Socially Responsible Virtual Assistant for Privacy Protection: Implementing Trustworthy AI*

Alžběta Krausová[1][0000−0002−1640−9594], Miloslav Konopík[2][0000−0001−7397−1658], Ondřej Pražák[2][0000−0001−5445−7792], Jakub Sido[2][0000−0002−7709−7512], Veronika Žolnerčíková[1][0000−0002−6363−0734], Václav Moravec[3][0000−0002−3349−0785], and Jaromír Volek[4][0000−0001−8407−811X]

[1] Institute of State and Law, Czech Academy of Sciences, Prague, Czech Republic
alzbeta.krausova@ilaw.cas.cz
[2] Faculty of Applied Sciences, University of West Bohemia, Pilsen, Czech Republic
[3] Faculty of Social Sciences, Charles University, Prague, Czech Republic
[4] FOCUS - Social Research and Marketing Agency, Brno, Czech Republic

Abstract. The paper introduces an AI-based virtual assistant VILEM whose primary aim is to strengthen individual right to informational self-determination on the Internet. VILEM helps users to manage their privacy settings, protect themselves against potentially abusive websites, and saves time of users as it presents relevant information on personal data processing in a comprehensible manner. The paper also presents how VILEM fulfills requirements on Trustworthy AI.

Keywords: Socially responsible AI · Trustworthy AI · Accountability · Responsibility · Transparency · Explainability · Privacy · Right to informational self-determination.

1 Introduction

Efficient privacy protection is one of the crucial values that we need to foster in our information based society. At the same time, preserving this value should not hinder the development of society, science, technology, and provided services. Unfortunately, processing personal data when accessing various online services, such as social media, can pose various risks for Internet users – namely undermining their ability to exercise control over own personal data [21].

The necessity and importance of processing personal data, however, raises as new services and applications are being developed. One of currently very popular trends is personalization. Personalization can be understood "as a process that changes the functionality, interface, information content, or distinctiveness of a system to increase its personal relevance to an individual" [8]. Personalization can be found in many forms. One of the most common forms is web personalization.

* This paper was supported by the Technology Agency of the Czech Republic under grant No. TL03000152 "Artificial Intelligence, Media, and Law."

Web personalization is a complex process. It is typically based on profiling which can be technically done namely with help of various kinds of cookies (first-party cookies, third-party cookies, Flash cookies, etc.) or with help of other means, such as IP addresses, URL form data, etc. [17]. A wide range of information collected from users, such as visited pages, dates and times of Internet usage or checked goods can be processed with machine learning algorithms to create users' profiles or profiles of groups of users with similar interests. Tracking Internet users across different websites for providing them with personalized services can be based, for instance, on fingerprinting or on browser cookies [6]. Fingerprinting is a method of identifying and tracking a device without cookies [38]. The term cookie refers to "a text string that is placed on a client browser when it accesses a given server" [11]. Research shows "that some websites set over 300 cookies" into users devices [11].

This practice causes problems to Internet users who are often not aware about placement of cookies or are perplexed with a large number of requests on granting consent with cookies, with long and incomprehensible privacy policies, multiplicity of actors, and overall information asymmetry they are facing. In 2016, Eurostat described how Internet users protected their privacy online. Citizens of the Netherlands, Germany or Finland were very much aware of the fact that they can be traced by cookies. Despite that Internet users were not very active with regard to changing their cookie settings in a web browser. In particular, in the Czech Republic less than 20 % of people changed their "browser settings to prevent or limit cookies use" [15]. A recent study in the Czech Republic showed that Czech citizens perceive themselves as powerless and react to the complex situation of protecting their own online privacy by giving up on a diligent approach and learning how to live with something that they perceive as "an oppressive power of an algorithm" [45]. The approach described in the Eurostat study and confirmed by the recent Czech study and suggests that Internet users are renouncing their rights. In fact, Internet users stated that they perceive exercising their privacy-related rights as impossible due to their limited technical skills as well as limited legal knowledge.

As individual autonomy is threatened in the online environment where there are many "little brothers" and individual choices are predetermined based on ubiquitous tracking and personalization [18], Internet users need to be provided with tools that would strengthen their position and help them to exercise their rights, namely their right to informational self-determination, i.e., the right of an individual to decide whether and up to what degree information related to their private life would be communicated to others. For this purpose we propose designing a virtual assistant based on artificial intelligence (AI) that would strengthen individual autonomy by providing users with functionalities allowing them to communicate their individual preferences in privacy protection to providers of online content and services.

This virtual assistant contributes to developing socially responsible AI. Although socially responsible approach to AI has been mentioned by research in the past [37, 10], the concept of *socially responsible AI* was defined in early

2021 [12]. The main objective of socially responsible AI is "addressing the social expectations of generating shared value – enhancing both AI intelligence and its benefits to society" [12]. At the same time the virtual assistant needs to comply with ethical and legal requirements set out in EU documents and laws.

Therefore, the aim of this paper is to introduce how we intend to implement and operationalize a socially responsible AI system that would assist Internet users with efficient protection of their online privacy and the right to their informational self-determination by providing them with an easy and freely available tool allowing them to administer their privacy preferences, reduce information asymmetry, inform them in a comprehensible manner, and educate them in the area of law and technology.

2 EU Legislation, Personal Data Protection, and Cookies in Practice

The tool we propose – our virtual assistant – will be initially available for users from the Czech Republic. Therefore, its operation must be based on and compliant with EU and Czech laws related to personal data protection and cookies.

This legislation is quite robust and additional various explanatory documents such as opinions of the European Data Protection Board or other bodies need to be taken into account [20–24, 40]. Protection of personal data on the Internet is regulated namely by the General Data Protection Regulation (hereinafter GDPR [41]) and the ePrivacy directive [13]. Internet users are typically provided with various privacy policies that inform them how a particular data controller processes their data. They can do so based on one of legal grounds set out in the Art. 6 par. 1 of the GDPR. Typically, data controllers process personal data based on consent. However, they can process personal data without users consent for instance when they have a legitimate interest to do so. In this case users (data subjects) can object against such processing according to Art. 21 par. 1 of the GDPR. Data controllers can process personal data for various purposes. Each purpose, however, must be based on one of the legal ground. Understanding the situation can, thus, become very difficult and complex.

The complexity of the situation increases in cases when cookies are used. Cookies play an important role in securing proper functioning of providing online content and online services. EU law recognizes them as legitimate tools, for instance, for "analysing the effectiveness of website design and advertising, and in verifying the identity of users engaged in on-line transactions" [13]. At the same time use of cookies has implications for Internet users as cookies are stored on their equipment and can, thus, interfere with the private sphere of users [14]. However, one needs to distinguish among different types of cookies [32].

Originally, cookies were considered a privacy preserving mechanism [31]. Unfortunately, the practice showed that cookies can be misused [4]. Legal reguirements on cookies are often neglected [34], consent with placing cookies is not acquired in a lawful manner (such as pre-ticking checkboxes [30], or implying consent [39]) or users face so called tracking walls as well as take-it-or-leave-it

choices [47]. Given the unfavourable environment, some public authorities decided to audit cookie compliance [36]. Misuse of personal as well as non-personal data from cookies can have serious impacts on Internet users and can result, for instance, in online price discrimination [43] or exploiting biases [46].

One of the solutions for achieving legal compliance regarding cookies is use of consent management platforms. As preparatory work for designing an AI-based virtual assistant, we needed to verify the level of use of consent management platforms in the Czech Republic. In the preparatory phase, we crawled a number of websites and tried to automatically identify how many of them are using standard cookie consent managers (like CookieBot or OneTrust) because it is much easier to automatically analyze consents on pages using such managers. As the detection was done with help of a rule-based system (using defined HTML structure and keywords), the results are only approximate. It is possible that a few pages were using consent managers contrary to the results or that on some pages the managers were not identified correctly. However, based on manual evaluation of some pages we can say it happened just in several cases. The results of this experiment are shown in Table 1. The results indicate that 314 pages out of 3649 used one of the tested consent management platforms and 809 pages probably do not mention anything about cookies at all.

Table 1. Use of consent management platforms in the Czech Republic.

Description	**Number**
OneTrust (CMP)	142
CookieBot (CMP)	16
Cookie Consent (CMP)	112
Funding Choices (CMP)	44
Cookies mentioned in Privacy Policy	2526
Probably no cookies used	809
Pages scanned in total	3649

The experiment shows that use of cookies on the Internet in the Czech Republic is quite inconsistent and, therefore, can be also confusing for Internet users.

3 VILEM: Virtual Assistant for Privacy Protection

3.1 The Idea behind VILEM

As suggested above, problems with online privacy protection and bad cookie practice led us to the idea that Internet users need to be much better equipped in order to face the growing information asymmetry, overload of information related to personal data protection on the Internet, and a growing number of requests on providing their consent with personal data processing and placing cookies into their devices. The principle of granting consent is in line with the legal principle

of personal autonomy and the right to information self-determination. As such, it needs to be maintained. At the same time, Internet users need to be provided with tools on how to exercise their will and rights in practice not to be paralyzed by practical effects of this legal requirement.

Therefore, we have designed an AI-based virtual assistant VILEM. Its name refers to the principle of autonomy as the etymological meaning of this word is "my will is my protection." Moreover, VILEM is an acronym that stands for **V**olition **I**nspirited by **L**egal **EM**powerment.

The idea of using technology to empower Internet users with regard to privacy protection online is not new. Apart from various plug-ins that help to block tracking by third-party cookies, there is, for instance, a solution that utilizes deep learning and helps Internet users to comprehend privacy policies – Polisis [28]. Another solution, a browser plug-in Robin, helps to monitor personalization process and to understand "individual information cocoons" [9].

The uniqueness of VILEM lies in its ability to return its users the *decision-making capacity* that would not be hindered by the necessity to exploit limited personal resources, such as time to search for relevant information, time to manually set up privacy preferences for each visited website, and biologically limited attention span. The following subchapter describes how VILEM shall function in practice.

3.2 VILEM's Functionalities

Form and appearance VILEM is designed in the form of a sidebar that appears when an Internet browser is opened. VILEM updates itself automatically once a user enters a website on a new domain or when new cookies are detected. It is accessible all the time and not only on demand. Currently, VILEM is designed only in the Czech language and for Czech users. When completed, VILEM will be available for free as a web plug-in.

Personalized privacy protection We presume that upon installing VILEM, users will fill in a survey regarding their privacy preferences. Our pilot empirical study that we conducted in the Czech Republic in December 2020 shows that some users trust certain websites more and are willing to share more information with them than with others. Moreover, 56 % of respondents stated that they prefer to assess each purpose of processing personal data individually [33]. Therefore, VILEM will enable users to set up their specific privacy preferences with regard to grounds for personal data processing according to the Art. 6 par. 1 GDPR [41], purposes for personal data processing set out in privacy policies, and individual types of cookies. The types of cookies have been preliminary determined based on analysis of options provided by consent management platforms and can be extended depending on continuous analysis. After completing an initial survey, VILEM will automatically set up cookie preferences when asked for consent by a website. Users will be able to change their privacy preferences any time. Moreover, they will be able to change settings manually for individual websites.

Providing information to users VILEM informs users about the information that the data controller needs to make available according to the GDPR. This information contains the name and contact details of the controller, the purpose of data processing, categories of processed personal data, and legal grounds for the processing (consent, contractual obligation, legal obligation, protection of vital interests, protection of a public interest, or a legitimate interest of the controller). Additionally, VILEM informs users whether the controller makes the data available to other parties, such as processors. In that case VILEM also provides users with respective contact details. Users should understand from the information provided that their consent is reversible, if already given, or optional, if not. The same goes for the stated legitimate purposes.

VILEM will also fulfill an educational role. It will inform users in simple terms about what provided information means and what can be done in each situation. For those interested in the topic and who will want to go into it in more depth, we will provide links to our website with educational videos (in preparation).

As problems with privacy management need not to be caused only by improper or overwhelming use of cookies, VILEM will also inform and educate users how to protect themselves in other situations. Namely, VILEM will recommend users to install some of the existing web plug-ins that prevent device fingerprinting.

Tool for managing cookies VILEM will enable users to forbid cookies unnecessary for website's functioning and inform them that a website is inaccessible without agreeing to certain types of cookies. In the future, VILEM should provide additional functions, such as enabling users to forbid pop-up notifications and informing them if a website contains paid promotions.

3.3 VILEM's Technical Background

Various methods can implement mapping of user preferences with specific rules offered by websites providers. With growing computational capabilities and more powerful hardware, automatic but rigorous analysis of textual data becomes more imaginable than before. VILEM can use any modern text classification approach for checking matches in privacy preferences. By using models that are able to handle some degree of semantic understanding, we can improve the model's ability to handle input data that differ in lexical realization but carry the same meaning as the training data. One example of such model is represented by BERT models [1] and its derivatives. We intent to use this class of models in VILEM.

The current trend in natural language processing is to use large neural network models pre-trained on huge data sets. Such data do not have to be manually labelled; we can use automatically generated datasets and design artificial tasks – so-called self-supervised learning – to extract knowledge about human language. These models are mainly intended for the English language. However,

researchers released models trained on a couple of languages simultaneously [42], which can help to increase the accuracy of such models by enlarging the dataset. We can also utilise models for narrow language groups, such as the Slavic language group [7] or even monolingual models trained for the Czech language [44].

These pre-trained models can be used directly only for a limited set of tasks. In our case, we will have to apply an additional fine-tuning step, in which a training set of manually annotated data will be collected. This annotated data shall be used to adapt the model for the task of classification of legal texts. With these pre-trained models we expect to achieve much better classification accuracy with less data when compared to an approach that do not rely on pre-trained models.

Given the growing data production and a constantly changing legal environment, modern society often searches for an easy and systematic way of solving legal issues. Complex but easy-to-use shelf-product solutions are often the first-choice tool for website operators who want to satisfy complicated legal requirements. Projects like OneTrust aim to deal with the changing environment. However, a non-negligible amount of web service providers still does not use such a systematic solution many providers do not even implement legal obligations at all. In this regard, VILEM will be able to easily analyse and solve the problem of matching users' preferences for individual on websites with mainstream systematic solutions due to the known structure of forms. VILEM will be able to focus only on textual content and its semantics. In non-systematic solutions, there will be one extra step – to identify the form and parse the statements with their controls. In the next step, VILEM will be able to analyse the texts, highlight match or mismatch in each statement and prefill the pop-up windows or privacy management forms for users. VILEM will be also able to recognise and send information in an aggregated form about potential violations of law to the respective public authority.

As VILEM will use techniques of natural language processing, we need to take extra care when preparing datasets for its learning. The preparation of the data is done manually by people with knowledge of personal data processing and its legal limits as well as the obligations imposed by the data protection legislation [41, 2]. The annotation is made in an environment specifically designed just for this task.

There are some specificities related to annotating in the Czech language and within the Czech legal culture. The first specificity lies in the workings of the language itself. The structure differs significantly from English, German and other languages used in areas where annotation of legal texts is more common than in the Czech Republic. Therefore, existing conventions from other countries are not usable for our work. The second specificity concerns the legal culture in the Czech Republic, which scarcely uses standardized templates. The governmental bodies, such as ministries and specialized public authorities (e.g., the Office for Personal Data Protection), do not provide them either. It is customary for the administrative bodies to provide guidelines on the creation of necessary docu-

ments instead. As a result, when annotating a Czech legal text one must expect a high level of variability in its structure as well as in the terminology.

The field of annotating Czech legal texts is not explored thoroughly. Nevertheless, more than one research project on this matter was completed in previous years. For data extraction, we follow the best practice set by the team on the Faculty of Law at Masaryk University [25] on the methodology for citation analysis and annotation conventions. The most significant results so far were presented in the research project Exact Assessment of the Relevance of Case-Law [16]. In the project, the focus however lied on the analysis of references present in the case-law of Czech courts. The part relevant for work on VILEM was the groundwork on manual annotation of data necessary for the automatic extraction of data by the tool [26]. Of course, other works based on manual annotation of legal texts exist, however they do not focus on the preparation of data for automated extraction. For VILEM to work, it has to be capable to learn to find patterns in various texts containing personal data processing information. We had to annotate with that in mind.

The challenges of texts containing terms and conditions for personal data processing are 1) variations in used legal terminology; 2) creativity in the phrasing of information obligations towards the user; 3) inconsistent level of detail of provided information; 4) purposeful omission of certain information. The obstacles we are facing differ from the ones the team of Masaryk University had to solve. For example, one of the problems they had was an unclear structure of case-law decisions that required the addition of functionality to their tool, enabling automated segmentation of the text [27]. In comparison, the most challenging part of VILEM is that the terms and conditions on personal data processing require a significant amount of different tags.

To prevent mistakes in the manual annotation that would have a negative influence on the functionalities of VILEM, the annotation is done by professionals in the area of personal data protection. This way, they are familiar with the terminology and it will be quicker for them to search for relevant data in the texts. Furthermore, their practical experience shall ensure that they can identify possible hidden information in the text. Such as unlawful limitations of the data subject's rights. These are written intentionally in a way that would confuse an an unprepared reader without professional expertise. In the future, we would like to enable the users of VILEM to send feedback in case they encounter an error made by VILEM, such as the inability to find all the information on personal data processing in the terms and conditions. This way, VILEM can improve, which is one of the upsides of using AI algorithms. That said, it is necessary to supervise the learning of VILEM on the data feedback, since it might be incorrect. It is bound to happen that the users will not be able to correctly identify the relevant legal meaning behind the phrasing of the text. It can be quite confusing for a consumer. Even so, the texts can be confusing to legal professionals as well.

Therefore, we have implemented the practice of multiple annotations of the same text. To make the manual annotations as precise as possible, we also created

an annotation manual. The annotation manual is inspired by the one used for the annotation of Czech judicial decisions [5]. It sets the general rules for annotation so that all the annotators can adopt the same or at least similar approach. On top of that all tags are accompanied by examples of how they can look like in different texts.

3.4 Involvement of VILEM's Users

Any user experience feedback is precious and can improve functioning of a system by adjusting the user interface or enlarging the training corpora. However, in every application, collecting user feedback can be tricky. Active feedback can be time-consuming and annoying for users. Moreover, recording users' behaviour may not be well accepted in a project dealing with privacy issues. However, VILEM can overcome these issues. We will let the users consider the benefit of making the system better and let them decise whether they would accept or deny sending anonymous automatic feedback upon installation of VILEM. Meanwhile, we will place feedback buttons in the applications for those who want to give active feedback.

We need to keep in mind that some serious problems can arise if users would have the possibility to affect the decision process of VILEM by sending feedback on incorrect annotation of legal texts. In the first place, a common user is not a lawyer, so that their reasoning can be simply wrong. Fortunately, modern models can handle non-systematic noise brought by users well. However, if there was some systematic misunderstanding of the law by the users, the model could drift to this potentially wrong interpretation. We will avoid this unwanted state by searching for a systematic deviation and investigating such singularities by professionals.

Nonetheless, the fact that the user would not be satisfied with the outcome of VILEM will be essential for us. We can solve this issue in several ways: by providing us with information why VILEM marked a statement as it had done in the first place and let the user share his own opinion on the subject for further processing. If VILEM was wrong, we would add this "outlier" to the training corpora. If VILEM was right, it could be a sign of an unclear understanding of the setting of users preferences in VILEM after installation.

3.5 Evaluation of VILEM by Czech Internet Users

In November and December 2020, we tested the first proof of concept and the user interface of VILEM. In December 2020, we conducted the first pilot empirical study and presented a mock-up version of VILEM to 50 Czech Internet users [33]. The respondents could get acquainted with VILEM through an introductory video. They were provided with description of VILEM's purpose and functionalities. Our aim was to get preliminary feedback before further development.

The feedback from respondents was very positive. 92 % of respondents considered such web plug-in as desirable. 94 % of respondents evaluated VILEM as

useful and 84 % considered it trustworthy. 56 % of respondents expressed that VILEM would strengthen their control over information and would help them to make the process of privacy protection more comprehensible to them. Respondents expressed their expectations that VILEM would help them to protect themselves from and block harmful websites as well as save their time. Only 4 respondents out of 50 were hesitant or negative about the use of VILEM. The main reasons were a general concern that VILEM would slow down a computer and a general distrust to any solution that needed to be installed into a computer [33].

The pilot study showed us that Czech users would welcome a technical solution that would strengthen their control over personal data, warned and protected them against threats (namely when a website requires more information than users are willing to provide), and instructed them what to do in certain situations.

The main lesson we took from the study is to design VILEM in such a manner that it shall provide a maximum level of information, choice and control to users an a very comprehensible and easy-to-understand manner. In order to strengthen trustworthiness of VILEM, we need to diligently implement and operationalize requirements on Trustworthy and Responsible AI. The following chapter will illustrate how we plan to do so.

4 Implementing Trustworthy AI

The term of Trustworthy AI was introduced by the High-Level Expert Group on Artificial Intelligence [29]. In order for AI systems to be well adopted by society, these systems ideally need to comply with a number of requirements.

Ethical Principles of Trustworthy AI AI systems will need to comply with four ethical principles on Trustworthy AI – respect for human autonomy, prevention of harm, fairness, and explicability. VILEM fulfills the rationale of all of the four principles. Its aim is to strengthen human autonomy by providing Internet users with a free tool for better management of own choices and hereby prevents harm that they could face by careless sharing of personal data. VILEM will not discriminate any user as it will be freely available to all Czech citizens. Moreover, functioning of VILEM will be explained to users in a comprehensible and transparent manner.

Key Requirements for Trustworthy AI AI systems will also need to comply with seven requirements. Compliance of VILEM is described below for each of the requirement.

Human agency and oversight As mentioned above, the main function of VILEM is to empower Internet users with regard to personal autonomy in the area of privacy preferences management. The same principle will be applied to VILEM as well. Users will have complete control over the web plug-in. They will be in

charge of setting-up their preferences and will be able to change them at any time.

Technical robustness and safety The main risk to technical robustness and safety would come from the side of users who could influence functioning of VILEM. Therefore, all input and feedback from users on problems related to malfunctioning will be checked manually.

Privacy and data governance VILEM will not collect or process personal data related to its users. All activity will be done only on the side of users. It will be possible to share data with us if a particular user will wish to do so for the purpose of improving the system. Users will have an option to share the data anonymously.

Transparency VILEM shall be completely transparent. We intend to share the code as open source. Moreover, users or any other person will be provided with information which training data was used. Namely, we will provide a list of privacy policies (including Internet links) that were used to train VILEM. We plan to provide annotated datasets upon reasonable requests to researchers for the purposes of checking proper functioning of the system. The datasets will not be provided publicly per se to protect intellectual property interests.

Diversity, non-discrimination, and fairness VILEM is designed as user-centric and will be made available to anyone for free.

Societal and environmental well-being By protecting users VILEM will contribute to overall societal well-being.

Accountability With regard to securing safety and robustness, functioning of VILEM will be continuously monitored and improved.

5 Future Challenges

Our virtual assistant VILEM is in the process of development. However, even after it will be finished, we will need to continuously update it, expand the training corpora and keep analyzing how law and privacy policies as well as cookie legislation and practice evolves. One of the upcoming challenges we will need to react to is a change in use of so called third-party cookies [19] use of which has already been reduced in relationship with adopting the GDPR (see [35]). Moreover, we need to monitor and update VILEM with regard to potential new legal obligations.

Acknowledgement

This work has been supported by the Technology Agency of the Czech Republic within the ETA Programme – No. TL03000152 "Artificial Intelligence, Media, and Law".

References

1. Devlin, J., Chang, M.W., Lee, K., Toutanova, K. BERT: Pre-training of Deep Bidirectional Transformers for Language Understanding. In: Proceedings of the 2019 Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies, Volume 1 (Long and Short Papers). pp. 4171-4186. 2019.
2. Act No. 110/2019 Coll., on Personal Data Processing (Czech Republic)
3. Aguirre, E., Mahr, D., Grewal, D., de Ruyter, K., Wetzels, M.: Unraveling the Personalization Paradox: The Effect of Information Collection and Trust-Building Strategies on Online Advertisement Effectiveness. Journal of Retailing **91**(1), 34–49 (2015). https://doi.org/10.1016/j.jretai.2014.09.005
4. Ahava, A.: Use (and Abuse) of Website Cookies under EU Privacy Law: Practical Tips for Better Compliance, https://www.lexology.com/library/detail.aspx?g=64772d95-c4c7-4ad0-8a5c-ab66ff564e1e. Last accessed 18 May 2021
5. Annotation manual for the project Methodology for the Case-Law Citation Analysis, project no. MUNI/A/0940/2015, http://citacnianalyza.law.muni.cz/content/cs/publikace/. Last accessed 18 May 2021
6. Arzubov, M., Shakhovska, N., Lipinski, P.: Analyzing ways of building user profile based on web surf history. In: 12th International Scientific and Technical Conference on Computer Sciences and Information Technologies (CSIT). IEEE Press (2017). https://doi.org/10.1109/STC-CSIT.2017.8098809
7. BERT in DeepPavlov, http://docs.deeppavlov.ai/en/master/features/models/bert.html. Last accessed 18 May 2021
8. Blom, J.: Personalization: a taxonomy. In: CHI EA '00: CHI '00 Extended Abstracts on Human Factors in Computing Systems, pp. 313-314. ACM (2000)
9. Bodo, B. B., Helberger, N. N., Irion, K. K., Zuiderveen Borgesius, F. F., Moller, J. J., van de Velde, B. B., Bol, N. N., van Es, B. B., de Vreese, C. C.: Tackling the Algorithmic Control Crisis. The Technical, Legal, and Ethical Challenges of Research into Algorithmic Agents. Yale Journal of Law and Technology **19**(1), 133–181 (2017)
10. Brundage, M., Avin, S., Clark, J. et al.: The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation. Report, Future of Humanity Institute (2018)
11. Cahn, A., Alfeld, S., Barford, P., Muthukrishnan, S.: An Empirical Study of Web Cookies. In: WWW '16: Proceedings of the 25th International Conference on World Wide Web, pp. 891-901. ACM (2016)
12. Cheng, L., Varshney, K. R., Liu, H.: Socially Responsible AI Algorithms: Issues, Purposes, and Challenges. 1-49 (2021). https://arxiv.org/abs/2101.02032
13. 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 (Directive on privacy and electronic communications)
14. Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004

on cooperation between national authorities responsible for the enforcement of consumer protection laws (Text with EEA relevance)
15. Eurostat: Digital economy and society statistics – households and individuals, https://ec.europa.eu/eurostat/statistics-explained/index.php. Last accessed 18 May 2021
16. Exact assessment of the relevance of case-law, https://starfos.tacr.cz/en/project/GA17-20645S. Last accessed 18 May 2021
17. Farafonov, G.: Personal data and personalization issues. Diploma thesis. University of Economics and Business, (2012)
18. Grafanaki, S.: Autonomy Challenges in the Age of Big Data. Fordham Intellectual Property, Media & Entertainment Law Journal **27**(4), 803–865 (2017)
19. Google ending third-party cookies in Chrome, https://www.cookiebot.com/en/google-third-party-cookies. Last accessed 18 May 2021
20. Guidelines 05/2020 on consent under Regulation 2016/976. European Data Protection Board (2020)
21. Guidelines 8/2020 on the targeting of social media users. European Data Protection Board (2021)
22. Guidelines 09/2020 on relevant and reasoned objection under Regulation 2016/679. European Data Protection Board (2021)
23. Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679. Article 29 Data Protection Working Party (2018)
24. Guidelines on transparency under Regulation 2016/679. Article 29 Data Protection Working Party (2018)
25. Harašta, J., Míšek, J., Hanych, M., Loutocký, P., Malaník, M., Šavelka, J., Štěpáníková, M., Myška, M.: Rozměry citací v právu a anotační konvence. Revue pro právo a technologie **8**(5), 51–73 (2017). https://doi.org/10.5817/RPT2017-1-4
26. Harašta, J., Šavelka, J., Kasl, F., Kotková, A., Loutocký, P., Míšek, J., Procházková, D., Pullmannová, H., Semenišín, P., Šejnová, T, Šimková, N., Vosinek, M, Zavadilová, L., Zibner, J.: Annotated Corpus of Czech Case Law for Reference Recognition Tasks. In: Sojka, P., Horák, A., Kopeček, I., Pala, K. (eds.). Text, Speech, and Dialogue: 21st International Conference. Cham: Springer Nature Switzerland AG (2018)
27. Harašta, J., Šavelka, J., Kasl, F., Míšek, J.: Automatic Segmentation of Czech Court Decisions into Multi-Paragraph Parts. Jusletter IT **4**, 1–10 (2019).
28. Harkous, H., Fawaz, K., Lebret, R., Schaub, F., Shin, K. G., Aberer, K.: Polisis: Automated Analysis and Presentation of Privacy Policies Using Deep Learning. In: USENIX Security 2018. (2018)
29. High-Level Expert Group on Artificial Intelligence. Ethics Guidelines for Trustworthy AI. European Commission (2019)
30. Jabłonowska, A., Michałowicz, A.: Planet49: Pre-Ticked Checkboxes Are Not Sufficient to Convey User's Consent to the Storage of Cookies (C-673/17 Planet49). European Data Protection Law Review **6**(1), 137–142 (2020). https://doi.org/10.21552/edpl/2020/1/19
31. Jones, M. L.: Cookies: a legacy of controversy. Internet Histories **4**(1), 87–104 (2020). https://doi.org/10.1080/24701475.2020.1725852
32. Koch, R.: Cookies, the GDPR, and the ePrivacy Directive, https://gdpr.eu/cookies/. Last accessed 18 May 2021
33. Krausová, A., Moravec, V., Volek, J.: Osobní asistent pro práci s algoritmickou personalizací obsahů: Pilotní analýza uživatelských znalostí a očekávání. Research report, Focus – Marketing & Social Research (2020)

34. Leenes, R., Kosta, E.: Taming the cookie monster with Dutch law – A tale of regulatory failure. Computer Law & Security Review **31**(3), 317–335 (2015). https://doi.org/10.1016/j.clsr.2015.01.004
35. Libert, T., Graves, L., Kleis Nielsen, R.: Changes in Third-Party Content on European News Websites after GDPR. Factsheet, Reuters Institute and University of Oxfors (2018)
36. Long, W. R. M., Rockwell, S. P., Cuyvers, L.: Developments in Cookie Regulation: French CNIL Declares Intent to Audit Websites for Cookie Compliance, https://www.lexology.com/library/detail.aspx?g=fea449a2-b5a4-4c6d-8d9e-5ffb79001790. Last accessed 18 May 2021
37. Mantelero, A.: AI and Big Data: A blueprint for a human rights, social and ethical impact assessment. Computer Law & Security Review **34**(4), 754–772 (2018). https://doi.org/10.1016/j.clsr.2018.05.017
38. Nikiforakis, N., Kapravelos, A., Joosen, W., Kruegel, C., Piessens, F., Vigna, G. Cookieless Monster:Exploring the Ecosystem of Web-based Device In: 2013 IEEE Symposium on Security and Privacy, pp. 541-555 IEEE (2013). https://doi.org/10.1109/SP.2013.43
39. Nouwens, M., Liccardi, I., Veale, M., Karger, D., Kagal, L.: Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence. In: CHI '20: Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems, pp. 1-13. ACM (2020). https://doi.org/10.1145/3313831.337632
40. Opinion 04/2012 on Cookie Consent Exemption. Article 29 Data Protection Working Party (2012)
41. 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, and repealing Directive 95/46/EC (General Data Protection Regulation)
42. Rönnquist, S., Kanerva, J., Salakosi, T., Ginter, F.: Is Multilingual BERT Fluent in Language Generation? In: Proceedings of the First NLPL Workshop on Deep Learning for Natural Language Processing, pp. 29-36. Linköping University Electronic Press (2019)
43. Sears, A. M. The Limits of Online Price Discrimination in Europe. The Columbia Science & Technology Law Review **21**(1), 1–42 (2018)
44. Sido, J., Pražák, O., Přibáň, P., Pašek, J., Seják, M., Konopík, M.: Czert – Czech BERT-like Model for Language Representation. 1-13 (2021). https://arxiv.org/abs/2103.13031
45. Volek, J.: Algoritmizovaná personalizace obsahů: Přínosy a ohrožení. Kvalitativní analýza uživatelských postojů a taktik. Research report, Focus – Marketing & Social Research (2020)
46. Wagner, G., Eidenmüller, H.: Down by Algorithms? Siphoning Rents, Exploiting Biases, and Shaping Preferences: Regulating the Dark Side of Personalized Transactions. University of Chicago Law Review **86**(2), 581–610 (2019)
47. Zuiderveen Borgesius, F. J., Kruikemeier, S., Boerman, S. C., Helberger, N.: Tracking Walls, Take-It-Or-Leave-It Choices, the GDPR, and the ePrivacy Regulation. European Data Protection Law Review **3**(3), 353–368 (2017). https://doi.org/10.21552/edpl/2017/3/9