der Privatheit relevant. Dieses Paradoxon wird darin gesehen,

---

sende Analyse Staben, J. (2016). Der Abschreckungseffekt auf die Grundrechtsausübung. Tübingen: Mohr Siebeck.

37 Richards, N. (2013). The Dangers of Surveillance. *Harvard Law Review, 126,* 1934, 1964; Kendrick, L. (2013). Speech, Intent, and the Chilling Effect. *William & Mary Law Review, 54,* 1633, 1657; Kaminski, M. E. & Witnov, S. (2015). The Conforming Effect: First Amendment Implications of Surveillance, Beyond Chilling Speech. *University of Richmond Law Review, 49,* 465, 517.

38 Krit. zur Annahme von Einschüchterung und Anpassungsdruck Bull, H. P. (Fn. 3), 802–803. Systematische empirische Befunde oder Studien werden allerdings nicht angeführt.

39 Für eine detaillierte Studie Penney, J. W. (2016). Chilling Effects: Online Surveillance and Wikipedia Use. *Berkeley Technology Law Journal, 31,* 117 ff.; ähnlich Marthews, A. & Tucker, C. (2015). Government Surveillance and Internet Search Behavior. *Working Paper,* 1 ff.

40 Hermstrüwer, Y. & Dickert, S. (2017). Sharing is daring: An experiment on consent, chilling effects and a salient privacy nudge. *International Review of Law and Economics, 51,* 38 ff.

dass die meisten Menschen zwar bekunden, viel Wert auf Privatsphäre zu legen, zugleich aber äußerst freigiebig mit den sie betreffenden Informationen umgehen.[41] Wie der Befund zeigt, muss sich die Wertschätzung für Privatsphäre jedoch nicht unbedingt in einer höheren monetären Bewertung personenbezogener Daten niederschlagen; sie kann auch eine Präferenz für abweichendes Verhalten und Freiheit von Konformitätsdruck beschreiben. Aus der geringen Bewertung von Daten lässt sich also nicht auf die fehlende Notwendigkeit einer Regulierung von Datenflüssen schließen. Zum anderen zeigt der Befund, dass Informationspflichten und das Design von Einwilligungsoptionen bisweilen gerade diejenigen Verhaltensweisen bewirken, die sie zu vermeiden suchen. Zweck von sichtbaren Einwilligungsoptionen ist schließlich die Befähigung zu besser informierten und freiwilligen Entscheidungen über die Datenpreisgabe. Gerade nicht bezweckt wird die Abschreckung abweichenden, aber rechtlich zulässigen Verhaltens. Die Steuerung von Einwilligungsentscheidungen ist daher nicht ohne Weiteres durch Regelungen zu erreichen, die – wie Informationspflichten – an den Prozess der Einwilligung selbst anknüpfen.

2. Regelungsansätze

Die klassische Schutzperspektive des Datenschutzrechts und dessen individualistische Konzeptionalisierung dürfen, ja müssen kritisch hinterfragt werden. Ein modernes „Datenrecht" muss neben der individuellen Schutzperspektive zunehmend auch Gemeinwohlbelange und die Gefahr von Marktversagen in den Blick nehmen. Dabei ist der Blick weniger auf die Technologie als solche denn auf den tatsächlichen Umgang mit ihr zu richten.

Die Normierung verschärfter Informationspflichten (Art. 13, 14 DSGVO) oder erhöhter Anforderungen an die Gestaltung von Einwilligungsoptionen ist ein möglicher Regelungsansatz, der das Risiko eines Marktversagens infolge von Informationsasymmetrien aber nur bedingt

41 Acquisti, A., Taylor, C. & Wagman, L. (2016). The Economics of Privacy. *Journal of Economic Literature, 54,* 442, 476–478; Norberg, P. A., Horne, D. R. & Horne, D. A. (2007). The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors. *Journal of Consumer Affairs, 41*, 100 ff.; Strandburg, K. (2005). Privacy, Rationality, and Temptation: A Theory of Willpower Norms. *Rutgers Law Review, 57,* 1235, 1264.

bändigen wird. Denn das klassische Regelungsmodell der Informationsbereitstellung durch Datenschutzerklärungen verursacht hohe Transaktionskosten (bzw. Lektüreaufwand), die eine effektive Beseitigung von Informationsasymmetrien erschweren.[42] Jüngere empirische Befunde deuten überdies darauf hin, dass selbst transparent gestaltete Informationen (beispielsweise warnende Boxen oder standardisierte Labels) kaum zur Informiertheit der Nutzerinnen und Nutzer beitragen und sich deshalb auch kaum auf das Einwilligungsverhalten auswirken.[43] In ähnlicher Weise wirken sich sprachlich konkret formulierte Datenschutzerklärungen nicht anders auf die Risikoeinschätzung aus als vage gehaltene Informationen.[44] Welche Regelungsansätze kann ein modernes Datenrecht dann überhaupt verfolgen?

Erstens ist eine sektorale Algorithmengenehmigung oder Algorithmenkontrolle denkbar.[45] Gegenstand einer solchen Kontrolle müssten die analysierten Datensätze selbst, die Prozesse der Algorithmen (einschließlich des Quellcodes), die Genauigkeit der Schlussfolgerungen sowie die einer Entscheidung zugrunde gelegten Kriterien sein.[46] Der Vergleich mit einem in größeren Zeitabständen prüfbaren körperlichen Gegenstand sollte gerade bei selbstlernenden Algorithmen nicht überspannt werden. Denkbar ist in diesem Zusammenhang aber die Schaffung von Institutionen zur unabhängigen Überprüfung von Algorithmen, etwa durch ein Algorithmenaudit oder eine „Algorithmenverbandsklage" zur Überwindung kollektiver Handlungsprobleme. Eine Erweiterung der bereits existierenden Datenschutzverbandsklage[47] erfordert allerdings in einem ersten Schritt klare normative Maßstäbe für den Einsatz von Algorithmen. Da selbstlernende Algorithmen adaptiver sind als menschengemachtes Recht, stellt sich die

---

42 McDonald, A. & Cranor, L. F. (2008). The Cost of Reading Privacy Policies. *I/S: A Journal of Law and Policy for the Information Society, 4,* 543 ff.; Bakos, Y., Marotta-Wurgler, F. & Trossen, D. R. (2014). Does Anyone Read the Fine Print? Consumer Attention to Standard-Form Contracts. *Journal of Legal Studies, 43,* 1 ff.

43 Ben-Shahar, O. & Chilton, A. (2016). Simplification of Privacy Disclosures: An Experimental Test. *Journal of Legal Studies, 45,* S. 41 ff.

44 Strahilevitz, L. J. & Kugler, M. B. (2016). Is Privacy Policy Language Irrelevant to Consumers? *Journal of Legal Studies, 45,* S. 69 ff.

45 Martini, M. (Fn. 7), 1488–1489.

46 Barocas, S. & Selbst, A. D. (Fn. 22), 677–693.

47 Dazu Halfmeier, A. (2016). Die neue Datenschutzverbandsklage. *Neue Juristische Wochenschrift,* 1126 ff.

Frage, ob die Normsetzung selbst künftig stärker durch Algorithmen begleitet werden kann und überhaupt soll.

Zweitens scheint eine Entscheidungsentlastung durch technische Einwilligungsassistenten sinnvoll, etwa durch sog. *personal information management services* (PIMS).[48] Diese technischen Assistenten könnten so gestaltet sein, dass die Nutzerinnen und Nutzer ihre Datenschutzpräferenzen eingeben und das Interface bei jeder Nutzung in einem automatisierten Verfahren prüft, ob die Datenschutzerklärung mit den eingegebenen Datenschutzpräferenzen übereinstimmt. Im Fall einer Diskrepanz müssten die Nutzerinnen und Nutzer eine spezifische Entscheidung darüber treffen, ob sie die von der Diskrepanz betroffene Datenverarbeitung freigeben möchten. Diese Systeme ließen sich auch mit lernenden Standardeinstellungen verbinden (*learning defaults*).[49] Eine Hürde besteht gegenwärtig darin, dass die DSGVO keine Anforderungen an die technische Formatierung von Datenschutzerklärungen und Veränderbarkeit von Standardeinstellungen stellt. Die Diensteanbieter haben überdies einen Anreiz, die entsprechenden Informationen und Kontrollhebel auf ihr Netzwerk zu verteilen, um informationelle Selbstbestimmungsentscheidungen zu erschweren. Übergangsweise erscheint daher eine flankierende Nutzung von Kurzinformationen in Seitenlänge (*One-Pager*) sinnvoll.[50]

Drittens scheint abweichend vom Omnibus-Ansatz der DSGVO (also einer flächendeckenden Regelung für alle Bereiche) eine sektoral differenzierte Regulierung nach dem klassischen deutschen Regelungsmodell[51] sinnvoll, insbesondere mit Blick auf die erörterten Erosionseffekte. In einigen Bereichen dürften die Einwilligungsfreiheit und Gleichheitsrechte –

---

48 Stiftung Datenschutz. (2017). *Neue Wege bei der Einwilligung im Datenschutz – technische, rechtliche und ökonomische Herausforderungen.* Abgerufen von https://stiftungdatenschutz.org/index.php?id=132..

49 Sunstein, C. R. (Fn. 18), S. 157–187; Sunstein, C. R. (2013). Deciding by Default. *University of Pennsylvania Law Review, 162,* 1, 48–56; Porat, A. & Strahilevitz, L. J. (2014). Personalizing Default Rules and Disclosure with Big Data. *Michigan Law Review, 112,* 1417 ff.

50 Dazu das Muster der vom Bundesministerium der Justiz und für Verbraucherschutz und IBM geleiteten Plattform „Verbraucherschutz in der digitalen Welt". Abgerufen von http://www.bmjv.de/DE/Themen/FokusThemen/OnePager/OnePager_node.html..

51 Eifert, M. (2017). Autonomie und Sozialität: Schwierigkeiten rechtlicher Konzeptionalisierung ihres Wechselspiels am Beispiel der informationellen Selbstbestimmung. In C. Bumke & A. Röthel (Hrsg.), *Autonomie im Recht* (S. 365, 382–383). Tübingen: Mohr Siebeck.

verstanden als soziale Grundrechte – nur durch Datennutzungsverbote angemessen gewährleistet werden. Art. 9 Abs. 1 DSGVO normiert ein solches Verbot für die Verarbeitung von Daten über die rassische und ethnische Herkunft, politische Meinungen, religiöse Überzeugungen oder die Gewerkschaftszugehörigkeit, aber auch von genetischen Daten, biometrischen Daten, Gesundheitsdaten oder Daten zur sexuellen Orientierung. Art. 9 Abs. 2 DSGVO erlaubt zwar eine Aufhebung dieses Verbots durch eine Einwilligung, belässt den Mitgliedstaaten aber einen Umsetzungsspielraum zur Einführung von Einwilligungsverboten. § 4a Abs. 3 BDSG normiert kein Verbot, sondern lediglich, dass sich eine Einwilligung ausdrücklich auf besondere Arten personenbezogener Daten i.S.v. § 3 Abs. 9 BDSG beziehen muss. Zur Vermeidung von Erosionseffekten scheint es jedoch angemessen, auch auf nationaler Ebene an sektoralen Verbotsregeln (beispielsweise wie in §§ 18, 19 Gendiagnostikgesetz [GenDG]) festzuhalten.

Viertens ist eine behutsame Neuinterpretation der Regeln zu *privacy by default*, Datenminimierung (Art. 5 Abs. 1c DSGVO) und Zweckbindung (Art. 5 Abs. 1b DSGVO) zu erwägen. Zu berücksichtigen wären dabei die Innovationspotentiale der Datenaggregation, vor allem aber die Anreize der Nutzerinnen und Nutzer zur Informationspreisgabe sowie die strategischen Anreize, die eine restriktive Datenschutzregulierung für die Datenverarbeiter schaffen kann. Strenge datenschutzrechtliche Anforderungen an die Einwilligung (beispielsweise ein strenges *Opt-in*-Erfordernis) können als Markteintrittsbarrieren für Nischendienstleister – also wettbewerbshemmend – wirken[52], sozial nützliche Formen prädiktiver Analytik erschweren[53] und einen Anreiz für noch aggressivere Datenerhebungspraktiken setzen[54]. Denkbar scheinen vor diesem Hintergrund eine Lockerung der Anforderungen an die *Datenerhebung*, etwa an die Zweckbestimmtheit bei der Einwilligung, und eine verschärfte Kontrolle der *Datennutzung*, soweit mit deren Hilfe den Einzelnen betreffende Entschei-

52 Campbell, J., Goldfarb, A. & Tucker, C. (2015). Privacy Regulation and Market Structure. *Journal of Economics & Management Strategy, 24*, 47–73.

53 Tene, O. & Polonetsky, J. (Fn. 18), 260–263.

54 Solove, D. J. (2013). Introduction: Privacy Self-Management and the Consent Dilemma. *Harvard Law Review, 126,* 1880, 1902.

dungen getroffen werden sollen.[55] Dies scheint auch insoweit angemessen, als die meisten und wohl größeren Risiken aus der nachgelagerten Verwendung und weniger aus der vorgelagerten Erhebung herrühren. Regulierer und Rechtsanwender sollten bei aller Vorsorgeorientierung Folgendes beherzigen: A priori schutzintensive Regeln zum Umgang mit Daten bergen nicht selten die Gefahr strategischer Gegenreaktionen, die sowohl dem Datenschutz als auch dem Wettbewerb schaden.

55 Krit. Cavoukian, A., Dix, A. & El Emam, K. (2014). *The Unintended Consequences of Privacy Paternalism.* Information and Privacy Commissioner, Ontario, Canada, S. 1, 3–10.