www.jusletter.ch

Rayan Houdrouge / Kathryn Kruglak

Are Swiss data protection rules ready for AI?

A comparison of Swiss data protection rules and those offered under the proposed EU AI Act

Against the background of the recently introduced new Federal Act on Data Protection in Switzerland, and the proposed Artificial Intelligence Act in the EU, this article addresses the question of whether Swiss data protection rules offer sufficient protection when it comes to AI. It does this by analysing: (i) the primary personal data protection risks posed by AI; (ii) Swiss personal data protection rules applicable to AI; (iii) the personal data protections in the proposed Artificial Intelligence Act; and (iv) how the Swiss personal data protection rules compare to the personal data protections in the proposed Artificial Intelligence Act.

Category of articles: Articles
Field of Law: Data protection, IT and law

Citation: Rayan Houdrouge / Kathryn Kruglak, Are Swiss data protection rules ready for AI?, in: Jusletter 27 November 2023

ISSN 1424-7410, jusletter.weblaw.ch, Weblaw AG, info@weblaw.ch, T +41 31 380 57 77

Contents

1. Introduction

[1] On 1 September 2023, the new Federal Act on Data Protection («**nFADP**»),[1] and its implementing ordinance («**nODP**»),[2] entered into force, ushering in new data protection rules in Switzerland.

[2] These new rules are the fruition of discussions that began over half a decade ago when, in 2017, the Swiss Federal Council proposed a bill entirely revising the Federal Act on Data Protection.[3]

[3] One of the primary impetuses behind the introduction of these new data protection rules was to ensure that Swiss data protection rules keep pace with rapidly evolving new technological developments.[4] The other was to account for changes to European Union («**EU**») data protection law introduced in the General Data Protection Regulation,[5] which was published on 4 May 2016 and became binding on 25 May 2018.[6]

[4] However, the technological and legislative landscape today is vastly different from the one that existed in 2017.

[5] In particular, recent advances in artificial intelligence («**AI**») are changing drastically the way in which data are collected and processed and the EU is inching closer to passing legislation comprehensively governing AI.[7]

[6] Against that background, this article analyses: (*i*) the primary personal data protection risks posed by AI (*Section 2* below); (*ii*) Swiss personal data protection rules applicable to AI (*Section 3* below); (*iii*) the personal data protections in the proposed AI Act (*Section 4* below); and (*iv*) how

1 RO 2022 491.

2 RO 2022 568.

3 *Message concernant la loi fédérale sur la révision totale de la loi fédérale sur la protection des données et sur la modification d'autres lois fédérales*, FF 2017 6565 (cited: «**FF 2017 6565**»).

4 FF 2017 6565, 6567.

5 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, OJ L 119, 4 May 2016, p. 1–88 (cited: «**General Data Protection Regulation**» or «**GDPR**»).

6 Art. 99 par. 2 GDPR.

7 European Commission, «Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS», COM/2021/206 final, as amended by: European Parliament, «Amendments adopted by the European Parliament on 14 June 2023 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD))», P9_TA(2023)0236 (cited: «**Artificial Intelligence Act**» or «**AI Act**»); see also European Parliament, «EU AI Act: first regulation on artificial intelligence» (14 June 2023) https://www.europarl.europa.eu/news/en/headlines/society/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence accessed 30 July 2023.

the Swiss personal data protection rules compare to the personal data protections in the proposed AI Act (*Section 5* below).

[7] It should be noted that this article does not cover general data protection rules in the EU, especially those contained in the GDPR, as the purpose of this article is to analyse the additional protections that would be afforded under the AI Act to see whether the AI Act provides protections for personal data with regard to AI that go beyond those contained in Swiss law and, if so, to analyse the advantages and disadvantages of these additional rules.

2. Primary data protection risks from AI

[8] At its essence, data protection concerns whether data may be collected and, if so, how the data may be collected, by whom they may be collected and, once collected, how they may be processed, stored and transferred.

[9] The reader will note that none of these aspects necessarily implies the use of AI, or even a technological component, in the collection and processing of data.

[10] That said, new technology often changes the ways in which data are collected and processed and the law must adapt to provide protections that are appropriate and adequate in light of these changes. For instance, widespread use of the Internet led to a need to have specific protections that could address personal data protection problems posed by cookies.[8]

[11] AI is no different.[9] It has the potential to change, and already is changing, how data are collected and processed; data protection laws will need to ensure that they provide appropriate and adequate protections that address these new ways of collecting and processing personal data.

8 See 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), OJ L 337, 18 December 2009, p. 11–36.

9 It should be noted that there is no universally accepted definition of AI. The European Commission originally proposed the following definition «*software that is developed with one or more of the techniques and approaches listed in Annex I [of the AI Act] and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with*». This was amended by the European Parliament, which adopted the OECD definition, based on the notion of AI systems; this definition states that «*[a]n AI system is a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments. AI systems are designed to operate with varying levels of autonomy*»(OECD, «Recommendation of the Council on Artificial Intelligence» (22 May 2019) OECD/LEGAL/0449); European Parliament, «Amendments adopted by the European Parliament on 14 June 2023 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD))», P9_TA(2023)0236; Tambiama Madiega, «Artificial intelligence act» (June 2023, European Parliamentary Research Service) PE 698.792, 3–4, 6–9).

[12] It is worth noting that much of the current media hype and discussions around AI following the launch of ChatGPT on 30 November 2022[10] concern generative AI (i.e. AI that collects data and then generates something new).[11]

[13] However, AI has other uses,[12] many of which also have personal data implications.

[14] In particular, AI has the capability, and is used, to (*i*) collect personal data on a mass scale, and (*ii*) automate the processing of personal data.

[15] For instance, AI may be used to engage in the mass collection of existing user-uploaded data from websites such as Facebook and then use the data for training purposes.[13]

[16] In this context, the use of AI to engage in mass surveillance, in particular, to collect biometric data, is especially problematic from a personal data protection perspective, as it can lead to infringements of many fundamental rights, such as the right to privacy; it also can infringe the right to free speech and assembly, as individuals may be afraid to exercise these freedoms if they believe they are being monitored.[14]

[17] Further, the UN Special Rapporteur for privacy has identified both big data and mass surveillance as areas in which it increasingly is interested[15] and the United Nations Human Rights Council has expressed its deep concern about surveillance «*in particular when carried out on a mass scale*».[16]

[18] In addition to collecting data on a mass scale, AI systems also may be involved in the automated processing of these data.

[19] In particular, AI can be used for the rapid processing of personal data collected on a mass scale for monitoring and surveillance purposes, such as through the use of facial recognition algorithms.[17]

---

10 See Bernard Marr, «A Short History Of ChatGPT: How We Got To Where We Are Today» *Forbes* (Jersey City, New Jersey, 19 May 2023) https://www.forbes.com/sites/bernardmarr/2023/05/19/a-short-history-of-chatgpt-how-we-got-to-where-we-are-today accessed 1 August 2023; Dan Milmo, «ChatGPT reaches 100 million users two months after launch» *The Guardian* (London, 2 February 2023) https://www.theguardian.com/technology/2023/feb/02/chatgpt-100-million-users-open-ai-fastest-growing-app accessed 1 August 2023.

11 See IBM, «What is artificial intelligence?» https://www.ibm.com/topics/artificial-intelligence accessed 2 August 2023.

12 See John McCarthy, «What is artificial intelligence» (12 November 2007) Stanford Computer Science Department, https://www-formal.stanford.edu/jmc/whatisai.pdf accessed 2 August 2023; IBM, «What is artificial intelligence?» https://www.ibm.com/topics/artificial-intelligence accessed 2 August 2023.

13 Melissa Heikkilä, «The rise of AI surveillance» *Politico* (Brussels, 26 May 2021) https://www.politico.eu/article/the-rise-of-ai-surveillance-coronavirus-data-collection-tracking-facial-recognition-monitoring accessed 31 July 2023.

14 See European Digital Rights (EDRi), «Open letter: Civil society call for the introduction of red lines in the upcoming European Commission proposal on Artificial Intelligence» (12 January 2021), https://edri.org/wp-content/uploads/2021/11/EDRi-open-letter-AI-red-lines.pdf accessed 9 August 2023.

15 OHCHR, «Special Rapporteur on the right to privacy» https://www.ohchr.org/en/special-procedures/sr-privacy accessed 1 August 2023.

16 A/HRC/RES/28/16.

17 Melissa Heikkilä, «The rise of AI surveillance» *Politico* (Brussels, 26 May 2021) https://www.politico.eu/article/the-rise-of-ai-surveillance-coronavirus-data-collection-tracking-facial-recognition-monitoring accessed 31 July 2023.

[20] For example, in June 2023, the French Sénat voted in favour of a bill paving the way for investigators and intelligence services to use large-scale biometric surveillance, in the form of facial recognition systems, to investigate certain types of crimes.[18]

[21] Moreover, in some instances, these algorithms have been used to identify suspects, sometimes leading to false arrests.[19]

[22] AI also can be used to collect employee personal data, as well as to process that data to monitor employee productivity and decide automatically who to fire.[20]

[23] In light of these new data protection risks posed by AI, it follows that specific protections are necessary to address: (*i*) the mass collection of personal data via AI, in particular, biometric data, and (*ii*) the use of AI to automate the processing of personal data.

[24] The following sections therefore analyse and compare the protections offered with regard to these points in the context of (*i*) Swiss law (*Section 3* below), and (*ii*) EU law (*Section 4* below).

3. Protections available under Swiss law

3.1. Introduction

[25] Although much of the current media hype around AI began following the launch of ChatGPT,[21] lawmakers have been contemplating the potential challenges posed by AI, including with regard to personal data protection, for much longer.

[26] Therefore, some of the concerns raised by AI are addressed by the nFADP (*Section 3.2* below).[22]

---

18 Le Figaro/AFP, «Le Sénat ouvre la voie à l'utilisation de la reconnaissance faciale» *Le Figaro* (Paris, 12 June 2023) https://www.lefigaro.fr/flash-actu/le-senat-ouvre-la-voie-a-l-utilisation-de-la-reconnaissance-faciale-20230612 accessed 31 July 2023; see also Melissa Heikkilä, «The rise of AI surveillance» *Politico* (Brussels, 26 May 2021) https://www.politico.eu/article/the-rise-of-ai-surveillance-coronavirus-data-collection-tracking-facial-recognition-monitoring accessed 31 July 2023; Nicholas Vinocur, «French politicians urge deployment of surveillance technology after series of attacks» *Politico* (Brussels, 30 October 2020) https://www.politico.eu/article/french-politicians-urge-deployment-of-surveillance-technology-after-series-of-attacks accessed 31 July 2023.

19 Melissa Heikkilä, «The rise of AI surveillance» *Politico* (Brussels, 26 May 2021) https://www.politico.eu/article/the-rise-of-ai-surveillance-coronavirus-data-collection-tracking-facial-recognition-monitoring accessed 31 July 2023; John General/Jon Sarlin, «False facial recognition match sent this innocent Black man to jail» *CNN* (Atlanta, Georgia, 29 April 2021) https://edition.cnn.com/2021/04/29/tech/nijeer-parks-facial-recognition-police-arrest/index.html accessed 31 July 2023; Jennifer Henderson, «Black mom sues city of Detroit claiming she was falsely arrested while 8 months pregnant by officers using facial recognition technology» *CNN* (Atlanta, Georgia, 29 April 2021) https://edition.cnn.com/2023/08/07/us/detroit-facial-recognition-technology-false-arrest-lawsuit/index.html accessed 8 August 2023.

20 See Pranshu Verma, «AI is starting to pick who gets laid off» *The Washington Post* (Washington, DC, 20 February 2023) https://www.washingtonpost.com/technology/2023/02/20/layoff-algorithms accessed 31 July 2023; U.S. Equal Employment Opportunity Commission, *Select Issues: Assessing Adverse Impact in Software, Algorithms, and Artificial Intelligence Used in Employment Selection Procedures Under Title VII of the Civil Rights Act of 1964* https://www.eeoc.gov/select-issues-assessing-adverse-impact-software-algorithms-and-artificial-intelligence-used accessed 31 July 2023.

21 See Bernard Marr, «A Short History Of ChatGPT: How We Got To Where We Are Today» *Forbes* (Jersey City, New Jersey, 19 May 2023) https://www.forbes.com/sites/bernardmarr/2023/05/19/a-short-history-of-chatgpt-how-we-got-to-where-we-are-today accessed 1 August 2023; Dan Milmo, «ChatGPT reaches 100 million users two months after launch» *The Guardian* (London, 2 February 2023) https://www.theguardian.com/technology/2023/feb/02/chatgpt-100-million-users-open-ai-fastest-growing-app accessed 1 August 2023.

22 See FF 2017 6565, 6692, 6642 and 6684.

[27] Moreover, some of these challenges already are addressed through other international and domestic legal bases (*Section 3.3* below).

[28] It also is worth noting that under the nFADP, existing personal data protections remain in place, including: data collection and processing must be lawful (Art. 6 par. 1 nFADP); done in good faith (Art. 6 par. 2 nFADP); and proportional (Art. 6 par. 2 nFADP). In general, for a private entity, lawful implies (Art. 21 par. 1 nFADP): (*i*) the consent of the data subject; (*ii*) an overriding interest; or (*iii*) a legal basis. For federal bodies, this implies a legal basis (Art. 34 par. 1 nFADP).

3.2. Under the nFADP

[29] The nFADP has provisions that cover certain issues that could arise with AI, in particular, (*i*) mass surveillance, including with regard to biometric data, and (*ii*) the automated processing of personal data.

3.2.1. Mass surveillance

[30] In proposing the nFADP, the Federal Council was aware of the concerns already raised with regard to mass surveillance and the resulting mass collection of personal data, in particular those expressed by the UN Special Rapporteur for privacy and the UN Human Rights Council regarding mass surveillance.[23]

[31] The nFADP, therefore, contains certain specific provisions related to mass surveillance, including: (*i*) special treatment of biometric data (*Point 3.2.1.1* below); (*ii*) the data protection impact assessment (*Point 3.2.1.2* below); (*iii*) logging (*Point 3.2.1.3* below); and (*iv*) data processing regulations (*Point 3.2.1.4* below).

3.2.1.1. Biometric data

[32] One aspect of mass data collection by AI that has garnered a lot of attention is the use of AI to collect biometric data.[24]

[33] In that context, it should be noted that already in 2017, the Federal Council clearly stated that it wanted the nFADP to address biometric data,[25] which it defined as «*personal data resulting from specific technical treatment and relating to physical, psychological or behavioural characteristics of an individual, which identify or confirm the identity of the individual. These include, for example, fingerprints, facial imaging, retinal scans, and even one's voice*».[26]

[34] This is reflected in the nFADP, under which biometric data now are classified as sensitive data (Art. 5 let. c nFADP), meaning their collection and processing are subject to additional protective measures, in particular when there is a mass collection.

---

23 See *Section 2* above.

24 See European Parliament, «Regulating facial recognition in the EU» (2021) 8 https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/698021/EPRS_IDA(2021)698021_EN.pdf accessed 2 August 2023.

25 FF 2017 6565, 6640.

26 FF 2017 6565, 6641.

[35] For instance, express consent is required for their collection (Art. 6 par. 7 let. a nFADP). Further, it is unlawful to communicate sensitive data to a third party (Art. 30 par. 2 let. c nFADP). Further, federal bodies only may process sensitive personal data when permitted to do so by a formal law (Art. 34 par. 2 let. a nFADP).

[36] Moreover, the large-scale processing of sensitive personal data is deemed high-risk processing, triggering the need to conduct a data protection impact assessment (Art. 22 par. 2 let. b nFADP – see *Point 3.2.1.2* below), keep a data log (Art. 4 par. 1 nODP – see *Point 3.2.1.3* below) and draw up data processing regulations (Art. 5 par. 1 let. a nODP – see *Point 3.2.1.4* below).

3.2.1.2. Data protection impact assessment

[37] Under the nFADP, a data protection impact assessment must be carried out in certain situations that are considered high risk.

[38] As a general rule, both the mass surveillance of public areas (Art. 22 par. 2 let. a nFADP) and the mass processing of sensitive data (Art. 22 par. 2 let. b nFADP) are deemed high risk and, therefore, require that a data protection impact assessment be carried out.

[39] Moreover, even without the presence of one of these two elements, the use of new technology, such as AI, to carry out the collection or processing of personal data is mentioned expressly as something that may create a high risk, resulting in the need to carry out a data protection impact assessment.

[40] The data protection impact assessment must: (*i*) include a description of the data processing that is planned; (*ii*) evaluate the risks; and (*iii*) enumerate the measures that will be taken to mitigate the risks.

[41] In addition, unless a data protection officer has been appointed, the data controller must consult with the Federal Data Protection and Information Commissioner («**FDPIC**») prior to processing any data if the impact assessment shows that, despite the proposed mitigation measures, the planned processing still could pose a high risk to the data subject.

3.2.1.3. Log

[42] When preventive measures are not sufficient to guarantee data protection and there is mass automated processing of sensitive data, the private data controller and processor must log the recording, modification, reading, communication, erasure and destruction of the personal data (Art. 4 par. 1 nODP).

3.2.1.4. Processing regulations

[43] The nODP also requires private data processors (Art. 5 par. 1 let. a nODP) and federal data processors (Art. 6 par. 1 let. a nODP) to draw up data processing regulations when there is mass processing of sensitive personal data.

[44] The regulations must contain, in particular: (*i*) information on the internal organisation; (*ii*) data processing and control procedures; and (*iii*) measures taken to ensure data security.

3.2.2. Automated processing

[45] The Federal Council's bill also shows that it had considered the risks posed by the automated processing of personal data when it proposed the new data protection rules.[27]

[46] This is reflected in the nFADP, which addresses, in particular, (*i*) profiling (*Point 3.2.2.1* below), and (*ii*) automated decisions (*Point 3.2.2.2* below).

3.2.2.1. Profiling

[47] The nFADP introduces two categories of profiling: (*i*) ordinary profiling, and (*ii*) high-risk profiling.

[48] Ordinary profiling is the automated processing of personal data involving the use of such data to evaluate personal characteristics of an individual, in particular, to analyse or predict the individual's work performance, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements (Art. 5 let. f nFADP).

[49] High-risk profiling is profiling that poses a high risk to an individual's personality or fundamental rights, because it leads to data matching (i.e. crossreferencing personal data to analyse an individual's essential personal characteristics).

[50] The nFADP contains specific protections with regard to profiling, especially high-risk profiling.

[51] For instance, express consent is required for profiling by federal authorities (Art. 6 par. 7 let. c nFADP) and high-risk profiling by private entities (Art. 6 par. 7 let. b nFADP) and federal bodies only may carry out profiling when permitted to do so by a formal law (Art. 34 par. 2 let. b nFADP).

[52] Moreover, data processing regulations also are required in the event of high-risk profiling by private data processors (Art. 5 par. 1 let. b nODP) and federal data processors (Art. 6 par. 1 let. b nODP).[28]

3.2.2.2. Automated decisions

[53] Under the nFADP, the data subject must be informed when an automated decision is made (i.e. a decision made exclusively based on the automated processing of personal data) when this decision has legal effects for the data subject or significantly affects the data subject (Art. 21 par. 1 nFADP).

[54] The data subject also must be informed of the possibility to submit their opinion regarding this decision and request that it be reviewed by a human (Art. 21 par. 2 nFADP).

---

27 See in particular FF 2017 6565, 6568, 6592, 6595, 6602, 6673 *et seq.*

28 See *Point 3.2.1.4* above for more information about data processing regulations.

3.3. Other sources

3.3.1. International

[55] The below overviews the primary personal data protections applicable in Switzerland under international law.

3.3.1.1. Convention 108+

[56] Convention 108+ is a Council of Europe convention. It is the modernised version of Convention 108, the first legally binding international instrument related to data protection.[29] Switzerland signed and ratified the convention in 1997.[30]

[57] Convention 108+ has specific protections with regard to the processing of biometric data uniquely identifying an individual. Although no specific reference is made to mass surveillance, Convention 108+ does require that the processing of biometric data only «*be allowed where appropriate safeguards are enshrined in law*» (Art. 6 par. 1 Convention 108+), and that «*[s]uch safeguards shall guard against the risks that the processing of sensitive data may present for the interests, rights and fundamental freedoms*» (Art. 6 par. 2 Convention 108+).

[58] Convention 108+ also has specific protections with regard to automated decisions. In particular, it states that individuals shall have the right not to be the subject of an automated decision without their views being taken into account (Art. 9 par. 1 let. a Convention 108+).

3.3.1.2. European Human Rights Convention

[59] Art. 8 of the ECHR[31] guarantees the right to private and family life.

[60] This has been interpreted by the European Court of Human Rights («**ECtHR**») as including the protection of personal data.[32]

[61] Further, in *Big Brother Watch and Others v the United Kingdom*,[33] the ECtHR ruled that the bulk interception of communications without sufficient oversight and safeguards, including an assessment of the proportionality, independent authorisation, supervision and *ex post facto* review, constitutes a violation of Art. 8 ECHR.

---

29 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108); Council of Europe, «Convention 108 and Protocols» https://www.coe.int/en/web/data-protection/convention108-and-protocol accessed 2 August 2023; Council of Europe, «Background» https://www.coe.int/en/web/data-protection/convention108/background accessed 2 August 2023.

30 Council of Europe, «Chart of signatures and ratifications of Treaty 108» https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=108 accessed 2 August 2023.

31 Convention for the Protection of Human Rights and Fundamental Freedoms (cited: «**European Human Rights Convention**» or «**ECHR**»).

32 See *Gaughran v the United Kingdom* App. no. 45245/15 (ECtHR, 13 February 2020); *Catt v the United Kingdom* App. no. 43514/15 (ECtHR, 24 January 2019); *Aycaguer v France* App. no. 8806/12 (ECtHR, 22 June 2017); Giorgio Malinverni, «La Cour européenne des droits de l'homme et la protection des données – développements récents» in: Astrid Epiney and Daniela Nüesch (eds.), Durchsetzung der Rechte der Betroffenen im Bereich des Datenschutzes/La mise en oeuvre des droits des particuliers dans le domaine de la protection des données (Schulthess Juristische Medien AG 2015) 1 *et seq*.

33 Szabó and Vissy v Hungary App. no. 37138/14 (ECtHR, 12 January 2016).

[62] Moreover, in *Szabó and Vissy v Hungary*,[34] the ECtHR ruled that there had been a violation of Art. 8 ECHR due to Hungary's use of new technologies in the mass monitoring of communications in the absence of a legal base providing sufficient protections.

[63] It should be noted that the Swiss Federal Supreme Court cited Art. 8 ECHR in its decision partially invalidating Zurich law permitting the use of surveillance through automated programmes.[35]

3.3.2. Domestic

3.3.2.1. Constitution

[64] The Swiss Constitution[36] also protects private life and family life (Art. 13 par. 1 Cst). Moreover, the Constitution specifically stipulates that this protection includes «*the right to be protected against the misuse of [. . .] personal data*» (Art. 13 par. 2 Cst).

[65] The Swiss Federal Supreme Court has stated that the protection provided under Art. 13 Cst. is similar to that afforded under Art. 8 ECHR.[37]

3.3.2.2. Criminal Procedure Code

[66] The Criminal Procedure Code[38] also contains specific dispositions regarding the collection of personal data in the context of criminal investigations.

[67] In the first place, the Criminal Procedure Code states that, as a general rule, «*[p]ersonal data must be obtained from the person concerned or with that person's knowledge unless the proceedings otherwise would be prejudiced or unreasonable inconvenience or expense would be incurred*» (Art. 95 par. 1 CrimPC) and when this is not done, the person must be informed immediately, unless an overriding public or private interest prevents it (Art. 95 par. 2 CrimPC).

[68] Moreover, the Criminal Procedure Code contains specific protections related to the covert use of software for the surveillance of telecommunications.

[69] Specifically, the prosecutor may order the use of such software for the purposes of intercepting and recovering the content of communications and telecommunications' metadata in their unencrypted form if the following conditions are met: (*i*) there is strong suspicion that certain serious offences have been committed; (*ii*) the seriousness of the suspected offence justifies surveillance; (*iii*) previous (less intrusive) investigative measures have been unsuccessful or such investigations would not have succeeded or would have been unreasonably complicated (Art. 269ter par. 1 let. a–c CrimPC, in conjunction with Art. 269 par. 1 and 3 CrimPC and Art. 286 par. 2 CrimPC). Moreover, such surveillance must be validated by a court (Art. 272 CrimPC).

[70] The Criminal Procedure Code also contains specific protections related to the covert use of surveillance devices.

---

34 Big Brother Watch and Others v the United Kingdom App. nos. 58170/13, 62322/14 and 24969/15 (ECtHR, 25 May 2021).

35 ATF 140 I 353, consid 8.3 *et seq*.

36 Federal Constitution of the Swiss Confederation of 18 April 1999, RS 101 (cited: «**Constitution**» or «**Cst**»).

37 See ATF 140 I 353, consid 8.3.

38 Swiss Criminal Procedure Code of 5 October 2007, RS 312 (cited: «**Criminal Procedure Code**» or «**CrimPC**»).

[71] Specifically, the prosecutor may order the use of such devices for the purposes of (*i*) listening to or recording private conversations; (*ii*) observing or recording private events and events in not generally accessible places; or (*iii*) establishing the whereabouts of persons or property (Art. 280 let. a–c CrimPC). Moreover, the devices only may be used with regard to a suspect (Art. 281 par. 1 CrimPC), although the monitoring of third parties' premises and cars is permitted if they are believed to be used by the suspect (Art. 281 par. 2 CrimPC). The conditions stated above with regard to the surveillance of telecommunications also apply and such surveillance also must be validated by a court (Art. 282 par. 1 CrimPC, in conjunction with Art. 269–279 CrimPC).

[72] Moreover, the Criminal Procedure Code also contains specific protections related to the surveillance (image and sound recordings) of public places.

[73] Specifically, the prosecutor or police may do so if: (*i*) based on specific information, there is reason to believe that a felony or misdemeanour was committed, and (*ii*) the investigation cannot be carried out in a less intrusive manner, or it would be unreasonably complicated to do so (Art. 282 par. 1 let. a–b CrimPC).

[74] It should be noted that this surveillance of public places relates to surveillance in the context of a criminal investigation. The police also have certain surveillance powers as part of their general policing role and these are not covered by the restrictions set forth in the Criminal Procedure Code.[39] Moreover, as these are cantonal and communal authorities, local data protection rules apply rather than the federal rules contained in the nFADP.

3.3.2.3. Labour Law and Employment Law

[75] It should be noted that employees benefit from an accrued protection of personal data under (*i*) labour law (i.e. public law provisions applicable to employees), and (*ii*) employment law (i.e. private law provisions applicable when there is an employment contract pursuant to Art. 319 *et seq.* of the Swiss Code of Obligations).[40]

a. Labour Law

[76] Art. 6 par. 1 of the Swiss Labour Act[41] requires employers to protect the health and personal integrity of their employees.

[77] This obligation is concretised in Art. 26 par. 1 of Ordinance 3 to the Labour Act – Health Protection,[42] which explicitly states that it is unlawful to use surveillance or monitoring systems for the purposes of monitoring the behaviour of employees at their workstations.

[78] Surveillance or monitoring systems may be used for other reasons (i.e. economic reasons or health and safety), but in this case, the monitoring systems must be designed and arranged in

39 Olivier Guéniat/Yanis Callandret/Murielle de Sepibus, in: Commentaire romand, Commentaire romand Code de procédure pénale suisse, 2019, no. 2 ad Art. 282 CPP and references cited; Yvan Jeanneret/André Kuhn, Précis de procédure pénale (2nd edn, Stämpfli 2018) 418–419.

40 Federal Act on the Amendment of the Swiss Civil Code (Part Five: The Code of Obligations) of 30 March 1911, RS 220 (cited: «**Code of Obligations**» or «**SCO**»).

41 Swiss Labour Act of 13 March 1964, RS 822.11 (cited: «**Labour Act**»).

42 The Ordinance 3 to the Labour Act – Health Protection of 18 August 1993, RS 822.113 (cited: «**OLT 3**»).

such a way as not to affect the health or freedom of movement of employees (Art. 26 par. 2 OLT 3).[43]

b. Employment Law

[79] Moreover, Art. 328*b* CO explicitly states that an employer only may handle employee personal data to the extent that the data concern the employee's suitability for their job or are necessary for the performance of the employment contract.

4. Proposed AI-specific protections in the EU: the AI Act

4.1. Introduction to the AI Act

4.1.1. Background

[80] The EU was mulling over the question of whether, and how, to govern AI long before ChatGPT appeared on the scene.

[81] In 2021, the European Commission proposed the first version of the AI Act.

[82] On 14 May 2023, possibly spurred on by the advent of ChatGPT, the European Parliament amended and then approved the AI Act.[44]

[83] The European Parliament is in talks with the EU States on the European Council regarding the final version of the AI Act.[45]

4.1.2. Overview

[84] It should be noted that the AI Act aims to govern all aspects of AI and, therefore, addresses a multitude of risks that may arise in relation with AI systems and does not limit itself to personal data protection aspects.

[85] The AI Act proposes enhanced protections against AI based on the risk presented by the AI system.[46]

[86] This is done by dividing AI systems into four different risk categories, each with their own rules.

[87] These categories are: (*i*) unacceptable risk (*Point 4.2* below); (*ii*) high risk (*Point 4.3* below); (*iii*) limited risk (*Point 4.4* below); and (*iv*) minimal risk (*Point 4.5* below).

---

43 See SECO, «Commentaire des ordonnances 3 et 4 relatives à la loi sur le travail Protection de la santé Approbation des plans» (Bern 2023) 326-1; SECO, «Liste de contrôle – Surveillance technique au poste de travail» (Bern 2021); Philippe Meier, Protection des données (Stämpfli 2011) 686 *et seq*.

44 European Parliament, PV 14/06/2023 – 10.6; European Parliament, «Amendments adopted by the European Parliament on 14 June 2023 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD))», P9_TA(2023)0236.

45 European Parliament, «EU AI Act: first regulation on artificial intelligence» https://www.europarl.europa.eu/news/en/headlines/society/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence accessed 4 August 2023.

46 Tambiama Madiega, «Artificial intelligence act» (June 2023, European Parliamentary Research Service) PE 698.792, 1, 3–6.

[88] Further, the European Parliament added a number of special rules that specifically address general-purpose AI/foundation models and generative AI (*Point 4.6* below).[47]

[89] The AI Act also contains provisions to address concerns about stifling innovation (*Point 4.7* below).

4.2. Unacceptable risk

4.2.1. Scope

[90] Unacceptable risk AI systems with regard to data protection include:[48]

- social scoring systems; these are AI systems that can classify individuals based on behaviour, socio-economic status, personal characteristics, etc. (Art. 5 par. 1 let. b a AI Act);
- biometric categorisation systems using sensitive characteristics, including gender, race, ethnicity, citizenship status, religion, sexual orientation and political opinions (Art. 5 par. 1 let. c AI Act);
- AI systems that analyse recorded footage of publicly accessible spaces through real-time and «post» remote biometric identification systems, including facial recognition (Art. 5 par. 1 let. d AI Act);
- predictive policing systems (Art. 5 par. 1 let. d a AI Act);
- AI systems that infer emotions of individuals in the areas of law enforcement, border management, workplaces and educational institutions (Art. 5 par. 1 let. d b AI Act); and
- AI systems that create or expand facial recognition databases through the untargeted scraping of facial images from the internet or CCTV footage (Art. 5 par. 1 let. d c AI Act).

4.2.2. Rules

[91] The putting into service and use of unacceptable risk AI systems are prohibited under the AI Act (Art. 5 par. 1 AI Act).

[92] Limited exceptions exist. For instance, the use of AI systems to conduct surveillance of publicly accessible spaces using biometric data is allowed if there is pre-judicial authorisation and doing so is strictly necessary for a targeted search connected to a specific serious criminal offense (Art. 5 par. 1 let. d d AI Act).

---

47 European Parliament, «Amendments adopted by the European Parliament on 14 June 2023 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD))», P9_TA(2023)0236; see also: Tambiama Madiega, «Artificial intelligence act» (June 2023, European Parliamentary Research Service) PE 698.792, 10; European Parliament, «EU AI Act: first regulation on artificial intelligence» https://www.europarl.europa.eu/news/en/headlines/society/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence accessed 4 August 2023.

48 See Tambiama Madiega, «Artificial intelligence act» (June 2023, European Parliamentary Research Service) PE 698.792, 10; European Parliament, «EU AI Act: first regulation on artificial intelligence» https://www.europarl.europa.eu/news/en/headlines/society/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence accessed 4 August 2023.

4.3. High risk

4.3.1. Scope

[93] High-risk AI systems with regard to data protection include AI systems in the following areas (Art. 6 par. 1 let. b AI Act):[49]

- biometric identification and categorisation of individuals (Annex III par. 1 point 1 AI Act);
- employment, worker management and access to self-employment (Annex III par. 1 point 4 AI Act);
- access to, and enjoyment of, essential private services and public services and benefits (Annex III par. 1 point 1 let. a AI Act);
- determining creditworthiness (Annex III par. 1 point 1 let. b AI Act);
- law enforcement; (Annex III par. 1 point 6 let. b, d, f and g AI Act); and
- migration, asylum and border control management (Annex III par. 1 point 7 let. b–b d AI Act).

4.3.2. Rules

[94] A risk management system must be established, implemented, documented and maintained in relation to high-risk AI systems (Art. 9 par. 1 AI Act).

[95] The risk management system must be run throughout the entire lifecycle of the system and must contain: (*i*) identification and analysis of certain known and reasonably foreseeable risks associated with the system; (*ii*) an evaluation of other risks that could arise in certain post-marketing circumstances; and (*iii*) the adoption of appropriate and targeted risk management measures designed to address the risks identified (Art. 10 par. 2 let. a–d AI Act).

[96] Moreover, logs must be maintained with regard to high-risk AI systems (Art. 12 AI Act).

[97] Further, high-risk AI systems must be designed and developed so as to ensure sufficiently transparent operation (Art. 13 par. 1 AI Act).

[98] High-risk AI systems also must be accompanied by intelligible instructions with correct and clear information (Art. 13 par. 2 AI Act).

[99] Additionally, high-risk AI systems must be designed to allow for human oversight during their use (Art. 14 par. 1 AI Act). They also must follow the principle of security by design and by default (Art. 15 par. 1 AI Act).

[100] These rules create a myriad of obligations for providers and users of high-risk AI systems (Art. 16–29 AI Act).

---

49 See Tambiama Madiega, «Artificial intelligence act» (June 2023, European Parliamentary Research Service) PE 698.792, 10; European Parliament, «EU AI Act: first regulation on artificial intelligence» https://www.europarl.europa.eu/news/en/headlines/society/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence accessed 4 August 2023.

4.4. Limited risk

4.4.1. Scope

[101] Limited-risk AI systems are other AI systems, which are designed to interact with individuals.

4.4.2. Rules

[102] Limited-risk AI systems are subject to certain transparency requirements.

[103] In particular, the AI system, the provider or the user shall inform the individual who is interacting with the AI system that they are interacting with an AI system. This must be done with in a timely, clear and intelligible manner, unless it is obvious (Art. 52 par. 1 AI Act).[50]

[104] Moreover, in general, users of permitted emotion recognition systems or permitted biometric categorisation systems shall inform the individual who is interacting with the AI system of the nature of the operation and obtain consent for processing personal data pursuant to the GDPR (Art. 52 par. 2 AI Act).

4.5. Minimal risk

4.5.1. Scope

[105] Minimal-risk AI systems are those not specifically covered under the AI Act.[51]

4.5.2. Rules

[106] As minimal-risk AI systems are not specifically covered under the AI Act, the AI Act does not contain rules governing them.

4.6. General-purpose AI, foundation models and generative AI

4.6.1. Scope

[107] The amended version of the AI Act, as adopted by the European Parliament, contains additional protections with regard to general-purpose AI, foundation models and generative AI.

[108] The terms general-purpose AI and foundation models often are used interchangeably and refer to AI systems «*trained on a broad set of unlabelled data that can be used for different tasks with minimal fine-tuning*».[52]

---

50 See European Parliament, «EU AI Act: first regulation on artificial intelligence» https://www.europarl.europa.eu/news/en/headlines/society/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence accessed 4 August 2023.

51 See European Commission, «Regulatory framework proposal on artificial intelligence» https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai accessed 6 August 2023.

52 Tambiama Madiega, «General-purpose artificial intelligence» (March 2023, European Parliamentary Research Service) PE 745.708, 1.

[109] Generative AI, such as ChatGPT, is a common example of a general-purpose AI/foundation model.[53]

4.6.2. Rules

[110] In particular, the AI Act requires that users of AI systems that generate or manipulate text, audio or visual content that falsely would appear to be authentic or truthful and which feature depictions of people appearing to say or do things they did not say or do, without their consent, inform the individual interacting with the AI system of this. This must be done in a timely, clear and visible manner and, when possible, the name of the person who generated the content also should be disclosed (Art. 52 par. 3 point 1 AI Act).

4.7. Innovation

[111] The AI Act requires all EU Member States to create at least one AI regulatory sandbox (Art. 53 par. 1 AI Act). Joint AI regulatory sandboxes, as well as sandboxes created by the European Data Protection Supervisor also are possible (Art. 53 par. 1 let. a-b AI Act).

[112] SMEs and startups may access the sandboxes free of charge (Art. 53 a let. c AI Act).

[113] Moreover, under certain circumstances (e.g. substantial public interest), personal data lawfully collected for other purposes may be processed, but solely for the purposes of developing and testing certain AI systems in the sandbox (Art. 54 par. 1 AI Act).

5. Comparison

[114] At its essence, the difference between the Swiss approach and the EU approach is that with the AI Act, the EU is looking to create a comprehensive regulatory framework governing AI across multiple sectors.

[115] As the scope of this article is personal data protection, the following sections: (*i*) compare the personal data protections offered under Swiss law with those in the AI Act (see *Point 5.1* below), and (*ii*) analyse the advantages (see *Point 5.2* below) and (*iii*) disadvantages (see *Point 5.3* below) of the Swiss approach when compared with the EU approach.

5.1. Personal data protection

[116] As mentioned in *Section 2* above, two primary areas where AI poses an increased risk from a personal data protection standpoint are: (*i*) the mass collection of personal data conducted by AI, in particular biometric data; and (*ii*) the use of AI to automate the processing of personal data.

[117] In this context, the following sections analyse whether Swiss law offers as much personal data protection, especially with respect to these two points, as that provided for under the AI

53 Tambiama Madiega, «General-purpose artificial intelligence» (March 2023, European Parliamentary Research Service) PE 745.708, 1; Tambiama Madiega, «Artificial intelligence act» (June 2023, European Parliamentary Research Service) PE 698.792, 10.

Act. To do so, the following sections compare Swiss personal data protections with those provided for under the different categories of the AI Act: (*i*) unacceptable risk AI systems (see *Point 5.1.1* below); (*ii*) high-risk AI systems (see *Point 5.1.2* below); (*iii*) limited-risk AI systems (see *Point 5.1.3* below); (*iv*) minimal-risk AI systems (see *Point 5.1.4* below); and (*v*) general-purpose AI/foundation models and generative AI (see *Point 5.1.5* below).

[118] Overall, it can be said that the personal data protection rules introduced under the nFADP, and contained elsewhere in Swiss law, offer a similar level of protection to those in the AI Act for the reasons outlined below with regard to private entities, but less protection with regard to State surveillance.

[119] It should be noted that this section does not analyse other protections offered in the EU, such as those in the GDPR, as the purpose of this article is to compare Swiss personal data protections with any specific, new personal data protections contained in the AI Act.

5.1.1. Unacceptable risk

[120] The AI Act would prohibit outright a certain number of AI systems. As noted above, some of these prohibited AI systems could be used to collect and process personal data and, in that context, pose personal data protection risks.

[121] Swiss law does not contain a list of prohibited AI systems.

[122] That said, the use of many of these prohibited systems would be unlawful in Switzerland.

[123] In particular, many of these systems would not meet the proportionality requirement contained in the nFADP.

[124] For instance, the FDPIC previously has stated that surveillance in publicly accessible spaces, when not carried out by the State, generally is not proportional.[54]

[125] In this sense, the Swiss system actually could provide better personal data protection for individuals, as the authorities and courts would need to examine systems on a case-by-case basis, based on the risks in that case. Therefore, it is possible that in some instances, AI systems not banned under the AI Act could be allowed in the EU, but not in Switzerland.

[126] That said, there also are some instances where not having such a blanket ban could provide less personal data protection.

[127] This is especially the case with regard to the use of remote biometric identification AI systems that analyse recorded footage of publicly accessible spaces, when done by the State.

[128] First, as general policing surveillance powers are not covered by the restrictions set forth in the Criminal Procedure Code, it falls on the cantons and communes to fix the rules, within the limits of international and federal law and, as explained above, these rules do not fall under the scope of the nFADP. This leads to a lack of clarity as to whether, and in what measure, video surveillance and facial recognition may be used in the context of general policing.[55]

54 FDPIC, «Vidéosurveillance de l'espace public effectuée par des particuliers» (24 July 2023) https://www.edoeb.admin.ch/edoeb/fr/home/datenschutz/ueberwachung_sicherheit/uerberwachung-oeff-raum-private.html accessed 10 August 2023.

55 Humanrights.ch, «Vidéosurveillance en Suisse: gare au flou juridique» (21 October 2018 https://www.humanrights.ch/fr/pfi/droits-humains/sphere-privee/videosurveillance-critique accessed 10 August 2023.

[129] Moreover, federally, the use of facial recognition systems is not forbidden, as long as it is expressly provided for in a formal law.[56]

[130] Further, the Criminal Procedure Code does not regulate explicitly the situations under which such systems would be permitted in the context of a criminal investigation and does not contain more stringent requirements beyond those applicable to the covert use of surveillance devices or observation of public areas, even though the use of AI could expand greatly the analytic capacity of both these measures.

[131] Therefore, at least with regard to remote biometric identification AI systems that analyse recorded footage of publicly accessible spaces, when done by the State, the personal data protections in Switzerland do not go as far as those proposed under the AI Act, as the AI Act would ban such systems entirely, except in certain instances, when pre-judicial authorisation has been obtained. That said, it should be noted that this blanket ban on facial recognition was only added by the European Parliament and it remains to be seen whether it will be included in the final version.[57]

5.1.2. High risk

[132] The nFADP also contains the notion of risk and specifically provides that certain high-risk personal data collection and processing trigger additional requirements.

[133] Under the nFADP, this high-risk personal data collection and processing triggers the obligation to carry out a data protection impact assessment and, in some instances, obligations to keep logs and draw up processing regulations.

[134] Moreover, it should be noted that the requirement for a Swiss data protection impact assessment is similar to the risk management system required under the AI Act for high-risk systems.

[135] Where the Swiss system particularly differs from the AI Act, is that there is no comprehensive list of high-risk areas.

[136] The nFADP lists both the mass surveillance of public areas and the mass processing of sensitive data (including biometric data) as being considered high-risk. Beyond this, other situations must be judged on a case-by-case basis to see whether they are high-risk, with particular attention being paid when new technology, such as AI, is used.

[137] In that context, again, the Swiss system could provide better protection, as the authorities and courts would need to examine systems on a case-by-case basis, based on the risks in that case, meaning that in some instances, the use of AI systems not considered high-risk under the AI Act would be considered so in Switzerland.

[138] Moreover, the general Swiss legal framework already provides certain accrued protections in some of the areas deemed high-risk under the AI Act.

[139] In particular, the collection of any data by federal bodies requires a legal basis and this legal basis must be a formal law when sensitive data are processed or there is profiling, meaning addi-

56 Federal Council, «Le Conseil fédéral approuve le crédit d'engagement pour le renouvellement du système AFIS» (31 May 2023) https://www.fedpol.admin.ch/fedpol/fr/home/aktuell/mm.msg-id-94141.html accessed 10 August 2023.

57 Gian Volpicelli, «Facial-recognition ban gets lawmakers' backing in AI Act vote» *Politico* (Brussels, 11 May 2023) https://www.politico.eu/article/meps-adopt-ai-act-text-in-committees accessed 10 August 2023.

tional protections would be offered with regard to access to certain public services and benefits, federal law enforcement activities and migration, asylum and border control.

[140] Further, the Labour Act and Code of Obligations provide additional protections regarding employee personal data, by forbidding the use of surveillance or monitoring systems to monitor the behaviour of employees at their workstations and, generally, limiting the personal data that may be collected.

5.1.3. Limited risk

[141] With regard to limited-risk AI systems, it should be noted that were those systems to be collecting or processing personal data, then information would need to be disclosed to the individual interacting with the system under the nFADP.

[142] This would create a similar, although not identical, obligation to the AI Act's transparency requirement, as information would need to be provided regarding, at the very least, the identity of the data controller, the purpose of the data collection and to whom data will be transferred.

[143] Moreover, were biometric data to be collected, express consent also would be needed under the nFADP, which would provide similar protections to those provided under the AI Act (which references the GDPR).

5.1.4. Minimal risk

[144] With regard to minimal-risk AI systems, it should be noted that were those systems to be collecting or processing personal data, then the protections mentioned under *Point 5.1.3* above still would apply.

[145] Therefore, this provides additional protections than those in the AI Act, as these systems are outside its scope.

5.1.5. General-purpose AI/foundation models and generative AI

[146] The protections mentioned under *Point 5.1.3* above would apply to general-purpose AI/ foundation models and generative AI.

[147] Therefore, Swiss data protection rules already afford some protection with regard to these new technologies.

[148] That said, the privacy notice required under the nFADP does not explicitly require that the data subject be provided with information regarding the generation or manipulation of content. However, in certain situations, an argument could be made that this information is necessary to understand the purpose of the data collection or to give consent. This especially could be the case when express consent is required, such as for the collection of biometric data.

5.2. Advantages of the Swiss approach

[149] The primary advantages of the Swiss approach are: (*i*) the ability to have a nuanced approach, rather than trying to cover all aspects of AI under one sweeping act (see *Point 5.2.1* below), and (*ii*) promoting innovation (see *Point 5.2.2* below).

5.2.1. Nuanced approach

[150] As noted above, there is no one accepted definition of AI.

[151] Therefore, in trying to both define and govern all aspects AI in one act, the EU approach risks not being nuanced enough.

[152] This creates two primary problems: (*i*) inadvertently excluding certain systems (see *Point 5.2.1.1* below), and (*ii*) overreaching (see *Point 5.2.1.2* below).

[153] The Swiss approach avoids these pitfalls, by not trying to define and govern all aspects of AI in one all-encompassing act.

[154] This allows for the introduction of new, specific protections into existing legislation, on an as-needed basis.

5.2.1.1. Exclusion

[155] Firstly, the EU approach risks having a definition which inadvertently excludes certain systems or is unfit to cover future systems that may emerge.

[156] For instance, in its submission regarding the European Commission's initial proposal, Algorithm Watch,[58] a non-profit research and advocacy organisation active in the field of automated decision making, advocated basing protection on the impact on individuals and society, rather than the type of technology and suggested focusing on the notion of the concept of automated and algorithmic decision-making systems, rather than AI *per se*.[59]

[157] For the most part, this feedback was not integrated in the European Parliament's amendments.

[158] By attempting to create definitive lists of AI systems that are unacceptable and that are high-risk, the EU approach increases this risk.

[159] In this context, it is worth noting that the European Parliament's decision to include special rules for general-purpose AI, foundation models and generative AI likely, at least in part, was driven by the recent launch of ChatGPT. This would seem to indicate that the European Commission's proposal was not entirely adequate or appropriate with regard to these new AI systems. Although, in this instance, it still was possible to modify the AI Act, once adopted, it no longer will be possible to easily modify the rules when new AI technologies emerge.

5.2.1.2. Overreaching

[160] Secondly, the definition of AI in the AI Act is broad. This is understandable, as both the European Commission and European Parliament would have been eager to minimise the aforementioned risk of inadvertently excluding certain systems.

---

58 Algorithm Watch, «Vision, Mission & Values», https://algorithmwatch.org/en/vision-mission-values/ accessed 8 August 2023.

59 Algorithm Watch, «Submission to the European Commission's Consultation on a Draft Artificial Intelligence (AI) Act» (August 2021), https://algorithmwatch.org/en/wp-content/uploads/2021/08/EU-AI-Act-Consultation-Submission-by-AlgorithmWatch-August-2021.pdf accessed 6 August 2023; Tambiama Madiega, «Artificial intelligence act» (June 2023, European Parliamentary Research Service) PE 698.792, 7.

[161] However, this is problematic in its own right, as it could create a risk of legal uncertainty with regard to whether a system falls under the scope of the AI Act.[60]

5.2.2. Innovation

[162] The AI Act sends a strong message that the EU wants to regulate AI proactively and creates a complex regulatory framework.

[163] Although not universally accepted, according to the Centre for Data Innovation, the AI Act would reduce AI investments by almost 20%.[61]

[164] In any case, many companies already have signalled their anxiety regarding the AI Act.[62]

[165] By not introducing similar legislation at this point in time, Switzerland is able to position itself as more innovation- and AI-friendly, making Switzerland more attractive to AI companies, and companies looking to get into the AI business.

5.3. Disadvantages of the Swiss approach

[166] The primary disadvantages of the Swiss approach are: (*i*) the risk of having different treatment, or no treatment, of AI depending on the field (see *Point 5.3.1* below), and (*ii*) not being in a position to act in a timely matter with regard to governing AI (see *Point 5.3.2* below).

5.3.1. Piece-meal solution

[167] Although, as mentioned above, there are problems with trying to define and govern all aspects of AI in one definitive act, in particular, with creating definitive lists of AI systems that are unacceptable and that are high-risk, the Swiss approach risks ending up with a piece meal solution.

[168] This would be disadvantageous for two primary reasons: (*i*) lack of legal certainty (see *Point 5.3.1.1* below); and (*ii*) unaddressed risks (see *Point 5.3.1.2* below).

5.3.1.1. Lack of legal certainty

[169] Firstly, the lack of a definitive notion as to which technologies present unacceptable risks (i.e. not proportional or threaten fundamental freedoms) or should be considered high-risk, means that the courts will need to fill in the gaps. This can lead to a lack of legal certainty, especially prior to leading case law being established.

---

60 See Big Data Value Association, «BDVA/DAIRO position paper Response to the European Commission's proposal for AI Regulation» (4 August 2021), https://www.bdva.eu/sites/default/files/BDVA_DAIRO%20response-feedback%20AI%20Regulation_Final.pdf accessed 6 August 2023; Tambiama Madiega, «Artificial intelligence act» (June 2023, European Parliamentary Research Service) PE 698.792, 7.

61 Tambiama Madiega, «Artificial intelligence act» (June 2023, European Parliamentary Research Service) PE 698.792, 7.

62 See Javier Espinoza, «European companies sound alarm over draft AI law» *Financial Times* (Brussels, 30 June 2023) https://www.ft.com/content/9b72a5f4-a6d8-41aa-95b8-c75f0bc92465 accessed 8 August 2023.

[170] For instance, a developer may not know whether their product ultimately will be allowed in Switzerland or a data controller may not know whether they ultimately will be allowed to use a certain system to collect or process personal data.

[171] In this context, there also is a risk of divergent case law or practice of the competent authorities when it comes to determining what is considered an unacceptable risk.

[172] This could lead to certain technologies being banned or subject to accrued protections in one legal domain, but not in another, which in turn could result in developers and users not knowing how to comply with Swiss rules.

5.3.1.2. Unaddressed risks

[173] Secondly, this approach could mean that risks go unaddressed.

[174] This is less of an issue in the field of data protection, as Swiss law already acknowledges the need for rules governing the protection of personal data and has a legal framework for doing so.

[175] However, although largely beyond the scope of this article, it should be mentioned that this is not true with regard to all areas where protection from AI might be needed. This especially is the case in emerging areas, such as the use of the AI to manipulate emotions and influence politics.

5.3.2. Timing

[176] Switzerland's robust legislative process means that it can take time for a new law to enter into force (i.e. discussions about the nFADP began in 2017).

[177] This means that in waiting to act with regard to AI until it is clearer how the field will develop, Switzerland risks being able to introduce into force a comprehensive law governing AI only after the need has emerged.

[178] In the meantime, gaps will be left to the courts and the authorities to fill (or not fill), which as noted above, creates legal uncertainty.

[179] Further, by not harmonising the introduction of measures governing AI with the EU, there is a risk that the solutions that Switzerland adopts later on will differ vastly from those in force in the EU (the so-called Swiss Finish).

[180] This presents challenges for companies looking to do business in Switzerland as it leads to situations where companies are forced apply a whole different set of rules if they wish to have a presence in Switzerland. Moreover, this is especially problematic given the cross-border nature of AI technology. It should be recalled that this already was the case under the previous FADP (with regard to the GDPR) and one of the reasons behind the adoption of the nFADP.

6. Conclusion

[181] Overall, now that the nFADP has entered into force, Switzerland should have adequate personal data protection rules with regard to AI that, in general, are not inferior to the additional personal data protections afforded under the AI Act.

[182] That said, there are inferior personal data protections with regard to the collection and processing of personal data by the State, especially in the context of mass surveillance of public areas and criminal investigations.

[183] In this context, more specific protections would have been welcome in the nFADP and it would be beneficial to introduce specific measures regarding AI systems and similar new technology into the Criminal Procedure Code.

[184] Nonetheless, overall, the Swiss approach has a number of advantages. In particular, by not trying to define and govern all aspects of AI in one definitive act and by not creating definitive lists of AI systems that are banned, the Swiss approach allows for a more nuanced approach to be taken and for innovation to be encouraged.

[185] However, the Swiss approach is not without its disadvantages. In particular, it could create a lack of legal certainty were divergent definitions of AI and risk to emerge in case law, while waiting for a formal law to be approved. Not harmonising Swiss law with the EU now also could result in companies having to apply one set of rules in the EU and another in Switzerland.

[186] However, given the current state of AI, the Swiss approach should allow for increased innovation and make Switzerland more attractive to AI and other new technology companies.

[187] In particular, rather than creating outright AI bans from the get-go, Switzerland is providing space for innovators and entrepreneurs to invent and create.

Rayan Houdrouge is a partner at Walder Wyss. He advises Swiss and multinational companies, among them disruptive technology companies, and international organisations on all employment-related matters. He has extensive experience in executive transfers, litigation, internal investigations, restructurings, business transfers and compensation packages, including for blockchain companies. He also has particular expertise in assisting HNWIs, especially with regard to residency and philanthropic matters. Rayan Houdrouge studied at the University of Lausanne (lic. iur.) and the New York University School of Law (LL.M. in Corporate Law).

Kathryn Kruglak is an associate at Walder Wyss. She advises clients on employment, data protection and immigration law, as well as social security and pension matters. Her areas of expertise also include Diversity Equity and Inclusion and blockchain and AI, especially regarding data protection aspects. She has particular experience with drafting employment contracts, termination agreements, personnel regulations, data protection regulations and privacy notices, conducting internal investigations, assisting international organisations and treating cross-border situations. Kathryn Kruglak studied at the University of Neuchâtel (BLaw, MLaw) and King's College London (LL.M., transnational law).