Legal, ethical and social impact on the use of computational intelligence based systems for land border crossings

Prof. Dr. Tina Krügel, LL.M.
Institute for Legal Informatics
Leibniz Universität Hannover
Hanover, Germany

RA Benjamin Schütze, LL.M. (Wellington)
Institute for Legal Informatics
Leibniz Universität Hannover
Hanover, Germany

Dipl.-Jur. Jonathan Stoklas
Institute for Legal Informatics
Leibniz Universität Hannover
Hanover, Germany

***Abstract* — This paper provides an overview on the most relevant legal, ethical and social implications arising from the use of computational intelligence based systems for land border crossings. Based on the automatic deception detection system (ADDS) developed in the iBorderCtrl project, issues such as the peculiarities of the interaction of humans with machines, profiling, automated decision-making and the risk of false positives can be identified and demonstrate how computational intelligence based systems can challenge fundamental legal and ethical principles. These include in particular the right to privacy, human dignity and the principle of non-discrimination. By further analysing the various issues, this paper seeks to provide some thoughts on remedies and safeguards which should be considered when developing computational intelligence based systems.**

Keywords — Law, Ethics, Fundamental Rights, Data Protection, Privacy, Computational Intelligence, Border Control

I. INTRODUCTION

The use of computational intelligence based systems is becoming more and more important from a practical point of view. These systems are not only capable of interacting with human beings, but also to decide on certain questions based on the input provided by an end-user and the underlying algorithm. To utilise these technologies, the EU-funded iBorderCtrl project [1] is currently developing a system to enhance the quality of border checks [2]. One particular aspect of this system is the use of an avatar interview with the traveller and deception detection technology, called "Automatic Deception Detection System" (ADDS): For an initial risk assessment regarding the traveller, a system for non-verbal behaviour analysis is being developed to detect whether a traveller is lying. The following article will first describe and analyse the technology developed in the course of iBorderCtrl as a possible use-case for computational intelligence based systems and then give an overview on the various legal, ethical and social implications. Following the results of iBorderCtrl as an European research project, the article will focus primarily on European legal sources. In general, rules on border crossings can be found in the various national legislations. It can be further refined by bilateral treaties. However, there is no statutory framework which could be applied on international level. From a privacy point of view, Convention 108 of the Council of Europe is the only viable global agreement, imposing minimum standards for privacy [3]. However, European rules on data protection might increasingly develop towards a standard even outside of the European Union, due to their widespread adoption by countries throughout the world enacting some or all of these rules [3].

II. DATA COLLECTION

A. The iBorderCtrl ADDS technology

The ADDS used in iBorderCtrl can be seen as a computational intelligence based system, as it interacts with human beings and analyses their behaviour. ADDS utilises a hierarchy of artificial neural networks which inform a deception score of a traveller whilst undertaking an avatar based interview. It is embedded in a two-stage process:

In a first stage, a traveller is asked to provide information concerning his/her person and the travel details. This information is being checked against various databases to determine whether the preconditions for crossing a border are met. Timewise, this step is detached from the border crossing, meaning that a traveller can pre-register a few days before the actual travel is scheduled. In order to verify whether the information provided by the traveller is correct, the traveller will be interviewed by a virtual avatar of a border guard in the pre-registration phase. The questions asked during the interview are based on the information registered by the system prior to the interview. By analysing the non-verbal communication of the traveller, the system verifies whether the information provided in the pre-registration was correct or whether there is a risk that the person made false statements in the pre-registration phase. Once the first stage is completed successfully, the traveller is allowed to approach the border crossing point, where an actual border check is being

conducted by the border guards, which is supplemented – among other things – by the results of the avatar interview.
To achieve this, the system observes non-verbal behaviour (so-called micro-gestures) while a traveller is being interviewed. Such observations can be semi-automatically analysed to quantify the likelihood of deceptive behaviour, i.e. false statements given by an interviewee. The system shall not only serve as an electronic aide to a human border agent, but shall be able to collect data autonomously by "communicating" directly with the travellers. Such communication shall be handled by a personalised avatar that will be created for each traveller. In addition, the avatar shall be capable of improving performance and accuracy as compared to human border guards, as it shall be able to individually adapt to each traveller's profile. Based on the data available on each traveller, this shall not only enable the iBorderCtrl ADDS to raise specific interview topics that are of higher relevance for certain travellers but may be irrelevant for others. All in all, the system will interact with the traveller autonomously by deciding on which questions to ask, how to behave (i.e. the avatar can adapt its behaviour to the behaviour of the traveller, such as acting rather sceptical if an answer seems to be not correct) and finally to assess the overall risk stemming from the traveller based on the information provided in the pre-registration phase and the results of the deception detection. This risk assessment will be delivered to the border guards, assisting them in their decisions during the actual border check in stage 2 on whether a person is allowed to cross the border, or if a thorough check might be required.

B. Impact of human-machine interaction

The interaction between humans and machines is an integral part of the ADDS system and the avatar interview. The purpose of those functionalities is to shift certain elements of the border check from the border crossing phase to the pre-registration, and, in consequence, from an interaction between border guards and travellers - both as human beings - to an interaction with a computer avatar. Neither the use of such technology nor guidelines regarding the interaction of humans and machines with regard to border checks are incorporated in the current legal system.
According to Article 7 Schengen Borders Code (SBC) [4], border guards shall, in the performance of their duties, fully respect human dignity, in particular in cases involving vulnerable persons. Additionally, Article 16 SBC stipulates that Member States shall ensure that the border guards are specialised and properly trained professionals, taking into account common core curricula for border guards [5]. These training curricula shall include specialised training for detecting and dealing with situations involving vulnerable persons, such as unaccompanied minors and victims of trafficking. If certain aspects of the border check are not being performed by border guards, but by an avatar, the principle of respecting the dignity of travellers is being challenged, as human dignity may be violated in multiple ways. In general, aside from the most obvious examples of a violation of human dignity such as torture [6], exposing people to inhuman treatment [5], slavery and bonded labour [7], there may also be cases where an interference with human dignity is less obvious and where a violation of human dignity may have numerous facets and dimensions, for example humiliation, degradation or ostracism against a person [8]. Furthermore, a person may not be "dehumanized", that refers to an act with which individuals or groups are stripped of their human characteristics or treated as less valued human beings [9]. Human dignity may also be violated by degradation, where the inherent value of a human being is deprecated [10].
These requirements very much reflect the concerns that arise when performing border checks: Both the behaviour of border guards as well as the measures performed during a border check have to fully respect human dignity. To this extent, the importance of decisions for the person as an individual, such as access or refusal, as well as the intensity of checks on privacy have to be considered. Consequently, with regard to the avatar interview, a variety of issues arise, which – on an abstract level – can be also transposed to the use of computational based intelligence systems in general.

C. Degradation of the traveller to an object

By having an interview with a computer avatar instead of a border guard, the traveller will be faced with a rather unusual environment: In fact, an interaction between humans and machines cannot be found in any other area of daily life currently. While there are certain approaches to facilitate the use of ICT-technology in certain areas, such as the consultation of a medical doctor via a webcam [11], there is still a human being actively involved in the process.
In order to fully understand the implication that arises from replacing human interaction with machine interaction, it is important to show the actual difference. Computer software usually follows a set of rules, specifying how the software should behave in certain situations. However, it is currently not possible to properly assess every detail in every situation. Therefore, computer software is not able to adapt to a situation in the same way a human being could. Non-typical situations therefore can be seen as a particular challenge for computational intelligence based systems, as providing rules for every possible situation appears to be impossible at this point in time, while the emotional needs of human beings should always be respected. This being said, various legal and ethical implications, particularly with human dignity, can arise, as the following examples show:

- If a person feels bad or starts crying, how could software adapt to this situation? Even if the avatar would be able to detect such behaviour, it would not be able to actually help the person by calming him or her down, as opposed to a human being (such as a border guard) who would have far more options to interact with the person.
- If a traveller is not able to properly reply to a question, e.g. because there is a non-typical situation which is not covered by the procedure which the software has to follow, people could feel helpless and/or uncomfortable

as opposed to interacting with a human being, who could adapt to the situation and provide guidance.

- Software might not be able to detect misunderstandings; if a traveller misunderstands a question and consequently gives a wrong reply, the software might assume that the person is lying rather than having just not understood the question correctly.
- As the avatar will also adjust its behaviour according to the behaviour of the traveller, wrong interpretations of the software could cause the avatar to react in a way which appears to be strange, frightening or inhuman to the traveller.

In addition, due to the technical nature of the avatar, a conversation would have to follow certain rules. In order to allow the software to properly process the answers, questions might have to be asked in a specific way in order to receive the answer in a specific format. The wording of those questions could appear to be strange to travellers, therefore reducing the social acceptance of such technologies.
This obviously poses difficult ethical challenges with regard to human dignity. The avatar interview should therefore seek to implement safeguards which ensure that situations as outlined above cannot occur.
It has to be noted though, that the ethical implications might change once the use of computational intelligence based systems is more common and people are used to interact with machines, as this could reduce inherent fears and uncertainties.

D. Avatar "behavior" and questions asked during the avatar interview

The questions raised during the avatar interview, from a legal point of view, have to be seen as data processing, as the answers of the traveller will be collected, recorded and further analysed as outlined in the following chapters. Following the principles stipulated in Article 8 of the Charter of Fundamental Rights of the European Union (CFREU), a statutory legal basis or consent of the traveller would be required in order to collect and process data [12]. The purpose of the ADDS system as outlined above is to shift the interview border guards would perform during a border-check to the pre-registration phase by using a virtual police avatar. This poses various legal and ethical concerns.
Firstly, on content-level [13], it has to be ensured that the questions would still serve their purpose – for instance, questions arising from the requirement to protect public health might not be feasible if asked several days before the actual border crossing. Asking unnecessary questions would violate the right to privacy [14].
Secondly, the overall format of the avatar interview should not violate the cultural or religious feelings of travellers. Therefore, it needs to be carefully assessed how border guards are trained to specifically respect cultural and religious feelings of travellers by adapting their behaviour accordingly. This could, for instance, cover questions such as the gender of the avatar (a female traveller should be interviewed by a female avatar and vice versa), a certain dress code, or certain habits, such as how to salute a person. Therefore, the avatar would have to be adapted for every interview not only based on the information provided by the traveller, but also based on his/her cultural background and religion. Adapting the avatar to every traveller individually would also help to ensure that the travellers does not feel to be treated like an object, but rather as an individual human being. In fact, it could be even seen as an advantage of a virtual avatar that it can change its appearance according to the needs of the traveller, as opposed to a human border guard.

III. DATA PROCESSING

A. Profiling

With regard to data processing, a peculiarity of computational intelligence based systems is that they rely on processing different kinds of data. As a matter of fact, this data also has to be collected, but the main impact on privacy arises from the processing aspect. From a legal point of view, this technique could be seen as profiling: 'Profiling' means *any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements* [15]. This most probably applies to the majority of computational intelligence based systems - with regard to the ADDS system developed in iBorderCtrl, the collection and processing of different forms of personal data (i.e. micro gestures and behavioural aspects) for the purpose of deception detection can be seen as profiling.
From a legal point of view, profiling poses a variety of risks: Due to the nature of profiling, the collection of different kinds of personal data is required. While the collection of personal data in itself is already subject to certain restrictions (e.g. requires a legal basis or consent of the data subject and compliance with the principles of processing personal data), the concentration of different categories of data of a person in the hands of one data controller may cause a severe intrusion into the privacy of a data subject [16].
Profiling, therefore, is subject to specific legislation. For a use-case such as proposed by iBorderCtrl, Directive 680/2016/EU would apply, as the scope of the Directive (art. 2) covers the processing of personal data by competent authorities for the purposes outlined in art. 1, which includes the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. According to recital 6 of the Schengen Border Code (Regulation 399/2016), border control should help to, among others, prevent any threat to the Member States' internal security, which would be within the subject-matter of Directive 680/2016/EU [17]. It has to be noted that in the current legal framework there is no legal basis for using an avatar interview such as the iBorderCtrl

ADDS system. However, a legal basis could be enacted based on the principles and rules outlined in Directive 680/2016/EU.
For data processing within the scope of Directive 680/2016/EU, the general principles relating to processing of personal data as outlined in article 4 have to be considered. These include that personal data has to be processed lawfully and fairly, collected for specified, explicit and legitimate purposes, and the processing has to adequate, relevant and not excessive in relation to the purposes for which they are processed [18]. Therefore, computational intelligence based systems have to be designed bearing in mind that only data which can be utilized for the desired purpose is being processed.
Apart from that, article 11 of Directive 680/2016/EU prohibits profiling in general, unless appropriate safeguards are applied. A particular risk that might arise within the iBorderCtrl ADDS is the different criteria that will be considered for assessing the individual risk score assigned to each traveller. As outlined in this section, it is important to ensure that these risk indicators do not discriminate against certain groups of persons without proper justification, in order to mitigate risks of stigmatisation and thus preserve traveller's human dignity and right to equal treatment. This is particularly important in the light of religious and cultural peculiarities as outlined above. As a matter of fact, article 11 (3) of Directive 680/2016/EU prohibits any profiling which would result in a discrimination against the data subject. This is also being reflected in recital 38, stating that profiling which results in discrimination against natural persons on the basis of personal data which are by their nature particularly sensitive in relation to fundamental rights and freedoms should be prohibited under the conditions laid down in Articles 21 and 52 of the CFREU [19].
As the increased risk that arises from profiling is inherited in the legal system, it also needs specific attention for developing computational based intelligence systems in general.

B. Automated decision making

Another specific aspect of computational intelligence based systems is the use of automated decision making processes by processing the data collected in the previous stage. This poses various legal and ethical challenges, in particular with the concept of equality and non-discrimination.
From a legal point of view, the Charta of fundamental Rights of the European Union (CFREU) deals with equality in chapter III, i.e. Art. 20 - 26. Of particular importance are Art. 20 ("Equality before the law") and Art. 21 (Non-discrimination) [20]. Similar to the CFREU, the European Convention on Human Rights (ECHR) prohibits discrimination in Art. 14 [21]. On top of this, constitutional and legal traditions of the Member States must be considered as well, as almost all EU/EEA Members States do have constitutional provisions concerning equality and/or non-discrimination.
As described above, the ADDS developed within iBorderCtrl obviously and quite heavily relies on information technology and automatization to make certain processes more effective. In fact, automatization is the fundamental basis of both conducting interactive interviews and assessing the risk stemming from a traveller. This may include automatization of decision making/supporting processes, which as soon as actual human beings may be affected by such decision, raise ethical questions *inter alia* with regard not only to human dignity, but also to the principle of non-discrimination. To this extent, the set of rules inherited in any computational intelligence based system must not violate against the principle of non-discrimination. The grounds outlined in article 21 CFREU (sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation) appear to be particularly relevant: As they are inherent properties of a person, they cannot be changed and offer a particularly high risk for discrimination [22]. Therefore, possible selectors for automated decision making should avoid focusing on these properties whenever possible.
The basis of legal considerations regarding automated decision making processes in the context of iBorderCtrl is Art. 11 Directive 680/2016/EU [23], which inherits the principles posed by fundamental rights as outlined above: It prohibits decisions bases solely on automated processing, unless authorised by Union or Member State law that provides appropriate safeguards.
From a legal point of view, it must be re-emphasised that Directive 680/2016/EU (as well as Regulation 679/2016/EU (GDPR)) mention "profiling" and "automated decision making" together. However, and despite both terms overlap to a great extent, they are two separate things: Profiling means broadly speaking "gathering information about an individual or group of individuals and analysing their characteristics or behaviour patterns in order to place them into a certain category or group, and/or to make predictions or assessments about *inter alia* ability to carry out a certain task or individual interests and/or preferences [24]. In contrast to this, automated decision making, refers to the ability to make decisions based on certain information, including personal information such as profiles without human interaction. The difference can be seen in the fact that automated decision making is the process of coming to a decision based on an already created profile. That means a collection of data is used to create a profile upon which then an automated decision can be made; can, however, also be taken by a human [25]. Both techniques can be seen as integral parts of computational intelligence based systems.
Hence it is to be decided, whether a system like the iBorderCtrl ADDS has to be seen as a system based on automated decision making. This would require that the automated decision produces adverse legal effects on the data subject, or otherwise significantly affects him or her [18].
Clearly this would be the case, if the decision as to whether a certain traveller will be admitted to the Schengen areas or not would be reached solely via automated means, without any human intervention and based on information previously gathered. However, the iBorderCtrl ADDS does not propose to automate the decision whether a traveller will be admitted to the Schengen area or not, but rather automates the process

to gather information from and regarding the traveller, leading to a risk score, which may then be taken into account by an actual border guard who will take the final admission or non-admission decision. Thus, as there is no legal decision on entry or refusal, from a legal point of view it seems questionable if a respective system would be regarded as automated decision making within the ambit of Art. 11 Directive 680/2016/EU.

On the other hand, and especially from an ethical point of view, one may argue that the decision taken by the system could be seen in the allocation of the risk score itself. This is because Art. 11 does not only include legal decisions, but also any other action which might have significant effect on the individual [26]. This includes any objective factors which make the data subject to feel negatively impacted [27]. The risk score could or almost certainly would to some extent pre-empt or anticipate the decision that will be taken by the border guard. This is because the border guard certainly will take the risk score into account when making the decision. If the risk assessment concludes that a certain traveller is a high-risk traveller it might be hard to imagine under what circumstances the border guard would overrule or differ from the automated risk assessment, because the data or parts thereof which led to a certain risk score were inaccurate or plainly false or because of flawed algorithms or software components. Therefore, it is fair to say that there is a certain risk that a border guard will plainly follow the assessment taken by the automatic risk score allocation, meaning that Art. 11 Directive 680/2016/EU and the included safeguards need to apply to minimise the risk of violations of fundamental rights. In that regard, recital 38 of the Directive mentions certain rights, e.g. that the data subject has to be informed about an automated decision making, as well as the right to obtain human intervention, in particular to express his or her point of view. Apart from that, recital 38 state that the data subject should have the right to obtain an explanation of the decision reached after such assessment or to challenge the decision. While the right to challenge an automated decision could be realised quite easily, explaining an automated decision might be rather challenging once computational intelligence based learning approaches such as artificial neural networks are used: Due to the independency of the system when computing a decision and the resulting "black box", it is not possible to accurately assess how exactly the system came to its decision, meaning that a data subject could not be provided with an explanation how the decision has been reached. This effect might also challenge the right to access as outlined in art. 14 of Directive 680/2016/EU, as it might remain unclear which categories of personal data have been actually considered and to which extent. One possible remedy in that regard could be to make at least parts of the algorithm transparent, or, if the algorithm is considered to be confidential, to inform the data subject about which categories of data have been (possibly) used. This solution could follow the overall approach applied by the Federal Court of Justice of Germany, which stated that an algorithm could be a trade secret, but that the data subject still had the right to be informed about which personal data is being used to compute a decision [28]. It has to be noted though, that this ruling did not consider computational intelligence based systems and the "black box" phenomenon, but rather algorithms in general.

However, this approach might be rather challenging in practice, as from a security agency's point of view, revealing any information on the functioning of an algorithm, including the categories of personal data which have been processed, might reveal confidential information about their procedures. In these cases, other measures have to be implemented, such as an ethics commission assessing the overall ethical implications caused by the use of such systems.

In any case, further safeguards could include a regular quality assurance to ensure a fair and lawful treatment of data subjects. This also includes regular testing of the algorithms involved to ensure that they are performing as intended and do not produce unsound results.

Additionally, the rights, and freedoms of the person, as defined in Recital 51 et seq., must be secured by appropriate technical and organizational measures such as applying pseudonymisation and anonymisation of personal data whenever possible.

General recommendations for a privacy-friendly implementation of profiling and automated decision-making can be also found in the draft guidelines issued by the art. 29 WP in the scope of regulation 679/2016/EU (GDPR) [29]. These guidelines should be also considered when developing computational intelligence based systems in general. Due to the fact that the GDPR and the Law Enforcement Directive have been enacted hand-in-hand and include rather similar provisions on profiling and automated decision-making, many of the good practice recommendations [30] could be also applied to uses-cases falling within the scope of the Directive, even though that the art. 29 WP guidelines focus on the GDPR as a legal basis.

C. The risk of false positives

One of these possible violations is the issue of "false positives": Results indicating that a certain condition is fulfilled, when in fact it is not. This could be caused by a variety of issues, such as flawed or equivocal rules for the risk calculation, misunderstandings or technical malfunctions.

1) Definition and classification of false positives & false negatives in the legal framework

A false positive in the scope of the ADDS means that, for instance, the system would indicate a hit on a person which, from a factual and legal point of view, would not be suspicious. A person would then be seen as a suspect and thus be harmed by negative consequences such as more intrusive measures (more thorough border checks) or even negative decisions such as a refusal. In consequence, a law-abiding person would not be treated as other law-abiding travellers, posing a discrimination against the person. While there is no law explicitly covering false positives and false negatives, legal and ethical issues can be seen in the light of fundamental

rights and the principle of non-discrimination as outlined e.g. in art. 20 CFREU [31].

On the contrary, computational intelligence based systems such as the ADDS could also pose the risk of "false negatives", in which a suspicious traveller would not be faced with appropriate checks due to a flawed risk assessment. As opposed to the aforementioned issue regarding false positives, this would objectively pose an unequal treatment as well, as the suspicious traveller would be treated differently as compared to other suspicious travellers. The impact on fundamental rights would be different in this scenario, though: In fact, the person affected by a false negative would not suffer from any negative consequences, meaning that this could not be seen as a discrimination of the affected person [32].

Last but not least, ethical concerns could arise on a broader scale, if the use of computational intelligence based systems such as ADDS would lead to less security within the Schengen Area, as security and physical integrity [33] are fundamental interests of every EU citizen as well.

2) Ethical implications of false positives

False positives might in addition lead to a number of ethical implications that have to be considered. As already explained above, the most obvious implication would be a discrimination against the traveller, who would not be treated as other law-abiding travellers, meaning that comparable scenarios are treated differently.

Apart from that, an affected person would suffer from the "burden of proof", meaning that he or she would have to convince a border guard that the information provided by the ADDS was not correct. In this regard, the options of the traveller are probably quite limited: If certain information is, for instance, derived from a database or produced on the basis of classified information, the traveller cannot be aware of the actual content. Therefore, they might encounter difficulties in explaining why they were affected by a false positive. However, the iBorderCtrl system would not be used to reason a refusal at the border – instead, a person would have to undergo a thorough check, which in these cases can be seen as the "burden of proof".

From an ethical point of view, one could consider that this might cause issues regarding human dignity; however, as border guards are obliged to respect human dignity under any circumstances, this should normally not cause any major concerns. It has to be noted, though, that every interaction with authorities on the grounds of a false-positive brings the traveller in a rather uncomfortable situation, i.e. as a thorough check consumes time and potentially stresses a traveller.

While there are no legal consequences affecting the travel yet, the false positive would cause a situation where the traveller would have to explain him-/herself. While a thorough check can neither be seen as a legal proceeding nor as a legal consequence affecting the travel as such, there might be certain overlapping aspects with the principle of the presumption of innocence: A traveller could feel stigmatised, as he or she would – from his/her point of view for no reason – be in this situation and would have to proof that the suspicions against him or her are wrong. However, as the false positive itself might be a reason for the border guards to conduct a thorough check, and as border guards – also without using the ADDS – would have to perform a thorough check if a person is suspicious from their point of view, this is not an issue directly stemming from the use of the ADDS system and therefore does not cause additional ethical issues.

Another aspect to be considered is the fact that a thorough check might require a deeper look into the background of the traveller, therefore causing a deeper intrusion into the traveller's privacy. As before, this could also happen if a traveller would be seen as suspicious by the border guards without any further input by technical systems. However, a well working IT-system could at least decrease the chance of false positives as compared to a system relying solely on humans.

IV. Conclusion

All in all, the use of computational intelligence based systems such as the ADDS component of the iBorderCtrl toolkit poses various legal, ethical and social challenges. While some of these implications are rather specific for certain use-cases, some general observations can be made:

In order to ensure a lawful development and implementation of such systems, a close collaboration of legal and technical experts is crucial. The various legal and ethical implications arising from a particular use-case have to be identified and safeguards have to be implemented wherever possible. As computational intelligence based systems could be used in a variety of use-cases, the legal and ethical implications which arise can be quite different. However, particular challenges most probably occur with regard to human dignity and the relation of humans and machines, as well as with the principle of non-discrimination. These challenges might range from issues in the very beginning (such as social acceptance of human-machine interaction) to issues in the data collection phase (human dignity and objectification of human beings) and in the data processing phase (false-positives, stigmatisation and burden of proof).

These rather general considerations are also reflected in the data protection framework: Both profiling (the automated processing of personal data to evaluate certain personal aspects relating to a natural person) and automated decision making (decisions made by a system purely relying on automated means) are subject to strict regulation, as outlined in Art. 22 of Regulation 679/2016/EU and Directive 680/2016/EU. At the same time, both can be seen as crucial aspects of use-cases relying on computational intelligence based systems. Consequently, computational intelligence based systems have to consider a variety of safeguards to ensure legal compliance, such as the right to human intervention.

In summary, computational intelligence based systems challenge the legal and ethical framework in various ways, making the lawful implementation of such systems rather

complicated. Therefore, upcoming technological and legal developments in this field have to be closely monitored.

ACKNOWLEDGEMENTS

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 700626. The authors would like to thank the iBorderCtrl consortium members for their feedback in understanding the technical backgrounds and therefore supporting the legal and ethical research of this technology.

REFERENCES

[1] Further information on the project can be found on the official website, www.iborderctrl.eu. The iBorderCtrl project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 700626.

[2] iBorderCtrl project flyer. [Online]. Available: http://iborderctrl.eu/sites/default/files/publications/iBorderCtrl%20flyer%20v6.pdf.

[3] G. Greenleaf. 2018. "The UN Should Adopt Data Protection Convention 108 as a Global Treaty: Submission on 'The Right to Privacy in the Digital Age' to the UN High Commissioner for Human Rights, to the Human Rights Council, and to the Special Rapporteur on the Right to Privacy", *SSRN eLibrary*. [Online]. Available: https://ssrn.com/abstract=3159846

[4] European Parliament and Council, Regulation (EU) 2016/399 of 9 March 2016 on a Union Code on the rules governing the movement of persons across borders (Schengen Borders Code). [Online]. Available: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016R0399.

[5] European Union, article 16 (1) of Regulation (EU) 2016/399.

[6] Council of Europe, Art. 3 of European Convention on Human Rights. [Online]. Available: http://www.echr.coe.int/Documents/Convention_ENG.pdf.

[7] Council of Europe, Art. 4 of European Convention on Human Rights. [Online]. Available: http://www.echr.coe.int/Documents/Convention_ENG.pdf.

[8] H. Jarass, „Charta der Grundrechte der Europäischen Union", in *Charta der Grundrechte der EU*, Jarass et al, 3rd edition 2016, Art. 4 Fn. 9.

[9] C. Calliess, "III. Charta der Grundrechte der Europäischen Union", in *EUV/AEUV*, Calliess/Ruffert et al, 5th edition 2016, Art. 4 Fn. 12.

[10] M. Borowsky, "Titel I Würde des Menschen (Artikel 1 - Artikel 5)", in *Charta der Grundrechte der Europäischen Union*, Meyer et al, 4th Edition, 2014, Art. 1 Fn. 39.

[11] Heise Online. Pilot project on video consultation of medial doctors. [Online]. Available: https://www.heise.de/newsticker/meldung/Video-Sprechstunde-Pilotprojekt-zur-Fernbehandlung-von-Patienten-3940570.html.

[12] Charter of Fundamental Rights of the European Union (2000/C 364/01). [Online]. Available; http://www.europarl.europa.eu/charter/pdf/text_en.pdf.

[13] The current procedural requirements will not be considered in this article.

[14] European Union, Art. 6 of Regulation 679/2016/EU and Art. 8 of Directive 680/2016/EU.

[15] European Union, Art. 4 (4) of Regulation 679/2016/EU and Art. 3 (4) of Directive 680/2016/EU.

[16] M. Martini, "Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)" in *Datenschutz-Grundverordnung*, Paal/Pauly et al, 1st edition 2017, Art. 22, Fn. 8.

[17] For the research project, regulation 679/2016/EU (General Data Protection Regulation) would apply.

[18] European Union, Art. 4 (1) of Directive 680/2016/EU.

[19] European Union, recital 38 of Directive 680/2016/EU.

[20] European Union, Charter of Fundamental Rights of the European Union (2000/C 364/01), [Online]. Available: http://www.europarl.europa.eu/charter/pdf/text_en.pdf.

[21] Council of Europe, European Convention on Human Rights. [Online].Available: http://www.echr.coe.int/Documents/Convention_ENG.pdf.

[22] *M. Rossi*, "III. Charta der Grundrechte der Europäischen Union", in *EUV/AEUV*, Calliess/Ruffert, 5th edition 2016, Art. 21 Fn. 1.

[23] Considering that the purpose of border checks is the prevention of crimes and threats to public security, Directive 680/2016/EU applies if the technology developed in iBorderCtrl is being used for border checks according to Art. 2 and Art. 1 (1) of the directive.

[24] Information Commissioner's Office, Feedback request – profiling and automated decision-making, 06.04.2017, P. 5 et seq. [Online]. Available: https://ico.org.uk/media/2013894/ico-feedback-request-profiling-and-automated-decision-making.pdf.

[25] A. Savin, Profiling and Automated Decision Making in the Present and New EU Data Protection Frameworks, P. 1. [Online]. Available: http://openarchive.cbs.dk/bitstream/handle/10398/8914/Savin.pdf?sequence=1.
[26] K. von Lewinski, "Datenschutz-Grundverordnung", in *BeckOK Datenschutzrecht*, Wolff/Brink et al, 22nd edition 01.11.2017, Art. 22, Fn. 37 et seq..
[27] K. von Lewinski, "Datenschutz-Grundverordnung", in *BeckOK Datenschutzrecht*, Wolff/Brink et al, 22nd edition 01.11.2017, Art. 22, Fn. 38.
[28] Federal Court of Justice of Germany, VI ZR 156/13, available at http://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=en&nr=66910&pos=0&anz=1.
[29] Art. 29 WP, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679. [Online]. Available: http://ec.europa.eu/newsroom/just/document.cfm?doc_id=47963.
[30] Art. 29 WP, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, p. 28 et seq.
[31] H. Jarass, „Charta der Grundrechte der Europäischen Union“, in *Charta der Grundrechte der EU*, Jarass et al, 3rd edition 2016,Art. 20 Fn. 7.
[32] H. Jarass, „Charta der Grundrechte der Europäischen Union“, in *Charta der Grundrechte der EU*, Jarass et al, 3rd edition 2016,, Art. 20 Fn. 11.
[33] European Union, Art. 3 of the Charter of Fundamental Rights of the European Union (2000/C 364/01). [Online]. Available: http://www.europarl.europa.eu/charter/pdf/text_en.pdf.