universität wien

MASTER THESIS

Titel der Master Thesis / Title of the Master's Thesis

„The Fundamental Right to Privacy in the European Union: Shortcomings in the Face of Social Scoring"

verfasst von / submitted by

Laura Kosanke

angestrebter akademischer Grad / in partial fulfilment of the requirements for the degree of

Master of Arts (MA)

Wien, 2019 / Vienna 2019

Studienkennzahl lt. Studienblatt / Postgraduate programme code as it appears on the student record sheet:	UA 992 884
Universitätslehrgang lt. Studienblatt / Postgraduate programme as it appears on the student record sheet:	Master of Arts in Human Rights
Betreut von / Supervisor:	Dr. Ben Wagner

Acknowledgements

In sincere gratitude, I would like to thank my thesis supervisor Dr. Ben Wagner, professor of the University of Economics and Business as well as director of the Privacy & Sustainable Computing Lab at Vienna. He encouraged me in my goal to write an innovative thesis, consistently allowed this paper to be my own work, but steered me in the right direction, especially during my topic search. Special thank is dedicated to Prof. Dr. Manfred Nowak and Walter Suntinger of the *Vienna M.A. in Human Rights* at the University of Vienna. Due to their valueable criticism, my research question is expressively precise. Also, I would like to acknowlege Prof. Dr. Mark Coeckelbergh, a member of the *High-Level Independent Expert Group on Artificial Intelligence* (HLEG) established by the *European Commission* (Commission), as well as Dr. Christof Tschohl as valueable interview partners who shared their concerns regarding social scoring. Without their advice, criticism, and input, this thesis would not be as innovative and valuable as it is for academics, lawmakers, and companies.

Beyond that, I am deeply grateful for the support of my dear friends and family; they were my steadfast anchor in stressful but exciting times.

✧

This thesis is dedicated to each and every individual who strives for a privacy-friendly world where nobody is left behind.

I. Table of Contents

I. List of Acronyms and Abbreviations

AI	Artificial intelligence
Art.	Article / Articles
Charter	Charter of Fundamental Rights of the European Union
Commission	European Commission
CJEU	Court of Justice of the European Union
CoE	Council of Europe
Data Protection Directive	Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data
DPWP	Data Protection Working Party
ECHR	European Convention for the Protection of Human Rights and Fundamental Freedoms
ECtHR	European Court of Human Rights
EDPB	European Data Protection Board
EU	European Union
EP	European Parliament
e-Privacy Directive	Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector
EU Treaties	Consolidated Version of the Treaty on the European Union and the Treaty on the Functioning of the European Union
Fashion ID	Fashion ID GmbH & Co. KG
FinTech	Financial technology
FRA	European Union Agency for Fundamental Rights
GDPR	Regulation (EU) 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
NGO	Non-governmental organisation
ML	Machine learning
Race Equality Directive	Council Directive 2000/43/EC of 29 June 2000 Implementing the Principle of Equal Treatment between Persons Irrespective of Racial or Ethical Origin
Para.	Paragraph / Paragraphs
SCHUFA	SCHUFA Holding AG
SMD	Social media data
TEU	Treaty on the European Union [original version]
TFEU	Treaty on the Functioning of the European Union [original version]
Trustworthy AI	Ethics Guidelines on Trustworthy Artificial Intelligence
UDHR	Universal Declaration of Human Rights
UK	United Kingdom
UN	United Nations
UN GA	United Nations General Assembly
US	United States of America
User	Social Media User
Verbraucherzentrale	Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V.

1. Introduction

Social media is part of most people's daily lives. Lending companies process *social media data* (SMD) to assess the debtor's creditworthiness. It comprises posts, likes, and contact lists or followers; depending on the contract, users provide social scorers with publicly published data or, also, data only provided for a certain group of followers. Credit assessments based on SMD are known as social scoring. As a cornerstone of such a business model, SMD are elemental. Put differently, social scoring relies partly or fully on SMD; sometimes social scorers rely also on other data such as financial data, sometimes SMD is their only source. Past online performances are collected, stored, and analysed by algorithms that can be based on *machine learning* (ML), an application based on *artificial intelligence* (AI). This new form of credit check targets individuals with a lack of savings and credit history who are unlikely to obtain a loan from a traditional financial institution. Individuals may apply for loans based on social scoring due to existential needs based on financial shortage, in which cases, they feel urged to consent to the social scoring practices. Financial dependencies on lending companies illustrate the asymmetry of power between the social media user and social scorer. Thus, data protectionists warn against inappropriate privacy intrusions. Human rights advocates see the fundamental right to privacy[1] and intertwined rights at stake.

On the first glace, one may associate such human rights violating techniques with China. Its social scoring system regularly causes outrageous news all over the world. However, the business model has also been successfully established in the *United States of America* (US), Australia, Indonesia, Nigeria, and other countries. Social scoring is also exercised in Member States of the *European Union* (EU) such as in the *United Kingdom* (UK), Poland, and Spain.

[1] The term "fundamental right to privacy" is not directly established by any legally binding legislation by the EU. However, Art. 1 of *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data* (Data Protection Directive) indicates the right to privacy to be a fundamental one: 'Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.' Put differently, the wording "in particular" suggests that the right to privacy is a fundamental right. The *Court of Justice of the European Union* (CJEU) interprets it in this way too (see Chapter 4.2.4.1). As the right to privacy comprises multiple fundamental and other rights (see Chapter 4.2.4.1), the term "fundamental right to privacy" is consistently used to describe its overarching legal frame of the privacy regulations by the EU.

Nonetheless, the EU lags social scoring and other AI-led techniques in a global comparison: In Germany, *SCHUFA Holding AG* (SCHUFA) attempted to introduce social scoring but failed; Kreditech was more successful but only sells its social scoring algorithms abroad, for instance, in Poland. The EU's Single Market Strategy was passed to keep up with global developments. Still at its beginning of social scoring, experts need to determine the applicable legal scope and shortcomings to prevent individuals particularly from infringements in their fundamental right to privacy. There is only little information on social scoring within the EU – both from a technical and legal perspective. Against this pressing background, this thesis is dedicated to answering the following research question: **What shortcomings does the EU need to improve when safeguarding the fundamental right to privacy in the case of social scoring?**

This research question deals with an up-to-date topic that has widely been ignored by researchers and politicians. Due to the pressing need to be answered, my research question is innovative in nature. Also, the outcomes of this thesis serve as a springboard for multiple stakeholders:

- Lawmakers benefit from unrecognized loopholes to be eradicated by introducing more comprehensive laws.
- Sustainable businesses may derive their own codes of conduct preventing daily social scoring practices by maxing out legal grey zones.
- Academia can conduct in-depth research building on this thesis and derive a catalogue of best practices in social scoring.
- Independent experts may also use this thesis for monitoring a social scoring company's role model function.
- Civil society and *non-governmental organisations* (NGOs) benefit from information about individual rights as well as legal shortcomings and consequences of social scoring. On this basis, civic movements may be formed to increase pressure on lawmakers and businesses to establish more sustainable scoring methods.

In general, this paper contributes to a world where respect for privacy increases and less people are left behind.

2. Methodology

This research is qualitative in nature and, thus, based mainly on qualitative data. Information comes from primary and secondary literature. Whereas the first part refers to research articles and expert opinions, the second part rests upon EU legislation and case law. The final part builds upon research articles, expert opinions, and legislation. In detail:

i. First, I explain the key terms and the concept of social scoring.

ii. Afterwards, I define the EU's privacy frame towards the issue of social scoring. In this frame, scholarly definitions of terms related to privacy, SMD, and credit scoring further set the stage for my thesis. I also examine soft and hard EU laws shaping the fundamental right to privacy. Among other legally binding documents, applicable hard law comprises the following sources:

   a. *Charter of Fundamental Rights of the European Union*[2] (Charter);
   b. *Regulation (EU) 2016/679 of the European Parliament (EP) 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*[3] (GDPR);
   c. CJEU *Case C-210/16 Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH*[4] (Case C-210/16).

   Despite hard law documents, soft law indirectly shapes the legal scope too. Although it is non-binding by nature, its interpretations may initiate legislative changes and help to elaborate the legal scope where it is not sufficiently defined by hard law. An analysis of its impacts on lawmakers is crucial – particularly regarding the *Ethics Guidelines on Trustworthy Artificial Intelligence* (Trustworthy AI).

iii. Based on that, an answer to the research question follows: On the one hand, Chapter 4.3 relies on a literature analysis of research articles and additional expert opinions: Trustworthy AI, the Commission's statements on reviewing existing standards, and

[2] Charter (2012) OJ C 326/391.
[3] GDPR (2016) OJ L 119/1.
[4] CJEU, C-210/16, *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH*, 5 June 2018.

responses by experts to current social scoring developments are referred to. Due to the innovative character of my research, a personal, analytical contribution in form of case studies on the EU's duties to protect the outlined fundamental right are part of the chapter. In the end, in line with both my reviewing and analysing outcomes, I shall be able to uncover shortcomings of the current EU's privacy policies.

iv. Finally, a brief conclusion and outlook will complement my research.

3. Social Scoring

Mining SMD to assess a person's credit score has spread in several countries such as Australia, the US, and the UK. Start-ups of the *financial technology* (FinTech) industry offer these services. In the subchapters of Chapter 3.1, the underlying business model which uses SMD for credit scoring is elaborated.[5] Beforehand, key definitions set the basis of such a concept. General privacy risks imply general legal difficulties; concrete shortcomings in EU law will be exclusively analysed in Chapter 4.3.

3.1 Key Terms

Setting the frame for the following chapter, terms such as "processing", "SMD", "credit score", "creditworthiness", and "social scoring" are defined in Chapters **Fehler! Verweisquelle konnte nicht gefunden werden.** to 3.1.4. After describing the credit scoring mechanisms, I am going to elaborate privacy concerns researchers have already generally warned against in Chapter 3.1.6.

3.1.1 SMD

In general, data are '[f]acts and statistics collected together for reference or analysis.'[6] SMD is data mined on social media websites such as Facebook, Twitter, or LinkedIn which 'allow people to write, share, evaluate, discuss, communicate with each other'[7]. Everybody who is somehow interacting on social media leaves a digital footprint. Such a person is called *social media user* (user). Their online behaviour illustrates their interactions revealing data. Such information collected is SMD.

3.1.2 Data Processing

Analysing data requires processing. Storing, retrieving, sorting, merging, assessing, and mining data are intermediate steps to derive an output from a certain data input;[8] initially

[5] Y. Wei et al., 'Credit Scoring with Social Network Data', *Marketing Science* 35, no. 2, 2015, p. 234 (accessed 6 May 2019).
[6] 'Data' (*Lexico Powered by Oxford*) <https://en.oxforddictionaries.com/definition/data> (accessed 29 April 2019).
[7] Y. Zhang et al., 'Research on Credit Scoring by Fusing Social Media Information in Online Peer-to-Peer Lending', *Procedia Computer Science*, vol. 91, 2016, p. 169 (accessed 15 Mai 2019).
[8] 'Electronic Data Processing', (*Lawinsider*) <https://www.lawinsider.com/dictionary/electronic-data-processing> (accessed 29 April 2019).

collected data is called input, assessed data reveals a certain result that is called output. The input is processed based on a certain set of rules or values set up by one or more human programmers. This set of rules roots into an algorithm, 'a sequence of computational steps that transform the input into the output.'[9] In other terms, data processing is 'the converting of raw data to machine-readable form and its subsequent processing […] by a computer'[1]. Nowadays, machine-readable, computational data processing is conditional to derive a certain outcome, as the social scoring industry works with huge sets of data collected from social media. Thus, social scorers rely on computational assistance: Algorithms collect input, meaning a user's interaction, or, more generally, online behaviour on social media. Afterwards, it assesses the output, the so-called "credit score".

'AIs can benefit a wide-range of sectors, such as […] financial risk management'[10], the Commission states. Depending on the business model, the controller superficially double-checks the output and might go into further detail where inconsistencies occur or fully relies on the algorithmic functioning powered by AI. The scope of AI is unclear as it is not a protected term but defined in several ways. HLEG AI defines,

> Artificial Intelligence refers to systems that display intelligent behaviour by analysing their environment and taking action – with some degree of autonomy – to achieve specific goals. […] Artificial intelligence (AI) systems are software (and possibly also hardware) systems designed by humans that, given a complex goal, act in the physical or digital dimension by perceiving their environment through data acquisition, interpreting the collected structured or unstructured data, reasoning on the knowledge, or processing the information, derived from this data and deciding the best action(s) to take to achieve the given goal. AI systems can either use symbolic rules or learn a numeric model, and they can also adapt their behaviour by analysing how the environment is affected by their previous actions.[11]

When applied to social scoring, AI-led systems root into computational techniques designed by a programmer with the goal of profiling a credit applicant (see Chapter 4.1.4) to assess credit risk and creditworthiness. The outcome determines the general credit decision and the height of the interests. ML – meaning a machine capable to improve its

[9] M. Hurley and J. Adebayo, 'Credit Scoring in the Era of Big Data', *Big Data*, vol. 18, no. 1, 2017, p. 159 (accessed 21 April 2019). See also T. Cormen et al., *Introduction to Algorithms*, Cambridge, MIT Press, 2009. – Data processing was not always computational by nature. Nowadays, most data processing is electronical. It is principally based on computing or, interchangeably, processing power.[9] (C. French, *Data Processing and Information Technology*, Boston, Cengage Learning EMEA, 1996.) Credit scoring is computationally conducted. In the following, "data processing" means "electronic data processing".
[10] Commission, 'Artificial Intelligence for Europe' (*Press Release*) IP/19/1893.
[11] HLEG AI, *Ethics Guidelines for Trustworthy AI*' (*Guidelines*), p. 36.

performance –[12] is one means social scoring can root in.[13] It learns from past incomes and its outcomes for future calculations.

3.1.3 Credit Scoring, Credit Risk, and Creditworthiness

Credit scoring – also credit rating or credit assessment – is a method of analysing a person's ability to repay borrowed money. It analyses the risk whether a potential borrower can repay the credit; the terms "credit" and "loan" are interchangeably used. According to Yuejin Zhang et al.,

> [c]redit risk is the possibility of loss that the bank will suffer after offering loan to the borrowers. It includes not only the actual risk of the borrowers failing to repay the loan on time, but also the potential default risk because of the downgrade of credit or decline of repayment ability of the borrowers.[14]

The result determines the borrower's creditworthiness – a credit applicant's ability to repay the credit liabilities according to the loan agreement. Especially in the case of social scoring, the ability to repay is rather based on characteristic traits rather than prosperity. Sait Gül et al. elaborate data that potentially flow into the process of credit scoring:

> [F]inancial institutions classify borrowers for lending decision by evaluating their financial and/or nonfinancial performances. […] The fundamental task of credibility measurement is the classification of applicants into risk groups. An applicant demonstrating good characteristics with regard to repayment strength and intention is considered as a creditworthy applicant. If an applicant has bad indications, it may be seen as an uncreditworthy one. The creditworthy applicants can be sorted into many groups with different purposes, such as determining credit limits and conditions stipulated by the lender.[15]

Good characteristics improve the credit score, bad ones lower it; a more detailed definition about good and bad characteristics is part of Chapters 3.1.5.1 to 3.1.5.1. Despite the rather rough criteria mentioned in these chapters, the exact functioning of credit scoring remains vague. According to Vlad Hertza, credit scoring is generally an opaque process.[16] Pre-set values are treated like a business secret.[17]

---

[12] 'Machine Learning' (*Merriam-Webster*) <https://www.merriam-webster.com/words-at-play/what-does-machine-learning-mean accessed> (accessed 9 May 2019).
[13] HLEG AI, p. 36.
[14] Zhang et al., p. 168.
[15] S. Gül et al., 'A Multiple Criteria Credit Rating Approach Utilizing Social Media Data', *Data & Knowledge Engineering*, vol. 116, 2018, p. 80 (accessed 20 April 2019).
[16] V. Hertza, 'Fighting Unfair Classifications in Credit Reporting: Should the United States Adopt GDPR-Inspired Rights in Regulating Consumer Credit?', *NYU Law Review*, vol. 93, 2018, p. 1714 (accessed 15 April 2019); See also F. Pasquale, 'The Black Box Society: The Secret Algorithms That Control Money and Information', *Contemporary Sociology*, vol. 5, no. 3, 2016, p. 25 (accessed 29 April 2019).
[17] 'Social Scoring System: Überwachung wie in China auch bei uns?', *PSW Group Consulting Blog* [web blog] <https://www.psw-consulting.de/blog/2018/12/27/social-scoring-system-ueberwachung-wie-in-

3.1.4 Social Scoring

Social scoring falls within the category of credit scoring. Therefore, it is also not transparent. One might argue it is even less transparent because data protectionists and scientists complain about 'scarce information about how alternative credit-scoring companies […] define "creditworthiness," or how they set target variables and label classes of borrowers to serve as examples for their machine-learning processes.'[18] To give an example, SCHUFA is not obliged to reveal the functioning of its credit scoring. It is deemed to be a business secret. In 2014, the German Federal Court of Justice ruled that SCHUFA does not have to reveal its scoring algorithm. The public discussion started already in 2012 when SCHUFA announced its decision to test social scoring based on Twitter and Facebook data.

This is what is known: Social scoring is a method to process SMD for a credit scoring to determine the credit risk and creditworthiness. It is based on an individual's online behaviour on social media.[19] In the following chapters, the term "social scoring" is used wherever processing SMD is part of the credit assessment. Where a credit applicant consented to the processing of a certain set of SMD set forth in the credit agreement, the social scorer may access these SMD; depending on the contract, the scorer may assess only public SMD or also those that are private, meaning SMD shared with nobody but oneself, a selection of friends, or all friends in one's contact list. Important features to be assessed are, inter alia, the language used in posts, likes, and friends in one's contact list on social media.

3.1.4.1 Language and Emotions

In a survey, Preoţiuc-Pietro et al. discovered publicly available features such as language in tweets reveal characteristics and, thus, facilitate credit scoring based on Twitter:

> We found that the proportion of tweets using vocabulary related to fear or joy, the ratios of tweets with links and retweets as well as topics discovered in the textual content have high predictive power. We also discovered that users perceived to be female, younger, African American, with lower education level, or anxious are associated with lower rates of income. On the other hand, users with

china-auch-bei-uns/> (accessed 14 June 2019); 'Prüfung der Kreditwürdigkeit: Schufa will Facebook-Profile auswerten', *Frankfurter Allgemeine Zeitung*, 7 December 2012 <https://www.faz.net/1.1776537> (accessed 14 June 2019). See also Hurley and Adebayo, pp. 179-180.

[18] ibid., p. 173.

[19] G. Waschbusch, 'Social Scoring' (*Gabler Banklexikon*, 16 November 2018) <https://www.gabler-banklexikon.de/definition/social-scoring-99668/version-348651> (accessed 16 May 2019).

> higher income post less emotional (positive and negative) but more neutral content, exhibiting more anger and fear, but less surprise, sadness and disgust. Finally, through an analysis on user language, we were able to highlight latent topics that discriminate users with high and low income, such as politics, specific technology topics or swear words.[20]

Similarly, but focussing on content rather than emotions, Sandra C. Matz et al. proved language used on Facebook can help in determining a user's credit score. They explain,

> a person who reported to be an accountant was assigned the average income of an accountant as indicated by the Annual Survey of Hours and Earnings released by the Office for National Statistics of the UK. Consequently, this occupation-based income measure is a rather rough proxy of participants' actual income that does not capture income variations within professions (e.g. an accountant working for a major strategy consultancy is likely to have a higher income than a self-employed accountant offering advice to small and medium-sized companies).

Their study goes further and elaborates the fact that 'Facebook Likes and Status updates not only predict self-reported income with the same degree of accuracy as standard socio-economic variables, but they also added incremental predictive power.'[21] Users were predicted to have a higher income when they used "the" and other articles due to an assumed 'higher intelligence or education'[22]. However, 'self-references, such as "me," have been found more frequent among individuals who are depressed or anxious'[23]. They were considered to have a lower income. The following two clouds illustrate the correlation of language to income. Table A relates to high incomes and table B to low incomes.

Similar to Preoţiuc-Pietro et al., Matz et al. discovered more profoundly that emotions are a valuable factor in predicting a borrower's credit score: Users with high incomes express positive emotions such as "looking forward to", "thanks" or "great" as well as activities such as "shopping" and "vacation" are related to high incomes. Conversely, researchers found out:

> Low income individuals are highly self-focused (e.g. I need, I can, I got, me), use colloquial language (e.g. idk, cuz), express negative feelings (e.g. hurt, hate, bored), and use more swear words and emoticons.[24]

[20] D. Preoţiuc-Pietro et al., 'Studying User Income through Language, Behaviour and Affect in Social Media', *PLoS ONE*, vol. 10, no. 9, 2015 (accessed 9 May 2019).
[21] S. Matz et al., 'Predicting Individual-Level Income from Facebook Profiles', *PLoS ONE*, vol. 14, no. 3, 2019, p. 10 (accessed 9 May 2019).
[22] ibid., p. 5.
[23] ibid.
[24] ibid., p. 6.

Further examples are illustrated in Figure 1.[25] Matz et al. explain, '[w]ords and phrases most positively correlated with income (top) and most negatively correlated with income (bottom), after controlling for age and gender.'[26]

Figure 1) Low- and High-Income Word Clouds

[25] ibid., p. 8.
[26] ibid.

3.1.4.2 Likes or Preferences

Likes on Facebook determine one's income and, therefore, the financial ability to repay a loan. Sandra C. Matz et al. predict users who like expensive brands earn more money. Lower[27]-income users like posts referring to luxury too, however, such posts describe luxury 'in a highly abstract and generalized way'[28]. Posts also 'often contain entire phrases'[29]. Figure 3 presents some concrete examples, starting with those which most accurately predict income. The left column shows low income, the right one high income.

Low income	High income
▪ if i text a person in the same room as me, i state at them 'til they get it ▪ We act like it's a secret drug deal when someone is just giving us gum ▪ All Thinks Tumblr ▪ Funniest Pics ▪ Amazing Things ▪ Eminem ▪ Don't EVER break a pinky promise. That stuff is LEGIT. ▪ Bullet for my Valentine ▪ Dentist, Stop Talking to Me, I Cant Talk Your Hand is in my Mouth ▪ Having a "sweatpants, hair tied, chillen with no makeup on" day	▪ The Smith Center ▪ Sheets ▪ The Cosmopolitan of Las Vegas ▪ Frankie J ▪ Beauty4Moms ▪ Janie and Jack ▪ Paula's Choice ▪ It Works Skinny Wrap Team ▪ Pier 39 ▪ X Out

Figure 2) Low- and High-Income Likes

3.1.4.3 Contact Lists or Followers

Social ties predict the borrower's creditworthiness by revealing their income, reliability, and social behaviour.

> Under the assumption of homophily, the notion that people are more likely to form social ties with others who are similar to them, we show that network data provide additional information about consumers and reduce the uncertainty about their creditworthiness."[30]

[27] Matz et al. did not further define what low or high income means.
[28] ibid., p. 6.
[29] ibid.
[30] Wei et al., p. 235.

Put differently, the less wealthy social media contacts and their credit scores are, the lower the credit applicant's score. In turn, the wealthier the contacts and their credit scores, the better the score for the credit applicant.

3.1.4.4 Accuracy

While generally able to differentiate between low and high incomes, the researchers admit their 'model is not sufficiently accurate to make fine-grained distinctions between a person making $70k or $75k a year.'[31] Still, the researchers' income prediction is surprisingly precise.

3.1.5 Mixed Financial and Social Scoring

According to the motto, 'all data is credit data'[32], social scoring does not necessarily rely on SMD only. It might comprise a combination of data sets as demonstrated in Chapter 3.1.5.1. Researchers have revealed parts of the algorithmic functioning of credit scoring by the FinTech start-ups Earnest, Kreditech, Lenddo, and ZestFinance. Kreditech analyses, inter alia, likes, friends, posts on social media; Earnest relies on LinkedIn – a social network offering information on jobs, education history and other online profile data.[33] In the following, I am going to elaborate ZestFinance's and Lenddo's business models in more detail. However, there is little insight into the actual functioning of these models, for instance, what value affects the credit score to what extent.

3.1.5.1 Example: ZestFinance

ZestFinance is partners with the leading US bank and credit card issuer Discover Financial Services for AI-based solutions for credit scoring. It uses a mixture of financial and non-financial data, among them SMD –[34] a successful model as Matz et al. evaluated after comparing traditional credit scoring and a mixture of both scoring based on financial data and SMD:

> Status Updates to the socio-demographic controls increased the variance explained between 10% (when compared to education) and 16% (when compared to personality). Even when taking the most comprehensive baseline of all socio-demographic and personality variables – which together explained 18% of the variance–adding Facebook Likes and Status Updates increased variance

[31] Matz et al., p. 9.
[32] Hurley and Adebayo, p. 148.
[33] ibid., p. 166.
[34] ibid.

explained by 6% to a total of 24% (r = 0.49). Notably, the incremental accuracy was mostly driven by Status Updates, with Facebook Likes adding none or little accuracy to the baseline models.

To a certain degree, online behaviour allows one to make conclusions about, for instance, a user's personality, demographics, postcode income, education, and socio-demographics as illustrated in Figure 1 below.[35] The higher the number behind the bar, the better the prediction of a user's credit score. Likes and status updates on Facebook can assess the credit default with a probability of 43 percent. Together with traditional data such as socio-demographics, the score can even be derived with a probability of 48 per cent.

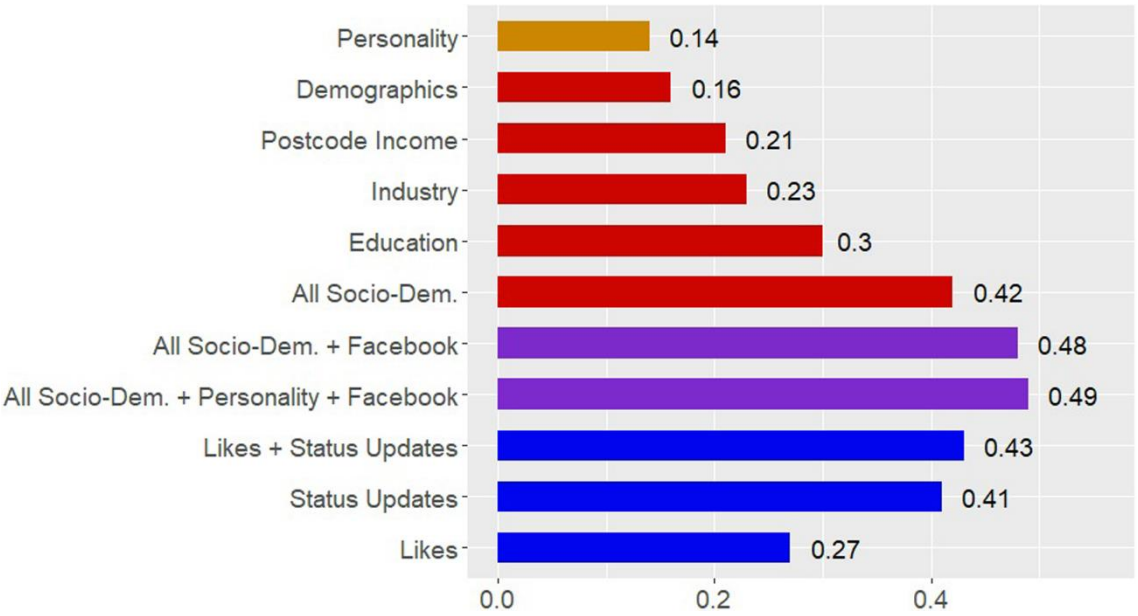

Figure 3) Product-Moment Correlations between Predicted and Actual Income

As illustrated in Figure 3, Hurley et al. elaborated three steps of ZestFinance's social scoring:[36]

(1) In the first step, the scorer needs to define their understanding of the term "creditworthiness". Hurley and Adebayo name this step 'defining the problem and specifying the specific variable'[37]. Also, important variables determining the credit score need to be set. Unfortunately, there are no more specific details on this specific

[35] Matz et al., p. 7.
[36] Hurley and Adebayo, pp. 175-176.
[37] ibid.

algorithm due to scarce information on explicit impacts and classifications of ZestFinance's understanding of creditworthiness.

(2) Afterwards, respected data needs to be collected. This data comprises social network data meaning SMD. Any 'information for any or all members of the borrower's social network' fall within the category of processed SMD.[38] Other data assessed are the applicant's data, public records, financial data, and reports from data brokers; these categories fall outside the scope of this research question; thus, I am not going to further discuss them. In the following step, collected data are transformed into a usable form for the final step.

(3) Important features are selected and, afterwards, combined into meta variables. Using different credit assessment tools, the final score can be evaluated.[39]

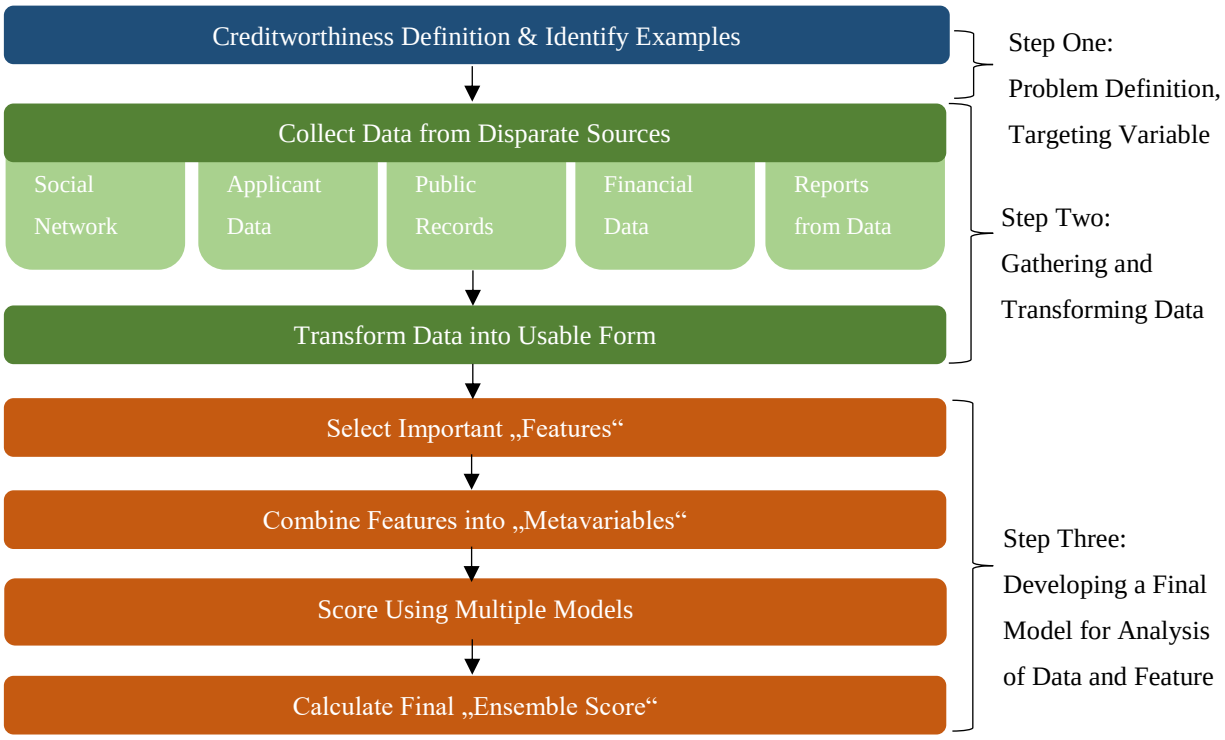

Figure 4) Three Steps of Credit Scoring Partially based on SMD

In summary, ZestFinance successfully combines traditional socio-demographic scoring practices and social scoring: Its algorithm does not only rely on personality, demographics, postcode income, industry, and education but also Facebook likes and

[38] ibid.
[39] An explanation of the models will not answer the research question; thus, I will not go into further detail.

status updates. Depending on the socio-demographics used, scientists found that the combination of both socio-demographic and social scoring increases the quality of their credit risk assessment by at least 8 per cent. Likes and status updates decrease the risk of credit default by 8 per cent.

3.1.5.2 Example: Lenddo

Lenddo offers its services on every region but Europe. The start-up gathers input from social media only.[40]

> Lenddo, reportedly assigns credit scores based on information in users' social networking profiles, such as education and employment history, how many followers they have, who they are friends with, and information about those friends […] Lenddo for instance, obtains applicants' consent to scan a variety of their online social accounts (Facebook, […] Twitter, LinkedIn […]) and sometimes also their phone activity.[41]

Besides assessing likes, language, and contact lists, the information given in the post influences the credit score. While analysing Lenddo's social scoring scheme, Wei et al. also discovered that social scoring works even better than traditional credit scoring which is based on financial data only: 'Scores can become more accurate as a result of modifications in social networks'[42]. SMD makes credit scoring more successful than traditional credit scoring. Much more information is not available, however, the above-mentioned studies of Matz et al., Hurley and Adebayo, Wei et al., D. Preoţiuc-Pietro et al., and V. Hertza indicate further mechanisms Lenddo might use to conduct social scoring.

3.1.6 General Concerns

Academics, data protectionists, and human rights advocates have raised concerns regarding techniques of social scoring. They might not only infringe upon a person's privacy but also discriminate against persons due to systematic flaws, data inaccuracy, and a lack of transparency. Also, due to a lack of transparency, it is unsure who is accountable for possible flaws. In the following subchapters, I am going to deal with these critiques in more detail.

---

[40] Wei et al., p. 234.
[41] ibid., p. 235.
[42] ibid., p. 234.

3.1.6.1 Transparency

As credit scoring mechanisms are not transparent, Wei et al. raise concerns about 'serious problems of transparency. Consumers have limited ability to identify and contest unfair credit decisions, and little chance to understand what steps they should take to improve their credit.'[43] Little about the algorithms is known. Algorithmic mechanisms are opaque; only presumptions can be made on their functioning. Nobody other than the credit scorer knows about the consequences of a certain set of data; even the credit scorer might not have a full insight into the functioning of their scoring algorithms due to ML.

3.1.6.2 Non-Discrimination

An opaque system can intentionally or unintentionally hide discriminatory values in the algorithmic scheme; unintentionally due to underlying stereotypes developing in discriminatory patterns or intentionally because there is no law to reveal one's social scoring algorithm and knowingly resorting to discriminatory mindsets. In the US, discrimination by a Facebook tool for social scoring was already discussed in the media. Journalist Robinson Meyer, writing for *The Atlantic*, informed his readers about Facebook securing an US patent to analyse one's list of friends for credit scoring. The document says,

> [w]hen an individual applies for a loan, the lender examines the credit ratings of members of the individual's social network who are connected to the individual through authorized nodes. If the average credit rating of these members is at least a minimum credit score, the lender continues to process the loan application. Otherwise, the loan application is rejected.[44]

In other words, if banks apply this practice, credit applicants are judged by their contacts instead of their personal and independent capability to repay the loan. 'It seemed straight out of the evil-tech-company playbook. […] [B]anks would deny mortgages to people because they lived in neighbourhoods that were to black'[45], Meyer fears. Those who live

[43] Hurley and Adebayo, p. 149.

[44] C. Lunt, 'United States Patent: 9100400 - Authorization and Authentication Based on an Individual's Social Network', (*United States Patent*, 4 August 2015) <http://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO1&Sect2=HITOFF&d=PALL&p=1&u=%2Fnetahtml%2FPTO%2Fsrchnum.htm&r=1&f=G&l=50&s1=9100400.PN.&OS=PN/9100400&RS=PN/9100400> (accessed 21 Mai 2019).

[45] R. Meyer, 'Could a Bank Deny Your Loan Based on Your Facebook Friends?', *The Atlantic*, 25 September 2015, https://www.theatlantic.com/technology/archive/2015/09/facebooks-new-patent-and-digital-redlining/407287 (accessed 22 Mai 2019).

in a Black area and, logically, most likely have more Black friends obtain a lower score. Evidence was delivered by Matthew A. Bruckner:

> African Americans tend to have lower incomes [, less wealth,] and lower credit scores than white Americans. If a borrower's application or pricing is based, in part, on the creditworthiness of her social circles, that data can lead to [unlawful] discrimination against minorities compared to white borrowers with the same credit scores.[46]

Like Bruckner and Meyers, Wei et al. warn against discriminatory practices, even if conducted without any intention to discriminate against credit applicants:

> Big-data tools [such as those for social scoring] may also risk creating a system of "creditworthiness by association" in which consumers' familial, religious, social, and other affiliations determine their eligibility for an affordable loan. These tools may furthermore obscure discriminatory and subjective lending policies behind a single "objective" score. Such discriminatory scoring may not be intentional[.][47]

Using tools such as contact lists or preferences, scorers can easily determine a person's religious or social background and, on this basis, discriminate against them.

3.1.6.3 Accuracy

Generalizations such as living in a Black neighbourhood or having Black friends do not lead to a qualitative credit assessment. Individuals are different, as such, one cannot derive pre-set values without individually examining them. Such features lead to inaccurate data because generalizations of certain groups make it impossible to assess the individual character but, instead, rely on the average expectation for the whole group.

These concerns can also lead to manipulation of social media accounts by their users to improve their credit score. They trick the system by letting the social scorers minimize their freedoms to like and share information on them with friends and followers. Additionally, people might start selecting contacts: They might delete old real-life friends but send friendship invitations to persons they consider having a good credit score. Such practices influence one's private life because of the social scoring system. Wei et al. found proof of this assumption. They investigated

> how the accuracy of social network-based scores changes when consumers can strategically construct their social networks to attain higher scores. We find that those who are motivated to

[46] L. Saunders, *Email from Lauren Saunders to Laura Temel*, cited in M. Bruckner, 'The Promise and Perils of Algorithmic Lenders' Use of Big Data', *Chicago-Kent Law Review*, vol. 93, no. 1, 2018, p. 28 (accessed 14 June 2019) [insertion by the author]. See also Email from Lauren Saunders to Laura Temel (30 September 2015) <https://www.nclc.org/images/pdf/rulemaking/treasury-marketplace-loan-comments.pdf> (accessed 14 June 2019).
[47] Hurley and Adebayo, p. 149.

> improve their scores may form fewer ties and focus more on similar partners. The impact of such endogenous tie formation on the accuracy of consumer scores is ambiguous.[48]

For obtaining a credit, they adjust to the process and give up their freedom of expression and private life due to the contacts' selection.

3.1.6.4 Systematic Flaw

Sait Güla et al. discovered that 'credit ratings tend to decrease when SMD is considered.'[49] Their study investigates the mechanisms of credit assessments partly based on SMD collected from Twitter. The follower growth rate as well as positive or negative sentiments influenced the score. This is because of Twitter – a platform known for rather negative news and emotions;

> microblog sites like Twitter are used as a complaint platform mostly sharing negative emotions and reports of situations which caused dissatisfaction. This fact should be considered while benefitting from social media data in credit rating approaches. On suggesting such a new method, we are aware of the necessity of comparing the results with the current ones.[50]

Negative tweets – although it is part of Twitter's complain culture – decrease the credit score. Of course, these are legal persons and not individuals. However, when already existing for companies, the step in the direction of increasing individual social scoring is even smaller.

In short, the lack of transparency in social scoring systems – intentionally or not – leads to an inaccurate assessment of an individual's credit score; it might be based on discriminatory values or systematic flaws based on false assumptions, for instance, insufficient generalizations regarding Twitter analyses. Both arguments are closely related to each other as discriminatory values stem from stereotypes which are based on generalizations.

3.2 Concluding Remarks

Chapter 3 described the basics of social scoring – processing SMD for evaluating the credit applicant's credit risk, creditworthiness, and, finally, credit score. Scarce information is published on algorithmic calculations and its pre-set values. Compared to those, SMD of the individual is analysed and categorized for the credit decision. Pre-set

[48] Wei et al., p. 134.
[49] Gül et al., p. 80.
[50] ibid., p. 97.

values comprise the applying user's language in posts, preferences, and online contacts or followers.

Unfortunately, there is a lack of information about concrete social scoring techniques, the underlying algorithmic values and other factors influencing the system, for instance, machine-learning. Academia has only scarce information on few social scoring business models. So far, scientists have revealed certain features that influence a person's credit score. The above-presented results lead to the following conclusions:

(a) Language and emotions: The more self-centred a post, the more negative the emotions expressed, and the more abstract expressions about luxury, the lower the credit score. On the other hand, the more rational a post, the happier the emotions expressed and the better the sentence structure, the higher the score;

(b) Likes: The poorer a joke a person likes, the lower their credit score. Also, users who like posts that abstractly refer to luxury have a lower score. Contrastingly, the more concrete the luxury brands liked, the better the score.

(c) Contact lists or followers: Users with a contact lists comprised of friends from a poor neighbourhood receive a lower credit score. Those who carefully choose their friends, for instance, evaluating their stance in society and prosperity, have a higher score.

This list bears no claim of being exhaustive but just touches the tip of the ice-berg; logically, one cannot claim for these data to be comprehensively reliable. For this reason, the above-mentioned information needs to be assessed carefully and cannot serve as a generalization for social scoring in general. The above bullet points describe a few indicators used to calculate a rough income, but do not explain applied values and further details on why and what degree the score changes. Put differently, research is unable to elaborate which exact pieces of SMD lead to scores.

Nevertheless, these indicators allow for conclusions on general risks and legal shortcomings lawmakers need to consider in legislation. General risks to be discussed are as follows:

i. Lacking transparency on social scoring: Due to little publicly accessible information, no party other than the social scorer knows what data is used which leads to what conclusion; maybe not even the scorer knows about it due to machine-learning that improves its system based on huge sets of data. Flaws can hardly be discovered –

except they are evident in the initial set of values directly determined by the programmer.

ii. Lacking accuracy in data: Values are based on generalizations which make it difficult to assess individual credit applicants and, therefore, might incorrectly calculate the credit risk.

iii. Discriminatory sets of values: Pre-set assumptions on, for instance, that Black neighbourhoods are less prosperous than White ones, is considered a discrimination in international law. More generally, evaluating a person's language, preferences, and contact list most probably reveals a person's race, colour, sex, language, religion, and social origin. A decision made on these characteristics is a decision based on protected grounds in international law; discriminatory decisions based on these are prohibited.[51]

iv. Systematic flaws: Twitter is known for tweets expressing negative emotions.[52] This is why emotions expressed on Twitter should not be a basis for scoring one's creditworthiness.

Such problems do generally exist in countries where social scoring is allowed and practiced. "The increasingly global nature of the financial services industry makes it necessary to comprehensively address international data security and privacy regulations"[53], Daniel Gutierrez claims. It is important to assess and legally minimize risks. Focussing on EU law, this thesis innovatively analyses legal loopholes or shortcomings in the face of emerging social scoring within the EU – a topic that has so far been widely ignored among academics. Focuses of this research include preventing a lack in transparency, data inaccuracy, discrimination, and systematic flaws which have been touched upon in Chapter 3.1.6. In Chapter 4.2, I need to elaborate the fundamental right to privacy as well as related rights. Whether the above-mentioned risks affect the EU and set privacy and anti-discrimination laws at risk will be discussed in more detail in Chapter 4.3. Also, further loopholes will be revealed.

[51] International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171, Art. 4.

[52] In this light, it would be interesting to evaluate accounts of politicians regularly complaining in a simple, emotional language.

[53] D. Guitierrez, 'Inside Big Data. Guide to Big Data for Finance', *Dell EMC*, White Paper, 2015, p. 4 (accessed 30 April 2019).

4. EU: Social Scoring and Privacy Regulations

In the EU, the financial market has not been taken over by social scoring yet. The FinTech market is thriving due to globalisation. EU-based FinTech have spread their business for almost a decade. The market will grow within the EU. For instance, the United Kingdom (UK) has revolutionised the lending sector with recent 'UK legislation facilitating the credit scoring of small and medium-sized enterprises'[54]. Private debtors may borrow money from online companies such as (a) MyBucks, (b) FriendlyScore, and (c) Big Data Scoring. Their business models are as follows:

(a) The Luxembourg-based company MyBucks has lent money based on social scoring assessments since 2011. It operates in two continents: Africa and Australia. Its business motto reads '[o]ur digital lending channels use Artificial Intelligence algorithms that can credit-score customers who has never been banked before.'[55] The FinTech company targets potential debtors who would not obtain a traditional bank loan, among other features, based on their financial records and credit history. MyBucks portraits 'behavioural traits'[56] via evaluating SMD – according to CEO Tim Nuy, the more the better. MyBucks' social scoring algorithm also gathers data from cell phones: 'Very active social media accounts are likely to be real people, and we make sure the information on the cellphone and the social media account tie together.'[57] After collecting SMD, it predicts a client's future debt default.[58]

(b) The London-based scorer FriendlyScore has conducted social scoring since 2013. It is present in European countries such as in Poland, Africa, Latin America and Asia.[59] Debtors need to select what data they choose to share; FriendlyScore asks for access to the following:

---

[54] J. Marriott and G. Robinson, 'To Score and to Protect? Big Data (and Privacy) Meet SME Credit Risk in the UK', *International Data Privacy Law*, vol. 7, no. 1, 2017, p. 48 (accessed 13 April 2019).
[55] 'Empowering Through Lending' (*MyBucks*) <https://corporate.mybucks.com/lending> (accessed 30 April 2019).
[56] P. Crosman, 'This Lender Is Using AI to Make Loans through Social Media' (*American Banker*, 28 December 2017) <https://www.americanbanker.com/news/this-lender-is-using-ai-to-make-loans-through-social-media> (accessed 30 April 2019).
[57] ibid.
[58] 'Artificial Intelligence' (*MyBucks*) <https://corporate.mybucks.com/technology> (accessed 30 April 2019).
[59] 'About Us' (*FriendlyScore*) <https://friendlyscore.com/about> (accessed 30 April 2019).

- **Social media accounts** to check your activity, friends and followers
- **Photographs** to verify your person
- **GPS location** to verify your home address and place of work
- **Device** details like type of Mobile your use
- **Family and friends** to use their creditworthiness to help yours
- **Bank details** wherever your bank account is in the world.[60]

Although credit applicants may choose which data they willingly share, FriendlyScore lays an emphasis on their promise that reads

> the more we will know about you, […] the higher your score can be. […] Nothing you share goes against you. When you share access to your personal information with us, most of the data we analyse is to prove you are who you say you are, and this will only ever improve your credit score, never lower it. So don't be worried about anything you post on social media negatively affecting your score – this simply won't happen. Plus all of the analysis is done by machines, with no human looking at any data.[61]

After an AI-led social scoring procedure that lasts 'a few seconds'[62], applicants receive an offer for a loan.

(c) The Estonia-based company Big Data Scoring has conducted social scoring since 2013. It has launched 'the first ever credit scoring model for European markets which is based purely on social media.'[63]

This list is not exhaustive. There are more EU-based companies conducting social scoring outside or even within the EU. Due to globalisation, more social scorers will process SMD for credit assessments within the EU. This is the reason why the research question of what legal shortcomings the EU faces regarding social scoring must be answered. It is an innovative answer and provides lawmakers, academics, activists, and, in general, civil society with important information on regulations to be better defined or passed.

Against this background, Chapter 4.1 provides a historical and definitional scope of the fundamental right to privacy. Chapter 4.2 provides a legal frame including the most important provisions – quoted mostly verbatim to be as precise and accurate as possible.

---

[60] 'Free Credit Scores. Check and Report' (*Friendly Score*) <https://friendlyscore.com/> (accessed 30 April 2019).
[61] 'Fast, Free and Easy Credit Scores' (*Friendly Score*) <https://friendlyscore.com/individuals/fast-free-and-easy-credit-scores> (accessed 14 June 2019).
[62] ibid.
[63] 'World's First Social Media Credit Scoring Model Launched for Europe' (*Big Data Scoring*) <https://www.bigdatascoring.com/press-release-worlds-first-social-media-credit-scoring-model-launched-for-europe> (accessed 30 April 2019).

Sources comprise primary[64], secondary[65], and supplementary[66] law. In addition, definitions and opinions by experts and academics are consulted which embed the cited EU privacy laws. Finally, Chapter 4.3 presents the EU's legal shortcomings in the face of social scoring and with reference to general risks mentioned in Chapter 3.1.6.

4.1 Key Terms

Before analysing loopholes in the EU's privacy regulations, I am going to set the operational basis by defining the key terms which privacy legislation[67] relies on. Giving a general understanding of the evolution of privacy rights helps to understand the bigger picture of the EU's legal provisions. First, I will briefly summarize the evolution of an overall "privacy" understanding that might help to understand the EU's "privacy" definition. Secondly, I am going to explain legal terms according to the EU's definitions of "personal and sensitive data", "data processing", and "profiling". These terms are crucial for the legal understanding of the legal privacy framework.

4.1.1 Digression: The Evolution of the Term "Privacy"

The evolution of an understanding of "privacy" began before the founding of the EU. To summarize its evolution is important in order to gain a better understanding of the term "privacy", which is not satisfyingly defined in EU or international law. Before EU

[64] Primary law, also known as primary sources, is 'comes mainly from the founding treaties'. (EU, 'The European Union's Primary Law' (*EUR-Lex*, 21 March 2018) <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM:l14530> (accessed 2 April 2019.) Other sources are amending and accession treaties, protocols annexed, or supplementary agreements amending specific sections of these legal documents.

[65] Secondary law can be divided into two categories of treaties: (1) Unilateral acts of both regulations, directives, decisions, opinions, and recommendations as well as atypical acts such as communications, recommendations; (2) conventions and agreements and interinstitutional agreements that affect the EU. In this paper the first category matters the most. (EU, 'Sources of European Union Law' (*EUR-Lex*, 13 December 2007) <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM%3Al14534> (accessed 25 April 2019).)

[66] Supplementary law consists of general principles of law, international law, and the CJEU's case law. It is 'non-written sources by European law […] used by the CJEU as rules of law in cases where the primary and secondary legislation do not settle the issue.' (EU, 'The Non-Written Sources of European Law: Supplementary Law' (*EUR-Lex*, 12 March 2018) <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM:l14533> (accessed 23 April 2019).) It may legally bindingly interpret EU law to fill out gaps in existing primary and secondary law.

[67] According to the HLEG AI, '[t]he law provides both positive and negative obligations […] but also with reference to what should be done and what may be done. The law not only prohibits certain actions but also enables others.' (HLEG AI, p. 6.) Positive law enables individuals, the right-holders, to possess or exercise a right. In turn, a negative right prohibits something, for instance, to invade another individual's privacy.

legislation could start to protect an individual's privacy, a certain zeitgeist needed to develop to derive the term "privacy" from the need for it. This spirit developed ever since Samuel Warren and Louis Brandeis voiced their zeitgeist in 1890. They claimed privacy suffered from unauthorized interferences by modern enterprises leading to mental pain and distress and worse than that of a bodily injury. The importance of the individual's protection was put in the centre. Through the craving for solitude, the claim for a right to privacy emerged. If entitled to legal protection, it must prevent invasions and 'is merely an instance of the enforcement of the more general right of the individual to be let alone.'[68] Accordingly, an individual's privacy is rooted in individual experiences when let alone from outside interferences. This is a negative obligation which means it is interpreted with reference to what cannot be done.[69] Framing the zeitgeist of their era, Warren and Brandeis urge to periodically verify the law, inter alia, due to the fast-moving information sector.

Another important definition of "privacy" was framed by Marek Safja, former President of the Polish Constitutional Tribunal. He defined, it is a

> the right to exclusively control this area of life that does not concern others, and in this area, freedom from the curiosity of others is a specific *sine qua non* condition for the free development of an individual[.][70]

This definition serves as the essence of the privacy regulations: An individual can decide which private information may be free from any intrusion. The right is not absolute; lawful limitations protect the privacy of others and protect public interests.[71] Privacy claims need to be carefully balanced with other rights of the data subject or others.

Yet, the privacy legislation is globally established in soft law *Article* (Art.) 12 of the Universal Declaration of Human Rights (UDHR):

---

[68] S. Warren and L. Brandeis, 'The Right to Privacy', *Harvard Law Review*, vol. 4, no. 5, 1890, p. 205 (accessed 15 April 2019).
[69] HLEG AI, p. 6.
[70] A "sine quo non" condition indicates a indispensable provision for achieving a certain goal, in this case 'for the free development of an individual'. (M. Safjan cited by M. Krzysztofek, *GDPR: General Data Protection Regulation (EU) 2016/679: Post-Reform Personal Data Protection in the European Union*, Köln, Kluwer, 2018, p. 10. See also 'Condition Sine Qua Non' (*Collins*) <https://www.collinsdictionary.com/dictionary/french-english/condition-sine-qua-non> (accessed 7 June 2019).)
[71] Krzysztofek, p. 10.

> No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.[72]

Freedom from any intrusion is also the core piece of the early idea of the "right to be let alone".

In 1960, the interpretation of "privacy", or rather privacy infringements, was also substantially influenced and expanded by William Prosser. He defined four characteristics of what privacy should be protected against: (1) intrusion into one's seclusion, solitude, or private affairs, (2) disclosure of embarrassing information, (3) defamation, and (4) appropriation of one's name or likeness.[73] Put simply, privacy comprises the possibility to cut off ties with the outside world, to keep information personal, to be free from slander, and to keep one's name to be free from misuse by any other party.

Put briefly, the term "privacy" has been used for approximately 130 years. Important steps were made by Warren and Brandeis, by Safja, the UDHR, and Prosser. There is no direct indicator that one of these events has influenced the EU's privacy legislation. However, it would not be shaped the way it is without Warren and Brandeis initial branding. I believe that historical developments build upon each other; as such, this digression gives insights into the definitional scope of "privacy". Key features are the ability to include or exclude the outside world from one's intimate, private moments. Two more features involve the freedom from slander, defamation and misuse from one's personal attributes such as one's name or, in general, personal and sensitive data.

4.1.2 Personal and Sensitive Data

According to EU law, personal data are defined by two criteria: (1) They relate to human beings and (2) enable an identification or even identify the person. Put differently, the ability to identify a data subject based on their data makes data personal; the person being identified by the data is called "data subject".[74] Personal information does not include

[72] UN GA Res 217 A, Art. 12.
[73] W. Prosser, 'Privacy', *California Law Review*, vol. 48, no. 3, 1960, p. 389; GDPR (2016) OJ L 119/1, Art. 4(1).
[74] Y. Poullet, 'Is the General Data Protection Regulation the Solution?', *Computer Law & Security*, vol. 34, 2018, pp. 773, 776 (accessed 18 June 2019).

information on a professional entity or so-called "legal persons"[75]. Natural persons who act on behalf of legal persons are protected by law.[76]

Under EU law, 'the scope of personal data is open-ended'[77]. A small piece of information may be sufficient to identify a person and upgrades that piece of information to personal data.[78] In specific circumstances generic data may become personal.

> For instance, information on a person's account balance is neutral, but when the amount is very high and unique in a community served by a local bank, it may be associated clearly with a specific member of that community.[79]

Similarly, the CJEU proclaimed in several cases that even when information does not directly relate to a person but can identify a person, it is considered to be indirectly identifying a person; such information are indirect personal data.[80] Similarly Data Protection Officer Mariusz Krzysztofek states, 'no category of information relating directly or indirectly to a natural person is "personal data" by its mere nature'[81]; no category of isolated data might necessarily identify a person. If data is not related to a person, privacy is always sufficiently respected – 'different people may have the same first name and surname and their identification may require the addition of other data, e.g. age.'[82] Biometric data such as iris scans have become increasingly important to identify a person in the digital age and are considered personal data.[83]

"Sensitive data" falls under the category of "personal data". It reveals an individual's racial or ethnic origin, political opinions or affiliations, trade union membership, religious or other beliefs, health status, or sexual life.[84]

---

[75] A legal person is 'an organisation or group of people who have (some of) the legal rights and responsibilities of an individual under the law.' ('Legal Person' (*Wordnik*) <https://www.wordnik.com/words/legal%20person> (accessed 30 April 2019).)
[76] ibid.
[77] Krzysztofek, p. 25.
[78] ibid.
[79] ibid.
[80] See CJEU, C-131/22 (2014), *Google Spain vs. Agencia Espanola de Protecctión de Datos*, 13 May 2014; CJEU, C-212/13, *Rynes vs. Urad*, 11 December 2014; CJEU, C-362/14, *Schrems vs. Data Protection Commissioner*, 6 October 2015.
[81] Krzysztofek, p. *25.*
[82] ibid.
[83] *IP* (FRA) and *Freedoms and Council of Europe* (CoE), *Handbook on European Data Protection Law*, EU, 2014, p. 40 (accessed 30 April 2019).
[84] Directive 95/46/EC of the EP and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (1995) OJ L 281, Art. 8.

In short, personal data are data that can identify an individual based on information and circumstances allowing an identification. Sensitive data fall within the category of personal data revealing race, ethnicity, trade union membership, political opinions or affiliations, beliefs, health status, or sexual life.

4.1.3 Data Processing and Responsibilities

The EU's legal definition of "processing" defines processing activities as 'operations performed upon personal data, in whole or in part by automatic means'[85]. Going one step further, processing personal data is any operation

> such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction performed upon personal data. The term "processing" also includes actions whereby the data leave the responsibility of one controller and are transferred to the responsibility of another controller.[86]

A decision maker for processing is a "controller"[87] who works as a single party or in a merger of more than one party, meaning as "joint controllers". More information will be given in Chapters 4.2.6.3.1 to 4.2.6.3.2.

On behalf of the controller, the "processor" – 'a natural or legal person, public authority, agency or other body' – processes personal data. A controller is 'the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data'.[88] Only in the case when the processor uses processed data for their own concern, the processor becomes a controller. Whoever receives data from the controller is referred to as a "recipient". Persons of a natural or legal character – distinct from the data subject and who do not act on behalf of the controller – are a third party and become a third-party recipient when they are separate from the controller but receive personal data from them.[89] A third party is '[a] natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data'[90]. In the case of cookies used for

[85] FRA and CoE, p. 46.
[86] ibid., pp. 47-48.
[87] GDPR, Art. 4(7).
[88] Data Protection Directive, Art. 2(e).
[89] ibid, p. 48.
[90] GDPR, Art. 4(10).

marketing purposes, data sets can be processed by the website providers themselves but can also be shared with third parties for their marketing purposes.

These definitions seem to be quite comprehensive, however, Krzysztofek states, indeed, a comprehensive definition of processing is not feasible due to changing technologies and, thus, remains open ended.[91]

4.1.4 Profiling and Automated Decision-Making

As the *European Data Protection Board* (EDPB) elaborated, profiling and automated decision-making are conducted in the banking and financal sector. For the first time ever, the EU broadly defined "profiling" in the GDPR.[92]

> [P]rofiling means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements[.][93]

The *Data Protection Working Party* (DPWP) states, '[t]he use of the word "evaluating" suggests that profiling involves some form of assessment or judgement about a person.'[94] This might be a credit assessment evaluating the economic situation based on personal preferences, interests, reliability, location, and – the most important factor – online behaviour. It is based on a profiling procedure that uses data about an individual from social media profiles or other social media sources. The EDPB gives further definition: '[p]rofiling is a procedure which may involve a series of statistical deductions […] based on the qualities of others who appear statistically similar.'[95] If person A has been scored already, scoring person B with similar character traits and social roots will be faster due to data that has already been calculated for person A. Using huge sets of data such as SMD makes it easier to compile profiles for social scoring. Social scoring controllers advocate for such practices to

> potentially allow for greater consistency or fairness in the decision making process (e.g. by reducing the potential for human error, discrimination and abuse of power); reduce the risk of customers

[91] Krzysztofek, pp. 24-29.
[92] More detailed information follows in Chapter 4.2.6.
[93] GDPR, Art. 4(4).
[94] DPWP, 'Guidelines on Automated Individual Decision-Making and Profiling for the Purpose of Regulation 2016/679' (*Guidelines*, 3 October 2017) WP251rev.01, p. 7.
[95] ibid.

> failing to meet payments for goods or services (for example by using credit referencing); or enable them to deliver decisions within a shorter time frame and improve efficiency.[96]

Automated decision-making reduces the workload for the social scoring company and the processing power of the computer used.

The EU classifies "profiling" into two categories: Art. 4(4) refers to 'any form of automated processing'[97] which is either (a) 'solely'[98] automated or (b) 'involve[s] some form of automated processing – although human involvement does not necessarily take the activity out of the definition.'[99] Although profiling may be done without automated means and automated decision-making is not necessarily related to profiling, automated decisions may be based on the profile of individuals based on 'derived or inferred data such as a profile of the individual that has already been created (e.g. a credit score).'[100]

The EDPB differentiates between three ways in which profiling may be used: There might be '(i) general profiling; (ii) decision-making based on profiling; and (iii) solely automated decision-making, including profiling, which produces legal effects or similarly significantly affects the data subject.'[101] In case of social scoring, at least (ii) and (iii) are used in the FinTech industry, as SMD are gathered and evaluated at least partly electronically by an algorithm. In the case of (ii), 'a human decides whether to agree the loan based on a profile produced by purely automated means'[102]. In the case of (iii), 'an algorithm decides whether the loan is agreed, and the decision is automatically delivered to the individual, without any prior and meaningful assessment by a human'[103]. In the case of solely automated processing, the EU passed further legal safeguards which will be elaborated upon and discussed in Chapter 4.2.6.

In summary, profiling includes huge sets of data social scoring controllers cannot gather and analyse themselves correctly and in a comparable speed as the AI-led system can. Social scoring roots into either partly or fully automated decision-making based on profiling conducted on SMD by the credit applicant. Personal data are the main feature

[96] ibid, p. 13.
[97] GDPR, Art. 4(4).
[98] ibid.
[99] DPWP, 2017a, pp. 5-7.
[100] ibid, p. 8.
[101] ibid.
[102] ibid, p. 9.
[103] ibid.

to be processed for determining credit risk, creditworthiness, and credit score. Such automated AI-led decisions based on profiling bear 'the potential to significantly impact individuals' rights and freedoms.'[104]

Concluding Chapter 4.1, it is evident that social scoring has entered the EU's financial market: FinTech start-ups such as MyBucks and FriendlyScore are EU-based credit scorers that, for now, provide their services outside of Europe but soon might provide them inside of Europe as well. Big Data Scoring has even launched the first credit scoring model for European markets purely based on social media. Such techniques affect at least the credit applicant's privacy. Against this background, this chapter provided the historical and definitional scope of the fundamental right to privacy. Historically, the term "privacy" was created in 1890 by Warren and Brandeis. The following most important privacy developments were initiated by Safja, the UDHR, and Prosser. The historical definition of the "privacy" comprises the ability to participate in and withdraw oneself from the outside world as well as the freedom from slander, defamation and misuse of one's personal and sensitive data. Although there is no direct connection to the EU's legal privacy framework, I believe historical developments build upon each other. Therefore, I believe historical privacy developments influenced EU law. To give an example, the right to be left alone is similar or equal to the right to seclusion dealt with in Chapter 4.2.2.1. EU law protects the processing of personal data, meaning data that enables companies to identify an individual. Sensitive data falls within the category of personal data; it reveals an individual's racial or ethnic origin, political opinions or affiliations, trade union membership, religious or other beliefs, health status, or sexual life. Connecting this introduction with the scope of the research question, personal data is the only source to be processed for social scoring which conducts automated profiling of the credit applicant based on its social media user data.

Chapter 4.2 elaborated the EU's legal privacy framework in more detail including respective legal sources.

[104] ibid, p. 5.

4.2 Legal Framework

In laying down the EU's scope of the fundamental right to privacy, one must refer to primary, secondary, and supplementary law[105]. The following list entails the most important and recent soft and hard documents dealing with privacy issues that are related to social scoring:

- *Consolidated Versions of the Treaty on the Functioning of the European Union* and the *Treaty of the European Union* (EU Treaties);
- *Convention for the Protection of Human Rights and Fundamental Freedoms* (ECHR) The ECHR was passed by the Council of Europe (CoE)[106];
- *Council Directive 2000/43/EC of 29 June 2000 Implementing the Principle of Equal Treatment between Persons Irrespective of Racial or Ethical Origin* (Race Equality Directive);
- Charter;
- *Directive 2002/58/EC of the EP and of the Council of 12 July 2002 concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector* (e-Privacy Directive);
- GDPR;
- Trustworthy AI.

4.2.1 EU Treaties

The EU Treaties formed the basis for the first legal protections against privacy intrusions. This comprises the most important treaties shaping the EU, consolidated on 7 June 2016, and comprise the following documents:

- Treaty on the European Union;[107]

[105] TEU, TFEU, and the Charter are approved by all EU Member States and considered as primary EU law. Regulations, directives, and decisions by the EU adopted by the EU institutions are secondary EU law. (FRA and CoE, p. 17.)

[106] As the EU is a contracting partner, the ECHR counts one of its most crucial legal documents regarding fundamental rights and freedoms such as the fundamental or human right to privacy. (ECtHR, 'Accession of the EU' (*ECtHR*) <https://www.echr.coe.int/Pages/home.aspx?p=basictexts/accessionEU&c=> (accessed 7 June 2019).)

[107] In its original version, the *Treaty on the European Union* (TEU) – also known as *Maastricht Treaty* – was signed on 7 February 1992 and entered into force on 1 November 1993. It established a pillar structure that was enact until the Treaty of Lisbon entered into force. Also, it introduced the creation of a shared European currency, the euro. Both topics lay outside the scope of this thesis. (See 'Treaty on the European

- Treaty on the Functioning of the European Union;[108]
- protocols;
- Annexes to the Treaty on the Functioning of the European Union;
- Declarations annexed to the Final Act of the Intergovernmental Conference which adopted the Treaty of Lison, signed on 13 December 2007;
- tables of equivalences.

It is directly applicable – meaning it is binding to and in every EU Member State without any exception.[109]

4.2.1.1 Right to the Protection of Personal Data

The treaty explicitly prescribes the right to the protection of personal data of an individual: 'Everyone has the right to the protection of personal data concerning them.'[110] However, this provision is not absolute and thus can be limited. The CJEU allowed the right to personal data protection to be restricted, if 'data disclosure is necessary for the aim pursued by the legislator'[111] and

> such limitations are provided for in statutory regulations or regulations issues on the basis of a statute, and only to the extent necessary to achieve the purposes specified […] such as public security.'[112]

Union (TEU)/ Maastricht Treaty' (*EP*) <http://www.europarl.europa.eu/about-parliament/en/in-the-past/the-parliament-and-the-treaties/maastricht-treaty> (accesses 7 June 2019).)

[108] The original Treaty on the *Functioning of the European Union* (TFEU) – also referred to as the *Treaty of Rome* – was signed on 25 March 1957 and entered into force on 1 January 1958. It shapes the constitutional basis of the European Union and counts as a founding treaty. (See 'Treaty on the Functioning of the European Union' (*EP*) <http://www.europarl.europa.eu/about-parliament/en/in-the-past/the-parliament-and-the-treaties/treaty-of-rome> (accessed 7 June 2019).)

[109] Krzysztofek, p. 11.

[110] EU Treaties (2008) OJ C115/13, Art. 16(1).

[111] Krzysztofek, p. 14.

[112] The CJEU case in question – *Case C-28/08 Commission v. Bavarian Lager of 29 June 2010* – dealt with the management of public funds and, after an internal proceeding dealing with the disclosure of the meeting's minutes, came to court due to an only restricted disclosure of personal data of the participants names who were responsible for the voting of public funds for a German brewery. Under the principle of transparency, diverging rights were the right to access to documents of the institutions, bodies, offices and agencies of the Union, regardless of their form, which is not absolute, and the right to data protection, if access to documents would reveal personal data of others. In conclusion, where public documents entail personal information, the fundamental right to privacy needs to be reconciled with several provisions on a case-by-case basis. Regarding the case, the Bavarian Lager complained about difficulties in importing German beer to the United Kingdom because the British legislation de facto favoured national producers. Bringing the case before the Court, the Bavarian Lager won in the first instance. However, on appeal of the Commission, the CJEU annulled the judgement. The Data Protection Regulation – superseded by the GDPR in 2018 – becomes applicable when documents contain personal data; the judgement is based on Art. 23 of the GDPR which I am going to explain and interpret in Chapter 4.1.7. It concluded that the Commission acted lawfully to reject the disclosure of the participants' names. Beyond that, the Bavarian Lager lacked a

In other terms, depending on the case, the right to the protection of personal data must be individually balanced.

4.2.1.2 Anti-Discrimination Provision

Rights must be realized without of any kind of prejudice;

> In defining and implementing its policies and activities, the Union shall aim to combat discrimination based on sex, racial or ethnic origin, religion or belief, disability, age or sexual orientation.[113]

Member States 'shall combat social exclusion and discrimination, and shall promote social justice and protection, equality between women and men, solidarity between generations'[114]. In other words, individuals must not be discriminated against due to these protected grounds.

In review, the rights to the protection of personal data and to be free from discrimination based on sex, racial or ethnic origin, religion or belief, disability, age or sexual orientation should be kept in mind when analysing the legal scope for credit scoring.

4.2.2 ECHR

The EU lawfully accessed the ECHR based on Art. 6(2) to (3) of the TEU.

> 2. The Union shall accede to the European Convention for the Protection of Human Rights and Fundamental Freedoms. Such accession shall not affect the Union's competences as defined in the Treaties.
> 3. Fundamental rights, as guaranteed by the European Convention for the Protection of Human Rights and Fundamental Freedoms and as they result from the constitutional traditions common to the Member States, shall constitute general principles of the Union's law.[115]

Being obliged to realize the rights and duties of this Convention, its provisions became general principles of EU law.[116]

4.2.2.1 Right to Respect for Private and Family Life

The ECHR ensures the right to respect for private and family life:

---

convincing purpose for obtaining personal data. Thus, consent for the disclosure of personal data and a legitimate purpose remain of crucial importance. The right to access to documents cannot automatically overrule the right to data protection. (Krzysztofek, p. 14. See also EU Treaties, Art. 15(1), 15(3); Charter, Art. 42; FRA and CoE, pp. 26-27.)

[113] EU Treaties, Art. 3(3).

[114] ibid.

[115] EU Treaties, Art. 6(2) to (3).

[116] Krzysztofek, p. 8.

> 1. Everyone has the right to respect for his private and family life, his home and his correspondence.
> 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.[117]

As some interferences into one's private and family life are lawful, this right is not an absolute right. In light of new interpretations, the above-mentioned article is interpreted in terms of privacy protection. Poullet elaborates regarding the two provisions,

> [t]he first one is the right to "seclusion"[118] which means the choice of the individual to decide when to retire from the world at large. The second one is that of entitlement to membership of the society and the opportunity to enter into multiple interrelationships with other members of it, by the right of "inclusion". It means to be able to take part to our democratic society fully and without undue constraints or manipulation.[119]

According to Poullet, Art. 8 grants the right to withdraw for a certain time from the outside world but, at the same time, to be able to participate whenever one wants. Of course, this possibility of withdrawing oneself would undoubtedly need a new connotation in times of the ubiquity of the Internet.

In *Taliadorou and Stylianou v. Cyprus*, judges of the *European Court of Human Rights* (ECtHR) decided that the respect for privacy includes the right to be left alone and obliges Member States to effectively protect private parties from unlawful infringements:

> Article 8 of the Convention requires not only that the State should refrain from action that would unjustifiably interfere with an individual's right to privacy but also that it should set up a system for its effective protection and implementation in cases of unlawful interference falling within its scope.[120]

Further detail about how such provisions should look like is missing; gaps must be filled in by lawmakers and legislation.

Also, the CJEU[121] referred to Art. 8 deriving a more concrete privacy provision:

---

[117] Convention for the Protection of Human Rights and Fundamental Freedoms (1950) 4.XI., Art. 8.

[118] This possibility of withdrawing him or herself "between the four walls of his or her house" undoubtedly would need a new dedication at the time of the ubiquity of the Internet. On that point, one refers to the "right to be forgotten" enacted by the GDPR but we suggest also the "right to a (relative) anonymity" (with exception for requirements of public and thirds' security) and the "right to log out", to be disconnection from the digital infrastructure as it was enacted by the former ISDN Directive and finally the "right to our digital home", the right to have no intrusion from outside in our personal digital equipment, enacted by the e-Privacy Directive, Art. 5. (Poullet, p. 778.)

[119] ibid.

[120] See ECtHR, *Taliadorou and Stylianou v. Cyprus*, no. 39627/05, 16 October 2008, para. 55.

[121] Zuiderveen Borgesius and Steenbruggen emphasis that '[t]he CJEU has the final say on the interpretation of EU law to ensure it is applied in the same way in all EU Member States. National judges in the EU can, and in some cases must, ask the CJEU for advice on how to interpret EU law… the CJEU is strictly speaking not bound to follow the interpretation of the ECtHR. However, in practice, both courts try to prevent

> It covers the physical integrity of the person (…). It can sometimes include aspects of the physical and social identity of an individual (…). Elements such, for example, as the sexual identification, the name, the sexual orientation and the sex life concern the personal sphere protected […] This provision also protects the personal right to development and the right to establish and maintain the relationship with other human beings and the external world (…). Although it was established in no former business that Article 8 of [European] Convention [of Human Rights] comprises a right to self-determination as such, the Court considers that the concept of personal autonomy reflects an important principle, which underlies the interpretation of the warranties of Article 8."[122]

This paragraph is crucial in which I will unravel the rights Art. 8 comprises. The CJEU ruled the right to respect for private and family life includes the following rights:

- the right to physical integrity of a person;
- the right to physical and social identity of an individual;
- the right to the personal sphere to be protected – meaning the protection from discrimination on grounds of name, sexual identification, sexual orientation, and sexual life;
- the right to self-determination;
- the right to establish and maintain a relationship with other individuals and the external world – meaning the right to inclusion and seclusion of the outside world.

Regarding the above-mentioned rights, (a) in general, (b) regarding the social identity, (c) regarding one's sex, (d) in general, and (e) are important to be kept in mind when dealing with legal shortcomings and loopholes in Chapter 4.3. Points of discussion should be the change in the credit applicant's social identity on social media, their sex, and relationship with others when applying for social scoring or the consequences, if they do not adjust their profile to social scoring values.

As demonstrated, the right to respect for private and family life influenced privacy regulations within the EU to a big extent – mainly due to the CJEU's judgement. It upgrades privacy to a right that is inclusive and exclusive. It embraces solitude and participation. Self-development is also important for an individual to have a right to private life, which falls under the umbrella of privacy. It entitles individuals to have the

conflicts and diverging interpretations, and regularly cite each other's case law.' (F. Zuiderveen Borgesius and W. Steenbruggen, 'The Right to Communications Confidentiality in Europe: Protecting Privacy, Freedom of Expression, and Trust', *Theoretical Inquiries in Law*, vol. 20, no. 1, 2019, pp. 304-306 (accessed 5 May 2019).)

[122] CJEU cited by Poullet, p. 778.

rights to physical integrity, physical and social identity, and to a protected private sphere on certain above-mentioned grounds.

4.2.3 Race Equality Directive

On 27 June 2000, the Race Equality Directive was adopted. It came into force on 19 July 2000. Although it mainly concerns European labour law, it explicitly defines the scope for services:

> Within the limits of the powers conferred upon the Community, this Directive shall apply to all persons, as regards both the public and private sectors, including public bodies, in relation to […] access to and supply of goods and services which are available to the public, including housing.[123]

Also, the Race Equality Directive is important in the face of social scoring as it defines direct and indirect discrimination.

4.2.3.1 Prohibition of Discrimination based on Racial or Ethnic Origin

The core of the Race Equality Directive is Art. 1 that prohibits 'discrimination on the grounds of racial or ethnic origin, with a view to putting into effect in the Member States the principle of equal treatment.'[124] Both indirect and direct discrimination against individuals are prohibited:

> 1. For the purposes of this Directive, the principle of equal treatment shall mean that there shall be no direct or indirect discrimination based on racial or ethnic origin.
> 2. For the purposes of paragraph 1: (a) direct discrimination shall be taken to occur where one person is treated less favourably than another is, has been or would be treated in a comparable situation on grounds of racial or ethnic origin; (b) indirect discrimination shall be taken to occur where an apparently neutral provision, criterion or practice would put persons of a racial or ethnic origin at a particular disadvantage compared with other persons, unless that provision, criterion or practice is objectively justified by a legitimate aim and the means of achieving that aim are appropriate and necessary.[125]

Even apparently neutral provisions can have a discriminatory effect on individuals which the directive requires to diminish.[126]

This directive applies in cases where somebody has given the instruction to any executive body: 'An instruction to discriminate against persons on grounds of racial or ethnic origin shall be deemed to be discrimination within the meaning of paragraph 1.'[127]

---

[123] Race Equality Directive (2000) OJ L 180/22, Art. 2.
[124] ibid., Art. 1.
[125] ibid., Art. 2.
[126] However, in case of social scoring and big data, AI-led algorithms seem to be neutral at the first glace – but accused to not be neutral but discriminatory what will be discussed in more detail in Chapter 4.1.9.
[127] ibid., Art. 2(4).

FinTech companies and their programmers of AI-led algorithms – even unintentionally – might indirectly discriminate against credit applications due to their discriminatory computational features.[128]

Ultimately, the Race Equality Directive requires Member States to protect individuals such as credit applicants from discriminatory services which are based on decisions made on racial or ethnic origin. Thus, social scoring decisions that increase the credit risk and decrease the creditworthiness, for example, because of a person's Nigerian background, are prohibited.

4.2.4 Charter

Known as a breakthrough in the EU's fundamental rights[129] history, the Charter is classified as primary law. It has the same value as the EU Treaties.[130] The provision is targeted at EU institutions, Member States, and all kinds of processors and controllers under EU law. The Charter supports a development towards a more privacy-friendly environment within the EU.

Importantly, the prescribed fundamental rights are not absolute in nature as Art. 52(1) reads:

> Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.[131]

Even the Charter's fundamental rights need to be balanced with each other. If mediation is unclear, in Art. 52(7) another solution is provided:

> The explanations drawn up as a way of providing guidance in the interpretation of this Charter shall be given due regard by the courts of the Union and of the Member States.[132]

---

[128] However, ML or self-learning algorithms cannot be traced back completely. Critics target the factor of accountability in this field what will be discussed in more detail in Chapter 4.1.9.

[129] Human rights and fundamental rights only have a slightly different connotation. FRA defines: 'The term 'fundamental rights' is used in the […] EU [ ] to express the concept of "human rights" within a specific EU internal context. Traditionally, the term "fundamental rights" is used in a constitutional setting whereas the term "human rights" is used in international law. The two terms refer to similar substance as can be seen when comparing the content in the Charter with that of the European Convention on Human Rights and the European Social Charter.' (FRA, 'Frequently Asked Questions' (*FRA*) <https://fra.europa.eu/en/about-fundamental-rights/frequently-asked-questions#difference-human-fundamental-rights> (accessed 17 June 2019).)

[130] Treaty of Lisbon Amending the Treaty on EU and the Treaty Establishing the European Communities (2007) OJ C 306/1, Art. 6(1).

[131] Charter, Art. 52(1).

[132] ibid., Art. 52(7). For further information on the CJEU mandate to balance and interpret EU law, I mention two cases the court dealt with: (1) In case of *Promusicae v. Telefónica de Espana*, the CJEU

On a case-by-case basis, judiciary powers reconcile opposing rights and, thereby, shape the scope of the respective right such as the one to privacy. The character of this right is not absolute, which makes it subject to interpretations and causes confusion of the definite borders of its scope.

4.2.4.1 Fundamental Right to Respect for Privacy or Private Life

For the first time in history, a document created by the EU indicates a fundamental right to respect for private and family life. Art. 7 almost copies Art. 8 of the ECHR verbatim: 'Everyone has the right to respect for his or her private and family life, home and communications.'[133] The only distinction made from the verbatim copy is the term "communications" instead of "correspondence". The latter one has a more traditional meaning; one thinks about traditional letters sent by post or telegraphs. In terms of evolving online communications, the first term has a more modern and fashionable connotation. The articles of the Charter have at least the same meaning as the ones in the ECHR – if not more:

> In so far as this Charter contains rights which correspond to rights guaranteed by the Convention for the Protection of Human Rights and Fundamental Freedoms, the meaning and scope of those rights shall be the same as those laid down by the said Convention. This provision shall not prevent Union law providing more extensive protection.[134]

Any ECHR predecessor provision might be novelized by provisions of the Charter or case law by the CJEU.

highlighted the importance of fairly reconcile opposing rights according to the principle of proportionality and EU law – in this case, the rights to respect for private life, protection of property and to an effective remedy. The internet provider Telefónica refused Promusicare, a NGO, access to personal data of certain customers. The Spanish Court referred the case to the CJEU to clarify whether personal data should be communicated to ensure the effective protection of copyright and introduce civil proceedings based on revealed personal data – knowing that the fundamental right to privacy would be affected; the protection of intellectual property is explicitly mentioned in Art. 17(2) of the Charter. Referring to Directives 2000/31, 2001/29 and 2004/48, read also in light of Art. 17 and 47 of the Charter, the CJEU concluded these directives, do not prevent Member States to disclose personal data for the purpose of civil proceedings and effective protection of copyright. (FRA and CoE, p. 33.) (2) In *Volker and Markus Schecke and Hartmut Eifert v. Land Hessen*, the CJEU noted that the right to data protection is not absolute but also that the disclosure of private data was unproportionate. Both parties Volker and Markus Schecke as well as Hartmut Eifert were beneficiaries of EU agricultural aid. Their names and the amount of money they received was held publicly available. Generally, as an object of general interest such an interference might be considered lawful, however, the CJEU found this an interference with their private life and into the protection of their personal data a disproportionate measure and declared this incident partially invalid with EU legislation. (FRA and CoE, pp. 29-30.)

[133] Charter, Art. 7.

[134] ibid., Art. 52(3).

Although the fundamental right to privacy is not mentioned verbatim, the fundamental right to private life bears the same meaning. The European Data Protection Officer states, "[t]he right to privacy or private life is enshrined in […] the European Convention of Human Rights (Art. 8) and the European Charter of Fundamental Rights (Art. 7)."[135] Also, in a press release the CJEU defines, in conjunction to the right to private life, the right to privacy as a fundamental right.[136] It is included more than just the Charter's Art. 7. Logically, the fundamental right to the protection of personal data is part of this right because such data contains personal and sensitive private information as defined in Chapter 4.1.2. For instance, family members might communicate via postings and chats. In doing so, social media activities obtain insights into one's home and private sphere.

4.2.4.2 Fundamental Right to the Protection of Personal Data

The Charter provides for everyone's fundamental 'right to the protection of personal data concerning him or her.'[137] Art. 8 upgrades the right to the protection of personal data of an individual to a fundamental right:[138]

> 1. Everyone has the right to the *protection of personal data* concerning him or her.
> 2. Such data must be processed *fairly for specified purposes* and on the basis of the *consent* of the person concerned or some *other legitimate basis laid down by law*. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.[139]

Art. 8(2) even goes even beyond the already established scope of the EU Treaties as it introduces three requirements when processing personal data:

(a) specified purpose, consent, or other legitimate aims determined by law;

(b) the right to access;

(c) rectification of one's personal data.

---

[135] 'Data Protection' (European Data Protection Supervisor) <https://edps.europa.eu/data-protection/data-protection_en> (accessed 17 June 2019).

[136] CJEU, 'An Internet Search Engine Operator is Responsible for the Processing that It Carries Out of Personal Data Which Appear on Web Pages Published by Third Parties' (*Press Release*, 13 May 2014) <https://curia.europa.eu/jcms/upload/docs/application/pdf/2014-05/cp140070en.pdf> (accessed 17 June 2019).

[137] Charter, Art. 8(1).

[138] The Treaty of Lisbon entered into force in December 2009. It lays down the legal basis for the amendments of the TEU and TFEU. As read in Art. 6(1) of the amended TEU, the Charter is accepted as primary EU law. (Treaty of Lisbon Amending the Treaty on the EU and the Treaty Establishing the European Communities (2007) OJ C 306/1, Art. 6(1).)

[139] Charter, Art. 8(1) to 8(2).

Put differently, Art. 8 provides for the protection of personal data by demanding fair processing based on consent or any other lawful reason. These novelties have been included in following legislation such as the GDPR and, thus, proven to be reasonable and up-to-date.

4.2.4.3 Fundamental Anti-Discrimination Provision

This primary law document contains a non-discrimination provision that must be linked to any other provision set forth in the Charter. Art. 21 reads

> [a]ny discrimination based on any ground such as sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation shall be prohibited.[140]

Regarding the fundamental right to the protection of personal data, any discrimination on grounds of race, colour, ethnic and social origin, and language are prohibited. This provision needs to be kept in mind when analysing the critique of discriminatory social scoring practices in Chapter 4.3.3.

As elaborated, the Charter is a breakthrough in the history of fundamental rights within the legal scope of the EU. It not only upgrades the right to the protection of personal data to the level of a fundamental right, but also establishes the fundamental right to respect for private and family life as an EU right. Taken together, they form the fundamental right to privacy.

4.2.5 e-Privacy Directive

The e-Privacy Directive was adopted on 12 July 2002 and entered into force on 31 July 2002. It focusses on rights related to the field of electronic communications. There are lawful limitations.[141]

4.2.5.1 Right to Respect for Private Life

It aims at ensuring privacy and particularises personal data and the protection of privacy exclusively in the electronic communications sector and offers provisions for the right for private life and confidentiality of communications in the digital sphere.

[140] ibid., Art. 21.
[141] e-Privacy Directive (2002) OJ L 201/37, Art. 10.

> It also guarantees the free movement of electronic communications data, equipment and services in the Union. It implements in the Union's secondary law the fundamental right to the respect for private life, with regard to communications[.][142]

It is, thus, closely intertwined with the above-mentioned Art. 7 prescribed in the Charter.

4.2.5.2 Harmonising Privacy-Related Provisions

The Directive aims at harmonising legal privacy-safeguards among the Member States.[143] Regarding social scoring, two features are crucial:

(1) Confidentiality of communications: Member States shall ensure that 'clear and comprehensive information […], inter alia about the purposes of the processing'[144] as well as the 'right to refuse such processing by the data controller'[145] is offered. If data processing is 'strictly necessary in order to provide an information society service'[146], one is allowed to deviate from this legally requested practice. Also, it regulates that individuals shall not be subject to automated decisions, if they significantly concern them and relate to personal aspects such as their 'performance at work, creditworthiness, reliability, conduct, etc.' Partly or fully automated social scoring falls into this category. If improperly conducted, flaws can distort a person's credit score who might not be able to obtain a credit and satisfy an existential need. A critical analysis of this topic will be conducted in Chapter 4.3.2.4.;

(2) location data other than traffic data: This feature relates to users or subscribers of public communications networks or publicly available electronic communications services. They may be processed, only with consent which can be withdrawn at any time or if transformed to anonymous data.[147] Also, users have the opportunity by simple means and free of charge to temporarily refuse respective data processing.[148]

---

[142] Commission, 'Proposal for a Regulation of the EP and of the Council concerning the Respect for Private Life and the Protection of Personal Data in Electronic Communications and Repealing Directive 2002/58/EC' (*Communication*) COM (2017) 10 final., p. 2.
[143] Directive 2002/58/EC of the EP and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector OJ L 201/37, Art. 1(1).
[144] ibid., Art. 5(3).
[145] ibid.
[146] ibid.
[147] ibid., Art. 9(1).
[148] ibid., Art. 9(2).

Both confidentiality of communications and location data other than traffic data are protected under this provision. If not prescribed otherwise, data subjects need to consent to data processing. According to the e-Privacy Directive, the definition of "consent" corresponds to the definition given in Art. 2 of the Data Protection Directive.[149] It reads as follows:

> "the data subject's consent" shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.[150]

This is crucial regarding social scoring as one could think about algorithmic scoring systems that do not only rely on language used in posts, but also on private messages and geodata from the location where the user interacts on social media.

Put in a nutshell, the e-Privacy Directive harmonises privacy-related provisions. Doing so, it picks up the Data Protection Directive's definition of "consent". Concerning social scoring, the e-Privacy Directive requires the protection of confidentiality of communications and location data other than traffic data. Its laws protect the user's right to respect for private life in the field of online communications and literally strengthens the Charter's fundamental right with the same name. It is currently under supervision to publish a more fashionable one, in conformity with online developments, which might include social media features such as posts and tweets.

4.2.6 GDPR

Besides the e-Privacy Directive, the GDPR is one of two key secondary law acts.[151] Repealing the Data Protection Directive, it was adopted on 14 April 2016 and entered

[149] ibid., Art. 2.
[150] Data Protection Directive, Art. 2.
[151] Initially, the e-Privacy Regulation should have been published at the same day as the updated GDPR. However, the e-Privacy Directive is in delay and has not been published yet; it aims at expanding the scope of personal data protection and covers establishments and legal units in the context of electronic communication to complement the GDPR. (Krzysztofek, p. 4.) The new e-Privacy Regulation aims to broaden the new legal scope by broadening the coverage of electronic communications frameworks or, in short, the term "communication". In the draft Recital, it reads as follows: 'The principle of confidentiality should apply to current and future means of communication, including calls, internet access, instant messaging applications, e-mail, internet phone calls and personal messaging provided through social media.' (Commission, 'Proposal for a Regulation of the EP and of the Council concerning the Respect for Private Life and the Protection of Personal Data in Electronic Communications and Repealing Directive 2002/58/EC' (*Communication*) COM (2017) 10 final, Recital (1).) Generally, one should bear in mind that recitals have no independent legal value; good legislation, however, mirrors its recitals in its provisions. (CJEU, Case C673/17 [2017], *Opinion of Advocate General Szpunar delivered on 21 March 2019,*

into force on 25 May 2018.[152] The GDPR aims at safeguarding 'all individuals within the European Union (EU) and the European Economic Area […]. The GDPR aims primarily to give control to citizens and residents over their personal data.'[153] Passing the GDPR, Member States need to adopt the full scope; the GDPR is a regulation, meaning a legislative act that 'must be applied in its entirety across the EU.'[154] It 'applies uniformly in all Member States'[155]. It added 'a number of duties for the data controller and right for the data subjects.'[156] The GDPR targets especially controllers or processors in the EU – regardless of whether the processing takes place in the EU or not;[157] thus, it targets social scorers such as FriendlyScore and Big Data Scoring.

The GDPR has three core aims:

i. regulating the processing of personal data and free data movement;
ii. protecting fundamental rights and freedoms while focussing on personal data protection and privacy;
iii. demanding no restrictions of such data movement.[158]

The GDPR can be restricted for economic interests such as the Single Market Strategy[159].

> […] (e) […] important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including

Planet49 v Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V., 30 November 2017, para. 71.)

[152] GDPR, Art. 94, Recital 171. – The Recital indicates that given consent does not need to be refreshed, if it is in accordance with the Data Protection Directive; '[w]here processing is based on consent pursuant to Directive 95/46/EC, it is not necessary for the data subject to give his or her consent again if the manner in which the consent has been given is in line with the conditions of this Regulation, so as to allow the controller to continue such processing after the date of application of this Regulation.' Further, Art. 94(2) does not only repeal the Data Protection Directive but also lays the legal basis for the European Data Protection Board, successor of the Working Party on the Protection of Individuals with Regard to the Processing of Personal Data established by former Art. 29.

[153] R. O'Dwyer, 'Cache Society: Transactional Records, Electronic Money, and Cultural Resistance' *Journal of Cultural Economy* 12, vol. 12, no. 2, 2019, p. 15 (accessed 18 June 2019).

[154] 'Regulations, Directives and Other Acts' (EU) <https://europa.eu/european-union/eu-law/legal-acts_en> (accessed 17 June 2019).

[155] GDPR, Recital 173, Art. 95; Krzysztofek, p. 5.

[156] P. Sokol et al., 'Honeypots and Honeynets: Issues of Privacy', *EURASIP Journal on Information Security*, vol. 4, 2017, pp. 3-4 (accessed 30 April 2019), p. 4.

[157] Krzysztofek, p. 22.

[158] GDPR, Art. 1(1).

[159] The EU's Single Market Strategy aims at reviving and modernizing the EU market's functioning while appropriately protecting the people. 'It is made up of targeted actions in three key areas: creating opportunities for consumers, professionals and businesses; encouraging and enabling the modernisation and innovation that Europe needs; ensuring practical delivery that benefits consumers and businesses in their daily lives.' (Commission, 'Upgrading the Single Market: More Opportunities for People and Business' (*Communication*) COM(2015) 550 final, p. 3.)

> monetary, budgetary and taxation a matters, public health and social security; […]; (i) the protection of the data subject or the rights and freedoms of others […].[160]

In short, the above-mentioned goal ii. is not pursued in an absolute way because the GDPR provisions may be restricted under certain circumstances.

4.2.6.1 Principles

The most relevant GDPR principles for data processing are fourfold:

i. lawfulness, fairness and transparency;
ii. purpose limitation;
iii. data minimisation;
iv. accuracy.[161]

In the following, I will explain them in more detail.

Lawfulness, Fairness, and Transparency

Data shall be 'processed lawfully, fairly and in a transparent manner in relation to the data subject'[162]. Assuring data that are in accordance with the law, just, and transparent, the GDPR regulates,

> principles of fair and transparent processing require that the data subject […] [is] informed of the existence of the processing operation and its purposes. The controller should provide the data subject with any further information necessary to ensure fair and transparent processing taking into account the specific circumstances and context in which the personal data are processed.[163]

Provisions to be initiated are as follows:

- To ensure lawfulness, data processing must be necessary for the realisation of a contract, the protection of 'vital interests of the data subject or of another natural person'[164], performances of public interest, compliance with the controller's legal obligation, or any other task for legitimate purposes.[165]
- To ensure fairness, algorithms must not contain bias capable of leading to discrimination.[166]

[160] ibid., Art. 23(1).
[161] ibid., Art. 5.
[162] ibid., Art. 5(1)(a).
[163] ibid., Recital (60).
[164] ibid., Art. 6(d).
[165] ibid., Art. 6.
[166] ibid., Art. 5(1)(a), Recitals (42), (71), (75), and (85).

- To ensure transparency, the controller must provide the data subject with further information 'to ensure fair and transparent processing'[167]. In the case of social scoring, the controller shall inform the credit applicant about 'the existence of automated decision-making, including profiling, […] and […] meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.'[168] An individual might feel that social scoring is opaque; they 'may find it challenging to understand the complex techniques involved in profiling and automated decision-making processes.'[169] Thus, the controller shall offer 'any further information necessary to ensure fair and transparent processing taking into account the specific circumstances and context in which the personal data are processed.'[170] Especially in the case of automated decision-making, the EDPB[171] urges the controller to strictly comply with the GDPR's provision to provide the data subject with transparent, concise, intelligible, and easily accessible information about the processing of their personal data.[172]

  > If the controller is making automated decisions as described in Article 22(1), they must: tell the data subject that they are engaging in this type of activity; provide meaningful information about the logic involved; and explain the significance and envisaged consequences of the processing.[173]

  Information shall be clearly explained 'to tell the data subject about the rationale behind, or the criteria relied on in reaching the decision.'[174] Meaningful information about the logic involved does

  > not necessarily [reveal] a complex explanation of algorithms used or disclosure of the full algorithm. The information provided should, however, sufficiently comprehensive for the data subject to understand the reasons or the decision.[175]

[167] ibid., Art. 13(2).
[168] ibid., Art. 13(2).
[169] DPWP, 2017a, p. 9.
[170] GDPR, Art. 60.
[171] As established by the GDPR, the European Data Protection Board issued further guidance, for instance, on the question of consent as well as automated-decision making and profiling. Their guidelines are considered soft law, i.e. they might influence the legal situations, however, one cannot rely on them since they are not legally binding. (GDPR, Art. 72.)
[172] WPWP, 2016, p. 9. See also GDPR, Art. 12(1).
[173] ibid., p. 25.
[174] ibid.
[175] ibid.

For further clarification, the EDPR exemplifies, a controller shall explain that a credit decision has been based on a score provided by another credit institute or based on data within their own company.[176] Such data may include

> the information provided by the data subject on the application form; information about previous account conduct, including any payment arrears; and official public records information such as fraud record information and insolvency records. The controller also includes information to advise the data subject that the credit scoring methods used are regularly tested to ensure they remain fair, effective and unbiased. The controller provides contact details for the data subject to request that any declined decision is reconsidered, in line with the provisions of Article 22(3).[177]

If a controller does so, fair, effective, and unbiased data are accurately gathered and analysed.

The principle of "lawfulness, fairness, and transparency" is based on the necessity of processing for the respective purpose, is conducted without bias and discrimination, and the procedure is comprehensively outlined for the data subject.

Purpose limitation

This criterion is met if personal data are

> collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes […].[178]

It should be in line with this original purpose or serve a purpose of public interest, scientific or historical research or statistics. Krzysztofek further elaborates, 'the purpose limitation principle […] relates to this very purpose, and this purpose should be communicated to the data subject'[179]. The right of the data subject is valued. However, if 'the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject' may be overdriven. Regarding lawful purposes for processing sensitive data, the laws are even more strict:

> Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.[180]

[176] ibid.
[177] ibid.
[178] GDPR, Art. 5(1.2)
[179] Krzysztofek, pp. 24-29.
[180] GDPR, Art. 9(1).

Processing sensitive data is allowed in cases with the data subjects' explicit consent – 'except where Union or Member State law provide that the prohibition referred to […] may not be lifted by the data subject'[181]. As long as explicit, lawful consent has been given or data have already been published by the data subject, processing sensitive data is in conformity with the GDPR.

Data Minimization

The principle of data minimization requires personal data is 'adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed'[182].

Accuracy

Regarding automated data processing and decision-making, this principle is one of the most important; an algorithmic calculation is flawed as soon as data is inaccurate.

> Decisions may be made on the basis of outdated data or the incorrect interpretation of external data. Inaccuracies may lead to inappropriate predictions or statements about, for example, someone's health, credit or insurance risk.[183]

A bias-led decision may affect individuals to different degrees. Therefore, the GDPR provides regulations for decisions based solely on automated processing:

> The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.[184]

Using the word "significantly" is vague; the GDPR lacks a proper definition. In that light, the EDPB speculates, 'decisions that affect someone's financial circumstances, such as their eligibility to credit'[185] 'could fall into this category'[186].

> 1. Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited. 2. Paragraph 1 shall not apply if one of the following applies: (a) the data subject has given to the processing of those personal data explicit consent for one or more specified purposes, except where Union or Member State law

[181] ibid., Art. 9(2)(b).
[182] ibid., Art. 9(2)(c).
[183] DPWP, 2017a, p. 12.
DPWP, 'Guidelines on Consent under Regulation 2016/679' (*Guidelines*, 28 November 2017) WP259 rev.01, p. 5.
[184] GDPR, Art. 22(1).
[185] DPWP, 2017a, p. 22.
[186] ibid.

> provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject; […] (g) processing is necessary for reasons of substantial public interest […].[187]

Also, a similar exemption for the issue of consenting is set in place for automated decision-making that significantly affects individuals. Chapters 4.2.6.2 and 4.3.2. provide with a more detailed elaboration on this issue.

4.2.6.2 Automated Processing and Profiling

The GDPR differentiates between three kinds of data: wholly or partly automated, as well as non-automated processing, if the data 'form part of a filing system or are intended to form part of a filing system.'[188] As elaborated in Chapter 4.1.4, automated decision-making and profiling may be intertwined. Social scoring is just one example.[189] Against the background, the GDPR establishes a legal basis for profiling.[190]

Automated decision-making is lawful where it is 'necessary for the entering of performance of a contract between the data subject and a controller, or when the data subject has given his or her explicit consent.'[191] If automated processing is conditional for a contractual service, automated processing is lawful. At least two parties need to agree to a contract, in which one could say that the contracting parties accept their professional agreement – in other words, they consent. Generally, automated processing is also lawful, if consent is given. Art. 22 even grants the right to object automated individual decision-making, including profiling in cases of, inter alia, social scoring:

> (1) The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.
> (2) Paragraph 1 shall not apply if the decision: (a) is *necessary for entering into, or performance of, a contract between the data subject and a data controller*; (b) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; *or* (c) is *based on the data subject's explicit consent*. […]
> (4) Decisions referred to in paragraph 2 shall not be based on special categories of personal data referred to in Article 9(1), unless point (a) or (g) of Article 9(2) applies and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.[192]

---

[187] GDPR, Art. 9 (1)-(2)(a), 9(2)(g).
[188] ibid., Art. 2(1); see also Krzysztofek, p. 19.
[189] For further information, please read Chapter 4.1.4.
[190] Referring to Chapter 4.1.4, credit profiling is a partly or fully automated procedure that aims at analysing the data subject's behaviour and predicting future behaviours 'concerning the […] economic situation, […] personal preferences or interests, reliability or behaviour, location or movements'. (GDPR, Art. 60.)
[191] ibid., Art. 71(1).
[192] GDPR, Art. 22. [*Emphasis* by Laura Kosanke.]

Especially the neglection of a right to object automated individual decision-making based on Art. 22(1)(a) needs to be kept in mind when assessing the legal shortcomings in Chapter 4.3.2.

4.2.6.3 Joint Responsibility

When companies sell collected data sets for marketing purposes, the concept of joint responsibility becomes more important. Thus, it was about time for the EU to introduce the legal concept of joint responsibility for joint controllers; Art. 26 of the GDPR sets a milestone.

> 1. Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers. They shall in a transparent manner determine their respective responsibilities for compliance with the obligations under this Regulation […] by means of an arrangement between them unless, and in so far as, the respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject. […]
> 2. The arrangement referred to in paragraph 1 shall duly reflect the respective roles and relationships of the joint controllers vis-à-vis the data subjects. The essence of the arrangement shall be made available to the data subject.[193]

Regarding social scoring, Art. 26 is crucial for holding both the social scoring controller as well as the social media controller responsible and liable for their processing: Facebook collects data from its social network for its own marketing purposes, whereas a social scorer such as MyBucks may process the same data sets for its credit scoring; they are jointly responsible for the data processing of the data sets they share and access.

Unfortunately, the concept of joint responsibility has not yet been sufficiently determined by the law. Two CJEU cases, referred to in Chapters 4.2.6.3.1 and 4.2.6.3.2, shape the provision more comprehensively.

4.2.6.3.1 Case C-210/16: Fan Page

The German Federal Administrative Court requested a primary ruling by the CJEU. In Case C-210/16 *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH*, the CJEU states,

[193] GDPR, Art. 26(1)-(2).

> an entity such as Wirtschaftsakademie [has] to be held responsible, as the administrator of a fan page[194] hosted on Facebook, in the event of an infringement of the rules on the protection of personal data.[195]

Administrators of fan pages and Facebook determine data provided by Facebook to be used for certain purposes and means, for example, marketing or social scoring. Therefore, they are joint controllers.

For further information, the administrator of the fan page benefits from Facebook's services: Offering insights into socio demographics and online behaviour of data subjects who have visited the fan page, data can be processed according to the determined purposes.

> The administrator must therefore be categorised […] as a controller responsible for that processing within the European Union […] within the meaning of Article 2(d) of Directive 95/46. The fact that an administrator of a fan page uses the platform provided by Facebook in order to benefit from the associated services cannot exempt it from compliance with its obligations concerning the protection of personal data.[196]

As joint controllers, the administrator of a fan page and Facebook are jointly responsible and liable for the data processing; they bear the responsibility to inform their data subjects and gather consent.

However, 'neither Wirtschaftsakademie nor Facebook Ireland Ltd notified the storage and functioning of the cookie or the subsequent processing of the data'[197]. Refraining from informing data subjects about and obtaining their consent for processing and its consequences result into a breach with EU law. However, the legal concept of "joint responsibility" has not been comprehensively determined.

As a result of Case C-210/16, the CJEU introduced a more fashionable concept of joint responsibility: An administrator of a fan page is considered a joint controller because joint controllers determine purposes and means for processing data provided by Facebook. Together with Facebook, an administrator is jointly responsible for the

[194] A fan page is a user account which may be used to receive more insights into the demographic data, interests, online shopping behaviour, and geo data by those users who visit it. By means of cookies remembering user actions and their custom preferences over time, the fan page administrators can reveal the users' personal data. (CJEU, C-210/16, *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH*, 5 June 2018, para. 15.)
[195] ibid., para. 66.
[196] ibid., para. 37-39.
[197] ibid., para 15, see also ibid., para. 1, 36.

processing and needs to stick to EU law. Respective legislation requires, inter alia, to obtain informed consent by data subjects.

Still, questions remain open: Are joint controllers equally responsible? If not, who evaluates the degree of responsibility? Case C-40/17 *Fashion ID GmbH & Co. KG* (Fashion ID) *v Verbraucherzentrale NRW e.V.* tries to give answers and to shape the legal interpretation of joint responsibility in more detail. Chapter 4.2.6.3.2 provides further information.

4.2.6.3.2 Case C-40/17: Fashion ID

The Higher Regional Court Düsseldorf requested a preliminary ruling by the CJEU in Case C-40/17. The German fashion retailer Fashion ID embedded a plug-in on its website: a Facebook Like button. Therefore, the IP address[198] of the data subject visiting Fashion ID's website was shared with Facebook – irrespective of whether the data subject has a Facebook account or presses the Like button.[199] Put differently, embedding the Facebook Like button on its website, Fashion ID enabled Facebook Ireland to place cookies on the website visitors' devices as well as to automatically receive the IP address and browser string. The core questions posed by the Higher Regional Court Düsseldorf reads as follows: Is Fashion ID a controller even if Facebook placed the cookies? If so, what obligations derive?[200] The judgement is currently pending before the CJEU.

Advocate General Bobek has already delivered his opinion.[201] It emphasises the question of '*who* bears the responsibility and *for what* exactly?'[202] He warns against the risk of holding everybody responsible:

> Making everyone responsible means that no-one will in fact be responsible. Or rather, the one party that should have been held responsible for a certain course of action, the one actually exercising control, is likely to hide behind all those others nominally "co-responsible", with effective protection likely to be significantly diluted.[203]

[198] An IP address is considered personal data. (ibid., para. 56.)
[199] CJEU, Case C-40/17 [2018], *Opinion of Advocate General Bobek, Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW e.V.*, 19 December 2018, para. 1, 17.
[200] ibid., para. 3.
[201] Christof Tschohl emphasised that opinions of advocate generals are generally taken over to a large extent in the final CJEU judgement. (Interview with Christof Tschohl, Vienna, 4 June 2019.)
[202] CJEU, Case C-40/17 [2018], *Opinion of Advocate General Bobek, Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW e.V.*, 19 December 2018, para. 53. [*Emphasis* by the author.]
[203] ibid., para. 79.

In his opinion, joint controllers need to be categorized into the party who is actively responsible for the processing and the one who just creates the frame for the other joint controller's processing. This raises another question of '*who* is supposed to obtain the data subject's consent and *for what purpose*.'[204]

As Art. 26 of the GDPR requires joint controllers to be jointly responsible and liable for and must be transparent in their data processing, the Advocate General emphases the CJEU's statement that 'operators may be involved at different stages of that processing of personal data and to different degrees'[205]. Joint controllers shall not be held responsible for the overall chain of processing but for that operation for which they share purposes and means. 'In the present case, the relevant stage (operations) of the processing corresponds to the *collection* and *transmission* of personal data that occurs by means of the Facebook "Like" button.'[206] According to him, although Fashion ID and Facebook Ireland may not use the same data, but purposes seem to be 'mutually complementary. Thus, they are jointly responsible because they share 'a commercial and advertising purpose'[207]. Fashion ID 'acts as a controller and its liability is, to that extent as well, joint with that of Facebook Ireland.'[208]

In short, once a party is identified as a controller, it must obtain the data subject's consent.[209] It must be given '*before* the data are collected and transferred'[210] and cover all processing operations 'for which the joint controllers are jointly liable, namely the collection and the transmission'[211].

Concluding his statements, General Advocate suggests the CJEU to answer the requested preliminary ruling in this way:

> A person that has embedded a third-party plug-in in its website, which causes the collection and transmission of the user's personal data […], shall be considered to be a controller […]. However, that controller's (joint) responsibility is limited to those operations for which it effectively co-decides on the means and purposes of the processing of the personal data. For the purpose of the assessment of the possibility to process personal data under the conditions set out in Article 7(f) of Directive 95/46, the legitimate interests of both joint controllers at issue have to be taken into account

[204] ibid., para. 77.
[205] CJEU cited by ibid., para. 97.
[206] ibid., para. 101-102. [*Emphasis* by the author.]
[207] ibid., para. 105.
[208] ibid., para. 106.
[209] See e-Privacy Directive, Art. 2(f) and Recital 17.
[210] CJEU, Case C-40/17 [2018], *Opinion of Advocate General Bobek, Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW e.V.,* 19 December 2018, para. 140. [*Emphasis* by the author.]
[211] ibid., para. 131.

> and balanced against the rights of the data subjects. The consent of the data subject obtained under Article 7(a) of Directive 95/46 has to be given to a website operator which has embedded the content of a third party. Article 10 of Directive 95/46 shall be interpreted as meaning that the obligation to inform under that provision also applies to that website operator. The consent of the data subject under Article 7(a) of Directive 95/46 has to be given, and information within the meaning of Article 10 of the same directive provided, before the data are collected and transferred. However, the extent of those obligations shall correspond with that operator's joint responsibility for the collection and transmission of the personal data.[212]

The General Advocate advises the CJEU to legally establish the concept of "joint responsibility" in correspondence to their conducted processing operations. This is a step forward to answer the above-mentioned question of "who bears responsibility for what exactly": Joint controllers are not necessarily equally responsible; however, the question of "for what exactly" joint controllers are responsible remains open. He does not elaborate a catalogue of responsibilities which could be consulted in cases of joint controllers.

In a nutshell, joint controllers are involved in data processing and share to a certain extent processing purposes and means. In this case, Fashion ID and Facebook collect and transmit data for commercial and advertising purposes. Joint controllers must comply with the law. One provision requires informed consent. Further information on obtaining lawful consent will be given in Chapter 4.2.6.4.

Concluding Chapter 4.2.6.3, Art. 26 on joint controllers and joint responsibility needs further legally-binding clarification. Joint controllers 'jointly determine the purposes and means of processing'[213]. They shall transparently regulate their responsibilities.[214] However, the question of how to determine their responsibilities has not been comprehensively answered. Also, joint controllers shall reflect their responsibilities and relationships towards the data subject. So far, a CJEU judgement on Case C-210/16 has strengthened and demonstrated the applicability of Art. 26. Regarding Case C-40/17, the General Advocate suggested in his final opinion that joint controllers need to be transparent in who bears the responsibility and for what operation. In other terms, he suggests that joint controllers are, to a certain extent, individually responsible as they are involved in the processing operation. One needs to consider whether a party is responsible for an active course of action or a nominal, rather passive co-responsibility by, for example, collecting and transferring data without using the data. Consequently,

[212] ibid., para. 142.
[213] GDPR, Art. 26(1).
[214] ibid.

Fashion ID should be considered co-responsible because it just sets the frame for Facebook Ireland's actual controlling. However, this case is still pending before the CJEU. Questions about how to determine the degree of responsibility remain open.

4.2.6.4 Consent

Consent is another key point of the GDPR's safeguards. It is defined as follows:

> '[C]onsent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.[215]

There are four necessary components for consent:

(a) Freely given: The data subject must be given a 'real choice and control'[216], the EDPB interprets; their definition is not legally binding but soft law. If the data subject feels either compelled to consent, suffers from disadvantages when not consenting, or consent is bundled up as non-negotiable part of terms and conditions, consent will not be valid. 'Accordingly, consent will not be considered to be free if the data subject is unable to refuse or withdraw his or her consent without detriment.'[217] Consent can neither become a counter-performance of the contract nor can it be acquired 'through the same motion as agreeing to a contract or accepting general terms and conditions of a service.'[218] It 'cannot be seen as a mandatory consideration in exchange for the performance of a contract or the provision of a service.'[219] Instead, the controller shall demonstrate the possibility of withdrawing consent without detriment.[220] The EDPB further describes, 'the controller needs to prove that withdrawing consent does not lead to any costs for the data subject and thus no clear disadvantage for those withdrawing consent.'[221] Due to the power imbalance of the credit scoring controller and the credit applicant, the burden of proof of the data subject having freely consented lies with the controller.[222] In light of evaluating whether consent has been

[215] ibid., Art. 4(11).
[216] DPWP, 'Guidelines on Consent under Regulation 2016/679' (*Guidelines*, 28 November 2017) WP259 rev.01, p. 5.
[217] ibid., p. 8.
[218] ibid., p. 16.
[219] ibid., p. 8.
[220] GDPR, Recital 42.
[221] DPWP, 2017b, p. 10.
[222] DPWP, 2017b, pp. 5, 20.

freely given, one must consider the context of trying to reach consent. The EDPB further states,

> any element of inappropriate pressure or influence upon the data subject (which may be manifested in many different ways) which prevents a data subject from exercising their free will, shall render the consent invalid. […] [For example,] [a] mobile app for photo editing asks its users to have their GPS localisation activated for the use of its services. The app also tells its users it will use the collected data for behavioural advertising purposes. Neither geo-localisation or online behavioural advertising are necessary for the provision of the photo editing service and go beyond the delivery of the core service provided. Since users cannot use the app without consenting to these purposes, the consent cannot be considered as being freely given.[223]

Similarly, if an applicant is unwilling to consent to social scoring, they will not obtain a loan. One might conclude that this is against GDPR law. However, one needs to consider that social scoring or automated decision-making defines consent as an inappropriate requirement for the performance of the contract between the data subject and controller.[224]

> When assessing whether consent is freely given, utmost account shall be taken of whether, *inter alia*, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.[225]

If a contract is based on the processing of personal data, consent is not conditional.

(b) Specific: The controller shall specify the purpose and separate information related to the necessary content for data processing with distinction to other reasons such as marketing.[226]

(c) Informed: Six pieces of information are crucial – namely, the controller's identity, processing purpose, type of data collected, possibility to withdraw consent, information about the data use for automated-decision making, and risks of data transfer.[227] The GDPR does not define a certain form of how information needs to be given. However, a 'clear and plain language'[228] should be used so that the message is 'easily understandable for the average person and not only for lawyers.'[229]

(d) Unambiguously indicated: The controller should obtain consent in a clear affirmative manner to be able to prove the data subject's actual consent.[230]

---

[223] ibid., p. 6.
[224] GDPR, Art. 71(1).
[225] ibid., Art. 7(4).
[226] DPWP, 2017b, p. 11.
[227] ibid., p. 13.
[228] ibid.
[229] ibid.
[230] Ibid., p. 15.

The EDPB simplifies these four consenting conditions:

> If obtained in full compliance with the GDPR, consent is a tool that gives data subjects control over whether or not personal data concerning them will be processed. If not, the data subject's control becomes illusory and consent will be an invalid basis for processing, rendering the processing activity unlawful.[231]

In Chapter 4.3.2, I will provide further details on the types of consent, for instance, formal consent and voluntary consent – an important distinction leading to a judgement of whether or not consent is freely given. First, I will refer to a General Advocate's opinion in Case C673/49 in Chapter 4.2.6.4.1. I expect this case to set a new benchmark for lawful consenting practices.

4.2.6.4.1 Case C673/17: Planet49

The German Supreme Court requested for a preliminary ruling by the CJEU concerning Case C673/17 on *Planet49 v Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V.* (Verbraucherzentrale).[232] Planet49 is a German online lottery. It required data subjects to enter their names, addresses, and to consent. The latter was required for being contacted about commercial offers by sponsors as well as for accepting the cookies. For consenting, the website presented two boxes – the first one was unticked, the second one pre-ticked: The unticked box on the commercial offers needed to be actively ticked; the pre-ticked box on the cookies did not require any action. Verbraucherzentrale claimed, pre-ticking a box is against the law requiring consent to be freely given, informed, specific, and unambiguous.

> The German Supreme Court asked for clarification concerning the question of
>
> what precisely are the requirements of informed consent which is to be freely given? Is there a difference as regards the processing of personal data (only) and the setting of and access to cookies? Which legal instruments are applicable?[233]

Still pending before CJEU, Advocate General Maciej Szpunar delivered his opinion on 21 March 2019. He believes pre-ticking a box is against the law. Both the 'processing of personal data or the more particular one of storing of and gaining access to information

[231] ibid., p. 3.
[232] CJEU, Case C673/17 [2017], *Planet49 v Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V.*, 30 November 2017.
[233] CJEU, Case C673/17 [2017], *Request for a Preliminary Ruling from the Bundesgerichtshof (Germany) Lodged on 30 November 2017, Planet49 v Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V.*, 30 November 2017.

by way of cookies' is covered by Art. 2 of the GDPR and Art. 3 of the Data Protection Directive.[234] Thus, data subjects need to consent in a free, informed, specific, and unambiguous way. Pre-ticking a box does not ensure this;

> one does not know whether […] a pre-formulated text has been read and digested. The situation is not unambiguous. A user may or may not have read the text. He may have omitted to do so out of pure negligence. In such a situation, it is not possible to establish whether consent has been freely given. […] For consent to be 'freely given' and 'informed', it must not only be active, but also separate. […] In particular, from the perspective of the user, the giving of consent cannot appear to be of an ancillary nature to the participation in the lottery. Both actions must, optically in particular, be presented on an equal footing. As a consequence, it appears to me doubtful that a bundle of expressions of intention, which would include the giving of consent, would be in conformity with the notion of consent under Directive 95/46. A user must be in a position to assess to what extent he is prepared to give his data in order to pursue his activity on the internet. […] A user must know whether and, if so, to what extent his giving of consent has a bearing on the pursuit of his activity on the internet.[235]

Consent cannot be considered freely given where one cannot actively and separately consent to different processing operations.[236] Art. 5(3) and 2(f) of the e-Privacy Directive read in conjunction with Art. 2(h) of the Data Protection Directive as well as Art. 4(11) of the GDPR are violated by the lottery's consenting practice.[237]

Understanding the process of data processing by cookies is complex. Thus, an asymmetrical level of information exists regarding the online provider and the data subject. Clear and comprehensive information must be offered because

> *any* average internet user […] cannot be expected to have a high level of knowledge of the operation of cookies. Thus, clear and comprehensive information implies that a user is in a position to be able to easily determine the consequences of any consent he might give. To that end he must be able to assess the effects of his actions. The information given must be clearly comprehensible and not be subject to ambiguity or interpretation. It must be sufficiently detailed so as to enable the user to comprehend the functioning of the cookies actually resorted to.[238]

Data subjects shall be informed about the functioning of cookies and consequences.[239]

Conclusively, the CJEU strengthens the concept of consent. Pre-ticking a box is unlawful as the data subject is not required to actively deal with the functioning and consequences of their consent concerning the processing of their personal and other data

---

[234] CJEU, Case C673/17 [2017], *Opinion of Advocate General Szpunar delivered on 21 March 2019, Planet49 v Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V.*, 30 November 2017.
[235] ibid., para. 62, 66-67.
[236] ibid., para. 74.
[237] ibid., para. 93.
[238] ibid., para. 114-115. [Emphasis by the author.]
[239] ibid., para. 119, 121.

and affecting their private sphere. The data subject must distinctly consent to each data processing operation.

Concluding Chapter 4.2.6, the GDPR is a secondary law act determining some important provisions relevant for social scoring – among them the right to object automated individual decision-making, including profiling. However, this right is not absolute and may be restricted under certain circumstances mentioned in Chapter 4.1.4. Generally, the GDPR aims to protect fundamental rights and freedoms while focussing on personal data protection and privacy. Against this background, it prescribes four principles: (i) lawfulness, fairness and transparency; (ii) purpose limitation; (iii) data minimisation; and (iv) accuracy – crucial criteria for the legal analysis in Chapter 4.3. The same counts for the requirements of automated processing and profiling, which may only be conducted if necessary for a contractual performance or when granted through consent. Consent must be freely given, specific, informed, and unambiguous.

Waiting for the preliminary ruling by the CJEU in both Case C673/17 and Case C-40/17, features of the fundamental right to privacy might be strengthened – among them the concepts of "consent" as well as "joint responsibility". The latter has already been shaped in more detail by the CJEU judgement in Case C-210/16; remaining questions such as who is responsible for what exactly might be answered when the two pending preliminary rulings will be published.

4.2.7 Trustworthy AI

The *High-Level Expert Group on Artificial Intelligence* (HLEG AI) established by the *European Commission* (Commission), published Trustworthy AI on 8 April 2019. The document rests upon the Charter, as the Commission stated in April.[240] Although AI can bring many advantages, it also brings new challenges and 'raises legal and ethical questions.'[241] Key requirements for Trustworthy AI are the following:

> Human agency and oversight: AI systems should enable equitable societies by supporting human agency and fundamental rights, and not decrease, limit or misguide human autonomy. Robustness and safety: Trustworthy AI requires algorithms to be secure, reliable and robust enough to deal with errors or inconsistencies during all life cycle phases of AI systems. Privacy and data governance: Citizens should have full control over their own data, while data concerning them will not be used

[240] See Commission, 'Artificial Intelligence: Commission Outlines a European Approach to Boost Investment and Set Ethical Guidelines' (*Press Release*) IP/18/3362.
[241] ibid.

> to harm or discriminate against them. Transparency: The traceability of AI systems should be ensured. Diversity, non-discrimination and fairness: AI systems should consider the whole range of human abilities, skills and requirements, and ensure accessibility. Societal and environmental well-being: AI systems should be used to enhance positive social change and enhance sustainability and ecological responsibility. Accountability: Mechanisms should be put in place to ensure responsibility and accountability for AI systems and their outcomes.[242]

These legally non-binding provisions will enter into a pilot phase in early 2020. The Commission emphasises the purpose of renewal by HLEG AI after having examined them.[243]

4.2.7.1 The Potential Scope in Line with the Commission's Purposes

Trustworthy AI was 'set up by the Commission'[244] to support the EU's Single Market Strategy. The HLEG AI outlined the Commission's motivation to set up Trustworthy AI:

> In its Communication of 25 April 2018 and 7 December 2018, the Commission set out its vision for artificial intelligence (AI), which supports "ethical, secure and cutting-edge AI made in Europe". Three pillars underpin the Commission's vision: (i) increasing public and private investments in AI to boost its uptake, (ii) preparing for socio-economic changes, and (iii) ensuring an appropriate ethical and legal framework to strengthen European values.[245]

In those communications, the Commission admits that, in a global comparison to China and the US, the EU lacks AI innovations: 'Europe is *behind in private investments* in AI which totalled around EUR 2.4-3.2 billion in 2016, compared with EUR 6.5-9.7 billion in Asia and EUR 12.1-18.6 billion in North America.'[246]

> This is why the European AI strategy has set ambitious, yet realistic, targets: in the Union, public and private investments in AI must be scaled up in order to reach the target of EUR 20 billion per year over the next decade.[247]

The Commission wants the EU to become a global AI leader. However, they state that '[f]urther developments in AI also require a regulatory framework that is flexible enough to promote innovations while ensuring high levels of protection and safety.'[248] At the same time it encourages '*the wider availability of privately-held data*, while ensuring full respect for legislation on the protection of personal data.'[249]

---

[242] Commission, 'Artificial Intelligence: Commission Takes forward its Work on Ethics Guidelines' (*Press Release*) IP/19/1893.
[243] ibid.
[244] HLEG AI, p. 1.
[245] ibid., p. 4.
[246] Commission, 'Artificial Intelligence in Europe' (Commission, 'Artificial Intelligence for Europe' (*Press Release*) IP/19/1893, p. 4. [*Emphasis* by the author].)
[247] Commission, 'Coordinated Plan on Artificial Intelligence' (*Communication*) COM(2018) 795 final, p. 3.
[248] Commission, 2018b, p. 8.
[249] Commission, 2018a, p. 10. [*Emphasis* by the author.]

Under the umbrella of the fundamental rights commitment, the Commission looks ahead to an extended ethical frame of Trustworthy AI that might have impact on legislation:

> While self-regulation can provide a first set of benchmarks against which emerging applications and outcomes can be assessed, public authorities must ensure that the regulatory frameworks for developing and using of AI technologies are in line with these values and fundamental rights. The Commission will monitor developments and, if necessary, review existing legal frameworks to better adapt them to specific challenges, in particular to ensure the respect of the Union's basic values and fundamental rights.[250]

Phrased differently, the Commission is willing to adjust the legal framework to, for instance, address challenges hindering AI technologies from flourishing – while ensuring fundamental rights.

4.2.7.2 HLEG AI's Purposes

Considering the Commission's purpose of improving the EU's stance in the global race for the best AI processes, HLEG AI states,

> [w]e want to ensure that we can trust the socio-technical environments in which they are embedded. We also want producers of AI systems to get a competitive advantage by embedding Trustworthy AI in their products and services. This entails seeking to *maximise the benefits of AI systems* while at the same time *preventing and minimising their risks*.

Thus, Trustworthy AI aims at paving the ethical ground for an economic and technological AI boom while capping risks.

The Guideline is directed at stakeholders to voluntarily improve trust into AI by setting the frame for ethical AI, indicating 'the development, deployment and use of AI that ensures compliance with ethical norms, including fundamental rights as a special moral entitlement, ethical principles and related core values.'[251] It is based on three components:

> 1. […] [AI] should be *lawful*, complying with all applicable laws and regulations; 2. it should be *ethical*, ensuring adherence to ethical principles and values; and 3. it should be *robust*, both from a technical and social perspective, since, even with good intentions, AI systems can cause unintentional harm.[252]

All components should be met throughout a product's life cycle and, ideally, harmonically overlap – although, 'in practice, … there may be tensions between these elements'[253].

---

[250] ibid., p. 16.
[251] HLEG AI, p. 37; see also ibid., pp. 2, 5.
[252] ibid., p. 2.
[253] ibid.

Although HLEG AI bases Trustworthy AI on all three components, its statements rather emphasise and elaborate the second and third ones.[254] It 'does not explicitly deal with Trustworthy AI's first component (lawful AI).'[255] HLEG AI hence states,

> statements are hence not meant to provide legal advice or to offer guidance on compliance with applicable laws … Nothing in this document shall be construed or interpreted as providing legal advice or guidance concerning how compliance with any applicable existing legal norms and requirements can be achieved. Nothing in this document shall create legal rights nor impose legal obligations towards third parties. ... These Guidelines proceed on the assumption that all legal rights and obligations that apply to the processes and activities involved in developing, deploying and using AI systems remain mandatory and must be duly observed.[256]

Although Trustworthy AI does not elaborate the legal basis, it builds upon fundamental rights as 'the most promising foundations for identifying abstract ethical principles and values'[257].

4.2.7.3 Ethical Contribution for Eradicating AI-Led Bias and Discrimination

The HLEG AI shares the Commission's view that laws should be modernized and adjusted to today's developments.

> Laws are not always up to speed with technological developments, can at times be out of step with ethical norms or may simply not be well suited to addressing certain issues.[258]

At this stage, Trustworthy AI comes into play. Offering concrete principles embedded in the frame of fundamental rights,[259] HLEG AI established a non-binding 'living document'[260] or guide to consult when it comes to building trust in and developing AI. Principles read, inter alia, as follows: Privacy and Data Governance, Human Agency and Oversight, Technical Robustness and Safety, Transparency, Diversity, Non-Discrimination and Fairness. The subprinciples Privacy and Data Protection, Quality and Integrity of Data, Prevention of Harm and Non-Discrimination are crucial regarding privacy issues in the face of social scoring. Most importantly,

> AI systems must guarantee privacy and data protection throughout a system's entire lifecycle. This includes the information initially provided by the user, as well as the information generated about the user over the course of their interaction with the system (e.g. outputs that the AI system generated for specific users or how users responded to particular recommendations). Digital records of human behaviour may allow AI systems to infer not only individuals' preferences, but also their sexual orientation, age, gender, religious or political views. To allow individuals to trust the data gathering

[254] ibid., p. 2.
[255] ibid.
[256] ibid., pp. 2, 6.
[257] ibid., p. 10.
[258] ibid., pp. 6-7.
[259] ibid., p. 10.
[260] ibid., p. 2.

> process, it must be ensured that data collected about them will not be used to unlawfully or unfairly discriminate against them.[261]

Such a non-discriminatory Privacy and Data Protection calls for a certain quality and integrity of data. Information 'may contain socially constructed biases[262]'.[263] To avoid such judgemental patterns, algorithms need to be free from prejudice. This is evidentially only achievable where data being processed can be tracked back to its origin. If the output cannot be reconstructed to its input, nobody can retrace possible biases. 'These cases are referred to as "black box" algorithms and require special attention.'[264] If the output and, thus, input is transparent, one might assess underlying biases and the outcome's quality.

HLEG AI did not only aim to eradicate biases in algorithms but also to diminish systematic discrimination based on an asymmetry of powers. These exist 'where AI systems can cause or exacerbate adverse impacts due to asymmetries of power or information, such as between … businesses and consumers'[265]. Trustworthy AI puts forward 'business-to-consumer domains … [which] should be user-centric and designed in a way that allows all people to use AI products or services, regardless of their age, gender, abilities or characteristics.'[266]

Altogether, HLEG AI calls for the realization of human rights and the eradication of biases and systematic discrimination. Additionally, it supports the Commission in striving for an economic and technological pursuit to catch up with the Chinese and US-American AI process. Whether or not this race goes along with the existing EU legislation and whether Trustworthy AI poses a risk to change it in a way to pre-empt law need to be discussed in Chapter 4.3. I am now going to focus on challenges in the face of social scoring.

---

[261] ibid., p. 14.
[262] AI bears a high risk of being rooted on biases; a bias is defined as 'an inclination of prejudice towards or against a person, object, or position' (ibid., p. 36.) It can arise in multiple ways. 'For example, in data-drive AI systems, […] bias in data collection and training can result in an AI system demonstrating bias. […] It can arise, for example, through the limited contexts in which a system in used, in which case there is no opportunity to generalise it to other contexts. Bias can be good or bad, intentional or unintentional. In certain cases, bias can result in discriminatory and/or unfair outcomes, indicated in this document as unfair bias.' (ibid., p. 36.)
[263] ibid., p. 17.
[264] ibid., p. 13.
[265] 'This is relates [sic] to the principle of proportionality […] Reference can also be made to the proportionality between user and deployer, considering the rights of companies (including intellectual property and confidentiality) on the one hand, and the rights of the user on the other.' (ibid., pp. 12-13.)
[266] ibid., p. 18.

In summary, Trustworthy AI itself is not legally binding. However, it can be considered soft law. The Commission mentioned, to monitor developments and to change existing legal standards, if necessary. Opponents of the Commission's statement might fear that legislation might be reduced or expanded to create more incentives for a better AI-friendly future. However, both the HLGE and Commission emphasised the fact that this development is under the umbrella of the fundamental rights framework. Opponents might stress the fact that especially privacy regulations are not absolute rights, i.e. they can be restricted to due several reasons, among them to balance individuals' rights or to uphold state security etc. A future prognosis is not feasible as nothing is determined – neither by the Commission or its expert groups nor the market or other stake holders. Thus, this development should be strictly monitored by experts, but also mention positive or even improved aspects of regulations concerning social scoring and, in general, AI.

4.2.8 Concluding Remarks

The following treaties are key pieces of legislation regarding the fundamental right to privacy in the face of social scoring:

(a) EU Treaties: Both the right to the protection of personal data and the right to be free from discrimination based on sex, racial or ethnic origin, religion or belief, disability, age or sexual orientation are legal trailblazers for the fundamental right to privacy;

(b) ECHR: The ECHR initiated the human right to respect for private and family life, which – after a CJEU's ruling – upgraded the right to a comprehensive privacy right. Rightsholders enjoy both inclusion in and seclusion from the outside world. It provides individuals with the rights to self-development, physical integrity, physical and social identity, private life, and privacy protection. The rights to seclusion, self-development, social identity, and private life are applicable in discussions about the lawfulness of social scoring within the EU. Chapter 4.3 will provide a detailed analysis on that matter;

(c) Race Equality Directive: Individuals shall be protected from discriminatory services on racial or ethnic grounds. Thus, people of colour shall not receive lower credit scores for the sole reason of their racial or ethnic origin, for example, for being a Black American due to Nigerian parents;

(d) Charter: Known as a breakthrough in history, the Charter established fundamental rights in the EU. It upgraded both the right to the protection of personal data established by the EU Treaties and the right to respect for private and family life set forth by the ECHR to a fundamental right in primary EU law.

(e) e-Privacy Directive: This document confirms the Charter's fundamental right for respect for private life and specifies its applicability in the field of online communications. Regarding social scoring practices, the most important provisions lay an emphasis on the protection of confidentiality of communications and location data other than traffic data. Experts develop a relaunch of the document which should have been published at the same time as the GDPR and aims to adjust it to today's digital challenges and developments;

(f) GDPR: The GDPR is applicable to the field of personal data processing, for instance, by social scorers. It focusses on the protection of personal data and privacy and requires controller to process personal data according to four principles: (i) lawfulness, fairness and transparency; (ii) purpose limitation; (iii) data minimisation; and (iv) accuracy. Automated data processing and profiling is lawful only if it is conditional for the performance of a contract or consented to; consent shall be freely given, specific, informed, and unambiguous. The GDPR and the CJEU Case C-210/16 strengthened the concept of "joint responsibility" by joint controllers.

Before closing Chapter 4.2, Trustworthy AI should be mentioned as an important soft law document, although it has no impact on the fundamental right to privacy in the face of social scoring; none of its provisions are legally binding yet. Trustworthy AI stresses its commitment to both: (i) the EU's fundamental rights framework and (ii) self-regulations by AI-using businesses such as social scoring start-ups. As the Commission recently stated that it might review existing standards considering new developments such as self-regulation, independent experts should closely monitor developments. Thus, it might be upgraded to become a key piece of legislation regarding privacy laws and social scoring. The focus should be on any trend that indicates a pre-emption of privacy legislation for the purpose of the EU's Single Market Strategy to keep up with AI developments in the US and China.

4.3 EU: Legal Shortcomings in the Face of Social Scoring

In elaborating the legal scope of privacy regulations within the EU, some legal difficulties have already been touched upon. Jane Marriott and Gavin Robinson warn,

> Big Data techniques and Open Data sources is expected to meet the stated economic policy goals, but in so doing it threatens to further hollow out information management norms and data subject rights enshrined in privacy and data protection law just as it is gathering unprecedented momentum in courts and on statute books across the EU. […] [P]rivacy-related safeguards are highly unlikely to address adequately the serious accuracy, transparency, and accountability concerns of individual data subjects.[267]

In regard to social scoring, Matz et al. confirm, '[p]rogressive data protection regulations, such as the GDPR […] may not fully prevent the technology presented in this paper from being used in a way that is potentially harmful to people.'[268] In the following, I am going to investigate the most pressing concerns against social scoring – namely:

(a) the critique that Trustworthy AI pre-empt privacy legislation;
(b) the question of whether online consenting meets the criteria of consent – particularly those requiring consent to be
    i. freely given despite the power imbalance;
    ii. informed despite click-wrapping;
    iii. unambiguous despite power imbalance and click-wrapping;
(c) the accusation of insufficient data accuracy, transparency, and accountability;
(d) the problem of measuring "joint responsibility";
(e) the general legal problem of too broad definitions in the face of social scoring.

4.3.1 Trustworthy AI: Pre-Empting Privacy Legislation?

Under the umbrella of the EU's fundamental rights commitment, the Commission initiated criticism indicating indirect impacts of Trustworthy AI:

> *While self-regulation can provide a first set of benchmarks* against which emerging applications and outcomes can be assessed, public authorities must ensure that the regulatory frameworks for developing and using of AI technologies are in line with these values and fundamental rights. *The Commission will monitor developments and, if necessary, review existing legal frameworks* to better adapt them to specific challenges, in particular to ensure the respect of the Union's basic values and fundamental rights.[269]

[267] Marriott and Robinson, p. 48.
[268] Matz et al., pp. 10-11.
[269] Commission, 2018a, p. 16. [*Emphasis* by Laura Kosanke.]

On the one hand, the Commission confirms its commitment to fundamental rights, but on the other hand it announces that self-regulation is a guiding value to be monitored to review or adjust the legal framework. Regarding the Commission's legal review in light of the EU's Single Market Strategy and its purpose to keep up with global AI-led technologies, such developments need to be monitored carefully to protect privacy from economic purposes.

Benjamin Wagner, Director of the Privacy & Sustainability Computing Lab at the Vienna University of Economics and Business, expressed concern:

> In this context, the role of "ethics" devolves to pre-empting and preventing legislation. When seen through this lens, ethical conduct cannot be seen as virtue or duty, it simply exists in order to prevent governmental regulation. The ethical models developed in this context are less about any specific model of practical ethics and instead oriented towards implementing practical political goals without explicitly having to make these goals concrete. As a result, avoiding any governmental regulation or respect of human rights can be couched in the language of ethics to make it seem more palatable to the general public.[270]

In plain language, Trustworthy AI provides for a development towards human rights self-regulations that might substitute, pre-empt, or prevent human rights law. Wagner cautions:

> Ethics – even in an applied sense – is distinct from the law and human rights. […] While admittedly the Commission does threaten more strict regulation of AI, it does not specify under what conditions this would take place or what this legislation would look like. Such legislative specification is however urgently necessary.

Further, Wagner believes, if Trustworthy AI sets the frame for self-regulations, it might pre-empt privacy law; the Commission would favour this self-regulatory framework before improving the legal framework. "AI ethics [Trustworthy AI] are essentially a quasi-binding instrument, which will be made binding only if it is sufficiently violated"[271], Wagner foresees. If Trustworthy AI, indeed, paves the way for quasi-legal self-regulation, one will need to sue a perpetrator before the court; this could be much more effort than to set laws instead of self-regulations.

Mark Coeckelbergh, a HLEG AI member, agrees that Trustworthy AI could pre-empt future laws; however, he states also the provisions will not minimize the existing laws:

---

[270] B. Wagner, 'Ethics as an Escape from Regulation: From Ethics-Washing to Ethics-Shopping?' (*The Privacy & Sustainable Computing Lab*, 11 July 2018) <https://privacylab.at/1064/ethics-as-an-escape-from-regulation-from-ethics-washing-to-ethics-shopping/>, p. 3 (accessed 17 June 2019).)

[271] ibid., p. 4.

> I don't think that exciting hard law is going to be reduced. What could happen is that, on the basis of this document, new laws are necessary but that new laws are not going to be made.[272]

However, Trustworthy AI has no hard law character. By nature, it cannot directly weaken existing legislation.[273] The pilot phase of testing Trustworthy AI will only start in early 2020; its practical impacts cannot be analysed yet. The potential impacts of Trustworthy AI on privacy issues in the face of social scoring need to be further monitored and analysed. Appealing to lawmakers to refrain from creating a law-pre-empting framework, Coeckelbergh urges for ethical strength:

> In Europe, we should be proud of to make things more ethical. I think, in the long run, it's in the interest, if they want to make business here we should have regulations for it. I think Europe should keep its commitment to ethical values.[274]

He calls upon stakeholders to confirm the ethical foundation of the EU by not favouring economic purposes before ethics and privacy protection.[275]

In conclusion, Trustworthy AI does not pose a threat to privacy legislation. The Commission's statement does. Predictions about future developments cannot yet be proven as correct; one can neither assuredly predict a negative, positive or status quo-maintaining development.

4.3.2 Consent

Only when consent is applied correctly does the opportunity to consent give the data subject personal control about their data. 'If not, the data subject's control becomes illusory and consent will be an invalid basis for processing, rendering the processing

[272] Interview with Mark Coeckelbergh, Vienna, 29 Mai 2019.
[273] ibid.; see also HLEG AI, pp. 6-7.
[274] Coeckelbergh.
[275] Against the background of balancing economic purposes and privacy protection, the EU urgently needs to discuss the value of (trading) data sets and privacy. Answers must be found to the following questions: Is there a red line for data processing? If so, when does privacy protection trump economic purposes? Answering those questions, one should bear in mind the doctrine "laesio enormis" which has been legally established by states such as Austria. It goes back to Roman history and reads as follows: 'If […] you […] sold property worth a higher price for a lower price, it is equitable that either you get back the land sold through a court order, refunding the price to the purchasers, or, if the buyer chooses, you get back what is lacking from the just price. The price is deemed to be too low if less than half of the true price has been paid. (R. Westbrook, 'The Origin of Laesio Enormis', *Raymond Westbrook* 50, no. 49, 2008, 40.) Transferring this doctrine to present times, a contract is contestable, if a reduction of the true value by half is evident. Lawmakers should consider such an approach for data protection laws because data trade is daily business for many companies. Considering social scoring, trading data is crucial for the business' functioning. Yet, the EU has not incorporated this field of law into its jurisdiction. Due to the scope of my research and page limit, I cannot go into more detail. Thus, I propose to answer the question of whether the doctrine "laesio enormis" is likely and lawful to be incorporated in EU law in another paper.

activity unlawful.'[276] To request consent prior to data being processed 'is intuitively central to ensuring information self-determinations [sic!] and has been a cornerstone of data protection law'[277]. Consent is a person's direct expression of autonomy which is given when the parties involved interact on one eye level; in the credit business, one can hardly identify two equal parties, as one of them is the investor and the other one the potential borrower who might face existential threats if they do not receive a loan.

Chapters 4.3.2.1 to 4.3.2.4 are going to evaluate whether the three most important GDPR requirements for consent are given regarding social scoring. The following analyses illustrate whether consent can be freely given despite power imbalances, informed despite click-wrapping, and unambiguous despite both power imbalances and click-wrapping.

4.3.2.1 Freely Given despite Power Imbalance?

The GDPR emphasises the fact that consent should be meaningful and freely given.[278] Advocate General's opinion in Case C673/17 has strengthened the legal requirement of actively freely given consent. However, he does not dissolve the underlying challenge concerning the inherent power imbalance between controller and data subject.

In the credit industry, the debtor and social scorer do not act independently, but co-exist in a state of dependence:[279] The debtor to the business conditions of the lender, the lender to provide the agreed financial service. However, a credit applicant is more dependent on the lender than the other way around, due to financial shortage. In turn, standard lenders have power due to their financial security which they can even expand by lending money; they do not need to satisfy their existential needs but thrive for profit. Logically, power imbalances are an inherent matter of fact in the credit industry and become even worse in the social scoring industry which targets a group of persons unlikely to receive a traditional bank loan for reasons of a lack in savings and a poor credit history. Debtors might feel increasingly pressured to comply with business conditions,

[276] DPWP, 2017b, p. 3.
[277] Marriott and Robinson, p. 64.
[278] GDPR, Art. 4(11).
[279] The debtor acts as data subject, the social scorer as controller.

for instance, to grant access to private or even sensitive data. Due to the financial imbalance, voluntary consent is questionable.

The above-mentioned provision shall not apply, if it 'is necessary for entering into, or performance of, a contract between the data subject and a data controller […] or […] based on the data subject's explicit consent.'[280] The second conjunction "or" indicates that a data subject has the right to not be part of automated decision-making when it either presupposes the implementation of the contract or they consented.

The EDPB similarly interprets the GDPR stating,

> [t]he processing must be necessary to fulfil the contract with each individual data subject. This may include […] processing credit card details in order to facilitate payment. […] There needs to be a direct and objective link between the processing of the data and the purpose of the execution of the contract. There needs to be a direct and objective link between the processing of the data and the purpose of the execution of the contract. If a controller seeks to process personal data that are in fact necessary for the performance of a contract, then consent is not the appropriate lawful basis.[281]

Put differently, consent is not conditional when it is necessary for the performance of such a contract. Zuiderveen Borgesius and Steenbruggen criticize,

> the GDPR allows a company to process personal data […] without the individual's consent. To illustrate: a company can process personal data if, in short, it has a legitimate interest to use the data, and that interest overrides the individual's interests. In consideration of the human rights and trust issues at stake, it is more appropriate to have a regime […] that prohibits interference […], unless under narrowly defined specific circumstances, or when the individual has given prior consent.[282]

If the automated processing of certain data is necessary to perform the actual contractual service, the individual's consent is no appropriate contractual baseline. To obtain the service, the data subject needs to confirm the contract. An effective right to withhold consent but to still receive the service – although maybe desperately needed – is non-existent. The right of the individual is systematically outbalanced in favour of the contracting business. In other terms, the credit applicant would be inferior to the social scorer's terms, conditions, and privacy regulations, if conducted based on the contract without additional consent for data processing.

For social scoring, consent is indeed necessary, as the e-Privacy Directive regulates as follows:

> Member States shall grant the right to every person not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated

[280] ibid., Art. 22(1)-(2).
[281] European Data Protection Party, 2018, p. 8.
[282] Zuiderveen Borgesius and Steenbruggen, p. 321.

> processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc.[283]

However, a social scoring agreement can exist with formal consent. It is not necessary to discern whether a person really and truthfully consents. The individual needs the contract and, thus, will consent to such conditions.[284] – Further, the GDPR regulates, in cases when the individual is significantly affected by, for instance, social scoring, they shall have the right to deny automated-decision making.

> The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.[285]

The term "significantly" is vague. Neither the GDPR nor other hard law has defined it more precisely. The EDPB – unable to provide legally binding interpretations – counsels, 'decisions that [significantly] affect someone's financial circumstances, such as their eligibility to credit'[286] fall into this category. The EDPB, however, warns against such a definition,

> someone known or likely to be in financial difficulties who is regularly targeted with adverts for high interest loans may sign up for these offers and potentially incur further debt. Automated decision-making that results in differential pricing based on personal data or personal characteristics could also have a significant effect if, for example, prohibitively high prices effectively bar someone from certain goods or services.[287]

Altogether, social scoring targets an individual's creditworthiness as it calculates the credit risk based on profiling, comprising huge sets of personal and sensitive data. The power imbalance between the lender and debtor seduces the latter to confirm to the terms, conditions, and privacy regulations of the lender. Otherwise, the debtor would not satisfy their financial need. Although the EU initiated legally binding regulations formally protecting right holders from involuntary consent, practically, it does not sufficiently protect its citizens. The flaw is inherent in the social scoring system.

283 e-Privacy Directive (2002) OJ L 201/37, Art. 5(2)-(3), 15(1).
284 Although the e-Privacy Directive serves prior to the GDPR, it does not enjoy the same status due to the legal character of a directive: Member States device their own laws in accordance with directives but, as long as they introduce them step-by-step, do not need to fully apply them.'(EU, 'Sources of European Union Law' (*EUR-Lex,* 13 December 2007) <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM%3Al14534> (accessed 25 April 2019).)
285 GDPR, Art. 22(1).
286 DPWP, 2017a, p. 22.
287 ibid., p. 22.

Generally, one can question whether consent on entering into a credit contract is freely given due to power imbalances and the likely greater need by the debtor to obtain a loan than by the lender to borrow money. Against that background, Poullet questions, '[d]oes the consent make possible a processing beyond the basic principle of what is proportionate?'[288] How meaningful is consent in any case where there is not equal power between the contracting parties? Does it generally violate the fundamental right to privacy or is it a matter of balancing the rights of the contracting parties? Are we moving towards a direction where business trumps individual rights? These are questions lawmakers urgently need to discuss with experts to pass appropriate laws that safeguard fundamental rights such as the one to privacy.

In conclusion, a power imbalance is inherent in the credit sector, even more so in the field of social scoring. Credit applicants need money due to financial shortage or even existential threats. They might not have a credit history and, thus, apply for social scoring assessments hoping to receive a loan. Consent can be considered formally not given freely because I do not think that credit applicants are keen on scorers assessing their private and sensitive data to calculate a score and decide about the credit. Although individuals shall have the right to refuse to be a part of automated profiling and decision-making, this right is solely formal and does not protect them from such techniques. Due to the power imbalance, credit applicants might feel forced to take part – without even truly willing to be part of; it might be an action motivated by despair. Also, one needs to consider the loophole prescribed by Art. 22(2)(a) of the GDPR: Objecting automated individual decision-making, including profiling, is not possible if it 'is necessary for entering into, or performance of, a contract between the data subject and a data controller'[289]. It is questionable when such an entering into or performance of a contract is indeed based on automated individual decision-making or whether there are more lenient means lawmakers could request.

[288] Poullet, p. 776.
[289] GDPR, Art. 22(2)(a).

4.3.2.2 Informed despite Click-Wrapping?

The GDPR also requires consent to be informed.[290] Click-wrapping, also called click-through agreements, are mainly used to make a data subject consent to a provider's terms and conditions; it requires clicking one or more boxes on the provider's website and bears the risk of not properly informing about possible consequences of practices such as social scoring. Clicking through the contract does not ensure meaningful, specific, informed, and unambiguous consent. Coeckelbergh confirms,

> it is a typical example where consent is guaranteed in a formal way but, in practice, people just click through. You also click through because there is not really an alternative. It is hard to avoid it. The whole problem has to do with the idea of consent." Instead of asking individual consent, I believe rather in a regulation that obliges businesses and services to do certain things for everyone without asking consent but just to do by laws by the government or the EU.[291]

If lawmakers decide to go with formal consent, the service-offering party can still act potentially unethically in a legal grey zone. Personally, I do not believe that the model of individual consent is necessarily the right way to protect credit applicants or, in general, users from uninformed consent when allowing click-wrapping for online-agreements.

More concretely, a clickthrough or clickwrap[292] survey by Obar and Hirsch discovered that 74 per cent of data subjects who entered into an online contract skipped reading the privacy policy, even though 97 percent agreed to it:

> Results reveal 74% skipped PP, selecting the 'quick join' clickwrap. Average adult reading speed (250-280 words per minute), suggests PP should have taken 29-32 minutes and TOS 15-17 minutes to read. For those that didn't select the clickwrap, average PP reading time was 73 seconds. All participants were presented the TOS and had an average reading time of 51 seconds. Most participants agreed to the policies, 97% to PP and 93% to TOS, with decliners reading PP 30 seconds longer and TOS 90 seconds longer.

Conclusively, most data subjects do not consent in a meaningful, informed nor unambiguous manner because they have not read the information and can most likely not understand possible consequences. The survey was based on clickthrough behaviour for a social media page.[293] Similar surveys with even more shocking results confirm the

---

[290] GDPR, Art. 4(11).
[291] Coeckelbergh.
[292] A clickwrap is an online agreement data subjects need to consent to use the service.
[293] A fictitious social media page was established. Undergraduate students from a public university in the USA were the target group. They could choose a "quick-join" clickwrap option similar to those on Facebook, Instagram, and LinkedIn. This option 'helps participants join services quickly through the bypassing of consent materials, accepting policies without having to access or read them. […] Participants could choose "Sign up! (By clicking Sign Up, you agree to NameDrop's privacy policy)".' (J. Obar and A. Oeldorf-Hirsch, 'The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services', *Information, Communication & Society*, vol. 1, 2018, pp. 10-11

"quick-join" trend;[294] it is desirable, if future survey concentrate on click-wrapping in the EU while applying for a credit based on a social scoring procedure. One can presume similar habits regarding social scoring agreements and conclude that clickthrough agreements do not ensure unambiguous, specific, and informed consent.

Regarding the social scoring-based FinTech sector, a data subject needs to consent to profiling based on automated decision-making or the data subject will not obtain a loan. Thus, Marriott and Robinson argue,

> where consumers have no choice other than to consent to the processing of their personal data when applying for credit, the significance of a legal rule designed to ensure such consent lies principally in its ability to inform those consumers of what processing is actually being carried out – and vice versa: knowledge of what processing is being performed is the only way to preserve the integrity of consent. In other words, […] the real value of a legal rule of consent may lie not in providing direct individual agency but in its indirect facilitation as a tool of transparency.[295]

They state that legally regulated consent is based on a transparent processing method which the data subject understands, instead of the question of consenting or not. One can only speculate whether a clickthrough agreement is enough for the legal requirements.

In short, click-wrapping – as easily written as the online agreement might be – does not sufficiently inform social scorers or, in general, users about online agreements. Studies found that the clear majority do not read them. The failure lies within the system because almost everybody does not read the agreements; only if just a few per cent would not read it, it would not be a systematic flaw. As nobody reads it, the click-wrapping systems providing information must be changed.

4.3.2.3 Unambiguous despite Power Imbalance and Click-Wrapping?

Unambiguous consent requires 'a controller to obtain consent in a crystal-clear affirmative act so that the data subject really consented to the processing, for instance, by the data subject signing the agreement.'[296] One might question whether clicking through

(accessed 18 June 2019).) If participants declined, they were directed to the privacy policy in order to read and reject or continue the process. (ibid., pp. 9-11.)

[294] See Y. Bakos et al., 'Does Anyone Read the Fine Print? Consumer Attention to Standard-Form Contracts', *The Journal of Legal Studies*, vol. 43, no. 1, 2014, pp 1–35; I. Ayres and A. Schwartz, 'The No-Reading Problem in Consumer Contract Law', *Stanford Law Review*, vol. 66, no. 3, 2014, pp. 545-610; V. Plaut and R. Bartlett, 'Blind Consent? A Social Psychological Investigation of Non-Readership of Click-through Agreements', *Law and Human Behavior*, vol. 36, no. 4, 2012, pp. 293-311; R. Mann and T. Siebneicher, 'Just One Click: The Reality of Internet Retail Contracting', *Columbia Law Review*, vol. 108, no. 4, 2008, pp. 984-1012.

[295] Marriott and Robinson, p. 65.

[296] EDPB, 2016, p. 15.

an online agreement provides for an unambiguous consent. The contract provider cannot know about the circumstances of the data subject's consent: Is it the data subject who consents? Are they pressured in any way? Justifiably, Marriott and Robinson 'emphasize the need for tighter regulation of automated decision-making and the processing of sensitive data in the context of credit risk industry.'[297]

In summary, legislation does not sufficiently protect individuals from consenting techniques that are rooted in legal grey zones and loopholes. Hard law does not specify under which circumstances clickthrough agreements may ensure a data subject's freely given, specific, informed, and unambiguous consent.

Clicking a box is barely enough; new means need to be developed and applications must be better informed about consequences of consenting to the business conditions. More comprehensive legally binding definitions on consent need to be passed, for instance, by the Commission or the CJEU. Questions to be answered are as follows:

- Is consent exclusively conditional for automated social scoring?
- How can the EU ensure consent to be freely given despite power imbalances?
- How can the EU ensure consent to be informed?
- How can the EU ensure consent to be unambiguously given?

This list is not exhaustive.

In Chapter 4.3.2.4, a case study is conducted which aims to illustrate these problems in further detail. The analysis deals with the EU's realization of its obligation to protect individuals from rights-violating and privacy-intruding consenting practices by social scorers.

4.3.2.4 Case Study: Protection against Unlawful Consenting Techniques?

Adaka has just finished her apprenticeship as an estate agent assistant. She was born and raised in a small EU town with a high proportion of migrant workers. Her parents are originally from Nigeria. Her father died when she was a child. She is going to work for a small company that sells real estate in the next bigger city. She must join customer meetings all over the city and its suburbs. As is it cheaper to live with her mother, and she needs to be mobile for her customers, she is looking for a small car for approximately

[297] Marriott and Robinson, p. 49.

3,000 euros. Her company cannot afford to buy her a work vehicle. She has a strong feeling that if she does not get a car, the company will fire her during her probation.

Since, Adaka has no savings, she applies for credits. Due to her lack of a credit history, traditional credit institutions declined her credit applications. In her despair for a credit, she found a website that advertises credits for persons with both little or no credit history and savings. They promise to assess her credit score within a few minutes based on her online behaviour on social media. If Adaka wants to start her apprenticeship, she has no other choice but to agree. She clicks through the terms and conditions as well the privacy regulations and obtains a loan. Adaka does not read everything in detail. Although the wording is phrased in a clear, plain, understandable language, she could not find information on how her SMD are being assessed and how they result in a credit score; this is typical and not only among social scoring companies.[298] Although she is not keen to share her personal data, she has no other choice but to consent to obtain the loan.

In the following section, I will answer the question of whether the EU failed in protecting Adaka from a disproportionate clickthrough agreement. There is no other alternative for Adaka than to be subject of automated credit scoring based on SMD.

Applicable Rights

Solely against the background of my research question, the most important and applicable right is the fundamental right to privacy.[299] As seen in the legal review of this thesis, it is inseparably shaped by the following EU legislation:

(a) the right to respect for one's private and family life,[300] which comprises
   i. 'the concept of personal autonomy'[301];
   ii. 'the personal right to development'[302];

[298] SCHUFA in Germany does not fully reveal its algorithm that is based on purely financial data so far.
[299] Each of the following rights have been laid down in the legal part of this thesis. However, for the reason of an easy reproducibility, I am going to cite most respective legislation which I am going to refer to in my case study.
[300] Charter, Art. 7; Convention for the Protection of Human Rights and Fundamental Freedoms (1950) 4.XI., Art. 8.
[301] CJEU cited by Poullet, p. 778.
[302] ibid.

iii. 'the right to establish and maintain the relationship with other human beings and the external world'[303], put differently, the right to inclusion;

iv. the right to be left alone[304] meaning seclusion from the outside world;

v. the condition of the consent of the person concerned or some other legitimate basis laid down by law;[305]

(b) the right to the protection of personal data;[306]

(c) the rights to refuse processing by a controller[307] and to protect as well as control the use of their personal data.[308]

Of course, the list of applicable rights in the respective situation is not exhaustive as fundamental rights are inseparably intertwined. Mentioning all the respective obligations goes beyond the scope of my research question.

The EU's Obligations to Protect

In realising the legal framework, the EU has passed to protect Adaka from rights-violating actions by the FinTech lender, the EU is the duty bearer specifically regarding the following obligations:

(d) ensuring that Adaka can maintain her professional relationship with the external world, phrased differently, to exercise her personal right to development to be able to do her apprenticeship;

(e) ensuring Adaka the right to be left alone from the FinTech lender in her private life to be free from privacy intrusions on her SMD;

(f) ensuring that social scoring roots into consent which needs to, inter alia, be informed and unambiguous;

[303] ibid.
[304] ECHR, *Taliadorou and Stylianou v. Cyprus*, no. 39627/05, 16 October 2008, para. 55.
[305] Charter, Art. 8(2). – The issue of consent is laid down in Art. 8(2) of the Charter, Art. 5(1) of the e-Privacy Directive, and Recital 42 as well as Art. 4(11), 7(4), 9(1) to (2)(b), 22(2), 42, and 71(1) of the GDPR.
[306] Charter, Art. 8(2); EU Treaties, Art. 16(1).
[307] e-Privacy Directive (2002) OJ L 201/37, Art. 5(3).
[308] ibid., Art. 14(3).

(g) ensuring her right to refuse automated processing by a controller – if not ensured, ensuring that automated data processing is conditional to perform the contract; in the latter case, consent for automated data processing is obsolete.

Of course, this list is also not exhaustive but names the most important EU obligations.

Rights Analysis

There are two differing ways to conclude this case study:

(1) Privacy provisions are not absolute. Balancing the rights of data subjects and those of the controllers is a necessary requirement: Adaka's social scoring is lawful because she consented to it by accepting the terms and conditions written in the click-wrapping agreement; both Adaka and the lender offer the other party a payment for the credit deal: personal SMD for a loan. The lender does not violate the above-mentioned rights (a)iv to be left alone and (b) to the protection of personal data. As a consequence, Adaka enjoys the rights (a)iii to maintain her professional relationship with the external world, (a)ii to personal development, and (a)iii to autonomy because her mobility increases. One could argue, the EU has passed regulations to enable social scoring. – This argumentation builds upon stretching out existing legal shortcomings. Also, the focus is on the professional consequences for Adaka; I disagree with this rights analysis.

(2) Instead of the economic focus, one should analyse the consequences for her private life – the most important feature of the applicable rights. One must focus on the consequences of her private life as the rights under (a) to (c) target the protection of her private life:

   i. The click-through agreement seduces Adaka, who is desperately applying for loans to be capable of working and making her living – existential needs. Adaka is clearly inferior to the lender. Had she refused the terms and conditions, she would not have gotten the contract because processing SMD is inherent to the business model. Her consent cannot be considered freely given because the social scorer benefits from its financial power imbalance. Even more: They misuse the requirement of consent, as click-wrapping formally provides it but hardly so when using the GDPR's criteria. Beyond that, Adaka did not read

everything but clicked through the agreement, a systematic flaw (see Chapter 4.3.2.2). Also, it is doubtful whether her click-wrapping consent is unambiguous (see Chapter 4.3.2.3). Consequently, the EU did not protect Adaka from the social scorer's consenting practices and let them violate (a)v the lawful condition of the consent of the person. If the EU does not pass a more comprehensive definitions on consent, it risks opening a privacy-intruding Pandora's box when allowing enforced, formal consent to be enough for the performance of a contract. Otherwise, it does protect the individuals against privacy-intruding consenting techniques. Instead of economic growth, individual rights need to be a priority.

ii. Whether or not one can accuse the social scorer of not providing Adaka with the possibility to use her (c) right to refuse an automated decision based on SMD processing is questionable. Consenting to the credit agreement's terms and conditions, including the assessment of credit risk and creditworthiness is conditional to receive the lending money. However, one should reflect on whether the current form of social scoring is necessary and whether more lenient means exist which enable a more privacy-friendly scoring for those who are poor in savings and credit history.[309] At the very least, the EU could ensure appropriate information for the credit applicants. It could pass both: Laws that require personal advice by a financial expert before consenting and transparency laws as a tool to provide Adaka with detailed insights into the scoring algorithm.

iii. To establish the relationship with her employer and clients, she gives up a certain degree of her (a)iv right to be left alone and (b) right to the protection of personal data. She becomes flexible and autonomous to conduct her profession but dependent on the lender's social scoring conditions. However, the exchange of personal data for money is disproportionate: Adaka will pay back the money including interest. The offered data cannot be taken back, just as the privacy infringement cannot be taken back even if the purpose limitation principle

[309] Due to the limited scope of this thesis, I cannot elaborate these issues in detail. These are guiding questions for academia, lawmakers, and the CJEU to assess and interpret legislation.

requires data to be deleted as soon as the purpose no longer exists. The EU did not protect Adaka from the dilemma of her (a)iv right to be left alone based on the lacking (b) right to protection of personal data to be at stake due to her will to enjoy (a)iii the right to establish and maintain relationships which was created by the social scorer.

iv. All of this affects her self-development and personal autonomy. She gave up her (a)i right to personal (data) autonomy to push ahead her (a)ii personal right to development. Of course, this rewards her with the autonomy to conduct her job, however, she had to give up her monopoly on her personal and sensitive data. – Is this proportionate? In my opinion, it is not. There should be more lenient means to reach social scoring goals. For example, the EU could pass a law obliging traditional banks and social scorers to work together in the process of contracting. Based on this cooperation, clients should personally consult a banker who, in exchange for a fee established in the contract, explains the terms, conditions, and privacy policy to at least make sure the credit applicant is fully informed about the consequences following the credit agreement. This way, consent is also unambiguous.

Following my argumentation, the EU did not sufficiently protect Adaka's rights mentioned under (a) to (c). Formal consent via click-wrapping cannot be considered lawful consent as the power imbalance enforces it. Of course, the processing of personal SMD is necessary for social scoring. Thus, it is less a discussion about (c) the right to refuse processing of personal SMD by the scorer but rather about (a)v consent to be informed about the contract and its consequences. Nevertheless, the goal cannot justify the means. Alternatives must be developed to score in a privacy-friendly way. Is unrealistic that the EU eradicates the power imbalance by requiring the credit industry to provide individuals with loans to uneconomical conditions. However, the EU could require social scorers to cooperate with local bank partners to, at the very least, ensure informed consent.

4.3.3 Systematic Discrimination

If not already, AI-led algorithms might open Pandora's box of unforeseen consequences. Critics warn against legally accepted systematic discrimination due to hidden biases in such algorithms, inter alia, those that assess an individual's social score based on SMD. The EDPB raises concern,

> profiling and automated decision-making can pose significant risks for individuals' rights and freedoms which require appropriate safeguards. Profiling can perpetuate existing stereotypes and social segregation. It can also lock a person into a specific category and restrict them to their suggested preferences. This can undermine their freedom to choose, for example, certain products or services such as books, music or newsfeeds. In some cases, profiling can lead to inaccurate predictions. In other cases it can lead to denial of services and goods and unjustified discrimination. […] Hypothetically, a credit card company might reduce a customer's card limit, based not on that customer's own repayment history, but on non-traditional credit criteria, such as an analysis of other customers living in the same area who shop at the same stores. This could mean that someone is deprived of opportunities based on the actions of others. In a different context using these types of characteristics might have the advantage of extending credit to those without a conventional credit history, who would otherwise have been denied.[310]

It warns against hidden biases in the analytics and discriminatory automated practices when it comes to AI-led big data techniques.

In particular, social scoring endangers the right to freedom from discrimination in the EU. For recapitalisation, the Charter contains the following anti-discrimination law:

> Any discrimination based on any ground such as sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation shall be prohibited.[311]

This right stands in conjunction with, for instance, the rights mentioned in Chapter 4 such as the ones to privacy, data protection, and to be left alone. However, anti-discrimination is not an absolute requirement but needs to be balanced with the rights of others. A credit application could be confirmed or dismissed based on a discriminatory rating procedure. Recapitulating social scoring practices mentioned in Chapter 3.1.4, it is evident that it comprises discriminatory automated means analysing user incomes based on the following:

- **Language:** Users tweeting or posting less emotional, i.e. positive and negative content, are scored higher than those who use a more emotional language led by, for instance, anxiousness, sadness and disgust. The more rational a tweet or post, the better the scoring. If emotions are used, the more joyful they are, the better. Those

[310] DPWP, 2017a, pp. 5-6, see also pp. 12, 22.
[311] Charter, Art. 21.

data subjects who cannot restrain their behaviour, but instead use swear words and express their anger, anxiousness, and sadness are scored lower. Person A is born into an environment that uses the higher-ranked language and thus has an advantage compared to Person B who has a lower ranking due to their language. Both Person A and B have no credit history or savings and apply for a credit at the same FinTech company who uses social scoring to assess the creditworthiness and height of interests.[312] Although language is a protected ground in the EU's antidiscrimination law, it is used for social scoring. Language serves as an indicator for unequal treatment. One might argue that like situations are treated in an unlike manner. However, opponents might consider this difference as a justified differentiation rather than a discrimination: This unequal treatment pursues the legitimate aim of drawing a conclusion to a credit applicant's financial status which is necessary to assess the credit default and derive thereof the credit decision and the percentage of the interests. Therefore, such opponents might conclude that the distinction based on a language assessment is based on reasonable and objective grounds. – In my opinion this action is not suitable to achieve the aim. People who know about the algorithm can trick the algorithm to that extent that its mechanism are known. Of course, this requires a certain level of education some social groups might lack. However, education is not guarantee for a high income –[313] there are still exceptions. Generalization leads to stigmatisation and those who break through the average-patterns might suffer from it. An individual assessment is necessary. Also, it is not a protected ground but inherently interlinked to several of them. Of course, such a technique is time-saving for FinTech companies because, once the algorithm is intact, the business model is lucrative. Although I cannot come up with an alternative, I cannot imagine that this is the least intrusive measure to gain a contract. Person B's fundamental right to privacy is at stake because of their style of language which they learnt as a child, perhaps from parents who did not have the chance to gain a higher degree in university.

[312] These bullet points outline discriminatory scenarios that will be the underlying basis for exemplification.
[313] However, Ben Graham and Charles Paul confirm the slogans 'The more you lean, the more you earn! Don't be a fool, stay in school! Education pays'. (See B. Graham and C. Paul, 'Does Higher Education Really Lead to Higher Employability and Wages in the RMI?', *Journal of Southeast Asian Economies*, vol. 35, no. 1, 2018, p. 3.)

- **Preferences:** Likes present an individual's interests and affirmations and are deeply rooted into their private life. Person A who likes certain luxury brand is ranked higher than Person B referring in a highly abstract and generalized way to luxury. Low-income individuals such as Person B also rather like entire phrases. Like the issue of language, individuals like what they are used to. Instead, Person A who was born into certain social groups, enjoyed a certain type of school etc., knows different things than their counterpart who has never entered a similar social group as Person A, for instance, admires luxury brands because of their taste in clothing although they would not be able to afford those clothes. The fashionista Person A obtains a credit with lower interests than Person B. This distinction is made based on, inter alia, their social origin and environment. Opponents might say everybody has the right to be interested in concrete luxury brands and everybody has the same chances. Nevertheless, individuals have different tastes and interests. Although the aim to profile credit applicants for credit scoring is legitimate, the unequal treatment is neither reasonable nor objective. There must be alternatives.
- **Friends or followers:** An individual's contact list influences the credit score. Credit scorers assume 'that people are more likely to form social ties with others who are similar to them'[314], Wei et al. revealed as already mentioned in Chapter 3.1.5.1. Person A's contact list consists of friends of an average wealthy social group and is ranked higher than Person B. The latter went to school in an area with a high unemployment rate, and for this reason many of his friends are not financially prosperous. Thus, this Person B obtains a credit with higher interests than the first one. – A like situation is treated unequal. The distinction is made because of, inter alia, one's social origin – a protected ground – and environment. The legitimate aim of assessing the credit default is legitimate, however, the action is not. The distinction is made on a stigmatising assumption. Alternatively, one should not assess the contact list but, for instance, offer to take guarantees by friends on social media chosen by the credit applicant who are being assessed in the same way.

[314] Wei et al., p. 235.

- **Posted profession:** Scoring companies such as Lenddo use the Annual Survey of Hours and Earning to roughly calculate a credit applicant's income. The higher the calculated income, the better the score; this is an indicator for unequal treatment. Person A works as a consultant, Person B as a hairdresser. Two credit applicants are treated in an unlike manner: Person B pays higher interests than the Person A. According to the survey, a consultant receives more money. The distinction is made based on money which falls in the category of property– a protected ground in EU law. Unequal treatment took place for pursuing the lenders' legitimate aim to calculate the credit default. The distinction is based rather on reasonable and objective than irrational and subjective grounds. However, the action is not the most suitable to achieve the aim. The survey relies on the average of the branch; however, Person A works for a small company for a month while Person B has been the leading hairdresser in a well-known hair salon for a couple of years. Both Person A and B do not hit the average criteria. One could argue this constituted a bias because it generalizes a whole branch of employees. Person B could even earn more money than Person A but the survey is not calculated with below- or above-average cases. An alternative is asking for the latest payroll. This practice might be more time-intense because AI-led algorithms might not be able to directly grasp the salary and human assistance might be needed. It would, however, be more precise and less stigmatising.
- **Gender**: Hurley and Adebayo found out that gender constitutes an indicator for unequal treatment.[315] Male applicants receive higher credit scores than women. – Person A is male; Person B is female. Person B pays higher interests. Due to an individual's gender, like situations are treated in an unlike manner. Gender says nothing about an individual's ability to repay one's loan. Critics might say that women, on average, earn less. However, this is based on societal, systematic, discriminatory patterns and biased view, for instance, the believe that women should give birth to children and due to their empathy raise them. Or, it is because woman just earn less and, thus, decide to raise children to have more money for the family

[315] Hurley and Adebayo, p. 149; see also W. Rice, 'Race, Gender, "Redlining," [sic!] and the Discriminatory Access to Loans, Credit, and Insurance: An Historical and Empirical Analysis of Consumers Who Sued Lenders and Insurers in Federal and State Courts, 1950-1995', *San Diego Law Review*, vol. 33, 1996, (accessed 31 May 2019).

life. The distinction is not based on reasonable and objective grounds. The action is not suitable to achieve the aim and not necessary as there are less intrusive measures to assess an individual's credibility.

- **Race**: In the same study, Hurley and Adebayo revealed that race is a factor for higher or lower credit scoring. The system, for instance, overtakes statistics that lead to underlying biases in its functioning.

  > Consumers' use of technology, shopping habits, social media practices, and other details are likely to vary by race and other sensitive factors. "Thirty percent of whites," for example, "use their mobile phone as their sole Internet connection compared to roughly forty-seven percent of Latinos and thirty-eight percent of blacks." When combined with other information, mobile and Internet usage practices could potentially be used as a proxy for race. If, during the process of ML, the model learns that race or another sensitive characteristic is highly correlated to credit risk, the model will attach greater significance to proxy variables that can serve as a stand-in for that sensitive characteristic. Even where data miners are careful, "they can still effect discriminatory results with models that, quite unintentionally, pick out proxy variables for protected classes."[316]

  Results do not go into further detail. One could reveal that more Black than White individuals cannot afford internet connection on their mobile on their phone as well as at home via Wi-Fi. Such a conclusion might lead to discrimination as the algorithm learns that Blacks, on average, have less money than Whites. Even if true, such distinctions root into systematic discrimination of society as, for instance, White individuals are preferred on the job market.[317] Race is an indicator for unequal treatment. Like situations are treated in an unlike manner based on the protected ground of race. The aim to score one's debtors is legitimate, however, the path to do so is not. The action is not suitable to achieve the aim. There must be least instructive measures or alternatives which do not focus on a discriminatory and racist practice.

Such criteria are based on biases, for instance, due to gender roles: women stay at home and care for their children and the household; ethnic origin: those who are not White suffer from stereotypes etc. Thus, it is important to eradicate biases. Coeckbergh states,

> It is really difficult to, in general, eradicate bias. In general, there will always be bias, but we can try to minimize it. We can do that with technical means, we can try to eradicate bias from data sets to have algorithms that are not biased. But this requires an awareness among IT people that what they are doing have impacts on things like bias. It is also important that smart companies who use such

[316] Hurley and Adebayo, pp. 182-183.

[317] Pager et al. revealed that even White ex-criminals are preferred over Black people. (See D. Pager et al., 'Discrimination in a Low-Wage Labor Market: A Field Experiment', *American Sociological Review*, vol. 74, 2009, p. 777 (accessed 18 June 2019).) – One can draw conclusions on the "race" or ethnic origin of individuals due to skin colour – although this is no guarantee for it to be true. White persons can have lived for generations in Nigeria, while Black person can have lived for generations in Sweden.

> techniques are accompanied and supported because they don't necessarily know much about societal problems and how to deal with it. It is more a societal issue – a really complex problem.[318]

Technical minimization of biases is possible because experts might evaluate some exemptions.

In short, concrete algorithmic steps for social scoring are hidden. Discriminatory practices go along non-transparent rating mechanisms; scholars could only reveal the tip of the iceberg. Nevertheless, it is concluded that discriminatory indicators play a role in credit assessments based on social scoring. Most likely, the above-mentioned factors are interlinked. Social scoring at least partly relies on existing discriminatory, systematic patterns, for instance, by drawing conclusions based on one or more of the following aspects: language, preferences, friends or followers, profession, gender, and race. As argued in this chapter, none of these categories gives reliable insights into a person's credit risk or creditworthiness. Assumptions based on generalizations and stigmatizations may harm the individual since no individual credit assessment can take place. In the following Subchapter 4.3.3.1, I am going to exemplify this hypothesis.

4.3.3.1 Case Study: Protection from Discriminatory Practices?

When Adaka starts her apprenticeship, she meets Tim who has applied for a loan of the same amount at the same time. However, Adaka pays an interest that is 5 percentage points higher than Tim's. He is White and lives with his parents in a good suburb. Adaka and Tim have the same credit history – apart from their social scoring credit, there is none. Like Adaka, he has no savings. However, he pays less. Adaka talks to a lawyer who asked the FinTech company for further information. He got some information. On average, people like Adaka who are female, Black, and live in a socially deprived area, received loans with higher interest rates. People like Tim who are male, White, raised in a good suburb and privileged to have received a proper education and language level received loans with lower interest rates.

Against this background, does the EU sufficiently protect Adaka against discrimination on protected grounds such as social origin, race, and gender?

[318] Coeckelbergh.

There are three indicators for unequal treatment:

(1) gender: Tim is male, Adaka is female;

(2) colour: Tim is White, Adaka is a person of colour;

(3) social origin: Tim lives in a rich suburb, Adaka in a socially deprived area.

Consequently, the distinction is made on the basis of the above-mentioned three protected grounds.[319] The credit scorer pursued the legitimate aim of assessing the credit applicants' creditworthiness and, thereof, to drive appropriate interests. However, the distinction is not based on reasonable and objective grounds. The action is not suitable to achieve the aim because Adaka might be much more reliant and hardworking than Tim and, thus, the candidate with a lower risk of credit default. The action is not necessary and wrong. There are better alternatives, for instance, a personality test both need to undergo before obtaining the loan. Of course, one would need to make sure the test is not based on biased assumptions.

Applicable Rights

Although the prohibition of discrimination is not absolute, [320] the EU does not sufficiently ensure it. The prohibition of discrimination stands always in conjunction with another EU law. Against this background, the following are applicable:

(a) the right to respect for one's private and family life,[321] especially the components
   i. 'the right to access to data which has been collected concerning him or her'[322],
   ii. and 'the right to have it [meaning personal data] rectified'[323],
   iii. 'the personal right to development'[324];

(b) the right to the protection of personal data[325] including the following aspects:
   i. fair processing,
   ii. and the right to rectification.

[319] Charter, Art. 21; Race Equality Directive (2000) OJ L 180/22, Art. 2.
[320] ibid, Art. 1; EU Treaties, Art. 3(3); Charter, Art. 21.
[321] ibid., Art. 7; Convention for the Protection of Human Rights and Fundamental Freedoms (1950) 4.XI., Art. 8.
[322] ibid., Art. 8(2).
[323] ibid.
[324] CJEU cited by Poullet, p. 778.
[325] Charter, Art. 8(2); EU Treaties, Art. 16(1).

Analysis

As '[p]rocessing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation'[326] is allowed where 'the data subject has given explicit consent'[327], the EU even paved the way for legal discrimination on protected grounds. The EU did not take appropriate measures to protect Adaka from the social scorer's discriminatory practices in conjunction with her (a) right to access all data which has been collected about her; her lawyer did not receive a detailed answer. Also, because transparency is lacking, she could not exercise her right to (a)ii and (b)ii have her data rectified. All in all, social scoring was conducted unfairly which infringed upon her right to (b)i fair processing. As a result, Adaka's (a)iii right to self-development is also less full-fledged than Tim's. Since he has more money to spend at the end of the month, he could save for his own apartment or other dreams he pursues. The EU has failed to protect Adaka from discriminatory social scoring services that concern both (a) her right to respect for her private life and (b) the right to protection of her personal data on SMD.

In conclusion, the EU should pass measures to ensure that balancing rights does not end in an unproportionate discrimination against individuals. Such provisions need to be targeted at social scoring practices relying on pre-set values such as gender and race. However, this affects AI-led algorithms in general.

4.3.4 Transparency for Accuracy and Accountability

Scoring companies do not want to give information regarding their algorithms. Existing laws do not sufficiently demand transparency. However, according to Hurley and Adebayo,

> [c]redit scoring companies treat their data sources as proprietary trade secrets. In practice, this means that consumers have no realistic means to understand which of the many seemingly inconsequential decisions they make each day could impact their credit ratings, and even less ability to challenge their scores, or test whether the input data are accurate.[328]

[326] GDPR, Art. 9(1).
[327] ibid., Art. 9(2.b).
[328] Hurley and Adebayo, pp. 179-180.

To give an example, in 2014, the German Supreme Court ruled that SCHUFA does not have to reveal its scoring algorithm; the public discussion started already in 2012 when SCHUFA announced it would test social scoring based on Twitter and Facebook data.[329] However, especially data protectionists were outraged. Thus, SCHUFA stopped its approach. Its partner, the Hasso-Plattner-Institut cancelled its contract due to misunderstandings in the public. Not only data protectionists but also German politicians were shocked – even those from the liberal party, a party that rather supports self-regulation instead of state regulation. His name is Rainer Brüderle. 'SCHUFA's plans go too far,' he said. 'Social networks, like a circle of friends, are part of a person's private life, and should therefore not be tapped.'[330] Although the CJEU ruled SCHUFA does not have to reveal its scoring secrets, SCHUFA made clear, '[w]e do not use any information from social media to compute our scores, likewise no names or other discriminating data.'[331] The CJEU's rule was counter-productive to citizens' and consumers' rights and beneficial for businesses. The judgement paved the way for a rights balance in favour of businesses instead of individuals – a failure of the CJEU.

As Marriott and Robinson argue, it is highly unlikely that existing laws 'address adequately the serious accuracy, transparency, and accountability concerns of individual data subjects.'[332] HLEG AI expert Coeckelbergh argues similarly:

> I think it is necessary to have legal measures that solve especially the problems concerning transparency and non-discrimination that certain kind of AI endanger. We already have the GDPR; there need to be discussions, if things should be made stronger: When it comes to explainability, there has been criticism that there is the right to information but not really full explainability. A good way to deal with responsibility and accountability, one should implement better measures for traceability.[333]

If a decision is made about you by people based on automated social scoring, the decision should be comprehensible for the conducting businesses so that contact persons are able to justify that decision, which means they need to provide information on how this

---

[329] 'Schufa will Facebook-Profile auswerten', *Frankfurter Allgemeine Zeitung*, 7 June 2012, https://www.faz.net/aktuell/wirtschaft/pruefung-der-kreditwuerdigkeit-schufa-will-facebook-profile-auswerten-11776537.html (accessed 17 June 2019).

[330] V. Medick and S. Weiland, 'Surfing for Details: German Agency to Mine Facebook to Assess Creditworthiness', *Spiegel Online*, 7 June 2012, https://www.spiegel.de/international/germany/german-credit-agency-plans-to-analyze-individual-facebook-pages-a-837539.html (accessed 30 April 2019).

[331] 'How Does Scoring Work at SCHUFA?' (*SCHUFA*) <https://www.schufa.de/en/about-us/data-scoring/scoring/scoring-work-schufa/how_does_scoring_work_at_schufa.jsp> (accessed 17 June 2019).

[320] Marriott and Robinson, p. 1.

[333] Coeckelbergh.

decision is made. It creates an obligation of informing people. There should be legal measures on how to make it transparent.[334] Matz et al. agree,

> consumers need to be made aware of the possibilities that predictive technologies hold, and the fact that social media data … can reveal a lot more about them than they might think.[335]

The reason for this is simple and was already indicated: Individuals have a right to information. They have the right to give informed consent, meaning to be informed about what is going to happen with the data – a provision that is not absolute. Huge sets of data, however, may not be intelligible to a layperson while it is intelligible to a computer.[336]

> Assuming that a diligent applicant could first identify an error among the thousands of entries in the credit scorer's raw data set, it is unlikely that the applicant would have the capacity to prove that the error resulted in a faulty score. As one study puts it, '[a] credit score rests upon [the scorer's] accrual of as many records and cross-correlations of a borrower's financial decisions as possible. [Credit scorers] then reductively collapse the entangled mass of correlations of those activities to a three-digit number, supposedly imbued with comparative social meaning.' Because the data transformation process likely involves numerous aggregations and combinations of data points, as well as subjective decisions by the data scientist, applicants are likely to have few means to effectively challenge their scores.[337]

Such faulty data sets can result in discrimination as exemplified in the last case study.

Thus, transparency cannot only help to discover discrimination but, as a logical consequence, also data accuracy. In the credit scoring industry, scorers rely on huge sets of data. The bigger the set, the more likely it is to be flawed.[338] As every individual has the right to have their data rectified,[339] the right involved with data accuracy is closely bound to the issue of transparency which increases pressure on scorers to assess creditworthiness to its most comprehensive and true extent. Of course, transparency is no miracle cure for accuracy and non-discrimination. However, it can reveal patterns that may be evaluated by experts and understood by laypersons. HLEG AI confirms, 'that transparency cannot prevent non-discrimination or ensure fairness, and is not the panacea against the problem of scoring.'[340] However, after algorithmic strategies have been revealed, individuals can evidentially claim for their rights to be protected before a court.

[334] ibid.
[335] Matz et al., pp. 10-11.
[336] Hurley and Adebayo, pp. 179-180.
[337] ibid.
[338] ibid., p. 178.
[339] GDPR, Art. 16.
[340] HLEG AI, p. 34.

To put it concisely, transparency is crucial for preventing inaccurate data, based on discriminatory sets of values, and a lack of accountability. Algorithms with a huge impact on individual's private life need to be more transparent to avoid systematic flaws: If the algorithmic functioning is revealed, academia and civil society can review the system and pinpoint weaknesses. Increasing the pressure to act, transparency may most likely increase the whole social scoring system. First, courts or lawmakers need to redefine the term "business secret". Economic growth cannot be counterbalanced with fundamental individual rights.

4.3.5 Joint Responsibility and Liability

Joint responsibility is more important than ever, especially when it comes to social scoring. Social media such as Facebook, LinkedIn, and Twitter provide data for social scorers to assess a data subject's creditworthiness. The first two parties are joint controllers who share to some extent processing purposes and means. Thus, they are responsible for their processing operations. Art. 26 of the GDPR as well as a CJEU judgement in Case C-210/16 has already manifested the concept of joint responsibility.

However, the EU faces challenges due to insufficient legal interpretations on how to determine the degree of responsibility and liability of data processing if more than one controller is responsible for the processing operations. General Advocate Bobek confirmed in Case C-40/17 that it is crucial to not only define the parties who bear responsibility but also for what exactly they are responsible. The EU needs to establish a kind of catalogue that determines different stages of responsibility in order to prevent unlawful processing operations for safeguarding the individuals' data and, ultimately, their privacy.

In short, the pending preliminary ruling by the CJEU in Case C-40/17 bears potential for a more comprehensive interpretation of the concept of "joint responsibility" and "joint liability" of joint controllers. It might clarify the question of what controller is responsible for what processing operation or action. So far, "joint responsibility" just determines controllers to be jointly responsible when they share purpose and means of their operations to a certain extent. This, however, is not enough to effectively hold them responsible and liable for the processing. Regarding social scoring, this concept must be

comprehensively interpreted, or individuals will further be exploited when it comes to their personal data and privacy.

4.3.6 Broad definitions

All the critiques mentioned follow one red line: Despite several legal definitions, lawmakers did not eradicate legal grey zones. Therefore, it is highly complicated to evidentially and clearly balance the rights against each other. Examples have been mentioned in the previous Chapters 4.3.1 to 4.3.4; catchwords are consent, non-discrimination, anti-discrimination, transparency, accuracy, and accountability. More concrete definitions are necessary to explicitly pinpoint legal loopholes. If not by lawmakers, the CJEU needs to further define the legal basis.

Part of this is also to define "privacy" in a more precise way than before while still leaving the opportunity to shape it in favour of individuals if future developments make it necessary to do so. In fact, there are more data than explicit privacy provisions. 'Data [p]rotection is nothing more than a *tool* to ensure Privacy and is a pre-condition of all our freedoms and our dignity'[341], Poullet criticises. Data protection itself is insufficient to protect an individual's fundamental right to privacy. An innovative narrative must be told, not about data protection but about a person's private life, the right to seclusion and inclusion – put simply, privacy in general.

Beyond that, HLEG AI raises a further concern, '[y]et even in circumstances where compliance with legal requirements has been demonstrated, these may not address the full range of ethical concerns that may arise.'[342] There might be even more issues that experts have not sufficiently thought about yet, because automated or even self-learning mechanisms will be improved and may develop a mechanism that is incomprehensible for a sole human being. In this light, HLEG AI calls upon lawmakers to clearly define,

> when and how AI can be used for automated identification of individuals and differentiating between the identification of an individual vs the tracing and tracking of an individual, and between targeted surveillance and mass surveillance. … The application of such technologies must be clearly warranted in existing law.[343]

[341] Poullet, p. 778.
[342] HLEG AI, p. 33.
[343] ibid., pp. 33-34.

This argument opens a whole new world of scientific questions that need to be answered but are outside the direct scope of this thesis. However, it is though necessary to mention it as it, at least indirectly, concerns social scoring that is by nature automated.

Altogether, the root cause of the critiques is definitions that are too broad and plenty of them do not explicitly target the provisions' connection to the fundamental right to privacy. To give some examples: What is consent and what specific regulations can diminish the above-mentioned loopholes? How much transparency is necessary for a process to be transparent? What set of values leads to what decision or how does it influence the credit score? Who is accountable for the credit score or, in general, AI-led technologies? This list of questions is not exhaustive.

4.4 Concluding Remarks

Besides the speculation that Trustworthy AI might introduce a trend towards self-regulations that may pre-empt law, the following points have been identified as shortcomings in EU law:

- **Transparency** provisions are lacking in the entire field of AI. Regarding this thesis, credit scorers do not offer full insight into their algorithms and calculations – although this is necessary for the individual to be informed about the scoring they are consenting to. Non-transparent processes might even further open a Pandora's box for discrimination because watchdogs such as academia, NGOs, and civil society cannot evidentially evaluate ongoing processes.
- **Consent** requirements do not comprehensively protect individuals from actions that infringe upon an individual's privacy. Formal consent by, for instance, clip-wrapping does neither ensure informed, specified, and unambiguous consent because one can click through the agreement without even reading and/or understanding it. Nor can such kind of consent ensure it is freely given, particularly because of the power imbalance between the scorer and credit applicant.
- **Anti-discrimination** laws are too weak to protect individuals from algorithmic flaws which are hard to reveal. Established algorithmic flaws support discriminatory regulations which lead to systematic discriminations of everybody who falls into a certain category, for instance, a social group which the algorithm scores down.

- **Accuracy** of data is at risk due to certain calculations, for example, living in a Black area decreases one's credit score. Besides being discriminatory, such a general criterion is not legitimate because there is no individual assessment.
- **Accountability** is hardly given because there is no agreement on who is accountable for scoring systems that contain flaws which might lead to discrimination: Is it the scorer, the programmer, or somebody else?
- **Joint responsibility** has been introduced as a vague concept. A pending ruling by the CJEU might clarify the question of what joint controller can be held liable for what action. No sufficient ruling has been passed yet which determines the degree of, on the one hand, a social media controller and, on the other hand, a social scoring controller can be held responsible for the SMD processing. It is hard to evaluate whom to hold liable for breaches with the law. Referring to the General Advocate's concern mentioned in Chapter 4.2.6.3.2, if everybody is responsible, joint controllers hide behind each other and none of them can be easily held liable for the processing.
- **Broad definitions** leave it to business practices or, if a business is sued, to courts to determine whether a certain social scoring method is allowed. To eradicate the risk that such a definition leads to unproportionate privacy infringements, lawmakers need to ensure further guidance through more comprehensive definitions established in EU hard law.

Conclusively, there are some provisions the EU has passed to ensure the fundamental right to privacy in the face of social scoring. However, there are still many loopholes that result in hard law shortcomings.

The final say in this argumentation is up to Marriott and Robinson who conclude:

> We cautioned against continued reliance on consent while welcoming the apparent shift in emphasis from protection to inclusion and empowerment through greater transparency, the possibility to contest a decision and the right to meaningful information about the logic involved in processing. For the lofty aspirations of the next generation of data protection law to have practical effect, stronger, more streamlined enforcement of the new regime must be allied to the building of meaningful dialogue between data privacy lawyers and regulators, those behind the code, and those who use it.[344]

[344] Marriott and Robinson, p. 69.

5. Conclusion

This thesis analysed the legal shortcomings upon which the EU needs to improve when safeguarding the fundamental right to privacy in the face of social scoring. This technique relies on processing SMD for assessing one's credibility and credit default. The result is called credit score which is analysed by an at least partly-, if not fully-automated algorithm.[345]

The most important applicable EU laws regarding social scoring legislation are the following:

- EU Treaties, especially Art. 3(3), 10, 16(1);
- ECHR, especially Art. 6(2) to (3), 8;
- Anti-Discrimination Directive, especially Art. 1, 2;
- Charter, especially Art. 6(1), 7, 8(1) to (2), 21, 52(1) and (3), 57 (7);
- E-Privacy Directive, especially Art. 1(1), 5(1) to (3), 9(1) to (2), 10;
- GDPR, especially Recitals 1, 42, 71, 85, 173 as well as Art. 1(1), 2(1), 3(1), 4(11), 5, 6, 7(4), 9(1) to (2) (a) to (c) and (g), 12(1), 13(2), 22(1) to (2), 23(1), 26, 60, 71, 95.

Due to the Commission's statement to observe trends in the light of self-development and to adjust respective laws, it might be that Trustworthy AI is going to have a bigger influence on privacy regulations than usual soft law; however, it is not as important yet and, thus, not part of the above-mentioned list.[346]

Regarding social scoring, legislation is not comprehensive and up-to-date. Policy makers need to discuss current developments. Answering this research question, it is evident that the EU faces shortcomings as described in Chapter 4.3. Particularly the following statements reveal major problems which need to be tackled:

(a) Social scoring is consented to online. Lawful consent requires to be free, informed, and unambiguous by the credit applicant. Click-wrapping is not the right way to gain consent because it cannot ensure consent to be informed; studies prove almost everybody does not read the terms and conditions as well as privacy regulations. It is more than questionable whether consenting is the right way to ensure that credit

[345] See Chapter 3.1. – Lenddo and ZestFinance are only two examples of social scoring companies. (See Chapters 3.1.5.1 to 3.1.5.1.)
[346] See Chapter 4.

applicants understand the consequences and to know about their alternatives. When it comes to social scoring, this issue is even more pressing because click-wrapping aggravates the situation due to a lack of information. Also, due to the inherent power imbalance within the financial sector, borrowers are more dependent on the lender. Conclusively, consent is a formality rather than a voluntary, reflected, and wholehearted act of agreeing; consent is not given freely.

(b) Regarding Art. 22(2)(a) on the right to object automated individual decision-making, including profiling, it is questionable whether consent is truly necessary for social scoring. The provision states that consent is not required when automated individual decision-making is necessary for social scoring. In this case, the data subject shall not have the right to object an automated social scoring decision; lawmakers have not yet determined whether social scoring falls into this definition. If consent is necessary, the EU must further clarify who is responsible for obtaining consent (see (e)).

(c) Partly- or fully-automated social scoring bears the risk of applying underlying biases in the process of credit assessment. This leads to problems with data accuracy. Once it is established in the algorithmic mechanism, systematic discrimination is takes place. Those few studies that have been obtained on the issue of credit scoring, reveal that, for example, Black women with little money and a certain type of language obtain a lower credit score. Such presumptions rely on generalizations and place individuals in a greater, more superficial category that might disadvantage them by deriving their illusive character traits. The EU needs stricter anti-discrimination provisions that cannot be easily overrun by any other right. The right to be free from discrimination should be more steadfast because it is the core of inequalities and the fundament of a world where people are left behind.

(d) Somehow automated algorithms are hard to decrypt – especially for laypersons. Hidden mechanisms of the company's secret system may contain bias, flaws and, thus, lead to discrimination. Decisions based on fully automated algorithms that are based on ML cannot be decrypted anymore – not even by the company's experts. They probably cannot derive why exactly the credit score has been assessed as it is.

(e) Insufficient transparency leads to a lack in accountability. The EU must answer the following question: Who is responsible for problems with accuracy, discriminating

algorithms, and flaws in the credit score? Otherwise, this shortcoming is a legally accepted loophole that will be harder to eradicate as time goes on; it will encounter more critiques by a growing number and power of social scorers. Therefore, demands have become louder to create a transparent credit scoring system. Improving transparency has the potential to eradicate discrimination due to pressure by individuals, activists, and politicians. One feature to increase transparency is so-called "joint responsibility" by controllers. Those sharing the same purpose and means are jointly responsible and liable for their processing operations. However, more comprehensive legally-binding interpretations must be published to answer the following questions: Who is responsible for what exactly? If controllers of social media and social scoring platforms are joint controllers, who is obliged to obtain consent? Pending before the CJEU, Case C-40/17 bears the potential to offer answers to these questions; academics need to monitor future developments.

(f) Many of these points come back to a basic problem: too broad definitions, or put differently, a lack of details. Questions remain open: What is real consent? Is automated individual decision-making, including profiling, necessary for social scoring? When is anti-discrimination negotiable? What exactly must be provided for when it comes to transparency? Are controllers of social media and social scoring platforms jointly responsible? If so, for which of the ongoing processing operations is each party responsible; who exactly is accountable? These questions must be answered – rather today than tomorrow.

(g) Regarding the recently published AI Ethics, critics have concerns about increasing shortcomings or loopholes by EU law. The Commission instructed to observe trends of self-regulation and, if necessary, to review existing standards in accordance with the EU's fundamental rights. Critics fear that existing standards might be opened to benefit AI technologies such as social scoring to keep up with global AI trends. These need to be further monitored to pre-empt a negative development of privacy and data protection laws.

The above-mentioned bullet points present the most pressing needs which must be discussed and satisfied as soon as possible.[347] Fundamental rights should not be negotiable when counterbalanced with economic growth that is rather benefiting businesses than individuals. Regarding social scoring, lawmakers need to discuss these problems before systematic violations of the fundamental right to privacy become part of our daily lives. The time to act is now.

[347] Of course, this list of criticism does not claim to be exhaustive.

II. Bibliography

'About Us' (FriendlyScore) <https://friendlyscore.com/about> (accessed 30 April 2019).

'Artificial Intelligence' (MyBucks) <https://corporate.mybucks.com/technology> (accessed 30 April 2019).

Ayres, I. and A. Schwartz, 'The No-Reading Problem in Consumer Contract Law', *Stanford Law Review*, vol. 66, no. 3, 2014, pp. 545-610 (accessed 18 June 2019).

Bakos, Y. et al., 'Does Anyone Read the Fine Print? Consumer Attention to Standard-Form Contracts', *The Journal of Legal Studies*, vol. 43, no. 1, 2014, pp. 1-35 (accessed 18 June 2019).

Bruckner, M., 'The Promise and Perils of Algorithmic Lenders' Use of Big Data', *Chicago-Kent Law Review*, vol. 93, no. 1, 2018, pp. 3-60 (accessed 14 June 2019).

CJEU, 'An Internet Search Engine Operator is Responsible for the Processing that It Carries Out of Personal Data Which Appear on Web Pages Published by Third Parties' (*Press Release*, 13 May 2014) <https://curia.europa.eu/jcms/upload/docs/application/pdf/2014-05/cp140070en.pdf> (accessed 17 June 2019).

Commission, 'Artificial Intelligence: Commission Outlines a European Approach to Boost Investment and Set Ethical Guidelines' (*Press Release*) IP/18/3362.

Commission, 'Artificial Intelligence: Commission Takes forward its Work on Ethics Guidelines' (*Press Release*) IP/19/1893.

Commission, 'Artificial Intelligence for Europe' (*Press Release*) IP/19/1893.

Commission, 'Coordinated Plan on Artificial Intelligence' (*Communication*) COM(2018) 795 final.

Commission, 'Proposal for a Regulation of the EP and of the Council concerning the Respect for Private Life and the Protection of Personal Data in Electronic Communications and Repealing Directive 2002/58/EC' (*Communication*) COM (2017) 10 final.

Commission, 'Upgrading the Single Market: More Opportunities for People and Business' (*Communication*) COM(2015) 550 final.

'Condition Sine Qua Non' (*Collins*) <https://www.collinsdictionary.com/dictionary/french-english/condition-sine-qua-non> (accessed 7 June 2019).

Cormen, T. et al., *Introduction to Algorithms*, Cambridge, MIT Press, 2009.

Crosman, P., 'This Lender Is Using AI to Make Loans through Social Media' (*American Banker*, 28 December 2017) <https://www.americanbanker.com/news/this-lender-is-using-ai-to-make-loans-through-social-media> (accessed 30 April 2019).

'Data' (*Lexico Powered by Oxford*) <https://en.oxforddictionaries.com/definition/data> (accessed 29 April 2019).

'Data Protection' (European Data Protection Supervisor) <https://edps.europa.eu/data-protection/data-protection_en> (accessed 17 June 2019).

DPWP, 'Guidelines on Automated Individual Decision-Making and Profiling for the Purpose of Regulation 2016/679' (Guidelines, 3 October 2017) WP251rev.01.

DPWP, 'Guidelines on Consent under Regulation 2016/679' (Guidelines, 28 November 2017) WP259 rev.01.

ECtHR, 'Accession of the EU' (*ECtHR*) <https://www.echr.coe.int/Pages/home.aspx?p=basictexts/accessionEU&c=> (accessed 7 June 2019).

'Electronic Data Processing', (*Lawinsider*) <https://www.lawinsider.com/dictionary/electronic-data-processing> (accessed 29 April 2019).

Email from Lauren Saunders to Laura Temel (30 September 2015) <https://www.nclc.org/images/pdf/rulemaking/treasury-marketplace-loan-comments.pdf> (accessed 14 June 2019).

'Empowering Through Lending' (*MyBucks*) <https://corporate.mybucks.com/lending> (accessed 30 April 2019).

EU, 'Sources of European Union Law' (*EUR-Lex*, 13 December 2007) <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM%3Al14534> (accessed 25 April 2019).

EU, 'The Non-Written Sources of European Law: Supplementary Law' (*EUR-Lex*, 12 March 2018) <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM:l14533> (accessed 23 April 2019).

EU, 'The European Union's Primary Law' (*EUR-Lex*, 2March 2018) <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM:l14530> (accessed 2 April 2019.)

'Fast, Free and Easy Credit Scores' (*Friendly Score*) <https://friendlyscore.com/individuals/fast-free-and-easy-credit-scores> (accessed 14 June 2019).

Fischer, B. and M. Mazewski, Analysis of Processing Electronic Communication Data on the Basis on Consent in the Light of Council's e-Privacy Regulation Proposal', *Journalism Research Review Quarterly*, vol. 4, 2017, p. 92.

FRA, 'Frequently Asked Questions' (*FRA*) <https://fra.europa.eu/en/about-fundamental-rights/frequently-asked-questions#difference-human-fundamental-rights> (accessed 17 June 2019).

FRA and CoE, *Handbook on European Data Protection Law*, European Union, 2014 (accessed 30 April 2019).

'Free Credit Scores. Check and Report' (*Friendly Score*) <https://friendlyscore.com/> (accessed 30 April 2019).

French, C., *Data Processing and Information Technology*, Boston, Cengage Learning EMEA, 1996.

Graham, B. and C. Paul, 'Does Higher Education Really Lead to Higher Employability and Wages in the RMI?', *Journal of Southeast Asian Economies*, vol. 35, no. 1, 2018, pp. 1-3 (accessed 18 June 2019).

Guitierrez, D., 'Inside Big Data. Guide to Big Data for Finance', *Dell EMC*, White Paper, 2015, pp. 1-14 (accessed 30 April 2019).

Gül, S. et al., 'A Multiple Criteria Credit Rating Approach Utilizing Social Media Data', *Data & Knowledge Engineering*, vol. 116, 2018, pp. 80-99 (accessed 20 April 2019).

HLEG AI, 'Ethics Guidelines for Trustworthy AI' (*Guidelines*).

'How Does Scoring Work at SCHUFA?' (*SCHUFA*) <https://www.schufa.de/en/about-us/data-scoring/scoring/scoring-work-schufa/how_does_scoring_work_at_schufa.jsp> (accessed 17 June 2019).

Hertza, V., 'Fighting Unfair Classifications in Credit Reporting: Should the United States Adopt GDPR-Inspired Rights in Regulating Consumer Credit?', *NYU Law Review*, vol. 93, 2018, pp. 1707-1741 (accessed 15 April 2019).

Hurley, M. and J. Adebayo, 'Credit Scoring in the Era of Big Data', *Big Data*, vol. 18, no. 1, 2017, pp. 148-216 (accessed 21 April 2019).

Krzysztofek, M., *GDPR: General Data Protection Regulation (EU) 2016/679: Post-Reform Personal Data Protection in the European Union*, Köln, Kluwer, 2018.

‘Legal Person’ (*Wordnik*) <https://www.wordnik.com/words/legal%20person> (accessed 30 April 2019).

Lunt, C., ‘United States Patent: 9100400 - Authorization and Authentication Based on an Individual’s Social Network’, (*United States Patent*, 4 August 2015) <http://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO1&Sect2=HITOFF&d=PALL&p=1&u=%2Fnetahtml%2FPTO%2Fsrchnum.htm&r=1&f=G&l=50&s1=9100400.PN.&OS=PN/9100400&RS=PN/9100400> (accessed 2 Mai 2019).

‘Machine Learning’ (*Merriam-Webster*) <https://www.merriam-webster.com/words-at-play/what-does-machine-learning-mean accessed> (accessed 9 May 2019).

Mann, R. and T. Siebneicher, ‘Just One Click: The Reality of Internet Retail Contracting’, *Columbia Law Review*, vol. 108, no. 4, 2008, pp. 984-1012 (accessed 10 June 2019).

Marriott, J. and G. Robinson, ‘To Score and to Protect? Big Data (and Privacy) Meet SME Credit Risk in the UK’, *International Data Privacy Law*, vol. 7, no. 1, 2017, pp. 48-69 (accessed 13 April 2019).

Matz, S. et al., ‘Predicting Individual-Level Income from Facebook Profiles’, *PLoS ONE*, vol. 14, no. 3, 2019, pp. 1-13 (accessed 9 May 2019).

Medick, V. and S. Weiland, ‘Surfing for Details: German Agency to Mine Facebook to Assess Creditworthiness’, *Spiegel Online*, 7 June 2012, https://www.spiegel.de/international/germany/german-credit-agency-plans-to-analyze-individual-facebook-pages-a-837539.html (accessed 30 April 2019).

Meyer, R., ‘Could a Bank Deny Your Loan Based on Your Facebook Friends?’, *The Atlantic*, 25 September 2015, https://www.theatlantic.com/technology/archive/2015/09/facebooks-new-patent-and-digital-redlining/407287 (accessed 22 Mai 2019).

Obar, J. and A. Oeldorf-Hirsch, ‘The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services’, *Information, Communication & Society*, vol. 1, 2018, pp. 1-20 (accessed 18 June 2019).

O’Dwyer, R. ‘Cache Society: Transactional Records, Electronic Money, and Cultural Resistance’ *Journal of Cultural Economy* 12, vol. 12, no. 2, 2019, pp. 1-21 (accessed 18 June 2019).

Pager, D. et al., ‘Discrimination in a Low-Wage Labor Market: A Field Experiment’, *American Sociological Review*, vol. 74, 2009, p. 777-799 (accessed 18 June 2019).

Pasquale, F., 'The Black Box Society: The Secret Algorithms That Control Money and Information', *Contemporary Sociology*, vol. 5, no. 3, 2016, pp. 367-368 (accessed 29 April 2019).

Plaut, V. and R. Bartlett, 'Blind Consent? A Social Psychological Investigation of Non-Readership of Click-through Agreements', *Law and Human Behavior*, vol. 36, no. 4, 2012, pp. 293-311 (accessed 10 June 2019).

Poullet, Y., 'Is the General Data Protection Regulation the Solution?', *Computer Law & Security*, vol. 34, 2018, pp. 773-778 (accessed 18 June 2019).

Preoţiuc-Pietro, D. et al., 'Studying User Income through Language, Behaviour and Affect in Social Media', *PLoS ONE*, vol. 10, no. 9, 2015, pp. 1-17 (accessed 9 May 2019).

Prosser, W., 'Privacy', *California Law Review*, vol. 48, no. 3, 1960, pp. 383-423 (accessed 28 April 2019).

'Prüfung der Kreditwürdigkeit: Schufa will Facebook-Profile auswerten', *Frankfurter Allgemeine Zeitung*, 7 December 2012 <https://www.faz.net/1.1776537> (accessed 14 June 2019).

'Regulations, Directives and Other Acts' (European Union) <https://europa.eu/european-union/eu-law/legal-acts_en> (accessed 17 June 2019).

Rice, W. 'Race, Gender, "Redlining," [sic!] and the Discriminatory Access to Loans, Credit, and Insurance: An Historical and Empirical Analysis of Consumers Who Sued Lenders and Insurers in Federal and State Courts, 1950-1995', *San Diego Law Review*, vol. 33, 1996, pp. 583-699 (accessed 3 May 2019).

Sokol, P. et al., 'Honeypots and Honeynets: Issues of Privacy', *EURASIP Journal on Information Security*, vol. 4, 2017, pp. 1-9 (accessed 30 April 2019).

'Schufa will Facebook-Profile auswerten', *Frankfurter Allgemeine Zeitung*, 7 June 2012, https://www.faz.net/aktuell/wirtschaft/pruefung-der-kreditwuerdigkeit-schufa-will-facebook-profile-auswerten-11776537.html (accessed 17 June 2019).

'Social Scoring System: Überwachung wie in China auch bei uns?', *PSW Group Consulting Blog* [web blog] <https://www.psw-consulting.de/blog/2018/12/27/social-scoring-system-ueberwachung-wie-in-china-auch-bei-uns/> (accessed 14 June 2019)

'Treaty on the European Union (TEU)/ Maastricht Treaty' (*EP*) <http://www.europarl.europa.eu/about-parliament/en/in-the-past/the-parliament-and-the-treaties/maastricht-treaty> (accesses 7 June 2019).

'Treaty on the Functioning of the European Union' (*EP*) <http://www.europarl.europa.eu/about-parliament/en/in-the-past/the-parliament-and-the-treaties/treaty-of-rome> (accessed 7 June 2019).

Wagner, B., 'Ethics as an Escape from Regulation: From Ethics-Washing to Ethics-Shopping?' (*The Privacy & Sustainable Computing Lab*, 11 July 2018) <https://privacylab.at/1064/ethics-as-an-escape-from-regulation-from-ethics-washing-to-ethics-shopping/>, pp. 1-4 (accessed 17 June 2019).

Warren, S. and L. Brandeis, 'The Right to Privacy', *Harvard Law Review*, vol. 4, no. 5, 1890, pp. 209-225 (accessed 15 April 2019).

Waschbusch, G., 'Social Scoring' (*Gabler Banklexikon*, 16 November 2018) <https://www.gabler-banklexikon.de/definition/social-scoring-99668/version-348651> (accessed 16 May 2019).

Wei, Y. et al., 'Credit Scoring with Social Network Data', *Marketing Science* 35, no. 2, 2015, pp. 234-258 (accessed 6 May 2019).

Westbrook, R., 'The Origin of Laesio Enormis', *Raymond Westbrook* 50, no. 49, 2008, 39-52.

'World's First Social Media Credit Scoring Model Launched for Europe' (*Big Data Scoring*) <https://www.bigdatascoring.com/press-release-worlds-first-social-media-credit-scoring-model-launched-for-europe> (accessed 30 April 2019).

Zhang, Y. et al., 'Research on Credit Scoring by Fusing Social Media Information in Online Peer-to-Peer Lending', *Procedia Computer Science*, vol. 91, 2016, pp. 168-174 (accessed 15 Mai 2019).

Zuiderveen Borgesius, F. and W. Steenbruggen, 'The Right to Communications Confidentiality in Europe: Protecting Privacy, Freedom of Expression, and Trust', *Theoretical Inquiries in Law*, vol. 20, no. 1, 2019, pp. 291-322 (accessed 5 May 2019).

Legal Sources

Charter of Fundamental Rights of the European Union (2012) OJ C 326/391.

CJEU, C-131/22 (2014), *Google Spain vs. Agencia Espanola de Protecctión de Datos*, 13 May 2014.

CJEU, C-212/13, *Rynes vs. Urad*, 1 December 2014.

CJEU, C-362/14, *Schrems vs. Data Protection Commissioner*, 6 October 2015.

CJEU, C-210/16 [2018], *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH*, 5 June 2018.

CJEU, Case C673/17 [2017], *Planet49 v Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V.*, 30 November 2017.

CJEU, Case C673/17 [2017], *Request for a Preliminary Ruling from the Bundesgerichtshof (Germany) Lodged on 30 November 2017, Planet49 v Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V.*, 30 November 2017.

CJEU, Case C673/17 [2017], *Opinion of Advocate General Szpunar delivered on 21 March 2019, Planet49 v Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V.*, 30 November 2017.

ECtHR, *Taliadorou and Stylianou v. Cyprus*, no. 39627/05, 16 October 2008.

Council Directive 2000/43/EC of 29 June 2000 Implementing the Principle of Equal Treatment between Persons Irrespective of Racial or Ethnic Origin (2000) OJ L 180/22.

Consolidated Version of the Treaty of the European Union (2008) OJ C115/13.

Convention for the Protection of Human Rights and Fundamental Freedoms (1950) 4. XI.

Decisions appointing the European Data Protection Supervisor and the Assistant Supervisor (2014) OJ L 351/9.

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (1995) OJ L 281.

Council Directive 2000/43/EC of 29 June 2000 Implementing the Principle of Equal Treatment between Persons Irrespective of Racial or Ethnic Origin (2000) OJ L 180/22.

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector OJ L 201/37.

Directive (EU) 2016/680 on the Protection of Natural Persons with Regard to the Processing of Competent Authorities for the Purpose of the Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties, and on the Free Movement of Such Data, and Repealing Council Framework Decision (2016) OJ L 119/89.

International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171.

Regulation (EC) No 45/2001 on the Protection of Individuals with Regard to the Processing of Personal Data by the Community Institutions and Bodies and on the Free Movement of Such Data (2001) OJ L 8/1.

Regulation (EU) 2016/679 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 95/46/EC (2016) OJ L 119/1.

Treaty of Lisbon Amending the Treaty on European Union and the Treaty Establishing the European Community (2007) OJ C 306/1.

UN GA Res 217 A.

UN GA Res 45/95, 14 December 1990.

Interviews

Coeckelbergh, M., Interview, Vienna, 29 Mai 2019.

Tschohl, C., Interview, Vienna, 4 June 2019.

III. Overview of Figures

IV. Abstract

Social scoring is the future of financial lending. It builds upon processing *social media data* (SMD) for a creditworthiness assessment. Spreading around the globe, social scoring is also practiced in some Member States of the EU. Before the business booms, it is crucial to assess the legal scope and shortcomings regarding the fundamental right to privacy to prevent systematic violations; breaches of the law are connected to a variety of other fundamental rights violations. Facing this development, this thesis is dedicated to answering the following question: **What shortcomings does the EU need to improve when safeguarding the fundamental right to privacy in the case of social scoring?** The first chapter describes social scoring systems and provides examples of the systems by Lenddo and ZestFinance. Secondly, the EU's legal scope is examined. Finally, the EU's legal shortcomings regarding social scoring practices are revealed.

Key words: EU • fundamental right to privacy • data protection • social scoring • automated individual decision-making

---

Social Scoring ist die Zukunft der Kreditvergabe. Es baut auf die Verarbeitung von Social-Media-Daten, die zur Bonitätsprüfung gesammelt werden. Das Geschäftsmodell verbreitet sich weltweit. Es wird auch in einigen Mitgliedsstaaten der EU praktiziert. Bevor das Geschäft boomt, ist es wichtig, den rechtlichen Rahmen abzustecken sowie dessen Defizite zu untersuchen, um systematischen Rechtsbrüchen vorzubeugen; Rechtsbrüche sind mit einer Vielfalt von weiteren Menschenrechtsverletzungen verbunden. Wegen dieser Entwicklung ist diese Masterarbeit der folgenden Forschungsfrage gewidmet: **Welche Defizite muss die EU ausbessern, um das Grundrecht auf Privatsphäre im Rahmen von Social Scoring zu gewährleisten?** Das erste Kapitel beschreibt Social-Scoring-Systeme und veranschaulicht solche von Lenddo und ZestFinance. In einem zweiten Schritt wird der rechtliche Rahmen der EU abgesteckt. Schließlich werden die rechtlichen Defizite der EU angesichts Social Scorings offengelegt.

Schlagwörter: EU • Grundrecht auf Privatsphäre • Schutz personenbezogener Daten • Social Scoring • automatisierte Entscheidungen im Einzelfall