JOURNAL OF LAW, TECHNOLOGY & THE INTERNET • VOL. 12 • NO. 2 • 2020 – 2021

THE AMERICAN WAY—UNTIL MACHINE LEARNING ALGORITHM BEATS THE LAW?

Dr. Asress Adimi Gikay[*]

Algorithmic consumer credit scoring has caused anxiety among scholars and policy makers. After a significant legislative effort by the European Union, the General Data Protection Regulation (GDPR) that has provisions tailored to automated decision-making (ADM) was implemented. When the EU Commission and the US Department of Commerce negotiated for US organizations to whom data from EU data controller is transferred to comply with the key principles of EU Data Protection Law under the EU-US Privacy Shield (PS) Framework, the Department of Commerce refused to incorporate the GDPR principles governing ADM in the PS Framework. The EU Commission accepted this refusal reasoning that where US companies make automated decisions with respect to EU data subjects, such as in consumer credit risk scoring, there are laws in the US that protect the consumer from adverse decisions. This view contradicts recommendations for implementing GDPR-Inspired law in the US to tackle the challenges of automated consumer credit scoring.

This article argues that despite the differences in the approach to the regulation of automated consumer credit scoring in the EU and the US, consumers are similarly protected in both jurisdictions. Furthermore, US consumer credit laws have the necessary flexibility to ensure that adverse automated decisions are tackled effectively. This article, through analyzing statutes, cases, and empirical evidence, demonstrates that the seemingly comprehensive legal rules governing ADM in the GDPR do not make the EU consumers better off. In addition, the challenges presented by the increasing sophistication of Artificial Intelligence (AI), especially machine learning, place both the EU and the US legal regimes in a

[*] Lecturer in AI, Disruptive Innovation and Law, Brunel Law School (Brunel University London). PhD with Honor in Individual Person and Legal Protections, Sant' Anna School of Advanced Studies, Pisa (Italy), SJD (Summa Cum Laude) & LLM, CEU (Budapest/New York). Brunel University London, Kingston Lane, Uxbridge Middlesex UB8 3PH. Email: asress.gikay@brunel.ac.uk.

similar position as neither jurisdiction is equipped to respond to autonomous, unpredictable, and unexplainable algorithms making decisions.

While the EU's risk-based approach to AI regulation adopted by the Draft AI Regulation which also contains provisions on regulatory sandboxing is a significant improvement, it does not significantly change the rules regarding algorithmic consumer credit scoring. Nevertheless, this is the approach that regulation should primarily adopt for the future.

CONTENTS

The American Way—Until Machine Learning Algorithm Beats the Law?

1. INTRODUCTION

THE CONTEXT

Any financial institution that engages in the business of lending money in the European Union (EU) or the United States (US) has the right and obligation to ensure a thorough assessment of the borrower's capacity to repay the loan. In the aftermath of the global financial crisis of 2008, attributed in part to the subprime mortgage crisis,[1] the responsibility to assess consumer borrowers' ability to repay has been more standardized and strengthened in both jurisdictions.[2] In modern credit risk assessment processes, the likelihood of the borrower defaulting is evaluated through a statistical method using the consumer's credit data and is reduced to a specific number—the credit score.[3] Over the years, creditworthiness assessment has evolved from interview-based assessment and decisions made by loan officers,[4] to automated decision-making with minimal human intervention. These decisions are based on data collected from the consumer, but also much more unlikely sources such as social networks.[5] These automated decisions in financial services have attracted the attention of scholars, regulators, and consumer advocacy groups who are often concerned that by using algorithms and big data, financial institutions may circumvent legal regimes that protect consumers and other vulnerable groups. This is due to the financial institution's use of predictive analysis

[1] IMAD A. MOSSA, GOOD REGULATION, BAD REGULATION THE ANATOMY OF FINANCIAL REGULATION102 (2015*); see generally* Steven Schwarcz, *Keynote Address: Understanding the Subprime Financial Crisis*, 60S. C. L. REV. 549-571 (2009).

[2] In the EU, one of the important pieces of legislations that emerged after the 2008 financial crisis is Directive 2014/17/EU of the European Parliament and of the Council of 4 February 2014 on Credit Agreements for Consumers Relating to Residential Immovable Property and Amending Directives 2008/48/EC and 2013/36/EU and Regulation (EU) No 1093/2010, 2014 O.J. (L 60) 3 [hereinafter "Consumer Mortgage Directive"]. In the US, The Dodd Frank Act introduced the Ability-to- Repay/Qualified Mortgage Rule — Regulation Z, effective 1/10/2014. The Dodd Frank Act introduced the Ability-to- Repay/Qualified Mortgage Rule — Regulation Z, effective 1/10/2014. The Consumer Financial Protection Bureau has issued a final rule to implement this regulation that provides eight criteria to determine the consumer's ability to pay on a mortgage. *See* 12 C.F.R. § 1026 (2013).

[3] CONSUMER FIN. PROTECTION BUREAU, *What is a credit score*, https://www.consumerfinance.gov/ask-cfpb/what-is-a-credit- score-en-315/ (last updated June 8, 2017).

[4] Matthew A. Bruckner, *The Promise and Perils of Algorithmic Lenders Use of Big Data*, 93 CHI.-KENT L. REV.3, 11-12 (2018).

[5] Nate Cullerton, *Behavioral Credit Scoring*, 110 GEO L. J. 808, 815 (2013); *see also* Yanhao Wei et al., *Credit Scoring with Social Network Data*, 35 MARKETING SCI. 234-258 (2015).

that may bypass decision-making which is based on the objective assessment of the individual consumer's circumstances.[6]
In the EU, the most significant legal instrument governing automated consumer credit scoring is the General Data Protection Regulation (GDPR)[7] which contains a few provisions tailored to Automated Decision Making (ADM).[8] The GDPR has triggered a great deal of change in how businesses manage personal data not only for entities established in the EU but also non-EU entities with a business link to the EU.[9] While it is yet to be proven whether the GDPR provisions on ADM achieve their intended objective of protecting the consumer from potentially arbitrary and opaque algorithmic decisions, it has been touted as a model for the regulation of not only data privacy in general but also automated consumer credit scoring in the US.[10]

In 2016, the EU Commission and the US Department of Commerce implemented the EU-US Privacy Shield (PS) Framework, under which US-based organizations to whom EU-based data controllers transfer data self-certify[11] to comply with the key principles of the GDPR.[12] The final document of the EU-US PS Framework excluded the principles of GDPR on ADM.[13]
In the US, the most significant federal statutes pertinent to ADM are the Financial Services Modernization Act of 1999, commonly known as the Gramm-Leach-

[6] *See* Giovanni Comandè, *Regulating Algorithms Regulation? First Ethico-Legal Principles, Problems and Opportunities of Algorithms, in* 32 STUDIES IN BIG DATA 169, 174 (Tania Cerquitelli, Daniel Quercia& Frank Pasquale eds., 2017); *see also* Matthew Adam Bruckner, *supra* note 4, at 26.
[7] Regulation 2016/679, of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive, Directive 95/46/EC, 2016 O.J. (L 119) [hereinafter "GDPR"].
[8] *See id.* at recital 71; arts. 2, 14, 20, 21, 22.
[9] Cedric Ryngaert & Mistale Taylor, *The GDPR as Global Data Protection*, 114 AJIL UNBOUND 5, 9 (2020).
For extra-territorial application of the GDPR, *see* GDPR, art. 3.
[10] Vlad E. Hertza, *Fighting Unfair Classifications in Credit Reporting: Should the United States Adopt GDPR-Inspired Rights in Regulating Consumer Credit*, 93 N.Y.U. L. REV. 1707, 1712 (2018).
[11] Commission Implementing Decision 2016/1250, of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protection Provided by the EU-U.S. Privacy Shield, 2016 O.J. (L 207).
[12] The EU-US Privacy Shield decision was adopted on 12 July 2016 and the Privacy Shield framework became operational on 1 August 2016. *EU-US data transfers*, EUR. COMM'N, https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/eu-us-data-transfers_en (last visited March 13, 2012).
[13] *See infra* section 4.3.2(B)(i).

Bliley Act (GLBA),[14] the Fair Credit Reporting Act (FCRA) and the Equal Credit Opportunity Act (ECOA). [15] Despite the existence of these sector specific legislation the EU Commission found to be satisfactory, studies claim that automated credit scoring is inadequately regulated in the US.[16] This aligns with the overwhelming sentiment that the US is lagging behind in terms of protecting consumer privacy.[17] In fact, in a New York University Law Review article, Hertza called for GDPR- inspired reform of the legal regimes governing ADM in consumer credit reporting in the US.[18]

The enactment of the first comprehensive privacy law in California in 2018—the California Consumer Privacy Act (CCPA) [19] – also seems to be suggestive of the pressure being felt by lawmakers in addressing privacy concerns in the US. This article argues that while US privacy law in general may require reform, the US does not need specific rules for automated consumer credit scoring. The existing literature calling for reform in the US is based on flawed premises that (a) the US legal rules governing consumer credit are incapable of addressing technology-driven legal challenges, and (b) the GDPR provisions on ADM effectively protect the consumer. Neither assumption has been closely examined or validated based on empirical evidence and the actual enforcement cases.

THE KEY CLAIM

This article argues that despite the differences in the approach to regulation of ADM in consumer loan underwriting in the EU and the US, the two legal jurisdictions respond to the phenomenon in a fairly similar manner. This article

[14] Gramm-Leach-Bliley Act, Pub. L. No. 106-102,113 Stat. 1338 (1999).

[15] 15 U.S.C. § 1691-1691(f).

[16] Mikella Hurley & Julius Adebayo, *Credit Scoring in the Era of Big Data*, 18 YALE J. L.& TECH. 148 (2016); *see also* Hertza, *supra* note 10.

[17] *See* Kelsy Wroten, *Why is America So Far Behind Europe on Digital Privacy*, N. Y. TIMES (June 8, 2019), https://www nytimes.com/2019/06/08/opinion/sunday/privacy-congress-facebook-google.html; *see also* Thomas Holt, *Data Privacy Rules in the EU May Leave the US Behind,* THE CONVERSATION(Jan. 23, 2019),https://theconversation.com/data-privacy-rules-in-the-eu-may-leave-the-us-behind-110330.

[18] Hertza, *supra* note 10 (arguing for a General Data Protection Regulation-inspired law for consumer credit scoring in the US and claiming that the US Fair Credit Reporting Act and the Equal Credit Opportunities Act are not sufficient to address the challenges of alternative credit scoring. Although Hertza focuses on algorithmic credit scoring, he calls for an overarching reform of US data protection law).

[19] Cal. Civ. Code § 1798.100 (West 2020).

examines statutory and relevant enforcement cases including judicial decisions in both jurisdictions.

First, the article aims to provide a comprehensive comparative analysis of the two legal regimes with respect to automated consumer credit scoring. Second, it shows that contrary to the prevailing view, the lack of recently implemented legal regime governing ADM in the US does not mean that US consumers are worse off when compared to their EU counterparts. Third, the challenge presented by the increasing sophistication of Artificial Intelligence (AI), especially machine learning, puts both the EU and the US in the same regulatory and legal quandary as neither jurisdiction is equipped to respond to autonomous, unpredictable, and unexplainable algorithms making critical decisions.[20]

RAISON D'ÊTRE

There are three main reasons behind writing this article. First, there are theories for reform in the US inspired by the GDPR for the regulation of ADM in the consumer credit industry,[21] whose validity requires scrutiny. Existing literature portrays the GDPR as a good model for reform—a view that this articles questions. The theory is tested by analyzing the legal regimes in the two jurisdictions as well as enforcement cases (including judicial decisions) and empirical evidence on consumer behavior. In the two years since the GDPR has been implemented, no such work has been undertaken, despite academics not being shy about alluding to the superiority of the GDPR in regulating ADM.

[20] Maja Brkan & Grégory Bonnet, *Legal and Technical Feasibility of the GDPR's Quest for Explanation of Algorithmic Decisions: of Black Boxes, White Boxes and Fata Morgana*, 11 EUR. J. RISK REGULATION 19, 49 (2020).

[21] Pasquale argues: "Data protection rules like the GDPR effectively raise the cost of surveillance and algorithmic processing of people. They help re-channel technologies of algorithmic governance toward managing the natural world, rather than managing people." Frank Pasquale, *Data Nationalization in the Shadow of Social Credit Systems*, L. POL ECON. PROJECT (June 18, 2018), https://lpeblog.org/2018/06/18/data-nationalization-in-the- shadow-of-social-credit-systems/. In his testimony before the United States Senate Committee on the Banking, Housing, and Urban Affairs he asserted that policymakers "…should look to Europe's General Data Protection Regulation (GDPR), which provides several standards for algorithmic accountability." Frank Pasquale, Exploring the Fintech Landscape, Written Testimony before the United States Senate Committee on the Banking, Housing, and Urban Affairs (Sept. 12, 2017),https://www.banking.senate.gov/imo/media/doc/Pasquale%20Testimony%209-12-17.pdf; *see also* Hertza, supra note 10(arguing why the US should adopt GDPR-Inspired legal regime specifically for ADM in consumer credit risk assessment).

Second, current legal developments could potentially depict US data privacy law as completely inapt to cope with technological challenges. On July 16, 2020, the Court of Justice of the European Union (CJEU) struck down the EU Commission's decision which held that the US has a privacy legal regime that provides adequate protection to EU consumers — 'the Adequacy Decision'[22]—that has been valid since 2016.[23] Under this judgment, Facebook Ireland and, as a consequence of the judgment, other EU data controllers were prohibited from transferring data to the US under the Adequacy Decision.[24] This judgment is likely to amplify the sentiment that US data privacy law in general is weak. The court found the Adequacy Decision invalid only because data subjects whose data are transferred from the EU do not have the same level of protection due to lack of protective safeguard for consumer rights *vis-à-vis* public authorities.[25] These rights include access and enforceable rights, as well as channels for an effective remedy in the context of data processing by public authorities in pursuit of national security interest and law enforcement.[26] In other words, the prevalence of state surveillance under various legislations, such as the Foreign Intelligence Surveillance Act (FISA)[27] and Executive Order 12333,[28] enables public authorities to access data from private actors without sufficient safeguards indicating that the US does not provide adequate data protection to EU consumers.[29] In the aftermath of the ECJ judgment, confusions about how good a model the GDPR is for reforming data privacy law pertaining to ADM are likely to reign, whilst the specific reasoning of the court is likely to be neglected.

Third, the general contentment with the provisions of GDPR governing ADM has the effect of deterring further necessary works that must be done to revise the rules. This article cautions about the false sense of security that seems to be prevailing regarding the level of consumer protection which the GDPR can provide.

[22] Data Prot. Comm'r v. Facebook Ir. Ltd. and Maximillian Schrems, Case C-311/18, 2020 ECLI:EU:C:2020:559, ¶198 (July 16, 2020).

[23] Commission Implementing Decision 2016/1250.

[24] Data Prot. Comm'r v. Facebook Ir. Ltd. And Maximillian Schrems, Case C-311/18, at ¶¶197-201.

[25] *Id.* ¶¶165-168.

[26] *Id.* ¶¶115-140, 203.

[27] 50 U.S.C. §§ 1801-1885(c).

[28] Exec. Order No. 12,333, 46 Fed. Reg. 59,941 (Dec. 4, 1981).

[29] Data Prot. Comm'r v. Facebook Ir. Ltd. And Maximillian Schrems, Case C-311/18, at ¶192.

It is not within the purview of this article to show the extent and manner in which US data privacy law should be reformed.[30] But, it argues that the rules governing ADM in the consumer credit industry available under the GDPR should not cloud the judgment of policy makers regarding the GDPR's actual efficacy/inefficacy with respect to ADM.

STRUCTURE

The article is divided into 6 sections. Section 2 provides a brief overview of ADM in consumer credit risk assessment. In this section, a succinct differentiation is made between various related and fundamental concepts namely, Algorithm, ADM, AI, and machine learning. While this section shortly addresses divergent theories about the definition of AI, it does not take a position on what an AI is because settling the definitional controversy around AI requires a separate work. For this reason, the article prefers the term ADM that encompasses all algorithmic decisions that remove human intervention significantly from the process. Section 3 analyzes the opportunities and risks in automated consumer credit scoring. This section examines efficiency, impartiality, and financial inclusion as benefits of automated consumer credit scoring, and inaccuracy and bias/discrimination as the concomitant risks. Section 4 investigates effective consumer protection in the EU and the US, by examining privacy consent and transparency in automated consumer credit scoring. It will be demonstrated that the legal rules and recent enforcement in the US show that a tailor-made legal regime is not required to address consumer vulnerability. Section 5 addresses the unique challenges of machine learning that limit the effectiveness of legal rules and suggests a holistic approach to tackling the challenge that both jurisdictions should adopt moving forward. It examines risk-based approaches to the regulation with respect to machine learning credit scoring and regulatory sandboxing as potential solutions to be adopted. The article argues while these solutions are adopted by the EU' Draft AI Regulation (hereinafter

[30] For insights into reforming US Privacy law, *see* Paul M. Schwartz, *Preemption and Privacy*, 118 YALE L. J. 902 (2009) (arguing that it would be a mistake for the United States to enact a comprehensive or omnibus federal privacy law for the private sector that preempts sectoral privacy law); Alan Charles Raul, et al., , *United States*, *in* THE PRIVACY, DATA PROTECTION AND CYBERSECURITY L. REV., 3 99-421 (Alan Charles Raul ed., 2019) (tracking the shift in US privacy regulation); Lindsey Barret, *Confiding in Con Men: U.S. Privacy Law, the GDPR, and Information Fiduciaries*, 49 SEATTLE UNIV. L. REV. (2019) (comparing and contrasting the US and European models of privacy regulation).

"DAIR"),[31] the proposed regulation does not satisfactorily implement the notion of risk-based approach. Section 6 will provide concluding remarks.

2. AUTOMATED CONSUMER CREDIT SCORING

2.1. CONSUMER CREDIT SCORING

Consumer credit scoring is a method of quantifying the credit risk posed by a borrower using a statistical method to determine the effect of various credit data associated with the loan applicant on the applicant's probability of default.[32] Credit scoring has been through several stages of evolution. There was a time when a person's standing in the community sufficed to strike a loan deal with a bank.[33] Historically, credit reporting agencies used to conduct consumer credit risk assessment through information collated by hired professional reporters who profiled potential customers.[34] The more modern and standardized procedure involved assessing creditworthiness based on information supplied by the customer, obtained from other conventional sources and face-to-face interview where loan officers exercised a discretion in their final decision.[35] Today, credit scoring has changed significantly with the technological advancement.

2.2. AUTOMATED CONSUMER CREDIT SCORING—THE RISE OF ALGORITHMS

Already in the 1940s, the credit scoring system started to introduce semi-automation that relied largely on manual implementation of the scoring system.[36]

[31] *Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts*, COM (2021) 206 final, (21 April 2021), https://ec.europa.eu/transparency/regdoc/rep/1/2021/EN/COM-2021-206-F1-EN-MAIN-PART-1.PDF

[32] Bd. of Governors of the Fed. Reserve Sys., Report to the Congress on Credit Scoring and Its Effects on the Availability and Affordability of Credit at S-1 (August 2007), https://www.federalreserve.gov/boarddocs/rptcongress/creditscore/creditscore.pdf; Loretta J. Mester, *What is the Point of Credit* Scoring, BUS. REV. (1997), https://www.philadelphiafed.org/-/media/frbp/assets/economy/articles/business-review/1997/september-october/brso97lm.pdf.

[33] Cullerton, *supra* note 5, at 880.

[34] Rachel O'Dwyer, *Algorithms are making the same mistakes assessing credit scores that humans did a century ago*, QUARTZ (May 14, 2018), https://qz.com/1276781/algorithms-are-making-the-same-mistakes-assessing-credit-scores-that-humans-did-a-century-ago/.

[35] Kenneth G. Gunter, *Computerized Credit Scoring's Effect on the Lending Industry*, 4 N.C. BANKING INST. 443, 443 (2000).

[36] Peter L. McCorkell, *The Impact of Credit Scoring and Automated Underwriting on Credit Availability in* the IMPACT OF PUBLIC POLICY ON CONSUMER PROTECTION 209, 209-10 (Thomas A. Durkin & Michael E. Staten eds., 2002).

A more advanced automated credit scoring was introduced in the 1950s by Fair and Isaac who believed that algorithmic decisions would be better than decisions based on human judgment.[37] The FICO score which is widely used by financial institutions today (about 90 % of top lenders in the US),[38] have various ranges for different financial products with 300-850 (for mortgage) —a higher score representing less risk.[39]

When a financial institution conducts FICO score for a loan applicant, the computer algorithm analyzes the applicant's credit risk based on his/her credit history(history of borrowing and repayment including default) held at the top three credit bureaus—Experian, Equifax and TransUnion.[40] The FICO scoring proprietary algorithm looks for patterns in the credit report data "that historically have been associated with payment defaults among consumers" on the basis of which it assigns the credit score.[41] Thus, the algorithm collects collates, classifies, and analyses thousands of data points to make a predictive decision. The criteria for FICO scoring are by far generally comprehensible, if not fully explainable—payment history (35%), credit utilization ratio (30%) length of credit history (15%), credit mix (10%), and credit inquiries (10%).[42] While the legitimacy of these criteria could be questioned on its own, FICO scores could also be wrong if the credit information received from the credit bureaus is inaccurate.[43]

In the realm of automated consumer credit scoring, FICO scoring algorithms could be regarded as the tip of the iceberg. In the FinTech sector, there are several online credit facilities where a decision on the consumer's application is processed instantly using machine learning algorithms without the involvement

[37] *Id.*

[38] *What is a Credit Score?*,MYFICO,https://www.myfico.com/credit-education/credit-scores#:~:text=A%20credit%20score%20tells%20lenders,by%2090%25%20of%20top%20lenders.

[39] Constance Brinkley-Badgett, *What Does FICO Stand For? What is a FICO Score?,*CREDIT.COM (Apr. 11, 2018),https://www.credit.com/credit-scores/what-does-fico-stand-for-and-what-is-a-fico-credit-score/.

[40] Jim Akin, *What are the Different Credit Scoring Ranges*?, EXPERIAN(June 23, 2020), https://www.experian.com/blogs/ask-experian/infographic-what-are-the-different-scoring-ranges/#s4.

[41] *Id.*

[42] Jeanine Skowronski, *What Is a FICO Credit Report or FICO Score?,* CREDIT.COM (Apr. 15, 2019),https://www.credit.com/credit-reports/credit-bureau/fico-credit-report/.

[43] *How do I correct errors on my credit reports?,* MYFICO, https://www.myfico.com/credit-education/faq/credit-reports/correcting-credit-report-errors#:~:text=To%20correct%20errors%20on%20your,report%20can%20hurt%20your%20score.

of a human decision maker.[44] Online lenders may use an algorithm and thousands of pieces of information about its customers to make a decision on short term loans in seconds.[45] Once the consumer submits an application, the algorithm collects data about the consumer supplied by the consumer and mined from different online platforms[46] and scores the applicant and decides either to grant or deny the loan or classify which type of loan the applicant is qualified for. There are several companies that provide machine learning software for credit risk assessment including Zestfinance, Kreditech and SAS.[47] All of these automated credit scoring systems have algorithms in common.

2.2.1. From Algorithms to Machine Learning

The underlying tool of any automated consumer credit scoring is an algorithm. According to Coormen, a computer algorithm is "a set of steps to accomplish a task that is described precisely enough that a computer can run it."[48] While some algorithms perform relatively simpler tasks such as computing a simple mathematical equation, others that are referred to as AI engage in complex decision-making process that involve mimicking human intelligence ("certain operations of human brain").[49] Thus, automated consumer credit scoring could be conducted by machine learning—a sub-field of AI[50] that uses computers to learn patterns and rules from data and experience.[51]

But, there is no agreement as to when an algorithm becomes AI rather than a tool that fails to meet the threshold of intelligence, leading to a significant

[44] Anna Oleksyuk, *5 Uses of Machine Learning in Finance and FinTech*, MEDIUM (Jan. 25, 2019), https://medium.com/@annoleksyuk/5-uses-of-machine-learning-in-finance-and-fintech-9cf4a7530695.

[45] Parmy Olson, *The Algorithm That Beats Your Bank Manager*, FORBES (Mar. 15, 2015),https://www.forbes.com/sites/parmyolson/2011/03/15/the-algorithm-that-beats-your-bank-manager/#2cf600d81ae9.

[46] Cullerton *supra* note 5, at 809.

[47] Niccolo Mejia, *AI for Credit Scoring – An Overview of Startups and Innovation*, EMERJ (Jan. 18, 2019), https://emerj.com/ai-sector-overviews/ai-for-credit-scoring-an-overview-of-startups-and-innovation/.

[48] THOMAS H. COORMEN, ALGORITHMS UNLOCKED 1(2013).

[49] Lauri Donahue, Comment, *A Primer on Using Artificial Intelligence in the Legal Profession,* HARV. J. OF L. TECH. (January 3, 2018), https://jolt.law.harvard.edu/digest/a-primer-on-using-artificial-intelligence-in-the-legal-profession.

[50] PEDRO DOMINGOS, THE MASTER ALGORITHM: HOW THE QUEST FOR THE ULTIMATE LEARNING MACHINE WILL REMAKE OUR WORLD 8(2015).

[51] YADONG CUI, ARTIFICIAL INTELLIGENCE AND JUDICIAL MODERNIZATION 120 (2020) ("It can be said that machine learning is the study of 'learning algorithms,' which are essentially advanced versions of ordinary algorithms that make computer programs smarter by automatically discovering and learning data rules.").

difference of opinion regarding the definition of AI.[52] Since many of the FinTech companies employ machine learning algorithms and possibly deep learning techniques,[53] and the legal challenges posed by machines learning are peculiar, the distinction between algorithms and AI is useful to bear in mind.

Kaplan argues that it is difficult to answer the question "what is artificial intelligence" because (a) of the lack of commonly agreed upon definition of intelligence, and (b) so far, machine intelligence and human intelligence bear no resemblance, [54] the latter making it questionable to define AI with human intelligence as a point of reference. In Turner's words, "[d]efining AI can resemble chasing the horizon: as soon as you get to where it was, it has moved somewhere into the distance."[55] Despite the tricky nature of AI, Turner argues that defining it is required because it is crucial to have a "specific and workable definition when describing conducts and phenomena which are subject to regulation."[56]

Turner takes a functional approach to AI by describing it as "the ability of a non-natural entity to make choices by an evaluative process."[57] According to him, AI should possess the ability to make choice autonomously and to weigh various principles in making a decision.[58] Turner's definition takes a narrow approach to AI. Surden distinguishes between machine learning and knowledge representation and reasoning (KR),[59] as branches of AI. While machine learning AI has "[t]he ability to automatically learn and improve from experience without being explicitly programmed,"[60] KR (Rule Based AI) operates based on pre-determined set of parameters.[61] Rule-Based AI may also be referred to as deterministic algorithm

[52] *Automating Society: Taking Stock of Automated Decision-Making in the EU*, ALGORITHM WATCH (2019), https://algorithmwatch.org/en/automating-society-2019/ ("Artificial Intelligence is a fuzzily defined term that encompasses a wide range of controversial ideas and therefore is not very useful to address the issues at hand.").

[53] Deep learning is an advanced form of machine learning. *See* Ignacio N. Cofone, *Algorithmic Discrimination Is an Information Problem*, 70 HASTINGS L.J. 1389, 1395 (2019). Although deep learning is considered to present even a heightened legal challenge, this article does not make a distinction between deep learning and machine learning as making such distinction is not required for the narrative of the article.

[54] JERRY KAPLAN, ARTIFICIAL INTELLIGENCE: WHAT EVERYONE NEEDS TO KNOW 1 (2016).

[55] JACOB TURNER, ROBOT RULES: REGULATING ARTIFICIAL INTELLIGENCE 8 (2019).

[56] *Id.* at 8-9.

[57] *Id.* at 16.

[58] *Id.* at 16-17.

[59] Harry Surden, *Artificial Intelligence and Law: An Overview*, 35 GA. ST. U. L. REV. 1305, 1337 (2019).

[60] *Id.* at 1311, 1315; *see also* Cofone, *supra* note 53, at 1394.

[61] Surden, *supra* note 59, at 1316.

because this type of AI "produces on a given input the same results following the same computation steps."[62]

Turner argues that the Rule-Based AI, which he identifies as Symbolic Program (or Good Old AI or Classical AI) does not qualify as AI.[63] He believes that any intelligence reflected in this type of program which functions with decision tree (if X, then Y), is of the programmer and not of itself.[64] The rationale behind this approach is that no matter how well the algorithm performs a computation, because the program follows the same rule written by the software programmer, it does not possess intelligence different from what the designer has embodied in it.[65]

If Turner's approach is followed, a human being that otherwise is considered intelligent would fail to be treated as an intelligent being. First, a human being for the most part learns from its surrounding environment[66] and is to a certain degree programmed to reproduce certain outcomes. This fact by itself does not make a human being a non-intelligent entity. A fully grown adult that for some reason is unable to improve its emotional intelligence[67] but computes the most complex mathematical problems with exceptional speed does not cease to be an intelligent being because mathematics is learned from someone and there is no improvement in any other aspect of its intelligence.

To be fair, it is possible to provide equally convincing reasons in support of Turner's narrow approached to defining AI. Unsurprisingly, any given definition of AI is amenable to criticism from various angles which makes attempt to provide a universal definition futile. While intuitively, this is concerning from the perspective of framing legal policies and rules, some argue that the lack of universal definition has helped grow the field and allowed researchers, practitioners, and developers to be guided by a rough sense of direction.[68] In the same vein, this article

[62] A. Bockmayr and K. Reinert, *Concepts: Types of Algorithm*, DISCRETE MATH FOR BIOINFORMATICS WS 10/11(Oct. 18, 2010), http://www mi fu-berlin.de/wiki/pub/ABI/DiscretMathWS10/runtime.pdf.

[63] Turner, *supra* note 55, at 18.

[64] *Id.* at 19.

[65] *See id.* at 18.

[66] Elsbeth Stern, *Individual differences in the learning potential of human beings*, NPJ SCI. OF LEARNING, Jan. 12, 2017, at 1.

[67] "[A]n emotional, intelligence competency is an ability to recognize, understand, and use emotional information about oneself that leads to or causes effective or superior performance." Richard E. Boyatzis, *A behavioral approach to emotional Intelligence,* 28 J. OF MGMT DEV. 749, 757 (2009).

[68] Peter Stone et al., *Artificial Intelligence and Life in 2030*, ONE HUNDRED YEAR STUDY ON ARTIFICIAL INTELLIGENCE: REPORT OF THE 2015 STUDY PANEL, 1, 12 (Sept. 2016), http://ai100.stanford.edu/2016-report.

does not intend to settle the definitional controversy in AI. It rather takes a broader approach by employing a generic term automated consumer credit scoring (or ADM) that encompasses both symbolic programs and machine learning. The cursory review of the controversy surrounding the definition of AI is necessary only to highlight on the fact that machine learning being a branch of AI presents an unprecedented legal challenge.

Machine learning scoring could effortlessly combine and analyze data collected from the consumer, third parties (like data brokers), public platforms (like social networking sites), and financial institutions related to the scoring service providers (or the financial institution) through complex contractual relationships.[69] This gives the entity conducting the credit risk assessment a wide range of data points.[70] Second, with algorithms, the data collection and analysis could be conducted in a fraction of second.[71] Third, there could be higher propensity for inaccurate data to go undetected and the consequences of the inaccuracies would go unmitigated.[72] Finally, automated scoring could mask discriminatory practices that allow financial institutions to remove factors that are defined as illegal from their scoring criteria by using proxies such as zip codes.[73] Ultimately, while the algorithm removes human oversight and potentially distances humans from liability for decisions, it could foster decisions that may not accurately reflect the consumer's personal circumstance based on co-relations rather than causation.[74]

While determinist algorithmic scoring raises many concerns, machine learning presents heightened regulatory challenges.[75] The ability of the machine to learn from its experience and to update its decision independently of human

[69] McCorkell, *supra* note 36, at 812.

[70] Daniel Faggella, *Machine Learning for Underwriting and Credit Scoring - Current Possibilities*, EMERJ (Apr. 3, 2020),https://emerj.com/partner-content/machine-learning-underwriting-credit-scoring/ (last visited Mar. 14, 2021).

[71] Adam C. Uzialko, *How Businesses Are Collecting Data (And What They're Doing with It)*, BUS. NEWS DAILY (updated June 17, 2020), https://www.businessnewsdaily.com/10625-businesses-collecting-data html (last visited Mar. 14, 2021).

[72] Bruckner, *supra* note 4, at 52-54; Kristin Johnson, Frank Pasquale & Jennifer Chapman, *Artificial Intelligence, Machine Learning, and Bias in Finance: Toward Responsible Innovation*, 88 FORDHAM L. REV. 499, 510 (2019); Michael L. Rich, *Machine Learning, automated Suspicion Algorithms and the Fourth Amendment*, 164 U. PA. L. REV. 871, 925 (2016).

[73] McCorkell, *supra* note 36, at 828.

[74] Karen Yeung, Algorithmic *regulation: A critical interrogation*, 12 REG. & GOVERNANCE 505, 516 (2018).

[75] "The decision-making process is deterministic, meaning that each step can in theory be traced back to decisions made by a programmer no matter how numerous the stages." TURNER, *supra* note 55, at 18.

oversight causes a great concern for scholars, consumers and policy makers.[76] The dynamic interaction of algorithm with big data[77] and its ability to make biased and discriminatory decisions without the corresponding duty of explanation represents a new chapter in the algorithmic regulatory challenge.[78] No legal regime today, including the GDPR, is equipped to deal with complex machine learning decision systems.

3. THE OPPORTUNITIES AND CHALLENGES IN AUTOMATED CONSUMER CREDIT SCORING

3.1. THE ADVANTAGES OF AUTOMATED CONSUMER CREDIT SCORING

Despite the growing concern about algorithmic decisions, algorithms are becoming an integral part of financial services today. Automated consumer credit scoring could provide three major benefits—efficiency, impartiality, and financial inclusion.

3.1.1. EFFICIENCY

Automated consumer credit scoring is deemed to be efficient as it increases the ease of using multiple data points with low transaction cost and enhances potentially more accurate decisions by increasing the amount of data point used to assess the consumer's credit risk.[79] In addition to utilizing the so-called traditional credit data, such as "loan or credit limit information, debt repayment history, account status, "credit inquiries," and "public records relating to bankruptcies,"[80] automated (alternative credit scoring) exploits non-traditional credit data, including "[r]ental payments, [m]obile phone payments, [c]able TV payments, [b]ank account information, such as deposits, withdrawals or transfers, [and][s]mall dollar

[76] Joshua A. Kroll et al., *Accountable Algorithm*, 165 U. PA. L. REV. 633, 660(2017).

[77]JAMES R. KALYVAS & MICHAEL R. OVERLY, BIG DATA: A BUSINESS AND LEGAL GUIDE 1 (2015).

[78]*See generally* Solon Barocas & Andrew D. Selbst, *Big Data's Disparate Impact*, 104 CAL. L. REV. 671 (2017).

[79] Nikita Aggarwal, *Law and Autonomous Systems Series: Algorithmic Credit Scoring and the Regulation of Consumer Credit Markets*, OXFORD BUS. L. BLOG (Nov. 1, 2018), https://www.law.ox.ac.uk/business-law-blog/blog/2018/11/law-and-autonomous-systems-series-algorithmic-credit-scoring-and.

[80]*The State of Alternative Credit Data: How the Financial Services Industry is Adopting and Benefiting from These New Data Sources*, EXPERIAN 4 (2018), https://www.experian.com/assets/consumer-information/white-papers/alternative-credit-data-paper.pdf.

loans."[81] It may even use insights from social media[82] and other digital footprints.[83] Consequently, automated consumer credit scoring is efficient on two fronts.

Automated consumer credit scoring eases and reduces the cost of processing alternative data including "social media footprints, psychometrics, online behavior data, and telecommunications data, including top-up patterns (for prepaid customers), mobile money use, and even calling patterns and contacts."[84] From the lender's point of view, algorithms can reduce the cost of acquiring and processing information using human labor and the potential loss from granting a loan to a credit-unworthy consumer.[85]

By increasing the data point that can be used for scoring, automated scoring could increase accuracy and reduce the incidence of refusing loan to a creditworthy consumer.[86] It could in turn ensure that credit is distributed efficiently.[87] Although there is no conclusive evidence that consumers ultimately gain from the efficiency stemming from accurate automated consumer credit scoring,[88] what is indisputable is that automated consumer credit scoring gives lenders a speed advantage in loan processing and thus in the short-run reduces transaction cost.

[81] *Id.* at 5.

[82] U.S. DEP'T OF THE TREASURY, OPPORTUNITIES AND CHALLENGES IN ONLINE MARKETPLACE LENDING 20 (2016),https://www.treasury.gov/connect/blog/Documents/Opportunities_and_Challenges_in_Online_Marketplace_Lending_white_paper.pdf.

[83] *See generally* Tobias Berg et al., *On the Rise of FinTechs: Credit Scoring Using Digital Footprints*, 33 R. FIN. STUD. 2845-2897 (2020), https://academic.oup.com/rfs/article/33/7/2845/5568311.

[84] FINANCIAL INCLUSION, INFRASTRUCTURE AND ACCESS UNIT, DISRUPTIVE TECHNOLOGIES IN THE CREDIT INFORMATION SHARING INDUSTRY: DEVELOPMENTS AND IMPLICATIONS, FINTECH NOTE NO. 3, WORD BANK GROUP 19 (2019).

[85] Kenneth G. Gunter, *Computerized Credit Scoring's Effect on the Lending Industry*, 4 N.C. BANKING INST. 443, 449 (2000).

[86] Mikella Hurley & Julius Adebayo, *Credit Scoring in the Era of Big Data*, 18 YALE J.L. & TECH. 148, 155-156 (2016).

[87] Susan Wharton Gates, Vanessa Gail Perry & Peter M. Zorn, *Automated Underwriting in Mortgage Lending: Good News for the Underserved?* 13 HOUSING POL'Y DEBATE 369, 372-73 (2002) (discussing the relative accuracy of automated underwriting and whether it has increased flow of mortgage credit to underserved consumers).

[88] A report published by the Bank of International Settlement presents several findings where Fintech borrowers perform traditional banks in terms of providing loans to consumers with lower credit scores, the report does not explain under what terms the loans are offered. *See* Leonardo Gambacorta et al., *How do machine learning and non-traditional data affect credit scoring? New evidence from a Chinese fintech firm* 4 (BIS Working Paper No. 834, December 2019).

3.1.2. Impartiality—From Algorithmic Score to an Impartial Loan Officer

One of the potential advantages of algorithmic decisions is objectivity and neutrality. In theory algorithms should remove human bias from the decision-making both by using neutral data points and by ensuring that the decision based on such data points is not manipulated to advance or perpetuate human bias. Nevertheless, the existing literature show a great skepticism toward algorithmic neutrality arguing that facially neutral factors may be used as proxy for prohibited characteristics,[89] while human biases could be replicated or even amplified by seemingly neutral algorithms.[90] As a matter of principle, automated consumer credit scoring ensures that loan officers do not insert their biases or malice in the decision-making process.

On many occasions, automated consumer credit scores have proven to be an incontrovertible and impartial evidence in claims of discrimination against banks in the US. The large body of literature in this field, zealously wanting to ring an alarm bell about algorithmic bias and unfairness, ignore some of the instances in which consumers have used their algorithmic scores to prove discrimination by human loan officers.

In *United States vs Deposit Guaranty National Bank*, the defendant bank engaged in discriminatory lending practice where "loan officers had broad discretion to make override decisions, known as judgmental overrides, for credit-scored loan applications—that is, decisions to deny credit to applicants who scored at or above the stated cutoff score for loan approval (high side overrides) and to grant credit to applicants who scored below that cutoff score (low side overrides)."[91] According to the claim, African American loan applicants were three times more likely to be rejected compared to white applicants.[92] The court entered a settlement order which, among others requirements, required the defendant to

[89] Anya E.R. Prince & Daniel Schwarcz, *Proxy Discrimination in the Age of Artificial Intelligence and Big Data*, 105 IOWA L. REV. 1257, 1267 (2020).

[90] *See* Philip Hacker, *Teaching Fairness Artificial Intelligence: Existing and Novel Strategies against Algorithmic Discrimination under EU Law*, 55 COMMON MKT. L. REV. 1143, 1146 (2020); Johnson et al., *supra* note 72, at 506; Nicol Turner Lee et al, *Algorithmic bias detection and mitigation: Best practices and policies to reduce consumer harms*, BROOKINGS (May 22, 2019), https://www.brookings.edu/research/algorithmic-bias-detection-and-mitigation-best-practices-and-policies-to-reduce-consumer-harms/.

[91] United States v. Deposit Guaranty National Bank, No. 3:99CV670, Settlement at 2, (S.D. Miss. 1999), https://www.justice.gov/crt/housing-and-civil-enforcement-cases-documents-119 (internal quotations omitted).

[92] *Id.*

establish $3 million compensation trust fund for the victims of its discriminatory lending practices.[93]

Wells Fargo Bank similarly engaged in a discriminatory lending practice in mortgage loan underwriting by placing African American and Hispanic American borrowers into subprime loans, "with adverse terms and conditions such as high interest rates, excessive fees, pre-payment penalties, and unavoidable future payment hikes, when similarly qualified Non-Hispanic white . . . borrowers received prime loans."[94] The African American and Hispanic American plaintiffs in the dispute had, in some cases, higher credit score than White applicants.[95] Wells Fargo settled the case for $175 million.[96]

In 2016, the Consumer Financial Protection Bureau (CFPB) and the Department of Justice (DOJ) secured a settlement of $10.6 million for discriminatory lending through redlining from BancorpSouth.[97] The story is the same—BancorpSouth engaged in discriminatory mortgage loan practice by providing loans to Caucasian Americans with about a 622 credit score while denying to African-Americans with credit score of 625, and according to the allegation with higher income and better credit history.[98] To the author's best knowledge, there are no similar cases reported in the EU.

The list of cases in which algorithmic credit scores were used to assert claims of discrimination could be long.[99] The obvious implication of these cases is that automated credit scoring may indeed compel financial institutions to uphold impartial decision making in loan underwriting. Although things are more complex when machine learning techniques come into the picture, the evidence does show

[93] *Id.*at 4.

[94] United States v. Wells Fargo Bank, Case 1:12-cv-01150, Doc. 1 at 4 (D.D.C. July 12, 2012), https://www.justice.gov/sites/default/files/crt/legacy/2012/07/12/wellsfargocomp.pdf.

[95] *Id.*

[96] Press Release, Dep't of Justice, Justice Department Reaches Settlement with Wells Fargo Resulting in More Than $175 Million in Relief for Homeowners to Resolve Fair Lending Claims (July 12, 2012).

[97] Press Release, Dep't of Justice, Justice Department and Consumer Financial Protection Bureau Reach Settlement with BancorpSouth Bank to Resolve Allegations of Mortgage Lending Discrimination (June 29, 2016).

[98] Complaint at ¶ 101, U.S. and Consumer Fin. Prot. Bureau v. BacnoSouth, 1:16-cv-00118-GHD-DAS (N.D. Miss. 2016).

[99] For example, see the Complaint for the pending litigation in *The Fair Housing Center v. Liberty Bank*, No. 18-cv-1654 (D. Conn. Oct. 4, 2018), https://www.consumerfinancemonitor.com/wp-content/uploads/sites/14/2018/10/Connecticut-Fair-Housing-Center-Inc.-v.-Liberty-Bank-complaint.pdf.

that consumers are not always the losers when an impartial and untampered algorithm speaks.

3.1.3. Financial Inclusion

The third potential advantage of automated consumer credit scoring is financial inclusion. Limited amount of research shows that alternative credit scoring is financially inclusive, i.e., provides access to financial services to those that are considered unscorable, invisible or credit unworthy.[100]

The traditional credit scoring system, due to the limited amount of data points it utilizes, is considered exclusionary, which could lead to lack of access to financial services to millions of citizens.[101] The US CFPB estimated in 2015 that 11% of American consumers to be credit invisible.[102] According to a survey conducted by the Federal Deposit Insurance Corporation (FDIC) in 2017, about 8.4 million households representing roughly 20 million citizens (6 percent of the households) were unbanked.[103] Although the overall figure in the EU in 2017 is relatively lower at 3.6%, there is a non-negligible percentage of consumers with no access to financial services in different Member States.[104]

With a continuous change in demographics created by migration, the difference in income, and opportunity in access to financial services, the issue of credit scoring and financial inclusion is likely to become more pertinent. A study in access to financial services shows alarming level of discrimination based on ethnic origin in the financial industry in the EU Member States.[105] A group of researchers sent banking related inquires to 1,281 banks in seven EU Member states using emails with "domestic names" and "Arabic Names."[106] Their finding showed a lower response rate in investment and loan related inquires coming from

[100] Nick Henry & John Morris, Scaling Up Affordable Lending: Inclusive Credit Scoring 10-12 (2018).

[101] *Id.*at 12.

[102] Kenneth P. Brevoort, et al., Data Point: Credit Invisible 6 (2015).

[103] *See* Fed. Deposit Ins. Corp., The 2017 National Survey of Unbanked and Underbanked Households 1 (2017).

[104] The report published by the European Central Bank shows that in the year 2017, there were around 10% unbanked households in Italy and Slovakia and 25% of households in Greece reporting not to have any financial accounts. *See* Miguel Ampudia & Michael Ehrmann, *Financial Inclusion: What's it Worth?* 3, 7 (Eur. Cent. Bank, Working Paper No. 1990, 2017), https://www.ecb.europa.eu/pub/pdf/scpwps/ecbwp1990.en.pdf.

[105] Matthias Stefan, et al, Ethnical Discrimination in Europe: Field Evidence from the Finance Industry 1-7 (2018).

[106] *Id.* at 1.

'immigrants' was a result of discrimination.[107] In a similar study conducted in Sweden that was published in 2016, focused on self-employed immigrants, established that self-employed European immigrants and non-European immigrants are more likely to be denied loans or be charged higher interest rates compared to native applicants, with the situation being worse for non-European immigrants.[108] Controlling for different variables that could justify differential treatment, the researchers concluded that the difference in terms of accessing loan could only be explained by discrimination.[109] In Spain, local banks have discriminated against vulnerable categories of consumers (mainly those with lower income, technological skills, or financial literacy).[110] Clearly, although not EU wide, these evidences shed a light on discrimination based on social or ethnic background in financial services in EU Member States.

Although tackling discrimination is one aspect of fostering it, financial inclusion requires financial institutions to actively and responsibly provide financial services that are appropriate to the needs of different consumers including the vulnerable ones.[111] How does automated consumer credit scoring play a part in this? Advocates argue that by increasing the type of data that is used to assess the consumer's creditworthiness, automated credit scoring allows financial institutions to embrace consumers that are otherwise ignored by financial institutions that use traditional (legacy) credit scoring.[112] In this regard, empirical evidence shows a mixed result. Lemieux and Jagtian, based on empirical studies, found that Fintech companies using alternative data provide consumer mortgage to underserved communities better than traditional banks.[113] By investigating practices of two peer-to-peer lending platforms using algorithms for credit risk assessment in the Netherlands, Buit concludes that FinTech lenders extend credit to borrowers who generally qualify for loan from conventional lenders.[114]

[107] *Id.*

[108] 69 LINA ALDÉN & MATS HAMMARSTEDT, DECRIMINATION IN THE CREDIT MARKET? ACCESS TO FINANCIAL CAPITAL AMONG SELF-EMPLOYED IMMIGRANTS 3-31 (2016).

[109] *Id.* at 5.

[110] Beatriz Fernandez-Olit et al., *Banks and Financial Discrimination: What Can Be Learnt from the Spanish Experience?*, 42 J. OF CONSUMER POL'Y 303, 319 (2019).

[111] Deepali Pant Joshi, Behavioral Insights Organization for Economic Co-operation and Development, Financial Inclusion and Financial Literacy (June 28, 2011), https://www.oecd.org/finance/financial-education/48303408.pdf.

[112] Majid Bazarbash, *FinTech in Financial Inclusion: Machine Learning Applications in Assessing Credit Risk* 2, (IMF, Working Paper No. 19/109, 2019).

[113] Catharine Lemieux & Julapa Jagtiani, *Fintech Lending: Financial Inclusion, Risk Pricing and Alternative Information* 34 (Fed. Reserve Bank of Phila., Working Paper No. 17-17, 2017).

[114] MARTHA ELISABETH BUIT, CONSUMER PEER-TO-PEER LENDING AND THE PROMISE OF ENHANCING THE ACCESS TO CREDIT: LESSONS FROM THE NETHERLANDS IN HUMAN RIGHTS,

3.1.4. AN OPEN QUESTION?

The three arguments presented in support of automated consumer credit scoring are efficiency, impartiality, and financial inclusion. Automated consumer credit scoring is recognized to enhance efficiency through speedy loan processing, reduced labor costs, and arguably accurate classification, and prediction.[115] Illustrating impartiality, several cases involving racial discrimination in the US also proved how algorithmic credit scores can be used to safeguard against discriminatory loan underwriting. So far, it is not clear whether automated credit scoring enhances financial inclusion as more empirical research is needed to validate the theory. Nonetheless, automated consumer credit scoring does not need to prove itself beneficial on all fronts. Algorithms replace a system where skilled operators manually compute credit scores by using various sets of data, which is considered cumbersome and costly.[116] At the very least, this efficiency benefit of automated consumer credit scoring should be assessed against the potential risks.

3.2. THE RISK OF AUTOMATED CONSUMER CREDIT SCORING

This section provides an in-depth analysis of the risk of automated consumer credit scoring. It focuses on two dominant risks (a) inaccuracy, and (b) bias and discrimination.

3.2.1. INACCURACY

A decision to grant or deny credit is critical both for the lender and the consumer. The lender has a legitimate interest in vetting the applicants to grant loan only to those who are creditworthy. The consumer's life may hinge on being granted credit. Financing education, a home, motor vehicle, and many other important aspects of the consumer's life in the modern world depend in many cases on accessing credit.[117] Those who are able to obtain credit have better chance of

CONSUMER PROTECTION AND VULNERABLE CONSUMERS (Cătălin Gabriel Stanescu & Asress Adimi Gikay, eds., Routledge, 2020) 188.

[115]Sarah Wheeler, *Disruptive mortgage automation technology from SoftWorks AI increases lender profitability: Trapeze solution delivers true touchless automation*, HOUSE WIRE (Mar. 12, 2019), https://www housingwire.com/articles/48405-disruptive-mortgage-automation-technology-from-softworks-ai-increases-lender-profitability/.

[116] Gunter, *supra* note 35, at 445.

[117]Doug Mattis, *The Meaning of Credit Access*, SELF (Mar. 15, 2016), https://www.self.inc/blog/the-meaning-of-credit-accesss#:~:text=It%20can%20mean%20the%20ability,credit%20should%20remain%20a%20possibility.

improving their personal lives whereas those who fail to meet the scoring criteria may end up going downhill, because one bad score may lead to a series of events that may further deteriorate the consumer's creditworthiness.[118] Hence, it is important that decisions are made with the utmost care and accurately reflect the circumstance of the consumer.

Inaccuracy is a great concern in credit scoring, not only for alternative credit scoring but also for traditional scoring system.[119] A 2013 FTC report revealed that 20% of consumers had at least one error on one of their three major credit reports, out of which 5% had an implication on their credit opportunity.[120] An investigative report in the UK consumer credit market published in 2014 showed that 38% of consumers who checked their credit report in the last two years had uncovered consequential errors in their credit report.[121] While it is alarming enough that errors in credit report are prevalent, it is even more concerning that correcting errors upon the consumer's request is difficult. Even if the consumer manages to do so, it happens only after the consumer has suffered a detriment. Sometimes, correcting an error in the consumer's data inserted and held by a credit bureau might take years and could lead to court litigation.[122]

Although big data-driven scoring is able to use an aggregate of different data, the data or the inference made based on it may be inaccurate because the data itself is obsolete or out of context.[123] The fact that the consumer has gone through personal insolvency a decade ago may be correct data, but it certainly is likely to be considered outdated and irrelevant to the current credit risk of the consumer at the time of application. If the consumer has gone through financial literacy programs and was able to meet his/her financial obligations successfully after the insolvency, an adverse decision based on the consumer's history of insolvency is

[118] *Id.*

[119] *See* FED. TRADE COMMISSION, REPORT TO CONGRESS UNDER SECTION 319 OF THE FAIR AND ACCURATE CREDIT TRANSACTIONS ACT OF 2003 (2012).

[120] Press Release, Fed. Trade Commission, In FTC Study, Five Percent of Consumers Had Errors on Their Credit Reports That Could Result in Less Favorable Terms for Loans (Feb. 11, 2013).

[121] David Mann, *More Than One In Three Credit Reports Contain Errors*, U SWITCH (Dec. 17, 2014), https://www.uswitch.com/media-centre/2014/12/more-than-one-in-three-credit-reports-contain-errors/?ref=affilinet~473347&utm_source=Affilinet&utm_medium=Affiliate&utm_campaign=473347.

[122] Tara Siegel Bernard, *An $18 Million Lesson in Handling Credit Report Errors*, N.Y. TIMES (Aug. 2, 203),https://www nytimes.com/2013/08/03/your-money/credit-scores/credit-bureaus-willing-to-tolerate-errors-experts-say.html.

[123] Federico Ferretti, *The Legal Framework of Consumer Credit Bureaus and Credit Scoring in the European Union: Pitfalls and Challenges — Overindebtedness, Responsible Lending, Market and Fundamental Rights*, 46 SUFFOLK U. L. REV. 791, 810 (2013).

likely to be inaccurate inference. For an algorithm, a history of bankruptcy perfectly indicates that the consumer is risky whereas a more nuanced approach with a touch of human judgment could lead to a different conclusion. Thus, accuracy, apart from incorrect data that may be supplied by a credit bureau, can emerge from an inaccurate inference being drawn from correct data.

3.2.2. BIAS AND DISCRIMINATION

Automated consumer credit scoring is not any different from judgmental credit scoring in the sense that norms of judgment including biases deeply entrenched in the society could affect the decision-making in both cases.[124] Stereotypical view of or blatant discriminations against a group could be implemented using algorithms that, could "replic[ate] and even amplify human biases."[125] Regarding machine learning, Hacker identifies two main causes of algorithmic biases: biased training and unequal ground truth.[126] Biased training occurs from incorrect handling of data, such as implicit bias in assigning value (output value) to certain data, or from biased selection of data for training.[127] It could also result from historically biased training data that issued to train the algorithm which is then applied to a particular group of the society which was not considered during the machine training phase.[128] According to Hacker, a bias

[124] For contrary evidence, see Adare et al., who assert that "[f]ace-to-face lenders reject Latinx and African-American applications approximately 6% more often than they reject similarly situated non-minority applicants for both purchase and refinance loans. In aggregate, our findings suggest that from 2009 to 2015, lenders rejected 0.74 to 1.3 million Latinx and African-American applications that would have been accepted except for discrimination. FinTech lenders, on the other hand, do not discriminate at all in the decision to reject or accept a minority loan application in our sample. This is consistent with algorithms acting in a profit-maximizing manner. Because our findings with respect to rejections must rely on proxies for certain variables utilized by the GSEs in approving loans, we note that these results are preliminary. But they nevertheless point toward the possibility that fully automated underwriting may reduce the incidence of discrimination in loan rejections." ADAIR MORSE ET AL., CONSUMER-LENDING DISCRIMINATION IN THE FINTECH ERA 7 (2019).

[125] Nicole Lee Turner et al., *Algorithmic Bias Detection and Mitigation: Best Practices and Polices to Reduce Consumer Harms*, BROOKINGS (May 22, 2019), https://www.brookings.edu/research/algorithmic-bias-detection-and-mitigation-best-practices-and-policies-to-reduce-consumer-harms/. For more information on human and machine biases, see generally Jon Kleinberg et al., *Human Decisions and Machine Predictions*, 133 Q. J. OF ECON. 237, 237-93 (2018).

[126] Hacker, *supra* note 90, at 1146.

[127] *Id*. at 1147.

[128] *Id.* at 1148 ("This is precisely what happened in a real case concerning applications to a UK medical school. For historical reasons, previously successful candidates happened to be predominantly white males; the model thus ranked white males higher when screening new candidates.").

resulting from unequal ground truth (the best approximation of reality) occurs when a trait that disparately impacts a particular group is used as a substitute variable in the decision making.[129] This constitutes what is referred to as proxy discrimination, which may be a result of conscious decision or implicit bias.[130]

While some indications of bias in automated credit scoring are reported,[131] today, there are not many documented cases of internationally discriminatory algorithms in the credit industry.[132] In 2009, American Express allegedly reduced the credit facility of Kevin Johnson, a Black American marketing and communication firm owner, although he had reportedly no bad credit history.[133] In its letter, the company stated that Johnson had shopped in a store which was patronized by people with poor payment history, which led to the decision to lower his credit facility.[134] Since the company did not state the specific store, "the only shopping trip [that Johnson could] determine was out of the ordinary was a

[129] *See id.* at 1148-49.

[130] *See id* ("... simply eliminating sensitive attributes from the model does not guarantee non-discrimination… redundant encoding makes it both more likely and harder to detect, as correlations multiply and discrimination hides behind seemingly neutral factors picked up by the algorithm.").

[131] *See* Will Knight, *Biased Algorithms Are Everywhere, and No One Seems to Care*, MIT TECHNOLOGY REVIEW (July 12, 2017), https://www.technologyreview.com/s/608248/biased-algorithms-are-everywhere-and-no-one-seems-to-care/ (noting the observation of an algorithmic bias author that "even those who know their algorithms are at a risk of bias are more interested in the bottom line than in rooting out bias."); *see also* Nicholas Diakopoulos, *What a Report from Germany Teaches Us About Investigating Algorithms,* COLUMBIA JOURNALISM REV. (Jan. 10, 2019), https://www.cjr.org/tow_center/investigating-algorithims-germany-schufa.php (discussing algorithmic bias of German Schufa score calculation and algorithmic accountability reporting as "an attempt to uncover the power wielded by algorithmic decision-making systems and shed light on their biases, mistakes, or misuse.").

[132] In this regard, there are findings that machine-learning-driven loan underwriting is less discriminatory and more inclusive. Researchers at the University of California Berkeley have concluded that minority groups in the US, i.e., African-Americans and Latinx, face less discrimination in FinTech mortgage lending than in face-to-face mortgage lending. Robert P. Bartlett, et al., *Consumer-Lending Discrimination in the FinTech Era* 2, 4 (UC Berkeley Pub. Law, Research Paper, 2019), https://papers.ssrn.com/sol3/papers.cfm?abstract id=3063448.

[133] *See* Ron Lieber, *American Express Kept a (Very) Watchful Eye on Charges*, N.Y. TIMES (Jan. 30, 2009), https://www.nytimes.com/2009/01/31/your-money/credit-and-debit-cards/31money.html; Carrie Teegardin, *Whatever Happened to Kevin D. Johnson, Part of Credit Card Debate*, ATLANTA JOURNAL-CONSTITUTION (Aug. 11, 2012), https://www.ajc.com/business/whatever-happened-kevin-johnson-part-credit-card-debate/cUneC23EknwhzHKe1nP4pI/.

[134] "Other customers who have used their card at establishments where you recently shopped have a poor repayment history with American Express." Teegardin, *supra* note 133.

September visit to a Wal-Mart in Southeast Atlanta. It was the first time he had used his American Express card at that store." [135] Kevin Johnson's story does not conclusively prove intentional discrimination. Moreover, publicly available evidence does not show whether the company took factors other than shopping pattern into account.

In 2019, the Finnish Data Protection Authority issued a decision against a credit company, Svea Ekonomi, for setting its algorithmic credit risk assessment to automatically reject credit applicants over a certain age (the applicant, Mr. Krister Linden, was age 83 by the relevant date). [136] This case shows a clear intent to discriminate against certain applicants based on age, executed by Svea Ekonomi, which is a prohibited practice in the EU. [137] Nevertheless, the practice is not pervasive and systemic in the credit industry.

3.2.3. The Risks of Automated Consumer Credit—A Recap

The preceding sections have examined the benefits and challenges of automated consumer credit scoring. Inaccuracy and bias/discrimination are identified as two important challenges. While literature proposes technical solutions to tackle them,[138] this article compares the solutions available in the EU and the US.

The US has not implemented specific law governing automated consumer credit scoring, and yet, there are legal rules responding to the phenomenon providing comparable consumer protection. With the aim of proving that the US

[135] Chris Cuomo, et al., '*GMA' Gets Answers: Some Credit Card Companies Financially Profiling Customers*, ABC NEWS (Jan. 28, 2009), https://abcnews.go.com/GMA/TheLaw/gma-answers-credit-card-companies-financially-profiling-customers/story?id=6747461.

[136] *Finnish DPA Ordered a Company to Change their Data Processing Practises*, GDPR REGISTER (May 22, 2019), https://www.gdprregister.eu/gdpr/data-processing-practises/.

[137] The EU Consumer Credit Directive, Recital 45 professes to incorporate the Charter of Fundamental Rights of the European Union. Directive 2008/48, of the European Parliament and of the Council of 23 April 2008 on Credit Agreements for Consumers and Repealing Council Directive 87/102/EEC, 2008 O.J. (L 133) 66; *See* Charter of Fundamental Rights of the European Union, Dec. 18, 2000, 2000 O.J. (C 364) 3 (including articles on protection of personal data, right to property, and non-discrimination). The applicability of EU non-discrimination law in the consumer credit market is well-established. *See generally* IRIS BENOHR, EU CONSUMER LAW AND HUMAN RIGHTS 130 (2013).

[138] *See generally* David Lehr & Paul Ohm, *Playing with the Data: What Legal Scholars Should Learn About Machine Learning*, 51 U. CAL. DAVIS L. REV. 653, 703-05 (2017) (arguing for addressing potential bias and discrimination at the state of training the algorithm through various techniques in addition to through rules that govern the machine learning decision at the stage of deployment).

has flexible consumer credit laws responding to the risk of automated consumer credit underwriting, comparable to the one in the EU, the ensuing section examines the most pertinent legal rules in the two jurisdictions.

4. Effective Consumer Protection in Automated Consumer Credit Scoring in the EU and the US

Legal literature has maintained that consumers are protected better in the EU in the field of automated credit scoring than their US counterparts.[139] Hertza provides an overview of the key provisions of the GDPR that he claims provide stronger consumer protection related to access to credit, emphasizing GDPR provisions governing consent and transparency. [140] Before examining the requirements of consent and transparency in the EU and the US, it is necessary to first analyze the GDPR's rules regarding the general prohibition of individual ADM and the exceptions thereof as consent and transparency requirements emerge from these rules.

4.1. GDPR's General Prohibition of Solely (Individual) ADM

The GDPR establishes that the data subject has the right not to be subjected solely to ADM that produces legal effects concerning them or similarly significantly affects them.[141] There are three exceptions to this prohibition of solely ADM. Pursuant to these exceptions, a solely ADM with legal effect or a similarly significant effect is permitted first, with the consent of the consumer, and second when the ADM is necessary for the formation or performance of a contract.[142] In both cases, the data controller must put in place measures to safeguard the data subjects' rights, freedoms and legitimate interests including the right to obtain human intervention, express their point of view, and contest the decision.[143] Third, a solely automated decision is permitted if authorized by EU law or law of a Member State to which the data controller is a subject.[144]

The GDPR's general prohibition of purely ADM including machine learning decisions presents three main challenges. First, if consumers are to be requested to provide consent for ADM regarding all matters (as consent is one of the requirements), it creates an unnecessary burden on businesses that should solicit

[139]Hertza, *supra* note 10, at 1730.
[140]*Id.* at 1729-41.
[141] GDPR at Art. 22(1).
[142] GDPR at Art. 22(1) & (2).
[143] GDPR at Art. 22(3).
[144] GDPR at Art. 22(2) (b).

consent even when the risk involved in applying ADM in question is appreciably low. The consent requirement has also other practical challenges examined in detail later (*see infra* § 4.2.1). Second, the GDPR does not provide a guideline on when a decision is necessary for the formation or performance of a contract, which may lead to uncertainty for businesses and consumers alike. Third, the possibility for allowing ADM if authorized by the Member States results in inconsistent implementation in different Member States.

According to a report published in 2019, only nine Member states used the derogation provision by allowing ADM without the consumer's consent in certain instances.[145] Although the other Member States may implement the derogation rule in the future,[146] the uncertainty this may cause to businesses operating in different Member States cannot be underestimated. This derogation rule can also be implemented to undermine consumer rights. The way in which this rule is implemented in Germany and the UK clearly demonstrates how a country may implement stringent or loose rules permitting ADM without the consumer's prior consent although not making the consumer better off in either case.

In Germany, solely ADM is allowed when consented to by the consumer or when necessary for the formation or performance of a contract as permitted under Article 22(2) (a) &(c) of the GDPR.[147] Germany implemented Article 22(2) (b) to allow ADM, i.e., without the consumer's consent only in case of insurance service contracts where the request of the individual (consumer) is granted.[148] This provision under German GDPR implementing law is interpreted to apply, among others, to cases of reimbursement and compensation under an insurance policy.[149] This approach limits solely ADM to two cases. The first one is pursuant to the insurance service contract where the outcome of the decision is positive (the request of the data subject was granted).[150] The second one is where the decision is "based on the application of binding rules of remuneration for therapeutic treatment and

[145]Access Now, *One year under the EU GDPR: An Implementation Progress Report- State of the Play, Analysis and Recommendations* 10 (May 2019), https://www.accessnow.org/cms/assets/uploads/2019/06/One-Year-Under-GDPR.pdf (noting that Germany "provides for sectorial exceptions, notably in the insurance context. Automated decisions can be used without individual consent and appeal mechanisms if the individual's request is granted (e.g., receives the full value of a claim).").

[146]*Id*. at 9.

[147] Gianclaudio Malgieri, *Automated decision-making in the EU Member States: The right to explanation and other "suitable safeguards" in the national legislations*, Computer Law & Security Review Volume 35(5), 1-26 (2019) at 7.

[148] Bundesdatenschutzgesetz vom 30. Juni 2017 (BGBl. I S. 2097).*translated in* https://www.gesetze hereafter" BDSD."

[149] *See* Gianclaudio Malgieri, *supra* note 147, at 7.

[150] BDSG at Art. 37(1) (1).

the data controller takes suitable measures in the event that the request is not granted in full, to safeguard the data subject's legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision."[151] In this case, the data controller has the duty to inform "the data subject of these rights no later than the notification indicating that the data subject's request will not be granted in full."[152]

The German approach that restricts solely ADM to insurance service contracts can certainly be regarded as a cautious approach that reduces the potential adverse effects of algorithmic decisions. However, it also unnecessarily restricts algorithmic decisions even in cases where the risk of harm could be appreciably low and could stifle innovation. There are countless scenarios in which a fully ADM may lead to a positive outcome for the data subject. Under the current German approach, individual ADM is not allowed even under those circumstances because of how Germany implemented the GDPR. To be fair, the exclusive focus on the implementation of the GDPR does not provide a complete picture of permitted cases of fully ADM in Germany. In the realm of administrative decisions, ADM is allowed in tax assessment in Germany based on specific statutes.[153] The scope of permitted cases of a solely automated decision can also be expanded by law as the very purpose of GDPR Article 22(2) (b) seems to achieve this— allowing Member States to evaluate sectors/cases in which they want to allow solely ADM and authorize it by law. Nevertheless, the choice of insurance service contracts, no matter what the justification, does not seem to be reasonable.

The UK approach is on the other extreme. In the UK, GDPR Article 22(2) (b) is implemented more liberally. Accordingly, significant fully automated decisions, meaning decisions that produce a legal effect or similarly significant effect on the data subject, which are not based on the consent of the data subject or necessary for the formation or performance of contract are allowed in any sector subject to *ex post facto* procedural safeguards.[154]

Pursuant to the relevant provision of the UK Data Protection Act (2018), a fully automated decision is permitted provided that, (a) the data controller, as soon as reasonably practicable, notifies the data subject in writing that a decision has

[151] BDSG at Art. 37(1) (2).

[152] *Id.* at Art. 37(1) (2).

[153]Marlies van Eck, *Automated administrative decisions and the law: Governments are using computers to make decisions in individual cases. How is this practice regulated?* (September 2018), https://automatedadministrativedecisionsandthelaw.wordpress.com/2018/09/03/automated-decisions-and-administrative-law-germany/

[154] UK Data Protection Act (2018) at Art. 14.

been taken based solely on automated processing.[155] "The data subject may, before the end of the period of 1 month beginning with receipt of the notification, request the data controller to—(i) reconsider the decision, or (ii) take a new decision that is not based solely on automated processing."[156]

Within a maximum of one month, subject to extension by two more months for a justifiable reason, the data controller must (a) consider the request, including any information provided by the data subject that is relevant to it, (b) comply with the request, and (c) by notice in writing inform the data subject of— (i) the steps taken to comply with the request, and (ii) the outcome of complying with the request.[157]

The provisions of the UK Data Protection Act implementing article 22(2) (b) of the GDPR in contrast with the sectoral approach in Germany,[158] adopts a more liberal approach, permitting fully automated decisions in all sectors subject to *ex post facto* procedural safeguards. While the German approach restricts automated decisions needlessly, the UK approach could potentially expose consumers and the public to arbitrary algorithmic decisions even in cases where the risk of harm is high. The *ex post facto* procedural safeguards may be abused by data controllers who may not necessarily disclose that the decision in question is made by an algorithm. If this happens, there is no way for the consumer to exercise the right to request for reconsideration of the decision.

In the UK, algorithmic decisions could be used in sensitive areas where the public has a strong interest in ensuring accuracy, fairness, and transparency. In 2019, legal action was instituted against the Home Office by the Joint Council for the Welfare of Immigrants, due to its use of an algorithm that allegedly discriminated against visa applicants based on race/nationality.[159] This algorithm was allegedly used to classify visa applicants according to risk as red, amber, and green.[160] The Home Office decided to scrap the algorithm in question in 2020.

[155] *Id.* at Art. 14(4) (a).
[156] *Id.* at Art. 14(4) (b).
[157] *Id.* at Art. 14(5).
[158] *See* Gianclaudio Malgieri, *supra* note 147, at 7.
[159] Henry McDonald, *'Home Office to scrap 'racist algorithm' for UK visa applicants',* The Guardian (August 4, 2020) https://www.theguardian.com/uk-news/2020/aug/04/home-office-to-scrap-racist-algorithm-for-uk-visa-applicants
[160] The Joint Council for Welfare of Immigrants, *'We won! Home Office to stop using racist visa algorithm'* (2020) https://www.jcwi.org.uk/news/we-won-home-office-to-stop-using-racist-visa-algorithm

Several local Councils use algorithms in decisions relating to welfare benefits.[161] It is questionable whether the existing procedural safeguards are sufficient to protect consumers from potentially arbitrary decisions made even in loan underwriting. At the very least, if the decision-makers comply with the duty to inform the consumer of the nature of the decision, the consumer might be able to contest the decision and secure human intervention, although the consumer might lose based on procedural error (failure to contest the decision in a month) or may carry a significant financial burden while challenging the decision including before a court.

The UK approach to the implementation of the GDPR clearly demonstrates that the EU's much commended legal regime does not necessarily protect the consumer from ADM as it can be implemented to allow solely ADM in a broad range of areas. A non-complying data controller could utilize ADM without the consent of the data controller and without establishing that the decision is necessary for the formation or performance of a contract under Article 14(UK), by putting in place procedural safeguards whether or not those procedural safeguards are genuinely meant to protect the consumer. In the case of machine learning decisions, the safeguards may not be adequately implemented in the first place (*see infra* § 5.1) Such as system cannot be proposed as a model system of law for consumer protection. In the proceeding sub-section, the requirements of consent and transparency that are regarded as instrumental in protecting the consumer are analyzed.

4.2. CONSENT AND CONSUMER PROTECTION

The GDPR is commended for giving data subjects control over their personal data,[162] in part through strict consent rules. Under the GDPR, the provision that consent should be secured for one or more specified reasons is one of six provisions, one of which must apply for the processing of personal data to be legal.[163] The GDPR requires that if consent is given in a "written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily

[161] Sarah Marsh, *'One in three councils using algorithms to make welfare decisions',* The Guardian (October 15, 2019) https://www.theguardian.com/society/2019/oct/15/councils-using-algorithms-make-welfare-decisions-benefits

[162] I van Ooijen & Helena U. Vrabec, *Does the GDPR Enhance Consumers' Control over Personal Data? An Analysis from a Behavioural Perspective*, 42 J. OF CONSUMER POL'Y91, 92-93, 103-04 (2019) (assessing the degree to which the GDPR gives consumers control over their data, finding that the GDPR does enhance individual control, but contains deficiencies that self-regulatory instruments may regulate).

[163] *See* 2016 O.J. (L 119) 36 (listing the six factors of lawful personal data processing under GDPR Article 6(1), one of which must apply).

accessible form, using clear and plain language."[164] More notably, ADM is permitted if necessary for the formation or performance of a contract, authorized by law or *consented to by the data subject.*[165] The consumer also has the right to withdraw their consent at any time.[166] In arguing that these consent rules enhance better consumer protection in the EU, Hertza states:

> While recognizing that there is no silver bullet to solve the difficult issues facing the consumer credit industry, this section identifies some ways in which the GDPR could inspire consumer credit legislation reforms. Big data and AI could increase the number of people that have access to credit. However, the discriminatory impact of the new technologies will outweigh the benefits, unless consumer credit regulation grants consumers access rights to the data used to determine their creditworthiness, and also grants consumers the right to deny access to certain personal data. The first steps required to achieve this goal are to extinguish the CRA versus non-CRA distinction up to a certain point, ***and to strengthen consent requirements*** and the right to refuse access to personal data.[167]

4.2.1. Fundamental Rights Approach to Data Protection in the EU and Consent

Data protection law in Europe is based on the conception that data protection is a fundamental right,[168] something the GDPR upholds.[169] Thus, the stringent consent requirements of the GDPR are crafted in this context. Nevertheless, the notion that stringent consent requirements would enhance consumer protection in algorithmic credit scoring is based on abstract analysis of the law. First, the EU consumers do not benefit from consent requirements as much

[164] 2016 O.J. (L 119) 37.

[165] Chris Jay Hoofnagle et al., *The European Union General Data Protection Regulation: What It Is and What It Means*, 28 INFO. & COMMC'N TECH. L. 65, 91 (2019).

[166] 2016 O.J. (L 119) 37.

[167] Hertza, *supra* note 10, at 1734 (*emphasis added*).

[168] *See* STEFANO RODOTÀ, REINVENTING DATA PROTECTION? 77, 80-81 (S. Gutwirth et al. eds., 2009); Paul M. Schwartz, *Global Data Privacy: The EU Way*, 94 N.Y. U. L. REV. 771, 773-74 (2019).

[169] Hoofnagle et al., *supra* note 165, at 79, 89.

as assumed or expected. Second, the fact that the consumer's data is obtained by a financial institution with consent has no causal link to how their data is processed in many cases.

Several factors contribute to the ineffectiveness of EU data protection consent rules. Research suggests that due to the sophistication of privacy policies and the complex systems of data collection coupled with the consumers' limited cognitive ability to process information, consumers do not have sufficient informational control.[170] First, data collection consent forms (terms and conditions) or privacy policies are adhesion contracts where the data subjects have no power to bargain.[171] Despite the GDPR requirement that consent be specific, informed, unambiguous, given freely, and entail affirmative action by the consumer, researchers argue that there are still challenges that weaken the consumers' control.[172] At the stage of collection, due to cognitive limitations, as well as the large volume of information, consumers are not able to properly filter and process information to make informed decisions.[173] Even if privacy agreements were negotiable, consumers would not have the time to adequately scrutinize them due to information overload and challenges to understanding technical jargon.[174]

A 2015 survey conducted by Eurobarometer (under the request of the European Commission, Directorate-General for Justice and Consumers) shows that the majority of respondents do not read privacy policies because they are too long, or because they are unclear or too difficult to understand, while a small percentage of the respondents simply assume that the law provides protection, or find it sufficient that there is a privacy policy on the website of the data controller.[175] This means that the majority of consumers could sign a privacy policy that might allow ADM without knowing it.

[170] Ooijen & Vrabec, *supra* note 162, at 96.

[171] *See* Michiel Rhoen, *Beyond Consent: Improving Data Protection Through Consumer Protection Law*, 5 INTERNET POL'Y REV. 3 (2016).

[172] Ooijen & Vrabec, *supra* note 162 at 100, 103-04.

[173] *Id.* at 94-95.

[174] *Id.* at 95 ("a Norwegian campaign-group established that it took almost 32 hours to read the terms and conditions of 33 representative smartphone apps . . . Note that this was solely the time it took to read the texts, let alone reflecting on the consequences of agreement to such policies.").

[175] *Special Eurobarometer 431: Data Protection Report*, at 87-88 (June 2015), http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_431_en.pdf.

One year after the GDPR was implemented, Eurobarometer published another survey in June 2019.[176] According to this survey conducted in all EU Member states, 37% of the participants responded that they do not read online privacy policies at all, while 47% and 13% read them partially and fully respectively.[177] Those who read privacy policies partially or do not read them at all indicated that privacy policies are too long (66%) unclear and difficult to understand (31%).[178] Some responded that it is sufficient for them to know that the entity they are dealing with has privacy policy(17%) while others believe that they would be protected by law anyway(15%) whereas others believe that websites will not honor privacy terms(10%).[179]

Privacy policies have gotten more complex as business methods become more sophisticated and businesses have become more aggressive with the realization of the economic value of personal data and the increased ability to collect it, process it, and make predicative analysis at a cheaper cost.[180] So, consumers accept terms and conditions for multiple online apps and transactions with no desire to waste their time reading complex non-negotiable privacy policies. Financial institutions can amend their terms and conditions unilaterally and send an electronic contract that the user has no meaningful control over. Those who read and understand can do little to change terms they do not like.

Recently, the CJEU handed down a judgment which specifies that internet sites cannot set cookies policies to require positive action for the consumer to opt-out of cookie based-tracking of the consumer behavior.[181] The judgment should address the rampant and continuous tracking of consumers' behavior for marketing purposes by requiring the consumer to untick pre-selected checkboxes.[182] When consumers that browse the internet are subject to surveillance by private companies who can access personal data and share it with third parties unless the consumer goes through pre-selected boxes to untick them, it is naïve to think that consent requirement is protecting consumers in the EU. Even after the judgment of the

[176] *Special Eurobarometer 487a: General Data Protection Regulation Report*, at 1 (June 2019), https://privacyblogfullservice.huntonwilliamsblogs.com/wp-content/uploads/sites/28/2019/06/ebs487a_en.pdf.

[177] *Id.*at 47.

[178] *Id.* at 51.

[179] *Id.*

[180] *See* Jennifer Shore & Jill Steinman, *Did you really agree to that? The evolution of Facebook's privacy,* TECH. SCI., (Aug. 10, 2015), https://techscience.org/a/2015081102.

[181] *See* Case C-673/17, *Planet49*, 2019 EU:C:2019:801.

[182] *See* Klaus Wiedemann, *The ECJ's Decision in ''Planet49'' (Case C-673/17): A Cookie Monster or Much Ado About Nothing?,* 51 INT'L REV. INTELL. PROP. & COMP. L. 543, 544 (2020).

CJEU, the cookies practices have not changed in the EU based on the author's personal encounter with hundreds of websites on weekly basis.

Based on the Eurobarometer report and consumer behavior, as well business practice, it is fair to conclude that overwhelming majority of the consumers have no control over their data. The stringent consent requirement of the GDPR is nothing more than a procedural requirement that ignores substantive consideration of whether the consumer has real opportunity to bargain and change the privacy related clauses.[183] Thus scholars who provide a cursory overview of the GDPR's provisions without investigating the actual practice have the onus of proving how the consent requirement protects the consumer in automated consumer credit scoring.

4.2.2. Market Oriented Approach to Data Protection in the US and Notice and Choice

In the US, data privacy is treated as a good that is subject to trading in the market rather than a right that merits a constitutional protection.[184] Nevertheless, a consent requirement, although not consistent across states and sectors and admittedly softer, is not entirely lacking. Data Privacy law in the US is sectoral[185] and governed by a combination of federal and state laws. The sectoral nature of US data privacy law is also a key feature of privacy law at state levels. For instance, California has different privacy laws for different sectors that require consent (notice and choice) for data collection and sharing with third parties,[186] despite California implementing a new privacy act.[187]

US privacy law is different from its EU counterpart in its philosophical foundation which prioritizes innovation over protection of data privacy rights, narrow definition of privacy harm and lack of a single enforcement agency, to mention the most important facets.[188] In line with this, consent mechanism in the

[183] *See* Rhoen, *supra* note 171, at 6; *see also* STEPHEN WEATHERILL, EU CONSUMER LAW AND POLICY 85 (2d ed. 2013).
[184] *See* Paul M. Schwartz & Kark-Nikolaus Peifer, *Transatlantic Data Privacy Law*, 106 GEO. L.J. 117, 132 (2017).
[185] *See* Schwartz, *supra* note 30 at 903-04.
[186] *See* CAL. BUS. & PROF. CODE § 22575 (2006); CAL. FIN. CODE § 4050 (2012).
[187] The California Constitutional Privacy Act applies to businesses with gross annual revenue or more than $25 million or businesses that buy, receive or sell the personal information of 50,000 or more consumers, households or devices. Compared to the GDPR, this is an odd way of designing privacy law that excludes many actors that can engage in invasion and breach of consumer privacy. *See* CAL. CONS. PRIV. ACT §1798.140(d) (A) & (B).
[188] *See* Barret, *supra* note 30, at 1065-81.

US, more accurately referred to as notice and choice[189] is regarded as soft.[190] Companies generally provide notice to the consumer on take-it-or-leave-it basis[191] whereas on paper, drafting adhesive privacy policy is not allowed under the GDPR.

In the field of consumer financial services, consent requirement is relatively comprehensive in the US as well. The GLBA has provisions that require financial institutions to protect the confidentiality and security of consumers' data, and requires them to provide notice to the consumer if they wish to disclose information to a third party.[192] The GLBA applies to financial institutions that provide loan, investment and insurance services.[193] It imposes an obligation on financial institutions to provide notice about the type of non-public personal information collected about the consumer, the origin of such information, as well as affiliated and non-affiliated third parties with whom the information may be shared.[194] Financial institutions are also obliged to inform the consumer of their right to opt out of the personal data sharing with non-affiliated third parties through a reasonable method and in a reasonable time.[195] Another relevant federal statute that governs consent is the FCRA which applies to Credit Reporting Agencies. The FCRA notice rule allows the consumer to opt out of disclosure by credit reporting agencies of their personal data to third parties.[196]

One of the most significant US legal rules on data privacy is found in the FTC Act. Section 5 of the FTC Act gives the agency the power to institute enforcement actions for unfair and deceptive trade practices.[197] The FTC has used its authority under section 5 to sanction data controllers for misrepresenting their privacy policy including not honoring them or not disclosing the exact scope of collection of the consumers' data.[198]

[189] *See* Daniel J. Solove, *Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880 (2013).
[190] *Id.* at 1071.
[191] *Id.* at 1073.
[192] Gramm-Leach-Bliley Act, Pub. L. No. 106-102, §§ 501-505, 113 Stat. 1338 (1999).
[193] *See* 15 U.S.C. § 6809(3) (2012).
[194] *See How to Comply with the Privacy of Consumer Financial Information Rule of the Gramm-Leach-Bliley Act*, FED. TRADE COMM'N 7, (2000), https://www ftc.gov/tips-advice/business-center/guidance/how-comply-privacy-consumer-financial-information-rule-gramm.
[195] *Id.* at 9.
[196] *See Fair Credit Reporting Act*, FED. DEP. INS. CO., (2015), https://www.fdic.gov/regulations/compliance/manual/8/viii-6.1.pdf.
[197] 15 U.S.C. § 45(a) (1) & (2). With respect to banks and financial institutions, this provision is enforced by other supervisory authorities including the Office of Currencies and Comptrollers.
[198] *See* FED. TRADE COMM'N, *Consent Order in the Matter of My Space LLC*, *File No. 102 3058*, 3 (2012), https://www ftc.gov/sites/default/files/documents/cases/2012/05/120508myspaceorder.p

The review of privacy notice rules in the US leads to three main conclusions. First, although the US notice system is critiqued for leaving room for consumers to accept adhesive contracts, the system does give the consumer the right not to disclose their data, unless the specific purpose for data collection, processing, and sharing are disclosed. In this context, consumers need to consent to ADM for a specific purpose. Second, the default rule in various sectoral statutes is that the data controller may share the data with third parties unless the consumer decides to opt out. This makes the consent system weaker in the US than the EU.[199]

Overall, in the US, although the requirement of consent is certainly not as stringent as in the EU in dictating the manner of framing the consent form, the US does protect the consumer in the field of consumer credit scoring. Even if there were gaps in consent requirement, the GDPR does not serve as a benchmark because even under its umbrella, consumers only have the illusion of control over their personal data. Only a handful of consumers may prevent businesses from getting their data for purposes they do not approve of, and only a tiny minority might negotiate to change privacy policies (if at all). Finally, only a handful of consumers would be able to bring legal action for breach of their privacy rights.

Last but not the least, even if it were assumed that US financial institutions could make automated decisions with consent obtained through adhesion contracts, that does not allow them to make inaccurate or discriminatory decisions. They cannot refuse to provide explanation to the consumers *ex post facto*. There are multiple effective sanctions imposed on CRAs for inaccurate reporting in the US which clearly demonstrates that consent in data collection and sharing does not necessarily provide a blessing for all sorts of subsequent decisions.[200]

df; *see also* FED. TRADE COMM'N, *Agreement on Consent in the Matter of Searr Holding Management, File No. 082 3099* 4-5 (2009).

[199] OMRI BEN-SHAHAR & CARL E. SCHNEIDER, MORE THAN YOU WANTED TO KNOW: THE FAILURE OF MANDATED DISCLOSURE 10 (2014) ("Disclosure is a ritual to be endured: patients are "consented," borrowers sign their way through closings, smartphone users "accept" terms, and Internet users are informed of privacy policies through linked scrolls. How can we not alter the white noise of disclosure? Lawmakers then turn up the volume to get our attention, and we close our ears to the din. In short, mandated disclosure seems plausible only on logically reasonable but humanly false assumptions. When buying software online, how many people click to read the terms of sale, much less read them, much less try to understand them, and much less succeed?").

[200] *See* discussion *infra* section 4.2.2.

4.3 Transparency and Automated Consumer Credit Scoring

4.3.1. Theories of Transparency

Another facet of the regulation of algorithmic decision-making is transparency which is regarded as an important component of ensuring algorithmic accountability. This sub-section overviews various theories of transparency in ADM and analyzes the legal rules on transparency in the EU and the US.

The debate regarding the scope of transparency required in automated credit scoring or even its necessity at all is polarized.[201] The reason for demanding transparency in ADM is ensuring that the decision maker explains its decision-making system to the consumer, the public and is held accountable for adverse decisions.[202] Transparency enhances consumer confidence in the system and provides the basis for accountability.[203] Nevertheless, how much should decision maker disclose? Is it possible to explain algorithmic decision in all circumstances? On these questions, there are three main theories that may serve as a basis for methodical analysis of this issue: (1) the black box, (2) the disparate impact, and (3) the opacity theories.

This article argues that neither the GDPR, nor the relevant rules in the US promote an optimal level of consumer protection because of the problem of explainability in machine learning.

A. The Black Box Theory

The black box theory has been dominant in legal literature and merits a serious scrutiny due to its uncompromising demand for transparency. To the best of the author's knowledge, the theory is pioneered, or at least expounded by Frank Pasquale who describes an algorithmic decision as a system where the input and output is known but how one becomes the other is unknown and calls for transparency in the logic of algorithms.[204] To achieve transparency under this theory, the decision makers should disclose, not only the input data used for the decision but also the output as well as the decisions tree (the weighing process for

[201] In one camp, scholars call for complete transparency. *See generally* FRANK PASQUALE, BLACK BOX SOCIETY: THE SECRET ALGORITHMS THAT CONTROL MONEY AND INFORMATION 7 (2015). On the other extreme, some scholars consider opacity to be the guiding principle for automated decisions. *See* Kroll et al, *supra* note 76, at 664-713.

[202] *See generally* PASQUALE, *supra* note 201.

[203] *Id.*

[204] *See* PASQUALE, *supra* note 201, at 8; *see also* Danielle Keats Citron & Frank Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 WASH. L. REV. 1, 67 (2016).

various variables) that should provide a clear account of how the algorithm functions and eventually to ensure algorithmic accountability[205] as well as algorithm auditing,[206] and transparency (as an end in itself).[207]

The black box approach has at least three essential requirements. First, the existence of ADM must be disclosed to the consumer.[208] Second, disclosure in cases of actual decision give information regarding the input and output as well as the logic involved in getting one from the other.[209] Third, the default rule of trade secret law that protects proprietary algorithms should change from assumption of secrecy to expectation of people's right to know.[210]

The black box approach has many objectives. Among others, it aims to subject algorithms to scrutiny of consumers impacted by algorithmic decisions and to allow public authorities to oversee algorithms through testing and auditing.[211] The black box theory aims to enhance the maximum transparency possible, whether it can achieve its objective is questionable. To be sure, the legal system in the EU and the US is not prepared to force disclosure of computer source codes to the consumer, to public enforcement authorities and to the judiciary.[212] Neither is the default rule of secrecy for proprietary algorithms reversed in both jurisdictions. Opponents of this view also point out the impracticality of the approach for several reasons (*see infra* 4.2.1.B).

B. The Opacity Theory

The opacity school of thought, holding that transparency in algorithmic decision making is not necessary, argues that algorithmic fairness can be achieved

[205] *See* Kroll et al, *supra* note 76, at 664-713.

[206] Pauline T. Kim, *Auditing Algorithms for Discrimination*, 166 U. PENN. L. REV. 189, 197 (2017).

[207] *See* Tal Z. Zarsky, *Transparent Prediction*, 2013 U. ILL. L. REV. 1504-70 (2013); *see also* Citron & Pasquale, *supra* note 201, at 20; Frank Pasquale, *Restoring Transparency to Automated Authority*, 9 J. TELECOMM. & HIGH TECH. L. 235, 235-6 (2011); Edith Ramirez, *Keynote Address at the Technology Policy Institute Aspen Forum: Privacy Challenges in the Era of Big Data: A View from the Lifeguard's Chair,* FED. TRADE COMM'N 8 (Aug. 19, 2013) https://www.ftc.gov/sites/default/files/documents/public_statements/privacy-challenges-big-data-view-lifeguard%E2%80%99s-chair/130819bigdataaspen.pdf.

[208] *See* Citron & Pasquale, *supra* note 204.

[209] *See id.* at 26; Danielle Keats Citron, *Technological Due Process* 85 WASH. U. L. REV. 1249–1313 (2007); *see also* Kate Crawford & Jason Schultz, *Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms*, 55 B.C. L. REV. 93 (2014).

[210] *See* Citron & Pasquale, *supra* note 204, at 21.

[211] *Id.* at 26.

[212] Robert Post, *Encryption Source Code and the First Amendment*, 15 BERKELEY TECH. L. J.713 (2000).

without being fully legally transparent.[213] According to this view, full transparency is not useful on the grounds that it (a) could enable people "game the system",[214] (b) is impossible due to trade secret law protecting algorithms,[215] and (c) may not necessarily lead to the understanding of how the algorithm functions.[216] In the context of machine learning, the theory holds that full disclosure is unhelpful because with every query and dataset, the software updates its decision making, and hence the existing decision rules become outdated, thereby rendering the disclosed information purposeless.[217]

The opacity theory suggests procedural regularity in ADM can be achieved by technical tools of software testing conducted feasibly only by industry experts and possibly in a self-regulation setting. [218] The opacity theory emphatically advocates for secrecy in algorithmic decision-making.[219]

From the consumer's perspective, the technical tools of transparency suggested by the opacity theory do not enhance true transparency. One of the proposed cryptographic techniques of transparency is Zero-Knowledge Proof (ZKP) —"protocols that enable one entity (called the prover) to convince another entity (called the verifier) of the validity of a mathematical statement, without revealing anything beyond the assertion of the statement."[220] In its ideal function ZKP is supposed to ensure that the public knows that a decision is made according to a specific procedure and would have a specific outcome, and the decision maker

[213]Kroll et al., *supra* note 76, at 657-60; *see also* Zarsky, *supra* note 207, at 1504-70.

[214]Kroll et al., *supra* note 76, at 657-60; *see also* Christian Sandvig, et al, *Auditing Algorithms: Research Methods for Detecting Discrimination on Internet Platforms, Data and Discrimination: Converting Critical Concerns into Productive Inquiry*9 (2014), https://pdfs.semanticscholar.org/b722/7cbd34766655dea10d0437ab10df3a127396.pdf?_ga=2.76779484.892963938.1581377623-552105405.1575505643 ("A major problem is that the public interest disclosure of just algorithms might be likely to produce serious negative consequences. On many platforms the algorithm designers constantly operate a game of cat-and-mouse with those who would abuse or 'game' their algorithm. These adversaries may themselves be criminals (such as spammers or hackers) and aiding them could conceivably be a greater harm than detecting unfair discrimination in the platform itself.").

[215]*See* Rebecca Wexler, *Life, Liberty, and Trade Secrets: Intellectual Property in the Criminal Justice System*, 70 STANFORD L. REV.1344 (2018).

[216] Kroll et al., *supra* note 76, at 638; *see also* Deven R. Desai & Joshua A. Kroll, *Trust but Verify: A Guide to Algorithm and the Law*, 31 HARVARD J. L. & TECH. 1, 33-34 (2018).

[217] Kroll et al., *supra* note 76, at 660 ("Online machine learning systems update their decision rules after every query, meaning that any disclosure will be obsolete as soon as it is made.").

[218] *Id.* at 662-69.

[219]*Id.* at 662.

[220] Rafael Pass, *Alternative Variants of Zero-Knowledge Proofs* (2004) (Licentiate Thesis, Cornell Computer Science).

is supposed to demonstrate that information without revealing anything that is considered a secret.[221]

If the decision making is challenged before court, an oversight body can compel the decision maker to demonstrate that the decision complies with the commitment they made publicly.[222] To summarize, the opacity theory calls for a default secrecy rule with limited transparency, implemented in a form of self-certification. As conceded by the proponents themselves, many of the tools are expensive,[223] and none of them encourage the disclosure of the source code to the public without putting in place protective mechanisms to guard trade secrets.[224]

The opacity theory is flawed on several levels. Its key drawback is the excessive dependence on self-regulation where the regulated entities' words and commitments are to be taken for granted until a consumer challenges a given decision-making process, at which point it would be subjected to third-party scrutiny. This theory is only as good as what companies are willing to do to be transparent.

There is some evidence from regulatory history that self-regulation or self-certification is not effective model of regulation. Before the 2008 global financial crisis, one of the credit rating agencies, Moody's, was reported to have had an error in its rating model—leading to triple A rating for assets with higher default risk.[225] Rather than correcting the error and rating the asset accordingly, Moody's only adjusted its model to justify the previous mistaken rating.[226] Credit Rating Agencies came under the spotlight largely due to the magnitude of the financial crisis. It is difficult to understand why complex cryptographic commitments or other technical tools of transparency will not be used by credit scoring companies or financial institutions to make false claims until they are exposed due to a major failure.

[221] Kroll et al., *supra* note 76 at 668 (arguing that ZKP "allows decisionmakers to build audit logs, which can be verified by the public to confirm that the decisionmaker applied the appropriate policy to the correct input in order to reach the stated outcome, all without revealing the decision policy itself and without revealing private data that might be included in the input or outcome.").

[222] *Id.* at 668-69.

[223] *Id.* at 661.

[224] *Id.* at 672-73.

[225] Claire Hill, *Why Did Rating Agencies Do Such a Bad Job Rating Subprime Securities?*, 71 U. PITT. L. REV. 585, 592 (2010).

[226] *Id.* at 593.

C. The Disparate Impact Theory

The disparate impact theory assumes that full transparency is not necessary, while also rejecting opacity. Thus, it demands the disclosure of the input and output in the scoring system.[227] Chander argues that unlike what can be read in Pasquale's Black Box, the transparency in algorithm design, what is needed is transparency in output and input.[228] His argument is that in the mysterious functioning of algorithms, it is difficult to understand how a given input becomes an output, and serves as the basis of a decision, whereas it is possible to determine what inputs are used and what impacts they have.[229] He explains that by focusing on the input and output, disparate impact of the outcome can be judged, and that is the only factor that should be taken into account in deciding whether an algorithmic decision is discriminatory or has a disparate impact on a specific group of consumers.[230]

4.3.2. TRANSPARENCY—THE RULES IN THE EU AND THE US

There are appreciable differences in legislative framework and legal rules governing transparency in automated consumer credit scoring in the EU and US. In spite of that, the existing legal rules achieve similar results in both jurisdictions in concrete cases.

A. The EU Approach to Transparency

Under the GDPR, the data subject has "the right not to be subject to a decision based solely on automated processing, including profiling, which produces

[227] Anupam Chander, *The Racist Algorithm?* 1041, UC Davis Legal Studies Research Paper Series (Research Paper No. 498). *Cf, with* Talia Gillis, *False Dreams of Algorithmic Fairness: The Case of Credit Pricing,* at 2 (Nov. 1, 2019)
https://scholar harvard.edu/files/gillis/files/gillis_jmp_191101.pdf (objecting to the disparate impact theory); Zarsky, *supra* note 207, at 1563-1568 (proposing transparency as a partial solution to be implemented both at data collection, analysis and policy decision making level. His analysis focuses on government agencies and thus it does not necessarily fit the purpose of regulating credit scoring).

[228] Chander, *supra* note 227, at 1024.

[229] *Id.* at 1024 ("What we need instead is a transparency of inputs and results, which allows us to see that the algorithm is generating discriminatory impact. If we know that the results of an algorithm are systematically discriminatory, then we know enough to seek to redesign the algorithm or to distrust its results.").

[230] *Id.*

legal effects concerning him or her or similarly significantly affects him or her."[231] In cases where an automated decision is authorized it "should be subject to suitable safeguards, which should include specific information to the data subject and the right to obtain human intervention, to express his or her point of view, to obtain an explanation of the decision reached after such assessment and to challenge the decision."[232] In this context, the GDPR imposes a requirement of transparency at three stages — (a) stage of data collection, (b) during data processing/decision, and (c) post-data processing/decision.[233]

The consumer has the right to know of the existence of automated decisions and the anticipated consequences of such decisions at that stage of data collection.[234] Furthermore, they have the right to obtain information as to whether personal data about him/her is being processed, including the existence of automated processing, the logic involved, and the significance and envisaged consequence of such processing.[235] While the first right allows the consumer to refuse consenting to automated processing of data, the second right allows the data subject to withdraw consent.[236] Hence, these transparency requirements that the GDPR put in place have the consequence of ensuring that the data subject is informed of the possibility of ADM. Comandé and Malgieri describe this as an *ex-ante* right to notification.[237] A third stage at which transparency is required in the GDPR is post-automated decisions where the data subject has "the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision."[238]

[231] GDPR Art. 22. Paragraph 2 recognizes exception, namely automated processing when necessitated for entering into or performance of contract between the data subject and the data controller and when allowed by the union's law and based on the data subject's consent.
[232] *Id.* at recital 71.
[233] *Id.* at art. 12.
[234] *Id.* at art.13(2) (f). "In addition to the information referred to in paragraph 1, the controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing: the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject." *Id.* When personal data are not obtained from the data subject, the corresponding provisions of Art. 14(2) (g) applies.
[235] *Id.* at Art. 15(1) (h).
[236] *Id.*
[237] Gianclaudio Malgieri & Giovanni Comandé, *Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation*, 7 INT'L DATA PRIVACY L. 243, 245 (2017).
[238] GDPR at Art. 22(3).

In all three stages of the transparency requirements, it seems that the data subject has the right to explanation under the GDPR, which would include the right to get explanation of the logic involved in the ADM.[239] Whether the GDPR in fact gives the right to explanation is debated, with some scholars disputing the existence of such right due to, among others, its incorporation in recitals without being reiterated in any of operative provision of the GDPR.[240]

Recitals do not have autonomous binding force as they can only be used to interpret the operative provisions of the legislation consistent with the spirit of the legislation concerned.[241] The interpretive role that can be played by recital 71 which contains the right to explanation on *ex post facto* basis is explained by Comandé and Maglieri, who argue that recital 71(a) does not derogate from, nor amend article 22, rather it merely clarifies and supplements it, and thus when an automated decision is made under article 22, the right to explanation is exercisable.[242]

The argument in favor of the right to explanation can be countered only adopting a formalistic legal interpretation, which lacks support in jurisprudence of the CJEU.[243] First, the right to explanation of the logic involved exists at the stage of data collection and data access. There is no plausible explanation that same right does not exist when the consumer wishes to challenge the same decision once it is made. Furthermore, to argue that the right to explanation does not exist on an *ex post facto* basis effectively nullifies right to contest, as contestation presupposes explanation. Indeed, this line of understanding aligns with teleological interpretation of law dominantly adopted by the CJEU where the meaning of a rule is constructed in light to its purpose and the overall context.[244]

[239] *Id.* at recital 63. With respect to an *ex post facto* right to explanation, Art. 22 of the GDPR does not give the data subject the right to an explanation. *Id.* at recital 71.

[240] *See* Sandra Wachter, *Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation*, 7 INT'L DATA PRIVACY L.76 (2017).

[241] Malgieri and Comandé, *supra* note 237, at 254-55.

[242] *Id.* at 255.

[243] The dominant interpretive approach of the ECJ is teleological or purposive approach where the Court interprets a given provision in the light of the objective, purpose, and overall context of the law. *See* Kohen Lenaerts, *Interpretation, and the Court of Justice: A Basis for Comparative Reflection*, 41 INT'L LAWYER 1011, 1017 (2007).

[244] *Id.*; *see also* Giulio Itzcovich, *The Interpretation of Community Law by the European Court of Justice*, 10 GERMAN L. REV. 538, 552 (2009).

While the right to explanation exists under the GDPR, the challenge is lack of clear ideas regarding the logic involved in automated processing.[245] Although the GDPR seems to address the most problematic aspect—understanding how the algorithmic decision-making works—by requiring the disclosure of the "the logic involved in the automated processing," it is far from sufficient to deal with the challenge, as scholars still struggle to explain what exactly it requires.

Comandé and Malgieri identify two elements of the algorithmic decision-making process, namely the functionality (the logic of the algorithm), and the contextual implementation of the functionality (with significance and the consequence).[246] Interpreting the term logic as the architecture of the algorithm, meaning its functionality, "significance and envisaged consequences" as the implementation of the overall decision-making process, such as the purpose, impact and human involvement, Comandé and Malgieri propose legibility—transparency and comprehensibility in both aspects of the algorithm.[247] They also recognize that trade secret law may limit legibility but suggest that it does not result in total denial of disclosure of information (at least the ones that do not have an adverse effect on the right of the data controller).[248]

Trade secret protection is an important obstacle to transparency. While a complete account is not provided here, it is worth highlighting the limiting effect of trade secrets on algorithmic transparency. The GDPR grants the consumer the right to explanation while maintaining that such right may not be exercised to the detriment of trade secrets of businesses.[249] Despite the appearance of the trade secret in recital 63 of the GDPR,[250] the GDPR has no specific operative provision dedicated to reconciling the potential conflict between right explanation and the need to preserve trade secrets. The EU Trade Secret Directive acknowledges that trade secrets shall not affect fundamental rights, including the protection of personal data.[251] Neither legal regime is clear as to where the protection of fundamental rights ends, and trade secret protection begins or vice versa.[252]

[245] Lilian Edwards & Michael Veale, *Slave to Algorithm? Why a 'Right to Explanation' is probably not the Remedy You are Looking for*, 16 DUKE L. & TECH. REV., 19, 49 (2017); *see also* Lehr & Ohm, *supra* note 138, at 707-08.

[246]Malgieri &Comandé, *supra* note 237, at 258.

[247] *Id.* at 265.

[248]*Id.*

[249]GDPR at recital 63.

[250]*Id.*

[251]Council Directive 2016/943, recital 34, 2016 O.J. (L 157) 1, 7.

[252] Maja Brkean and Grégory Bonnet, *Legal and Technical Feasibility of the GDPR's Quest for Explanation of Algorithmic Decisions: of Black Boxes, White Boxes and Fata Morganas*, 11

In 2014, the German Federal Court of Justice, based on the now-repealed Data Protection Directive concluded that the data subject has the right to access all their personal data used in credit scoring, but has no right to access (a) how the scoring algorithm weighed various factors, and (b) how the reference groups used to arrive at a credit score were comprised.[253] This essentially means that the consumer has the right to access the inputs and the output, the latter as a natural consequence of the decision being handed to the consumer. Under the directive, the prevailing approach in Germany seems to be the disparate impact theory of transparency where it is sufficient for the consumer to access the input and the output without the need for disclosing the internal functioning of the algorithm. As shown later, this is no different than what can be achieved using the provisions of the FCRA in the US.[254] One caveat to be added is that the German Court decision is based on the Data Protection Directive, not under the GDPR.[255] Nevertheless, the wordings of the recitals in the two legal instruments on the role of trade secret in limiting disclosure are identical.[256]

In the unchartered territory of machine learning, the GDPR's provisions on the right to explanation are as helpless as any other old legal rule. The challenges machine learning presents are multifaceted. Machine learning decisions could be opaque to the consumers, to the financial institution, and even to the algorithmic software creators themselves. In exceptional cases where machine learning credit scoring is permitted (consented to, necessary for the formation or performance of contract)[257] it may be employed. The seemingly comprehensive transparency rules of the GDPR would serve no meaningful purpose in that case.

To conclude, the GDPR provisions on transparency are impracticable for two reasons. First, trade secret law may be invoked not to disclose the internal logic of the algorithm. So far, this has been the case under the previous data protection

EUROPEAN J. OF RISK REG. 18, 40 (2020) ("From a legal perspective, it therefore remains rather unclear which set of rules should take precedence in case of conflict of trade secrets with data subjects' rights."); *see also* Gianclaudio Malgieri, *Trade Secrets v Personal Data: a possible solution*, 6 INT. DATA PRIVACY L. 102 (2016) (presenting additional optimistic approaches to the relationship between transparency and trade secrets for algorithms).

[253] Hunton Andews Kurt, *Federal German Court Rules on Credit Scoring and Data Subject Access Rights*, HUNTON PRIV. BLOG (January 29, 2014) https://www.huntonprivacyblog.com/2014/01/29/federal-german-court-rules-credit-scoring-data-subject-access-rights/.

[254] *See infra* ii (The Fair Credit Reporting Act's Transparency Provisions).

[255] Kurt, *supra* note 253.

[256] Cf. GDPR at recital 63; Council Directive 95/46/EC, recital 41, 1995 O.J. L. 281, 31, 35 (1995).

[257] GDPR at art. 6(2) (a-c).

law, at least in Germany. Given that the provisions governing ADM remained the same under the GDPR, the likelihood that trade secret protection is invoked in a similar fashion is high. Second, in case of machine learning credit scoring, it may not actually be possible to disclose anything as the system can be a black box to all stakeholders. Therefore, any reform proposal that calls for emulating the GDPR regarding ADM does not take into consideration the practical obstacles that undermine transparency and effective consumer protection.

B. The US Approach to Transparency

In the US, there are no tailored legal regimes applicable to ADM including in consumer credit scoring. Automated consumer credit scoring is governed by the FCRA.[258] Before discussing the key transparency provisions of the FCRA, a brief overview of the EU-US PS framework which extends the key principles of EU data protection law to organizations operating in the US is useful as it underlines the different regulatory approaches to ADM prevailing in the two jurisdictions.

i. The EU-US Privacy Shield Framework

Due to the absence of comprehensive data protection law in the US, data controllers transferring data from the EU to US should ensure that they process the data by respecting the privacy rights of EU data subjects. The EU-US PS Framework was created to achieve this purpose.[259] Although the EU Commission's adequacy decision regarding the PS Framework was struck down by the CJEU on July 16, 2020,[260] its history and the manner in which it was structured provides an excellent insight into how US consumer credit law addresses ADM. Under the PS Framework, certain principles of the EU data protection law must be implemented by the US organizations that wish to comply with the framework based on self-certification.[261]

[258] 15 U.S.C. §§ 1681(g)(1)(B)(i-ii), 1681(a)(5)(D).

[259] The EU-US Privacy Shield decision was adopted on July 12, 2016 and the Privacy Shield framework became operational on August 1, 2016. *See EU-US Data Transfers,* EUROPA, https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/eu-us-data-transfers_en.

[260] *See* Data Prot. Comm'r v. Facebook Ir. Ltd. and Maximillian Schrems, Case C-311/18, n. 201 (July 16, 2020).

[261] Council Implementing Decision 2016/1250, recital 14, 2016 O.J.L. 207, 1, 3 (July 12, 2016), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.207.01.0001.01.ENG.

While the PS framework was not a complete extension of the EU data protection law to participating organizations, the key principles of the GDPR are restated and should be implemented.[262] Nevertheless, the Commission and the US Department of Commerce decided not to add any of the rules of the GDPR governing ADM in the PS framework.[263] According to the Commission's adequacy decision, ADM has limited application today and in areas where it occurs such as in consumer lending, the existing US legal regimes provide specific protections against adverse decisions.[264] The decision also indicated the need to closely monitor the area as ADM is an evolving phenomenon.[265] Finally, the decision anticipated a study to be conducted on ADM and to be presented as a part of the first and second annual review of the PS Framework.[266] The adequacy decision remained in effect after the second annual review.[267] Consequently, the PS Framework excludes automated data processing which means that US-based companies that self-certify to comply with PS Framework were not required to comply with the GDPR provisions governing ADM. The FCRA act remains the applicable legal regime in the US today.

ii. The Fair Credit Reporting Act's Transparency Provisions

The first rule under the FCRA that aims to enhance transparency allows the consumer to access its file from consumer reporting agencies.[268] Hence, "[e]very consumer reporting agency shall, upon request . . . clearly and accurately disclose to the consumer all information in the consumer's file at the time of the request."[269] The FCRA defines file broadly as "all of the information on the consumer recorded

[262] There are seven principles, each entailing their own legal obligations that organizations must comply with under the PS framework. These are the Notice Principle, the Data Integrity and Purpose Limitation Principle, the Choice Principle, the Security Principle, the Access Principle, the Recourse, Enforcement and Liability Principle, and the Accountability for Onward Transfer Principle. *Id.* at recitals 20–28.

[263] *Id.* at recital 25.

[264] *Id.*

[265] *Id.*

[266] *Id.*

[267] *See* Staff Working Document SWD (2018) 497 Final, accompanying document Rep.from the Comm'n to the Eur. Parliament and the Council, at 4-5, COM (2018) 860 final (Dec. 19, 2018).

[268] The term "consumer reporting agency" means "any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports." 15 U.S.C. § 1681a(f).

[269] 15 U.S.C. § 1681a(g).

and retained by a consumer reporting agency regardless of how the information is stored."[270] If the consumer requests only a credit file, the CRA has the obligation to inform the consumer that they have the right to request and obtain a credit score.[271] Additionally, the consumer has the right to obtain summary of their rights on a model form prepared by the CFPB.[272]

The CRA has the obligation not only to disclose a consumer file but also a credit score if requested by the consumer together with the statement that "the information and the credit score model may be different than the credit score that may be used by the lender."[273] Generally, lenders have no duty to provide credit score to consumers *ex ante.*[274] Nevertheless, lenders that take adverse action, have the obligation to provide the consumer's credit score along with name and address of the CRA that provided the information to the lender.[275] While the FCRA gives the consumer the right to dispute the accuracy of information held by the CRA,[276] it imposes several obligations on CRA, including obligations to take reasonable steps to ensure the maximum possible accuracy of consumer reports.[277]

Based on the overview of the FCRA rules on transparency, a few conclusions can be drawn. First, there is no prohibition of ADM in consumer credit risk assessment in the US. A fact-finding article published in 2018 revealed that "in the US, automation, as opposed to human decision-making, is generally viewed as less biased and a way to improve effectiveness, as well as a cost-saving measure."[278] The legal regime on automated credit scoring reflects this sentiment. Second, the consumers' right to information about credit report or credit score does not necessarily include the right to obtain how the given credit score is calculated. The consumer has the right to obtain their credit score along with the key factors used in the scoring.[279] Nevertheless, similarly to EU consumers, US consumers

[270] *Id.*

[271] *See* 15 U.S.C. §§ 1681 g(a)(6), g(f)(1).

[272] 15 U.S.C. § 1681g(c)(1).

[273] 15 U.S.C. § 1681g(f).

[274] 15 U.S.C. §1681g(f)(6).

[275] 15 U.S.C. §1681m(a)(3)(A).

[276] 15 U.S.C. §1681b(b)(3)(B)(IV).

[277] 15 U.S.C. § 1681e(b).

[278] Gabriela Bodea, et al., *Automated decision-making on the basis of personal data that has been transferred from the EU to companies certified under the EU-U.S. Privacy Shield: Fact-finding and assessment of safeguards provided by U.S. law* 22–23, (European Commission Final Report)(Directorate-General for Justice and Consumers)(October 2018).

[279] S*ee* 15 U.S.C. § 1681 g(f)(1)(C). 15 U.S.C. § 1681 g(f)(2)(B) defines the term "key factors" as "all relevant elements or reasons adversely affecting the credit score for the particular individual, listed in the order of their importance based on their effect on the credit score."

equally enjoy the right to legally challenge adverse decisions regardless of the limited information available.

There are multiples cases in the US involving ADM that led to massive fines. In 2018, the FTC imposed a large fine on Realpage (CRA) for inaccurate credit reporting.[280] Although the dispute involves credit report of potential tenants, the process, provides insight into how consumers use the US legal regime to confront ADM, including for consumer credit scoring.[281] In this case, Realpage conducted a criminal background check on rental applicants using an automated system.[282] Through name and birthdate of the applicant, the algorithm matches the applicant with available criminal records.[283] This software program wrongly attributed criminal records to certain applicants (e.g., finding matches between Anthony Jones 10/15/67 and Antony Jones 10/15/67).[284] Realpage was fined for deploying a defective algorithm.[285]

In a more pertinent case, in 2017 the CFPB fined Conduent LLC (formerly Xerox Business) $1.1 Million for inaccurate consumer credit reporting using an automated process.[286] As a third-party service provider, Conduent provided automated auto loan consumer credit reporting to lenders and credit reporting agencies.[287] The information provided by Conduent was used to determine whether the consumer qualified for loan or favorable loan terms.[288] The automated consumer credit information provided by Conduent contained errors of various categories in the files of over 1 million consumers, including a report of involuntary repossession of vehicles, or errors on other critical consumer information including account default related information.[289] Thus, Conduent used defective software to automate the credit reporting,[290] and was held accountable under the FCRA.

[280] *Texas Company Will Pay $3 million to Settle FTC Charges That it Failed to Meet Accuracy Requirements for its Tenant Screening Reports*, FED TRADE COMM'N (Oct. 16, 2018), https://www.ftc.gov/news-events/press-releases/2018/10/texas-company-will-pay-3-million-settle-ftc-charges-it-failed.

[281] *Id.*

[282] *Id.*

[283] *Id.*

[284] *See id.*

[285] *Id.*

[286] *CFPB Fines Xerox Business Services $1.1 Million for Incorrect Consumer Information Sent to Credit Reporting Agencies*, CONSUMER FIN. PROT. BUREAU (Nov. 20, 2017), https://www.consumerfinance.gov/about-us/newsroom/cfpb-fines-xerox-business-services-11-million-incorrect-consumer-information-sent-credit-reporting-agencies/.

[287] *In re* Conduent Business Servs. LLC., 2017 C.F.P.B. 0020 (consent order) (Nov. 17, 2017).

[288] *Id.*

[289] *Id.* at ¶ 10.

[290] *Id.* at ¶ 12 et seq.

iii. Oldy but Goody

The FTC and CFPB enforcement actions reveal that the existing legal rules are capable of addressing technology-based challenges. In the case of Conduent, even if it is a third party that provided consumer credit information, it is under obligation to provide accurate credit reporting.[291] In the case of Realpage, provisions of the FCRA have been applied to an automated criminal background check.[292] The two cases demonstrate that the FCRA is capable of protecting the consumer from adverse decisions, as much as the GDPR could, notwithstanding the fact that it was enacted without explicitly addressing ADM. Nevertheless, it is also likely that in more complex cases, the US consumer would be able to win a judicial battle by compelling the data controller to disclose the decision-making process under electronic discovery procedure.[293] Thus, despite the difference in the legal rules in the two jurisdictions, the outcomes of legal controversies are likely to be the same in both jurisdictions. Nevertheless, advanced machine learning credit scoring presents an elevated challenge that legal rules in both jurisdictions are ill-prepared to tackle.[294]

5. The Limits of the Law and the Future of Automated Consumer Credit Scoring Regulation

5.1. Machine Learning Consumer Credit Scoring—A Dead End

This article is a response to the prevailing view that consumers are more vulnerable in the US than in the EU in the sphere of algorithmic credit scoring. It has countered this view by examining the effectiveness of some of the legal rules that are perceived as useful tools to protecting the consumer including consent and transparency in the EU and demonstrated that US consumer credit law responds to ADM in consumer credit scoring in a comparable manner. But, the key arguments as well as the real cases used as illustration involved automated systems using the so-called classical AI, a computer program that follows pre-determined set of rules to produce an outcome. Automation can also be based on more advanced AI

[291] The respondent is defined as a service provider and thus is a covered entity under 12 U.S.C.S. § 5481(26) (2021).

[292] Realpage was defined as a Consumer Reporting Agency within the meaning of the FCRA 15 U.S.C. § 1681 a(f). It was found, among others, to be in violation of 15 U.S.C. § 1681e(b) which requires ensuring accuracy in consumer credit reporting.

[293] *See generally* Laura Hunt, Comment, *Trending: Proportionality in Electronic Discovery in Common Law Countries and the United States' Federal and State Courts*, 43 UNIV. BALTIMORE L. REV. 279, 288 (2014).

[294] *See infra* Section 5.

systems include computer programs that update themselves as they encounter more data.[295] This AI system known more loosely as machine learning could attain autonomy and have agency (the ability to evaluate principles and make choices).[296] Thus, while rule-based AI is fairly controlled by a human agent as the software programmer writes specific instruction for the decision making process, machine learning might be out of control unless some procedure is put in place to keep humans in the loop. Hence, the policy concerns raised by the two are quite different.

Machine learning may be effectively used for profiling online and customizing search results as well as performing other tasks with different socio-economic consequences. The use of machine learning techniques to profile individuals outside consumer credit scoring is criticized for, among others, misclassification of individuals based on characteristics that have nothing to do with them, with serious implications including potential discrimination and deprivation of individual autonomy.[297]

Certainly, attempting to regulate the most advanced form of machine learning using old legal rules is doomed to reach a dead end. Although there is no evidence of the use of autonomous, unexplainable AI system in the consumer credit industry, should such technology be deployed, the solution cannot be found in tweaking the existing legal rules or even overhauling the law, whether in the EU or the US. Even the GDPR's presumably well-thought through and comprehensive rules are inapt to regulating machine learning decisions. Commenting on the GDPR's right to explanation rule, Nick Wallace argues:

> More importantly, those who drafted the GDPR do not seem to understand that it is often not practical or even possible, to explain all decisions made by algorithms. For example, autonomous vehicles are controlled by a multitude of algorithms that make many kinds of decisions. It is possible to log these actions, but it would take hours of work by highly-paid data scientists to render them intelligible. Often, the challenge of explaining an algorithmic decision

[295] *Id.*

[296] Brent Daniel Mittelstadt et al., *The Ethics of Algorithms: Mapping the Debate*, 3 BIG DATA & SOC'Y 1, 3 (2016) ("Machine learning is defined by the capacity to define or modify decision making rules autonomously."); *see also* Rachel Wilka et al., *How Machines Learn: Where Do Companies Get Data for Machine Learning and What Licenses Do They Need?*, 13 WASH. J.L. TECH. & ART 217, 223 (2018).

[297] Comandè, *supra* note 6, at 176.

> comes not from the complexity of the algorithm, but the difficulty of giving meaning to the data it draws on.[298]

Today, even governments acknowledge the unpreparedness of the legal regimes to address machine learning decisions. The United Kingdom's Government Office for Science noted that "most fundamentally, transparency may not provide the proof sought: simply sharing static code provides no assurance that it was actually used in a particular decision, or that it behaves in the wild in the way its programmers expect on a given dataset."[299]

Machine learning decisions require a holistic and cautious approach to regulation that strikes a fair balance between encouraging innovation and consumer protection. In this last section of the article, key features of regulation of machine learning consumer credit scoring are laid out.

5.2. Risk-Based Approach to Regulation

Any regulatory authority that is anxious about pervasive machine learning decisions in the credit industry should reject the temptation to impose a categorical ban or a prohibition that might stifle innovation. The more sensible solution is to adopt sector specific and risk-based approach,[300] where if the benefits of machine learning decision are outweighed by the costs of erroneous decisions, the system should be banned or be subject to stricter scrutiny. Machine learning decisions raise different types and degrees of concern in different spheres. To discuss a reasonable policy framework for the regulation of machine learning decisions, those different areas should be identified, isolated, and regulated, unless specific explanation is offered to create a general regulatory framework.

The European Commission's White Paper on Artificial Intelligence issued in 2020 introduced a risk-based approach to future regulation of AI acknowledging

[298] Nick Wallace, *EU's Right to Explanation: A Harmful Restriction on Artificial Intelligence*, TECHNOZONE360 (Jan. 25, 2017), https://www.techzone360.com/topics/techzone/articles/2017/01/25/429101-eus-right-explanation-harmful-restriction-artificial-intelligence htm.

[299] Government Office of Sciences, *Artificial intelligence: opportunities and implications for the future of decision making* 16 (2015), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/566075/gs-16-19-artificial-intelligence-ai-report.pdf.

[300] Frederik J. ZuiderveenBorgesius, *Strengthening legal protection against discrimination by algorithms and artificial intelligence*, 24 THE INT'L J. OF HUMAN RIGHTS 1572, 1586 (2020).

that the current legal regime including the GDPR does not necessarily address certain aspects of AI.[301] The white paper proposes a two-step analysis. The first step is to identify certain AI applications that are generally regarded as high risk.[302] The second step is to determine whether a given application within a sector is likely to pose a significant risk.[303]

In April 2021, the EU Commission published a Draft AI Regulation that adopted the risk-based approach.[304] The DAIR has three categories of AI systems to which different legal requirements apply. These are AI systems that pose (a) unacceptable risk (banned), (b) high risk, and (c) limited risk.[305] An AI system used for the assessment of the creditworthiness of natural persons (consumers) is listed as a high-risk AI System under Annex III of the DAIR.[306] With respect to high-risk AI Systems, stringent *ex ante* requirements are applied. These requirements relate to risk management, data governance, transparency, record keeping, human oversight, and robustness.[307]

High risk AI Systems including those used for credit scoring are expected to meet the requirements of conformity that must be monitored *ex ante,*[308] for instance that a credit scoring algorithm is not used unless it does not pose risk to the rights of the consumers (conformity). The requirements are imposed *ex ante* with compliance supervised by the relevant state authority. The DAIR does not address the rights of consumers aggrieved by an algorithmic decision (the right to human intervention, explanation, and redress). These rights of the consumer (data subject) are still to be governed by the GDPR unless the DAIR is revised before it is adopted to change the *status quo*. Hence, if a scoring algorithm is approved to be put to use and yet makes an inaccurate or discriminatory decision, the DAIR does not have rules that the consumer can use for redress. Although some of the rules including the one that requires automatic record-keeping allow the errors to be traced easily that the consumer can potentially use in a legal proceeding, the DAIR is not designed to address the rights of consumers that they can directly enforce.

[301] EU Commission, *White Paper: On Artificial Intelligence - A European approach to excellence and trust* (COM (2020) 65 final, 2020), 17.
[302] *Id.*
[303] *Id.*
[304] *See supra* note 31.
[305] EU Commission, *New rules for Artificial Intelligence – Questions and Answers* (April 21, 2021), https://ec.europa.eu/commission/presscorner/detail/en/QANDA_21_1683#1.
[306] DAIR Annex III, 5(b). AI systems put into service by small scale providers for their own use are not regarded as high-risk AI Systems.
[307] DAIR at Arts. 8 et seq.
[308] *Id.* at Arts. 40 et seq.

The current risk-based approach, therefore, does not resolve some of the underlying problems in ADM in consumer credit risk assessment (e.g., the difficulty in explaining machine learning decisions and the degree of disclosure of information that is considered sufficient to satisfy the right to explanation). Although the DAIR's risk-based approach which treats consumer credit scoring AI Systems as high risk is appropriate and the *ex-ante* conformity requirements are robust, the approach does not necessarily satisfactorily protect the consumer from machine learning decisions. For instance, one of the rules under the DAIR states that "High-risk AI systems that continue to learn after being placed on the market or put into service shall be developed in such a way to ensure that possibly biased outputs due to outputs used as an input for future operations ('feedback loops') are duly addressed with appropriate mitigation measures."[309] This provision clearly concedes that biased outputs may occur and in the case of machine learning decisions, the user of the system should take mitigating measures for the future. If taking a mitigation measure for the future is the most the law can expect deployers of machine learning algorithms to perform in case of biases, it is fair to conclude that remedy to the aggrieved consumer is not the priority. This triggers further related questions. Does that mean for instance a machine learning decision can be made in credit card, car loan, and mortgage loan applications provided that the AI System has fulfilled the *ex-ante* conformity rules? Does that mean biased decisions in these cases are to be addressed by way of implementing mitigation measures for the future? The response to these questions appears to be affirmative and it is not reassuring for EU consumers.

Granted, a financial institution might not use machine learning when making important decisions such whether to grant a mortgage loan. But under the DAIR, there is nothing that prevents them from doing so, if they have obtained the necessary *ex ante* approval for the machine learning algorithm. This a dangerous position to take while designing a legal framework for such a complex phenomenon. The legal framework in this area, in addition to the overall risk-based approach should be designed on sectoral basis. Thus, algorithmic credit scoring requires its own legal framework that takes into account different types of credits.

5.3. REGULATORY SANDBOXING

Regulatory sandbox is one of the most debated and increasing accepted notions in the field of financial technology. In its most basic form, regulatory sandbox is "a regulatory 'safe space' for experimentation with new approaches

[309] *Id*. at Art. 15(3).

involving the application of technology to finance."[310] As of July 2020, there are over 40 countries around the globe including the United States that have either announced or implemented some kind of regulatory sandbox.[311] There is no consensus on the objective for implementing regulatory sandboxes. The United States Department of Treasury in its 2018 report called for a regulatory sandbox that aims to enhance financial innovation.[312] But, Allen argues that objectives of regulatory sandbox should include not only encouraging innovation but also protecting consumers and ensuring market stability.[313]

While regulatory sandbox is premised on an entry barrier for Fintech companies due to excessive regulatory burden,[314] it provides regulators the opportunity to observe the regulatory challenges posed by a financial technology in a controlled environment,[315] working with a FinTech company that provides financial products or services to consumers without complying regulatory requirements.[316]

Current legal rules are ill-equipped to respond to a plethora of challenges that could emerge from machine learning credit risk assessment. A regulatory sandbox would provide an ideal environment for regulators to understand benefits of various innovations and the risks they pose to consumers along with the possible safeguards. According to the National Conference of State Law, fifteen US states have either proposed or implemented regulatory sandbox laws.[317]

[310] Dirk A. Zetzsche, et al, *Regulating a Revolution: From Regulatory Sandbox to Smart Regulation*, 23 FORDHAM J. OF CORP. & FIN. L. 31, 45(2017).

[311] Digital Financial Services Observatory, *Regulatory Sandboxes,* COLUM. BUS. SCH. (2016), https://dfsobservatory.com/content/regulatory-sandboxes.

[312]U.S. Dep't of Treasury, *A Financial System that Creates Economic Opportunity for Nonbank Financials, Fintech, and Innovation* 17, 168 (2018), https://home.treasury.gov/sites/default/files/2018-07/A-Financial-System-that-Creates-Economic-Opportunities---Nonbank-Financi....pdf ("[F]ederal and state financial regulators establish a unified solution that coordinates and expedites regulatory relief under applicable laws and regulations to permit meaningful experimentation for innovative products, services, and processes. Such efforts would form, in essence, a "regulatory sandbox" that can enhance and promote innovation.").

[313] Hilary J. Allen, *Regulatory Sandboxes*, 87 GEO. WASH. L. REV. 579, 583(2019).

[314]*Id.* at 587.

[315]*Id.* at 583.

[316] William Magnuson, *Regulating Fintech*, 71 VAND. L. REV. 1167,1224-25(2018).

[317]Heather Morton, *Financial Technology and Sandbox 2015-2019 Legislation*, NCSL (2019), https://www.ncsl.org/research/financial-services-and-commerce/financial-technology-and-sandbox-2015-2019-legislation.aspx#:~:text=Arizona%2C%20Kentucky%2C%20Nevada%2C%20Utah,legislation%20to%20create%20regulatory%20sandboxes.

Under New York regulatory sandbox program, the company concerned has twelve months,[318] subject to additional six months' extension[319] to test its product transaction with not more than 50,000 consumers that must be residents of New York State.[320] Consumers have the right to get full disclosure of the nature of the product or service they receive.[321]

The CFPB also introduced a regulatory sandbox program effective from September 2019. [322] The CFPB is criticized for its leniency toward market regulation by exposing consumers to potential abuses as it permits companies to test their products without complying with regulatory requirements, with no administrative sanction or liability under private law.[323]

Legal scholars investigating machine learning decisions are criticized for their focus largely on the deployment of the algorithm and the actual decision makings (the running model) rather than investigating other important stages in machine learning process. [324] Lehr and Ohm argue that "another reason legal scholars in particular need to focus on playing with the data is that combatting harms at the running-model stage is often too little too late."[325] They argue that rather than focusing on discrimination at running model and during data collection, discrimination is tackled better if an intervention is made at "several key, often overlooked, stages of machine learning." [326] They assert for instance that "mitigating algorithmic discriminations require intervening during model tuning and model training."[327] "Model training includes tuning, assessment and feature selection." [328] Thus, an algorithm could be modified if it makes a disparate classification at the stage of tuning.[329] Regulatory sandboxes could be designed not

[318]New York Regulatory Sandbox Act, N.Y. § 705(a) (2018), https://legislation.nysenate.gov/pdf/bills/2017/S9188.

[319] § 705(b).

[320] § 703(d).

[321] § 704(e).

[322] CFPB, *Policy on the Compliance Assistance Sandbox,* (Docket No. CFPB-2018-0042)(Sept. 10, 2019), September 10, 2019), https://files.consumerfinance.gov/f/documents/cfpb_final-policy-on-cas.pdf.

[323] Matthew J. Razzano, *An Unsafe Sandbox: Fintech Innovation at the Expense of Consumer Protection?,* 2019U. OF ILL. L. REV. 132, 132-39(2019).

[324]*See* Lehr & Ohm, *supra* note 138.

[325]*Id.* at 657.

[326]*Id.* at 705.

[327]*Id.* at 704.

[328]*Id.* at 696.

[329]*See* Kamishima T. et al., *Fairness-Aware Classifier with Prejudice Remover Regularizer In* MACHINE LEARNING AND KNOWLEDGE DISCOVERY IN DATABASES 35-50 (Peter Flach, Tijl De

only to ensure inclusiveness in the machine learning training, but also to allow regulatory agencies to obtain real time feedback on the challenges that could be faced during the process.

Much can be written about flaws in the way the New York or CFBC programs have been designed. For instance, the lack of cap on transaction values that can be involved in a service benefiting from a regulatory program is problematic because, one way of reducing consumer harm is to allow low value transactions. Moreover, stronger cooperation between regulatory authorities and the regulatory sandbox program recipients, including an exchange in technical knowledge is lacking in both programs. Nevertheless, a carefully designed regulatory sandbox could be valuable in regulating AI in the credit industry by balancing various competing interests including consumer protection and encouraging innovation.

The DAIR has also provisions on regulatory sandboxing.[330] The DAIR's provisions are woefully inadequate to address various challenges relating to implementing a successful regulatory sandboxing program that advances innovation while not undermining consumer rights. As the DAIR's provisions are to be implemented by the EU Member States through further legislation, it would be futile to critique its limited number of provisions. Member States should invite wider public participation in designing their implementing legislation.

6. CONCLUSION

Scholars have juxtaposed EU and US legal rules on ADM. The consensus seems to be that the EU approach to the regulation of ADM is superior due to the GDPR's comparatively detailed provisions on transparency in ADM, as well as its stringent consent requirements in addition to the applicable general prohibition of significant solely ADM. This article rejects this conventional wisdom and has argued that US consumer credit law has the necessary flexibility in accommodating the challenges emanating from ADM in consumer credit until the point where complex machine learning decisions are applied. The latter is a dead end both for the EU and US legal regimes. The real question is where we go from the dead end?

First, any regulatory intervention should balance the advantages of efficiency and inclusiveness (if any) in financial services on the one hand, and

Bie, &Nello Cristianini, eds., 2012); *see also* Moritz Hardt et al., *Equality of Opportunity in Supervised Learning,* 8-10, ARXIV.ORG (2016), https://arxiv.org/pdf/1610.02413.pdf.

[330] DAIR Arts. 53-55.

consumer protection from potential inaccuracy and biases/discrimination on the other. The legitimacy of any law is judged ultimately by its ability to strike a fair balance between the costs and benefits, and its ability to maximize the benefits and minimize the cost incurred by society.

The GDPR provisions governing ADM, although a good starting point for regulatory debate, by no means achieve a fair balance between encouraging innovation and consumer protection. Its general prohibition of solely ADM has the potential to stifle innovation without making the consumer better off as in Germany or to expose consumers to abuses as in the UK. The GDPR's provisions pertaining to consent and transparency in relation to ADM are as good as legal rules found in decades' old consumer credit laws in the US. This article emphasizes therefore that if the US wishes to implement regulatory regimes on ADM in the consumer credit industry, the GDPR is not the model to emulate.

Regarding complex machine learning decisions, the article proposed a risk-based approach to regulating, and the heightened use of regulatory sandboxing to allow FinTech companies to experiment their products in more fair and transparent manner. Although the EU's DAIR has incorporated both recommendations, it is far from addressing the complex challenges of machine learning.