[redacted]

‘Robo-Lenders versus the Defenders of (personal) Data’: Assessing the extent to which the UK data protection framework mitigates the risks of automated/AI credit risk assessment

Word count: 5082

Introduction

"Data is the new oil".[1] First coined over ten years ago, this simple phrase reflects an increasingly complex landscape of advancements in technology such as 5G networking, cloud computing,[2] big data analytics,[3] and, central to this paper, artificial intelligence and machine learning.[4] Combined, these technologies continue to usher the global economy into an unprecedented and '*paradigm shifting'*[5] 'age of data'.[6] What this means is that, across industries there is an increasing reliance on data based digital services to perform tasks that would typically be managed offline. This spans from sectors such as advertising, as in, the algorithmic curation of an individual's news feed,[7] to the finance sector, where use of the similar computer models may be used to assess a client for a mortgage and /or loans.[8]

In this age, large amounts of personal and non-personal data, including name, date of birth, online identifiers, location data, social media, marital status, schooling history, housing history, health data, immigration data etc,[9] are continually extracted to aid business processes. This is known as 'Big data'.[10] Joined by its corresponding technologies, data has thus become the 'new oil' a vital, seemingly endless and indispensable resource aiding businesses in their working operations.[11]

Following this, As reported by Cisco,[12] the financial services sector continues to be the largest user of these technologies. This comes as no surprise, as the growth of the financial sector has been said to be synonymous with technological growth.[13] This is exemplified through financial technology (FinTech)

[1] First coined in 2013 by mathematician. See, Charles Arthur,' Tech giants may be huge, but nothing matches big data' (The guardian, Aug 2013) <https://www.theguardian.com/technology/2013/aug/23/tech-giants-data > accessed 22 Aug 2024

[2] Steven Dickens, 'The Future Of Cloud Computing: AI-Powered And Driven By Innovation' (Forbes, 2024) https://www.forbes.com/sites/stevendickens/2023/07/28/the-future-of-cloud-computing-ai-powered-and-driven-by-innovation/ accessed 22 Aug 20204

[3] Ibid

[4] Ibid

[5] LEXIS GARCIA, 'The AI Paradigm Shift Is Reshaping the Tech Industry. Here's How Investors Can Capture Growth.' (Investors daily, Feb 2024) < https://www.investors.com/ibd-videos/videos/artificial-intelligence-reshaping-tech-how-investors-capture-growth > accessed 22 Aug 2024

[6] N-1

[7] Catherine E Tucker, 'The Economics of Advertising and Privacy' (2012) 30 International Journal of Industrial Organization 326

[8] Ibid

[9] Ana Cristina Bechara Garcia, 'Algorithmic discrimination in the credit domain: what do we know about it? AI & SOCIETY (2024) 39:2059–2098

[10] Ibid

[11] R Zaman, M Hassani & BF van Dongen, 'Data Minimisation as Privacy and Trust Instrument in Business Processes' in A Del Río Ortega, H Leopold & FM Santoro (eds), *Business Process Management Workshops* (BPM 2020) (Lecture Notes in Business Information Processing vol 397) 95.

[12] Splunk, Industry report, 'The data Age is Here, Are You ready?' (Splunk, Cisco, 2023) <https://www.splunk.com/en_us/pdfs/gated/ebooks/data-age.pdf > accessed 22 Aug 2024

[13] Ibid

products such as digital currencies amd blockchain technology.[14] A format of this is additionally seen in the use of 'robo- lenders'-automated, usually ai powered software that make use of borrower's personal data, both financial and social,[15] to estimate their credit worthiness in order to determine their access to finance. The use of automated lenders has very quickly become the norm in the UK financial sector.[16]

On the one hand, this insight may echo the seemingly fictional fear of 'algorithmic governance',[17] an apocalyptic scenario where smart computers, in this case, robot lenders, determine finance access, without recourse in situations of unfavourable outcomes.[18] In this case, one would not be wrong, as related risks of intelligent algorithms, or AI are regularly published and warned against by scholars and regulators alike.[19] Risks such as the discriminatory bias of algorithms, the lack of transparency of assessment models and the concern for the degradation of personal data in light of excess data mining.[20]

On the other hand, financial services providers may continue to utilise the full or partial use of sophisticated algorithms to calculate credit risk, as a celebration of innovative development in its own right, given the innovative history of the sector.[21] Moreover, It is widely reported that this method creates financing opportunities for underserved markets,[22] introduces efficiency to an otherwise slow process, and garners large investments for continued innovation, internal structures and industry standard setting.[23]

Nonetheless, the associated risks of AI decision making continues to balloon into a greater issue, forcing governments all around the world to pay close attention to statutory and regulatory solutions.[24] With the continued growth and investment into 'fin-tech' operations, these risks are as urgent as they

[14] Ibid

[15] N- 9

[16] Nikita Aggarwal, 'The Norms of Algorithmic Credit Scoring' The Cambridge Law Journal, 80 [2021], pp 42–73

[17] FCA How can we ensure that Big Data does not make us prisoners of technology? Helbing D et al (2019) Will democracy survive big data and artificial intelligence? Towards digital enlightenment. Springer, New York, pp 73–98

[18] Ibid

[19] Lerong Lu *, 'Reconceptualising Fintech: technological innovations in international finance, commercial applications and legal issues' Journal of International Banking Law and Regulation. [2024], 39(1), 14-25

[20] UK GOV. ' A pro innovation Approach to AI regulation' (Report, Department for Science Health and Technology, 2023) < https://www.gov.uk/government/publications/ai-regulation-a-pro-innovation-approach/white-paper > accessed Aug 22 2024

[21] Ibid

[22] Ibid

[23] Ibid

[24] Clifford Chance, 'Global AI Regulation - Clifford Chance' (Clifford Chance, 2023) < https://www.cliffordchance.com/insights/thought_leadership/ai-and-tech/global-ai-regulation.html#:~:text=Globally%2C%20there%20are%20calls%20for,focused%20on%20managing%20AI%20risks.%22 > accessed 22 Aug 20204

are permanent. The task of governments globally is to create regulatory frameworks that can balance innovation with protection. In the UK for example, in order to tackle the growing risks, a mix of statute and regulatory solutions have been employed.[25] Amongst these can be seen the Information commission (ICO), the financial Conduct Authority (FCA) and of central importance to this paper, the General Data Protection Regulation UK (UKGDPR).

The aim of this essay is to determine the extent to which the legal framework of the UK adequately responds to the data protection risks of automated/AI credit risk assessors. To this end, this paper is divided into four headings. The first concerns the development of lending algorithms and clarifies the terms to be used in the rest of the essay. The second heading addresses in greater detail, the highlighted risks of opacity, discrimination and data insecurity in data mining. Part 3 focuses the central analysis, measuring the extent to which the UKGDPR responds to these risks. Finally, heading four presents' proposals for strengthening the UK regulatory framework all-round, in order to address said risks, after which the essay draws a conclusion of the explored points.

S.1 Automated Credit Risk Assessment: Key Terms and Development

This section first seeks to track the development of the use of automated decisions making the credit assessments of the financial sector. Next it will explain key terms in order to facilitate understanding for the rest of the essay.

To begin, Concerning the development of automated credit assessment, It is well known that in the financial sector, the development of automating business decisions is not new.[26] For example, the use of computerised tools to assess burrower risk in loaning decisions has gone on since the 1940's development of credit scoring models.[27] In this past, credit risk was calculated based on algorithmic models which factored in data sets, financial and non-financial, such as marital status and gender.[28]

The difference now, and the reason why automated credit models are increasingly reported to be risky, is because contrary to the less advanced models of the past, current credit risk models having developed in tow with the rise of 'big data' processes, thus drawing on exponentially larger and more

[26] n- 19
[27] Bee Wah Yap, Seng Huta Ong and Nor Houseline Mohamed Husain, 'Using Data Mining to Improve Assessment of Credit Worthiness via Credit Scoring Models' (2011) 38 Expert Systems with Applications 13274 <https://www.sciencedirect.com/science/article/pii/S0957417411006749>. Accessed 22Aug 2024
[28] Ei, the purpose of the US 's Equal Credit Act was to mitigate this discrimination

varied sources of data to produce their outputs.[29] This is called data mining.[30] In the current period, the central issue of credit risk algorithms is that data continues to be mined in large, varied and vacuous amounts, suggesting that all of a person's 'digital footprint' is examined by these in human models, and defining access to the key societal resource of debt finance. [31]

While the overall positive impact of this development is celebrated both in and out of the financial sector, the technology continues to accelerate and thus risks continue to ballon. The key risks of automated credit assessment to be weighed in this essay include discriminatory profiling, transparency issues concerning 'black box' processes, and the risk of surveillance society at the rate of current data mining.

Next, the key terms utilised throughout the essay will be outlined. First, the term 'automated decision making' is not a monolithic concept. This term covers both algorithmic decisions making, and Artificial intelligence operations. Central to these two processes is that they make use of large data, or 'big data' as previously seen, in order to analyse, extract and draw conclusions to supplement, or solely make decisions/ produce output.[32]

Following this, Algorithmic decision making relates involves the use of computational methods to manipulate data in order to either make decisions or supplement human decision making.[33] It is thus divided into two kinds. This manipulation involves collecting, storing and processing large volumes of customer and business data in order to carry out decisions central to business operations. An example can be seen in simple search engine processes on catalogue websites. As opposed to machine learning powered AI, this form does not generate new output.

Artificial intelligence (AI) on the other hand, covers many forms and as such has no central definition. Given this, it may refer to the 'theory and technological developments'[34] of computing that enable the performance of operations that mimic human intelligence.[35] AI may be broadly divided into strong AI, weak AI, Machine learning and deep learning. As the European Commission expert group on AI informs, overall, these forms carry out three central functions: Reasoning and decision making,

[29] Current credit modelling off big data

[30] N-27

[31] Ibid

[32] Lerong Lu, Reconceptualising Fintech: technological innovations in international finance, commercial applications and legal issues

[33] Ibid

[34] James Tobin, House of Lords, 'Artificial intelligence: Development, risks and regulation' (House of Lords, 18 July 2023)

[35] Ibid

learning (such as machine learning) and robotics.[36] For the purpose of this paper, only the first two will be relevant.

While both algorithmic operations and AI will be analysed as ‘automated decisions’, AI relates to algorithmic operations in that it is also a computer science field but differs in that it takes on more advanced functions (such as data analytics across large data sets to determine fraudulent behaviour)[37] and seeks to model human intelligence, in particular, modelling a sense of ‘logic and rationality’, as related to decision making.

In addition, throughout the essay, the terms; credit risk assessment, AI credit modelling, Automated credit risk assessment, AI credit scoring, credit scoring, sophisticated credit modelling, and all similar sounding terms, will be used to refer to the same phenomena- the use of deep learning/ machine learning technologies, utilising big data, to estimate the borrowing risk of a client.[38]

S.2 Related Risks of Robo-lending

This section analyses the risks of AI credit rating at the centre of this essay, namely, transparency or opacity risks, discriminatory risks and data insecurity risks.

To begin with, a key risk of AI credit modelling is the lack of transparency that is sometimes inherent to the models used. In a House of Lords publication on artificial intelligence, it is reported that AI forms like deep learning, may generate unexplainable outputs.[39] This phenomenon in the context of credit evaluation is otherwise known as ‘black box’ output. This may be seen in situations where a borrower may be rejected a loan or deemed ‘bad credit’ due to unexplainable and thus unknowable variables assessed.

The effect of this may be seen in two folds. As a first example, this may be related to the discrimination issue, where a lending decision is made against a member of a discriminated group, but due to the opaqueness of process, investigation cannot be conducted, thus denying justice to the applicant, and an operations maximization opportunity to the lender.

[36]independent high-level expert group on artificial intelligence set up by the European commission, ‘a definition of ai: main capabilities and disciplines’ (European Commission report, 2019)https://www.aepd.es/sites/default/files/2019-12/ai-definition.pdf> accessed 22 Aug 2024

[37] Oliver Wyman, ‘The Impact of Ai in financial Services’ (Oliver Wyman report, 2023)

[38] *Ibid*

[39] N-34

Another instance of the impact of this is risk is that it may be on the borderline of illegal activity, as, in countries like the UK where data protection standards are high, the level of transparency required is bypassed by these models. It is reported that banks are in the pilot phase of establishing these models. It poses a ballooning risk if not addressed at this crucial time. A window of sorts.

Next, another risk posed by AI or automated lending models is that they may amplify the discriminatory biases of society. In a general sense it has been well studied by scholars such as Noble, in her book *algorithms of oppression,* that AI models reinforce negative and discriminative stereotypes of groups of people such as black and minority groups.[40] In the field of AI credit assessment this manifests as the denial of singled out groups of people from accessing debt finance for conducting ie business credit, mortgage payment etc at the same level and ease as their non discriminated counterparts.[41]

The wider effect of this is the potential blocking out key groups from financial services, reinforcing lower standards of living and continuing bias. Nonetheless, it has been argued that contrary to popular belief, intelligent credit models *reduce* levels of credit discrimination, as the bias is stronger in cases where loan vetting is done by humans.[42] This argument, while insightful, fails to consider that while humans may be more biased in credit assessment, the fact that lending models have been built off these biases, and continuously perpetuate them, suggests that any 'equalising benefits' of the automated lenders is easily outweighed.

The final risk of automated lending to be analysed in this essay is the risk of data insecurity inherent to data mining. It is aged practice that credit assessments require a broad range of data spanning from financial data such as credit history and income, to non-financial data such as gender, marital status and home location area.[43] This is heightened by the introduction AI and machine learning technologies as they depend on data mining- the process of continually extracting and analysing large data sets in order to have the 'data bank' which facilitates its generative output. [44]The consequence of this dependence on data sets is that financial firms are now more vulnerable to data leaks and breaches, where the financial information of their clients is exposed, either due to cybercrime or vulnerable

[40] Noble SU, Algorithms of Oppression: How Search Engines Reinforce Racism (NYU Press 2018)

[41]Kehinde Andrews, 'UK banks have a racial discrimination problem. It's time they admitted it' (The Guardian , 2017)< https://www.theguardian.com/commentisfree/2017/jan/13/uk-banks-racial-discrimination-black-victims-fraud > accessed 22 Aug 2024

[42] Fredrick Zuiderzee,' Discrimination, Artificial Intelligence and Algorithmic Decision Making' (Council of Europe, 2018) <https://rm.coe.int/discrimination-artificial-intelligence-and-algorithmic-decision-making/1680925d73 > accessed 22 Aug 2024

[43] N-33 pg. 2

[44] Volume of data mined in fintech's, Lilit Melkonyan, ' How Big Data Is Reshaping Fintech: Open Banking' (PLAT, March 20222) < https://plat.ai/blog/big-data-reshaping-fintech/ > accessed Aug 22 2024

data security / algorithmic systems,[45] leading to problems like fraud and identity theft, market manipulation and wider impact on the economy, such as loss of trust In the banking system,[46] as well as high costs to the banking firms.[47] For example, in 2014, following its integration of computerised ways of managing its data, banking firm JP Morgan experienced a data breach,[48] caused by a exploitation some vulnerabilities of its algorithmic systems. The personal data of over 80 million of its clients, including their names, social security numbers, emails and mailing addresses were exposed, leaving openings for hackers and issues of identity theft.[49] These examples highlight the risk of data security, that grows as banking firms continue to integrate disruptive and data intense technologies such as artificial intelligence in a range of finance operations including credit risk assessment. Nonetheless, in the face of the explored risk, it is well reported that data mining benefits the process of credit risk modelling as it is more efficient than other methods to delivering services,[50] enabling firms to offer more and manage more customers.

To counteract this, the UK government has introduced limits on the kind of data that can be mined. However, in this age of machine learning and advanced credit models, financial firms bypass this measure by mining other forms of data, seemingly unrelated, but suggestive of credit risk.[51] These go as far as examining a borrowers shopping activity, social media use, and levels of interaction with their networks.

In summary, this section has overviewed the growing risks central to the development of automated lending. The next section aims to weigh these risks against the UK's data protection tool, the General Data Protection Regulation.

[45] Forbes Business Council, 'The Biggest Data Leaks and How to Prevent Them from Repeating' (23 October 2023) https://www.forbes.com/councils/forbesbusinesscouncil/2023/10/23/the-biggest-data-leaks-and-how-to-prevent-them-from-repeating/ accessed 22 Aug 2024

[46] Ibid

[47] Roger Smith, 'Technology, The Future and Us' [2015] 165 NLJ 7635 pg. 7

[48] Fluid Attacks, 'Top Financial Data Breaches' (n.d.) https://fluidattacks.com/blog/top-financial-data-breaches/

[49] Ibid

[50] Darics, 'Data Mining: A Key Tool to Improve Banking Business Processes' (n.d.) https://www.datrics.ai/articles/data-mining-a-key-tool-to-improve-banking-business-processes#:~:text=By%20evaluating%20past%20financial%20behaviors,of%20defaulting%20on%20future%20loans.> accessed 2024

[51] Ann Befit and Laura Diets Chy, 'GDPR Series: The Risks with Data Profiling' (2016) 17(2) *Privacy and Data Protection* 6

S.3 Analysing the strength of the GDPR against the Risks of Robo-lending

The General Data Protection Regulation (GDPR) is the recent Data Protection regulation developed by the EU. It is maintained by the UK, with minimal changes, to correspond with the 'adequacy' measure of the EU's policy of maintaining their standard of data protection with third countries.[52] As such, the GDPR, or more specifically, the 'UK GDPR' is the presiding law of data protection in the UK. On the one hand, as the UK is known to be at the forefront of data economy innovation,[53] the GDPR has been praised to be the 'most developed data protection law currently in force'.[54] This underscores the significance of the following analyses beyond a jurisdictional choice as it may be argued that the GDPR essentially reflects the state of data protection regulation on a more global scale.[55]This section aims to weigh the prior explored risks of robo lending against the protections of the UK GDPR. Regarding terms, this section will use UK GDPR and GDPR to refer to the similar regulations, as it focuses both on UK and wider EU application.

To begin, it will be determined the extent to which the GDPR grapples with the transparency issue of robo-lending. As discussed, automated lending gives rise to transparency issues, arising from processes concluded by 'opaque'[56] and complex credit models which, in calculating borrower risk, deliver unintelligible complex reasonings or none at all. This is known as the 'black box issue'.[57] This gives rise to issues of trustworthiness, limited recourse to correction, compensation or justice, given that wrongly calculated or 'hallucinated 'factors cannot be properly inferred.

This issue can be said to be clearly relevant to the scope of the GDPR, given that the theme of transparency is one of its three building blocks.[58] This principle is one formulated to facilitate the exercise of the autonomy of the data subject by facilitating informational access regarding personal data and data processing purposes of the controller, otherwise consolidated into the 'right to be informed'.[59] Good transparency practice by a firm reflects accessible provision of certain information as contained in articles 13 and 14. Further, where the firm or controller engages in processes with

[52] Ibid

[53] 'UK AI Sector Most Valuable in Europe, New Report Reveals' (n.d.) *Holyrood* https://www.holyrood.com/news/view,uk-ai-sector-most-valuable-in-europe-new-report-reveals#:~:text=The%20UK%20is%20home%20to,2023%20injected%20into%20innovative%20technology.> accessed august 22 2024

[54] Alexander J Wulf and Ognyan Seizov, '"Please Understand We Cannot Provide Further Information": Evaluating Content and Transparency of GDPR Mandated AI Disclosures' (n.d.)

[55] To an extent. Other jurisdictions are in the legislative process for developing new, more current laws to grapple with exploding technologies such as AI examples include the EU AI Act

[56] N-44

[57] The Black Box Society the Secret Algorithms That control money and information (FP)

[58] Lawfulness, fairness and transparency Article 5

[59] Ibid

legal or similar effects,[60] the information must meaningfully include the logics of the decision, its significance, and any consequences the data subject may face.[61]

Next, in application to the automated credit assessment risk of opaque operations, the effectiveness of the GDPR will be examined. On the one hand, other than the critical risk of unexplainable AI, the clear provisions of the GDPR provide simple guidelines on ways that firms can become more transparent regarding their AI augmented practices, suggesting its commitment to fostering transparent practices. Examples include article 14, stipulating the provision of a privacy policy where information such as ai use can be clearly stipulated.[62] Nonetheless, as exemplified by a 2023 report by the Evident AI Index,[63] only 6 out of 50 of top banks assessed, between Europe and the US have incorporated privacy notices or other forms of disclosure that inform the public about their AI integration steps. This shows that despite the clear steps to improving transparency given by the GDPR, in practice it fails to effect change, particularly in the age of AI finance.

This next portion weighs the strength of the GDPR against the discriminatory risks of robo lending. as previewed in the preceding section, AI credit models utilise the profiling of characteristics such as race, religion, age etc. giving rise to discriminatory potential, as the classifications of high risk or low risk factors mirror human biases.[64] In modelling the credit risk of borrowers, this leads to static social groupings reflecting 'risk' in historically underserved groups, subjecting them to differential treatment where their access to finance is made more difficult.

Following this, the GDPR article that can be said to apply is article 22, which covers the profiling of individuals. This provision holds that the data subject has the right 'to not be subject to a **decision** based on **solely automated decisions,** including **profiling**, which produces **legal effects** concerning him or her **or similarly affects** him or her' (emphasis mine).[65] Here, the regulation takes an approach of prohibition where said decisions have adverse effect on the data subject, in that they assess personal data for i.e., credit, jobs and 'similarly legal effects'.[66] The exceptions being particular situations, continued under article 22(2) including contract, public requirement and consent.[67] The reasoning here is one of protecting the autonomy of the data subject in engaging such decisions.

[60] Right to be informed
[61] FCA AI UPDATE
[62] Article 14
[63] https://evidentinsights.com/ai-index/
[64] Challenging algorithmic profiling: The limits of data protection and anti- discrimination in responding to emergent discrimination. Monique Mann, T Matzner, 2019
[65] Article 22(1)
[66] Explanatory notes 71
[67] Article 22(2)

To continue, considering the effectiveness of the regulation, it may be argued that the GDPR has only recently become effective to fulfil its purpose, stated as preserving individuals' autonomy against impactful profiling. This is because there has been seen to be a lack of clarity concerning exactly what kind of decisions are classed as significantly affecting the data subject. While the explanatory notes give examples such as fully automated credit scoring and job applications,[68] given the non-enforceability of the preamble notes, credit scoring was not considered an impactful decision up until 2023.

2023 witnessed a landmark court ruling by the CJEU regarding German credit assessment firm schafa against OQ, german claimant.[69] Here, OQ was denied a loan based on a credit score given by schufa, a german credit rating firm. OQ consequently requested access to her information, as well as erasure, to which schufa provided only a broad explanation. Schufa declined the access request based on the fact that it was a third party who only provided the credit score, of which the german bank used to ultimately make the decision. OQ complained to the supervisory authority, who rejected, leading to the appeal to the court. Here, the court ruled that despite the fact that the german bank made the ultimate decision, Schufa's credit score valuation constituted a 'determining role',[70] and thus a form of automatic decision making according to article 22(1). The impact of this ruling is the introduction of more clarity, allowing for financial firms and their internal or third-party data analytics to be captured by the GDPR, allowing for greater and more accurate enforcement of automated decisions,[71] for both the firms that make the final decisions and specifically, the third-party firms who utilise big data to manage the calculation and/profiling of individuals according to credit risk. Thus, it has been seen that, in the area of profiling/discrimination risks of credit risk modelling, the GDPR which began as ambiguous has developed into an accurate tool, able to keep up with current robo-lending in the face of big data.

Finally, the strength of the UKGDPR in mitigating the risk of data insecurity consequent to data mining will be addressed. As discussed in section 2, data insecurity is the risk of data breach and algorithmic exploitation present to financial firms utilising sophisticated credit models. Data insecurity is brought about by the employment of data mining- the gathering and analysis of large data sets to generate decisioning outputs. Due to financial firms now utilising large volumes of data for their business operations, the data they hold is perpetually at risk of being leaked or otherwise

[68] Ex 71
[69] OQ v Land Hessen SCHUFA Holding AG, C-634/21, ECLI-EU-C-2023-957
[70] Para 50
[71] Ibid

manipulated, giving rise to fraud, loss of firm integrity and market manipulation, affecting the firm and its clients alike.[72]

In order to address this risk, a relevant provision of the GDPR is that of data minimisation. This principle, written for the purpose of data protection, states that personal data shall be *'**adequate, relevant and limited** to what is necessary in relation to the purposes for which they are processed ('data minimisation')'*.[73] This means that data controllers, in this case, financial firms, must limit the data they collect to *only* what is needed, for the specific purpose it has been collected for. (purpose limitation principle).[74] The legislative intention of this principle is that data is processed to a minimum so strict that, alongside purpose and storage limitations, disallows data processors from using data that has not been authorised by the data subject,[75] thus preserving the autonomy of the data subject.

In application to the issue of the data mining risks of fintech's, it is argued that data minimisation applied, finance firms collect less data, and so, at any given time, do not have excess data available for manipulation. [76] This mitigates the data mining risks of leakage for example, since the hackers are known to be more attracted to firms with exploiting storage systems.[77]

Conversely, the weakness of this argument is exposed by the fact that data minimisation as a principle has been part of the GDPR framework since its predecessor, the data protection directive,[78] yet still struggles to be implemented today. Building on this, it is argued instead that while data minimisation may have more effective application in industries such as the medical sector,[79]it is simply *incompatible*[80] to deal with big data utilisation of the finance sector. This view, put forward by scholars such as Zarsky, emphasises the opposition of big data practices versus the minimisation principle.[81] He argues that, as opposed to the medical sector, the finance industry is incentivised to keep data for as long as possible, since, for example, larger data sets model more accurate analysis as pertaining to historical data, consumer behaviour, etc.[82] It has therefore been shown that, against the

[72] Ibid
[73] GDPR article 5 (1) (c)
[74] Purpose minimisation principle
[75] Recital 39
[76] I Zdarsky, Tal (2017) "Incompatible: The GDPR in the Age of Big Data," Seton Hall Law Review: Vol. 47: Is. 4, Article 2.
[77] Ibid
[78] Data protection Directive – data minimisation principle
[79] Yardena Ivanova, 'The Role of the EU Fundamental Right to Data Protection in an Algorithmic and Big Data World' in Dara Hallinan, Ronald Lens, Serge Gut Wirth and Paul De Hart (eds), *Data Protection and Privacy* (Vol. 13, Data Protection and Artificial Intelligence, Hart Publishing, forthcoming)
[80] Ibid
[81] Ibid
[82] Aiming, 'Big Data Driving the Future of Finance' (n.d.) https://www.ayming.co.uk/insights/opinion/big-data-driving-the-future-of-finance/ accessed augh 2024

risks of data mining in the finance sector, the GDPR principle of limitation fails to gain ground because the finance sector is incentivised to keep data.

To conclude, this section set out to evaluate the strength of the UKGDPR against the growing risks of AI credit risk assessment, given as opacity, discriminatory risks and data mining insecurity respectively. The GDPR was highlighted to be an innovative regulation in regard to the world stage. The principles concerned were transparency, profiling and data minimisation. Against opacity risk, it was found that, despite its straightforward steps to building transparency, its enforcement is weak in the current practice of the finance sector. Further, it was found that in regard to discriminatory risks, though unclear at first, through case law it has developed into more accurate effective tool, directly applicable to the practice of AI credit risk modelling, capable of mitigating the risk of potentially discriminatory profiling. Finally, the GDPR principle of data minimisation was found to be almost ineffective in the current fintech climate, given that firms are more incentivised to collect data than store it, to build data bases for analytics in the current age of 'big data'.

S.4 Proposals to amend or address highlighted issues

Continuing on from the prior section, this section aims make recommendations concerning the weaknesses of the GDPR against mitigating opacity, discrimination and data insecurity risks, as well as the risks themselves. This will be treated in a broad approach, highlighting solutions such as legislative supplement, regulatory cooperation and CSR to motivations with the view to funding ethical AI use in the financial sector.

To begin, legislative supplement is one way that the GDPR can be made more effective at mitigating AI credit modelling risks. For example, in regard to the issue of GDPR inefficiency in tackling discrimination, it is suggested by scholars such as Mann, that the GDPR be read together with anti-discrimination law.[83] Her reasoning follows that, as the GDPR and European charter on human rights both focus on the rights of the (data) subject, enforcing anti-discrimination law alongside may form a potent combination for mitigating data/ AI related discrimination.[84] Another way that statute may fill the gap of data subjects' protection to update the relevancy of the GDPR in the AI age is through the

[83] Mann, M., & Matzner, T. (2019). Challenging algorithmic profiling: The limits of data protection and anti-discrimination in responding to emergent discrimination. Big Data & Society, 6(2). https://doi.org/10.1177/2053951719895805
[84] Ibid

use of supplementary regulation such as the AI regulation of the EU [85] and white paper stage AI regulation in the UK.[86]

Another suggested proposal towards the mitigation of robo lending risks is seen a step down from statute level, in the cooperation of global cooperation of AI regulators and financial regulators. [87] For example, the UK is doing this through the newly formed Digital Regulation Cooperation Forum (DRCF). They are a collective made up of the Information Commissioners Office (ICO), the Competition Markets authority (CMA), the Office of Communications (Ofcom) and the Financial Conduct Authority (FCA).[88] This cooperation exemplifies the kind of cooperation that the increasingly data focused economy may greatly benefit from. Amongst their most recently stated goals, they have stated a focus on tackling the risks of AI, facilitated through their collaboration through greater research access and cross industry enforcement.[89]

The final suggested proposal towards the general treatment of robo lending risks is the increased focus on corporate social responsibility (CSR) in FinTech's and banking firms more generally. With emerging risks such as cyber security and climate change,[90] given that the risks affect both finance firms and their clients alike, it is becoming increasingly importance to recognise and motivate their sense of public responsibility. One way that this is being done is through increasing focus on banks as stewards of the public.[91] Here, banks take up ethical roles, permeating management and governance structures, responsible investments,[92] and innovative financial products such as green bonds.[93] As they adopt a more ethical and public facing role, it is believed that this will permeate the general data privacy outlook of the sector, leading to higher incentives to i.e. innovate more ethical ways of using private data.

[85] European Commission, 'Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act)' COM (2021) 206 final, 21 April 2021 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206

[86] Alexandra Giannopoulos, Jeff Ausloos, Sylvie Delacroix and Helene Janssen, 'Intermediating Data Rights Exercises: The Role of Legal Mandates' (2022) 12(4) *International Data Privacy Law* 307

[87] Regulatory co-operation: data protection and financial regulation (Journal of International Banking & Financial Law Journals) 01 Sep 2019Stuart Levi 2019 Volume 34 > Issue 8 > Articles > Regulatory co-operation: data protection and financial regulation – (2019) 8 JIBFL 542

[88] Information Commissioner's Office, 'Digital Regulation Cooperation Forum' (n.d.) https://ico.org.uk/about-the-ico/what-we-do/digital-regulation-cooperation-forum/ accessed 22 Aug 2024

[89] Digital Regulation Cooperation Forum, 'Workplan 2024-25' (n.d.) https://www.drcf.org.uk/__data/assets/pdf_file/0030/283188/DRCF-Workplan-202425.pdf accessed 22 Aug 2024

[90] Digital Regulation Cooperation Forum, 'Workplan 2024-25' (n.d.) https://www.drcf.org.uk/__data/assets/pdf_file/0030/283188/DRCF-Workplan-202425.pdf accessed 22 Aug 2024

[91] Financial Conduct Authority, 'Towards More Effective Stewardship' (n.d.) https://www.fca.org.uk/news/speeches/towards-more-effective-stewardship

[92] Ibid

[93] Ibid

In conclusion, this section has proposed some recommendations towards enhancing the GDPR's effectiveness, as well as the mitigation of robo-lemding risks in a more general sense. These proposals include legislative supplementation through laws such as anti-discrimination laws to mitigate AI discrimination. Another proposed recommendation is seen in the cooperation of regulatory bodies such as the DRCF towards harmonising enforcement in the digital economy. Finally, incorporating corporate social governance leads to a stronger sense of public responsibility.

Conclusion

In conclusion, as a consequence of the disruptive technology of AI/ Machine Learning, the increasing global shift into a more digital economy and the resulting availability and valuation of 'big data', many industries are moving with the tides of innovation, to transform their operational processes and adjust to the new risks. The finance sector is no exception, especially given its age-old practice of being at the forefront of technological innovation and investment. At present however, the change is unprecedented and can be said to be a paradigm shift, as such legislation cements itself as a facilitator of change. Given this, the central query of this essay set to determine the strength of the UK data protection legislation, the UK/GDPR, against the growing risks associated with the use of automated or AI credit risk assessment in the finance sector. To this end, the paper was divided into four headings.

The first section explored the development of credit risk assessment. In addition, it discussed key terms that were used throughout in order to facilitate understanding. These terms included automated decisions, algorithms and credit risk assessment, as well as the ways they varied for language's sake, yet keeping similar meanings. The second heading of the essay addressed the risks of AI credit risk modelling that would be central to the main evaluation against the law, discussing and analysing them. They were given as; 'black box' or opacity risks, seen in the unreadability of sophisticated algorithms, discrimination risks, referring to the likelihood of algorithms to reproduce societal biases, and data security risks consequent to 'big data' mining.

The third section treated the main analysis of the risks against the UK/GDPR. It was seen that, against opacity, despite being formulated with clear implementation it faces enforcement weakness in current AI banking. In regard to discrimination or profiling with risks of discrimination, it was seen that, though introduced with a level of vagueness, recent case law has enabled clear application in the specific area of credit risk modelling, with detail given to big data analytics. Finally, when weighed against data security risks of data mining, it was seen that the UK/GDPR principle of data minimisation is difficult to enforce in the age of big data banking that is incentivised to build, rather than reduce data sets. As such it was seen that the UK/GDPR is generally weak against the new age of banking. Finally, the fourth section set out proposals to address the analysed risks in a wider sense. These solutions were given as legislation supplementation, regulatory cooperation, and encouragement of CSR initiatives.

Bibliography

- Fredrick Zuiderzee, *Discrimination, Artificial Intelligence and Algorithmic Decision Making* (Council of Europe, 2018) https://rm.coe.int/discrimination-artificial-intelligence-and-algorithmic-decision-making/1680925d73 accessed 22 August 2024

- Ann Befit and Laura Diets Chy, 'GDPR Series: The Risks with Data Profiling' (2016) 17(2) Privacy and Data Protection 6

- 'UK AI Sector Most Valuable in Europe, New Report Reveals' (Holyrood, n.d.) https://www.holyrood.com/news/view,uk-ai-sector-most-valuable-in-europe-new-report-reveals#:~:text=The%20UK%20is%20home%20to,2023%20injected%20into%20innovative%20technology. accessed 22 August 2024

- Aiming, 'Big Data Driving the Future of Finance' (n.d.) https://www.ayming.co.uk/insights/opinion/big-data-driving-the-future-of-finance/ accessed August 2024

- Alexander J Wulf and Ognyan Seizov, '"Please Understand We Cannot Provide Further Information": Evaluating Content and Transparency of GDPR Mandated AI Disclosures' (n.d.)

- Alexandra Giannopoulos and others, 'Intermediating Data Rights Exercises: The Role of Legal Mandates' (2022) 12(4) International Data Privacy Law 307

- Ana Cristina Bechara Garcia, 'Algorithmic Discrimination in the Credit Domain: What Do We Know About It?' (2024) 39 AI & Society 2059

- Bee Wah Yap, Seng Huta Ong and Nor Houseline Mohamed Husain, 'Using Data Mining to Improve Assessment of Credit Worthiness via Credit Scoring Models' (2011) 38 Expert Systems with Applications 13274 https://www.sciencedirect.com/science/article/pii/S0957417411006749 accessed 22 August 2024

- Catherine E Tucker, 'The Economics of Advertising and Privacy' (2012) 30 International Journal of Industrial Organization 326

- Clifford Chance, ‘Global AI Regulation - Clifford Chance’ (Clifford Chance, 2023) https://www.cliffordchance.com/insights/thought_leadership/ai-and-tech/global-ai-regulation.html#:~:text=Globally%2C%20there%20are%20calls%20for,focused%20on%20managing%20AI%20risks.%22 accessed 22 August 2024

- Darics, 'Data Mining: A Key Tool to Improve Banking Business Processes' (n.d.) https://www.datrics.ai/articles/data-mining-a-key-tool-to-improve-banking-business-processes#:~:text=By%20evaluating%20past%20financial%20behaviors,of%20defaulting%20on%20future%20loans. accessed 2024

- Digital Regulation Cooperation Forum, 'Workplan 2024-25' (n.d.) https://www.drcf.org.uk/__data/assets/pdf_file/0030/283188/DRCF-Workplan-202425.pdf accessed 22 August 2024

- European Commission, 'Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act)' COM (2021) 206 final, 21 April 2021 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206

- Financial Conduct Authority, 'Towards More Effective Stewardship' (n.d.) https://www.fca.org.uk/news/speeches/towards-more-effective-stewardship

- Fluid Attacks, 'Top Financial Data Breaches' (n.d.) https://fluidattacks.com/blog/top-financial-data-breaches/

- Forbes Business Council, 'The Biggest Data Leaks and How to Prevent Them from Repeating' (23 October 2023) https://www.forbes.com/councils/forbesbusinesscouncil/2023/10/23/the-biggest-data-leaks-and-how-to-prevent-them-from-repeating/ accessed 22 August 2024

- Helbing D and others, 'How Can We Ensure That Big Data Does Not Make Us Prisoners of Technology?' in D Helbing and others (eds), *Will Democracy Survive Big Data and Artificial Intelligence? Towards Digital Enlightenment* (Springer 2019)

- Independent High-Level Expert Group on Artificial Intelligence Set Up by the European Commission, 'A Definition of AI: Main Capabilities and Disciplines' (European Commission Report, 2019) https://www.aepd.es/sites/default/files/2019-12/ai-definition.pdf accessed 22 August 2024

- James Tobin, 'Artificial Intelligence: Development, Risks and Regulation' (House of Lords, 18 July 2023)

- Kehinde Andrews, ‘UK Banks Have a Racial Discrimination Problem. It’s Time They Admitted It’ (The Guardian, 2017) https://www.theguardian.com/commentisfree/2017/jan/13/uk-banks-racial-discrimination-black-victims-fraud accessed 22 August 2024

- Lilit Melkonyan, ‘How Big Data Is Reshaping Fintech: Open Banking’ (PLAT, March 2022) https://plat.ai/blog/big-data-reshaping-fintech/ accessed 22 August 2024

- Lerong Lu, 'Reconceptualising Fintech: Technological Innovations in International Finance, Commercial Applications and Legal Issues' (2024) 39(1) Journal of International Banking Law and Regulation 14

- Lexis Garcia, ‘The AI Paradigm Shift Is Reshaping the Tech Industry. Here's How Investors Can Capture Growth’ (Investors Daily, Feb 2024) https://www.investors.com/ibd-videos/videos/artificial-intelligence-reshaping-tech-how-investors-capture-growth accessed 22 August 2024

- Mann M and Matzner T, 'Challenging Algorithmic Profiling: The Limits of Data Protection and Anti-Discrimination in Responding to Emergent Discrimination' (2019) 6(2) Big Data & Society https://doi.org/10.1177/2053951719895805

- Nikita Aggarwal, ‘The Norms of Algorithmic Credit Scoring’ (2021) 80 Cambridge Law Journal 42

- Noble SU, *Algorithms of Oppression: How Search Engines Reinforce Racism* (NYU Press 2018)

- Oliver Wyman, ‘The Impact of AI in Financial Services’ (Oliver Wyman Report, 2023)

- OQ v Land Hessen SCHUFA Holding AG, C-634/21, ECLI-EU-C-2023-957

- R Zaman, M Hassani and BF van Dongen, 'Data Minimisation as Privacy and Trust Instrument in Business Processes' in A Del Río Ortega, H Leopold and FM Santoro (eds), *Business Process Management Workshops (BPM 2020)* (Lecture Notes in Business Information Processing vol 397, Springer 2021)

- Roger Smith, ‘Technology, The Future and Us’ [2015] 165 NLJ 7635

- Splunk, ‘The Data Age Is Here, Are You Ready?’ (Splunk, Cisco, 2023) https://www.splunk.com/en_us/pdfs/gated/ebooks/data-age.pdf accessed 22 August 2024

- Steven Dickens, ‘The Future Of Cloud Computing: AI-Powered and Driven By Innovation’ (Forbes, 2024) https://www.forbes.com/sites/stevendickens/2023/07/28/the-future-of-cloud-computing-ai-powered-and-driven-by-innovation/ accessed 22 August 2024

- UK Government, ‘A Pro-Innovation Approach to AI Regulation’ (Department for Science, Health and Technology, 2023) https://www.gov.uk/government/publications/ai-regulation-a-pro-innovation-approach/white-paper accessed 22 August 2024

- Yardena Ivanova, 'The Role of the EU Fundamental Right to Data Protection in an Algorithmic and Big Data World' in Dara Hallinan, Ronald Lens, Serge Gutwirth and Paul De Hert (eds), *Data Protection and Privacy* (Vol. 13, Data Protection and Artificial Intelligence, Hart Publishing, forthcoming)