Digitizing risks and risking citizen rights

La Fors, Karolina

Publication date:
2016

Document Version
Publisher's PDF, also known as Version of record

Digitizing risks and risking citizen rights:

Prevention practices and their legal and socio-technical implications for the lives of children and migrants

"Proefschrift ter verkrijging van de graad van doctor aan Tilburg University op gezag van de rector magnificus, prof.dr. E.H.L. Aarts, in het openbaar te verdedigen ten overstaan van een door het college voor promoties aangewezen commissie in de aula van de Universiteit op woensdag 2 november 2016 om 16.00 uur door Karolina La Fors,
geboren op 8 september 1981 te Jászberény, Hongarije".

Promotor: Prof. mr. Corien Prins

Copromotor: Dr. Irma van der Ploeg

Overige leden van de promotiecommissie:

Prof. mr. Paul Vlaardingerbroek
Prof. dr. Simone van der Hof
Prof. dr. Louise Amoore
Dr. Colette Cuijpers
Dr. Veronica Smits

Table of contents

Foreword

Writing a PhD, for me, has been an experience incomparable to any other undertaking in my life. This has been something I could never imagine before, a period that accompanied and shaped a quite important and eventful part of my life.

Change has been a crucial rhythm that provided challenges but also kept this project together: moving from one city to another, becoming part of a new team, studying and learning new concepts, participating at highly inspiring PhD schools, starting a relationship, getting married, becoming a mother, moving with the family, changing patterns to finish the PhD project. These are only some of the changes that often seemed uneasy to accommodate a PhD trajectory to. Yet, in retrospect, a spot for finishing the PhD thesis remained somehow on the top of the priority list of my life. I have to acknowledge, though, that towards the end of the PhD trajectory, the thesis itself became a regularly unwelcome 'part of the family' that my family members also needed to 'live with'. For all their sacrifices, support, and most of all understanding, I am deeply grateful to Rob and Chris. I also have to express my deep gratitude for my parents, who cared enough to take the plane multiple times to be with Chris so that I could dedicate time to advance my writing.

Furthermore, I am completely certain that this project would not have come to such a positive end without Prof. Corien Prins. Corien, I am most deeply thankful for you. Our paths have crossed each other many, many times since the first time you interviewed me in Hungary via phone and accepted me for the Research Master in Law in Tilburg. When I needed a supervisor, you offered your help and guidance and graciously put up with the reality that, in the last period of the writing process, I could not devote my time fully to the PhD. Yet, each time I delivered pieces of work, you have shown confidence in me and have given advice that I needed in order to bring the articles, chapters and the whole research itself to a nice ending. The choice of writing the thesis on the basis of articles has of course also provided more work for you. Yet, it simultaneously offered me a unique track of profound writing experience. To conclude, I am most of all grateful for your optimism in people, including me. I am certain that seeing and approaching problems not as 'further trouble sources' but as challenges to overcome, as you have always shown it to me, is the most fruitful way to accomplish success. Thank you!

Moreover, I am also very grateful for my second supervisor Dr. Irma Van der Ploeg, who selected me for the DigIDeas project. Becoming part of the DigIDeas team meant becoming part of a quite interdisciplinary and international team. The dynamics of the team also impacted my way of thinking. I am highly thankful for opportunities that allowed me to gain inspiring insights into Science and Technology Studies—mostly actor-network-theory, surveillance studies, and philosophy of technology. All these insights enriched my legal analysis and reflections on how legislation and the rule of law works—and how it should work in practice. My way of thinking has been transformed by the way in which constructivist thoughts started to shape my research proposal and slowly also my perception of 'things' in life. I am not saying I started 'seeing like a survey', as John Law offers, or began to 'categorise onion-eaters per hamburger' as Susan Leigh Star points out. Yet, my perception of things has certainly raised questions about their 'origins' and framings, and ever since I became immersed in the STS literature. Thank you for your help in discovering such theoretical and methodological viewpoints.

My gratitude should also reach Jason Pridmore, who was our post-doc in the DigIDeas team. Through Jason, I was not only exposed to a great deal of surveillance studies concepts, but also to a large amount advice—'in a Canadian package'—about how to survive and keep going as a PhD candidate. Thank you

for your help in framing ideas and research proposals, for giving feedback and, in general, for being willing to listen when I faced unseen challenges. I also have to thank very much Govert Valkenburg, who offered me really great practical tips and feedback on how to write well for a pure STS audience. He has been there with encouragement, and even coaching when my empirical research stood before a first great test. Moreover, he has always been open to providing feedback if needed. Thank you Govert!

During the DigIDeas project, I also had the good fortune to participate at wonderful international and Dutch spring, summer, and winter schools—some organized by WTMC—and conferences, and I am very grateful for these opportunities. Getting to know other PhD candidates and scholars in the field filled the lonely process of writing with understanding and recognition, and provided a boost of new inspiration.

My thanks should also reach my former colleague, Vlad Niculescu-Dinca, with whom I discussed abstracts, difficulties of the writing process, and issues about how to balance personal life and scholarly work. I thank you very much for your feedback and thoughts throughout my research trajectory. Isolde Sprenkels was also a colleague during the DigIDeas project, and our relationship developed into a lasting friendship. Iso, let me also thank you very much for being there when I needed you and for being open to conversations about how to develop our research as well as how to accommodate our personal lives to it. I am very happy that we became such good friends.

At last but not least, the Tilburg Institute for Law, Technology and Society (TILT) has also provided a substantial support to finish this PhD thesis. Thank you to everyone at TILT who gave me feedback as well as intellectual, technical, and moral support in the finish. The publication of the bounded collection of articles also benefited from TILT's financial support.

Finishing this thesis provides a great feeling of accomplishment, and I wish every PhD researcher pursuing this great dream to experience this feeling in their future. Good luck and lots of success everyone!

Introduction

Context

This thesis focuses on the application of Identity Management (IDM) technologies[1] for the assessment of risks within the context of Dutch citizen-government relations. The technologies analysed range from the development of risk evaluation systems in order to profile citizens against a variety of risks and to the implementation of citizen identification technologies.

Digital identity management deals with the digitization, registration, processing and classification of personal information. These practices are going through a rapid evolution which involves a diversity of new information and communication (ICT) systems, tools and methods in citizen-government relations (e.g.: storage devices, databases, profiling methods, data-collection practices and data-mining techniques). IDM technologies are part of systems which serve to facilitate citizen-government relations. This is exemplified by the growing number of e-governmental services introduced to foster efficiency in bureaucratic interactions, as well as the introduction of several technology-intensive travel documents and entry-exit systems at borders. However, the processes for the management of these data are not always transparent, and they create an obscure net of digital and non-digital links in which personal data sets, or "digital personas" can emerge, grow, transform and become impossible to erase. IDM technologies are often connected to larger information management systems[2]. The processes in which these systems are involved enable and contribute to an advanced and dynamic differentiation (e.g.: registration of individual characteristics) amongst citizens in daily practice through an increased reliance on collecting personal data within contexts of healthcare, public safety, national or international security, immigration and other spheres of public-private interactions.

Although the growth in collecting personal data allows for more individualized treatment of citizens, this collection also fosters the use of this data for collective interests. Increasingly the collective interest of security has begun to supersede other concerns and has become a primary objective in the development of new IDM technologies. Given the prominence of security interests and the fast development of digitalized prevention methods in various public domains, this thesis aims to provide a critical analysis of the consequences of using such systems in the day-to-day lives of citizens in general, and two particularly vulnerable groups in particular: children and migrants. Each of these groups can be regarded being in a more vulnerable position than regular citizens. Therefore reflecting upon their position is useful in order to draw a better picture of the digitally mediated developments influencing democratic citizen rights and citizenship in general. These two groups seem, furthermore interesting for analysis because in their case forms of collective security interests, such as preventing child abuse and anti-social behaviour towards children, and identity fraud, illegal entry and related crimes concerning migrants appear difficult to balance with other interests, such as the protection of personal data, private life and non-discrimination. As the Dutch

[1] *Identity management technologies* serve to establish 'identities' (defined as personal data sets). This includes the identities of persons subject to the system, in this case children and migrants, as well as those professionals (e.g.: technicians, doctors, security agents, border guards, etc.) who interact with this system on a regular basis. These systems serve to both determine identification and allow for differing levels of access control in the process.

[2] Clark, R. 'Human identification in information systems: management challenges and public policy issues' (1994) 7(4) The Information Society, 6–37.

Data Protection Authority stressed in one of its recent reports, for instance, beyond the complexity of digital networks the scant knowledge of data protection of certain professionals dealing with youth care at Dutch municipalities can also contribute to detrimental implications on children's and families' lives[3].

Theoretical and empirical resources

The intensive deployment of IDM technologies and the exponential growth in the capacity of databases indicates a gradual shift in administrative identification procedures even across borders within the EU (see for instance, "STORK 2.0 Project" 2015[4]). Registering information is no longer a problem as is also evident in discussions with respect to Big or Open Data. A trend is there, where government agencies increasingly tend to trust and rely on IDM technologies that are able to process larger amounts of data, which is believed to deliver higher quality assessments, including preventative evaluations. A report by the Dutch Scientific Advisory Council of the Government describes this eagerness for more data as a shift from 'e-government' towards information-led, or 'I-government' practices[5]. Yet, how to sort data (and according to what parameters) brings a whole new dimension of selective practices regarding people's lives, and the legal boundaries of such data-sorting practices need continuous evaluation. The necessity of such evaluation has also been underlined by a recent comparative legal analysis on the use of Big Data by the Dutch Scientific Advisory Council of the (Dutch) Government[6].

The new European data protection regime will give clear new requirements to the sorting out of data. The enforcement of such principles as 'privacy by design' and 'privacy by default' and new rules prescribing 'data protection impact assessment,' 'data breach notification,' 'data portability' or the new 'right to be forgotten' provide a great addition of regulative tools in order to prevent the misuse and harmful effects of digital technologies on citizens' lives. The practical, daily enforcement of these principles and legal prescriptions presents quite some challenges, however. Scholars have already raised criticisms, even before the introduction of the new European General Data Protection Regulation. For instance, Van Dijk, Gellert and Rommetveit argue that the form in which data protection impact assessments can be mandatorily issued by the data controller authorities raises concerns because *'merging risks and rights in the proposed fashion could change their meanings into something hardly predictable.'*[7] This is especially troublesome within the context of risk assessment practices on children and migrants, because of the ambiguity of what a risk can constitute in itself. Given the controversial ways in which digitalized correlations are designed to produce a certain risk profile on child or a migrant, to predict what rights of these persons could be jeopardized by the very design and implementation of such risk forecasting technologies raises further controversies and unfortunately do not strengthen the legal position of these groups.

---

[3] 'Gemeenten onzorgvuldig met privégegevens burgers' *NOS.nl* (Den Haag 19, April 2016). Retrieved on June 6th, 2016 from <http://nos.nl/artikel/2100176-gemeenten-onzorgvuldig-met-privegegevens-burgers.html>

[4] STORK 2.0., EU project of the 7th EU Framework Programme, Project web-site consulted on 22nd May 2014 from <https://www.eid-stork2.eu/>

[5] Prins, C., Broeders, D., Griffioen, H., Keizer, A.-G. & Keymolen, E. 'iGovernment Synthesis' Wetenschappelijke Raad voor Regeringsbeleid, Den Haag (WRR, 2011)

[6] Van Der Sloot, B. & Van Schendel, S. 'International and comparative legal study on Big Data' Wetenschappelijke Raad voor Regeringsbelied, Den Haag (WRR, 2016)

[7] Van Dijk, N., Gellert, R., & Rommetveit, K. 'A Risk to a Right? Beyond Data Protection Risk Assessments'. (2016) 32(2) Computer Law & Security Review, 31–50.

Other rights introduced by the new data protection regulation could however be helpful to strengthen their position when they are exposed to scrutiny by such preventative systems. The new 'right to be forgotten' could become a good example for this. Yet, this right also raised questions especially in terms of how to invoke such a right in practice and what legal and technological settings would serve as best pre-conditions for such a right. For instance, Mayer-Schonberger in his encompassing and thought-provoking analysis sees the practical feasibility of the right to be forgotten by means of furnishing personal data with 'expiration dates'[8]. Bartolini and Siry outline a view of the practical enforcement of a right to be forgotten by exploring notions of consent withdrawal[9]. In general, Koops remains sceptical about the implementation of this right in practice. Amongst other things he points out that, on the one hand, when deciding who to turn to with a request for data erasure *'much will depend on the concrete distribution of responsibilities between provider and users defined in the terms and conditions.'* On the other hand, he also stresses that the *"multiplying character of Internet data"* will significantly complicate the erasure of data[10]. While bearing in mind these criticisms, the implementation of such a right in certain risk profiling cases of children, for instance, could be a very helpful legal remedy in getting rid of the potentially stigmatizing effects of a long-lasting risk profile. The security related to how such risk profile data should be stored also remains a crucial issue for this thesis.

Therefore, the potential of the new 'data breach notification' principle will also be useful to assess. Notwithstanding data protection De Hert and Papakonstantinou appreciate the principle of 'data breach notification' introduced by the new data protection regulation, they remain sceptical as to how such notifications shall be best effectuated in practice[11]. Still a major benefit of this principle is that data protection authorities will earn unprecedented powers to make companies improve the personal data security and privacy of their clients by rendering this principle an additional obligation for data controllers. Yet, the effectiveness of these powers will still have to be proved in practice. Bisogni studies the effectiveness of data breach notification laws in general, and based on his model he concludes that the *"implementation of more severe DBNL has higher impacts on decreasing the number of notified breaches, but context changes and actors behaviour drive this impact to lose its significance, in absence of any countermeasure such as ad hoc law amendments or revision."*[12]

In opposition to the earlier, the new prescriptions related to profiling in the GDPR will be highly beneficial, for instance to evaluate the preventative risk assessment practices of Dutch authorities on children. The prescription related to profiling (Art. 20) is a widely applauded achievement of the GDPR. The new regulation specifies that any measure based uniquely on automated data processing that has legal effects on 'natural persons' would count as 'profiling.' Yet, a set of scholars highlight different aspects of non-transparency around these practices. Koops points out, for instance, that putting this new principle into practice will create significant challenges as a consequence of "*increasingly automated operations on data—think of cloud computing and profiling—*

[8] Mayer-Schonberger, V. *Delete: the Virtue of Forgetting in the Digital Age.* Princeton (US), Woodstock(UK), (Princeton University Press 2009)

[9] Bartolini, C., & Siry, L. 'The right to be forgotten in the light of the consent of the data subject' (2016) 32(2) Computer Law & Security Review, 218–237.

[10] Koops, B. 'Forgetting footprints, shunning shadows. A critical analysis of the "right to be forgotten" in big data practice' (2011) 3(8) Scripted, 229-256. Retrieved on March 12th 2013 from <http://script-ed.org/wp-content/uploads/2011/12/koops.pdf>

[11] De Hert, P., & Papakonstantinou, V. 'The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals' (2012) 28(2) Computer Law & Security Review, 130–142.

[12] Bisogni, F. Evaluating Data Breach Notification Laws - What Do the Numbers Tell Us? (2013) In TPRC 41: The 41st Research Conference on Communication, Information and Internet Policy (pp. 1–21). Retrieved on February 22nd 2014 from <http://ssrn.com/abstract=2236144>

that data controllers themselves do not fully understand or know the details of. How can one effectively exercise the right to being informed, the right to access, to right to correction[…]?"[13]. Furthermore, Ferraris, Bosco and D'Angelo make the criticism that even this regulative novelty with respect to profiling could not provide effective remedy with respect to the negative implications of profiling on fundamental rights and democratic principles, such as certain forms of liberty, because profiling processes do not routinely *"allow the citizens to challenge the reasoning behind the process"*[14]. In addition to that, Moerel and Prins criticize the position of companies who through the massive use of Big Data analytics, *"without knowing the reasons behind a systematically identified correlation, will treat the chances presented by these correlations as facts"* to act upon or deal with[15]. These insights are particularly useful for the risk assessments practices on children and migrants, because such instances of non-transparency behind risk profiling decisions can be especially harmful regarding these groups.

Certain Dutch authorities when carrying out preventative profiling on children and migrants fall within the domains of criminal justice and law enforcement, and therefore their risk assessment practices would be considered legitimate. Given these practices for the analysis in this thesis I will also rely on certain prescriptions of the new Police and Criminal Justice Data Protection Directive. Concerning this new directive De Hert and Papakonstantinou appreciate its 'data-centric approach' instead of a 'data-user centric approach' to data protection, because during law enforcement data processing the purpose of processing is leading much more than the focus on the user or controller of data. This is significantly different compared to regular data processing. For instance, criminal justice authorities argue that they thrive on 'hearsay' and need to use and retain data for purposes earlier unknown, including profiling. Furthermore, they also stress that suspected criminals should not be informed of being in a police database, neither should they get access to it[16]. The effect of this new Directive on fundamental rights still has to be tested. Until then, the perceptions of scholars in surveillance studies and Science and Technology Studies concerning the controversies around digital technology are useful to inform data protection and human rights centred analysis in this thesis and draw more informed conclusions. In the following paragraphs I have gathered together a handful of useful concepts from surveillance studies and STS to show this.

The architecture of risk profiling systems, especially due to the increasingly obscure network of digital channels (especially in the world of Big Data) evokes a 'panoptic-like effect' as these can both be seen to construct and foster an impression and experience of constantly being under surveillance[17]. The continuous and complex observations that these systems carry out, reveal the characteristics of what David Lyon calls the "surveillance society," in which surveillance has become part of our everyday life[18]. It is surveillance based on an "algorithmic attentiveness"[19], one

---

[13] Koops, B. 'The trouble with European data protection law' (2014) 4(4) International Data Privacy Law, 250–261.

[14] Ferraris, V., Bosco, F. & D'Angelo, E. 'The impact of profiling on fundamental rights.' Working Paper 3 of the 'Protecting citizens' rights, fighting illict profiling' project. (2013) Retrieved on February 14th 2015 from <http://www.unicri.it/special_topics/citizen_profiling/PROFILINGproject_WS1_Fundamental_1110.pdf>

[15] Moerel, L., & Prins, C. *Privacy voor de Homo Digitalis: Proeve van een nieuw toetsingskader voor gegevensbescherming in het licht van big data en Internet of Things* In Homo Digitalis, Den Haag (Nederlandse Juristen Vereniging, 2016)

[16] De Hert, P., & Papakonstantinu, V. (2012). 'The Police and Criminal Justice Directive Comments and Analysis' (2012) 22(6) Computer and Law Magazine, 1-5. Retrieved on January 12th 2013 from <http://www.vub.ac.be/LSTS/pub/Dehert/411.pdf>

[17] Foucault, M. (translated by Alain Sheridan). *Discipline and Punish: The Birth of the Prison.* (New York: Vintage 1977). First published in French as Surveiller et punir, (Gallimard, Paris, 1975)

[18] Lyon, D. (2001). *Surveillance society. Monitoring everyday life.* Buckingham(UK), Philadelphia(US), Open University Press

[19] Amoore, L. 'Algorithmic war: everyday geographies of the war on terror' (2009) 41(1) Antipode: Journal of

that has certain features. First, it has an overall capacity to feed personal information into algorithms that make certain data significant in relation to 'normal' and 'abnormal' or risky characteristics. Secondly, the ability to flag these data as 'abnormal' or 'risky' bears potentially serious consequences for the persons under scrutiny. Thirdly, these systems provide a relatively permanent and continual form of data capture. This facilitates the detailed and complex surveillance of citizens in which certain information gains importance for governmental agencies. This "algorithmic attentiveness" is also an evident technique within Dutch policy areas of healthcare, public safety, border control and immigration.

This attentiveness, for instance during risk profiling can also be regarded as an aspect of security[20] that is apparent in youth healthcare[21] and social work practices. The way certain problems are defined within these fields resonates equally with the evolving perceptions about who to include and exclude. Child abuse cases are most illustrative of such problems, especially since there seems to be no consensus about what constitutes 'child abuse' in itself. Ian Hacking refers to perceptions about child abusers and child abuse as follows: *"Anyone who feels differently is already something of a monster. We are so sure of these moral truths that we seldom pause to wonder what child abuse is."*[22]. Such questions raise further questions about what certain public safety or security problems are, how are they framed, to what legal rules and principles can they be linked to and what legal remedies provide appropriate assistance to implement and use digital systems that are aimed at preventing such problems.

In the specific case of youth healthcare practice, for instance, as Van de Luitgaarden[23] suggest that the framing of identities already happens amongst professionals, children and parents on a case-by-case basis through interactions. Yet, such interactions are increasingly enhanced by the new information systems and IDM technologies that youth care professionals work with. When such a technology-enabled practice is carried out with a preventive stance it may "harm a good diagnosis"[24], for example uncertainties about a risk in relation to the child may reinforce unnecessary precautions and could even have harmful effects on the child. The extent to which such judgments may occur and what legal and socio-technical implications of preventative practices are apparent on children's families' lives and on the work of professionals constitute core part of the analysis in this thesis.

A set of such implications can be described as unfair modes of inclusion and exclusion. Because IDM technologies for risk assessment in their complex relationships to authorities, laws, policies, professionals, children and migrants are 'more than neutral'[25] through their use they enact and reinforce practices of inclusion and exclusion. These technologies both fulfil political goals in offering more efficient and smoother ways for the selection and 'management' of people, and they also transform citizen-government relations through their operation. For instance, IDM technologies often draw new – or accentuate already existing – differences between citizens,

---

Radical Geography, 49–69.

[20] Boyle, P., & Haggerty, K. 'Spectacular security: Mega-Events and the Security Complex' (2009) 3 International Political Sociology, 257–274.

[21] Horstman, K. Inaugurial speach: Dikke kinderen, uitgebluste werknemers en vreemde virussen. Filosofie van de publieke gezondheidszorg in de 21e eeuw. (2010, Maastricht University), Maastricht

[22] Hacking, I. 'The Making and Molding of Child Abuse' (1991) 17(2) Critical Inquiry, 253–288.

[23] Van de Luitgaarden, G. *Knowledge and knowing in child protection practice.* PhD thesis, (2011, University of Salford), Salford (UK)

[24] Monasso, T. 'Electronic Exchange of Signals on Youth at Risk: A value perspective' in Van der Hof, S. & Groothuis, M. (Eds.) *Innovating Government* (41–57). Den Haag (2011 Asser Press)

[25] Feenberg, A. *Critical Theory of Technology.* Oxford (UK) (1991, Oxford University Press)

differences that have the potential to be highly discriminatory[26]. Bowker and Star explained that technology-mediated selective processes enact certain types of discriminations by the very fact how categories have been designed and drawn together for selection processes. Such discriminations are also exemplified through the preventative use of IDM technologies. This thesis notes that methods of and for sorting citizens have been increasingly 'delegated'[27] to automated systems and practices performed by IDM technologies. The delegation of sorting methods to IDM technologies is seen to represent a 'best solution' for a diversity of complex socio-political, cultural and economic problems related to citizens. These 'solutions' are predicated on such judgments that mutually assign certain selection criteria of citizens to IDM technologies, and information management systems to which these technologies are often connected. In practice, the use of IDM technologies reinforces these criteria, and thereupon also automates and speeds up judgments.

Government agencies use personal data as an essential resource to speed up judgments and pinpoint the need for forms of intervention, or what Amoore describes as "actionable intelligence"[28]. This "actionable intelligence" can be regarded as a useful concept for the analysis in this thesis, as such intelligence is a driving force in identifying those citizens - children or migrants - who are considered 'at risk' and 'as a risk.' While this "actionable intelligence" is constructed within technology-intensive relationships, it is relevant to consider that both technology and the relationships in which it is embedded can constrain behaviour, in fact as Akrich refers to technology: "the composition of a technical object constrains actants in the way they relate both to the object and to one another"[29]. Some of the undesired effects of these constraints become apparent in practice, when for instance data sets between databases are processed. The transfer of biometric data among databases shows such effects as for instance falsely accused persons based on a fingerprint match. 12 years after the infamous case of Brandon Mayfield questions still arise as to how his fingerprint could have been mistaken by fingerprints of a terrorist[30]. Although the "informatization of the body" through these biometric technologies has already provoked much political, ethical, societal debate[31]. The fact that the combination of these various biometric technologies still form the basis of 'multimodal' screening processes and that these 'multimodal' systems are being increasingly taken up by both public and private agencies suggests that controversies may only intensify (especially in the era of Big Data). The broad scale use of biometric features as identification and identity verification material - also used within the context of immigration and border control practices on migrants - are perhaps best exemplified by digital identification cards [32]. In this case, a great deal of trust is "inscribed" into these cards [33] since they

---

[26] Bowker, G. C., & Leigh Star, S. *Sorting things out: Classification and its consequences*. Cambridge (US) London (UK): (1999, MIT Press)

[27] Latour, B. 'Give Me a Laboratory and I will Raise the World' in M. Knorr-Certina, K. D. & Mulkay (Eds.) *Science observed: perspectives on the social study of science* (pp. 141–171). London, Beverly Hills, New Delhi (1983, SAGE publications)

[28] Amoore, L. 'Lines of sight: on visualization of unknown futures' (2009) 13(1) Citizenship Studies, 17–30

[29] Akrich, M. (1992). 'The De-scription of Technical Objects' in W. Bijker & J. Law (Eds.) *Shaping Technology / Building Society: Studies in Sociotechnical Change* (pp. 205–224). Cambridge, MA (MIT Press, 1992)

[30] Office of the Inspector General. 'A review of the FBI's handling of the Brandon Mayfield Case', Washington D.C., (US Department of Justice, 2006) Retrieved on 16th March 2014 from <https://oig.justice.gov/special/s0601/final.pdf>

[31] Van der Ploeg, I. 'The Politics of Biometric Identification Normative aspects of automated social categorization.' *Biometric Technology & Ethics*, BITE Policy papers No. 2., Rotterdam (Rotterdam Institute for Healthcare Management & Policy, 2005)

[32] Lyon, D. *Identifying Citizens: ID cards as Surveillance.* Cambridge (UK); Malden (US) (Polity Press, 2009).

[33] Latour, B. 'Technology is society made durable' in J. Law (Ed.), *A Sociology of Monsters; Essays on Power, Technology and Domination* (pp. 103–131). London, New York (Routledge, 1991)

contain valuable personal data for verification and are difficult to counterfeit[34]. Yet when these artefacts are evaluated closely, there is a significant weakness in relation to their establishment and operation. A biometric identification card requires 'breeder documents' – such as a birth certificate – in order to authenticate and verify the applicant's data before it is issued. As such, the entitlement of a particular person to receive one of these 'technologically enhanced' cards relies on these less verifiable, less secure source documents[35]. Identification cards and passports[36] as technologically enhanced tools are fundamentally undermined by being based on these weak stemming documents. As the analysis will demonstrate in the chapters of this thesis the latter scientific thought has been found very useful to assess the empirical material with respect to migrants and by this to inform legal analysis and answer parts of the research question.

The above selected legal and surveillance studies and STS-based conceptions are far from constituting an exhaustive list. In this introduction they only served to pinpoint a couple of crucial directions where the analysis of this thesis should and will take the reader during the assessment of the broader legal and socio-technical implications of risk assessment technologies on children's and migrants' lives. Examples of false accusations[37] have already shown that digitalized prevention performed in practices of youth care, law enforcement and border control can present huge challenges for those exposed to these practices. Consequently, these challenges will put the current and the newly drafted data protection framework as well as the existing human rights tools and to some extent our democratic principles to the test. Therefore, it is essential to analyse how preventative measures are enforced through the use of IDM technologies in relation to such groups as children and migrants that can be viewed as being at the 'peripheries of (democratic) citizenship'. To scrutinize the legal and societal implications of the use of such technologies on such fundamental rights as privacy, non-discrimination and, for instance, the best interests of the child or such principles as liberty and equality when enacted in practice are key for a democratic society.

IDM systems in two domains

"Near the beginning of Les Misérables, the main character, Jean Valjean, is released from prison and offered temporary shelter by the Bishop of Digne. However, Valjean's desperate situation, one that includes lack of food and resources, motivates him to steal silver from the Bishop's home. When the local authorities catch Valjean, something unexpected happens. The Bishop goes above and beyond what most human beings would do. He covers for Valjean and does not allow him to be taken to jail [by Javert, the desperate police officer who wants to catch him]. Valjean is deeply moved by the Bishop's action on his behalf. He does not take this moment for granted and 'pays it forward' throughout his life, aligning his own choices with

[34] Dodge, M., & Kitchin, R. *Codes of Life: Identification Codes and the Machine-Readable World*; London (CASA, 2004) 1-47. Retrieved on November 11th 2011 from <http://www.casa.ucl.ac.uk/working_papers/paper82.pdf>

[35] Salter, M. *The rights of passage: passports in international relations.* Colorado (US), London (UK): (Lynne Rienner Publisher, 2003)

[36] Torpey, J. *The invention of the passport: Surveillance and Citizenship.* Cambridge, New York (Cambridge University Press, 1999)

[37] Munro, E. *The Munro review of child protection Part one: A system analysis.* London (Department for Education of the United Kingdom, 2010). Retrieved on 11th February 2011 from <http://www.education.gov.uk/>

what was modelled for him in that fortunate moment […] The Bishop comes to Valjean's rescue based on what seems fair and humane to him."[38]

Jean Valjean, the classic character created by Victor Hugo, can be regarded as a perfect example of an 'outcast' citizen, who wants to return to society - a man with a difficult childhood and a 'suspected' newcomer to a city after spending time in jail. His past as a convict becomes common knowledge – even without digital technologies - to those who meet him. The continuous projection of his negative past on him, first of all by the police officer Javert, becomes almost a 'self-fulfilling prophecy'; until he meets someone who approaches him differently and starts to look for the good in him by trusting him as much as one human can trust another. At the same time, the relationship between Valjean and Javert, who continuously follows Valjean so that he can pre-emptively put him in jail because of his 'risky' past, to differing degrees depicts characteristics that can be thought similar to the relationship between children and the current Dutch youth care, youth healthcare and criminal justice authorities, and to the relationship between migrants and Dutch border control, criminal justice and immigration authorities. For it is claimed that the kind of trust that can be granted by someone to a child or a migrant becomes increasingly embedded in and predicated upon the relationships to digital technologies. The digitally mediated relations between children and government authorities and migrants and government authorities provide reflections on the evolution of digitalized citizen-government relations in general.

This thesis will show that the risk-oriented perspective that professionals are required to take while digitally evaluating a child or a migrant against previously defined risks is something that complicates the relationship between government officials and children, and government officials and migrants. Furthermore the fact the youth care related data are not always properly protected amongst others due to the lack of data protection knowledge of professionals only adds to the complexities[39]. These digitalized practices, although installed to serve the noble purpose of preventing these very problems from happening, can also be regarded as contributing to undermine the trust in migrants, children and their families. Moreover, how these digitalized practices both from the perspective of migrants and children perform instances of inclusion and exclusion within these groups fairly needs analysis.

Against such a background, the legal analysis will explore whether the fine line between preventative digital profiling and unintended, yet digitally mediated prejudice can still be separated out in citizen-government relations by focusing on these two groups. The thesis will assess from a legal perspective the interplay between the good intentions behind preventative practices, the often risk-oriented glass of professional authorities and both the digitally designed (e.g.: risk categories to prevent risks) and the in-practice emerging implications of technology use and how each of these components influence the life chances of such 'in-between' citizens as children and migrants and indirectly society as a whole.

---

[38] Retrieved on January 12, 2016 from http://www.centertheatregroup.org/uploadedfiles/plays_and_tickets/productions/2011/les_miserables/files/lesmis_edres.pdf See also the relevant chapter in Hugo, V. *Les Miserables*, Volume I, Book 2nd, Chapter XII – The Bishop works - London(UK), New York(US), Victoria(AUS) (Penguin Group, 1980)

[39] Hartholt, S. 'Privacy jongeren jeugdhulp slecht beschermd' *Binnenlandsbestuur* (Den Haag, 25 April 2016) Retrieved on May 31th 2016 from <http://www.binnenlandsbestuur.nl/sociaal/nieuws/privacy-jongeren-jeugdhulp-slecht-beschermd.9532480.lynkx>

Why children and migrants?

Both children and migrants are groups affected by the changes in perceiving security through a broadened taxonomy of risks and the embracing of new technologies for risk evaluation. Both groups are seen as being at the periphery of citizenship, considered vulnerable due to their lack of certain legal entitlements, and this also illustrates the multifaceted concept of 'security' as both groups are increasingly considered being 'at risk' or 'as a risk.' The connection between being 'at risk' and being perceived 'as a risk' constitutes a conceptual symmetry between these groups in this thesis. The analysis will thus shed light on how IDM technologies and security systems affect the relationship of children to government authorities and migrants to government authorities and how these relationships mutually shape these technologies.

First, the Dutch policy domains of youth healthcare, youth care and also in part law enforcement will be analyzed as they increasingly shape and are shaped by public safety. The case of a 3 year old Dutch girl[40] generated particular media and policy interest in concerns about children being 'at risk.' In this case, youth healthcare workers and other agencies involved with the girl were blamed for not having adequately shared data on the child, and if they had done so the child's death could have been prevented. With this case marking the tip of an iceberg, as digitalization had already been initiated, the problem of child abuse was translated into a problem of information sharing. For this technology became seen as an important facilitator to prevent further problems. In order to address this, three main technological systems were proposed and developed. One serves to register children's healthcare data, involving in part the categorization and signaling of risks. It is called the Digital Youth Healthcare Registry (hereinafter, DYHR). The second is a specific risk signaling and forecasting system for the public safety of children (and citizens), called the Reference Index High Risk Youth (hereinafter, RI). In the RI, risk signals are sent from other, linked technological registration systems that youth care institutions work with. Between the DYHR and the RI there is an overlap in function. The DYHR's section of risk registration is connected to the RI and, upon registration, risk signals are automatically sent from the DYHR to the RI. The third system is called ProKid 12- SI (hereinafter, ProKid), which is a preventative risk signaling system used by the police in order to signal problems concerning children, their homes and their families. Through the use of the DYHR, the RI and ProKid, risks are projected for all children nationwide, and these children become understood in light of these risks through the interrelated processes of prevention. Therefore, the extent to which certain automatically enabled processes contribute to the construction of risks, as well as how these risks are indicative of specific problems within the mechanism of prevention, need to be analyzed. The way certain problems are indicated is significant for children's lives, since these problems become referential to the type of intervention which will be assigned to them.

Secondly, Dutch border control and immigration contexts and to some extent the law enforcement context will be analysed. The status of a migrant becomes established through and after an identification procedure in these contexts. There are various categories of migrants which are established, including asylum seekers and illegal and legal immigrants, and in this thesis I also include travellers under the term migrants. After the establishment of their status, asylum seekers are often seen as being 'at risk,' illegal migrants 'as a risk' and legal migrants and travellers to a

[40] Edemariam, A. 'After Savanna', *The Guardian* (London, 1 December 2008) Retrieved on 12th May 2015 from <https://www.theguardian.com/society/2008/dec/01/child-protection-baby-p-netherlands>

much lesser extent as either of these. Within the contexts of border control, immigration and law enforcement, instances of identity fraud and illegal entry among migrants and identity fraud among suspected and convicted criminals contributed to the introduction of high-tech biometric identification systems and risk profiling systems at national level. Two biometric identification systems, the Immigration and Naturalization Service (INS) console within immigration and border control practices, and the PROGIS console within law enforcement practices, exemplify this and are in the focus of this thesis. In part also influenced by current political discourse within the EU concerning such goals as minimizing risks of terrorism, potential criminal activities and social liabilities that illegal migrants might pose for EU citizens, one risk profiling system, called the Advanced Passenger Information system (hereinafter, API) used at Schiphol Airport to screen travellers by border control authorities also constitutes the focus of analysis in this thesis. In order to sort out potential perpetrators by using these systems, in practice all migrants are considered suspicious and screened against security threats ('as a risk'), including identity fraud, illegal entry, international crime and even potential terrorism. Yet, many of them can be particularly vulnerable since they have often been forced to leave their homeland, have very little financial resources, and have no official status ('at risk'). The threats and problems migrants are associated with both as potential perpetrators and as victims are always part of processes that mutually implicate each other. When migrants become perceived in light of these risks within digitalized prevention processes, this can also result in false accusations, with the detrimental implications of such digitalized decisions on their lives.

The implications on both children's and migrants' lives require empirical and legal analysis for two reasons. First, because through these practices children and migrants become, in the administrative sense of the word, citizens and digitally mediated decisions of inclusion or exclusion related to them are carried out. Secondly, the implications of the practical use of digital risk assessment technologies on this 'becoming citizens' allow for unnecessary and unfair exclusions of citizens. Therefore the empirical insights can help the legal assessment from both data protection and human rights perspectives and also in seeking proper legal remedy and other forms of compensation for the victims.

Given these contexts, one of the objectives of this research is therefore to enrich the legal analysis by exploring the implications of use of such technology on citizens' lives through case studies focusing on the peripheries of citizenship. As also highlighted above, children and migrants are two most vulnerable groups at the peripheries of citizenship, and they are considered most illustrative of the multifaceted concept of 'security' for this thesis by being increasingly considered both 'at risk' and 'as a risk.' While government owned IDM technologies become operational in the name of 'bureaucratic' efficiency and public security and national defence, their influence on individual freedoms and security – specifically those of these most vulnerable groups – pose acute concerns. Such concerns can be the discriminative treatment of persons through identification procedures that violate their religious, cultural or other rights. While the use of these systems depicts a drive to further stimulate the standardization of personal identification and risk assessment techniques, it also depicts a drive to make the diversity of citizens increasingly and individually identifiable, distinguishable but also comparable. This as we will see leads to a variety of controversies and ultimately to the fallacy that these systems can prevent risks. What often lacks in public discourse is that these systems also bring new risks. Although migrants and children can be regarded as being at the periphery in light of the risks that youth care policy goals attempt to prevent, and in the case of migrants in light of the risks prioritized on the agendas of national and international politics, the aspects forming Dutch youth care policy and immigration policy,

international crime prevention at national level and prevention goals related to immigration policy, international crime and terrorism at international level do not form the prime focus of this thesis.

Problem description

The increasing reliance upon the preventative use of identity management systems within citizen-government relations and more specifically within the contexts of youth care, youth healthcare, criminal justice, immigration and border management are indicative of how security has become a crucial lens through which citizens in general and children and migrants in particular are evaluated and understood. Digitalization within these contexts has undoubtedly brought advantages, for instance, in terms of efficiency, or in the context of travellers the facilitation of their movement. Yet, the unintended consequences the design and daily use of these systems can bring for the lives of children and migrants from the perspective of the EU's new data protection regime, children's rights prescriptions and human rights principles have not yet been analysed and reflected upon. Notwithstanding this, children and migrants are more vulnerable to the detrimental implications stemming from the production of digital risk profiles than regular citizens. Compared to adults, these groups often lack legal entitlements, and awareness or knowledge of digital identity management and risk assessment practices. Assessing the position of children and migrants as vulnerable groups is useful to reflect upon the use of IDM systems and the legal and societal position of citizens in relation to government authorities in The Netherlands in general. Therefore, this thesis sets out to conduct empirically informed legal analysis, while bearing in mind the following main research question:

What are the implications of the design and use of preventative IDM systems for the legal and societal position of citizens within different contexts of citizen-government relations in The Netherlands; and what is the potential of the EU data protection as well as the ECHR fundamental rights regime to prevent and remedy the potential risks of such system-use for the lives of citizens?

There are several sub-questions which follow from this:

- *How does a digitalized risk profile emerge in practice regarding a child and how does this influence the child's legal and societal position as well as become a risk for children's lives?*
- *What is the potential of the EU data protection regime and the children rights' framework of the ECHR in mitigating the risks of the digitalized prevention practices on children's lives?*
- *How are migrants perceived by digital monitoring practices, and what are the implications of these practices on their status: are they themselves at risk, non-risk or do they pose a risk?*
- *What is the potential of the EU data protection regime and the human rights' framework of the ECHR in mitigating risks that digitalized prevention practices regarding migrants can bring about?*
- *To what extent can commonalities between the digitalized risk assessment practices regarding children and migrants be helpful in mitigating their vulnerable position by means of regulatory instruments, in particular given the risks that emerge from these practices?*

Methodology

In order to answer these research questions, this thesis focuses on two specific case studies, children and migrants that are illustrative of the use of new IDM technologies for preventative use within Dutch citizen-state relations. The analysis of case studies involves legal research that is informed by empirical insights. The latter includes semi-structured interviews with professionals; detailed system demonstrations including descriptions of these systems in use; legal analysis of relevant existing and newly drafted data protection rules and human and children's rights prescriptions as well as desk-research regarding useful concepts from surveillance studies and Science and Technology Studies, more specifically from Actor Network Theory. The empirical research entails the practical experiences of system developers and users, as well as system demonstrations. Interviews have been conducted with different youth healthcare workers using (or having designed) the Digital Youth Healthcare Registry, youth care professionals working in one way or another with the Reference Index High Risk Youth or police professionals working with ProKid SI 12-. Furthermore, officers who used or took part in designing the INS console, the PROGIS console or the API system, such as those of the INS, the Royal Netherlands Marechausee and the Dutch Alien Police have been interviewed in different Dutch cities. In this way the diversity of localities and local traditions and routines have also been accounted for in the analysis. I interviewed 15 professionals (some of them on multiple occasions) related to the case study on children and 12 professionals (again, some on multiple occasions) related to the case study on immigrants over a period of two years. By no means can these interviews give exhaustive insights into the working practices. Yet, the insights are very useful to reflect upon the legal position of children and migrants in light of the potential of these new risk assessment technologies. The insights are furthermore helpful to open a discussion about concepts of security risks in light of such fundamental rights as for instance the right to a private life, the right to data protection and such principles as proportionality, subsidiarity, fairness, lawfulness, legitimacy and indirectly also liberty and equality.

Structure of the thesis

This dissertation consists of six chapters, three of these (chapters 1, 2 and 4) have been published as contributions in two books, and three (chapters 3, 5 and 6) have been published in the form of scientific journal articles. Chapters 1, 2 and 3 assess the legal and socio-technical implications of digital prevention systems introduced in Dutch youth care, healthcare and criminal justice on children's and families' lives. Chapters 4 and 5 deal with the legal and societal implications of the daily use of two Dutch identification systems and one risk profiling system on migrants lives. Chapter 6 draws conclusions about the normative potential of current and future data protection rules and the potential of human rights principles with respect to the commonalities that frame the vulnerable, 'at risk' position of children and migrants as a result of the use of these risk evaluation systems.

More specifically, chapter 1 deals with the problem of how the increasing reliance on the Dutch Digital Youth Healthcare Registry, the Reference Index High-Risk Youth and the ProKid SI 12- systems are implemented and used to provide a 'better, more complete' view of children who might

potentially be victims of such threats as abuse, negligence or educational problems, such as dropping out of school or who might potentially form a threat themselves by developing or having already developed anti-social or delinquent behaviour. In this first chapter we argue that the operation of the risk assessment systems entails not only the installation of the right software and operating it properly, but also that extensive work needs to be done to operate them as intended, and make them cover the rather ambiguous realities of children lives, which in fact results not only in the representation but also in the 'construction' of risks. Furthermore, the first chapter argues and demonstrates with empirical examples that behind these technologies there is a logic that expands these systems: if a digitalized risk assessment fails, the answer is to implement new modes of digitalized risk evaluation.

Chapter 2 focuses on the legal aspects of digitalized profiling of children in Dutch child-care contexts. It analyses specifically the future implications of the proposed data protection rules on the current practices of profiling children by forms of individualized risk assessment. As in the earlier chapter, the daily use of the Dutch Digital Youth Healthcare Registry, the Reference Index High-Risk Youth, and the ProKid SI 12- system provides illustrations of the problems inherent in such profiling. The negative implications of using these systems and determining how these implications can be addressed by legal means is essential in order to protect both societal interests as well as the individual privacy and data protection interests of children and families.

Chapter 3 in particular analyses the ProKid SI 12- system as it is situated within the Dutch justice system as a 'tricky' preventative tool to assess children below the age of 12 against a variety of risks both as victims and as potential perpetrators. Empirical examples show that the preventative digitalized profiling modes challenge a set of fundamental children's rights principles such as 'the child's assumption of a constitutive role in society,' its 'privacy' and at times also 'the assumption of innocence of a child until proven guilty.' Ambiguities furthermore also relate to Dutch legal prescriptions, according to which the police shall perform law enforcement tasks, although prevention tasks directed at youth would not qualify as such tasks. Moreover issues also relate to the fact that while using ProKid other systems that process strictly law enforcement data of persons above the age of 12 are also consulted in order to form a risk qualification about a child.

Chapter 4 deals with the second group of citizens at the periphery: migrants. It analyses how migrants become increasingly focussed upon through framing them as being 'at risk' or 'as a risk.' To illustrate the ways in which migrants become perceived as a consequence of using digital screening processes, two biometric identification systems – first the INS console implemented and used within the Dutch immigration chain, and secondly the PROGIS console introduced and used within the Dutch law enforcement chain – will be analysed. As a risk profiling system to assess travellers against a variety of risks, a third system, the so-called Advanced Passenger Information system will also provide empirical details about how travellers can become framed 'as a risk.'

Chapter 5 shows, by means of other empirical details about the three systems discussed in chapter 4, what kind of implications the use of these systems bring about from the perspective of both existing and future data protection rules and from the viewpoint of fundamental human rights. Although The Netherlands, through its commitments as member state and border country of the EU, has significant risk forecasting responsibilities and duties to screen immigrants and travellers crossing the Dutch Schengen border, the empirically fostered legal analysis shows that the pitfalls of the extensive use of these risk evaluating systems can easily bring new risks for the lives of migrants.

Chapter 6 provides a critical evaluation of the similarities between children and migrants as vulnerable groups. The aim of the chapter is first to bring commonalities between children and migrants to the fore and evaluate whether the legal framework properly deals with the implications of preventative identity management technologies on the lives of children and migrants. Secondly, the chapter also intends to assess whether the legal framework reinforces this vulnerability or mitigates the vulnerable

position of children and migrants. To explore the ways in which professionals can be made more reflexive about the pitfalls of their technology use and how the legal framework can provide help to remedy the negative implications of using these systems on children and migrants' also constitutes crucial part of this chapter.

Accepted and published as Chapter 5 in Y. van der Ploeg and J. Pridmore (Eds.) Digitizing Identities: Doing Identity in a Networked World, (2015), Routledge, New York (pp. 103-124).

Thesis chapter II.

Risk Identities: Constructing Actionable Problems in Dutch Youth

Karolina La Fors-Owczynik and Govert Valkenburg

1. Introduction

Dutch child-care policy has become increasingly focused on making the lives of children more and more 'transparent'. This is accomplished by connecting multiple digital databases and aggregating data about children and the persons to which they are connected. This is to give the most complete picture possible of children who may be at some sort of risk. This is believed to increase the success rates of interventions made in the lives of these children (Keymolen & Prins 2011: 21). The (potential) problems these systems are to address include abuse and negligence within families, educational problems including dropping out of school, and petty criminal behaviour such as shoplifting, nuisance and vandalism.

In this chapter, we explore developments in 'completing the picture' of children through the use and development of youth-care related databases. First, we argue, these systems are not just a matter of installing the right software and operating it appropriately. Rather, it requires a lot of work to make the systems work, and literally make them match a rather complex and ambiguous world. Second, while this work is intended to make the risks visible, it also inevitably obscures some of the realities it tries to represent, which in turn entails that some of the risks are 'constructed' rather than merely 'represented'. Finally, we observe that the whole logic of the system is such that it tends to expand: if it fails in some sense, the response is typically to install more risk assessments, to implement more risk indicators, and start the risk identification processes earlier in a child's life.

It is perhaps not that surprising that a comprehensive approach to youth risks includes the establishment of the most complete possible set of information from a variety of professionals, as this increases the likelihood that a risk or future wrong is identified in time. One of the explicit aims of national youth-care policies is that 'no child should go unseen' (Inspectie Jeugdzorg, 2008).[1] However, we will show that the ever increasing demand for information on a child does not always work out the way it was intended, for example when stigmatization arguably occurs (Dutch Youth Institute, reported by NOS, 2010).

Risk and prevention are not simple concepts. On the contrary, in this context they refer to complex arrangements of children, professionals, institutions, personal records, data technologies, legal statuses, communication protocols, and professional routines. Within the Netherlands, youth care is organized across medical, educational and law-enforcement institutions. In practice, this means that risks are identified and shared among various youth healthcare organisations, police departments, schools, judicial institutions such as the Child Protection Council and the Youth Care Bureau, municipalities, emergency departments of hospitals, social workers, housing companies, sport clubs and a variety of

[1] This chapter contains numerous phrases that we translated from Dutch to English. We take full responsibility for the translations, and choose not to point this out throughout the entire text. Only with proper names, we add the Dutch original when possible.

other organizations involved with youth. We show that some problems occurring in child care are in fact owing to the heterogeneity across parties.

We will discuss three database systems currently used in the Netherlands. First, we discuss the Digital Youth Healthcare Registry (DYHR, or Digitaal Jeugdgezondheidszorgdossier in Dutch). It is designed for the registration of healthcare information on children between 0-19 years. Second, we discuss the Reference Index for High Risk Youth (RI, or Verwijsindex Risicojongeren in Dutch). The RI is a large-scale risk signalling system that connects various digital systems, youth care organizations and professionals by providing digital exchange of risk signals about children and youngsters aged between 0 and 23 years in the Netherlands. Finally, we discuss ProKid 12- (pronounced 'ProKid twelve-minus'). This is a tool for risk assessment on children aged between 0-12 years, used nationwide by the police. In ProKid, colour codes are assigned to children, reflecting various levels of estimated risk.

At face value, it appears as if 'risks' are simply identified and then communicated through particular networks and relationships. On the one hand, 'risks' indeed appear in the form of simple indicators such as classifications, signals, and colour codes. These forms make risks 'actionable'. On the other hand, the indicators consolidate extensive assessments. When indicators arrive at a new location, they are in turn interpreted and re-imbued with a potentially different meaning, instigating different interventions. This occurs because of divergent backgrounds of professional knowledge, routines, codes of conduct, and anything else on which professional practices may just differ. As we will continue to argue, the work done to deal with risks is successful in some ways, and perilous in others.

2. Risk assessment systems for youth in The Netherlands

Following Dutch youth policy, both youth care and law enforcement have increasingly become geared towards prevention: problems are to be solved proactively before they become real. 'Risks' and their identification serve to make problems actionable before they actually occur. Indeed, wordings such as "making risks visible", or "making the child transparent"[2] often appear in youth policy. This eagerness for making visible the potential problems of children is reflected by mottos from professional reports: "to establish a comprehensive approach to children" (Berkeley & Van Uden, 2009), "to create a complete view of children", and "no child should go unseen" (Inspectie Jeugdzorg, 2008). Identifying those who might be responsible for future crimes provides the rationale of many prevention practices. As one professional explains:

> *"The goal initiating ProKid was to ensure that police officers in the field work more efficiently. What you see with the police is that normally they respond to an incident. Only when something happens, the police are called, and then they arrive to start an investigation. […] The idea was that you want to know the 5% of people that are responsible for 60% of all crime incidents. If you know them, you can focus on the 5% of children who may actually come in contact with the police." (ProKid professional, city A)*

This 'making visible' of children's problems serves a two-tier purpose: first, it facilitates the identification and classification of the 'abnormal', and second, by consequence, it makes these abnormalities actionable, or at least presents the indispensable object for action. This practice is justified by the assumption that intervention will be more effective if it takes place earlier. This entails a need for early identification of risks. Thus, early risk assessments on youth are considered essential resources for professionals.

[2] The paradoxical point that transparency strictly refers to a particular kind of 'invisibility' will not be elaborated further here.

Emphasis on prevention is also evident in other areas of youth care, such as for example youth healthcare (Gorissen, 2002; Mathar & Jansen, 2010). The availability of interconnected risk identification systems also facilitated police corps and social workers to increasingly carry out pro-active actions, and prevent harms not suffered and crimes not committed yet by youth (Min. van Veiligheid en Justitie, 2012). At the same time, youth healthcare professionals increasingly take up tasks that shift from counselling and support towards the prevention and control of youth and the crimes they potentially commit (Friessen, Karré, & van der steen, 2011). This preventive approach to youth care and the according arrangements of organizations have received wide acclaim in professional policy discourse. The consensus seems to be that the results are good and investments justified (ACTIZ, 2012).

2.1. Digital Youth Healthcare Registry

In the Netherlands, children aged between 0-19 are screened periodically through consultations with healthcare professionals. These occur at specialized youth healthcare offices for children from 0 to 4 years, and by school doctors for children from 5 to 19. The Digital Youth Healthcare Registry (DYHR) is a healthcare database used for the registration of children's psychological, social and cognitive data. Use of the DYHR by school doctors and advice centres became mandatory as of 2010.

In the DYHR, a child's record is kept as a Basic Data Set (BDS). In addition to generic medical data (weight, height, visual and auditive capacity, etc.), the BDS contains indicators that could be regarded as risk indicators. Most prominent among these is the list of "invasive events" that was part of the 2011 version of the BDS (Nederlands Centrum Jeugdgezondheid, 2011). This includes suspected physical abuse, serious illness of the parents, parental divorce, alcohol abuse by the parents, and teenage pregnancy. Notably, as this list was found to be too much of a straightjacket, it was replaced by a 'free text field' in the subsequent version (Nederlands Centrum Jeugdgezondheid, 2011, 2013). Although the text field now allows for less specified ('free') descriptions of risk, it remains a significant indicator for risk. Also, while the 'freedom' to report increases, it is still only a freedom to report risks, which entails that the possibilities for a child to become risk-profiled grow.

2.2. Reference Index for High-Risk Youth

The Reference Index for High-risk Youth (RI) is a comprehensive risk signalling system that connects a variety of digital systems. It enables youth care organizations and professionals to digitally exchange risk signals on children and young adults aged 0-23 years. It is an infrastructure rather than a single system. Each time a risk is identified and entered into a local system, this identification is automatically forwarded to the national RI. The aforementioned DYHR as well as other youth healthcare practices in general are connected to the RI (Rouvoet, 2007; *Wet op de jeugdzorg*, 2005) and it has been operational since 2010.

The RI facilitates the communication of alerts regarding children among professionals. The transmitted risk signals represent potential harms. The risk signals only consist of risk flags, and are not automatically supplied with explanatory information, nor any other content of the children's files. The only information accompanying the risk flag are the name of the professional who issues it, the name of the organization the professional works for and the name of the child the signal is related to (Nouwt & Hogendorp, 2010). The concealment of more substantial information was demanded by the Dutch Medical Association (Dutch: KNMG, Koninklijke Nederlandse Maatschappij tot Bevordering der Geneeskunst), as the RI would otherwise have posed too much of a privacy and confidentiality encroachment.

2.3. ProKid 12-

ProKid 12- is a risk categorization system for children between 0 and 12 years. The child's address serves as the primary key to the database. ProKid employs four colour codes to represent risks: white, yellow, orange and red, respectively signifying a growing gradation of concern. White signifies that no risks have been identified as yet, yellow represents a possible development of risks, orange indicates that problems and even criminal behaviour have already occurred, and red symbolizes children who have repeatedly shown criminal behaviour, or of whom multiple cases of suspicion have been recorded (Abraham, Buysse, Loef, & Dijk, Van, 2011). Following a pilot phase, the system has been in operation nation-wide by the Dutch police as of 2013 (Tweede Kamer, 2012).

The risk categories and their attributions are based on behavioural-scientific models, and explicitly aimed at early detection of potential criminal behaviour of children. The attribution of colour codes is done automatically, by means of algorithms, on the basis of information in other large police databases. These include the Basic Facility for Law Enforcement (BFLE, or Basisvoorziening Handhaving in Dutch) as well as the Basic Facility for Forensic Investigation (BFFI, or Basisvoorziening Opsporing in Dutch). Information from ProKid is shared among youth care partners if a ProKid manager decides that there is reason to do so.

3. Doing 'risk' in practice

Identifying and eliminating youth risks is complex work. Numerous professionals are involved, ranging from educational and social practitioners, to healthcare workers and legal and police professionals. By definition, the knowledge one professional has of a child is always limited: not so much because they do their work poorly or because they have limited resources, but because any profession has things on which it focuses and things on which it does not. A medical professional 'sees' different things than a police officer or a school teacher.

In recognition of this partiality of knowledge, the information systems introduced above are explicitly set up to meet the challenge of crossing boundaries between professions. The systems are intended to yield a more comprehensive view of the risks that children are exposed to than any single profession could have by itself. This sharing of information is increasingly seen as an essential resource for a range of youth care professionals in the execution of their daily preventive tasks (RadarAdvies). The emphasis is adopted by many regulations that legally stimulate the deployment of digital risk profiles. The Public Health Act (*Wet Publieke Gezondheid*, 2008) requires professionals to digitally register data including risks about children in DYHR. The Law on the Reference Index (Rijksoverheid, 2010) stimulates the aggregation of risk profiles on children by a variety of professionals involved in youth care.

However, it turns out that the sharing of information is not just a panacea to eliminate risks. Managing the information requires work of its own, and while often fruitful, this work is also at times difficult and frustrating. One corollary of the fact that professions frame problems differently is that seemingly the same information might have different meanings and implications in different situations. In the doctor's office, a mother with a medical problem might be just that, but from a social-work perspective, more structural problems might be suspected. In choosing between these options, a healthcare professional may need more comprehensive information from other professionals, which may not be available through mere risk indicators.

Risk indicators are compact representations of risks. They may be shaped as, amongst others, categories, colour-codes or signals. While facilitating communication, indicators also consolidate comprehensive

assessments, complex sets of information and tacit professional knowledge. An indicator (at least partly) obscures the process of risk identification. This (at least partly) precludes their discussion and revision, and indicators become more fixed *de facto*. A perfect example is the use of colour codes in the ProKid system, which turn out to be both elegantly compact and sources of confusion (Willems & Van der Heijden, 2011: 3).

The practices in which individual professionals operate are more unruly than the ideal of comprehensive risk identification suggests. Between different institutions and professions, consensus is often lacking on what a risk exactly is. A youth healthcare professional, for instance, explained her frustration over this problem, and how it troubles her ability to assess risks:

> *"You see the categories with a red checkmark, with certain families the screen is almost only red. You still need to read the record [underlying the checkmarks], and you can relatively quickly figure out what the problems are. But it is often difficult to fill in the risk assessment form, or to risk-score children, because there is no clear definition of risks. For instance, a 'sleeping problem' of a child can be just that, but it can also be a symptom of issues between the parents; or it can be caused by cultural elements that are just different between one family and another." (CB-nurse, city D)*

While the meaning of the symbolic representation of the risk may remain unclear, its presence in a graphic material form seems to express a very clear urgency for action. Yet, if professionals find themselves confronted with this urgency, they obviously want to be sure that they can tell a sleeping problem from parental tensions before proceeding to action. While an indicator is aimed to deliver 'actionability', it also carries ambiguity. This ambiguity entails that different professionals may conclude to different 'optimal' solutions.

Within the RI, similar ambiguities occur in the presentation and interpretation of risks. One professional using the RI reports that it often remains unclear what others mean by particular risk signals. This is owing to the fact that the contents of children's records are not shared for privacy and confidentiality reasons.

> *"Professionals have a web-based system, which can send signals automatically. In addition, we have also some 'soap connections' [automated connections]. Risk signals can be sent directly to the RI, if professionals register a risk in their own files. But they only send signals, no content. We do not know what the risk signal is about." (RI manager, city B)*

Finally, the very definitions of risks within the context of ProKid are themselves ambiguous. This is remarkable, as ProKid is based on standards that explicitly describe when a child needs to be scored with a white, yellow, orange or red flag. For example, the orange code is to be attributed to children "who either have at least once been registered as suspects of a serious crime (such as animal abuse, arson, sexual offences, public violence or robbery) or more than once have been reported as missing. Furthermore, a child can also be profiled with an orange flag, if he/she has been reported as a suspect five times or more, or he/she it has been registered five times in relation to various incidents, or if he/she has been reported ten times or more as a victim or a witness." (Willems & Van der Heijden, 2011: 3) This orange colour code thus represents a rather heterogeneous set of problems, the complexity and heterogeneity of which remain implicit. Within the orange class, the distinctions between perpetrators, victims and witnesses vanish. Whereas the colour codes were intended to speed-up the assessment of reports by offering a quick summary, the resulting ambiguity compels police officers to yet investigate the whole background of an issue.

On top of these direct identifications of risks – in the sense that professionals explicitly regard something as a risk and enter it into the system – risks are also constructed indirectly, through what could be called

'circumstantial evidence'. Such construction is particularly facilitated by systems that are connected to ProKid, such as the BFFI. The following quote shows how a risk identification emerges in, or 'between', these systems. It is the result of observations made by a police officer at a crime scene, which are not directly related to the crime, but may be related to a child:

> *"[…] when our officers are at an address, and find drugs, […] this information becomes registered in BFLE. But if they find a baby bottle in the kitchen, and ask whether there is a baby; and the inhabitants of the house answer: 'No, the bottle belongs to my sister who comes here occasionally'. If the officer cannot find hard information about whether we need to seek care for the baby, or who exactly lives there, to what extent the person makes something up… and the officer has a bad feeling[about it], and wants to use the information [about the bottle], he can register it in BFFI. We, ProKid managers, can see that." (ProKid manager, city C)*

This 'soft' information will eventually become relevant in risk assessments done by means of ProKid. It thus adds to the whole assemblage of early warnings and early risk identification, so as to further help prevention. This emergence of risk identification is exemplary for what happens when multiple institutions become involved: risk identifications propagate through systems, through which their genesis fades out of scope, and their content becomes more solidified.

Early detection and a comprehensive view hinge importantly on communication and the distribution of information.

> ***"[****The DYHR] helps you to create a better problem overview. You can provide better advice and guidance based on the information it contains. […]Previously, we had a hand-written 'integral paper record' in which you needed to search for information manually. Now, you click on a section and it appears immediately before your eyes in a digital format. Extracting, sharing and analysing data from the digital dossier is much faster.****" (CB-nurse, city D)*

Yet communication and distribution of risk assessments are not just that. They are mechanisms, mobilized to bring a variety of professionals together and promote communication between them. In the view of one RI manager, such promotion of communication and the matching of risk signals are beneficial to rendering multiple problems with children visible. The infrastructure brings those aggregated problems under the attention of professionals. As the RI manager explains:

> *"The number of [risk signal] matches increases over time. For us, this indicates that professionals increasingly contact each other over a child's case. In 2008, we had 30,000 signals and 2,277 matches. In 2009, we had 30,313 signals and 3,100 matches. Up until now [July 2010], we have had 30,081 signals and 3,500 matches. […] The idea behind the system was to arrange a child's case as a point of connection between professionals. Thus, children with multiple problems would become visible earlier, […] receive better help, in case they have multiple problems within a family. Such complexity needs to be addressed comprehensively, so that a child will not be 'ping-pong-ed' between professionals, each of them needing to start the child's assessment from scratch." (RI manager, city A)*

However, this leaves untouched the fact that risk-related data potentially represent different issues for different professionals. For example, the police officer managing ProKid reported her difficulty to interpret what the colour-coded risks symbolize. For example, concerning one incident, the police officer explained her hesitation in assessing the gravity of the incident and reducing it to a single risk indicator:

> *"The problem we encounter with ProKid is that we get our colour lists in Excel each week, but we also need to read all the reports and what a yellow or a red colour symbolizes. If there is a report about a child, who has set something on fire, we only know that it has set something on fire. We do not know whether it has set a newspaper on fire, or a whole school building, for instance. So, you have to read the reports to learn the severity of the crime. This is important for your risk analysis." (ProKid manager, city B)*

It is not straightforward what kind of risk information is to be shared between the police and youth care institutions. This is partly the consequence of the fact that policies to stimulate co-operation between law enforcement and youth care organizations are still developing. The following manager doubts the validity of the instruments in practice, even though they are 'scientifically founded'. He explains that it would be better to exchange information already if files of children are tagged with orange, yellow and even white flags:

> *"If I see a child who has just a yellow or white coloured registration – and I know this does not yet qualify it for sending to the Youth Care Bureau – but the child's friend is 'red' in the system; then I bring this extra information into the case discussion within the Youth Care Bureau." (ProKid manager, city B)*

The professional thus seeks his own way in dealing with colour codes, and looks for ways to include information that would otherwise *not* fit into the system. Particularly, information from the social environment of the child is sought to be incorporated.

Numerous examples exist of when the smooth, digital sharing of information obscures rather than improves the view of professionals on children. For example, the distribution of erroneous information shows a perilous irreversibility:

> *"Everything I register goes instantly into the computer and can be monitored. […] If someone has filled in something wrong, then I need to receive an email query whether I would take out the wrong information. Until then, [the wrong information] remains in the file." (CB-doctor, city A)*

This quote indicates how risks are foregrounded and consolidated by digital mediation. On the one hand, the registration of data is distributed in such a way that it becomes instantly visible for professionals in different locations. This is supposed to be helpful for the early identification of risks. On the other hand, erasing these data from files becomes a highly work-intensive process. Erasure is not automated, but involves extensive e-mail correspondence. This means that, in case of erroneous information, the rapid sharing adds confusion rather than clarity, as corrections are always delayed. As the information is predominantly about risks, and the identification of those risks travels much faster than their possible correction, the system *de facto* favours the emergence of risks over their correction.

This is where the systems clearly show a non-neutrality between the negative realities of risks, and potential positive realities that may be articulated to oppose them. They are designed to store not just any information, but a particular selection of information. This entails that some information cannot be stored, even if a professional assesses the information as relevant, and even if the data is seemingly neutral or innocent.

4. Risk prevention biting back

As we have discussed, the DYHR, the RI and ProKid systems all in some way manage risk identities of children. Also, each system connects multiple practices, providing channels between different professions. In this section, we discuss this identity management across professional boundaries as an 'ontological practice of selection' (Bowker & Leigh Star, 1999; I. Hacking, 1991; Ian Hacking, 1986; Law, 2008). Whether something counts as 'normal' or 'abnormal', 'deviant', 'at risk' or 'as risk' always has consequences for the very world those attributed classes describe, which makes this 'description' also a performative affair. One intended consequence is that these classes offer a ground for preventive action. Yet, not all consequences are intended or justified, and we will articulate some of the structural issues that carry unintended consequences.

The dominant idea informing the installation of the risk assessment systems is that transparency, visibility and comprehensiveness are key to prevention of youth problems (Keymolen & Prins, 2011; Van der Hof, Leenes, & Fennell-van Esch, 2009). We approach this 'making visible' as an ontological affair, as risk identification also *transforms* the problems that are identified. For sure, there are serious and real problems among youth that merit intervention by social workers and other professionals. Clearly, these problems must first be identified, if possible before they actually emerge, before any intervention can be made. However, the shape in which these problems are articulated does not stand in a one-to-one, unequivocal relation to what actually happens in the life of the child. We show that the DYHR, the RI and ProKid do indeed identify real problems, but that they also transform these problems, represent them in non-neutral ways, and introduce ambiguities of their own.

To identify risks in children and make them actionable, risks are consolidated into indicators: items on which children are scored, and which offer justification for a particular intervention to be made. On the one hand, such indicators are compact and practical: they reflect the severity of a situation, and instigate interventions. On the other hand, these indicators conceal a lot. A percentage, a colour code or a 'yes/no' item hides the work through which a professional arrives at the indicator. This work includes professional interpretation and judgment, professional discretion, conversation with a range of other professionals, intuition, tacit knowledge, contextual knowledge, etc. The necessity of these non-formalized ingredients is recognized by official reports and guidelines (Inspectie Jeugdzorg, 2008), yet they are not reflected by the indicator itself. Even if formal standards are in place that specify how an indicator is to be scored, as with the colour codes above, this formalized part of the assessment is never the whole story (for otherwise we would not need professionals but only administrative clerks or even computers to do the assessment).

In addition to identification, the systems are about communication and distribution of risk assessments. More specifically, communication is to take place between different practices of youth care, and these practices employ potentially incompatible approaches. This entails that the identified risks need to be presented in multiple ways, that they are mobilized for multiple programmes, that they are to fulfil multiple tasks, and that they will be imbued with different meanings across situations. Communication in this sense is not the transparent transport of information, but complex work of translation across boundaries.

The use of indicators as tokens of complex judgments makes such communication possible in the first place. Indicators are 'mobile': they are compact and can be conveniently passed on to another professional. They are also 'immutable': as they are deeply rooted in the practices that establish them, it becomes hard or even impossible to deny or contest them. As 'immutable mobiles' (Latour, 1987), indicators are able to mobilize a wide range of actors by their alerting characteristic. At the same time, the compactness that allows their mobility entails a continuous need to reinterpretation and adjustment to local knowledge, traditions, codes of conducts and objectives.

While crossing disciplinary boundaries, the aforementioned concealment enables indicators to help keeping responsibilities in place. For example, even though intensive sharing of data between medical and non-medical youth-care professionals was pursued by connecting the DYHR and the RI, the Dutch Medical Association KNMG pled for strict limitations on the sharing of medical information. Obviously, the KNMG held paramount the privacy and confidentiality of patient data. The 'best interest' of the child should be the touchstone for whether or not medical data would be shared (KNMG, 2009). By reducing such complex information to single indicators, exchange of that information became possible in the first place.

Offering both 'transport' and 'seclusion' of information, risk indicators are perfect examples of what have been conceptualized as *boundary objects*: entities that are ambiguous and flexible enough to work in different contexts, but also stable enough to meaningfully connect between those contexts (Star & Griesemer, 1989; Star, 2010). They deliver some of the promises for which the information systems were installed, namely the connection of different professional practices. At the same time, what they actually convey is not a simple representation of a pre-existing reality, but a particular construction of that reality.

Once these indicators are established, they become harder to modify. To some extent, they start to live a life of their own, not least because the exact conditions under which they were established become invisible. While they are supposed to be representations of chances and possibilities for deviance, deviance also becomes more 'real': it 'exists' as representations presented by the systems. The reality of the issues in part consists of a certain irreversibility, once an indicator has been assigned to a child. As one RI manager explains:

> *"The problem is that the Reference Index at the time of its introduction was presented as a 'Concern reporting system', similar to the 'concern reports' police write. You know, it created among professionals an idea of quite a 'serious and heavy' system. Hence, professionals are often afraid of signalling anything in there, although in practice it is just an alerting system and only contains data from the municipality register. This fear to signal is a pity." (RI manager, city D)*

We observed that professionals sometimes become hesitant to enter issues into the system, as they cannot oversee the effects their data input might bring about elsewhere. The same professional expresses her own fear of the potential consequences of risk profiles. Quite delicately, a few minutes later, she reports:

> *"...oh while I am showing you this, I have almost put a risk flag on my own child,that is something I would absolutely not want as a mother..." (RI manager, city D)*

The 'making real' of risks through the establishment of indicators is not just in making a solid representation of what is already there. This 'solidification' is not neutral, but prioritizes risks: indeed, they are *risk* indicators, and a risk constitutes a negative frame and calls for action. The risk assessment system does not accommodate positive realities or anything else that could mitigate or oppose an observed risk. One professional explained her frustration at not being able to register that a child is doing well:

> *"Many professionals who have already been working for years within youth healthcare, notice for instance, that they cannot register signals in the system that reflect that things are going well for the child. I find it to be frustrating that I can only register negative things, only risks, and not that the kid is doing well. The system only allows you to record risks. For example, that the child is hyperactive. It is as if children can only have problems. If things are going well for the child, then I would like to register that, but I cannot." (CB nurse, city D)*

The system is geared towards prevention, but it *de facto* disallows professionals to retract concerns if they think the measures would be too much or unnecessary.

Although solidifying risks is intended to ease professional communication across practices, certain translations of risks into technological software or scripts (Akrich, 1992) can be sources of frustration for professionals. A quote from an interview with a ProKid managing professional exemplifies this. For ProKid, changes of address are key. However, the system is not able to register two addresses with one child. This is potentially problematic:

"Address changes in the [ProKid] system are not connected to changes in the municipal registry.[3] When a police officer reports on an address, [the data] are checked automatically against the municipal registry. However, if parents divorce and move to two different addresses, and they arrange co-parenthood, the child is usually registered only at the mother's address. So, if a problem occurs at the father's address, ProKid unfortunately misses out on that." (ProKid manager, city B)

The inability to associate two or more addresses with a child is seen to hamper risk assessments. This is more than just a design flaw. It is a technological solidification of the social norm that children live with their married parents. Oddly, it opposes the tendency of risk assessments to extend into the broader social environment of children beyond their immediate family (see below).

5. Proliferation of risk assessment

The preoccupation with risks as actionable, negative realities parallels a proliferation of risk indicators. It is one thing that risk indicators are arranged in ways that they can be shared easily between different professionals. It is another thing that risk assessments and the communication of those risks seems to engender an ongoing expansion of the number of risk indicators.

This connects to what Van der Ploeg (1998) observed in the context of pre-natal care. She showed that pre-natal interventions are always susceptible to the critique that the intervention would have been more effective if it had been made earlier, when the problem was supposedly still smaller and easier to encapsulate. This instigates ever more intensive and earlier screening. Van der Ploeg describes this as the "logic of infinite regression". In the present case, a similar logic suggests that risks linked to children can be dealt with better if their registration is more comprehensive and indeed earlier.

We will discuss three dimensions of this multiplication of risk indicators. First, practices of risk assessment increasingly include the family of the child explicitly in the registration of risks. Second, a similar development is visible regarding the broader social environment of the child. Third, as suggested, there is an assumption that earlier identification of risks leads to their being better manageable. In conclusion, these three developments culminate in the growth of the number of indicators.

5.1. Extending the view onto the family

The attention paid to a child's family in youth care practices continues to increase and to be integrated formally in the system. A police officer working with ProKid, for instance emphasizes the influence of parents on their children. As changes of the parents' relationships may have serious consequences for a child, according to him, these should be part of a child's risk assessment. The following example illustrates how a risk profile of a new family member may affect a child's colour code in ProKid:[4]

"Many times you see, the mother is divorced and has a child, and the child gets a report. The child is reported as hyperactive. Then, later the mother starts a new relationship with a man, who moves in at the same address. If the mother's new boyfriend, for instance, already has a police record, or has been involved in domestic violence, this creates a high risk factor for the child. The child lives at one address with this man. Therefore, the yellow colour of the address [in the child's record] will turn into orange[...]Another example is when the mother has been caught with shop-lifting, and then she explains that she did the shop lifting because of her severe circumstances, e.g.: 'otherwise I am not able to feed and take care of my child'. This also constitutes a risk factor." (ProKid manager, city B)

[3] In the Netherlands, municipalities maintain central registries of addresses of all their inhabitants.
[4] One assumption underlying ProKid is that incidents with persons living at the child's address constitute a risk factor for the child. Therefore, they are to be reported.

Beyond criminal concerns, the profiling of parents also plays a central part during risk assessments in youth healthcare practices. Screening the health conditions of parents constitutes a significant part of health screening processes for children. In the use of the DYHR, the social and financial statuses of parents increasingly receive attention from professionals, and they are taken into account when assessing the health risks children may be exposed to:

> *"You need to know of possible healthcare risks; whether the parents, for instance, have a [social or financial] problem. Moreover, if the parents have problems, the broader picture need to be looked at, and not only the child. It is possible that you have already noted down issues in the DMO protocol.[5] For example, the parents might be unemployed, have high debts, or the child has been taken out of the family home, etc. These issues […] importantly influence the child's development." (CB nurse, city D)*

In some youth healthcare practices, even the extended-familial relations are considered essential for an adequate risk assessment. A professional using the DYHR shares her frustration at not being able to properly assess a child's risk profile, as assessment of the broader social environment of the child was not possible with the digital system at the time. This complicated her work, as here knowledge remained incomplete. She could not see a child's relation to its step-father, step-mother or to its grandparents. She argues that familial relations should be made more visible:

> *"You actually need a structural description of the family. I mean all those relatives with which the child interacts daily. So far, only the biological father and mother are registered in the [DYHR] record, but not the stepfather, stepmother, stepbrothers and stepsisters. Or, if the child often stays with grandpa or grandma, then the grandparents need to be registered in the dossier, too. But the system does not allow for such registration, unfortunately. Nowadays, there are a lot of divorces. We should also make those family relations visible, I think." (CB nurse, city D)*

In contrast to this, the RI contains a novel 'family functionality'. This functionality increases the number of family members that can be made relevant in a risk profile of a child. It also increases the number of youth care professionals that are connected to the RI. In particular, it ropes in professionals who are not focusing on the child but on older (even adult) brothers, sisters, and on parents.

5.2. Expansion into the broader social environment

Another dimension of proliferation is the increasing attention paid to the larger social environment of the child within practices connected to ProKid. Even the behaviour of neighbours can be relevant to a child's assessment:

> *"Suppose there was a fight between neighbours. […] Then, I know that the children of the neighbours have probably been involved in that fight, too. The police come and make a report. Then, in ProKid, I see that a child from one address fought with a child from the neighbouring address. I can then check back in time, and see that these children's fathers also fought, two years ago. I can then connect these things, and that is the analysis I do." (ProKid manager, city B)*

This shows how multiple profiles, including the profile of the neighbour or the father, are drawn together in a ProKid-based analysis. From these combined risk profiles, risk factors to which the child is exposed are identified and registered more sophisticatedly in the child's ProKid record.

[5] The DMO protocol is a standard, early signaling/warning instrument used within Dutch youth healthcare practices in order to assess children aged 0-4 years. (Hielkema, de Winter, de Meer, & Reijneveld, 2008)

In addition to familial and social relations, ProKid even brings forward a child's relations to animals. ProKid incorporates behavioural-scientific research findings holding that the way children interact with animals is indicative of the risks a child might pose to society in the future:

> *"We also have another, somewhat strange risk factor in our list: animal abuse. If a child abuses an animal at an early age, then, according to the scientific findings of Radboud University of Nijmegen, that child has a higher inclination for sexual abuse at a later age. We relied on scientific explanation to include such a category into the system." (Police officer responsible for ProKid project, city B)*

Also the child's friends' risk profiles are made part of risk assessments. Links between friends' risk profiles increase the weight attributed to those profiles:

> *"If I see a child who has a 'yellow' or 'white' colour code, and although officially the case is 'not yet worth' being sent to the Youth Care Bureau (YCB),[6] but if a friend of that child is 'red' in the system, then I share this extra information [about the 'yellow' or 'white' colour coded child] during the case discussion within YCB." (ProKid manager, city B)*

These examples demonstrate that the proliferation in social space is becoming visible as a redefinition of social roles. Children who are diagnosed as being 'at risk', are increasingly also treated themselves 'as risk': behavioural-scientific evidence suggests that children who are exposed to risks, run a greater chance to become perpetrators themselves. While this is taken as a reason for additional care, and not, say, for pre-emptive punishment, it is indicative of the logic of ever earlier and more comprehensive detection. What is more, indicators attributed to persons surrounding the child not only offer more risk indicators against which a child is to be assessed, but also intensify the preventative monitoring of persons who are seen to fall within the social space of a child.

5.3. Extension in time

The third dimension of this proliferation of risk assessment concerns time. One example is provided by the installation of so-called "pre-signals" into the Reference Index. These are flags that can be added to a child's record in the local Reference Index. If such a flag is set, on any new information added about the child by a different youth care agency, an automatic email is sent to the institution that originally set the flag. Differently, a 'real' match leads to an email being sent to *all* those institutions that have signaled a risk about the same child in the reference index. These pre-signals are not forwarded to the National Reference Index, neither are they 'matched' by any automatic process. Pre-signals provide opportunities for early warning, legitimated by the consequences of the pre-signal being comparably limited. However, they remain part of socio-technical assessments, and stimulate earlier evaluations and consequently interventions. Likewise, the aforementioned advancement of colour codes based on indirect risks can be seen as a proliferation into time: issues surface earlier, and this is thought to improve prevention.

Proliferation in time not only concerns the past, but also the future. The RI distinguishes between 'active' and 'passive' risk signals. The active state of a signal refers to the period a risk signal can be automatically matched:

> *"Each signal has an expiration date. […] For instance a police signal remains for 3 months, a signal from an educational institution for 6, signals of other organizations generally remain for 12 months, and we keep BYC signals for 24 months in RI. Signals can be matched only during these periods. […] According*

[6] According to the ProKid instructions, each case with a 'red' or 'orange' colour code needs to be forwarded directly to Bureau Youth Care (Hensen, 2010: 34).

to the new Youth Care Act, after a signal becomes passive, it remains visible for another 5 years on the web-site. Afterwards, it must be deleted." (RI manager, city C)

Despite technical restrictions, such as the absence of automated matching, the 'passive state' in practice produces an extension of the time a signal remains actionable for professionals. Within this period, a 'passive' signal keeps presenting a negative reality that should be mended:

"This passive signaling allows for another professional to use the source of the passive signal, in order to acquire information from the professional about the child." (RI manager, city D)

The constructions of pre-signals and 'passive' signals in the RI, and the colour-code classifications of risks in ProKid epitomize the proliferation of risks in time. Risk indicators accompany a child on a longer time span in practice, thus offering a longer window of opportunity for preventive intervention.

5.4. Ever more indicators

Taken together, these developments lead to a growth in the number of risk indicators. In addition, difficulties of communication across various professions are often attributed to a certain incompleteness in the available information on a child (Inspectie Jeugdzorg, 2008). This incompleteness instigates the addition of ever more risk indicators, which are thought to be more usable in different contexts if these indicators are more diverse and comprehensive. If risk assessments work imperfectly in one context or another, the response has been to add more indicators so as to increase the likelihood that they contain information that is meaningful in a particular context. Certainly, professionals working with these systems are not necessarily uncritical or naïve about such additions. Quite the contrary, the removal of the fixed list of invasive events from the BDS described earlier reflects a critical stance, as does the recognition that building systems are a matter of trial and error.

The mere growth of the number of indicators perpetuates and amplifies problems that we have observed so far. Opacity and ambiguity are more likely to cause problems if there are more indicators to materialize them. Similarly, the increasing number of indicators combined with their 'permanence' increases the chances for a child to become and remain qualified as being either 'at risk' or 'as a risk'. Also, the increasing number of connections between risk factors, colour codes, risk signals and risk profiles and their surrounding practices increases the chance that combinations of those indicators produce a 'hit'. As Van der Hof (2010) argues, while the DYHR eases the circulation of information, the resulting escalation of information itself poses new difficulties for professionals, as the most problematic cases become more troublesome to sort out. What is more, 'less serious' issues increasingly raise alerts, because the large number of indicators makes the system in a way too sensitive.

All of the issues described are the consequence of a sincere pursuit of good care for children. New risk indicators often result from new scientific evidence and the recognition of real flaws in care practices. However, practices of youth care and the digital systems through which they operate entail a proliferation that brings severe problems of their own.

6. Conclusion: it's hard not to be at risk

Modes for identifying and preventing risks in youth care in the Netherlands are being reconfigured in unprecedented manners. Prevention is performed by a growing range of youth care and law enforcement organizations, systems and professionals. The problems they face include various forms of child abuse, anti-social behaviour and medical problems. Attempts to solve these problems occur through the use of

comprehensive digital means, and the enrolment of ever more socio-technical practices of youth care, as well as an extension of what is thought to be relevant. Involved practices currently include the police, healthcare professionals, social workers, municipality administrators, educational institutions and debt counselling services.

Underlying all these developments is the sincere aim of improving the protection of children. First, this aim is translated in a need for ever more information and improved sharing of information and translated into digital technology. Second, this need for information is transformed into a pursuit of 'making children transparent', or to create a 'comprehensive picture' of the child. Third, as we have shown, this picture is subject to the dynamics that spawns risk assessments in various ways described above.

In this study, the practices of youth care seem to be built on the presumption that risks are pre-existing and real, and can be made more actionable by making them visible. While we do not deny the *existence per se* of such risks, our analysis shows that in practice a very *specific reality* of risks is constructed. Risk indicators proliferate, propagating ambiguities and interpretational problems. Making risks 'real' and existent in the form of technologically mediated indicators also transforms chances of deviance into real expectations. Particularly, the gradual transformation from a child 'at risk' towards a child 'as risk' is to be understood as a consequence of this proliferation.

This study suggests that the mentioned practices of youth care 'produce' risks in two ways. The first refers to the construction of risks as risk indicators. This construction is key to making risks actionable and for initiating prevention. The second sense raises more concern. The dynamics of consolidating risks into indicators and of the proliferation of those indicators simply raises chances for a child to become subject to a regime of care or raised attention. In many cases, this will be justified, however, in other cases problematic.

These 'false positives' are recognized, but accepted as a 'cost' of the system. The spokesman of an umbrella organization[7] for Dutch youth care agencies responds to recent findings that 10% of all suspicions of child abuse reported to the Advice and Reporting Centre Child Abuse (ARCC, in Dutch: Advies en Meldpunt Kindermishandeling, AMK) - a sub-organization within Bureau Youth Care - were false.

> *Journalist: The Dutch Youth Institute argued today in the daily newspaper 'Trouw'[8] that families feel stigmatized, if they are falsely accused [of child abuse]. Do you recognize this?*
>
> *Spokesman: Yes. If for a small circle of professionals risks remain known about a child, and if parents return to the GP, they know that a suspicion had been registered and investigations took place. We argue, however, that this price we must pay for the remaining 90%. That is more than 14000 children per year in The Netherlands where investigations happen correctly. In these cases, it proves to be crucial that investigations happen. So this [10% false suspicion] is a consequence that we cannot entirely prevent."* (NOS, 2010)

Despite this acceptance, our analysis has shown that such negative side-effects are contingent upon particular technological choices, such as the reduction of complex observations to simple indicators. Side-effects include false-positives, the impossibility to indicate that a child is doing well, and emerging ambiguities of risk indicators that entail misunderstandings between care practices. Solutions for these effects may not be in finding better technological solutions, nor would we argue for an abolition of risk assessments as if they were only bad. Rather, improvement could be sought in reconsidering *how* risks

[7] <http://www.mogroep.nl/>

[8] <http://www.trouw.nl/tr/nl/4492/Nederland/article/detail/1087513/2010/02/09/Een-op-tien-meldingen-kindermishandeling-vals.dhtml>

are made present, and whether technological, professional and organizational elements could be arranged differently, such that they present those risks in ways that invite reflexivity, and awareness of the side-effects showcased in this chapter.

Bibliography

Abraham, M., Buysse, W., Loef, L., & Dijk, Van, B. (2011). *Pilot ProKid 12-Signaleeringsinstrument geevalueerd*. Amstedam. Retrieved from http://www.dsp-groep.nl/getFile.cfm?dir=rapport&file=12wbprokid_eindrapport_Pilots_Prokid_geevalueerd_met_Engelse_samenvatting.pdf

ACTIZ. (2012). Flyer: preventie door jeugdgezondheidszorg loont. Retrieved August 30, 2012, from http://www.vng.nl/onderwerpenindex/jeugd/jeugdgezondheidszorg/publicaties/flyer-preventie-door-jeugdgezondheidszorg-loont

Akrich, M. (1992). The De-scription of Technical Objects. In W. Bijker & J. Law (Eds.), *Shaping Technology / Building Society: Studies in Sociotechnical Change* (pp. 205–224). Cambridge, MA, MIT Press.

Berkeley, E., & Van Uden, A. (2009). *Risicojongeren Een bundeling van inzichten uit onderzoek, beleid en praktijk over een effectieve aanpak*. Den Haag. Retrieved from www.nicis.nl/dsresource?objectid=69077

Bowker, G. C., & Leigh Star, S. (1999). *Sorting things out Classification and its consequences*. Cambridge (US) London (UK): MIT Press.

Brief van de minister van veiligheid en justitie (2012). Retrieved from https://zoek.officielebekendmakingen.nl/kst-29279-147.html

Friessen, M., Karré, P. M., & van der steen, M. (2011). *Zorg door de staat Gevolgen van gemeentelijke keuzes in de jgz*. Retrieved from http://jgz.captise.nl/Portals/0/PDF/Essay_Zorg_door_de_staat_compl.pdf

Gorissen, W. (2002). *Kennis als hulpbron: het gebruik van wetenschappelijk kennis bij beleidsvorming in de jeugdgezondheidszorg voor 4-19 jarigen*. University of Utrecht, Utrecht. Retrieved from http://igitur-archive.library.uu.nl/dissertations/1977547/inhoud.htm

Hacking, I. (1991). The Making and Molding of Child Abuse. *Critical Inquiry*, *17*(2), 253–288.

Hacking, Ian. (1986). Making-up people. In T. Heller & E. D. Wellbery (Eds.), *Reconstructing individualism, authonomy, individuality and the self in Western Thought* (pp. 222–236). Stanford University Press. Retrieved from http://www.icesi.edu.co/blogs/antro_conocimiento/files/2012/02/Hacking_making-up-people.pdf

Hensen, M. (2010). *Op weg naar een regionale aanpak kindermishandeling*.

Hielkema, M., de Winter, A. F., de Meer, G., & Reijneveld, S. A. (2008). *Project: Effectiviteit van vroegsignalering binnen het programma Samen Starten.* Retrieved from http://www.zonmw.nl/nl/projecten/project-detail/effectiviteit-van-vroegsignalering-binnen-het-programma-samen-starten/samenvatting/

Jaarverslag 2007 Inspectie Jeugdzorg. (2008). Utrecht.

Keymolen, E., & Prins, C. (2011). Jeugdzorg via systemen. De Verwijsindex Risicojongeren als spin in een digitaal vangnet. In D. Broeders, C. M. K. C. Cuijpers, & J. E. J. Prins (Eds.), *De staat van informatie*. Amsterdam: Amsterdam University Press. doi:10.5117/9789089643100

KNMG: EKD niet te breed toegangelijk maken. (2009). Retrieved from http://knmg.artsennet.nl/Nieuws/Nieuwsarchief/Nieuwsbericht-1/KNMG-Elektronisch-Kinddossier-niet-te-breed-toegankelijk-maken.htm

Latour, B. (1987). *Science in action: How to follow scientists and engineers through society*. Cambridge, Massachusetts: Harvard University Press, Cambridge, Massachusetts.

Law, J. (2008). On sociology and STS. *The Sociological Review*, *56*(4), 623–649.

Mathar, T., & Jansen, Y. J. F. M. (2010). Introduction. In Thomas Mathar & Y. J. F. M. Jansen (Eds.), *Health Promotion and Prevention Programmes in Practice: How Patients ' Health Practices are Rationalised , Reconceptualised and Reorganised*. Transcript Verlag, Bielefeld. Retrieved from www.transcript-verlag.de/ts1302/ts1302.php

Nederlands Centrum Jeugdgezondheid. (2007). Basis Dataset jeugdgezondheidszorg versie 2.0. Retrieved December 18, 2012, from http://vorige.nrc.nl/redactie/doc/bds.pdf

Nederlands Centrum Jeugdgezondheid. (2011). Inhoud voorstel 127.

Nederlands Centrum Jeugdgezondheid. (2013). Basisdataset Jeugdgezondheidszorg v.3.2.1.

NOS. (2010). Veel onterechte meldingen over kindermishandeling. Netherlands: Nos.nl. Retrieved from http://nos.nl/audio/135462-veel-onterechte-meldingen-over-kindermishandeling.html

Nouwt, S. ., & Hogendorp, J. (2010). Landelijke Verwijsindex Risicojongeren ingevoerd. Retrieved from http://knmg.artsennet.nl/Nieuws/Nieuwsarchief/Nieuwsbericht-1/Landelijke-Verwijsindex-Risicojongeren-ingevoerd.htm

RadarAdvies. (n.d.). Preventief Risicosignaleringsinstrument jongeren en overlast. Retrieved from http://www.radaradvies.nl/producten/preventief_risicosignaleringsinstrument_jongeren_en_overlast/521

Rijksoverheid. Wet Verwijsindex risicojongeren van kracht op 1 augustus 2010 (2010). Rijksoverheid. Retrieved from http://www.rijksoverheid.nl/documenten-en-publicaties/persberichten/2010/07/09/wet-verwijsindex-risicojongeren-van-kracht-op-1-augustus-2010.html

Rouvoet, A. (2007). *Alle kansen voor alle kinderen beleidsprogramma Jeugd en Gezin 2007-2011(verkorte versie)*. (Rijksoverheid.nl, Ed.). Den Haag. Retrieved from http://www.rijksoverheid.nl/documenten-en-publicaties/rapporten/2007/09/14/alle-kansen-voor-andere-kinderen-beleidsprogramma-jeugd-en-gezin-2007-2011-verkorte-versie.html

Star, S. L. (2010). This is Not a Boundary Object: Reflections on the Origin of a Concept. *Science, Technology & Human Values*, *35*(5), 601–617. doi:10.1177/0162243910377624

Star, S. L., & Griesemer, R. J. (1989). Institutional Ecology, "Translations" and Boundary Objects: Amateurs and Professionals in Berkeley's Museum of Vertebrate Zoology, 1907-39. *Social Studies of Science*, *19*(3), 387–420.

Tweede Kamer. Vaststelling van de begrotingsstaten van het Ministerie van Veiligheid en Justitie (VI) voor het jaar 2013 (2012). Tweede Kamer der Staten General. Retrieved from http://www.eerstekamer.nl/behandeling/20120918/memorie_van_toelichting_5/document3/f=/vj30e2quaryj.pdf

Van der Hof, S. (2010). Het elektronisch kinddossier: kansen en kantekeningen. In G. Munnichs, M. Schuijff, & M. Besters (Eds.), *Databases: Over ICT-beloftes, informatiehonger en digitale autonomie* (63rd ed., pp. 54–62). Den Haag: Rathenau Istituut. Retrieved from http://arno.uvt.nl/show.cgi?fid=113415

Van der Hof, S., Leenes, R. ., & Fennell-van Esch, S. (2009). *Framing citizen's identities: The construction of citizen identities in new modes of government in The Netherlands, research on personal identification and identitiy management in new modes of government.*

Van der Ploeg, I. (1998). *Prosthetic Bodies: Female embodiment in Reproductive Technologies*. Maastricht University.

Wet op de jeugdzorg (2005). Retrieved from http://wetten.overheid.nl/BWBR0016637/geldigheidsdatum_25-04-2010

Wet Publieke Gezondheid (2008). Retrieved from http://wetten.overheid.nl/BWBR0024705/geldigheidsdatum_12-12-2012

Willems, M., & Van der Heijden, M. (2011). *Provinciale Pilot Vroegsignalering risicojeugd 12-*. Retrieved from http://www.nogveiligerhuis.nl/UserFiles/File/thema_jeugd/Publicatie Spectrum Gelderland Vroegsignalering risicojeugd 12 min(1).pdf

Accepted.

To be published in Nadya Purtova, Samantha Adams, Ronald Leenes (Eds.) Under observation: The synergies, benefits and trade-offs of eHealth: Springer Publishers, Den Haag (2016, forthcoming)

Thesis Chapter III.

Profiling 'anomalies' and the anomalies of profiling: Digitalized risk assessments of Dutch youth and the new European data protection regime

Karolina La Fors-Owczynik

Abstract

A key component of the proposed data protection rules outlined in the General Data Protection Regulation (GDPR) is that any measures based solely on automated data processing that have legal effects on 'natural persons', including children, count as 'profiling'. Currently, the digitalized profiling of children in Dutch child-care policies has gradually gained prominence in efforts to detect or prevent child abuse and anti-social or delinquent behaviour. This chapter analyses how the proposed data protection rules will impact the current practices of profiling children and creating individualized risk assessments in the Netherlands. To illustrate the problems raised by such profiling, this paper analyses the professional use of three profiling registries: the Dutch Digital Youth Healthcare Registry, the Reference Index of High-Risk Youth, and the ProKid SI 12- system. Investigating the negative implications of the use of these and determining how these implications can be addressed by legal means is crucial to striking a proper balance between the interests of society, privacy and data protection, and individual children and families. Although each registry is meant to prevent problems and serve the 'best interests' of children and society, their use produces new risks, including the possibility for erroneous criminal prognosis, stigmatization, and discrimination. By drawing upon empirical data and legal analysis, this paper argues that the use of these technologies by authorities and healthcare providers in the Netherlands will challenge new data protection provisions and that it is therefore necessary to reframe the data protection regime to better protect "the best interest of the child" as established by the United Nations Convention on the Rights of the Child.

1. Introduction

On 25 January 2012, the European Commission released the draft proposal for the European General Data Protection Regulation (GDPR). This was a landmark event because the GDPR is intended to replace Directive 95/46/EC, which has been the primary legal instrument regulating data protection in Europe since 1995. Under the GDPR, the legal basis of data protection, as understood since the 95/46/EC Directive was adopted, would change remarkably. The latest (final) version of the GDPR was released on 15 December 2015 by the European Council, and includes proposed amendments made to the earlier text promulgated by the European

Parliament. For purposes of the analysis conducted in this paper, I rely on this latest (European Council) version.

In drafting new data protection rules, the European Commission chose to rely on two separate legal frameworks: one for the protection of 'regular personal data' (i.e. the GDPR) and one for the protection of personal data during criminal and judicial proceedings (a separate Directive). Therefore, together with the proposed regulation, the Commission introduced the Police and Criminal Justice Data Protection Directive. The latter would replace the 2008/977/JHA Framework Decision. Interestingly, the regulation and the directive establish separate legal bases for regulating commercial and public and security-related data, including specific rules for often criticised practices like profiling within these contexts.

Given these developments, this paper examines how the proposed data protection regime, when adopted and enforced, will be able to cope with the problems presented by profiling children on the basis of risk assessments[1]. For this purpose, the digitalized risk profiling practices of the Dutch government will be used as illustrations. Furthermore, the paper seeks to investigate what social problems, such as the possible negative implications for children's lives, emerge as a consequence of these risk profiling practices, and how these negative implications can be properly addressed by modifications to the proposed data protection rules.

Today, the preventative, digital profiling of 'anomalies' such as child abuse and anti-social or delinquent behaviour by children constitute prominent mechanisms that professionals in the Dutch youth healthcare, youth care, and criminal justice sectors rely on[2]. Connecting multiple digital databases and aggregating and sharing data of preventative import concerning children and other persons connected to them have been seen as optimal and efficient ways to orchestrate the prevention of abuse and undesirable behaviour. This digital transition has been bolstered by regulatory and administrative changes within the contexts of Dutch youth care and law enforcement. One such change took shape in 2013, when the administrative set-up of the Dutch police corps became more centralized, as 25 regional police units were reorganized into 10. A major transition affecting the Dutch youth care system occurred in January 2015, when the provision of professional care for children was transferred from provinces to municipalities. Although the new data protection regime, including the proposed legal specifications about profiling are not yet finalised, the proposed specifications about profiling are considerably improved as compared to those in Directive 95/46/EC. This paper analyses the implications of three risk assessment systems in light of the proposed rules, an analysis that is useful, on one hand, to assess the capacity of the new regime to deal with the problems raised by creating risk profiles of children and, on the other, to see what this could mean for future risk profiling cases of children by government systems. Furthermore, the choice to evaluate the new regime is motivated by the vulnerable (legal and social) position of children compared to adults and by the concerns scholars have raised with respect to the legitimacy of digitalization in youth care. Scholarly concerns relate to how the government will manage to keep up with controlling data flows and providing transparency as laid down by the Dutch Data Protection Act[3] and the European General Data Protection Proposal (Klingenberg & Lindeboom, 2013).

[1] By children, I mean in this article all persons between 0-23 years. This is a practical choice. I simply followed the definition used by the Reference Index High-Risk Youth, which uses the broadest age definition for a child among the three systems analysed here. Therefore, by this term I mean children assessed by any of the three systems.

[2] The Minister of Youth and Family: André Rouvoet explained in an interview (van Wijck, 2009), that during his 13 year carrier being an MP he experienced no discussion on the topic of child abuse, therefore how glad he was that the topic was finally put on the top of political agendas.

[3] Wet Bescherming Persoonsgegevens 2000 (Data Protection Act) Retrieved on 10th August 2014, from < http://wetten.overheid.nl/BWBR0011468>

This article is organised in four sections. Section two provides an overview of the three risk profiling systems, including a review of their advantages and disadvantages. Subsequently, section three presents relevant provisions of the current and the upcoming EU data protection regime with respect to profiling. After a few words on the methodology used in this research (section four), section five discusses key advantages of profiling systems as well as the main, scholarly criticisms raised with respect to digitalized profiling methods. Based on empirical findings, section six argues that the proposed data protection provisions will fall short of providing protection for children within the contexts of current risk profiling practices of children by the Dutch government. Additionally, these practices create new problems or risks for children related to the registration, daily use, and erasure of the risk assessments created and used for profiling purposes. After a discussion (section seven) on how law might provide protection for these side effects, section eight concludes in answering whether the new EU data protection assessments of risk profiling systems concerning youth would be better supplemented by a stronger focus on fundamental rights of children (as elaborated in the UN Convention on the Rights of the Child).

2. Overview of the three risk profiling systems

2.1. Digital Youth Healthcare Registry

The Digital Youth Healthcare Registry (DYHR, or Digitaal Dossier Jeugdgezondheidszorg in Dutch) is designed for the registration of healthcare information on children (and, indirectly, about their close families) between 0-19 years of age. This system has been used since 2009 nation-wide in The Netherlands. A set of Dutch laws provides the legal framework for the Digital Youth Healthcare Registry—for instance, Art. 5 of the Dutch Public Health Act (Wet Publieke Gezondheid, 2008), which prescribes the digitalization of health records. The Individual Healthcare Professions Act (Wet op de beroepen in de individuele gezondheidszorg, 1993) is a second law that applies to the DYHR. This act specifies confidentiality requirements for professionals regarding the sharing of patient data. The registry is also legally controlled by a third statute, the Act on Medical Treatment Contracts Acts (Wet Geneeskundige Behandelingsovereenkomst, 1994). This act defines conditions for accessing patients' files. The Dutch Data Protection Authority underlined the importance of the principle that sharing children's healthcare data for preventing child abuse must be proportionate. Because the DYHR is connected to the risk signalling system, the Reference Index for High Risk Youth, data sharing can and should remain efficiently minimized(CBP, 2007). The time limit for data retention in DYHR is 15 years.

2.2. Reference Index for High Risk Youth

The second system is the Reference Index for High Risk Youth (RI, or Verwijsindex Risicojongeren in Dutch), a large-scale risk-signalling platform connecting a variety of digital databases, youth care organizations and professionals. This platform allows for the digital exchange of risk signals about children and youngsters in the Netherlands between the ages of 0 and 23. When risk signals are shared, no information is shared other than the signal. Only the name of the child and the youth care organization concerned about the child is linked to the signal. This is done for the sake of privacy so that no confidential information is shared instantly with a risk signal. After two professionals of different organizations have signalled a risk about the same child, a certain 'alarm bell' goes off in the RI, and the two professionals need to

contact each other and share more information about the specific child. The legal basis of the Reference Index lies in the adjusted Dutch Youth Care Act (Wet op de jeugdzorg, 2010) and in the Law on the Reference Index High Risk Youth(Rijksoverheid, 2010). A large number of local systems are used nation-wide since 2010. All local RIs are set up in such a manner that each of them is also linked to a national system. In the national reference index all risk signals registered in local RIs are logged. A risk signal remains for max. seven years in the system. Although a risk signal can only be matched with other risk signals for two years, after that period a signal still remains visible for professional by being archived for 5 additional years(Oerlemans & Bruning, 2010).

2.3. ProKid 12- SI

The third system is ProKid 12–SI (pronounced 'ProKid twelve minus SI'), a system used nationwide since 2014 by the police to assess children aged between 0 and 12 years. A child's file comprises two parts: one column for the evaluation of the child and one for the assessment of his/her home address against four colour-coded risk categories. Each colour—from white to yellow, orange and red—demonstrates an increasing degree of risk. The evaluation of a child's home address involves the risk qualification (the eventual bad influence) of family members and other related persons living at the same address with the child. A colour in a child's file can change over time.[4] ProKid is controlled by a number of Dutch laws (Social Support Act, Public Health Act, Youth Care Act, the Compulsory Education Act, Police Act) that define responsibilities of state, provincial and local governments regarding the care of young people. The development of a 'comprehensive multidisciplinary chain approach for youth' underpins this legal framework. Part of this approach is a working process called "early identification and referral"(Goedee & Rijkers, 2010), introduced in 2007 to stimulate co-operation between the Dutch police and a primary youth care organization called Bureau Youthcare[5]. Until January 2015, this working process also provided a basis for ProKid[6]. Although according to Dutch penal law children under the age of 12 cannot be prosecuted, the aim of ProKid sets a precedent as it in fact carries out digitalized prevention work on children under the age of 12 years. Given ProKid is a system used by the police, the Police Data Act applies to the data processing and thus legitimizes this use. The time limit for retaining data in ProKid is set by 5 years.

2.4. Advantages of DYHR, RI and ProKid

The Dutch Digital Youth Healthcare Registry (DYHR) had been intended to replaces paper records and improves the healthcare 'image' of each child by using digital record keeping in which a more extensive set of categories are seen to offer improvement. A more elaborate categorization would help build a better view of a child, which would assist in preventing child abuse cases. In this respect, the possibilities for a doctor or nurse to detect the physical or

[4] Controversies around these systems also provide reasons for thorough analysis. For instance, the Dutch government's ability to safeguard transparency and the proper protection of personal data had already been raised as focal points for investigation in light of such IDM systems (Klingenberg & Lindeboom, 2013). These issues raise further controversies as to how to orchestrate legally, administratively and technically the preventive profiling of children in each of these sectors. Controversies also surround the vividly disputed potential negative implications the transition in the youth care and law enforcement sector might cause, as well as the government's increasing push to exchange data(Goedee & Rijkers, 2010) across sectors.

[5] As of January 2015 Bureau Youthcare organizations are abolished and their tasks are taken over by other certified youth care organizations and the municipalities.

[6] As of January 2015 Bureau Youthcare organizations do not exist in their old form anymore in The Netherlands. Due to the decentralization process in youth care, the tasks earlier performed by Bureau Youthcare had been redivided and redistributed between newly certified youth care organizations and city halls.

psychological implications of family problems on a child is easier and more visible for a variety of healthcare professionals who have access to the record. The link between the DYHR and the Reference Index (RI) High Risk Youth helps to improve communication and information sharing from the DYHR in regard to the signalling of such risks as abuse or domestic violence associated to a child. A major impetus for the design and installation of the RI was the need to improve information exchange between different youth care professionals and organizations when professionals were aware of problems concerning the same child. The risk signalling 'alarm bell' infrastructure of the RI among professionals, when it signals correctly, can be considered the primary advantage of the system.

ProKid SI 12- is a digital system to prevent problems that children might suffer from in their closest social environment and problems that children can cause to others by their anti-social or delinquent behaviour. When performed accurately, enhancing prevention by digital means and can save children from potential further harm. This is valued as the prime advantage of ProKid.

2.5. Disadvantages of DYHR, RI and ProKid

Although the new European data protection regime has not yet been accepted and used as a lens to assess preventative digital risk-profiling practices in children via DYHR, RI and ProKid, the systems have already earned the critical attention of scholars. The profiling[7] of children by the Digital Youth Healthcare Registry (DYHR), which had previously been called the Electronic Child Record (ECR), received public[8] and academic criticism in its primary stage. The DYHR is based on a 30-page description of more than 1000 standard categories called the Basic Dataset (van Dijk, 2008), according to which risks related to children are registered[9]. The main Dutch professional organization responsible for healthcare, the Royal Dutch Medical Association (in Dutch: Koninklijke Nederlandsche Maatschappij tot bevordering der Geneeskunst—KNMG)[10] raised its concerns specifically with respect to the accessibility of DYHR profiles and argued for strict limitations. Van der Hof and Keymolen highlight such side effects of profiling by the DYHR what they call an "identity turned into stone". By this they refer to the consequence of retaining data for 15 years in a DYHR profile, which can cement a digital snapshot image of a child. Simply by remaining in the file for 15 years, this image can negatively influence a child's life in the future. By the "stigmatized identity", Van der Hof and Keymolen also note that the digital record can influence professionals in ways that at times could hamper a face-to-face dialogue with a child: *"preconceived opinions can stand in the way of an open and fair contact"* (2010: 320).

Profiling practices by the Reference Index High Risk Youth have also been exposed to criticism. The Reference Index is a risk signalling system or *"a spider in the web"* (Keymolen & Prins, 2011) to which a large variety of youth care professionals are connected by posting only risk signals of a child that are based on risk profiles. The National Reference Index is a

[7] Despite a newly emerging trend where online profiling gains importance[7], the risk profiling of children by Dutch government technologies such as the Digital Youth Healthcare Registry, the Reference Index High Risk Youth and the ProKid 12- SI system occur against an already defined set of criteria, and those criteria should be set by standards in healthcare, youth care or law enforcement in The Netherlands. Each match between a profile and a child is regularly nominative and shows that a child is associated by name to a risk category.

[8] Elektronisch Kinddossier eind 2010 ingevoerd - < http://webwereld.nl/beveiliging/42055-elektronisch-kinddossier-eind-2010-ingevoerd#>

[9] Each category definition emerges as natural or innocent to the person it characterizes, yet when personal attributes captured within categories become benchmarks upon which decisions of exclusion or inclusion are made, the BDS categories can also be seen as 'carriers' of certain selective politics (Suchman, 1994).

[10] For more information about this, please see: <http://knmg.artsennet.nl/Nieuws/Overzicht-nieuws/Nieuwsbericht/39762/KNMG-Elektronisch-Kinddossier-niet-te-breed-toegankelijk-maken.htm>

single umbrella system under which all local reference indexes hang. The system is designed in such a way that if two professionals post a risk signal about the same child, a match emerges as a certain alarm bell indicating that the two professionals need to initiate contact and discuss the child's case. With each risk signal posted in a local system, a copy of that signal simultaneously enters the national reference index. Keymolen and Broeders identified a shortcoming of this set-up by showing that it allows for *"sharing information without fully grasping the context of this information"* (2011) among professionals. Van der Hof raised her concerns regarding the extensiveness of the Reference Index. According to her, the Reference Index can prevent those children who are most in need from receiving adequate help as a consequence of the requirements that professionals should abide by when screening children(2011).

ProKid SI 12- is primarily a prevention system implemented by the Dutch police to assist in digitalized risk-profiling work on children. The colour-coded profiles for ProKid are developed by behavioural scientists(Nijhof, Engels, & Wientjes, 2007): white, yellow, orange and red correspond to an increasing gradation of concern in relation to a child should he/she be a victim, a witness of violence or a perpetrator. Both children and their home addresses can be assigned colour codes. If the colour of the address darkens, the colour code of the child also darkens. This colour code shows a growing risk in the child's social environment; for instance, if a child's family member has a police record, this qualifies as a direct bad influence on a child's development. Registration can remain in the system for a maximum of five years. ProKid has been operational nationwide since 2013 and, as such, it is unparalleled[11]. The risk-profiling practices of children by ProKid have been exposed to fierce criticism. For example, in Schinkel's view, ProKid is a technology that materializes a penalizing pressure or "pre-pressure"(2011) on children who are exposed to what Lyon calls *"surveillance as social sorting"* (2003). Moreover, Bruning *et al.*, advising the Dutch Child Ombudsman, argued for broader transparency for parents regarding how a risk calculation is made in ProKid and that professionals should balance between risk and protecting factors as their top priority when assessing a child(2012).

Schinkel formulates an overall criticism regarding profiling by each of the three above-mentioned technologies and the developments accompanying their introduction within Dutch youth healthcare, youth care and law enforcement in general. According to him, these systems epitomize certain forms of *"technologies of security"* (Foucault, 2004). In Schinkel's view, there are two main negative effects of profiling by these systems: the extensive *"normalizing effects on the Dutch population"* and the significant contribution of these systems to the *"prepressive construction of a risk population"* (2011).

Although all of these criticisms are highly valuable and necessary, they did not address the practical implications the Digital Youth Healthcare Registry and the Reference Index High Risk Youth have on the General Data Protection Regulation and, more specifically, the practical implications of ProKid on the Police and Criminal Justice Data Protection Directive. To demonstrate these implications, the following section reveals an analysis based on empirical insights from professionals working in different cities and institutions in the Netherlands using the DYHR, the Reference Index or ProKid.

[11] Minister van Veiligheid en Justitie (2012), 29 279 Rechtsstaat en Rechtsorde Nr. 147 Brief van de minister van veiligheid en justitie aan de Voorzitter van de Tweede Kamer der Staten-Generaal, Den Haag

3. Profiling children in light of current and new data protection rules

The Digital Youth Healthcare Registry and the Reference Index High Risk Youth fall under the 95/46/EC Directive and after the proposed Regulation comes into effect, this new regime applies to the processing of data by means of both systems. Given that data from the ProKid SI 12- system is not exchanged in a cross-border setting, only very limited parts of the Framework Decision 2008 can be seen applicable. Yet, when the Police and Criminal Justice Directive becomes enforced, ProKid will fall under this regime. For this reason, the relevant provisions of this new regime will also be analysed.

Although the 95/46/EC Directive is implemented in the Netherlands through the Dutch Data Protection Act, the directive "lacks child specific rules" (Van der Hof, 2014). Art. 21, for instance, only defines specifications regarding the sharing of children's healthcare data (La Fors-Owczynik, 2015). In light of the current data protection legislation, this lack of child specific rules constitutes great challenges when looking for legal safeguards for children from the side-effects of digitalized profiling practices, such as the risk profiling performed by Dutch government agencies.

From the perspective of profiling prescriptions concerning how data shall be processed is also crucial. Art. 5 of the 95/46/EC Directive prescribes with respect to data processing, leading principles such as lawfulness. Yet, it allows member states to specify conditions for lawful processing. On the contrary, GDPR specifies conditions for lawfulness and fairness by including principles, such as transparency and data minimisation, and by defining liabilities for the controller.

Art. 7 of the 95/46/EC Directive specifies conditions for lawful processing, such as the data subject's consent or the necessity criterion of data processing (*i.e.*, for public interests). GDPR, however, adds to these criteria the balancing of interest criterion. By the time the GDPR is in force, the latter criterion is essential to rely on when it comes to the risk profiling of children by government systems.

Arts. 10 and 11 of the 95/46/EC Directive are also of utmost importance for risk profiling practices of children because these articles specify the information obligation of the controller towards the data subject. The GDPR builds on these specifications, but it introduces a far broader set of obligations for the data controller in Art. 11, Art. 12, and Art. 14. Art. 12 sets out conditions for transparency when the data subject exercises his/her rights. Moreover, Art. 14 specifies that the data controller shall inform the data subject about the data processing. For instance, with respect to the storage period of data, it also prescribes the "right to lodge a complaint to a supervisory authority" for the data subject. Art 15 of GDPR follows up on Art. 14 and defines the right of access of the data subject. As a precondition to the right of access, Art. 18 prescribe the right to data portability, meaning that upon request of the data subject the data controller shall facilitate the transfer of the data subject's data from one system to another. The right to data portability or the right to lodge a complaint do not exist in the current directive. Yet, Art. 13 of the 95/46/EC Directive provides derogations for the information obligation of the controller and for the right of access of the data subject. Art. 14 of GDPR expands conditions for derogations for the information obligation and for the right of access. The latter derogations, when the GDPR will be in effect, would also be applicable for all three risk-profiling systems of children analysed in this article.

The 95/46/EC Directive specifies general provisions regarding profiling in Art. 15. It granted *"the right to every person not to be subject to a decision, which produces legal effects concerning him and which is based solely on automated processing of data intended to evaluate certain aspects related to him…"*.

GDPR Art. 20 specifies much stronger provisions with respect to profiling. First, that *"the data subject shall have the right not* to *be subject to a decision based solely on automated*

processing, including profiling*, which produces legal effects concerning him or her or similarly significantly affects him or her. ..[and that profiling] is based on the data subject's explicit consent".*

However, compared to the June version (2015) of the GDPR, in the December version (2015) of the text certain specifications regarding profiling have been erased. In the June version Art. 20 included, for instance, that "*profiling that has the effect of discriminating against individuals on the basis of race or ethnic origin, political opinions, religion or beliefs, trade union membership, sexual orientation or gender identity, or that results in measures which have such effect, shall be prohibited.*" Moreover, prescriptions have also been erased relating to that "*profiling which leads to measures producing legal effects concerning the data subject or does similarly [and] significantly affect the interests, rights or freedoms of the concerned data subject shall not be based solely or predominantly on automated processing and shall include human assessment, including an explanation of the decision reached after such an assessment.*"

The latter two specifications, if kept intact in the December version of the GDPR, could have further fostered the protection of citizens against profiling, including children, via the GDPR and also compared to the relevant prescriptions of the 95/46/EC Directive. However, the final version of Art. 20 lifted the limitations of the Directive, which specified that measures stemming exclusively from 'automated individual decisions' constitute profiling. The new regulation expanded the scope of protection by involving any measure of profiling that has legal effects on 'natural persons', including children. Although Art. 20 generally prohibits measures based on automated profiling, as Kuner critically noted, it includes exemptions that are "broad and ill-defined" and could potentially lead to harmonization problems and excessive use(2012). Furthermore, Costa and Poullet highlight that the regulation shifted from the conception of profiling that is the "classical automated individual decision" and refers to data that is directly related to an individual to automate reasoning regarding that person(2012).

Although the complete prohibition of profiling children has been deleted from the final form of the regulation(Hornung, 2012), it introduced another new legal safeguard: the data subject's consent to profiling. In line with this, the *"data processor must ensure that distinguishable conditions exist for the data subject to consent to profiling"* (ibid, 2012: 259). The introduction of this new consent is different from the consent to data processing, which was first established by Arts. 7 and 8 of the 95/46/EC Directive. The risk assessment systems under study are designed to score children against risks; each system has a legitimate aim that is cemented by law. If the GDPR is in force, Art. 20(1a, b) allows profiling if such activity is set by Union or Member State law. Therefore, because risk profiling by the three systems is set by Dutch law, the data subject's consent to profiling by these systems would not be applicable. As Koops argues, for citizens, it is impossible to opt out of data processing by government systems because citizens cannot simply choose a different government(2014).

Beyond derogations as to the prescriptions of GDPR by national law, Art. 21 of the GDPR also defines restrictions from the rights and measures laid down by GDPR, if data processing is aimed at safeguarding national security, defence, public security, or 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"*.

When GDPR is enforced, all of the provisions discussed above will apply for DYHR and the Reference Index High-Risk Youth.

Given that the ProKid system is a national police system, as mentioned earlier, it falls under the Dutch Police Data Act. Due to its national character, only limited parts of the Framework Decision 2008/977/JHA are applicable. For instance, Art. 3 defines the requirements for data use by law enforcement authorities including its proportionality,

lawfulness and legitimate purpose. However, after the Police and Criminal Justice Data Protection Directive is implemented in Dutch law, the relevant provisions will also be applicable for data processing activities performed by the ProKid system. The Directive specifies that profiling by "means of automated processing" should be prohibited unless national law provides for it otherwise (Art. 27). During such profiling practices, *"suitable measures to safeguard the data subject's legitimate interests"* must be ensured. According to the Dutch government, the main benefit of the EU Proposal on the Police and Criminal Justice Data Protection Directive with respect to profiling remains *"mainly in the transparency obligations [Art. 28] and Art. 14 deserves further attention in this context"* [12]. This is a fair observation, given that the directive allows for extensive options where profiling practices via national laws can flourish.

4. Methodology

The methods applied in researching the issues addressed in this article encompass both legal desk-research and analysis and empirical research.[13] In combining both methods, this research is staged in the tradition of science and technology studies and more precisely, actor-network theory. This approach is particularly valuable for the issues addressed in this article, given that it allows a better understanding of how the unintended implications or risks of using digital risk assessment technologies occur and what these implications can mean for children and families in the current and new data protection regime. The empirical data are collected with 18 semi-structured interviews that the author conducted with professionals using one of the three systems in different cities of the Netherlands. The interviewees were selected on the basis of a set of predetermined criteria (among them were professionals that had been involved in the design process or were daily users of these systems). The selected interview quotes presented below show the unforeseen analysis and typical implications that can arise as a consequence of the design and daily use of these systems. In the discussion, these implications are assessed against the background of the current and upcoming data protection regime. The quotes aim to demonstrate two things. First, the current text of the data protection regime could lead to controversies regarding the risk profiling of children. Second, the examples also depict controversies inherent in the design and use of risk profiles.

5. Problems raised by profiling systems generally

Although profiling citizens has long been a delicate subject within data protection discussions(Hildebrandt, 2008; David Lyon, 2001; Rubinstein, Lee, & Schwartz, 2008; Van der Hof, Leenes, & Fennell-van Esch, 2009), its importance has only grown with the development of an extensive set of Internet-based and inter-connectable digital technologies and ubiquitous systems. These technologies are seen as the means to increase opportunities for different forms of success in different fields and disciplines. Ubiquitous systems are regularly installed to collect a broad range of behavioural information on persons(Canhoto & Backhouse, 2008; Manders-Huits, 2010; Van Eijk, Helberger, Kool, Van der Plas, & Van der Sloot, 2012).

---

[12] Brief van de Staatssecretaris van Veiligheid en Justitie over het 'EU-voorstel: Richtlijn bescherming persoonsgegevens bij gebruik door politiële en justitiële autoriteiten (COM(2012)10) en EU-voorstel Verordening algemeen kader bescherming persoonsgegevens (COM(2012)11)' (2013)

[13] Part of the empirical data in this article can also be found in K. La Fors-Owczynik & G. Valkenburg *'Risk identities: constructing actionable problems in Dutch youth*', in Digitizing Identities: Doing Identity in a Networked World (Eds.) Van der Ploeg, I. & Pridmore, J. (Routledge, 2015). Part of empirical data concerning ProKid can also be found in K. La Fors-Owczynik Minor protection or major injustice? Children rights' and digital preventions directed at youth in the Dutch justice system [2015] 31 Computer Law and Security Review 651-667

Such information is then used to design and offer more 'tailor-made' services for citizens, including commercial(Benoist, 2008; Pridmore, 2012; Zarsky, 2010), medical(Jansen & de Bont, 2010; Oudshoorn, 2011), judicial(Hoogstrate & Veenman, 2012; Koops & Leenes, 2005), employment-oriented(Henman, 2004; Leopold & Meints, 2008), online or social media-related services(Leenes, 2010). Profiling and profiling technologies, therefore, are widely regarded as tools to create opportunities for 'improving' the image of the profiled subjects by aggregating data about them in different ways that can depend on a large variety of interests.

However, beyond the benefits that each digital profiling practice is set to achieve, substantial academic literature has already directed attention towards the shortcomings of these practices. Hildebrandt notes, for instance, that abuse is not the major problem with profiling, *"but the fact that we have no effective means to know whether and when profiles are used or abused"* (2008: 318). Shoemaker highlights the data subject's lack of control over the type of profile that is made about him/her: an image of the profiled person emerges without his/her "desired and expected input into the process" (2009: 14). Similarly, Prins advocates for establishing more control for the profiled subjects by providing more transparency about the profiling processes(2007); she also raises concern with respect to the 'responsibility' of data processors towards data subjects. She claims that within the current largely complicated web of digital systems, it has become nearly impossible for a citizen to find the right data processor who, in that moment, is responsible for processing a persons' data(2014: 56). Furthermore, Van der Hof and Prins argue specifically about commercial profiling and the ways in which data are aggregated and projected onto customers. They also describe how profiles are "personalized" (2008) and used to steer consumers' choices in ways that are opaque to those subjected to these practices. A major concern of Koops and Leenes is that profiling practices—because they occur without the involvement of the subject—are manipulative and at times are even confining to persons' autonomy(2005). McKenna argues similarly and advocates for considering where the boundaries remain when it is argued that eventual crimes can be prevented by advanced profiling techniques: "it comes down to the issue of personal autonomy of the individual and the need for there to be awareness of what is happening" (2012: 15). Schermer raises among others that a major concern of profiling is that individuals are often judged on the basis of group characteristics and not on their own characteristics(2011). This could lead to incorrect or discriminative decisions what he explains as the "de-individualisation" effect of profiling. Gray and Citron also formulate concerns regarding the large-scale behaviour-steering effects of massive profiling techniques in a post 9/11 US environment. They argue, for instance, that individuals with different religious and cultural backgrounds are more sensitive to profiling and surveillance in general. They explain that individuals in the US often perform "self-censoring" to prevent becoming suspected persons of national security interest(2013). Children's rights scholars further argue about profiling practices by systems such as ProKid that they have a "stigmatising" effect(Bruning *et al.*, 2012). Yet, this risk is not limited to ProKid. For instance, if a risk profile from the DYHR or a risk signal from the RI is shared, the use of these data can also discriminatively affect a child.

A common denominator in all of the criticisms regarding profiling relates to the fact that whatever the purpose of profiling might be, as a form of surveillance(De Vries, 2010; Foucault, 1977; Lyon, 2006; Schinkel, 2011), profiling continuously produces asymmetrical power relationships between profilers and those subjected to profiling. This asymmetry emerges immediately in favour of the profiler by the time he or she gathers data about its subject. The more data that is gathered about the profiled persons within these relationships, the more 'hegemonic' a profiler can become. Several attempts have been made to legally empower profiled persons—for instance, by assigning "property rights" (Prins, 2006, 2010; Samuelson, 2000; Sholtz, 2000) to them or by potentially establishing a 'fundamental right to identity'(De Hert, 2008; Gutwirth, 2009; Prins, 2007). Lately, for example, GDPR introduced the possibility

of fining companies or other profilers who unlawfully collect data about a person[14]. Furthermore, data protection principles such as 'informed consent' and the right of a person to 'individual self-determination' can all be regarded as legal constructions to empower the person being profiled and to shrink his or her hierarchical distance in relation to the profiler. Yet, in an era of ubiquitous computing, profiling has increasingly become a manner of gathering enormous amounts of information about persons simply because— for instance, as Van der Ploeg argues about biometric sensing technologies at airports—persons in these profiling practices are increasingly seen as being "available" (2010). When not their name per se, but rather information about their behaviour, biological traits and habits are of more interest, then the mechanisms of legal empowerment seem to fall short in providing adequate counter balance. Because, profiling today has increasingly shifted away from its classical form - when data about a specific person was gathered to provide more 'personalized' services for him/her - towards the previously mentioned more group-oriented and typology-producing practices where the profiled subject can remain anonymous, the General Data Protection Regulation (GDPR) aims to tackle the new challenges(De Hert & Papakonstantinou, 2012) inherent in these new profiling practices. Practice shows however that challenges remain also concerning the classical form of profiling practices, especially in regard to children and digital risk-assessment practices by the Dutch government.

6. Problems or 'anomalies' raised by risk profiles in light of the changes brought by the GDPR

6.1. Constructing[15] risk profile data

What risk?

In light of the GDPR, when we take a closer look at the perception of risks by professionals a significant shortcoming of all three risk-assessment systems can be identified. To assess what counts as a risk in practice, it is essential to evaluate the implications of a digital risk registration from the perspective of the (current and the new) data protection regulation. Professionals explain that to define and construct what counts as a risk within their systems is a major difficulty in their daily work. A nurse, for example, working with the Digital Youth Healthcare Registry explained the following:

> "…it is often difficult to fill in the risk-assessment form or to risk-score children because there is no clear definition of risks. For instance, a 'sleeping problem' of a child can be just that, but it can also be a symptom of issues between the parents; or it can be caused by cultural elements that just differ between one family and another." (CB-nurse, city D)

A notification (often a letter) to the parents of a child must accompany any risk registration within the Digital Youth Healthcare Registry notification by law.

A doctor from another city shares her working method regarding how she indicates a risk:

> "If you look at the list [of children], you first see the risk items and you will not see regular issues. While say a mother is crying to me that she cannot manage to breastfeed. We have just been talking about this. Then, I would not register this as a risk because she is not a risk mother.

[14] For this prescription, see ECJ, Luxembourg, 13 May 2014, C-131/12

[15] Here, the word construction certainly does not intend to suggest that risks are made up of thin air, but the risks within the administration of professionals become existent, noticeable and actionable for others through their digital registration.

> But, I want to remember this issue and I think it is useful that this issue is indicated in red [as other risks] in the child's file because during the next consultation another colleague will check it together with other risks." (CB-doctor, city A)

The latter quote suggests that when an issue is indicated as red in a child's digital file, this could steer the attention of any colleague who views files towards those files, which contain red check-marks, including the particular baby's file mentioned above. This occurs because the digital files are set-up in such a manner that a red check mark in a child's file usually provides a risk indication and would primarily catch the attention of professionals. Yet, at the same time, it is difficult for a colleague who opens the files to determine whether a 'red check-marked' file constitutes a 'real risk' or only 'highlighted issues'. Therefore, the conclusion can be drawn that transparency regarding what a risk is or what a 'risky issue' constitutes often remains a puzzle for professionals who view children's digital files.

The two excerpts above both demonstrate that the definition of a risk registration can remain unclear even to those professionals who handle a child's data. Registering a risk is not always that complicated and risk signs are not always that ambiguous because not all doctors and nurses may find the registration of different types of risks difficult. Yet, the two quotes raised above show that a risk signal can easily obscure what the difficulties are and the professional decisions leading up to a risk sign in a child's digital profile. In this regard, uncertainty regarding what constitutes a risk can still be regarded as an elementary problem that is not primarily about abiding by the rules of profiling as set by the 95/46/EC Directive and in the future by GDPR, but about how to conduct profiling under these conditions. In line with this, evaluating the extent to which the 'principle of data quality' is enforced (as set by Art. 6 of the 95/46/EC Directive) is also necessary. Moreover, for future cases, when the GDPR will already be in force, the uncertainty regarding what constitutes a risk would challenge Art. 5 and Art. 6 of the GDPR. Additionally, the data controller's obligation to be transparent regarding the processing of data, especially towards a child (Art. 12 GDPR) would also be challenged. Overall, the above issues are not something the GDPR, even when enforced in the future, can adequately address alone because the regulation beyond the essential principles of proportionality, subsidiarity, fairness and lawfulness does not prescribe specific conditions that can lead up to the registration of digital data, which in our case is a risk registration about a child. Therefore, when professionals have difficulties determining what type of a digitally indicated risk is associated to a child, the extent to which digitalized prevention is always performed in the best interest of the child needs legal scrutiny. During this scrutiny, GDPR prescriptions could desirably be complemented with children's rights perspectives, such as the child's right to privacy and the child's best interest.

Funding for registering risks?

Ambiguity regarding risk constitutes a common problem, and can lead to what the Dutch government coined recently as an 'overreaction to risk within the Dutch youth care (Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, 2013). Ambiguity regarding what a risk can be within digital registration work is largely a consequence of simplifying the term 'risk' into a technological sign. Notably, the digital risk data/sign after being transferred strips off the originating problem from its exact context for a professional, who only receives and views the risk signal on a monitor. The registration of risks, for instance, in the Reference Index High-Risk Youth can also be surrounded with certain circumstantial biases. A local Reference Index manager shares details regarding her work in a given Dutch city as follows:

> "Since the end of 2009, there have been new funding conditions in [city name] … The conditions are as follows: organizations have to report to AMK and the Reference Index if they receive funding and are busy with youth, education, coaching or policy. If they do not report

about such issues, there is a good chance that such an organization (a kindergarten or other organization concerned with the well-being of children) loses its funding provided by the municipality. That is a push, so that all such organizations report about child issues to the Reference Index. We, as Reference Index, have to check whether they do such a reporting and are entitled to get their funding. 550 organizations received funding from municipality units, and we need to control them, whether they register risks or not and whether they get in touch with each other." (RI manager, city A)

The above insight shared by a manager demonstrates that the registration of risks in the Reference Index in some places[16] is influenced by the ways in which financing is allocated to the institutions connected to the Reference Index. If posting a risk signal can be regarded as a representation of care, then the ways in which this care at certain times and at certain places is steered both financially and administratively depicts a strict control of processes. Keymolen and Broeders argue that a mix of care and control is present in profiling practices performed by the Reference Index(2011). As the above quote demonstrates, a financial (or existential) motive can also push professionals to actively register risks in RI in a given city[17]. Questions arise, however, regarding the extent to which this administrative set-up serves the best interest of the child as provided by the CRC. Furthermore, the extent to which this financial motive to register a risk in a child's file is in line with principles set by Art. 6 of the 95/46/EC Directive is important. Under the proposed GDPR, cases of financial steering in the risk registration are troublesome given both the data minimization principle and the transparency principle (the data controller's obligation to inform the data subject of the conditions related to the data processing, in particular, when the data processing concerns children). However, perhaps an even more serious issue arises as to the general capacity of the GDPR to circumvent or fight the emergence of such financial biases within risk-profiling practices as those mentioned above. This is a severe issue because it cannot be identified with certainty, whether the main motives behind submitting a risk signal were only to serve the best interest of the child or to serve rather managerial and even existential interests of youth care agencies. It is at this point that the UN Convention on the Rights of the Child could afford additional protection in that it requires an assessment that is broader than merely data protection-related issues.

Unfair profiling?

The preventative, colour-code based registration of risks in ProKid happens through incident codes coming from two other strictly law enforcement databases: the Basic Facility for Law Enforcement (BFLE, or Basisvoorziening Handhaving in Dutch) and the Basic Facility for Forensic Investigation (BFFI, or Basisvoorziening Opsporing in Dutch). Incident notifications from these systems are crosschecked with the addresses of children already registered in ProKid. When an incident involving a child (so far unknown by ProKid) occurs, that child is registered at his/her home address. Yet, not all of the addresses of close family members of a child are 'viewed' in the system:

"Address changes in the [ProKid] system are not connected to changes in the municipal registry[18]. When a police officer reports on an address, [the data] are checked automatically against the municipal registry. However, if parents divorce and move to two different addresses and they arrange co-parenthood, the child is usually registered only at the mother's address. So,

[16] The financial steering of risk registration in the Reference Index High-Risk Youth is not a nationwide phenomenon, but it depends on the choices local governments make.

[17] Certainly, this observation only applies to the specific city where the interviewee coordinated and managed the registration of risk signals by all partner organizations linked to the system.

[18] In the Netherlands, municipalities maintain the addresses of all their inhabitants through central registries.

> if a problem occurs at the father's address, ProKid unfortunately misses out on that." (ProKid manager, city B)

Although the goal of ProKid is to provide a picture that is as complete as possible about the child, the very set-up of the system seems to unfairly profile children because children do not receive equal attention. Those whose family members live at the same address receive more attention than those whose family members live at addresses that are different from the child's. Elsewhere, this has been called "a technological solidification of the social norm that children live with their married parents" (La Fors-Owczynik & Valkenburg, 2015). Given this phenomenon and refraining from advocating for the inclusion of more addresses in a child's file, it would be worth discussing the extent to which the profiling of children by ProKid occurs fairly and lawfully, as set by Art. 3 of the Framework Decision 2008/977/JHA. After the Police and Criminal Justice Data Protection Directive is ratified, the principles of fairness and lawfulness will remain crucial and will be prescribed by Art. 4. Therefore, the capacity of the directive in addressing such inconsistencies in risk profiling and data aggregation, as the above quote demonstrates, is worth debating. Moreover, the extent to which unfair profiling falls entirely within the capacity of the Directive and whether it could be complemented with children's rights assessments from the perspective of "the best interest of the child"(Art 3. of the CRC) is also worth debating.

The above examples demonstrate that assigning a risk profile to a child is not without controversies, which often renders the extent to which pivotal principles of the GDPR and the Police and Criminal Justice Data Protection Directive are enforced in relation to profiling and data processing disputable. The next section, however, demonstrates that using risk profiles raises additional issues.

6.2. Using risk profile data

No option to register improvements.

When using the Digital Youth Healthcare Registry, the built-in norms in the system, at times, not only to steer(Oudshoorn, 2011), but also to dominate and limit professionals' choices:

> "Many professionals who have been working for years within youth healthcare notice, for instance, that they cannot register signals in the system that reflect that things are going well for the child. I find it to be frustrating that I can only register negative things, only risks, and not that the kid is doing well[19]**.** The system only allows you to record risks—for example, that the child is hyperactive. It is as if children can only have problems. If things are going well for the child, then I would like to register that, but I cannot." (CB nurse, city D)

This quote shows that the Digital Youth Healthcare Registry is not only a healthcare system but also a de facto public safety instrument that occasionally overshadows features that a regular healthcare system would need to address, such as the possibility of registering improvements in one's healthcare status. Because registering positive developments about a child is unavailable in the system, the use of risk profiles in DYHR raises questions regarding how the socio-technological set-up of the DYHR fosters principles relating to data quality as laid down by Art. 6 of the 95/46/EC Directive. Furthermore, in light of the quote, it can be discussed, how the principles of fairness and transparency as specified by Art. 5 of the GDPR would be of assistance for similar cases of risk profiling children. Furthermore, the inability to register good things in a child's file raises questions regarding the extent to which the features of the DYHR

[19] This phenomenon has been raised as a problem by 2/3 of the interviewed youth healthcare professionals.

serve high-quality public healthcare, as required by Art. 3 of the Dutch Public Health Act (Wet Publieke Gezondheid, 2008) or the "best interest of the child" as laid down by the UN Convention on the Rights' of the Child.

No distinction between perpetrators, victims and suspects.

When using risk profiles in the ProKid system, the same colour code can be assigned to victims, witnesses or perpetrators. For instance, the colour yellow depicts a profile, in which a child has been registered '3-9 times' either as a victim or as a witness. Yellow is also the colour code of a child who has been registered once as a suspect of a light incident'(Abraham, Buysee, Loef, & Van Dijk, 2011).[20] A professional explains the following information concerning how a perpetrator's profile influences the risk profile of an eventual child witness:

> "Many times, you see, the mother is divorced and has a child, and the child gets a report as being hyperactive. Then, later, the mother starts a new relationship with a man, who moves in at the same address. If the mother's new boyfriend, for instance, already has a police record or has been involved in domestic violence, this creates a high risk factor for the child (especially if he/she sees something similar). The child lives at one address with this man. Therefore, the yellow colour of the address [in the child's record] will turn into orange [...]" (ProKid manager, city B)

This set up of the ProKid system, however, if enforced, would not meet recital 18 of the Police and Criminal Justice Data Protection Directive, which specifically states that:

> "a clear distinction should be made between personal data on suspects, persons convicted of a criminal offence, victims and other third parties, such as witnesses, persons possessing relevant information or contacts and associates of suspects and convicted criminals."

Although the correlations designed in the colour-coding system of ProKid between perpetrators, victims and witnesses are grounded in behavioural science, using the same (coloured) risk profile on a child witness, victim or perpetrator seems problematic in light of recital 18. Furthermore, the fact that no distinction is made between perpetrators, suspects and victims in the classification system of ProKid also collides with the enforcement of children's rights, which require that "no child shall be subjected to arbitrary or unlawful interference with his or her privacy" (Art. 16).

Despite certain existing standards for police officers working with ProKid regarding the types of risk profiles to share with youth care professionals[21], exchanging risk profile information is not straightforward in practice. For instance, a standard prescribes that red colour-coded profiles of children—the colour that signifies perpetrators—need to be submitted to Bureau Youthcare[22](Nijhof *et al.*, 2007)(Nijhof et al., 2007). Although the standard does not show that a child's file and colour code in ProKid can influence the file of another child, this

[20] About further descriptions of colour codes in ProKid please see: Abraham, M., Buysee, W., Loef, L., & Van Dijk, B. *Pilots ProKid Signaleringsinstrument 12- geëvalueerd Pilots ProKid Signaleringsinstrument 12- geëvalueerd* (DSP-groep, 2011)

[21] In 2007 to facilitate collaboration between the Dutch police and Bureau Youthcare, a flagship organization within Dutch youth care, which collaboration also forms the basis for ProKid: "Early identification and referral" policy had been introduced. About this, see more in: Goedee, J., Rijkers, A. *Zorgsignalen van de Politie: Over het werk process 'Vroegsignaleren en doorverwijzen' tussen Politie en Bureau Jeugdzorg* (Ministerie van Jeugd en Gezin, 2010)

[22] The interviews that provided empirical material for this article were conducted before 2015. As of January 2015, as a consequence of the administrative reorganization of Dutch youth care Bureau Youthcare organizations do not exist anymore, but their tasks are redistributed to municipalities and newly certified agencies of youth care. The police share its concerns in relation to children with other parties according to the new set-up of the organizations in charge of youth care.

has become a daily routine of practitioners. One professional provides the following explanation on this issue:

> "If I see a child who only has a yellow or white coloured registration—and I know this does not yet qualify it for sending to the Bureau Youthcare—but the child's friend is 'red' in the system; then I bring this extra information into the case discussion within Bureau Youthcare." (ProKid manager, city B)

A white or yellow registration usually signifies a child as a victim or a witness. Yet, the risk profile of this child is shared with Bureau Youthcare because a friendship relation was drawn between the child with the yellow profile and another child who is profiled red in the system. Randomly drawing such a correlation[23] into a risk profile about a child by the time the Police and Criminal Justice Data Protection Directive will be in force would question the extent to which Art. 4, prescribing these conditions for the processing of data as lawfulness, transparency and fairness, is respected. The preventative move of the professional, moreover, raises questions regarding the extent to which such profiling affects a child discriminatorily and whether the criterion "in the best interest of the child" is acted upon.

Risk profile for a baby through indirect evidence.

Given that data registration, in practice, involves more than just the standard that is certainly useful and necessary to sustain professional flexibility and allow room for improvisation. The fact that police officers can freely register a child in the system shows that a child can relatively easily become risk profiled by ProKid:

> "[…] when our officers are at an address and find drugs, […] this information becomes registered in BFLE. But, if they find a baby bottle in the kitchen and ask whether there is a baby, and the inhabitants of the house answer: 'No, the bottle belongs to my sister who comes here occasionally'. If the officer cannot find hard information about whether we need to seek care for the baby, or who exactly lives there, or to what extent the person is making something up… and the officer has a bad feeling [about it] and wants to use the information [about the bottle], he can register it in BFFI[24]. We ProKid managers can see that." (ProKid manager, city C)

If the directive was in place, this quote would lead to questions with respect to whether the transparency principle of Art. 4 in the Police and Criminal Justice Data Protection Directive is enforced. According to this, any personal data should be "processed lawfully, fairly and in a transparent manner in relation to the data subject". The directive permits the collection and processing of data for purposes of prevention. However, the fact that data about the mentioned baby and their parents is registered in a police database without their knowledge and that through the link of that database to ProKid a risk profile can emerge in ProKid about the baby, this raises questions regarding the extent to which the processing of data and the risk profiling by ProKid happens lawfully, fairly and transparently. Furthermore, to address the most important issue at hand—namely, the potential, long term, discriminatory and stigmatising effect risk profiling can cause for a baby—it is essential to perform a complementary children rights' assessment because these effects reach beyond the capacity of the new data protection regime.

---

[23] As the interviews demonstrated drawing random correlations in ProKid is possible, because the technological settings allow for a rather horizontal – information visible on more children – view of children and because the system promotes professionals to take up digitally depicted issues which they see as providing better prevention.

[24] The Basic Facility for Forensic Investigation (BFFI, or Basisvoorziening Opsporing in Dutch) is a law enforcement database of the Dutch police, where a variety of observations of police officers are registered.

To share or not to share (healthcare information).

The ways in which youth healthcare information can be shared beyond the medical profession, especially for risk profiling purposes that are geared towards fostering public safety interests, is perhaps one of the most regulated areas in the Netherlands[25]. Yet, with the rise of the Reference Index High Risk Youth, the sharing of medical information has become situated in a context where new, digitalized prevention practices appear to redefine certain rules. In a large Dutch city, there is a specialized organization in youth care called the Municipal District Organization for Comprehensive Approach (in Dutch: Deelgemeentelijke Organisatie Sluitende Aanpak, DOSA). Youth care professionals can turn to this agency when problems in a family become too complex[26]. A case manager of this organization provided the following explanation concerning how the sharing of healthcare data is smoothened in practice as a consequence of the digital notification their organization receives about each signal and match in the Reference Index:

> "… if you have a RI match, it is an innocent thing. You can then approach a doctor and say: 'You do not have to open up the whole dossier in front of me, but are you busy with this child, are there concerns?' Especially, if we are in touch with a GP who is almost not allowed to say a word according to the Dutch Individual Healthcare Profession Act […] To give an example, I was very happy with the information we provided. That doctor said: 'I have here a mother who is always depressed and has all kinds of bodily and physical complaints. But, she does not want to say much, and I cannot figure out what the problem is. I can transfer her to an internist and give her Valium, but then I am only fighting the symptoms. Is she known to you?' Then, I answer: 'Yes she is known to us because there are serious concerns about all [of] the children: there is an annoying ex, the children do not do well at school, one child had been in contact with the police. So, it is no wonder the mother looks like she does in your practice.' If the GP knows all this, then the GP can ask whether there are financial problems, for instance. He can ask questions more specifically, without prescribing big doses of medicine […]. This is the affectivity of the system […] and how far RI risk reporting can go. I can really benefit from such a signalling system." (DOSA-manager, city A)

The above example demonstrates the direct consequences of sharing medical information, which stem; on the one hand, from the existence of the RI system and from the ways an in-between organization manages youth care in a large Dutch city. The 95/46/EC Directive provides grounds within which derogations from the restrictions on processing sensitive data, including healthcare data, are allowed. The GDPR extended these requirements and specified that sensitive data—including medical information - *"in relation to fundamental rights and freedoms deserve specific protection as the context of their processing may create important risks for the fundamental rights and freedoms […]; such data should not be processed, unless processing is allowed in specific cases set out in this Regulation,…"(Recital 41).*
Furthermore, the extent to which the data subject (both the mother and her child) had been informed of this data processing (as laid down by Arts. 10 and 11 of the 95/46/EC Directive and in the future by Art. 12 of GDPR) would be worth investigating. Given the explanation of the RI manager regarding how the doctor shared health data, if the GDPR was in force, Art. 9 would permit sensitive data processing if the processing of data concerning health is

[25] See about this the Individual Healthcare Professions Act(Wet op de beroepen in de individuele gezondheidszorg, 1993) which entails confidentiality requirements for professionals about how to share patients' data, or the Act on Medical Treatment Contacts Act (Wet Geneeskundige Behandelingsovereenkomst, 1994) which entails prescriptions about accessing patients' files.

[26] DOSA organisations have a helicopter view of youth care related organizations and professionals and are notified about each risk signal and match registered in RI. DOSA professionals are not responsible for solving cases but for only assisting other professionals in solving them.

necessary, for instance "for occupational medicine […] or public health purposes". Yet, a major issue would fall beyond the framework of the data protection regime. The question arises concerning the extent to which the 'privacy of the child' as a fundamental children's right had been enforced when the DOSA professional exchanged information about a child with another doctor in a well-intended manner.

All of the above examples demonstrate that using risk profiles, and processing data for the purposes of profiling via the Digital Youth Healthcare Registry, the Reference Index High Risk Youth and the ProKid systems can evoke rather controversial situations in practice. If the GDPR and the Police and Criminal Justice Data Protection Directive were already be enforced, these issues would challenge a set of prescriptions of these legal instruments.

6.3. Erasing risk profile data

This section addresses certain issues concerning the way in which children's risk profiles can be erased. The obligation to take all steps necessary to erase incorrect data is set out by Art. 6(e) of the 95/46/EC Directive. Art. 16 of the GDPR also discusses this in more detail when it deals with the right to rectification. The right to erasure or the right to be forgotten as laid down by Art. 17 of the GDPR, however, has been introduced as a new right. This right concerns all types of data, especially in relation to children, and it can be considered pivotal because risk profiles can significantly affect a child's adult life as well. Therefore, the potential of the "right to be forgotten" or the "right to erasure" (Art. 17 of the GDPR) by deleting children's risk profiles or links to their risk profiles is essential. Yet, as we will see, enforcing this right in practice would be quite a Gordian knot.

Dealing with erroneous risk registration.

A school doctor using a version of DYHR explains her difficulties in correcting data in children's files as follows:

> "We can check each other (colleagues) and see what we have registered in the file about a child. But, we cannot correct data, even a risk, in the file, for instance, after a health check case is closed. Only the application manager can reopen the health check case and a child's file. Doctors cannot. We need to notify the manager. […]On the top of that, it is not easy to find the problematic data in the file again." (school doctor, city E)

Another professional using DYHR shared a similar frustration concerning the shortcomings inherent in the set-up of the system with regard to deleting incorrect information. The implications of this information for the data subject can be severe:

> "Everything I register instantly goes into the computer and can be monitored. […] If a colleague has filled in something wrong, even a risk, then I [the manager] need to first receive an email query from him/her about whether I would take out the wrong information from a child's file. Until then, [the wrong information] remains in the file and professionals with access can check it." (CB-doctor, city A)

The General Data Protection Regulation in recital 30 specifies how to respond with respect to erroneous data: *"every reasonable step should be taken to ensure that personal data which are inaccurate are rectified or deleted […], and time limits should be established by the controller for erasure or for a periodic review".* Erroneous data should be rapidly corrected according to the prescriptions of the GDPR; the mentioned practices show that correction can indeed take a substantial amount of time. If the GDPR had been accepted, both examples would raise additional questions about how data subjects are informed when erroneous data are stored (Arts.

10 and 11 of the 95/46/EC Directive and Art. 12 of GDPR) and how their rights to object to the processing of (incorrect) personal data (recital 53 GDPR) are respected. The DYHR, however, is linked to the Reference Index High Risk Youth through risk signals, and therefore, any risk signal in the DYHR (only a signal; no further details of medical import) becomes simultaneously visible as an alert in the RI. This means that through automated connections, erroneous risk profiles can spread across systems for a longer period of time. The above-mentioned difficulty in correcting and erasing data also demonstrates this danger. The issue demonstrated by the two examples also touches upon fundamental principles and raises questions concerning how an incorrect risk registration and, more importantly, a lengthy process of correction can be regarded as being in "the child's best interest".

Retained data after expiration remains relevant.

Data retention requirements for the DYHR, RI and ProKid also differ with respect to the conditions under which data can become erased from a child's file. Both the 95/46/EC Directive and the Framework Decision 2008 point towards national legislations in regard to data retention limitations. Data can be retained for 15 years in DYHR, for seven years in RI and for five years in ProKid. Although a risk signal in RI officially expires after 12 months, signals in practice can be retained for varying periods, depending on which organization connected to RI submitted the specific signal:

> *"Each signal has an expiration date. […] For instance, a police signal remains for three months; a signal from an educational institution for six. Signals of other organizations generally remain for 12 months, and we keep BYC signals for 24 months in RI. Signals can be matched only during these periods. […] According to the new Youth Care Act, after a signal becomes inactive, it remains visible for another five years on the website. Afterwards, it must be deleted." (RI manager, city C)*

The above quote demonstrates that depending on which organization submits a signal about a child to RI, the data retention period can either be longer or shorter than 12 months. Signals after the expiration of the given period become inactive and cannot be matched anymore. Yet, they remain visible in a child's file for another five years to assist other professionals:

> *"An inactive signalling allows another professional to use the source of the inactive signal, in order to acquire information from the professional busy with the child earlier." (RI manager, city D)*

The additional five years, however, is a de facto lengthening of the period during which risk profile data remain available for further profiling purposes concerning a child. If the GDPR was in force, this would run afoul to the transparency principle and the data minimization principle of Art. 5. Moreover, this also demonstrates that the (data retention) law on the books differs from the law in practice.

In a similar manner, signals that are not based on risk profiles but are only based on the gut feelings of professionals—called pre-signals in RI—can also prolong the period under which a risk profile can be assigned to a child. In this respect, both inactive signals and pre-signals can be viewed as a means by which the scope of prevention and the risk-profiling period de facto "expands in time" (La Fors-Owczynik & Valkenburg, 2015). Because the basis upon which a pre-signal can be lodged in the system (gut feelings) is quite obscure, this renders the grounds for erasure quite ambiguous as well. These features of pre-signals raise questions on multiple fronts regarding the extent to which the transparency principle in the 95/46/EC is met. For future cases when GDPR is in force, the use of inactive signals and pre-signals can challenge the enforcement of the transparency principle and the requirement for the data controller to provide clarification about the data minimization principle for the data subject as laid down by Art. 5 of the GDPR. Because data subjects are informed neither about pre-signal registrations nor about the reasons for such registrations,

the enforcement of the data controller's obligation to inform the data subject about the processing of data, as provided by Art. 12 would also be challenged. Finally, the existence of inactive signals and pre-signals as a routinely used means for risk profiling children in RI raises questions regarding the enforcement of Art. 20. The latter defines *"the right not to be subject to a measure which produces legal effects concerning this natural person or significantly affects this natural person"*.

The issues raised above, moreover, show that fundamental rights are also at stake. Notably, beyond their envisaged preventative benefit, the extent to which inactive signals and pre-signals enforce the fundamental right that "no child shall be subjected to arbitrary or unlawful interference with his or her privacy" (Art. 16 of CRC) is questionable. The GDPR specifies significant limitations with respect to profiling children. The preventative prolonging of the lifetime of a risk profile by pre-signals and inactive signals, however, raises questions about whether the best interest of the child is not overshadowed by the preventative public safety objectives. At the same time, when a child's risk profile needs to be erased, the capacity of the GDPR to protect "the best interest of the child" proves to be insufficient.

7. Discussion as to the normative state of the new data protection regime in light of the empirical findings

As is shown by the empirical data provided in this article, the new Data Protection Regulation and the Police and Criminal Justice Data Protection Directive will have a strong impact on data protection in light of risk profiling practices on children.

Although the GDPR introduces that *"children (...) deserve specific protection of their personal data, as they may be less aware of risks, consequences, safeguards and their rights in relation to the processing of personal data*"(Recital 29), it does not specify conditions for profiling children because it only addresses commercial parties. When children are profiled by government agencies, both the GDPR and the Police and Criminal Justice Data Protection Directive apply. Both regimes allow for profiling, provided the provisions and conditions set under these regimes and their national implementation are respected.

Therefore, although not yet in force, the GDPR still has relevance. The empirical evidence shows examples of ambiguities and difficulties when professionals must decide what constitutes a risk. It is at this point, for instance, that Art. 5 of the GDPR dealing with data quality shows its relevance.

Art. 8 of the GDPR stipulates the conditions that are "applicable to child's consent in relation to information society services". The GDPR, however, does not provide conditions for risk profiling practices by governments with regard to children. However, the extent to which the GDPR shall take up this as a purpose is of course debatable. Yet, when parents or guardians of a child are considered causing a risk to a child (*e.g.*: child abuse) and children are profiled against these risks by government agencies, a special guardian would be useful to represent the 'best interest of the child'.

With respect to the discriminatory effects of profiling, in regard to children, the effects of profiling practices can only be judged and demonstrated in the long run. However, the empirical evidence presented in this article clearly shows that children can run risks as a consequence of certain discriminatory effects inherent in the use of the three analysed systems. The GDPR explicitly prescribes that fundamental rights as laid down by the Charter of Fundamental Rights of the European Union shall be respected during data processing. If the use of digital technologies may indeed be shown to have discriminatory effects on children and other data subjects, Art. 33 of the GDPR prescribes that the data controller shall initiate data protection impact assessments. The analysis shows that such data protection impact

assessments should be performed coupled with relevant prescriptions of the UNCRC. Given the specifics of this type of data processing, this analysis would be beneficial in strengthening the legal position of children against discrimination.

Art. 14 of the GDPR stipulates that the data controller shall inform the data subject about the processing of data, for instance, and about the data retention period. As the empirical findings demonstrated (*e.g.*: pre-signals and inactive signals in RI), the information obligation of the data controller (Art 14 of the GDPR) is a tool of powerful legal potential. This would mean that the controller is required to inform the data subject (or guardian) about the registration of any type of risk data about a child held and used by government agencies. Hence, if the new regulatory regime is indeed implemented and upheld, more transparency will be realised with regard to the processing of children's data by means of the systems discussed in this article.

The empirical examples have shown that when the new data protection regime is adopted and applied in daily practice, the new regime provides more safeguards than the 95/46/EC Directive. The complexity of the regulation will certainly lead to difficulties in its practical enforcement. However, adding children right's based specifications to the current text could largely foster the effectiveness of the regulation and the legal position of children during government-led, preventative profiling practices directed at children in any EU member state.

8. Conclusion

> "Children deserve specific protection of their personal data, as they may be less aware of risks, consequences, safeguards and their rights in relation to the processing of personal data."[27]

As demonstrated above, the daily risk profiling practices conducted by the Digital Youth Healthcare Registry, the Reference Index High-Risk Youth, and the ProKid 12–SI systems would collide with many of the provisions of the proposed GDPR. This certainly means that the new data protection regime would offer a variety of legal tools to exploit in practice when it comes to the risk profiling of children. However, the analysis has also shown that the data protection regime often becomes difficult to interpret.

The interviews that provided empirical material in this article have been somewhat limited by the specific research purposes of the current research. Notably, the interviews were geared toward highlighting what implications can come from using these systems. To provide a diverse set of issues as a priority, the analysis collected as many issues as possible that were comparable in many practices. This has meant a limitation in the data collection and analysis. Still, the empirical findings to provide valuable insights in relation to controversies that are inherent in the design of DYHR, RI and ProKid and the construction, use and erasure of risk profiles. These controversies outlined the limitations of the new data protection regime. With regard to risk profiling practices concerning children by the government systems assessed here, the new data protection regime would offer a variety of legal tools. The analysis of empirical data further demonstrated that the data protection regime, even if it was in effect, could not provide protection from the long-term stigmatising effects that the creation of a risk profile can cause for a child in the future. The difficulties in erasing erroneous risk profile data and the practical prolonging of the life of a child's risk profile have both underlined the possibilities that these practices infringe on fundamental principles of respect for the rights of children. The data protection regime in its current form could not provide adequate protection for children

[27] Recital 29 of the General Data Protection Regulation of the European Union (15 December 2015)

from these shortcomings, which, as we have seen, are the consequences of risk-profiling practices themselves.

However, practice has also shown that ambiguities around the term 'risk' complicate issues, and at times, they render it virtually impossible to interpret such principles in the context of the new data protection regime. The impossibility to opt-out from risk-driven monitoring and the use of each of these three risk assessment systems by Dutch government agencies cannot be discussed within the framework of the new data protection regime. The regime is simply not meant to address issues preceding the registration of any risk data, including data about children by government organisations. Furthermore, the impossibility of registering improvements in the DYHR, the RI or in ProKid, the financial steering inherent in the risk-signaling processes by RI, and the unfair ways in which risks are assigned to only one address of a child in ProKid all point to issues that reach beyond the limitations of the new data protection regime. Simultaneously, these issues highlight that practical implications of a certain technology design and related policy goals can jeopardize fundamental children's rights. The problems raised in this discussion question the extent to which a primary intention behind these systems—namely, to prevent harm to a child—can be achieved, when the built-in norms and ambiguities around the registration and interpretation of a child's risk profile result in additional risks.

The extent to which the new data protection regime could and should be equipped with means to address issues similar to those mentioned above remains a pivotal topic for discussion. This is especially so because the analysis of the new data protection regime, in light of the illustrations provided by the empirical findings presented above, also supports Koops's argument in relation to the new data protection regime: "Law in the books does not always become, nor does it always resemble law in action"(2014: 256). However, in light of the preceding analysis, the capacity of the (current) data protection regime in providing legal remedy to certain side effects of risk profiling by these systems proved that the use of such tools as the UN Convention on the Rights of the Child in order to better protect "the best interest of the child" is indispensable. The ways in which risk profiles are constructed and used and the conditions under which profiles are retained and erased have shown that the new data protection regime would fall short of serving the "best interest of the child" as required by Convention on the Rights of the Child. On the one hand, a child's risk profile can be created relatively easily, given the extensive set of categories and norms according to which a risk flag can be assigned to a child. On the other hand, examples have shown that erasing a risk profile—or even information contained in such a profile—is often very difficult.

In addition to the following prescriptions of the Convention on the Rights of the Child, a more 'context-oriented' reading of the data protection regime could also be of help. The data protection regime already favours fundamental rights, such as the right to privacy or the right to data protection. The prescriptions towards 'privacy by design' and 'data protection by default' also demonstrate this. Yet, each of these principles bears ambiguities around the term privacy and the term data protection. To tackle the difficulties of defining and interpreting privacy within profiling practices in relation to children, Nissenbaum's hypothesis of 'privacy as contextual integrity' provides a nice alternative(2004). To see and define privacy through norms that govern different contexts differently would allow for a variety of other values to be enforced. For those professionals who perform risk profiling of children through any of the three systems discussed above, implementing a 'privacy as contextual integrity' approach in their daily practice would be very useful to balance the interests that are more in favour of fundamental values. Moreover, building in ethical values (Silverstein, Nissenbaum, Flanagan, & Freier, 2006) when designing information technologies in relation to children is indispensable. For instance, registering good things or improvements in a child's behaviour within the ProKid system, or as raised elsewhere (La Fors-Owczynik, 2015) by erasing risks,

could in some cases grant a certain 'right to be forgotten' to a child. This, in practice, could mean a 'right to be forgiven', as the specific risk a child was linked to via a ProKid profile disappears. Considering the positive effects such steps can have on the development of children is essential.

Although reporting of and profiling 'anomalies' concerning children in the Netherlands pervades public discourse, the problematic consequences of digital profiling practices are far less prominently discussed. This article assessed the capacity of the newly proposed European data protection regime to adequately respond to the risks stemming from the digital risk profiling practices of children by the Dutch government. Risk-profiling practices by each of the three systems are well intended and meant as necessary solutions to prevent harm from occurring to children. However, raising awareness of the newly emerging risks that stem from the very use of these systems is essential. Furthermore, the analysis can also be helpful to cultivate reflexivity in the new data protection prescriptions amongst professionals who assess children against risks by the DYHR, RI and ProKid.

Despite the positive results that can be attributed to these systems—for instance, the timely notice of child abuse—the observations concerning the drawbacks of these systems are informative of the implications that government-led risk profiling practices can have with respect to children. The analysis also underlined the necessity of assessing how the best interest of the child is served by these systems (including unwritten principles such as the right of a child to learn from small mistakes). Given the current stage and the potential direction in which the text of the new data protection regime might develop, the analysis in this article provides a glimpse of what the regime could mean within contexts of government-led risk profiling of children. In doing so, it noted that the new data protection regime will not and cannot be the single solution against the issues stemming from the creation and use of such digital risk profiles of children.

Acknowledgements

The research which enabled this chapter had been funded via the DigIDeas project, which was granted to Dr. Irma van der Ploeg by the European Research Council under the European Union's Seven Framework Programme (FP7 2007–2013)/Grant No. 201853/. Moreover, I am very grateful to Prof. Corien Prins for her support and insightful comments on this chapter.

Bibliography

Abraham, M., Buysee, W., Loef, L., & Van Dijk, B. (2011). *Pilots ProKid Signaleringsinstrument 12- geëvalueerd Pilots ProKid Signaleringsinstrument 12- geëvalueerd*. Den Haag, WODC

Benoist, E. (2008). Collecting Data for the Profiling of Web Users. In Hildebrandt, M. & S. Gutwirth (Eds.), *Profiling the European citizen Cross-disciplinary perspectives* (pp. 169–184). Den Haag, Springer Science

Bruning, M. R. ., Van den Brink, Y. N. ., de Jong – de Kruijf, M. P. ., Olthof, I. W. M. ., & Van der Zon, K. A. M. (2012). *KINDERRECHTENMONITOR 2012 - Adviezen aan de Kinderombudsman* -. Kinderombudsman, Den Haag.

Canhoto, A., & Backhouse, J. (2008). General description of the definition of profiling. In *Profiling the European citizen Cross-disciplinary perspectives*. Den Haag Springer Science

CBP. (2007). Brief aan de Minister van Jeugd en Gezin. Retrieved from https://cbpweb.nl/sites/default/files/downloads/th_dossier/ano071029_brief_rouvoet_inzake_verbreding_ekd.pdf

Costa, L., & Poullet, Y. (2012). Privacy and the regulation of 2012. *Computer Law & Security Review*, *28*(3), 254–262.

De Hert, P. (2008). Identity management of e-ID, privacy and security in Europe. A human rights view. *Information Security Technical Report*, *13*(2), 71–75.

De Hert, P., & Papakonstantinou, V. (2012). The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals. *Computer Law & Security Review*, *28*(2), 130–142.

De Vries, K. (2010). Identity, profiling algorithms and a world of ambient intelligence. *Ethics and Information Technology*, *12*(1), 71–85. http://doi.org/10.1007/s10676-009-9215-9
Foucault, M. (2004). Securité, territoire, population, Cours au College de France, 1978-79. Paris: Seuill/Gallimard.

Foucault, M. (trans. by A. Sheridan (1977). *Discipline and Punish: The Birth of the Prison*. New York: Vintage.

Goedee, J., & Rijkers, A. (2010). *Zorgsignalen van de Politie Over het "Vroegsignaleren en doorverwijzen" tussen Politie en Bureau Jeugdzorg*.
Gray, D., & Citron, D. (2013). The Right to Quantitative Privacy. *Minnesota Law Review*, *98*, 62–144.

Gutwirth, S. (2009). Beyond identity? *Identity in the Information Society*, *1*(1), 123–133.

Henman, J. (2004). Targeted! Population Segmentation, Electronic Surveillance and Governing the Unemployed in Australia. *International Sociology*, *19*(2), 173–191.

Hildebrandt, M. (2008). Defining Profiling: A New Type of Knowledge? In M. Hildebrandt & S. Gutwirth (Eds.), *Profiling the European citizen Cross-disciplinary perspectives*. Den Haag: Springer Science

Hoogstrate, A. J., & Veenman, C. J. (2012). *Informatiegestuurde grenscontrole Verkenning ten behoeve van het gebruik van selectieprofielen in het kader van grensbeheer*. Rijksoverheid, Den Haag. Retreived on 14th October 2014 from <https://www.rijksoverheid.nl/documenten/rapporten/2012/09/06/informatiegestuurde-grenscontrole-verkenning-ten-behoeve-van-het-gebruik-van-selectieprofielen-in-het-kader-van-grensbeheer>

Hornung, G. (2012). A General Data Protection Regulation for Europe? Light and shade in the Commission's draft of 25 January 2012. *SCRIPTed*, *9*(1), 64–81.

Jansen, Y. J. F. M., & de Bont, A. A. (2010). The role of screenings methods and risk profile assessments in prevention and health promotion programmes: an ethnographic analysis. *Health Care Analysis : HCA : Journal of Health Philosophy and Policy*, *18*(4), 389–401.

Retrieved on 23rd February 2014 from http://www.pubmedcentral.nih.gov/articlerender.fcgi?artid=2970818&tool=pmcentrez&rendertype=abstract

Keymolen, E., & Broeders, D. (2013). Innocence Lost : Care and Control in Dutch Digital Youth Care, British Journal of Social Work 43 (1): 41-63.

Keymolen, E., & Prins, C. (2011). Jeugdzorg via systemen. De Verwijsindex Risicojongeren als spin in een digitaal vangnet. In D. Broeders, C. M. K. C. Cuijpers, & J. E. J. Prins (Eds.), *De staat van informatie*. Amsterdam: Amsterdam University Press.

Klingenberg, A. M., & Lindeboom, J. (2013). Lost in e-government: bevat de Algemene verordening gegevensbescherming voldoende waarborgen voor burgers bij gegevensverwerking door de overheid? *Privacy & Informatie*, *8*, 273–278.

Koops, B. (2014). The trouble with European data protection law. *International Data Privacy Law*, *4*(4), 250–261.

Koops, B. & Leenes, R. (2005). "Code" and the Slow Erosion of Privacy. *Michigan Telecommunication and Technology Law Review*, *12*(1) 115–188.

Kuner, C. (2012). The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law. *Privacy and Security Law Report*. Retrieved on 3rd May 2014 from http://amcham.dk/files/editor/Data_privacy_-_Kuner_EU_regulation_article.pdf

La Fors-Owczynik, K. (2015). Minor protection or major injustice? Children's rights and digital preventions directed at youth in the Dutch justice system. *Computer Law and Security Review*, *31*(5), 651–667.

La Fors-Owczynik, K., & Valkenburg, G. (2015). Risk identities: constructing actionable problems in Dutch youth. In I. Van der Ploeg & J. Pridmore (Eds.), *Digitizing Identities: Doing Identity in a Networked World*. New York, Routledge,

Leenes, R. (2010). Context Is Everything Sociality and Privacy in Online Social Network Sites. In M. Bezzi, P. Duquenoy, S. Fischer-Hübner, M. Hansen, & G. Zhang (Eds.), *Privacy and identity management for life* (pp. 48–65). Springer Berlin Heidelberg.

Leopold, N., & Meints, M. (2008). Profiling in Employment Situations (Fraud). In M. Hildebrandt & S. Gutwirth (Eds.), *Profiling the European citizen Cross-disciplinary perspectives* (pp. 217–237). Den Haag, Springer Science

Lyon, D. (2001). *Surveillance society. Monitoring everyday life*. Buckingham (UK, Philadelphia (US), Open University Press

Lyon, D. (2003). *Surveillance as social sorting: surveillance, risk and digital discrimination*. London: Routledge.

Lyon, D. (ed.) (2006). Theorizing surveillance: The panopticon and beyond. Cullomption (UK), Portland (US), Willan Publishing.

Manders-Huits, N. (2010). Practical versus moral identities in identity management. *Ethics and Information Technology*, *12*(1)

Mckenna, A. (2012). Profiling and manipulating Human behaviour: a core contemporary privacy concern, 1–19. Retrieved on 22nd September 2013 from http://kar.kent.ac.uk/29654/

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. (2013). *Risicoregel reflex in de jeugdzorg ? Verkennede analyse van de bestuurlijke valkuil van overreactie op risico's en incidentedn in de jeugdzorg*. Den Haag.

Nijhof, K. S., Engels, R. C. M. E., & Wientjes, J. A. M. (2007). Crimineel gedrag van ouders en kinderen. *Pedagogiek*, *27*(1), 29–44.

Nissenbaum, H. (2004). Privacy as contextual integrity. *Washington Law Review*, 119–158.
Oerlemans, J., & Bruning, R. (2010). De Verwijsindex risicojongeren: hulpverleners als privacyjuristen? *Privacy & Informatie*, (3), 116–123.

Oudshoorn, N. (2011). *Telecare technologies and the Transformation of Healthcare*.

Pridmore, J. (2012). Consumer Surveillance: Context, Perspectives and Concerns in the Personal Information Economy. In K. Ball, K. D. Haggerty, & D. Lyon (Eds.), *Handbook of Surveillance Studies*. Routledge. New York

Prins, J. E. J. (2006). Property and Privacy: European Perspectives and the Commodification of our Identity. In L. Guibault & P. B. Hugenholtz (Eds.), *The Future of the Public Domain, Identifying the Commons in Information Law* (pp. 223–257). Kluwer Law International. Den Haag

Prins, J. E. J. (2007). Een recht op identiteit. *Nederlands Juristenblad*, *82*(14), 849.

Prins, J. E. J. (2010). Digital Diversity : Protecting Identities Instead of Individual Data. In L. Mommers & A. Schmidt (Eds.), *Het binnenste buiten: Liber amicorum ter gelegenheid van het emeritaat van prof. dr. Aernout Schmidt*. Den Haag

Prins, J. E. J. (2014). Privacy in geding: Expliciteren, wegen en beperken van belangen. In M. S. Groenhuijsen & A. Soeteman (Eds.), *Recht in geding* (pp. 51–59). Boom Juridische Uitgevers. Den Haag

Rijksoverheid. Wet Verwijsindex risicojongeren van kracht op 1 augustus 2010 Retrieved on 22nd January 2011 from http://www.rijksoverheid.nl/documenten-en-publicaties/persberichten/2010/07/09/wet-verwijsindex-risicojongeren-van-kracht-op-1-augustus-2010.html

Rubinstein, I. S., Lee, R. D., & Schwartz, P. M. (2008). Data Mining and Internet Profiling: Emerging Regulatory and Technological Approaches. *The University of Chicago Law Review*, *75*(1), 261–285.

Samuelson, P. (2000). Privacy As Intellectual Property? *Stanford Law Review*, *52*(5), 1125–1173.

Schermer, B. W. (2011). The limits of privacy in automated profiling and data mining. *Computer Law and Security Review*, *27*(1), 45–52. http://doi.org/10.1016/j.clsr.2010.11.009
Schinkel, W. (2011). Prepression: the actuarial archive of new technologies of security. *Theoretical Criminology*, *15*(4), 365–380.

Shoemaker, D. W. (2009). Self-exposure and exposure of the self: informational privacy and the presentation of identity. *Ethics and Information Technology*, *12*(1), 3–15.

Sholtz, P. (2000). The Economics of Personal Information Exchange. *First Monday*, *5*(9).

Silverstein, J., Nissenbaum, H., Flanagan, M., & Freier, N. G. (2006). Ethics and children's information systems. *Proceedings of the American Society for Information Science and Technology*, *43*(1), 1–7.

Van der Hof, S. (2011). Het gedigitaliseerde kind - Over de onevenwichtige relatie tussen burger en overheid in de eJeugdzorg. Retrieved on 13th March 2014 from http://www.recht.nl/vakliteratuur/familierecht/artikel/308903/het-gedigitaliseerde-kind-over-de-onevenwichtige-relatie-tussen-burger-en-overheid-in-de-ejeugdzorg/

Van der Hof, S. (2014). No Child's Play: Online Data Protection for Children. In S. et al. Van der Hof (Ed.), *Minding Minors Wandering the Web: Regulating Online Child Safety* (pp. 127–141). The Hague: Asser Press.

Van der Hof, S., & Keymolen, E. (2010). Shaping minors with major shifts : Electronic child records in the Netherlands. *Information Polity*, *15*(4), 309–322.

Van der Hof, S., Leenes, R, & Fennell-van Esch, S. (2009). *Framing citizen's identities: The construction of citizen identities in new modes of government in The Netherlands, research on personal identification and identitiy management in new modes of government*. Wolf Legal Publishers, Nijmegen

Van der Hof, S., & Prins, C. (2008). Personalisation and its Influence on Identities, Behaviour and Social Values. In *Profiling the European citizen Cross-disciplinary perspectives* (pp. 111–117). Springer Science. Den Haag

Van der Ploeg, I. (2010). Security in the Danger Zone: Normative Issues of Next Generation Biometrics. In E. Mordini & D. Tzovaras (Eds.), *Second generation biometrics: The ethical, legal and social context* (pp. 287–303). Springer. London

Van Dijk, E. (2008). De Basisdataset: de inhoudelijke basis van het digitaal jgz-dossier. RIVM, Den Haag

Van Eijk, N., Helberger, N., Kool, L., Van der Plas, A., & Van der Sloot, B. (2012). Online tracking: questioning the power of informed consent. *Info*, *14*(5), 57–73.

Van Wijck, F. (2009). Logisch dat de huisarts in jeugdzorg altijd in beeld is. *Huisarts in Praktijk*, 22–25.

Zarsky, T. (2010). Responding to the Inevitable Outcomes of Profiling: Recent Lessons from Consumer Financial Markets, and Beyond. In S. Gutwirth, Y. Poullet, & P. De Hert (Eds.), *Data protection in a Profiled World* (pp. 53–74). Springer. Den Haag

COMPUTER LAW & SECURITY REVIEW 31 (2015) 651–667

Available online at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

Minor protection or major injustice? – Children's rights and digital preventions directed at youth in the Dutch justice system

Karolina La Fors-Owczynik *

Tilburg Institute for Law, Technology and Society (TILT), Tilburg University, The Netherlands

Keywords:
Children's rights
Risks
Digitalisation
Prevention
Law enforcement

ABSTRACT

The United Nations Convention on the Rights of the Child (CRC) is the most essential placeholder for protecting children's rights internationally. In support of its leading principle: "the best interest of the child" (Art. 3) a growing number of digital technologies are employed in different contexts of life, including contexts of justice and youth care. Therefore, when children enter the juvenile justice system and become objects of proactive, digitalised investigations, CRC rights are even more pivotal. Yet, as academic discourse demonstrates, children's rights are increasingly under pressure within law enforcement (Bruning, 2010; Kilkelly, 2001). This paper sets out to explore a relatively undiscussed topic, namely the digitalised preventative policing practices on children under the United Nations CRC. The discussion by way of illustration centres around an initiative taken in recent years in The Netherlands, ProKid SI 12- (ProKid). Grounded in a public rhetoric where 'crimes against children' and 'crimes committed by children' are viewed as equally important issues to prevent, the risk profiling system ProKid is employed by the Dutch police as a solution for both. Empirical details about ProKid demonstrate, however, that its preventative profiling routines challenge several CRC principles such as, for instance 'the child's assumption of a constitutive role in society', its 'privacy' and perhaps most importantly 'the assumption of innocence of a child until proven guilty'. The use of ProKid frames children as potential perpetrators even when they are registered as victims of violence. In the light of the challenges raised, this paper aims to open up the debate about the risks ProKid and similar initiatives bring along for children, and their families and about the CRC's potential to address these.

1. Introduction

As more risks are identified in almost all aspects of citizens' everyday life in the 21st century, risk assessment modes and technologies are increasingly employed within professional practices in Western societies. Ulrich Beck's "risk society"[1] progressively has grown into what Barry calls the "blaming society",[2] which in her view is primarily "concerned with risk avoidance and defensive practices".[3] Although different types of individuals have

* Tilburg Institute for Law, Technology and Society (TILT), Tilburg University, P.O. Box 90153, 5000 LE Tilburg, The Netherlands. Tel.: +31 621403891.
E-mail address: k.owczynik@uvt.nl.

[1] Beck, U. Risk society: Towards a new modernity (SAGE publications 1992).

[2] Barry, M. 'Effective Approaches to Risk Assessment in Social Work: An International Literature Review' 2007 Retrieved 8th March 2014 from <http://scotland.gov.uk/Resource/Doc/194419/0052192.pdf>.

[3] Ibid.

http://dx.doi.org/10.1016/j.clsr.2015.07.003
0267-3649/

become objects of these routines, children are often a prominent group within these routines, because they are seen as a group 'at the margin' due to their psychological, social or legal immaturity and less-developed awareness. Hence, their protection from a wide range of risks often justifies a significantly larger set of prevention modes, than the protection of adults would. Practices of care and prevention of potential harm to youth are some prime examples internationally, where technology-based risk prevention in assessing children, becomes prioritised and situated higher and higher on political and professional agendas. Specifically, *child abuse* and *anti-social behaviour* of youth have long been prime concerns to prevent internationally.[4] To foster the prevention of such problems the so-called identity management technologies (IDM)[5] for risk assessment are increasingly seen as inevitable 'solutions'.

Child abuse and the anti-social behaviour of youth have recently been pushed to the forefront[6] in The Netherlands. ProKid SI 12- (henceforth: ProKid), a risk profiling, IDM system on children aged between 0 and 12 years has been introduced and used by the police in The Netherlands in order to prevent a range of problems children might be victims or perpetrators of. Risk signals both about 'crimes against children' and 'crimes committed by children' are registered in ProKid and form risk profiles of children. The in-built standards and the daily use of ProKid are initiated to forecast potential problematic futures children might develop by monitoring, diagnosing and signalling issues associated with a child already in the present. This article will demonstrate that although the purpose of ProKid is to prevent law enforcement related problems associated with a child, the very use of ProKid brings risks for children and their families as a consequence. These risks challenge the enforcement of childrens' rights as prescribed by a prominent regulatory instrument issued by the United Nations: the Convention on the Rights of the Child (CRC). Given that initiatives similar to ProKid are being used in various countries, the principal aim of this article is to explore the CRC's potential to address the risks stemming from the use of these systems.

The ProKid SI 12- system emerged at a time when the Dutch government undertook two of its most comprehensive changes in its recent administrative history: one within its justice system and one within its youth care system. First, as of 2013, a transition affected the Dutch police corps: a picture of a more centralised 'national police' emerged when 25 police corps units became reduced to 10. Second, within the Dutch youth care system as of January 2015 the management and distribution of professional care for children has been moved from provinces to municipalities. Although this comprehensive change was argued as being necessary to reduce costs and increase efficiency in the provision of care by professional organisations, critical voices raised their concerns. For instance, the Dutch Child Ombudsman who safeguards and controls the enforcement of CRC in The Netherlands shared his professional reservations about whether the purposes of efficiency and budgetary cuts during this transition in the youth care sector did not jeopardise such primary principles as "the best interest of the child" (Art. 3 CRC). Moreover, scholars shared their worries about the legitimacy of this decentralisation in youth care with special regard to the extent to which the government remains able to control data flows and maintain its duty of transparency under the Dutch Data Protection Act[7] and the European General Data Protection Proposal.[8]

The effect of both transitions should be considered against the background of an increase in the use of "surveillance and identification technologies"[9] by the police as well as youth care organisations.[10] Although prevention had for long been a top priority within Dutch youth care,[11] the extensive use of IDM systems, as well as the practice of sharing large amounts of personal data between partners involved, is a relatively new phenomenon.[12] ProKid SI 12- as a system in assisting the police to conduct digitalised preventative work is unparalleled.[13] Academic literature criticised ProKid as a technology producing a certain preventative, penalising pressure or "pre-pressure"

[4] For international examples, see section 2.2. The following systems, for instance in the USA: 'Partnership for youth at risk' <http://www.partnershipsforyouthatrisk.org/sections/registration/registration_main1.htm; in Australis: 'High Risk Youth Register' <http://www.dhs.vic.gov.au/cpmanual/practice-context/children-in-specific-circumstances/1014-high-risk-adolescents-hra-practice-requirements/3>; or in the UK for period of time: the Contact Point (see also Hoyle, D. 'ContactPoint. Because every child matters?' (2010) The encyclopaedia of informal education <www.infed.org/socialwork/contactpoint.htm>.

[5] *Identity management technologies* in citizen–state relations are digital systems which perform the identification and verification of citizens and allow for differing levels of access control for government authorities. These systems serve to establish 'identities' (defined as personal data sets) within citizen–state relations. This includes the identities of persons subject to the system, in this case children and families, as well as those professionals (e.g.: technicians, doctors, police men, etc.) who interact with such systems on a regular basis.

[6] The Minister of Youth and Family: André Rouvoet explained in an interview (van Wijck, 2009), that during his 13 year carrier being an MP he experienced no discussion on the topic of child abuse, therefore how glad he was that the topic finally reached the top of political agendas.

[7] Wet Bescherming Persoonsgegevens 2000 (Data Protection Act) Retrieved on 20th July 2014, from <http://wetten.overheid.nl/BWBR0011468>.

[8] Klingenberg, A.M. & Lindeboom, J. 'Lost in e-government: bevat de Algemene verordening gegevensbescherming voldoende waarborgen voor burgers bij gegevensverwerking door de overheid?' (2013) 6 Privacy & Informatie 273.

[9] Lyon, D. *Identifying Citizens: ID cards as Surveillance.* (Polity Press 2009). Lyon, D. *Surveillance society Monitoring everyday life* (Open University Press 2001).

[10] The Digital Youth Healthcare Registry (in Dutch: Digitaal Dossier Jeugdgezondheidszorg) or the Reference Index High Risk Youth (in Dutch: Verwijsindex Risicojongeren) are two examples of such systems.

[11] Gorissen, W. *Kennis als hulpbron: het gebruik van wetenschappelijk kennis bij beleidsvorming in de jeugdgezondheidszorg voor 4-19 jarigen* (University of Utrecht 2002). Mathar, T., & Jansen, Y. J. F. M. 'Introduction' in T. Mathar & Y. J. F. M. Jansen (eds), *Health Promotion and Prevention Programmes in Practice: How Patients ' Health Practices are Rationalised, Reconceptualised and Reorganised* (Transcript Verlag, 2012).

[12] Tilley, N. (ed), *Handbook of crime prevention community safety* (Willan Publisher 2013).

[13] Minister van Veiligheid en Justitie (2012), 29 279 Rechtsstaat en Rechtsorde Nr. 147 Brief van de minister van veiligheid en justitie aan de Voorzitter van de Tweede Kamer der Staten-Generaal, Den Haag.

on children who appear on its radar.[14] Yet, thus far ProKid which is situated in a law enforcement organisation in the Dutch justice system and connected to 'pure' law enforcement databases[15] has not yet been assessed from a children's rights perspective, as laid down by CRC. This is crucial in order to identify, which interests ProKid tends to promote: the 'best interest of the child' or the 'interest of public safety'.

Given that complete transparency about the child or in other words the 'complete erasure of a child's privacy' by government systems such as ProKid under no circumstances could it be viewed as being in the child's best interest, not even if such transparency would be argued as being in the interest of public safety,. Hence, a high degree of privacy can be seen as being continuously necessary and in the best interest of the child. Consequently, in order to evaluate the implications of ProKid on the 'best interest of the child' assessing the implications of ProKid on the child's right to privacy is absolutely critical.

Therefore, the article starts with a discussion in Section 2 of the prescriptions of CRC for digital identity management practices and more specifically for the child's right to privacy. The CRC perspective provides a useful analytical lens to explore the implications of ProKid on children's and families' lives. When it comes to children, the definition of privacy in CRC is broader than that, for instance, in the European General Data Protection Regulation (GDPR). This broadness is deemed justifiable as the word privacy is repeatedly used as being inseparable from settings concerning personal data protection in the text of GDPR.[16] Whereas the strength of the definition of privacy in CRC is that it encompasses more than only prescriptions about personal data processing. Certainly, the CRC perspective also includes the prescriptions of the data protection regulation on a child's privacy, but since it is broader it also allows for the consideration of issues that data protection regulations usually do not. Notably, it gives room for instance for considerations of whether or not data concerning a child, should be registered in systems such as ProKid at all. As the CRC prescribes the most universal, child specific set of fundamental rights and values.

Furthermore, the section will also investigate how the right to privacy is underpinned by a selection of international legislative tools. These include three ECHR case laws on children's privacy within law enforcement. The case laws are chosen specifically in law enforcement, because in these cases the ECHR decided in favour of a 'child's right to privacy' versus 'public safety interests'. These judgments are crucial, because as scholars have shown within Dutch law enforcement court cases CRC rights are most rarely considered versus public safety interests.[17] The chosen ECHR court cases emerge therefore as being useful, as ProKid is an instrument that has as its main objective preventing children from developing delinquency.[18] ProKid also shows a priority for safeguarding public safety interests and as such also affects the right to privacy of a wide range of children and others related to them on a daily basis.

Subsequently, Section 3 explores the challenges around ProKid within The Netherlands by providing empirical insights into practices, where the purpose, design and use of ProKid challenge CRC rights and sometimes even jeopardise the enforcement of the convention. These insights are the results of self-conducted, semi-structured interviews with police officers working with ProKid in different cities in The Netherlands prior to January 2015.[19] Based on these insights, Section 4 analyses the potential of CRC as a legal instrument to enhance the protection of children's rights, even when it comes to risks stemming from the very use of ProKid. The conclusion focuses on the main challenges the Convention faces in light of the discussed developments around systems such as ProKid. This includes themes for discussions about how to address both the risks ProKid is designed to prevent and the risks that stem from those ProKid profiling methods, which frame children being 'at risk' of committing a crime and 'as a risk' in committing a crime in the future.

2. The UN Convention on the Rights of the Child (CRC) and digital identity management (IDM) systems in children–state relations

The United Nations Convention on the Rights of the Child (CRC) was adopted in 1989. Since this event, it has been the most essential agreement for protecting children's rights and values internationally.[20] Because this convention

[14] Schinkel, W. 'Prepression: the actuarial archive of new technologies of security' (2011) 15(4) Theoretical Criminology, 365.

[15] About 'pure' law enforcement systems connected to ProKid, see page 12 of this article.

[16] About this see, for instance, Amendment 37, 43, 44 and 49 in the text of the GDPR. Amendment 37, for instance frames privacy along the enforcement of principles of data minimisation and purpose limitation. Amendment 43 concerning personal data breach uses the terms personal data and privacy almost as synonyms. Amendment 44 in a similar manner frames personal data and privacy as terms that can replace each other, when it praises the potential of thorough impact assessments in protecting them. Amendment 49, furthermore frames the principles of privacy by design and privacy by default through the ways in which data protection restrictions need to be effectuated. The text of the GDPR had been retrieved on 12th December 2014 from: <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0212+0+DOC+XML+V0//EN>.

[17] About this, consult further: De Graaf, J. H., Limbeek, L. M. B., Bahadur, N. N. & Van der Meij, N. *De toepassing van het internationaal verrag inzake de rechten van het kind in de Nederlandse rechtspraak 1 Januari 2002–1 September 2011* (Ars Libri, 2012).

[18] For more, please see the section on ProKid.

[19] As of 1st of January 2015 the Institution of Bureau Youth Care have been abolished and other institutions became certified to carry out the tasks of Bureau Youth Care in The Netherlands. This constitutes part of the large transition operation, within which youth care tasks have been transferred to Dutch city councils. Moreover, city councils need to establish professional relations with newly certified youth care institutions in order to safeguard the quality of care.

[20] Alston, P. and Tobin, J., *Laying the Foundations for Children's Rights: An Independent Study of some Key Legal and Institutional Aspects of the Impact of the Convention on the Rights of the Child* (UNICEF, 2005).

specifies that children need to enjoy protection from harm and that when children are accused of criminal behaviour, any legal procedure must occur by focussing closely on the enforcement of their rights, the CRC is an indispensable legal source of prevention practices aimed at forecasting problems associated with children. The convention is particularly relevant when prevention is performed associated with children by such digital risk assessment systems as ProKid, as used by the Dutch police. Furthermore, the CRC has had a 'direct working'[21] in Dutch law since 1995, including legal areas for such parties to the justice system as the police. The CRC has already been part of a great variety of court cases,[22–24]all of which demonstrate, however, that the CRC's direct working remains de facto indirect up until a court rules on the direct working of its provisions.[25]

The convention was the first treaty to define children as rights holders. Separate articles are devoted to define prescriptions for children who are categorised as victims or witnesses of violence or who are accused of a form of perpetration. The fact that the Conventions speak together about all these three categories implies the relevance of the educative character of the CRC towards all children. However, distinctions between these categories remain highly relevant because children categorised by any of these categories need different forms of assistance (for instance, a child victim could need psychological help first whereas an accused child could need judicial assistance). Examples of CRC principles particularly relevant from the perspective of prevention and such government-owned identity management systems as ProKid, which is geared towards assessing and categorising children into any of the three above categories, include the following: (1) "no child shall be subjected to arbitrary or unlawful interference with his or her privacy" (Art. 16); (2) "assuming of a constructive role in society about a child" (Art. 40); and (perhaps most importantly) (3) "the assumption of innocence of a child until proven guilty" (Art. 40). Such principles are often not part of discussions in relation to such IDM systems as ProKid because data protection regulations are usually considered to cover them already. Notably, when data are processed in line with such regulations, CRC prescriptions mostly remain untouched.

The CRC is also the first legal instrument to establish the right to privacy for children as a basic fundamental right. However, it does not specify data protection as a separate fundamental right of children.[26] Although the UN Human Rights Committee, the drafter of the convention, cautioned about registering and processing information digitally on children by either public or private parties,[27] the CRC remains a less-prominent instrument to consult regarding prevention practices using digital systems on children. This instrument, however, proves to be crucial for use. The CRC right to privacy has a much broader definition of privacy than do, for instance, EU data protection instruments,[28] as mentioned earlier. However, the CRC right to privacy also can be considered a precondition to or part of other children's rights such as the above-mentioned Art. 40. This proves to be highly relevant because risk registrations about children in ProKid do affect these principles. Furthermore, children's right to privacy can also be viewed as a continuous weight that can be used to counter other values and interests. Within law enforcement, for instance, it is countered by public safety interests the balancing of which constitutes an essential part of prevention practices and risk calculations by ProKid. Hence, the following section assesses how children's right to privacy as laid down by the CRC, including their right to digital privacy, also is strengthened by other legal instruments covering children–state relations.

As we will see in the next section, the European Convention for Protection of Human Rights and Fundamental Freedoms strengthens CRC rights already by its applicability to all persons, including children. The Charter of Fundamental Rights and Freedoms of the European Union enforces CRC rights by its higher legal enforceability within the EU. Furthermore, the Proposal for the General Data Protection Regulation of the European Union strengthens the CRC's capacity because it introduced new rights and prescriptions rooted in fundamental values, for instance, about how to design systems. Moreover, European Court of Human Rights case laws, more specifically those three to be demonstrated, exemplify that the ECHR is explicit about the positive obligations of signatory states with respect to their duty to enforce persons' fundamental right to privacy. The various ways in which these legal instruments reach effectivity are all applicable to children, particularly to those assessed by ProKid.

2.1. *Children's right to privacy*

First, the European Convention for Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as amended) establishes the right to private and family life. Moreover, it provides for exceptions under which public authorities are allowed to infringe on this fundamental right. Although this convention does not specify a right to private life for children, it includes children because Art. 1 states that

[21] 'Direct working' means that after an international treaty becomes ratified in The Netherlands it becomes directly part of Dutch national legislation.

[22] HR 7 Maart 2014, 13/04683.

[23] Rb. Arnhem 16 Februari 2010, BL6961.

[24] HR 7 Maart 2014, 13/04683.

[25] Research about the implementation of CRC within Dutch court decisions shows that the Convention is least applied in criminal law cases compared to other jurisdictions. Its influence is marginal as in such cases the best interest of the child is generally outbalanced versus public safety interests. About this, see also: De Graaf, J. H., Limbeek, L. M. B., Bahadur, N. N. & Van der Meij, N. *De toepassing van het internationaal verrag inzake de rechten van het kind in de Nederlandse rechtspraak 1 Januari 2002–1 September 2011* (Ars Libri, 2012).

[26] Van der Hof, S. 'No Child's Play: Online Data Protection for Children' in S. van der Hof and B. van den Berg and B. Schermer (eds), *Minding Minors Wandering the Web: Regulating Online Child Safety* (Asser Press, 2014). Hodgkin R. and Newell P. *Implementation Handbook for the Convention on the Rights of the Child* (UNICEF, 1998).

[27] Detrick, S. *A commentary on the United Nations Convention on the Rights of the Child* (Martinus Nijhoff Publishers, 1999).

[28] Data protection instruments are indispensable means. Yet, they could more often be complemented with relevant prescriptions of the CRC when it comes to the digitalisation of children's personal data.

it applies to "everyone" and Art. 14 allows no distinction amongst its legal subjects with respect to their age.

Second, on the EU level, the Charter of Fundamental Rights and Freedoms of the European Union[29] can be considered a children's rights instrument. Art. 7 of the charter establishes the right to private life and Art. 8 explicitly acknowledges the right to data protection as a separate individual human right. The fact that the rights to private life and to data protection are separate rights and one can be infringed separately from the other shows a broad interpretation of privacy,[30] from which all children's rights can benefit. The Charter is consistent with all human rights law and, given its purpose to consolidate human rights law amongst EU member states, it is a unique legal instrument to enforce children's rights, including their right to privacy. Because the charter has the same legal power as any other EU treaty, the charter in relation to ProKid can be considered a strengthening of the enforcement of CRC rights.

2.1.1. *General Data Protection Regulation in relation to privacy*

Because the right to privacy and the right to data protection are separate fundamental rights, this section is devoted to highlighting their close relationship in practice to a third legal instrument, the EU proposal for General Data Protection Regulation.

It is crucial to highlight that when privacy impact assessments[31] investigate the effects of digital identity management systems on persons' privacy, they mostly take the approach of investigating how data are processed, stored and shared. In practice, this often means that although the right to privacy and to data protection are separate fundamental rights, how implications for the right to privacy are assessed de facto implies assessment of implications for the right to data protection. Therefore, this sub-section focuses on how data protection prescriptions facilitate the right to privacy of children. To assess this from the perspective of the new EU Data Protection Regulation is useful because the latter introduces important changes with respect to the current data protection framework.

Although the prescriptions of the current data protection framework set by the 95/46/EC directive are implemented and integrated in Dutch law through the Dutch Data Protection Act, this law is quite limited on the subject of protection of children's personal data. Art. 21 of the current Data Protection Act only specifies that the prohibition on sharing or using healthcare data (including the data of children) by parties in the Dutch justice system, for instance, under the Dutch Youth Care Act is inapplicable if the use of such data is necessary to fulfil their work as set by law.[32] Although this provision provides room for the registration and sharing of certain healthcare data relevant to children's safety via ProKid, Art. 22 also specifies that sensitive data and data with respect to unlawful or objectionable behaviour of a person (including the behaviour of children) as defined by a judge can also be shared if that behaviour is against Dutch laws. The latter prescription can be considered a limiting of the sharing of children's personal data by the police through ProKid particularly because a judge must define what counts as unlawful or objectionable behaviour. Although the data controller of ProKid is the Ministry for Security and Justice, as data are registered by the police, when certain files of children profiled by ProKid are transferred to youth-care institutions or to city councils, the data controller also changes to the relevant ministry responsible for these institutions. Thus far, no data request or claim is known to have been submitted to any of these data controllers on behalf of children by their parents or guardians. This could in part result from the procedure that only those 'at risk' registrations concerning children are communicated to their parents or guardians, although they are also shared by the police with particular authorities responsible for youth care.

However, the EU proposal for a General Data Protection Regulation[33] testifies to a new approach in prescribing the protection of fundamental values via data protection through principles such as 'value-sensitive design' and the employment of 'privacy-enhancing-technologies'. This also has implications for current Dutch data protection rules and the processing of data within and beyond ProKid. Concerning children's right to privacy the "current data protection regulation lacks child-specific rules",[34] which could have been helpful in clarifying the position of children under digital surveillance. However, the proposal for the General Data Protection Regulation is specific about children. The proposal takes, for instance the definition of the child from the UN CRC and considers everyone below 18 years of age a child. It includes such elements as the data subject's 'right to be forgotten' and the 'right for

[29] Charter of Fundamental Rights of the European Union [2000] OJ C364/01.

[30] De Hert, P. & Gutwirth, S., "Making sense of privacy and data protection: A prospective overview in the light of the future of identity, location-based services and virtual residence", in IPTS, Security and Privacy for the Citizen in the Post-September 11 Digital Age: A Prospective Overview. Report to the European Parliament Committee on Citizens' Freedoms and Rights, Justice and Home Affairs (LIBE), July 2003, IPTS Technical Report Series, 111–162.

[31] Privacy impact assessments (PIAs) regularly 'translate' the assessment of privacy into the assessment of personal data processing. Although privacy includes though how data are processed, it also includes many more aspects of life, including those aspects where the idea of registering data at all can remain questioned or simply undone due to, for instance reasons of privacy. For such PIAs see, for instance: <https://ico.org.uk/for_organisations/data_protection/topic_guides/~/media/documents/library/Data_Protection/Practical_application/pia-code-of-practice-final-draft.pdf>; <http://www.norea.nl/readfile.aspx?ContentID=67485&ObjectID=918136&Type=1&File=0000040117_NOREA%20A4%20Privacy%20Impact%20Assessment%2003%20WEB.pdf>; Toetsmodel Privacy Impact Assessment, Rijksdienst, Retrieved on 8th January 2014, from: http://www.rijksoverheid.nl/documenten-en-publicaties/publicaties/2013/06/24/toetsmodel-privacy-impact-assessment-pia-rijksdienst.html.

[32] About this, please see further Art. 21 of the Dutch Data Protection Act.

[33] Proposal for a General Data Protection Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)2012/0011 – C7-0025/12.

[34] Van der Hof, S. 'No Child's Play: Online Data Protection for Children' in S. van der Hof and B. van den Berg and B. Schermer (eds), *Minding Minors Wandering the Web: Regulating Online Child Safety* (Asser Press, 2014).

erasure of data' in an online environment (Art. 17). Because these latter rights are observed to apply "in relation to personal data which are made available by the data subject while he or she was a child" (Art. 17), the proposal introduces not only unique rights for children's rights to privacy but also for their right to data protection. The EU proposal provides further safeguards for children by the explicit prohibition of profiling of children because this type of automated processing of data cannot concern children. These newly established rights and prescriptions of the General Data Protection Regulation all support the enforcement of children's right to privacy and other CRC rights.

2.1.2. *International case law and the right to digital privacy of minors*

The European Court of Human Rights' case law can be considered a fourth, quite strong legal means to allow the significance of children's right to privacy and of CRC rights in general to be raised. Within ECHR case law, there has traditionally been little reflection upon the protection of the digital privacy of children. However, the number of cases in which the Court addressed the vulnerable position of minors in the context of their digital connections has grown in recent years.[35] The case law is chosen specifically in the area of law enforcement because in these cases the ECHR clearly decided – although by referring to Art. 8 of the European Convention on Human Rights and not directly to Art. 16 of CRC – in favour of a 'child's right to privacy' versus 'public safety interests'.[36] Second, in all these cases, the ECHR issued positive obligations for states – in one case for The Netherlands – about the child's right to privacy. These judgments proved to be particularly important because academic research already demonstrated that within Dutch law-enforcement court cases, a child's right to privacy and CRC rights in general are rarely balanced against public safety interests. This increases the necessity of the three ECHR cases in this article because ProKid, an instrument to maintain public safety by prevention, affects the right to privacy of a large number of children and their families and friends on a daily basis in encounters with Dutch law enforcement and beyond. Without precedent, judgments that are made about the privacy effects of systems directly comparable to ProKid, that is, the chosen ECHR judgments, are useful to provide general guidance about the privacy implications of such systems as ProKid. Although the first case concerns children's privacy in general, it sets a remarkable precedent even prior to the rise of the CRC with respect to this right.

In 1985, *X. and Y v. the Netherlands*,[37] the European Court of Human Rights for the first time convicted a state of having violated a child's privacy. The father of a 16-year old mentally ill girl, who had been living in a home for mentally handicapped children, filed a complaint. According to the father, his daughter was raped. Because of her mental condition, he wanted to file a report himself about the crime to the Dutch police. However, according to the Dutch Criminal Code, only the victim herself could report such a crime. Because the father could not file a report on behalf of his daughter and his daughter's mental problem made her unable to file one, no investigation was initiated under the Dutch Criminal Code. Consequently, the girl's parents filed a complaint under Art. 8 of the ECHR against The Netherlands. They argued that the right to respect family life should include the right for parents to report a crime to law enforcement authorities and allow for a criminal investigation in case their daughter became a victim of abuse. The ECHR found that The Netherlands provided insufficient protection for the child under the Dutch Criminal Code and that Art 8. of the ECHR thus was violated by the Dutch state.[38] This was the first time the ECHR found a state openly guilty of breaching Art. 8 of the Convention in relation to a child. From the perspective of ProKid, this judgment is highly relevant. Although crime-related actions of parents and guardians are influential in what risk image is projected on their children by ProKid, the role of parents or guardians in protecting their children from becoming victims of or from committing such actions is not reflected equally within the risk assessment schemes of ProKid. In light of the above judgment, reflecting the protecting role and potential of parents in this scheme could improve the ways in which parents and guardians are currently viewed by ProKid.

S and Marper vs. UK[39] from 2008 is the second case. The case concerns the digital privacy of children within law enforcement procedures. One of the applicants was an 11-year-old boy who was charged with attempted robbery. His fingerprints and DNA samples were taken and registered in the UK DNA database. After he was acquitted he requested the police to destroy his biometric data, but the police rejected the request. Consequently, the applicant requested judicial review at the national court and the European Court of Human Rights. At the ECHR, he argued that the police's retention of his biometric data violated Art. 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms. The Grand Chamber upheld the applicant's complaint and agreed with the violation of Art. 8:

> "the retention at issue constitutes a disproportionate interference with the applicants' right to respect for private life and cannot be regarded as necessary in a democratic society."

[35] See also, for instance the case of Reklos & Davourlis v. Greece No. 1234/05, 2009, EMLR 16; Krone Verlag GmbH & Co KG and Krone Multimedia GmbH & Co KG v. Austria App. No. 33497/07, (ECtHR 17 April 2012); Von Hannover v. Germany App. No. 59320/00, 2004, 40 EHRR 1.

[36] About this, see further: De Graaf, J. H., Limbeek, L. M. B., Bahadur, N. N. & Van der Meij, N. *De toepassing van het internationaal verrag inzake de rechten van het kind in de Nederlandse rechtspraak 1 Januari 2002–1 September 2011* (Ars Libri 2012) Court cases show that the strength of national laws, such as that of the Dutch Police Act, often emerge as stronger reference points than the CRC or other human rights documents. See further, for instance: HR 7 Maart 2014, 13/04683; Rb. Arnhem 16 Februari 2010, BL696; HR 7 Maart 2014, 13/04683.

[37] App. No. 8978/80, 1985, 8 EHRR 235.

[38] Groothuis, M. 'The right to Privacy for Children on the Internet: New Developments in Case Law of the European Court of Human Rights' in S. van der Hof and B. van den Berg and B. Schermer (eds), *Minding Minors Wandering the Web: Regulating Online Child Safety* (Asser Press, 2014). Haeck, Y., & Brams, E. *Human rights and civil liberties in the 21st century* (Springer, 2014).

[39] App. No. 30562/04 and 30566/04, 2009, 48 EHRR 50.

Furthermore, this case includes a handful of unique ECHR judgments in which the court emphasised the special position of children within the criminal justice system[40] and referred to Art. 40 of the CRC:

> "the retention of the unconvicted persons' data may be especially harmful in the case of minors, given their special situation and the importance of their development and integration in society. The Court has already emphasised, drawing on the provisions of Article 40 of the United Nations Convention on the Rights of the Child of 1989, the special position of minors in the criminal-justice sphere and has noted, in particular, the need for the protection of their privacy at criminal trials".

These passages of the above judgment are of particular value regarding how assessments are performed by using ProKid. Although the registry produces risk indications about children who are victims, accused of a crime, or who commit a crime, the above passages of the ECHR judgment de facto condemn the retention of data by members of the justice system when such data concern accused persons – and the judgment can be interpreted similarly regarding victims. Furthermore, the judgment also underlines the necessity for distinguishing between victims, suspects and convicts.

The third case, *KU v. Finland*,[41] concerns the digital privacy of children on the Internet, the only case so far that specifically addresses this issue. The case addressed cybercrime, more specifically, the fraudulent use of a child's personal data on the Internet, which led to the child's forced, digital exposure to paedophiles. In 1999, an unknown person posted an advertisement on the Internet in the name of a 12-year child without his knowledge. The advertisement contained information about the boy's desire to meet others for intimate relationships. The boy only learnt about the ad when a response landed in his mailbox from a paedophile. The boy's father requested the police to find out who posted the ad, but the telecommunications provider refused the demand of the police to unveil the identity of the ad poster because it considered itself bound by Finnish telecommunication legislation. The police's request under the Criminal Investigation Act to divulge the identity of the ad poster was also refused by the Helsinki District Court because it found that without stronger evidence, it only constituted a calumny of a person. However,

> "the Court preferred to highlight the notion of private life [Art. 8 of ECHR], given the potential threat to the boy's physical and mental welfare and his vulnerable age."

It formulated further a condemnation:

> "The Court considered that the posting of the Internet advertisement about the applicant had been a criminal act which had resulted in a minor having been a target for paedophiles. It recalled that such conduct called for a criminal-law response and that effective deterrence had to be reinforced through adequate investigation and prosecution. Moreover, children and other vulnerable individuals were entitled to protection by the State from such grave interferences with their private life."

The judgment sets a precedent by underlining the positive obligation of each member state to continuously update and modify their legal system – including its criminal law and other legal fields specialising in mass media, Internet and telecommunications,[42] so that children could enjoy sufficient protection from risks on the Internet. The judgment proves to be a revelation with respect to how colour-code indications are set-up and risk indications are performed by ProKid. First, it clearly concerns a crime related on the one hand to the home environment of the child, but on the other hand, a crime that is performed by persons living far away from the child's home. In other words, the harm came not directly from any influence of persons living in the home of the child. Second, this judgment underlines state authorities' obligation to take all measures to protect individuals, particularly children, from digital risks. At the same time, the judgment also bears the implication that state authorities in particular should live up to the above obligation, in regard to potential negative consequences of risk profiling practices such as those performed with ProKid.

2.1.3. *Interim conclusion*

Because of the above, CRC rights and particularly children's right to privacy are strengthened in different forms by legal tools such as the Charter of Fundamental Rights and Freedoms of the European Union, the Proposal for General Data Protection Regulation of the European Union and different ECHR case laws. In three ECHR cases in particular, all concerning the privacy of children, Art. 8 of the European Convention on Human Rights was used as a reference source. However, because all three cases addressed issues concerning children, they indirectly strengthen children's right to privacy including their digital privacy as laid down by the UN Convention on the Rights of the Child. The three judgments further show that this duty of states towards government authorities in particular, including law enforcement authorities, must be approached strictly because their collection and processing of personal data can have potentially negative consequences on children's lives and their ability to develop their life and identity. To conclude, a relevant lesson can also be drawn from the above court cases for the design and use of such identity management and, in particular, preventative, risk assessment systems on children such as ProKid. By following CRC principles during the design and use of such systems, future ECHR court cases on the privacy of children could be avoided. In light of this point, the above rulings stimulate the enforcement of the CRC.

[40] Bellanova, R., & De Hert, P. 'Le cas S. et Marper et les données personnelles: l'horloge de la stigmatisation stoppée par un arrêt européen' (2009) 4 (76) Cultures & Conflits 101. Koops, B. 'Law, Technology and Shifting Power Relations' (2010) 25 (2) Berkley Technology Law Journal 973.

[41] App. No. 2872/02, 2008 (2009), 48 EHRR 1237.

[42] Groothuis, M. 'The right to Privacy for Children on the Internet: New Developments in Case Law of the European Court of Human Rights' in S. Van der Hof and B. van den Berg and B. Schermer (ed), *Minding Minors Wandering the Web: Regulating Online Child Safety* (Asser Press, 2014).

2.2. IDM systems and pitfalls of their use

Identity management systems serve to establish 'identities' (defined as personal data sets) within citizen–state relationships. This includes the identities of persons subject to the system, in this case children and families, and those professionals (e.g., police or technicians) who interact with systems, such as ProKid, on a regular basis. Identity management systems are used on a large scale and in different forms internationally, ranging from biometric identification systems, e-government solutions to a growing number of administrative systems introduced to assess persons against various forms of risks within citizen–state relations.[43] The dynamics by which these systems produce vast amounts of information about citizens have also been referred to as contributing to an "information-intensive government",[44] or information-led government called "i-government".[45]

This information intensity in itself seems to be a development that is 'common' to present-day society. However, when being used, IDM systems are highly capable of extensive surveillance of persons[46] and thus intrusion into individuals' privacy and their freedoms.[47] They extend an ever expanding steering or disciplining effect on human behaviour,[48] performing discriminative selections amongst citizens[49] and encompassing unintended secondary implications for citizens' lives, a phenomenon also known as function creep.[50] Scholars in science and technology studies stress the normative effects emerging between IDM technologies and their users because both continuously and mutually affect one another throughout all the actions to which they become parties.[51] Users and their technologies both share responsibility for transformations occurring from the use of IDM technologies.[52] Inspired by these observations, an analysis of ProKid from a CRC perspective lends itself to being very relevant and necessary in a democratic society.

Such an actuality results in a generally large increase in the number of IDM technologies and the extent to which children are exposed to digital risk assessment within youth care and policing practices internationally. Examples of systems similar to ProKid are operational in other countries such as the U.S. (Partnership For Youth At Risk – PFYR).[53] The Partnership for Youth At Risk started in 2000 as a fire-setting-prevention program for youth and evolved into an educational, incident register. Each registration in PFYR happens after an authority connected to the system, such as the police, Juvenile Justice Services or therapists, reports a fire-setting incident by a young person aged between 5 and 18 years. Subsequently, parents also are notified by PFYR so that they can register their child into the PFYR educational programme. The programme is aimed at developing the registered child into a person more reflective about his/her deeds and thus prevent his/her recidivism.

Another registry called Contact Point in the United Kingdom is particularly interesting from the perspective of the analysis in this paper. Contact Point was only operational for a short time. Interestingly, due to a governmental decision, Contact Point was inactivated and the gathered data deleted as of 2010.[54] The reasons given for termination included fierce criticisms of the registry's centralised set-up and the system's potential for extensive and long-term surveillance of a large part of society.[55] In particular, each registration about a child updated a central database that a wide range of professionals could access, which was a perceived breach of children's right to privacy of the CRC (Art. 16) and their families' privacy in ECHR (Art.8). Basing reasons for the termination of Contact Point on children and human rights arguments in the UK is a unique and rather atypical although encouraging phenomenon that runs counter to a current tendency in Western societies to register high-risk youth.[56] Moreover, reliance upon such registries is growing.

---

[43] Hildebrandt, M., & Gutwirth, S. (eds) *Profiling the European citizen* (Springer Science, 2008).

[44] Lips, M., Taylor, M., & Morgan, J. 'Identification practices in government: citizen surveillance and the quest for public service improvement' (2008) 1 Identity in the Information Society 135.

[45] Wetenschappelijke Raad voor het Regeringsbeleid (WRR) *iGovernment Synthesis Report 86* (Amsterdam University Press, 2011).

[46] Lyon, D. *Surveillance society Monitoring everyday life* (Open University Press, 2001).

[47] Nissenbaum, H. 'Privacy as contextual integrity' (2004) 79 Washington Law Review 119. De Hert, P. 'Identity management of e-ID, privacy and security in Europe A human rights view' (2008) *13*(2), Information Security Technical Report, 71. Hildebrandt, M., & Gutwirth, S. (eds) *Profiling the European citizen* (Springer Science, 2008). Koops, B.-J., & Leenes, R. 'Code and the slow erosion of privacy' (2010) 12 Michigan Telecommunication and Technology Law Review, 115.

[48] Vedder, A. 'Convergerende technologieën, verschuivende verantwoordelijkheden' (2008) 34 (1) Justitiele verkenningen 54.

[49] Bowker, G. C., & Leigh Star, S. *Sorting things out Classification and its consequences* (MIT Press, 1999). Van der Ploeg, I. *'Security in the Danger Zone: Normative Issues of Next Generation Biometrics'* in Mordini, E. & Tzovaras, D. (eds) *Second Generation Biometrics The Ethical, Legal, and Social Context* (Springer, 2012).

[50] Prins, J. E. J. 'Function creep: over het wegen van risico's en kansen' (2011) 37(8) Justitiele Verkenningen 9. Van der Hof, S. & Groothuis, M. (eds) *Innovating Government Normative, Policy and Technological Dimensions of Modern Government* (Asser Press, 2011).

[51] Latour, B. *Science in action: How to follow scientists and engineers through society* (Harvard University Press, Cambridge, Massachusetts, 1987). Law, J. & Mol, A. *Situating Technoscience: an inquiry into spatialities* (Lancaster University, 2003).

[52] Suchman, L. *Human-Machine Reconfigurations: Plans and Situated Actions* (Cambridge University Press, 2007). Oudshoorn, N. *Telecare technologies and the Transformation of Healthcare* (Palgrave Macmillan, 2011).

[53] About 'Partnership for youth at risk' see: <http://www.partnershipsforyouthatrisk.org/sections/registration/registration_main1.htm>.

[54] Contact Point was in place to register 'risk summaries' about all children in the UK in order to prevent potential cases of child abuse and other crimes related to youth.

[55] Hoyle, D. 'ContactPoint. Because every child matters?' 2010 The encyclopaedia of informal education <www.infed.org/socialwork/contactpoint.htm>.

[56] Australia, for instance, developed a governmental protocol for child protection professionals. The High Risk Youth practice requirements serve to signal and assist youth associated with risks. About this, see further: <http://www.dhs.vic.gov.au/cpmanual/practice-context/children-in-specific-circumstances/1014-high-risk-adolescents-hra-practice-requirements/3>.

2.3. *Plea for a CRC-based perspective within digital identity management of children*

This paper argues that fundamental children's rights such as those laid down in the Convention on Rights of the Child can be used to broaden the legal framework for the use of digital surveillance technologies on children. Nevertheless, the role these rights might play has not received much attention because it is data protection regulations that are regularly brought to the table as a source of legal 'help'. This is due in part to the fact that rather complex notions of identity and privacy of children are often "translated"[57] into seemingly simple problems of personal data.[58] Although the production, processing and storage of personal data and the protection of privacy are two different issues, as mentioned earlier, a variety of privacy impact assessments[59] shows that handling the problem of production, processing and storage of personal data by regulation often is considered 'adequate' protection of the individual's privacy. Consequently, the use of identity management technologies is often discussed (only) in terms of personal data protection. This reflects a certain assessment of identity management technologies as pure instruments through which personal data pass unchanged. In other words, the constructive effects stemming from the very use of technologies on privacy and identity of persons are often not considered, mostly because there is no legal liability established for technologies only for their users. Although data protection regulations are indispensable for protecting children's personal data, it would be worthwhile to rely more heavily on the opportunities offered by the CRC, allowing the pitfalls and risks for children stemming from the very use of these technologies to be specifically addressed in light of this dedicated fundamental rights regime.

3. CRC challenges in light of the initiative and practical implementation of ProKid

To assess CRC challenges with respect to ProKid in particular, this section addresses the issue in two sub-sections. First, the initiative of ProKid will be assessed. This includes a description of its system and an analysis of certain aspects from a CRC perspective, which could be viewed as underpinning and legitimising the initiative of ProKid. The first sub-section ends with a discussion about already-raised issues surrounding the initiative and system of ProKid. The second sub-section provides a more practice-oriented approach and details a set of effects regarding the purpose, design and daily use of ProKid on relevant CRC prescriptions.

3.1. *ProKid: its initiative*

ProKid SI 12- (henceforth, ProKid) has been initiated as a risk-signalling system by the Dutch police to signal children under the age of 12 years who might either be victims, witnesses or perpetrators of some form of a crime. The basis of ProKid is to be found in a number of Dutch laws (Social Support Act, Public Health Act, Youth Care Act, the Compulsory Education Act, Police Act) which describe responsibilities for state, province and local government levels regarding the care of young people. A number of fundamental principles underlie the legal framework within which the development of a comprehensive multidisciplinary chain approach for youth is described. One of these principles is formulated in a working process implemented in 2007 to foster collaboration between the Dutch police and Bureau Youthcare that, up until January 2015, also formed the basis for ProKid: "Early identification and referral".[60] The justifications for this collaboration and, more specifically, the initiative of ProKid have been that the police and Bureau Youthcare could improve their information-exchange and more successfully prevent children from developing criminal behaviour.[61]

These reasons remained the same; however, due to the mentioned administrative and legal change as of January 2015, the sharing of information by the police and youth care institutions became restructured and channelled differently. Up to that point, the police had reported directly to Bureau Youthcare about all concerns they had about children and that they deemed important that Bureau Youthcare knew about. However, as of January 2015, the existing Bureau Youthcare institutions have been abolished in The Netherlands through the new Youth Care Act, and their associated tasks have been transferred to city councils and to other newly certified institutions. Therefore, the police must report to different institutions depending on the issue with a child. For instance, child abuse and domestic violence cases in which children are also involved need to be reported to the so-called Advice and Reporting Centre Domestic Violence and Child Abuse (ARCDC).[62] For other issues with children, including those indicated by ProKid, the police must inform the newly certified youth care agencies or city councils.[63]

The Ministry for Safety and Justice approached the development and implementation of ProKid without a primary CRC consideration in mind.[64] However, the stated objective – to prevent children from developing a criminal behaviour – can be considered as serving Art. 3, "the best interest of the child". Thus far, the Dutch Data Protection Authority did not issue any specific opinion about ProKid. However, the authority issued

[57] Latour, B. *Science in action: How to follow scientists and engineers through society* (Harvard University Press, 1987).
[58] About this see also footnote 29.
[59] Ibid.
[60] Goedee, J., Rijkers, A. *Zorgsignalen van de Politie: Over het werk process 'Vroegsignaleren en doorverwijzen' tussen Politie en Bureau Jeugdzorg* (Ministerie van Jeugd en Gezin, 2010).
[61] About this, see further: ibid, pp. 8.
[62] Advice and Reporting Centre Domestic Violence and Child Abuse (ARCDC).
[63] Schreuder, E. *Privacy Impact Assessment (PIA) deelproject Justitiële Keteninformatisering 'Risico' s en Privacy by Design bij de justitiële ketenberichten voor de Jeugdwet'* (Net2Legal, 2014) Retrieved on 14th December 2014 from: <http://www.voordejeugd.nl/attachments/article/1570/Bijlage%20PIA%20Keteninformatisering.PDF>.
[64] *Afsluitende Uitgave Programma Aanpak Jeugdcriminaliteit* (Ministerie van Veiligheid en Justitie, 2011) Retrieved on 17th of July 2012, from: <http://www.wegwijzerjeugdenveiligheid.nl/fileadmin/w/wegwijzerjeugdenveiligheid_nl/oudesite/doc/criminele_jongeren/afsluitende_uitgave_programma_aanpak_jeugdcriminaliteit.pdf>.

Table 1 – ProKid colour-code classifications (including criteria for both a child and his or her living address).[70]

Category	Behavioural indicators	Living address of the child
White: No risk indication, most likely a safe zone	Maximum of two registrations as a victim or as a witness	A minimum of two registrations of the living address as the location of an incident *and* A maximum of 5 registrations of the co-habitants of the child
Yellow: Indication of a rising risk potential	3–9 registrations as a victim or as a witness, *or* A minimum one registration as a suspect of a light incident *or* One time registration as a missing person	A minimum of 3 registrations of the living address as the location of an incident, *or* More than 5 registrations of co-habitants of the child in the system, *or* The sum of the two above mentioned registrations is 6–14
Orange: Indication of 'problem youth'/'problem address'	A minimum of 10 registrations as a victim or as a suspect, *or* A minimum of 5 registrations as a suspect of a light incident (for instance, shoplifting) *or* A minimum of 5 registrations as a victim or as a witness related to different types of incidents, *or* More than one-time registration as a missing person, *or* One registration as a suspect of a serious crime	The sum of the incident registrations at the living address of the child and the registrations of co-habitants of the child is 15–29, *or* 1–2 registrations of domestic violence at the living address, *or* One registration of child abuse at the address of the child
Red: Alarm phase (indication of criminal youth/ alarm address)	A minimum of two registrations as a suspect of a serious crime	The sum of the incident registrations at the living address of the child and the registrations of co-habitants of the child is 30 or greater than 30, *or* More than two registrations of domestic violence at the living address of the child, *or* More than one registration of child abuse at the address

a negative opinion[65] concerning the registration and exchange of information about children aged between 6 and 12 years by a system of a Dutch cluster institution that is involved with youth, called Safety House[66] (in Dutch: Veiligheidshuis): *"Children aged under 12 years are not criminally prosecuted. The processing of their data in the system under study is therefore not consistent with the objective of the [Safety House] consultations and that is against the law."*[67]

Behavioural scientists from Radboud University of Nijmegen developed the colour codes for ProKid[68]; white, yellow, orange and red codes signify a growing gradation of concern. Both children and their living addresses can have assigned colour codes (see Table 1). Assigning children white signifies that no risk has been identified yet, yellow represents a possible development of risks, orange indicates that problems and even criminal behaviour have already occurred, and red symbolises children who have repeatedly shown criminal behaviour, or of whom multiple cases of suspicion have been recorded. Concerning the living addresses, yellow signifies either that earlier incidents have been registered at the address or that a person living at the same address has multiple incident registrations[69](for more yellow indicators, see Table 1). Yellow, for instance, can signify a higher number of incidents related to the address or of police registrations related to a person living at the same address, or the combination of these registrations. An orange code can signify, for instance, that the sum of incidents registered at the address and about persons living at the same address is greater than 15 (for more orange

[65] *Veiligheidshuizen onzorgvuldig met gegevens van minderjarigen: CBP onderzoekt gegevensuitwisseling in veiligheidshuizen* (CBP, 2011) Retrieved on 2nd of December 2013, from: <https://cbpweb.nl/nl/nieuws/veiligheidshuizen-onzorgvuldig-met-gegevens-van-minderjarigen>.

[66] Within Safety Houses representatives of youth care, law enforcement and municipal administration organisations gather and discuss cases of delinquent children (and families) in order to initiate adequate assistance. See also: <http://www.veiligheidshuizen.nl/>.

[67] See link in footnote 59.

[68] Nijhof, K. S., Engels, R. C. M. E. & Wientjes, J. A. M. 'Crimineel gedrag van ouders en kinderen' (2007) 27 (1) Pedagogiek, 29.

[69] Abraham, M., Buysee, W., Loef, L., & Van Dijk, B. *Pilots ProKid Signaleringsinstrument 12- geëvalueerd Pilots ProKid Signaleringsinstrument 12- geëvalueerd* (DSP-groep, 2011).

[70] Table translated into English from: Abraham, M., Buysee, W., Loef, L., & Van Dijk, B. *Pilots ProKid Signaleringsinstrument 12- geëvalueerd Pilots ProKid Signaleringsinstrument 12- geëvalueerd* (DSP-groep,

indicators, see Table 1). Red can signify that the combination of incidents registered at the same address and incidents persons living there have been involved in are greater than 30 (for more, see Table 1). If a child already has a colour-coded file in ProKid and an incident occurs at the living address of the child, a darker colour is assigned to the child's address. That assignment also influences the colour-code of the child living there. It becomes automatically darker (for example, from yellow to orange). Each time the colour of the address darkens, the code of a child darkens too, symbolising that a risk in his/her closest social environment has emerged for a child. After a maximum of 5 years, a registration must be deleted from ProKid. ProKid has been operational nationwide since 2013.[71]

The risk categories and their attribution are explicitly aimed at the early detection of potential criminal behaviour of children. The assignment of colour codes is automated by means of algorithms, and conclusions about assigning a code are drawn from information in other large police databases. These include the Basic Facility for Law Enforcement (BFLE, or Basisvoorziening Handhaving in Dutch) and the Basic Facility for Forensic Investigation (BFFI, or Basisvoorziening Opsporing in Dutch). Information from ProKid is also shared amongst youth care partners who have not yet switched to digital systems. ProKid managers have been invited to the weekly discussions organised by Bureau Youthcare until the end of 2014 [72] in which the invited ProKid manager could decide whether there is reason to share information about a registered child with other professionals. ProKid managers have been enjoying a relatively large freedom in defining criteria according to which they submit cases to Bureau Youthcare, except for one general standard that requires practitioners to consistently submit red coloured files to Bureau Youthcare by the time such a file appears in the system.[73] As of January 2015, these files need to be forwarded to other responsible youth care institutions depending on the nature of a case. This specific information-sharing practice of the police towards Bureau Youthcare and as of January towards other institutions through ProKid is in line with the "Early detection and referral" duty of the Dutch, which was introduced in 2010.[74] Because the system is considered purely a preventative tool to be used by the police, ProKid is an unparalleled example of its type because it is not a police system used during criminal investigations. However, it is regularly and primarily framed as a police instrument to facilitate the protection of children both from harm coming to them and harm they might cause themselves. Therefore, to learn how the purpose, design and daily use of ProKid challenges CRC prescriptions, two aspects are chosen first as being particularly beneficial to the analysis of ProKid: its legitimisation and the controversies associated with it.

3.1.1. *Legitimisation of ProKid*

Art. 3 of the CRC specifies that the "best interest of the child" as a principle enjoys utmost priority with respect to issues in relation to children. In general, the initiative and system of ProKid can be considered as in line with the prescriptions of Art. 3. because it is meant to facilitate protection of children both from forms of violence and from their developing anti-social behaviour or certain crime dispositions. Both purposes can be considered in "the best interest of the child"; however, the responsibility of the state to provide such protection for children, in this case with the help of ProKid, is not straightforward according to CRC principles.

Art. 18, 19 and 20 of the CRC leave the primary responsibility with the parents to care for and protect their children. Only in the case that a child's parents become unable to perform this duty adequately or at all should states take up responsibility and intervene in a family's life to provide the best care for a child. From the perspective of children's rights, however the Dutch Supreme Court issued a judgment on September 21, 2012, perhaps the most important section of which reads as follows:

> "The state has the duty to safeguard the rights and interests of children, even in regard to minors without a permit. These children cannot be held responsible for the actions of their parents or other family members."[75]

This judgment changed the dominant view of the Dutch state that parents are primarily responsible for the wellbeing of children and explicitly assigned to the state primary responsibility for the care and welfare of children. To protect children from any forms of maltreatment executed in any physical or mental form against them, Article 19 allows for governments to employ whatever means[76] are considered most appropriate to prevent such issues. Given the above judgment of the Supreme Court, ProKid can be considered a system legitimately installed by the government amongst others to sustain what is prescribed by Art. 18, 19 and 20.[77]

Art. 6 also prescribes a duty "to ensure to the maximum extent possible the survival and development of the child". The duty to prevent children from developing forms of anti-social

[71] Tweede Kamer, Vaststelling van de begrotingsstaten van het Ministerie van Veiligheid en Justitie (VI) voor het jaar 2013 (Tweede Kamer der Staten General, 2012).

[72] The parents of those children whose case has been forwarded by ProKid managers to Bureau Youthcare (or to other certified youth care institutions as of January 2015) receive a letter of notification about this action. For more, please consult Abraham, M., Buysee, W., Loef, L., & Van Dijk, B. *Pilots ProKid Signaleringsinstrument 12-geëvalueerd Pilots ProKid Signaleringsinstrument 12- geëvalueerd* (DSP-groep, 2011).

[73] Ibid.

[74] Kruize, G. & Gruter, P. *Kattenkwaad of misdaad in het verschiet? Een evaluatie van het werkproces "Vroegsignaleren en doorverwijzen 12-delictplegers"* (Amsterdam – ATENO Bureau voor criminaliteitsanalyse, 2013).

[75] HR 21 September 2012, NJ 2013/22, m. nt. Alkema, JV 2012/458, m.nt. Slingerberg AB 2013/30, de Vries; LJN: BW5328.

[76] In February 2011 a 'General Comment 13 on Article 19 of the Convention of the Right of the Child The right of the child to freedom from all forms of violence' had been adapted which outlines for governments how to develop tools (administrative, legislative and other) to maintain this right of children. (See also Lee, Y. & Svevo-Cianci, K. 'General Comment no. 13 to the Convention on the Rights of the Child: The right of the child to freedom from all forms of violence' (2011) 35(12) Child Abuse & Neglect, 967).

[77] For more, see also the Dutch 'Youthcare Act' and Goedee, J., Rijkers, A. *Zorgsignalen van de Politie: Over het werk process 'Vroegsignaleren en doorverwijzen' tussen Politie en Bureau Jeugdzorg* (Ministerie van Jeugd en Gezin, 2010).

or delinquent behaviour can also be considered in line with this prescription. More specifically, to prevent anti-social and delinquent behaviour of children, the 'Youth Care Act'[78] and the 'Social Support Act'[79] set out further norms for professionals about how to address issues related to such behaviour of youth in The Netherlands. ProKid can in part be considered a system to maintain Art. 6 of the CRC. Therefore, the CRC articles reflected upon in this section can be viewed as provide legitimisation for the establishment and use of ProKid by the Dutch government.

Although the introduction and use of ProKid appears legitimate on the grounds raised above, developments related to the CRC within the judicial areas in which ProKid is implemented raise certain controversies. The following section describes three main controversies concerning both the design and use of ProKid in the affected jurisdictions. First, these communicate a more accurate picture of the dilemmas with respect to the design and use of the system. Second, they are useful for analysing the potential of the CRC within the context of ProKid.

3.1.2. *Controversies associated with ProKid*

3.1.2.1. Prevention or law enforcement. The first controversy centres on the issue that ProKid has primarily been initiated for use by the police as a preventative system and not as one for criminal investigations of youth. Children under the age of 12 years cannot be held responsible within penal law procedures.[80] However, ProKid assesses precisely children below that age. According to Art. 13 of the Dutch Police Act, however, there is agreement *"on the deployment of police forces for the purpose of maintaining public order and assistance or care, respectively, for the purpose of criminal law enforcement and to serve justice"*. However, the purpose, design and daily use of ProKid, as we will see in the next sections, epitomises an evolution in which a seemingly caring orientation by the police towards youth is reasoned with law enforcement arguments. This in itself could perhaps be part of a tendency in which boundaries between youth care and law enforcement tasks in relation to youth increasingly blur. However, such blurring is often controversial and heavily criticised by legal scholars: *"child welfare and public order should not be mixed but take advantage of each other's professionalism and continue to pursue a clear delineation of tasks"*.[81] Such criticism finds even more foundation in light of Dutch court rulings about the relevance of the CRC. As the earlier Dutch court rulings in law enforcement cases have shown, the CRC's relevance is minor in criminal cases compared with other jurisdictions in Dutch law. A major criticism is that the 'best interest of a child' is regularly outweighed by 'the interest in maintaining public order'.[82] The criticism about the scarce incorporation of the CRC within criminal law practices and the urge for a more CRC-driven law enforcement is not only a Dutch-specific issue but also is raised internationally: *"criminal law fails to provide practical and effective protection for the [CRC] rights guaranteed by Art. 3"*.[83]

3.1.2.2. Data protection 'light' for the police also on children under 12?. A second controversy concerns data protection prescriptions. The Dutch police as a law enforcement body according to the Police Act are subjected to a 'lighter' data protection regulation[84] than are other public or private parties to allow for the police and other law enforcement bodies to gain extra pieces of information during criminal investigations. However, that the police are legally not allowed to conduct criminal investigations on persons under the age of 12 and that ProKid is used specifically for digital assessment of children under 12 years of age, surfaces not only ethical but also legal contradictions. If the police do not perform law enforcement but only prevention on children, then how can a 'lighter data protection' rule apply for the police concerning the use of ProKid? This seems a fair question to raise, particularly because ProKid is digitally connected to other Dutch law enforcement databases that 'strictly' contain law enforcement information. These are the already-mentioned Basic Facility for Law Enforcement and the Basic Facility for Forensic Investigation. The police have exemptions from the general data protection laws through the Police Data Act for the gathering and processing of such information. Such digital connections might be acceptable in relation to perpetrators, but are legally and ethically questionable in relation to child victims and witnesses both on the grounds of the Police Data Act and of such CRC prescriptions as Art. 39, which assigns special protection for child victims and witnesses of violence.[85] Furthermore, because, as mentioned earlier, child victims, witnesses and those accused of perpetration require different types of assistance, upholding the distinction between child perpetrators, victims and witnesses proves to be highly desirable and very much in the best interest of a child.

---

[78] Wet op de Jeugdzorg 2004 (Youth Care Act) Retrieved on 5th June 2014, from http://wetten.overheid.nl/BWBR0016637/.

[79] Wet Maatschappelijke Ondersteuning 2007 (Social Support Act). Retrieved on 29th October 2013, from http://wetten.overheid.nl/BWBR0020031/.

[80] Politiewet 2012 (Police Act). Retrieved on 10th June 2014, from http://wetten.overheid.nl/BWBR0031788/.

[81] Bruning, M. R. 'De wettelijke taken van de jeugdbescherming. Hoe kan vanuit de jeugdbescherming bijgedragen worden aan de veiligheid in wijken en buurten? Mogelijkheden en onmogelijkheden' (2010). Speech given at *Themabijeenkomst Samenwerken op het gebied van veiligheid en jeugdbeleid Statenzaal Provincie Zuid-Holland*, May 2010.

[82] De Graaf, J. H., Limbeek, L. M. B., Bahadur, N. N. & Van der Meij, N. *De toepassing van het internationaal verrag inzake de rechten van het kind in de Nederlandse rechtspraak 1 Januari 2002–1 September 2011* (Ars Libri, 2012).

[83] Kilkelly, U. 'The Best of Both Worlds for Children's Rights? Interpreting the European Convention on Human Rights in the Light of the UN Convention on the Rights of the Child' (2001) 23(2) Human Rights Quarterly, 308.

[84] Wet politiegegevens 2007 (Police data Act). Retrieved on 12th April 2014 from http://wetten.overheid.nl/BWBR0022463/.

[85] The 'Guidelines on Justice and Matters involving child victims and witnesses of crime' which is routed in CRC prescriptions also states that *"child victims and witnesses are particularly vulnerable and need special protection[. . .] in order to prevent further hardships and trauma that may result from their participation in the criminal justice process"*. See further: *Guidelines on Justice and Matters involving child victims and witnesses of crime* ECOSOC Resolution, 2005/20 of 22/July/2005. Retrieved on 26th November 2014 from <http://www.un.org/en/ecosoc/docs/2005/resolution%202005-20.pdf>.

3.1.2.3. *Anti-social behaviour is not equivalent to delinquent behaviour*. A third source of controversy lies in the fact that ProKid is designed both to prevent problems of child abuse and anti-social behaviour of children. There is a general international consensus that any form of child abuse is unacceptable. In line with this, Art. 19 of the CRC prescribes that governments "protect the child from all forms of physical or mental violence, injury or abuse". The issue of anti-social behaviour of children is more complicated. The CRC has no clear definition or prescription about what legal principles should guide professionals to prevent anti-social behaviour of children, if they have not yet committed crimes but show signs of anti-social behaviour. The CRC only prescribes guidance for cases when children are already in conflict with the law; for example, Art. 40 prescribes that each child "must be treated in a way that promotes the child's sense of dignity". Whether this principle could be interpreted as a general requirement against all children, including those who show anti-social behaviour, requires children's rights discussions.

3.2. *ProKid: its practical operation*

These three main controversies provide many grounds for a thorough CRC analysis of ProKid with respect to its specific purpose, design and daily use. First, according to prescriptions of the Dutch penal law, as mentioned earlier, children under the age of 12 years cannot be held responsible for law breaking. However, the purpose, design and daily use of ProKid shows an evolution in which law enforcement and care categories increasingly overlap. For instance, the fact that the status of child victims, witnesses and perpetrators of crime can fall under the same colour code demonstrates such overlaps and raises questions relevant to the CRC.

3.2.1. *Purpose and design of ProKid*

Concerning the purpose and design of ProKid, the following CRC articles are relevant.

3.2.1.1. *Art. 16.* To systematically register issues about children in ProKid who have not committed any crime but are, for instance, witnesses challenges Art. 16 of the CRC. Discussions about whether the ProKid practices on innocent children constitute arbitrary or unlawful interference with these children's privacy need to be held both in professional and public forums.

3.2.1.2. *Art. 39.* The Dutch Police Act requires the police to facilitate the provision of care for children; however, such facilitation does not directly imply that the police themselves would be allowed to take up the task of providing care for children. Through the unprecedented introduction and use of ProKid, however, the Dutch police de facto undertake a preventative youth care task. The legitimacy of the police acting in the role of youth care provider is a crucial topic to discuss. In light of Art. 39 of the CRC, the following question arises: to what extent is risk profiling of children by the police comply with the prescription, *"Parties shall take all appropriate measures to promote physical and psychological recovery and social reintegration of a child victim . . . Such recovery and reintegration shall take place in an environment which fosters the health, self-respect and dignity of the child"*. To what extent does the Dutch state live up to these prescriptions and take care that neither the dignity of the child nor the conditions of his/her social environment are jeopardised by the very risk profiling practice of the police? A more practical question emerges in light of the risk profiling practice regarding the argument that ProKid is a system used purely for preventative youth care purposes by the police. Why keep the age limit of children assessed by the system at 12 years and not use the age limit of 21 years prescribed by the Youth Care Act? If the system does not produce – not even in its effects – 'criminal records', why follow the 12-years age limit prescribed by the Dutch Police Act? This act prohibits law enforcement investigations against children under the age of 12. This logic suggests an implicit law enforcement reasoning behind the set-up of ProKid. This reasoning can also be deciphered from how requirements for assigning a colour in ProKid are arranged.

3.2.1.3. *Art. 40.* At first sight, colour-codes provide no distinction between victims, witnesses and perpetrators because the behavioural scientific underpinnings of ProKid suggest that any child registered as a victim has the potential to develop into a perpetrator during his/her life.[86] The impossibility to distinguish at first sight between victims, witnesses and potential perpetrators through the colour coding of ProKid challenges Art. 40 section 2(i) of the CRC. The extent to which those practitioners who view the ProKid files consider profiled children innocent because this is prescribed by the right of every child "to be presumed innocent until proved guilty" remains unclear. The blurring of boundaries between child victims and perpetrators shakes the ground upon which prevention practices for recidivist youngsters and victims of child abuse or of domestic violence have been shaped and purposefully separated by dividing legal jurisdictions (e.g., into criminal law or youth care law).

This occurs to some extent because the maintenance of public order is considered a common interest, whereas the right of the child is in practice often juxtaposed against this common interest to imply only the right of one individual child. Certainly, children's rights, as with any human rights, imply a common relevance for all and should be practiced accordingly.

3.2.2. *The daily use of ProKid*[87]

The Kinderechtenmonitor[88] devoted a section to advise the Child Ombudsman about focussing on the extent to which it is transparent for parents how a risk calculation is made in ProKid, whether parents are informed about such a risk registration,

[86] Abraham, M., Buysee, W., Loef, L. & Van Dijk, B. *Pilots ProKid Signaleringsinstrument 12- geëvalueerd Pilots ProKid Signaleringsinstrument 12- geëvalueerd* (DSP-groep, 2011).

[87] Parts of the empirical material in this section also appeared in La Fors-Owczynik, K. & Valkenburg G.: 'Risk identities: constructing actionable problems in Dutch youth' in Digitizing Identities, (Routledge, forthcoming in 2015).

[88] Kinderrechtenmonitor: in English 'Children rights' monitor' is a journal of the Dutch Child Ombudsman's office.

and how professionals balance between risk and protection factors during their decision making about a child.[89]

The use of ProKid in daily practice shows that risk factors come earlier than 'protecting' factors when deciding about a risk profile for a child. This is in part so because in practice, risk profiles of a large number of persons influence the risk qualification of a child. More than only the family members' profiles living at the same address with the child contribute to the colour code of a child because this is formally integrated into the system. A ProKid manager explains that during assessments, growing attention is focussed on the child's larger social environment, from where 'bad influences' are registered as aggravating factors for a child's development:

> "Suppose there was a fight between neighbours. [. . .] Then, I know that the children of the neighbours have probably been involved in that fight, too. The police come and make a report. Then, in ProKid, I see that a child from one address fought with a child from the neighbouring address. I can then check back in time, and see that these children's fathers also fought, two years ago. I can then connect these things, and that is the analysis I do." (ProKid manager, city B).

This demonstrates that the criminal profiles of neighbours are also incorporated into the risk calculation about a child. Furthermore, practice demonstrates that the risk profiles of a child's friend also become relevant for assigning risks to a child in ProKid:

> "If I see a child who has a 'yellow' or 'white' colour code, and although officially the case is 'not yet worth' being sent to Bureau Youthcare (BYC),[90] but if a friend of that child is 'red' in the system, then I share this extra information [about the 'yellow' or 'white' colour coded child] during the case discussion within BYC." (ProKid manager, city B).

The risks identified in relation to the father, the neighbour or the friends of a child are combined and observed to provide a 'more sophisticated' risk image about a child. Simultaneously, these associations between profiles increase the concern about the wellbeing of a given child.

The urgency to associate and register, for instance, the antisocial or criminal behaviour of a parent – living at the same address with a child – as an aggravating concern for the development of the child is based upon arguments of behavioural science. One main argument for these is that children having been witnesses or victims of violence at home will develop a predisposition to crime in their future. Taking this seriously appears to be a legitimate effort of the state and in line with Art. 3 of the CRC as protecting children from wrong influences can be viewed as being in their best interest. However, how this protection is put in place by ProKid requires a broader CRC discussion. The digital registration of risk associations to parents and, as observed, even to neighbours and friends of a child, can also be viewed as building a de facto 'pre-criminal' record for the child through a quasi-determination that the past wrongdoings of others will actually develop a criminal from a child. These digital risk associations in ProKid are first delegated from the 'guilt' of persons who fall within the child's social environment to the child, although he/she has not done anything anti-social or criminal. Second, the use of ProKid intensifies a risk-based surveillance of persons associated with children.

Therefore, on the one hand, the behavioural scientific argumentation upon which ProKid standards are based and the ways in which practitioners address calculating and associating risks to children can be considered reifying de facto risks as 'real' expectations.[91] On the other hand, "risks are uncertainties"[92] about children's futures; by digitally recording such 'uncertainties', expectations become 'visible' and drive a certain, present reality that such risk-profiled children will become actual criminals in the future. This raises questions about the extent to which Art. 16 and Art. 39 are respected when ProKid is used in such predictive ways.

Beyond associating other persons' criminal behaviour to children's risk profiles, practice shows that risk predictions about a child are also based on the child's relationship to animals:

> "We also have another, somewhat strange risk factor in our list: animal abuse. If a child abuses an animal at an early age, then, according to the scientific findings of Radboud University of Nijmegen, that child has a higher inclination for sexual abuse at a later age." (Police officer responsible for ProKid project, city B).

The author has no intention of questioning the behavioural scientific underpinnings, such as animal abuse,[93] upon which ProKid standards are based. Furthermore, it fully acknowledges the severity of issues, for instance child abuse and antisocial behaviour constitute and that the goal to prevent these problems includes the use of behavioural scientific research in ProKid. However, again, when a wrongdoing of a child, in this case animal abuse, becomes registered in ProKid, the real expectation of a child's criminal development grants no room for a child to prove the opposite of this expectation. This is largely the consequence of the technological impossibility to register the opposites of risks, such as good behaviour, in the system. That any prevention mode in relation to children under 12 years of age is primarily educative, challenges the prescriptions of Art. 29d regarding *"preparation of the child for responsible*

[89] Bruning, M. R., Van den Brink, Y. N., de Jong-de Kruijf, M. P., Olthof, I. W. M. & Van der Zon, K. A. M. *Kinderrechtenmonitor 2012 – Adviezen aan de Kinderombudsman* (Universiteit Leiden, 2012).

[90] According to the ProKid instructions, each case with a 'red' or 'orange' colour code needs to be forwarded directly to Bureau Youthcare – see also Hensen, M. *Op weg naar een regionale aanpak kindermishandeling* (GGD Regio Nijmegen en GGd Rivierland, 2010).

[91] See also La Fors-Owczynik, K. & Valkenburg, G. 'Risky identities: from identifying risks to constructing youth 'at risk' and 'as risk' in The Netherlands in van der Ploeg, I. & Pridmore, J. (eds) Digitizing Identities (Routledge, forthcoming in 2015).

[92] Van Asselt, M. B. A. 'De politike rol van risico-assessments' (2012) *Magazine Nationale Veilighied en crisisbeheersing*, 56.

[93] For information about 'animal abuse' as a scientific underpinning, which in ProKid is turned into a standard indicator of future criminal behaviour, see also p. 24 in Abraham, M., Buysee, W., Loef, L. & Van Dijk, B. *Pilots ProKid Signaleringsinstrument 12- geëvalueerd Pilots ProKid Signaleringsinstrument 12- geëvalueerd* (DSP-groep, 2011).

life in a free society". Questions could be raised about the extent to which the urge to register and render risks digitally visible associated with a child is not becoming a goal on its own? To what extent does such digital 'diagnostic' registration of only risks help the actual care process? Is such registration "proportionate" to children's circumstances (Art. 40 3b) and to their positive development? Moreover, to what extent does the use of ProKid still – at least in its current form – serve primarily the "best interest of the child" (Art. 3 of the CRC) and not "interests of public safety"? Although ProKid is used as a tool to facilitate care, and not, for example, for pre-emptive punishment, it is indicative of the logic that more indicators attributed to persons surrounding the child offer more risk indicators against which a child is to be assessed. Consequently, the likelihood of a child being considered 'at risk' or 'as risk' grows exponentially.

Another example further depicts such exponential growth in risk indicators. The following shows how a risk indicator emerges in 'between' technological systems because of a police officer's observation at a crime scene, which observation has no direct link to the actual crime:

> "[. . .] when our officers are at an address, and find drugs, [. . .] this information becomes registered in BFLE.[94] However, if they find a baby bottle in the kitchen, and ask whether there is a baby; and the inhabitants of the house answer: 'No, the bottle belongs to my sister who comes here occasionally'. If the officer cannot find hard information about whether we need to seek care for the baby, or who exactly lives there, to what extent the person makes something up. . . and the officer has a bad feeling[about it], and wants to use the information [about the bottle], he can register it in BFFI.[95] We, ProKid managers, will see that." (ProKid manager, city C).

The 'soft' data about the baby bottle become a relevant risk factor during assessments, although the information is registered in another police system that is used for purposes of criminal law enforcement. Because data registered in BFFI are meant to be alerting, information in such systems only increases the scope of ProKid and contributes to the ambiguity regarding what exactly leads to a risk qualification about a child. At the same time, it only solidifies the need for the very system of risk assessment by ProKid. The possibility for such exponential growth in risk indicators throws into question whether the system and the practices associated with it versus the objectives the system serves are proportionate (Art. 40 3b).

3.3. *Interim conclusion*

Based on the above insights, a conclusion can be safely drawn that CRC rights are indeed challenged on many levels by the working of ProKid. Challenges emerge concerning the purpose, design and daily use of the system. Questions can be raised, first about the extent to which Art. 40 can be safely enforced, if algorithms in ProKid, for instance, about an anti-socially behaving child suggest to police officers that such a child develops into a criminal in the future. "The presumption of innocence of the child" becomes challenged.

Second, it is questionable to what extent Art. 29 is enforced if, technologically, only risks can be registered. To register only risks allows no room for building a digital record of good deeds of a child and for enforcing Art. 29. The lack of any possibility to build such a 'good record' challenges prescriptions about "the best interest of the child". Such registration would restore what the 'bad deed' register precisely does now; it gradually destructs the 'credibility of a child' from a law enforcement perspective. A good deed register could allow for the restoration of this credibility. For society to flourish, such credibility proves to be perhaps even more desirable than before. Given the ease by which a child can earn a risk registration in ProKid, to take the effort of caring about a child's credibility by registering good deeds could largely support that a child grows into a responsible person in a free society (Art. 29). The latter can be considered in particular in the best interest of a child (Art. 3).

Third, with respect to a victim or witness child, the registration of such a child in ProKid jeopardises the enforcement of Art. 40 2b because the underlying argument in ProKid to register such a child is to prevent him or her from developing a problematic or delinquent behaviour in the future.[96] Furthermore, a child victim or witness in ProKid immediately becoming associated with a perpetrator who automatically worsens the image of the child allows for discussions about the extent to which Art. 29, Art. 16 and Art. 3 are well enforced by this technological association between victims, witnesses and their perpetrators.

Fourth, when using ProKid, the police rely on other police databases that contain strictly law enforcement data and therefore fall under the regular regime of the Police Data Act. Consequently, the extent to which such data aggregation enforces the child's right to privacy as prescribed by Art. 16 and is in the "child's best interest" (Art. 3) is questionable. Art. 16 appears to be challenged already because of the use of strictly police databases in combination with ProKid. ProKid is used on children under 12 years of age who should not be prosecuted; hence, the exceptions from the Dutch Data Protection Act provided by the Police Data Act would not apply for police when they use ProKid. The complementary use of other police databases, such as BFLE or the BFFI within the network of ProKid, however, appears to overreach data protection jurisdictions because law enforcement data from the mentioned two databases are used for prevention by ProKid. As long as the Police Data Act is applicable as a 'lighter' data protection regulation for regular police databases, the use of such databases for preventative purposes on children through ProKid allows for the blurring of boundaries between the data protection jurisdictions – one for the Dutch police and one for all other data flow types. This blurring endangers the enforcement of the CRC.

[94] BFLE – Basic Facility for Law Enforcement.
[95] BFFI – Basic Facility for Forensic Investigation.
[96] About this basic goal of ProKid, see also pp. 18 in Abraham, M., Buysee, W., Loef, L. & Van Dijk, B. *Pilots ProKid Signaleringsinstrument 12- geëvalueerd Pilots ProKid Signaleringsinstrument 12- geëvalueerd* (DSP-groep, 2011).

4. CRC: its potential to protect children's rights

Despite its imperfections and general criticism of human rights being relative, the United Nations Convention on the Rights of the Child is a highly potent and unique instrument, thus far being the only legally binding tool that considers children as fundamental rights holders.

However, as the international and Dutch court rulings also demonstrated, the Convention's immense potential is always part of a balancing of interests. Dutch criminal court cases have shown that if a balancing finds a place between the interests of public safety and children's rights, Dutch court decisions mostly favour interests of public safety. Therefore, the potential of the CRC can be better exploited if the CRC becomes employed and enforced in mundane practices of professionals, in our case within Dutch policing practices in which ProKid is used. Therefore, from a CRC-perspective, it is desirable not to wait until an issue with ProKid reaches court. To enforce the CRC, certain debatable children's rights challenges related to the daily profiling practice of ProKid, such as those detailed earlier, need to be addressed first.

First, providing room to build a digital record of the good deeds of a child could help to enforce Art. 29 and Art. 3. The registration of an 'improved image' might possibly compensate for the 'bad image' of a child registered earlier and favour Art. 29. and Art. 3. Such a compensatory feature in ProKid is desirable because with the present set-up of the system, if a family member or co-habitant of the child has a registered record by the police, that record further overshadows the image of the child (see, for instance the yellow, orange and red colour-code descriptions on the living address of the child). This characteristic de facto raises difficulties for a child in avoiding a potential criminal future.

Second, the enforcement of Art. 40 could be improved if the 'bad image' of a perpetrator was not immediately associated in ProKid to a child victim or witnessed as a directly bad influence. Art. 3, Art. 16 and Art. 29 could also be better enforced if such technological associations between victims, witnesses and their perpetrators had a more flexible and differentiated, individually oriented character. Whether and how associations between children and adult perpetrators need to be registered and scored are in themselves not only legal but also ethical questions. However, if possibilities for such associations between children and adult perpetrators are already implemented in ProKid, the option of whether such an association of a child to a perpetrator should be digitally registered in ProKid is a question that a ProKid user must investigate per child. The possibility for the ProKid-using police officer to opt out, or in other words not to register such an association if in the officer's view registering such an association would not be in the child's best interest, should be accepted as an option. This is worth considering because practice also demonstrated that the ease of associating not only family members and co-habitants but also friends, neighbours and animals to the child's profile as a negative influence allows for a child to become easily profiled as risky. At the same time, however, expunging such a profile, which according to certain scholars can be considered "stigmatizing",[97] proves to be quite difficult. At present, risk data are kept for 5 years; however, given the number of persons and their problems who can become involved in a child's risk profiling process, the consequences of one risk registration on another associated registration to a child, in practice, can span a period much longer than 5 years. Although the alerting potential of ProKid is necessary, to build more flexibility into such risk registrations, enabling children to move beyond their risk profile proves also to be in their interest.

Third, making arrangements for a more structured usage of strictly law enforcement databases in relation to the preventative system of ProKid would be highly desirable to strengthen the CRC and, in particular, the CRC-granted right to privacy. As a first step, such arrangements could take shape by differentiating the methods by which digital connections can be established between police databases and ProKid if the issue at hand involves a child perpetrator, victims or witnesses. This also could help clarify how the two different data protection regulations are met – the Dutch Police Data Act by the police and the General Data Protection Act for all other data flows. This would allow for the combined use of strictly law enforcement databases, and ProKid would neither cross data protection jurisdictions nor blur their boundaries. Such arrangements could be highly beneficial to enforce the CRC in general and Art. 16 in particular.

Fourth, a CRC approach should allow for questions about whether a data registration is desirable at all in the first place, while bearing in mind Art. 3 of the CRC. A CRC approach allows for debating the extent to which it is under all conditions in "the best interest of the child" to keep a registration of a child for 5 years and whether an earlier erasure of data could not be better in the child's favour. This could allow for the enforceability of a right that is even more applicable in light of the troubles with which children under the age of 12 can become associated. This right, named "the right to be forgotten" in a recent European Court of Justice decision,[98] became acknowledged as enforceable under certain circumstances within the context of Internet providers and consumers. However, this decision is not applicable to law-enforcement organisations within the justice system who perform prevention work on children, and the enforcement of such a "right to be forgotten" bears significant challenges for daily practices.[99] However, this decision could inspire more-CRC-based reasoning during the prevention practices of ProKid, particularly because within its context, a "right to be forgotten" could de facto mean a "right to be forgiven" within the Dutch justice system for a child.

Beyond these four specific suggestions for technological and legal changes, the potential of the CRC with respect to ProKid can gain a general boost from the insights of science and technology studies, such as the perspective that problem

[97] Bruning, M. R., Van den Brink, Y. N., de Jong-de Kruijf, M. P., Olthof, I. W. M. & Van der Zon, K. A. M. *Kinderrechtenmonitor 2012 – Adviezen aan de Kinderombudsman* (Universiteit Leiden, 2012).

[98] ECJ, Luxembourg, 13 May 2014, C-131/12.

[99] Koops, B.-J. Forgetting footprints, shunning shadows. A critical analysis of the "right to be forgotten" in big data practice (2011) 3(8) Scripted 229.

translations also demonstrate. To follow how problem definitions of child abuse and anti-social behaviour of children are translated into problems of information-sharing and later into digital data processing allows asking questions about the extent to which these problem translations actually help to address the 'original problems' and whether CRC rights are considered throughout such translations adequately. Insights from other disciplines can also be of help, such as relevant fields of psychology. Philip Zimbardo, for instance, the psychologist who became famous through his prison study at Stanford University, criticises general criminal behaviour predictions by arguing, "Personality predicts only when people are in the same situation [. . .] personality does not predict across time and across very different situations."[100] This suggests that a child victim or a witness of a crime cannot be considered with one hundred percent certainty a future criminal, if only certain registered occasions or situations provide for such a claim. Such observations from other disciplines, which plead to assess each person according to his/her individual situation and needs, leave more room for CRC considerations.

5. Conclusions

The use of ProKid SI 12- allows framing children as potential perpetrators, even when they are registered as victims of violence: *"The scientific basis for ProKid is a number of behavioural indicators(such as truancy, bullying, cruelty to animals, profanities, hanging out on the street without supervision or witnesses or victims of sexual abuse or domestic violence) which have proven to be risk factors for criminal careers."*[101] The framing of children being 'at risk' of a crime such as child abuse or domestic violence and that such a digital profile by itself allows for these children to be viewed 'as a risk' of becoming a future perpetrator, constitutes perhaps the greatest challenge of the CRC. The fact that children who show anti-social behaviour are observed as much 'as a risk' as those children who are already proven criminal delinquents, does not allow much space for the educative component of the CRC. These issues need to be addressed so that the CRC can gain power in daily practices.

Therefore, the empirical examples and their analyses have been intended, first to advocate for the building of a CRC-informed reflexivity and awareness amongst ProKid-user professionals concerning the potential effects from the daily use of ProKid for children's rights. Preferably, this should include not only training about how to use ProKid to register risks on children but also children's rights training addressing what the effects of such registrations may be in practice in light of the convention. All this could assist in developing a CRC-driven routine amongst practitioners.

Second, a general remark is that currently existing privacy and data-protection impact assessments could be broadened into larger CRC impact assessments. These would preferably be performed not only in the test phase of a technology but also repeatedly during the daily use of systems. This would create a capacity to reflect upon basic children's rights principles that, during the 'translation' of children's rights principles into data protection rules, often become drawn into the background or viewed as being already covered by data protection rules.

Third, the example of ProKid is of international relevance. Legal, societal and technological conclusions from the observed drawbacks of the system could be informative regarding the working of ProKid and similar systems[102] and about their potential negative implications for the CRC internationally.

To conclude, when we examine more closely the Dutch national court rulings in law enforcement[103–105]and the purpose, design, and particularly the colour-code standards of ProKid and how these standards become interpreted by professionals[106] in daily practice, a certain mindset becomes visible. This mindset shows that the expectation that a child will become a criminal at the end of the day often appears to outweigh the need to protect the child's privacy. However, this mindset should be challenged and perhaps desirably changed in a democratic society. This is essential to meet the CRC prescriptions and the conclusions raised by the earlier ECHR court rulings, both being applicable for all signatory states including The Netherlands. However, such a change requires a combination of elements, which would not only include regulative changes such as, for instance, the already mentioned 'right to be forgotten' during risk profiling practices on children. However, CRC-based changes affect numerous societal, administrative and technological parties. Changes could manifest in cases, for instance, in which certain less severe risks become unregistered or registered in a balanced manner. This could serve that the digital construction of risk profiles about children would not lead to some forms of major injustice towards profiled children. Risk profiles of children, for instance, could become erased, and long digital records of children's deeds performed before the age of 12 would not be kept for a long period. All this could improve chances for minors not only to be protected and to live with a 'right to be forgiven' but also, importantly, to live in a strict but hopeful and forgiving society within The Netherlands and beyond.

Acknowledgements

The research leading up to this article has been subsidised through the DigIDeas project which was granted to Dr. Irma van der Ploeg by the European Research Council under the European Union Seventh Framework Programme (FP7 2007–2013)/ Grant No. 201853/. Furthermore, I would like to particularly thank Prof. Corien Prins for her support and very useful comments on this article.

[100] Zimbardo, P. *The Lucifer Effect Understanding how good people turn evil* (Random House, 2007).

[101] Abraham, M., Buysee, W., Loef, L. & Van Dijk, B. *Pilots ProKid Signaleringsinstrument 12- geëvalueerd Pilots ProKid Signaleringsinstrument 12- geëvalueerd* (DSP-groep, 2011: 18).

[102] For international examples of such systems, please see Section 2.2.

[103] HR 7 Maart 2014, 13/04683.

[104] Rb. Arnhem 16 Februari 2010, BL6961.

[105] HR 7 Maart 2014, 13/04683.

[106] The second quote on page 19 also exemplifies a relatively free interpretation of colour code standards.

Accepted and published as Chapter 13 in Y. van der Ploeg and J. Pridmore (Eds.) Digitizing Identities: Doing Identity in a Networked World, (2015), Routledge, New York (pp. 103-124).

Thesis chapter V.

Migrants at/as risk: Identity verification and risk assessment technologies in The Netherlands

Karolina La Fors-Owczynik and Irma van der Ploeg

1. Introduction

International policy discourse on migration shows a tendency to prioritize securing citizens over securing migrants (Tsianos & Kuster, 2010). Practices geared toward the sorting out of entitlements to access and residence of migrants mobilize a discourse that increasingly frames them as *posing risks* to the societies of their host countries (Leers, 2012; Leers, 2011), notwithstanding the fact that only a small minority of migrants are associated with criminal offences, e.g., organized crime, illegal entry, human trafficking, or terrorism. In the main, migrants with refugee or asylum seeker status, as well as those seeking this designation, arrive as a consequence of wars, natural disasters, political or economic unrest, human trafficking, international crime, or a combination thereof. These immigrants can be regarded as being *at* risk. Although technological systems of migration and border control are generally installed to prevent threats to a country's inhabitants, including threats associated with migrants, countries also have a human rights obligation to assist and protect vulnerable migrants. Today, the perspective on migrants as vulnerable and at risk seems to lose traction.

This chapter discusses how migrants and travellers are increasingly framed as posing a risk to the Netherlands. More specifically, we analyse the way that modes of prevention (Bigo & Guild, 2005; Broeders, 2009), and their associated risk assessment systems have come to focus on translating specific problems around migrants into problems of identity fraud, illegal entry and illegal residence. The ways in which these problems are defined and managed has directed attention towards improving the establishment and the management of '*identity*'[1]. These identification practices have ethical implications because they may be instrumental in discriminative exclusion and inclusion. For this reason, we focus in particular on identification and risk assessment practices performed by border control, migration, and law enforcement agencies.

In the Netherlands, the constellation of border and immigration agencies is known as the 'alien chain', and that of law enforcement agencies as the 'criminal justice chain'. Establishing migrants' and travellers' identities, and organizing fraud-proof identity management systems have high priority within both chains. This is pursued by elaborate risk profiling practices, identity management systems, and sharing of information along and between the range of agencies within the chains, such as the Alien Police, The Royal Military Police, and the Immigration and Naturalization Service (IND).

Whereas terms such as 'identity', 'prevention', and 'risk' concerning migrants suggest a certain self-evidence at first sight, these terms derive their meaning from complex arrangements of local, national and international institutions, digital technologies, legal settings, and professional practices. This is also evident in the international commitments The Netherlands has to a broad range of information exchange tasks, including information on migrants and travellers. As part of the European Union, The Netherlands is, for instance, committed to performing policing tasks through using the national database of the

[1] In opposition to the identity management discourse, where 'digital identity' is often equated with a collection of personal data, this chapter regards identity as a 'multi-layered concept', as something "interactive, mediated, relational, and dynamic, as opposed to something pre-given to be 'expressed' or 'registered' (Van der Ploeg; 1999).

Schengen Information System (SIS[2]) and exchanging data within the pan-European law enforcement organization, Europol[3]. The Netherlands is also obliged to enforce the Dublin convention[4], which prescribes member states to determine whether or not an asylum seeker has submitted a prior application in another member state. As part of these assessments, the fingerprint database EURODAC[5] is consulted. Another obligation for the Dutch government is the exchange of visa data on migrants through the Visa Information System (VIS[6]). Given that the Dutch sea border also constitutes part of the EU's external border, the Netherlands actively participates within the EU's border management organization FRONTEX[7]. For example, the Dutch also aggregate and share data on illegal entry through the EU's border surveillance system, EUROSUR[8]. Beyond these European organizations and systems, a large variety of national and local organizations exist in the Netherlands that deploy local border control, immigration, and law enforcement procedures. The two identification systems, as well as the risk profiling system analysed in this chapter, are embedded within these European and Dutch regulatory and technological settings, yet operated solely in The Netherlands.

These three systems are the following: first, the identification and verification console of the Dutch Immigration and Naturalisation Service, the INS-console, second the console of the information provision program (in Dutch: Programma Informatievoorziening Strafrechtsketen) within the Dutch criminal law chain, the PROGIS-console, and the Advanced Passenger Information-System, the API-system. Although they differ significantly, as they are situated in different practices and operated for different purposes, this chapter aims to articulate some shared characteristics and implications of their use. We suggest that all three systems contribute to a shift that increasingly frames migrants as *posing* a risk, as opposed to potentially being *at* risk. Moreover, we aim to show how the quest for 'accurate identity', and the technologies used to approach this goal, transform the problem in specific ways, and, in the process, create new uncertainties and risks for those subjected to them. We argue that this happens because of the particular way problems of identity fraud and illegal entry are translated (Latour, 1987) into specific technological solutions.

To illustrate this dynamic, the next section first introduces the systems under study, and briefly describes how identity verification of certain categories of migrants and risk profiling of travellers is enabled by these systems. The third section discusses how the 'accuracy of identity' and an accurate 'risk profile' are produced, by focusing on the development of 'risk indicators'. The fourth section looks a bit deeper into the functioning of the systems in practice, and identifies a number of pitfalls in the socio-technical production of 'identity', and 'risk'. The analysis is based on empirical data from interviews with professional users of these systems within the alien and law enforcement chains, and guided by actor-network theory (Akrich, 1992; Latour, 1987) and a material-semiotics informed approach (Law, 2009). The final section draws the arguments together, and concludes that the technological quest for 'accurate identification' and risk prevention introduces a range of new risks for migrants.

2. Prevention systems in Dutch immigration, law enforcement and border management

'Risk prevention' with regard to identity fraud, illegal entry, and international crime has a high priority in Dutch immigration policy (Leers, 2012). In the discourse on improving this prevention, visual metaphors dominate: migrants and their associated risks need to be made 'more visible' (WRR, 2011), and there is a need for more 'complete and accurate pictures' of migrants. A report by the Dutch

[2] SIS - <http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/schengen-information-system/index_en.htm>
[3] Europol - < https://www.europol.europa.eu/content/page/about-us>
[4] Dublin Convention - <http://europa.eu/legislation_summaries/justice_freedom_security/free_movement_of_persons_asylum_immigration/l33153_en.htm>
[5] EURODAC - <http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/asylum/identification-of-applicants/index_en.htm>
[6] VIS - <https://secure.edps.europa.eu/EDPSWEB/edps/Supervision/VIS>
[7] FRONTEX - <http://frontex.europa.eu/>
[8] EUROSUR - <http://frontex.europa.eu/intelligence/eurosur>

Advisory Committee on Alien Affairs, for instance, describes a need for acquiring a 'better view on asylum seekers' (Tweede Kamer, 2005), and another report from the Ministry for Foreign Affairs similarly emphasizes the need for a more 'comprehensive picture' of migrants (Min. van Binnenlandse Zaken, 2013). The need for improving this 'visibility' is invariably addressed through the introduction of advanced digital technologies for identity verification and risk assessment purposes. The INS-console, the PROGIS-console, and the API system exemplify such technologies.

2.1. The INS-console

The INS-console is a biometric fingerprint scanning and facial photographing system employed by the Immigration and Naturalization Service (INS, in Dutch: *Immigratie en Naturalisatie Dienst*) of the Dutch Ministry of Interior Affairs. The European Council Regulation (EC) No. 380/2008 prescribes that all EU member states, including the Netherlands, register "a *photograph […] and two fingerprints taken flat and digitally captured"* in each residence permit issued to a third-country national. 'INS-consoles' have been installed specifically to meet this regulation by producing facial photographs and 'high quality' digitally scanned fingerprints. These data are then incorporated into the residence permits of non-EU migrants *("Vingerafdrukken op verblijfsdocumenten", 2013)*. First, it was only allowed to register scanned fingerprints and personal photographs on the residence permits. But as of 1st of March 2014 a legal change allows for the registration of the mentioned biometric features in a central database, in the Basic Facility for Aliens[9](*Besluit van 21 januari 2014 tot wijziging van het Vreemdelingenbesluit 2000[…], 2014*). During every subsequent verification process, the residence permit holder places his/her fingers on a reader and the images are compared with the fingerprints stored on the permit. Residence permits furnished with these biometric features are considered to increase certainty about the permit holder's identity, and that the document truly belongs to the immigrant to whom it has been issued (Teveen, 2013). Enrollment in the system will eventually include all third-country nationals acquiring a residence permit. However, when the interviews used in this paper took place, the INS had only begun enrolling asylum seekers. Our analysis in subsequent sections of the ways in which 'identity' and 'risk' are translated and performed within this system, thereby reinforcing the trend of shifting perceptions from seeing them being *at* risk to seeing them *as* risk, therefore pertains only to this particular subgroup of migrants.

The digital fingerprint scanning by the INS-console is considered an improvement upon previous enrollment procedures for asylum seekers. That procedure involved rolling the applicant's 10 fingers in ink, and producing prints on paper, the so-called *dactyslips.* All original dactyslips are archived in the Dutch National Research Information Service (dNRI). Copies of these sheets are subsequently transferred to a central European system called Eurodac where they are checked against those already registered. In case of a 'no-hit', the fingerprints are registered, and the application will be processed. In case of a 'hit', this is taken as evidence of 'asylum shopping', or at least as evidence that an earlier application has been submitted by the same person in another EU country. Eurodac is the main tool for the execution of the Dublin Convention (Council Regulation (EC) No 2725/2000) that determined that one cannot apply for asylum in more than one of the EU member states, and that the country of first application remains responsible for that person and their application (Van der Ploeg, 1999). In addition to checking in Eurodac, copies of applicants' dactyslips are registered in the Basic Facility for Aliens (Basis Voorziening Vreemdelingen), an IND database containing data on all migrants in The Netherlands, and in the law enforcement database HAVANK (Het Automatisch Vingerafdrukkensysteem Nederlandse Kollektie, or Automated Fingerprint system Dutch Collection).

2.2. PROGIS system

Prevention of identity fraud by convicted criminals is a key target within the Dutch law enforcement chain. Although this particular issue is part of a much wider concern, it has recently been pushed to the forefront after several prisoners were found to be others than those who were actually sentenced. Therefore, the Dutch Act on Identification of suspects, convicts, and witnesses (Wet

[9] The new bill also enables a significant extension of use of biometrics throughout the alien chain.

identiteitsvaststelling verdachten, veroordeelden en getuigen, 2009), prescribes law enforcement authorities to 'establish the identity' of suspects, convicts and witnesses to crimes by taking their digital fingerprints and facial photographs.

In line with this law, the police and other judicial authorities introduced a new[10] biometric system, the PROGIS-console (PROGIS), to guarantee that "the right person is punished" ('Politie: grondige identificatie voorkomt identiteitsfraude - Security.NL', 2012). At the end of an identity verification and enrollment process, which involves taking a facial photograph and scanning ten fingers, a so-called 'ID-state' is produced. This ID-state meets the objective of the Dutch Ministry of Security and Justice in acquiring a "more integrated, criminal person image" (in Dutch: *integraal strafrechtelijk persoonsbeeld* (2011), in that it is claimed to ensure a person's identity during criminal investigations.

The enrolment of suspects and witnesses in PROGIS constitutes the entry point to the Dutch criminal justice system. From that point on, the 'established identity' on the ID-state becomes the reference point against which all fingerprints and facial images taken at later moments in the procedure are cross-checked and verified. In order to use the same person's file between criminal justice agencies, each PROGIS ID-state is linked to a so-called criminal justice chain number (CJCN, in Dutch: *strafrechtsketennummer* - SKN), and stored in a central database, the Criminal Justice Chain Database (CJCD). The CJCN is meant to harmonize the administration of cases among agencies. In case of recidivism, this database allows for updating a criminal record. This occurs when separate criminal cases become associated with the same person through one CJCN.

Remarkably, it has been the Dutch Alien police that was tasked with operating PROGIS for the criminal justice chain, primarily because of the experience and expertise they acquired through conducting identity research[11] on migrants within the alien chain. However, biometric data produced by PROGIS is only used by partners within the criminal justice chain to verify whether a person's data is already registered in the CJCD. Therefore, if an immigrant offends or becomes a criminal suspect, they, would be enrolled in PROGIS the same as anyone else in The Netherlands. We are less interested here in the specific framing of an immigrant as posing a risk in the sense of being a suspect in the context of a particular crime investigation.[12] Our concern here regards the particular framing as risk that is performed with the very enrolment – either as a suspect or witness - in PROGIS. The likelihood for a migrant to become suspected of identity fraud, for instance, is higher than for 'regular' residents, since the identification process for immigrants is in general far more complicated than that for Dutch citizens, and therefore more prone to error. Along this line, section four highlights how the very use of PROGIS can increase the chances for a migrant to be framed as *identity fraudster*.

2.3. The Advanced Passenger Information System (API)

Within the context of border control, travellers from non-EU states are routinely assessed against risks of illegal entry (e.g., fraudulent visa or passport), international criminal activity, or threats to national security (e.g., terrorism). All these problems have contributed to the development of more orchestrated

[10] The digital fingerprint scanning via PROGIS is new compared to the classical dactyloscopy routine of law enforcement practices. This entails the ink-based fingerprinting of suspects in remand and convicted criminals, and the production of dactyslips. Dactyslips are digitally copied and saved in two major police databases: in AFDC, and in the Facility for Verification and Identification (FVI, in Dutch: *Voorziening voor Verificatie en Identificatie*, VVI)(Min. van Veiligheid en Justitie, 2011). (The original sheets are submitted to and archived by the Dutch National Research Information Service/dNRI/.) The fingerprints taken by PROGIS during the identification process are regularly compared with fingerprints stored in AFDC. If fingerprints have not been registered yet, dactyslips are produced and their copies transferred to AFDC. In case a suspect is an alien, fingerprints are also compared with the BFA.

[11] The Dutch Alien Police operates PROGIS from the back office, including an extra control function. Back office tasks were granted to the Dutch Alien Police based on the already accumulated experience of this unit in conducting identity research on immigrants within the alien chain. These tasks include establishing the identity of suspects by PROGIS, which can involve 'identity research' on immigrants. (Leers, 2011)

[12] Immigrants who overstay their visa, who are not part of an asylum seeking process, or who have simply no identity documents all are enrolled in PROGIS as illegal residents.

risk profiling practices of passengers internationally. Problems of international crime and terrorism generated new modes of data exchange, as EU agreements on the exchange of Passenger Name Records (PNR) of travellers with the US (2012), Canada (2006), and Australia (2012) exemplify. In fact, airports transformed into ever more advanced security checkpoints (Schouten, 2014), where, beyond facilitating the mobility of travellers, the filtering out of 'untrustworthy' passengers grew into a top priority.

The Advanced Passenger Information project (henceforth: API) is situated at Schiphol Airport and is part of a larger programme called Sustained Border Management[13] (in Dutch: *Verbeterd Grensmanagement*) in The Netherlands. API has been developed to meet EU (EC, 2004/82/EG) and national regulations for the sole purpose of preventing *illegal entry* into the Netherlands, and is used by Dutch border control and immigration authorities to check all travellers moving through Schiphol Airport against 'API profiles'. A wide range of passenger attributes, including behavioural characteristics, air travel histories, modes of plane ticket purchase, and classifications of personal belongings, are assessed against these API profiles,

In 2010, the International Civil Aviation Organization (ICAO), the World Customs Organization (WCO), and the International Air Transport Association (IATA) revised the guidelines for API. According to these guidelines, part of the flight information from the "departure control system" (DCS) of airlines and individual passengers' data from the machine readable zone of the travel document and passengers' seat and baggage information need to be included in the API dataset. This dataset can be extended to include a maximum of 39 items (depending on country-specific legislation). The EU also follows the international API guidelines. Carriers of incoming and outbound flights in the EU are obliged by the Directive 2004/82/EC *(Min. van Immigratie, Integratie en Asiel, 2012)* to submit information on passengers to border control authorities prior to their departure, which also applies to the Netherlands. Such data may be kept by these authorities for a maximum of 24 hours. Leers 2011 suggests in a policy analysis about the work of the Dutch Royal Military Police, Dutch Customs Services, General Intelligence and Security Service, and the Immigration and Naturalisation Service, as well as test results of the API project, that if these agencies could gain access to passengers' travel document data and check that data against API risk profiles before travellers cross the border, this would foster security, more efficient processes by agencies, as well as smoother border crossing of travellers.

API data and profiling are perceived as pivotal elements in apprehending migrants involved in human trafficking. While on the one hand being construed as useful in the protection of potential victims, by identifying those 'at risk' of this and other, related crimes (e.g., prostitution or exploitation of illegal workers), API data are, on the other hand, also considered useful in identifying those *posing* a risk, in particular regarding illegal entry. Our analysis in section four will indicate how both uses of API profiles can, in fact, merge into each other, thus casting doubt on the proclaimed affectivity of each.

3. Doing risk: building 'indicators'

The prevention of potential problems associated with migrants hinges in part upon the sharing of information between practitioners, organizations, and technological systems. Both the prevention of identity fraud through identity documents, and of *illegal entry* through risk profiling methods are shaped by the ways in which classifications, standards, watch lists, and other tools are implemented. This 'operationalisation', in turn, takes the form of marking specific personal and other characteristics as 'indicators'. Although such indicators are seemingly straightforward characteristics, they are in fact the result of a considerable amount of work (La Fors-Owczynik & Valkenburg, this volume). Moreover,

[13] The Dutch Sustained Border Management programme is coordinated by the Department of Identity Management and Immigration of the Ministry of Interior Affairs. This includes four sub-projects: Passenger Related Data Exchange (PARDEX) – budget for PARDEX is frozen at the moment (Sanders, 2012) -, Advanced Passenger Information (API), no queue (No-Q) and a Registered Traveller (RT) programme. PARDEX is a central system intended for sharing passengers' information (acquired prior to their travel) with law enforcement agencies. The No-Q and RT (Registered Travellers) are aimed at fostering automated border passage for all EU passengers based on machine-readability of travel documents.

framing risks, i.e. a *possible* future occurrence, as something detectable in the present, requires an *expectation* to be translated into observable categories, which, at the same time, renders these risks more 'real'. In addition, and despite their apparent simplicity, risk indicators need to be continually interpreted by professionals. The efforts to determine and interpret risk indicators involve an opaque set of problem transformations by different actors that introduce a range of ambiguities concerning the functioning of the technologies.

3.1 Establishing 'proof' of identity': revisiting the "entry-point paradox"

Ambiguities around what constitutes a risk of identity fraud also emerge in the ways in which 'identity' is established within the configuration of PROGIS. Although this system is intended to provide more accurate ways of identifying persons by biometric and other technologies, thus to prevent the risk of identity fraud, enrollment in the system requires prior 'proof' of identity:

> *"PROGIS-consoles do not check the authenticity of ID documents before a person becomes enrolled. […] so, professionals must know IDs. New European documents are all made of polycarbonate, such as Polish IDs, for instance. If you drop one, you hear a tinny sound. Therefore, while being busy with someone, policemen often let documents "accidentally" fall. If a document sounds dull, that indicates fakeness." (PROGIS-professional, city A)*

The above quote exemplifies two points. First, ID documents are not checked for authenticity by PROGIS; instead, professionals must decide whether an ID document used at enrollment is genuine or fake. Second, the potential problem of identity fraud is transformed into observable indicators, such as, in this particular example, *the sound of a falling ID card*. Thus, a general problem of identification, one that Roger Clarke (1994) labeled the *"entry-point paradox"* resurfaces here: the accuracy of each digital identification or verification system, however sophisticated, is only as strong as its weakest link, which often lies right at the start of the whole procedure, the authenticity of 'breeder documents' (e.g., IDs, birth certificates). This clearly is an issue in PROGIS, where its claimed technologically enhanced accuracy, in practice, may depend upon an improvised trick that is anything but high-tech or accurate.
In a similar vein, the INS console is claimed to provide an 'accurate identity' for migrants, while also requiring prior 'identity proof' from them. A professional identifying so-called 'invited refugees'[14] via a mobile INS-console in refugee camps explains:

> *I: How can you be sure that the [undocumented] person you want to identify with the INS-console is the one he/she claims to be?*
>
> *P: That you never know. I can give you a basic answer: I can only hope that the person who said something about him/herself to me, said the same thing to our UNHCR[15] colleagues. It can be two times a lie, but since I cannot figure this out, I must be satisfied with the consistency of the refugee's story." (INS-professional, city D)*

The above excerpt indicates once more the 'clay feet' of many high-tech identification and verification systems today. Sometimes all one has to go on at enrolment is a minimum level of consistency in a claimed identity, life or flight story. In the final analysis, it is still the experienced worker 'in the field' whose judgement about the credibility of someone's personal account carries weight. Whether this is to be seen as a strength or a weakness – some may find this remaining human element reassuring – it is a key element in the functioning of such systems that is usually left out of the accounts of technological accuracy and their role in combating identity fraud

[14]Most countries have signed agreements about inviting a given number of refugees. The Netherlands invites a maximum 500 refugees yearly. INS professionals select these refugees by visiting camps and conducting research about who shall become entitled to an invitation.
[15] Refugee camps are generally run by UNHCR and local authorities.

3.2 Turning attributes into indicators for 'illegal entry'

Building risk profiles from indicators visible in the Advanced Passenger Information system shows similar shifts in localization of the problem. The problem, here, is 'illegal entry', and the localization may be quite literal, in the sense that geographical locations and travelling routes may become part of a particular risk profile:

> *"Ultimately, you want to focus on every flight, but you need to build this up gradually. Where does our first priority lie? […] if other partners also have problems with flights from a given country, than there must be something wrong with those flights. If 5 professionals from different organizations say the same about 3 places, than there is something risky with those flights." (API-professional, city A)*

The same professional explains how a range, or a combination, of rather generic attributes and characteristics of passengers on flagged flights are turned into risk indicators.

> *"You can discover that […] 'facts' about persons traveling from those risk flagged places are also important, these help you learn the type of persons you look for. […] you often search for particular men or women of a certain age, behaviour, clothing or travel companions. I often check passengers against such indicators."*

As indicated earlier, API profiles are also used to prevent illegal entry connected to international crime like human trafficking. An IND official, who also manages API, describes how particular instances of this crime are sometimes spotted through the API profiling:

> *"We did quite well with that profile and stopped many women who were glad and grateful for what we did. We were also happy we could protect them from becoming prostitutes. […] The funny thing is that a month after we started to screen flights against the profile, trafficked women no longer travelled directly to Madrid, but took the route: Amsterdam - Paris - Barcelona - Madrid. The change in the route assured us that the profile was good, and that criminal organizations are well informed. The API profile […] did well. This allowed us to indicate for the minister the usefulness of API data and the importance of binding several issues together in one profile." (API-manager, city A)*

Interestingly, this quote illustrates as well how the API system based profiling may contribute to the convergence, if not conflation, of protecting migrants *at* risk (of trafficking and sexual exploitation) with prevention of travellers *posing* a risk (of illegal entry). There is no need to doubt the intentions of border guards in any way in order to legitimately raise the question whether stopping someone at the border casts them as victim or as perpetrator, as it unclear whether this is followed by sending them back, prosecuting them, or really helping them. The fact that traffickers changing their routes is taken as a sign of success of the profile, and could indicate that it is above all the mere prevention of illegal entry that counts.

It is also clear that professionals do not merely follow standardized protocols or automated decision processes. Seeing certain attributes of travellers as risk indicators can also be based on tacit knowledge and acquired experience:

> *"If I only consider what is registered in the system, I would only follow the system. The moment I look at my quantitative data analysis and indicators suggest that persons who smuggle others always have a red cap on, I also start 'qualitative research'. If I only focus on persons with red caps I would not see if someone is smuggling people in yellow rain boots, for instance. You have to rely on your senses […] and adjust your profile." (API-professional, city A)*

We repeatedly heard about professional's 'gut feelings' being the reason for modifying risk profiles and introducing new indicators. Thus a shared or hybrid agency exist between human actors and automated systems, that makes the process leading up to the decision who will be assigned a risk qualification, and who will be stopped for further inspection, rather obscure. The constant need to amend API profiles and the flexible conception of indicators renders the process even more elusive.

A major part of the work in identifying risk associated migrants is about fixing the ambiguities, uncertainties, and (im)probabilities concerning what, in practice, constitutes such risk. Yet, the whole idea of detecting and preventing risk in this context requires the presumption that risks are somehow

observable; a presumption that lies at the basis of the efforts to develop indicators for them. This section, however gave examples suggesting that the particular indicators used within the operation of the INS-console, the PROGIS-console, and the API system, sometimes increase ambiguities and uncertainties about risks. Moreover, as the next section aims to make clear, the very use of these three systems generates a proliferation of such 'indicators', and requires workarounds to make them function, that, together, have the ironic effect of increasing the perception rather than the prevention of risk.

4. Pitfalls of making risks 'visible'

To distinguish those entitled to enter the country, obtain employment, or receive government support, from those who pose a security risk has always been a politically laden process. Pivotal in this is the conceptualization of identity as something fixed, and verifiable. As Caplan and Torpey (2001) argue, identification processes transform the 'who' question into 'what kind' of a person that someone is. This shifts the search for identity towards the classification of personal characteristics into categories. Similarly, Btihaj argues that "*this collapse of the "who" into the "what" [...] indicates their [identification modes] inherent limitations in capturing the ambiguity of identity and the complexity of the lived experience"*(Btihaj, 2010: 6).

Technological innovations like machine readable passports, e-IDs, and biometric identification systems exemplify efforts for producing certainty about a person's identity (Bigo & Guild, 2005; Caplan & Torpey, 2001; Holowitz & Noiriel, 1992; Lyon, 2009). However, this certainty rests on the acceptance of a series of problem translations that remain unexamined by those operating the systems, but that nonetheless each introduce uncertainty and possibility of error (Van der Ploeg & Sprenkels, 2011).

Continuing this line of thought, in this section we argue that efforts to make the risks of identity fraud and illegal entry visible requires a particular type of visibility, one that always could have been otherwise. Moreover, we show how the particular visualization of risk produced by the INS and PROGIS consoles and the API system inscribes these risks onto material objects such as clothing or personal belongings, and body parts.

The practices within which these systems are used exemplify that 'identity' and 'risk' are increasingly constitutive of each other: to identify immigrants presupposes risk assessments, and to assess immigrants against risks involves practices of identification and identity verification. As much as identification practices are increasingly about extensive categorization and registration of personal attributes and modes to verify these, risk assessments of immigrants are increasingly about cataloguing a growing number of personal attributes as risk indicators. That is to say, if an immigrant's 'identity' does not conform to a norm during a verification process by the INS- or PROGIS-console, or if certain attributes of an immigrant match with an API risk profile, that identifies them as a 'risky migrant'.

In the following we highlight how operating the systems discussed creates additional 'risks'. The systems all have their weaknesses and fallibilities that may be exacerbated when agencies exchange information, and repeat procedures in different systems. The next section demonstrates how this occurs in the field, and provides further examples of how problems of identity fraud, illegal entry or related crimes by immigrants become translated into other issues within the configurations of the INS-, PROGIS-console, and API system.

4.1 False positives and false negatives

The INS-console was intended to provide 'improved' biometric data for verification by skipping a translation step within the fingerprinting processes (see section 2). In the new system, fingerprints are directly digitally scanned, so the scanning of the ink-based dactyslips is no longer necessary.

> *P: The problem was that if you take a dactyslip [...] a fingerprint consists of lines. If you put here a magnifying glass, then you see that the lines consist of stripes and points, that's a print of a scanned fingerprint. What happens now with the Dactyslip is that the sheets [of the inked fingerprints] become digitalized and the lines of your fingerprint are transformed into stripes and points. So, you have a large*

quality loss. The moment you scan fingerprints by the INS-console, the quality becomes in any case higher. A bad digital fingerprint scan is probably still better than the best photocopy of an original dactyslip." (INS-console operator, city A)

However, the improved quality and matching rates turn out not to be as straightforward as this. In order to attain the expected accuracy of verification, significant workarounds are needed, that show how risk assessment and identity verifications still rely on assessments independent of the system:

"I: How about the lady with whom it went wrong?

P: […] the system says 'no match' for her fingers […] Are we going to refuse that lady a residence permit, because the prints might not be hers? […] The lady was a Somali national, and although Somalis do that, she had not mutilated her fingerprints […], I checked her fingers myself. Then I took her prints and got a 40 % result. I was like: what is this? […] if you clean your fingers, then the prints are worse, if they are greasy, you gain better prints. What are the oily spots on your skin? It is here [points to side of nose] and on your forehead. So, to get good prints we ask people to rub these spots […]. Yet, these techniques were not helpful. Finally, the project manager said, put her four fingers on the scanner and fold them a little around the table, then you have the right pressure. It was not easy, but we improved the fingerprint quality. We achieved 80 %; that was good quality." (INS officer, city A)

What we see in this excerpt is how the accuracy of the system is in fact something that takes a lot of effort and additional "techniques" to achieve. More specifically, the system is made to perform well because the actual risk assessment is done differently, and turned out negative ('no risk'): When her fingerprints fail to give a match, an asylum seeking woman from Somalia is first suspected of perhaps trying to sabotage the verification process by mutilating her fingertips because she is Somali ("Somalis do that"). The specific risk indicator for that type of sabotage (having mutilated fingertips) is subsequently checked visually by the IND officer: ("I checked her fingers myself"). After satisfying himself this way that no fraud is attempted, the negative verdict of the system is not believed, and all effort goes into the production of a better fingerprint scan. The belief in the first assessment is so strong, that even if all this fails, the project manager is asked to step in and help out to achieve a positive verification.

The other side of this is that any reliance on such a system introduces significant new risks for those whose fate depends on being believed, and whose identity claim of being at risk. That is, a recognised refugee with right of stay, is 'verified' this way. Instead of the promised accuracy and certainty of digitalized biometric identity verification, a number of highly contingent factors determine whether a person passes this verification test, including the assessment by the operator, the manager, the availability of the right levels of pressure and greasiness of the fingers to be scanned.

But often enough, if a person's fingerprints turn out to be unreadable within the configuration of a digital biometric system, this is perceived as an indicator of potential identity fraud. Consequently, the owner of the fingerprint becomes suspect, and changes from a person claiming to be at risk into one that is perceived as risk. This is the case even though it is known that there are more problems with the fingerprinting systems.

For example, the PROGIS-console, although equally intended to improve accuracy, is acknowledged to have an in-built risk of failure, stemming from a weaker predecessor system:

"Webfit is the predecessor of PROGIS, and was the first program using fingerprints that were taken digitally. In Ter Apel, the Alien Police said: we tried out Webfit, but it did not work for us and it took too much time to work with it. The program of Webfit was actually installed in such a way that it always delivered negative results for asylum seekers when verifying their fingerprints. Webfit turned out to have only been tested on Dutch fingers […]; despite updates, the basis for PROGIS is still Webfit." (INS professional about PROGIS)

Ironically, a system intended for the highly diverse population of international refugees and asylum seekers had been tested on a relatively homogeneous population ("Dutch fingers"), thus rendering it basically unsuitable for its purpose.

Here we see the rather paradoxical conception of the body underlying the very idea of biometric technologies as automated identification and authentication tools playing out (Van der Ploeg, 2011) on the one hand, biometrics is based on the biological fact that every individual is physically unique. No two fingerprints are identical, everybody's irises are different from those of another, the same way that no two faces, voices, or retinas are exactly the same. This is the condition of possibility of the very idea of biometric technologies as identification tools.
On the other hand, however, there is a simultaneous assumption of *similarity*: every human person is assumed to have a clearly audible voice, a set of ten fingerprints, two irises, and a recognizable face, and so on. Though hardly ever mentioned as such, this assumption of similarity is as crucial to the functioning of biometric systems as is the assumption of uniqueness.
With respect to the human bodily features used in biometrics, this means that there is an assumption of normality that is defined as a range of variations that constitute 'the normal'. Such notions of normality are built into the equipment: hand scanners have particular shapes and sizes, with designated places to put the fingers; fingerprint systems are designed for the registration and comparison of a particular number of fingerprints, (most systems use one, two or ten), and a particular range of ridge definition; cameras to scan faces are directed at a specific height, and the accompanying face recognition software often works best for a particular shade range of skin colour, and so on. In the case of PROGIS, and its underlying legacy software Webfit, it is this assumed similarity that turns out to be unwarranted, and causing trouble.
The question is, however, for whom it causes trouble. The quote shows operators disqualifying the system: it does not work for them, and it takes too much time to operate. The other side of the coin, however, is that an unsuccessful enrollment or verification may equally well be attributed to the asylum seeker, casting suspicion on them. In a context where policy aims at limiting admittance of refugees, and prevailing distrust of migrants' identity claims is the very reason for introducing technologies that come with the promise of accuracy and certainty, one may wonder who will get the benefit of doubt in any concrete instance of failed recognition on the work floor. This is why we suggest that these systems introduce new risks for the people subjected to them.
In a different way, and for a different set of travellers and migrants, the API system based profiles constitute new risks as well. As described earlier, a traveller can become framed as 'risk' if a match emerges between the attributes of this passenger and an API profile:

> *"[…] we were informed by Madrid that a gang is trafficking women from South- and Central America for prostitution. […] We learnt that these women use Amsterdam as a transit; therefore we built a profile on flights from South and Central-America. We wanted to see all the women, in the age group of 18-24 years, travelling through Amsterdam to Madrid. If a match emerged on these four criteria, then the system signalled that passenger. Since not all female passengers were being trafficked, you had to ask what travel purpose a passenger had. […] there were often no reasons for a stopping, but these are indicators you base your profile on.*

What the above illustrates, however, is how a particular combination of rather general attributes renders a person suspect if a match with the API profile occurs. The very generality of the attributes mentioned - a certain age range or gender - demonstrates the limitations of risk assessments by API. False positives are certain to be many. This highlights that an API profile, and the indicators it is built on, do not really 'capture' risks, but rather mediate and displace the ambiguities and inherent uncertainties of risk.

4.2 Organizational boundaries and information exchange

'Visualization of risk is also done by information exchange between different agencies within the alien and law enforcement chains. This information exchange implies a certain *"partiality of professional knowledge"* (La Fors-Owczynik & Valkenburg in this volume) as each profession focuses on different things, and digital technologies are perceived to overcome inter-agency boundaries between immigration, border control, and law enforcement practices. The following interview excerpt demonstrates that during these communications professional and organizational boundaries are actively maintained. This is in part a consequence of the ways in which knowledge exchange brings along

overlap of tasks between separate local practices. The different identification tasks of the Alien Police for law enforcement and immigration demonstrate that intensive efforts, - or *'boundary work'* (Gieryn, 1983) – are undertaken to protect the integrity of the immigration and law enforcement chains. Yet, these same efforts make cooperation possible between these professions:

> *"P: INS is a distant chain partner of the Aliens Police, but not one that can access the criminal justice database [database for PROGIS-data]. That is separate.*
>
> *K: Yes, but the INS also does identification.*
>
> *P: Yes, […] the INS very often contacts the Aliens Police, and explains: 'Listen, we have someone in detention, but we would like to present him/her [at the embassy]'. Then we [Alien Police] start an identity investigation, but not at the PROGIS-console, but according to our identity investigation task on aliens within the alien chain. So we put the whole PROGIS issue aside. As you see cooperation [with the INS] is there. (PROGIS professional, city B)"*

The distinct functions of the Alien Police in establishing persons' identities within the law enforcement chain via PROGIS, and within the alien chain by comprehensive investigations on 'undocumented' migrants, draw boundaries between the law enforcement and immigration chains. Although these boundaries serve to maintain legally underpinned distributions of work, authority, and responsibility, they also frustrate the INS- and PROGIS-console operators:

> *"We both have the same goal to prevent identity fraud, and one-time registration, and multiple use. And then, of course, legislation should also cooperate in this, a new bill is in progress […]. But now there are two parallel trajectories and I hope they will meet in the best interest of the alien. Because currently assessments are done double, and why? Why don't you look for cooperation? (INS-console operator, city A)*

As "assessments are done double" through enrolment in the PROGIS- and INS-consoles sometimes, the risk of something going wrong, and someone's identity thereby becoming suspect, increases. Risks are *"situated"* entities in the bodies of knowledge upon which they are based (Suchman, 2009), and contingent upon the different socio-technical network within which they emerge. The introduction of new systems, the double use of systems, and the information exchange between them and the organizations that operate them, thus all generate additional risks of error, the burden of which will befall on the people subjected to them. The new legislation currently underway referred to in the quote is presented to reduce the occurrence of this problem by proposing to have one central database for all biometric data used in the alien chain, the BVV mentioned above; at the same time, however, the use of biometrics throughout the various IND and border management procedures is significantly extended, as are the number of agencies that will be legally entitled to enter data or access this database. The Privacy Impact Assessment on this new legislation, conducted by the Ministry of the Interior, identifies a range of 'risks' connected to the new network of systems, such as, for instance, a risk of 'data overload', and emphasises the need for a range of risk reduction measures (*Privacy impact assessment m. b. t. de wijziging van de Vreemdelingenwet 2000*, 2013)

5. Conclusion: technology shifts and proliferates 'risks'

Dutch efforts to reduce identity fraud and illegal entry in the context of migration have come to concentrate on prevention in recent years. Policy makers were calling for a 'better, more complete picture' of migrants in order to enable effective risk assessment of migrants and travelers entering the country. This led to an increased reliance on information systems and digital identification. This chapter has focused on three recently introduced systems for identifying and verifying those posing a risk: the Advanced Passenger Information system for profiling travelers, and the biometrics based identity verification systems within the alien and law enforcement chains, the INS-console and the PROGIS-console.

Our analysis has highlighted how none of the socio-technical configurations of these technologies delivers the flawless accuracy hoped for. While in some respects improvements regarding the prevention of identity fraud and illegal entry by travelers and migrants may have been achieved, a closer look into the way these systems work in practice has shown how a range of potential system fallibilities lead to a shift in localization of the problems rather than a solution.

With the use of the systems, new risk indicators are developed, that amount to new norms concerning what a valid identity is, and, hence, what a trustworthy migrant is. Conforming to these new norms is a challenge also for legitimate migrants and travelers, involving aspects trivial outside the context of digital identification: the 'machine-readability' and greasiness of ones fingertips, or the age at which one travels a particular route at a particular moment. The (in)ability to produce readable fingerprints, or a particular combination of rather general attributes such as country of origin and age/gender may come to inspire distrust in a particular traveler's identity claim. This happens despite the fact that most of these systems, to some extent at least, are built on clay feet: to enter one of the systems for identity verification, one needs to provide a primary proof of identity, the validity of which cannot be checked by the system itself. Hence, a range of tricks, experiential knowledge and trust comes into play in order to assess the reference identity proofs on which all later translations and verifications come to rely.

The consequences of this are twofold. On the one hand, it seriously undermines the trust put into the technology, and the belief that the latest technology delivers what it promises: accurate and strong verification, and identification of those migrants posing a risk of fraud or becoming illegal residents. In this sense, these technologies may foster a false sense of control, security and successful 'prevention'.

On the other hand, however, these 'clay feet' may cause a failure of protection of those most in need for it: from being a refugee fleeing from risk for life and limbs, an asylum seeker confronted with the systems set up to keep out those deemed non-eligible for the protection offered by asylum status, may find themselves being recast as *posing* a risk: a failure to enroll may be met with suspicion of a deliberate attempt to avoid successful registration; a false negative during subsequent verification may cast them as identity fraudster. They may chance upon operators, who, for some reason, and unlike the ones interviewed for this chapter, are little inclined to guide them carefully through either the enrollment or the later verification processes with the range of workarounds required to make the system perform. In this sense, these systems, and the belief in them, actually pose new risks for those coming to our borders for protection against risk.

The Privacy Impact Assessment on the new legislation mentioned above, with its extensive enumeration of 'risks' to migrants' rights posed by the increased reliance on, and extended use of biometrics throughout the alien chain proposed in the new bill within the Netherlands' legislature, underscores this view. Even though it includes a range of risk mitigating measures - for this issue of false negatives, that is, a failure of the systems to match two sets of fingerprints from the same person, for example, it proposes a mandatory check by a dactyloscopic expert in case of mismatch – it remains to be seen how effective and feasible these will turn out to be. The proliferation of 'risks' when using the INS- and PROGIS-consoles and the API profiles underlines the pivotal need for all involved to remain reflective about the pitfalls the use of these systems can bring along for the lives of persons assessed by them.

Bibliography

Agreement between the United States of America and the European Union on the use and transfer of passenger name records to the United States Department of Homeland Security Official Journal of the European Union This. (2012). *Official Journal of the European Union*, (108), 5–14.

Akrich, M. (1992). The De-scription of Technical Objects. In W. Bijker & J. Law (Eds.), *Shaping Technology / Building Society: Studies in Sociotechnical Change* (pp. 205–224). Cambridge, MA, MIT Press.

Besluit van 21 januari 2014 tot wijziging van het Vreemdelingenbesluit 2000 in verband met de uitbreiding van het gebruik van biometrische kenmerken in de vreemdelingenketen in verband met het verbeteren van de identiteitsvaststelling van de vreemdeling (2014).

Bigo, D., & Guild, E. (Eds.). (2005). *Controlling Frontiers: Free Movement into and within Europe*. London: Ashgate.

Broeders, D. (2009). *Breaking down anonymity. Digital surveillance on irregular migrants in Germany and the Netherlands*. Erasmus University of Rotterdam, Rotterdam

Btihaj, A. (2010). Recombinant Identities: Biometrics and Narrative Bioethics. *Journal of Bioethical Inquiry*, *7*(2), 237–258.

Caplan, J., & Torpey, J. (Eds.). (2001). *Documenting Individual Identity: The Development of State Practices in the Modern World*. Princeton University Press.

Clark, R. (1994). Human identification in information systems: management challenges and public policy issues. *The Information Society*, *Vol. 7*(No. 4), pp 6–37.

Council of the European Union. (2004). Council Directive 2004/82/EC on the obligation of carriers to communicate passenger data. *Official Journal of the European Union*, *6*(1), 24–27.

Council of the European Union. (2012). Council Decision of 22 September 2011 on the signing, on behalf of the Union, of the Agreement between the European Union and Australia on the processing and transfer of passenger name record (PNR) data by air carriers to the Australian Customs and Border. *Official Journal of the European Union*, *55*(7), 1.

Council Regulation (EC) No 2725/2000 concerning the establishment of "Eurodac" for the comparison of fingerprints for the effective application of the Dublin Convention. (2000). *Official Journal of the European Union*, *(OJ L316)*, 1–10.

Council Regulation (EC) No. 380/2008 of 18 April 2008 amending Regulation (EC) No 1030/2002 laying down a uniform format for residence permits for third-country nationals. (2008). *Official Journal of the European Union*, *2007*(1683), 1–7.

EU Commission. (2006). Commission decision of 6 September 2005 on the adequate protection of personal data contained in the Passenger Name Record of air passengers transferred to the Canada Border Services Agency. *Official Journal of the European Union*, 49–60.

European Council. Richtlijn 2004/82/EG Van de Raad van 29 april 2004 betreffende de verplichting voor vervoerders om passagiersgegevens door te geven. , Official Journal of the European Union 24–27 (2004).

Gieryn, T. F. (1983). Boundary-Work and the Demarcation of Science from Non-Science : Strains and Interests in Professional Ideologies of Scientists Boundary-work and the demarcation of science from non-science: strains and interests in professional ideologies of scientists. *American Sociological Review*, *48*(6), 781–795.

Holowitz, D., & Noiriel, G. (1992). *Immigrants in Two Democracies: French and American Experiences*. NYU Press.

Latour, B. (1987). *Science in action: How to follow scientists and engineers through society*. Cambridge, Massachusetts: Harvard University Press, Cambridge, Massachusetts.

Law, J. (2009). Actor Network Theory and Material Semiotics. (B. S. Turner, Ed.)*The New Blackwell Companion of Social Theory*. John Wiley and Sons Ltd.

Leers, G. (2011). *Kamerbrief over het aanpak van illegaal verblijf in reactie op het WODC-rapport illegalenschatting 2009*. Retrieved from http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/kamerstukken/2011/07/08/aanpak-van-illegaal-verblijf/aanpak-illegaal-verblijf-in-reactie-op-het-wodc-rapportl.pdf.

Leers, G. (2012a). *Kamerbrief over het gebruik van passagiergegevens in het grensbeheer* Retrieved from http://www.rijksoverheid.nl/documenten-en-publicaties/kamerstukken/2012/03/12/kamerbrief-over-het-gebruik-van-passagiersgegevens-in-het-grensbeheer.html

Leers, G. (2012b). *Notitie inzake openbare orde bevoegdheid burgermeester.pdf*. Retrieved from http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/brieven/2012/05/08/brief-minister-leers-aan-logo-gemeenten/brief-minister-leers-aan-logo-gemeenten.pdf

Lyon, D. (2009). *Identifying Citizens: ID cards as Surveillance*. Cambridge (UK); Malden (USA): Polity Press.

Min. van Binnenlandse Zaken. (2013). *Basis Start Architectuur Architectuur van de Vreemdelingenketen Kennis delen, Informatie gebruiken, Samen doen*. Retrieved from http://www.e-overheid.nl/images/stories/architectuur/architectuur van de vreemdelingenketen.pdf.

Min. van Veiligheid en Justitie. (2011). Het Fundament Progis. Retrieved from http://www.vka.nl/sites/default/files/downloads/Boekje Progis Het Fundament.pdf

Min. van Veiligheid en Justitie. (2011). *Protocol identiteitsvaststelling (strafrechtsketen)* (pp. 1–36). Retrieved from http://www.rijksoverheid.nl/documenten-en-publicaties/brochures/2011/12/22/protocol-identiteitsvaststelling.html

Politie: grondige identificatie voorkomt identiteitsfraude - Security.NL. (2012). Retrieved September 03, 2012, from http://www.security.nl/artikel/42902/1/Politie:_grondige_identificatie_voorkomt_identiteitsfraude.html

Privacy impact assessment m. b. t. de wijziging van de Vreemdelingenwet 2000. (2013). Retrieved from http://www.rijksoverheid.nl/documenten-en-publicaties/rapporten/2013/06/25/privacy-impact-assessment-mbt-de-wijziging-van-de-vreemdelingenwet-2000.html

Sanders, D. (2012). Ministerie van Veiligheid en Jusitie stopt met bouw PARDEX systeem. *Computable*. Retrieved from <http://www.computable.nl/artikel/nieuws/overheid/4728459/1277202/ministerie-vj-gestopt-met-bouw-pardexsysteem.html>

Schouten, P. (2014). Security as controversy: Reassembling security at Amsterdam Airport. *Security Dialogue*, *45*(1), 23–42.

Suchman, L. (2009). Embodied Practices of Engineering Work. *Mind, Culture, and Activity*, *7:1*, 4–18.

Teveen, F. (2013). *JBZ-Raad; Brief regering; Reactie op de brief van de Commissie Meijers van 24 januari 2013 over het EURODAC-voorstel* (pp. 1–6).

Tsianos, V., & Kuster, B. (2010). *Mig@net - Transnational digital networks, migration and gender, Deliverable No. 6: Thematic Report "Border Crossings" (WP4)*.

Tweede Kamer. Terugkeerbeleid (2005). Retrieved from http://www.acvz.org/publicaties/RM_A12a.pdf

Van der Ploeg, I. (1999). The illegal body: "Eurodac" and the politics of biometric identification. *Ethics and Information Technology*, *1*(4), 295–302.

Van der Ploeg, I. (2011). Normative Assumptions in Biometrics: On Bodily Differences and automated classifications,. In S. Van der Hof & M. M. Groothuis (Eds.), *Innovating Government - Normative, policy and technological dimensions of modern government* (pp. 29–40). IT & Law Series, T. M. C. Asser Press, Springer.

Van der Ploeg, I., & Sprenkels, I. (2011). Migration and the Machine-Readable Body. In H. Dijstelbloem & A. Meijer (Eds.), *Migration and the New Technological Borders of Europe* (pp. 68–104). Palgrave Macmillan.

Vingerafdrukken op verblijfsdocumenten. (2013). Retrieved from http://www.ind.nl/Nieuws/Pages/Vingerafdrukkenopverblijfsdocumenten.aspx

Wet van 18 juli 2009 tot wijziging van het Wetboek van Strafvordering, het Wetboek van Strafrecht en enige andere wetten in verband met het verbeteren en versterken van de vaststelling van de identiteit van verdachten, veroordeelden en getuigen (2009).

WRR. (2011). iOverheid. Amsterdam: Amsterdam University Press/WRR. Retrieved from http://www.ioverheid.nu/_pdf/9789089643094_ebook.pdf

Available online at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

Monitoring migrants or making migrants 'misfit'? Data protection and human rights perspectives on Dutch identity management practices regarding migrants

Karolina La Fors-Owczynik *

Tilburg Institute for Law, Technology and Society (TILT), Tilburg University, Tilburg, The Netherlands

Keywords:
Migrants
Data protection
Human rights
Risk
Biometrics
Identification
Profiling
Immigration
Border control
Law enforcement

A B S T R A C T

Record numbers of migrants and refugees fleeing violence and poverty in parts of Africa and the Middle East present the European Union with unprecedented challenges, including in determining their identity as well as status. In recent years problems of identifying immigrants have been addressed in order to fight identity fraud and illegal entry of migrants. As a result, a wide variety of digital systems have been introduced to orchestrate an effective, preventative modus of identification of migrants. Digital systems are in particular geared towards spotting those migrants who (are about to) commit identity fraud or who enter the territory of EU member states illegally. Although the key aim of the digital systems is framed to protect the administrative, geographic and legal borders of the member state and the safety of its population, empirically based studies demonstrate that these systems bring new risks for migrants themselves. This article intends to contribute to the discussion on the use of digital systems for managing the movement of migrants by analysing identification and risk assessment systems from the perspective of the new European data protection regime and the European Convention on Human Rights. For this purpose, two identification systems – the so-called INS console within the Dutch immigration and border sector, and the PROGIS console within the law enforcement sector – are analysed. A third is the Advanced Passenger Information system operated at Schiphol Airport by border control and immigration services. Against the background of the position of many migrants finding themselves at risk in their home country and of the two legislative frameworks mentioned above, this article addresses two issues. First, the analysis focuses on how migrants are perceived by digital monitoring practices: are they themselves at risk, non-risk or do they pose a risk? In the EU, migrants must prove that their case is worthy of asylum status because they are 'at risk' from political unrest or other life-threatening circumstances in

* Tilburg Institute for Law, Technology, and Society (TILT), Tilburg University, P.O. Box 90153, 5000 LE Tilburg, The Netherlands. Tel.: +31 621403891.
E-mail address: K.LaFors@uvt.nl
http://dx.doi.org/10.1016/j.clsr.2016.01.010

their home country. Yet, empirical data gathered through semi-structured interviews show that simply abiding by the standards during an enrolment process of the INS console, rather than being 'at risk', a migrant can easily be categorised as 'posing a risk' (La Fors-Owczynik & Van der Ploeg, 2015). Second, this article aims to investigate what the capacity of the new data protection regime is in protecting migrants from being framed as 'a risk' or a 'misfit' stemming from the use of digital systems. Given this second aim, the following discussion also intends to explore the extent to which the European Convention on Human Rights can provide an additional legal remedy for migrants being digitally categorised in a manner that is detrimental to them.

1. Introduction

> *Refugees and migrants across Libya face rape, torture and abductions for ransom by traffickers and smugglers, as well as systematic exploitation by their employers, religious persecution and other abuses by armed groups and criminal gangs. . .*[1]

Seventy years after the end of the Second World War, with tens of thousands of immigrants having ventured across the oceans in the hope of a better life, Europe's southern and eastern borders are now more than ever sites of mass immigration from Syria, Iraq, Libya and the southern corners of Africa where migrants are reportedly putting their lives at risk every day. As the above quote from a recent Amnesty International report demonstrates, the incomprehensibly horrific cruelties that migrants have become exposed to in traditional – yet since 2009 lawless – transit states such as Libya exacerbate the risks of crossing the Mediterranean Sea. No matter what the dangers of the traumatising boat disasters are, or how abusive the circumstances of the human trafficking can be, migrants embark daily on a journey with the desperate hope of sanctuary within the EU borders. The International Organization for Migration (IOM) described about these immigrants' journey to Europe as the 'most deadly route for irregular migrants'.[2] Such extraordinary and clearly negative circumstances these immigrants find themselves in has prompted discussion on their human rights and the mechanisms that can be established to protect them from being at risk, not least from the cruel practices of those who take advantage of their position.

However, the situation also provides ammunition for those who advocate stricter quotas for immigrants ('Germany presses for quota system for EU migrant distribution, 2015) and tighter controls on identity fraud and the status of migrants. In the Netherlands, the discussion is focused among other things on the opportunities as springboards that large Dutch harbours such as Rotterdam could offer migrants travelling to the UK, similarly to the situation in the French city of Calais. The rhetoric therefore also shapes the current discourse in EU member states on how migrants[3] and refugees are seen. The unprecedented challenges that the flood of migrants constitute both for the EU and the Netherlands increasingly evokes a tendency by which immigrants are framed and categorised as posing a risk rather than being at risk (see also La Fors-Owczynik and Van der Ploeg, 2015).

Bearing in mind the enormous human as well as political challenges that Europe currently faces, the prime goal of this article is to outline some less visible challenges behind the broader theme of people immigrating to or travelling in Europe. Key themes are the developments in and consequences of the use of digital tools in border controls, and immigration and law enforcement practice. The analysis, based on practices in the Netherlands, will also show that there is a subtle interaction between how migrants are digitally categorised or framed and the use of digital technology in border controls, and immigration and law enforcement practices. To demonstrate this interaction, three identity management systems[4] are assessed: two identification systems and one risk assessment system employed by the Dutch authorities. The analysis of this interaction and the empirical findings show that the use of these monitoring systems has the effect of framing migrants as 'a risk' or making them viewed as a 'misfit' in the hosting society. Given this finding, the analysis subsequently aims to contrast this effect with the relevant provisions (such as those with respect to profiling) of the new European data protection regime. In doing this, the analysis aims to shed light on whether the design and use of the systems used for migrant control is in accordance with the new EU data protection rules. Also, it offers the opportunity to reflect on whether the new data protection regime can indeed act as an instrument to address certain negative effects stemming from the ways in which digital technologies are used to categorise migrants. Finally, the article explores the extent to which a human rights

[1] *Libya: Horrific abuse driving migrants to risk lives in Mediterranean crossings* – <https://www.amnesty.org/en/articles/news/2015/05/libya-horrific-abuse-driving-migrants-to-risk-lives-in-mediterranean-crossings/> Retrieved on 12 May 2015.

[2] *IOM: journey to Europe, most deadly route for migrants* – <http://www.ecre.org/component/content/article/70-weekly-bulletin-articles/844-iom-journey-to-europe-most-deadly-route-for-irregular-migrants.html> Retrieved on 5 May 2015.

[3] When I refer to *migrants* in this article, I consider both immigrants and regular travellers who want to cross the Dutch border or pass an identification check-point for immigration or law enforcement and therefore are required to undergo assessments by any of the three systems discussed in this paper.

[4] *Identity management systems* serve to establish 'identities' (defined as personal datasets). This includes the identities of persons subject to the system, in this case migrants, as well as those professionals (e.g. technicians, security agents, border guards, etc.) who interact with this system on a regular basis. These systems serve to both determine identification and allow for differing levels of access control in the process.

perspective can provide additional protection for migrants, by discussing the operation of the digital systems under the European Convention on Human Rights.

The methodology for this analysis is based on legal desk research influenced by insights from science and technology studies (STS), specifically from actor–network theory (ANT). ANT is particularly useful for legal analysis. First, because it helps to show how risks emerge from the use of these systems, and more importantly because a major part of the legal challenges are intertwined with exactly how problems become framed and 'translated' (Latour, 1987) into other problems in practice. For instance, problems of identity fraud or illegal entry are 'translated' into lack of digital information and problems of data quality, or privacy problems into data protection issues. Empirical data[5] for this assessment had been gathered via semi-structured interviews with professionals who use these systems in various Dutch cities.

Following this Introduction, Section 2 gives an overview of current Dutch digital border management and immigration practices and existing scholarship relating to the advantages and disadvantages of biometric identification and risk profiling techniques within immigration and border control practices. The section argues for the incorporation of human rights perspectives during data protection assessment.

Section 3 then provides descriptions of the three systems, and the negative consequences of using these systems on the lives of migrants. By using examples, the section argues that the negative consequences stemming from the use of these digital systems can easily and often falsely categorise migrants as 'posing a risk'.

Section 4 follows up this argument and establishes the relevance of the European Convention on Human Rights (ECHR) with respect to the implications of identity management technologies and risk profiling systems on migrants. Supported by case law, the right to asylum and the right to privacy – established within the fundamental rights framework in its broadest sense – are argued as being of special relevance for those migrants subjected to the INS and PROGIS consoles and to assessment by the Advanced Passenger Information (API) system.

Section 5 then defines some relevant specifications of the new European General Data Protection regime concerning identification practices by the INS and PROGIS consoles and for the risk profiling practices by the API system. By means of empirical insight resulting from self-conducted, semi-structured interviews with immigration, border control and police officers in various Dutch cities, the implications of the practical use of these systems on migrants' lives will be assessed in part against the existing data protection regime, and against the relevant prescriptions of both the new EU Data Protection Regulation and the Police and Criminal Justice Data Protection Directive. Finally, these implications are also evaluated from the perspective of the European Convention on Human Rights.

Section 6 concludes by providing themes for further discussion relating to such essential principles of democracy as proportionality and to the practical relevance of such important questions as how to balance broader societal interests, such as security, with the interests of individual migrants such as the right to privacy and the right not to be discriminated against.

2. Digitalised borders

Data have become a primary resource in today's society. Being part of the European Union and the Schengen area Dutch immigration, border control and law enforcement authorities traditionally led the introduction and use of high-tech (often biometric) identification technologies or other digital systems to assess and differentiate citizens by acquiring data. Given the record number of immigrants and refugees and the current rate of migration from the Middle East and Africa, these systems appear indispensable in 'sorting out' migrants. Since December 2014, for instance, the Netherlands became an active member of the European Border Surveillance System (EUROSUR) (EC/1052/2013). Dutch participation assists in reducing the number of illegal immigrants entering the EU by fostering data acquisition, exchange and analytics at the external borders and between member states. Data-led border control practice has become typical. For instance, the Dutch Customs Services also routinely rely on advanced analytics based on substantial data feeds supplied via such automated systems as the Excise Movement Control System[6] and the Export Control System.[7] EU law (2013/1052/EC) manages and fosters population flow, such as that of travellers and immigrants, to ensure that security threats stemming from border-crossing activities, such as illegal migration or international crime on various migration routes are minimised. At the same time, modern migration policy, such as in the Netherlands (*Wet modernmigratiebeleid*, 2013), prescribes that migrants shall be quickly and effectively sorted out.

The following sections discuss two issues that are key in realising the aforementioned policy ambitions being facilitated by the use of digital tools: identification of migrants (including identity verification requirements) and their profiling. Subsequently, various controversies and human rights implications are discussed.

2.1. *Identification*

Identification is a crucial step in border control, immigration decisions and law enforcement practice within immigration. Migration management boils down to either permitting or denying entry to persons, and to this end various instruments aim to establish and verify the 'accurate' identity of travellers and immigrants.

[5] Part of the empirical data in this article was also used in 'Migrants at/as Risk: Identification and Risk Assessment Technologies in The Netherlands' in Van der Ploeg, I. & Pridmore, J. (eds.) *Digitizing Identities: Doing Identity in a Networked World* (Routledge 2015).

[6] http://ec.europa.eu/taxation_customs/taxation/excise_duties/circulation_control/index_en.htm.

[7] Both systems are designed to enhance the capacity of the Customs Services to filter out cases of fraud by identifying risk patterns in transactional data feed of traded goods ('Inzet van Analytics bespaart douane kosten en brengt effectiviteit in grenscontrole, 2015).

Historically, identity documents (Caplan and Torpey, 2001; Lyon, 2009), and more recently identity management technologies, are seen as inevitable instruments to confirm that an ID bearer is authorised to hold the document, on the basis of which entry can either be granted or refused. Traditionally the state used rather neutral ways to determine whether persons were allowed or denied certain entitlements. The rapid development and the greater use of increasingly technologically 'secured' ID documents and verification devices within the context of immigration and border management, also known as the 'new technological borders of Europe' (Dijstelbloem and Meijer, 2011), appear less neutral. As will be shown, they became focal check-points for (identity) fraud prevention. This practice, as will be demonstrated, is also increasingly true for Dutch law enforcement practices.

2.2. *Profiling*

Within the context of border management and immigration, to intercept the movement of migrants by profiling traditionally differs from forms of identification and identity verification. Profiling is primarily used to prevent such threats as illegal migration, human trafficking and other forms of international organised crime. Profiling does not target particular persons in the first instance, but rather groups of travellers (Dijstelbloem and Broeders, 2014; Wilson and Weber, 2008) and looks for 'types of persons' (Prins, 2014). Within law enforcement, in addition to the above purposes, a profile is also often used to identify new criminal offenders or recidivists. The characteristics are however important for both practices of profiling and identity verification. Profiles within immigration and border control practices are construed based on predefined characteristics of particular persons who have previously been found guilty of some form of crime, such as identity fraud or illegal entry. When constructing profiles these characteristics serve as 'historical data' to rely upon. Subsequently, profiles can be projected on every traveller at border crossing points such as airports. A profile, or the dataset generating a risk flag on a person, is regularly updated over time. This is done mostly in order to adapt to the changes in the behaviour of those persons who have triggered the interest of profilers (Hildebrandt, 2008).

At present, the use of risk profiles constitutes an integral part of the recent 'information-led border control policy' in the Netherlands (Hoogstrate and Veenman, 2012). One of the reasons for this is that risk profiling travellers during border control and immigration practices is encouraged by EU law. According to Directive 2004/82/EC, airlines are required to significantly broaden the set of passenger data they already submit to border control authorities. In the Netherlands, this broadening also serves such priorities as, for instance, stopping travellers suspected of human trafficking[8]: 'to have an eye and an ear for signs of human trafficking is essential in order to tackle it'.[9] Yet, the tendency to update profiles underlines the rhetorical belief in identity management (IDM) systems as being adequate solutions to prevent illegal entry, identity fraud or other forms of crime. The digital profiling of a potential identity fraudster or other 'risky citizen' has recently become a more frequently used practice within Dutch citizen–state relations including border control and immigration practices. However, not only does illegal migration constitute a prime focus for prevention, but also the economic benefits. For instance, the Dutch 'Fraudulent Surcharges Approach Act' (*Wet Aanpak Fraude Toeslagen*, 2014) prevents government payments being sent to social benefit fraudster migrants since January 2014. These Dutch policy developments and related events contribute to the fact that identification, identity verification and risk profiling practices directed at migrants have increasingly become not only the means but also the ends in border management, immigration and law enforcement practices today.

2.3. *Advantages and controversies surrounding identity management systems*

2.3.1. *Advantages*

The fact that these identity management systems have become both the means and increasingly the ends in border management, immigration and law enforcement worldwide shows great faith in the ambitious promises these systems offer to citizens and governments. First and foremost is to prevent harm, such as terrorism, other national security threats, international crime or related issues, coming from outside, and to 'enact' (Law, 2009) the protective prerequisites of a physical border. Second, borders are demarcations that facilitate citizens' free mobility. Identification technology, such as RFID or biometrics, has been used to secure and facilitate global travel, immigration, law enforcement and other administrative dealings with citizens for decades. This also shows that they are seen as being successful in meeting the expectations that governments and citizens have of them.

Following the attacks in New York, London, Madrid, and recently in Paris, IDM technologies have been promoted as indispensable means of forecasting potential 'terror attacks' (Aradau and van Munster, 2005, 2008) and more mundane security threats such as various forms of international crime (Zedner, 2010) and illegal migration. Although we can never be sure how many attacks have been prevented in using the systems, attacks that were apparently prevented demonstrate their success (McNeil et al., 2011). An overwhelming majority of these systems is bound by compliance with international standards, such as those of the ICAO (e.g. biometric standards in passports) or Interpol (records of international criminals) and also with international agreements, such as those between the US, UK, Canada, Australia and New Zealand (an interlinked biometric database shared by these countries[10]), or that between the EU and US (EU–US exchange of passenger

[8] As of 1 January 2005, Art. 273a of the Dutch Criminal Code (*Wetboek van Strafrecht*) came into force, which broadened the definition of human trafficking.

[9] *Aanwijzing mensenhandel* <http://wetten.overheid.nl/BWBR0032576/geldigheidsdatum_29-06-2013 >.

[10] Lewis, P. (2008); 'FBI to get UK biometric hook up?', *The Register*, 15 January 2008, pp. 1 et seq. <http://www.theregister.co.uk/2008/01/15/uk_biometrics_us_canada_aus_independence_waste/>.

name records (PNR)[11]). Biometric data, electronic signatures and RFID chips, for instance, are embedded in new generation passports in many EU member states (including the Netherlands[12]). The push for equipping passports with biometrics has largely been attributed to political arguments. The US Department of Homeland Security (DHS) claimed, for instance, that ID documents with biometrics are 'more trustworthy' and allow for easier management of entry–exit systems at their borders.[13]

In other words, the personal datasets that are produced are used in what Benjamin Muller has termed the 'age of identity assurance', in which governmental agencies use personal information for profiling and risk assessment (2004: 285). Personal data used in such practices are essential in indicating the need for various forms of intervention, or what Amoore describes as 'actionable intelligence' (2009: 20). This 'actionable intelligence' is a driving force in the 'construction' and 'reinforcement' of those citizens – through establishing and using their status – who are considered in need of help, or who are 'at risk', and those who are considered as constituting some form of threat, or are being viewed 'as a risk'. Muller calls such categorisation practices 'sovereign discrimination', which enable the selective goals of a government to intervene in the lives of its citizens and of those that enter its borders (2004: 281).

Within current Dutch discourse, the new digital ways, in which identity fraudsters have been filtered out in the past year, are deemed a success both from the perspective of maintaining security by law enforcement and of gaining economic benefit by stopping or preventing government payments to unentitled citizens (Ministerie van Velighied en Jusitie, 2014).

Beyond the need to maintain security, especially if we look at the huge numbers of incoming migrants, data-driven border control and immigration, or in other words forms of 'information-intensive government' (Taylor et al., 2007), also needs to fulfil the growing expectations of efficiency. For instance, identity checks at borders can be done much more quickly using digital identity verification than without it. Although the focus is mostly on combating fraud, there is also enormous pressure on border guards and immigration officials to control migrants efficiently. Hence, migrants leaving their digital footprints, or what Ericson and Haggerty refer to as their 'data doubles' (Haggerty and Ericson, 2000), is an important requirement for efficiency.

2.3.2. *Controversies*

Beyond the laudable reasons of security and efficiency, government identification and profiling activities are also subject to both public and scholarly criticisms. The Dutch situation is illustrative in this respect. In 2014, the Dutch Data Protection Authority expressed reservations in its annual report[14] with respect to the privacy abusive effects that profiling practices can have for citizens in their relations either with government authorities, commercial companies or private parties in the Netherlands. Numerous scholars expressed criticism from the perspective of how these systems frame the profiled persons' identity as something pre-established (De Vries, 2010), instead of framing identity as something dynamic emerging from the relations in which it is continuously embedded (Van der Ploeg, 2005a, 2005b). Hildebrandt defines as a major concern that, through the ways in which profiling practices emerge, citizens will have 'no effective means to know when profiles are used or abused' (2008). The Dutch government also recently shared its concerns, for instance, regarding the central registration of all air passengers' data at EU level ('Regeringspartijen tegen Europees database vluchtgegevens, 2015). Its main argument is that risk profiling based on immense amounts of traveller data could easily lead to false accusations against travellers.

Furthermore, and often beyond the scope of the assessment of digital profiling methods, IDM systems and the ways in which they are used are not neutral. In fact, Akrich infers: 'the composition of a technical object constrains actants in the way they relate both to the object and to one another' (1992: 206). These constraints become visible in practice when, for instance, profile datasets are processed between databases and used as if they were pure 'representation of persons'. Schouten, in his science and technology based analysis of airport security profiling systems at Amsterdam Airport, for instance, critically concludes that 'translations in the airport security apparatus represent a contrary movement, rendering airport security a technical matter for experts rather than a public one' (2014: 37).

The intense and rapid deployment of biometric technologies and risk profiling systems based on the aggregate of travellers' personal, behavioural and physical data is taking place on an increasingly broad scale. The 'informatization of the body' by these technologies has already provoked a number of political, ethical, societal and cultural concerns (Ajana, 2010; Amoore, 2006; Ceyhan, 2008; De Hert and Sprokkereef, 2009; Schouten, 2014; Van der Ploeg, 2005a, 2005b). Despite international standards, agreements and forms of political advocacy backing such identity management systems, practice demonstrates that these systems are indeed fallible (Magnet, 2011; Schouten, 2014; Van der Ploeg and Sprenkels, 2011) and can result in discrimination (Lyon, 2002, 2009). The consequences of their imperfections for certain citizens' lives epitomise this. One well-publicised and still relevant side-effect of biometrics is illustrated by the case of Brandon Mayfield, who was

[11] Commission of the European Communities 2007, 'Proposal for a Council Framework decision on the use of Passenger Name Record (PNR) for law enforcement purposes', Brussels – <http://ec.europa.eu/commission_barroso/frattini/archive/COM(2007)654%20EN.pdf>.

[12] The Dutch *De Telegraaf Reiskrant* (2009) reports on the first biometric document issued to a Dutch citizen – <http://www.telegraaf.nl/reiskrant/4887056/__Eerste_biometrische_paspoort_uitgereikt__.html?p=30,3> .

[13] The Dutch *ZDnet Nederland* (2005) reports on the EU's request to the US for extra time to accomplish the obligatory introduction of biometric passports within the EU – < http://www.zdnet.nl/news/44553/europa-wil-uitstel-invoering-biometrisch-paspoort/>.

[14] College Bescherming Persoonsgegevens *Dutch Data Protection Authority Annual Report* 2014, retrieved on 12 May 2015 from <https://cbpweb.nl/en/news/dutch-dpa-presents-its-annual-report-2014-extra-attention-paid-profiling>.

falsely accused of having been involved in the 2004 Madrid terror attacks based on a wrong fingerprint match.[15]

Although in the above case Mayfield was compensated, such instances of failure ironically lead to rhetoric, which articulates the need to perpetually improve identity documents and systems. This is perhaps best exemplified by digital identification cards (see Lyon, 2009). In this case, a great deal of trust had been 'inscribed' into these cards (Latour, 1992) since they contain valuable personal data for identity verification and are made difficult to counterfeit (Dodge and Kitchin, 2004). Yet, if these cards are evaluated closely, there is a significant weakness in relation to their production and operation. A biometric identification card requires 'stemming documents' – such as a birth certificate – in order to authenticate and verify the applicant's data before it is issued. As such, the entitlement of a particular person to receive one of these 'technologically enhanced' cards relies on these less verifiable, less secure stemming documents (Clark, 1994; Salter, 2003). Despite their weaknesses and inability to continuously maintain security, biometric systems are still looked upon as being invincible and their continuous improvement is believed to prevent cases of identity fraud and illegal entry. Yet, the fact that failures can even sustain such systems is largely a consequence of the ways in which, as Van der Ploeg argues, identification problems are translated into other problems, and on the other hand that 'each translation implies interpretation' (2005b). As Ajana asserts, clandestine migration remains the 'indicator of the inescapable failure of biometrics to be totally in control of movement' (2010).

However, migrants perpetually adjust to the digitally mediated requirements of these systems that verify their identity and require them to produce information about themselves. Mark Salter suggests, for instance, that the way in which individuals have adjusted to the rules of airports show how travellers have become disciplined, 'docile bodies' (Foucault, 1977; Salter, 2007). Travellers are prepared 'to confess' their personal information in front of these systems in order to gain passage. Data are then verified against personal datasets processed in the configuration of IDM technologies, a practice Salter refers to as the 'confessionary complex' (2007: 57).

Another controversy relates to the non-neutral nature of the use of the technologies and the manner in which the applications determine the ways in which people are dealt with. The practices outlined above are never 'innocent' in that migrants are 'sorted into categories' (Bowker and Leigh Star, 1999). Suchman explains that, at the micro-level, categories epitomise how political processes for the exclusion and inclusion of persons emerge (1994). Such selective processes have generated tension between governments and their citizens for a long time, tensions that are evident in policy debates over information sharing and what Schwartz calls the 'privacy collision' between the EU and the US (2013). Other forms of tension, such as discrimination against immigrants via digital border management are also apparent in different contexts within Europe (Bigo, 2013; Broeders, 2009). Amoore describes the categorising practices causing these tensions as gradually building an 'architecture of enmity', as the 'projected images and stereotypes' that are embedded in these categories make 'threat and antagonism possible' (2007: 218). This architecture aims to secure society by first defining and separating out those who are seen or understood as 'others', namely not a part of the society to be secured (ibid.: 218). Yet, as regards biometrics being part of this architecture, Van der Ploeg and Sprenkels explain that digital fingerprints, photographs or satellite images are not pure representations of migrants, but are reconstructions of migrants by digitalisation (2011). Dijstelbloem and Broeders describe these 'reconstructions' circulating across databases and networks as 'non-publics' (2014). In their argument, a difference between publics and 'non-publics' is crucial, as these categories '*capture specific moments in time and specific spatial locations where the categorization of persons emerges in association with more (green-listed), less (black-listed) or unclear, ambiguous (grey-listed) rights*' (ibid.: 33).

Although the distinction between the publics and non-publics is useful to make when entitlements are assigned to migrants, these concepts still separate the virtual data from the actual person. Therefore, Ajana's concept of 'recombinant identity' (2010), which is '*the terminal point at which data recombine into an identity in the concrete, corporeal and material sense*', lends itself being more useful to assess the three systems in this article. Using this concept, Ajana offers a perspective that allows us to analyse the developments away from the oft-used distinction between the virtual persona (data on a person) and an actual living individual. This is essential as it requires us to move away from the 'pure' data protection debate towards a broader one, that data protection questions also incorporate a human rights perspective (i.e. dealing with values of and respect for human individuals on the one hand and their personal data on the other).

2.4. *Plea for human rights perspectives beyond data protection assessments*

The need for human rights perspectives beyond 'pure' data protection assessments is essential as IDM systems are often perceived and described as 'neutral' instruments, as mere tools to assist in efficient and effective migration procedures. A risk related to such a perception is that it depicts these systems as being merely 'technical', separate from the human involvement necessary to operate them and give them 'a human face'. Often, when issues arise as a consequence of the functioning of these technologies, such as for instance privacy invasion, an assessment by means of the rather technical legal instrument of data protection regulation is regarded as sufficient. As detailed elsewhere (La Fors-Owczynik, 2015), privacy impact assessments also exhibit this narrow perspective (Rijksdienst, 2013; Schreuder, 2014). Therefore, data protection assessments accompanied by human rights considerations could redound to IDM techniques not becoming such 'ends' or tools in border management, which only necessitate technological fixes when societal problems arise from their use. Such a combined assessment should precede the actual implementation of these systems in order to better facilitate the relevance and practical enforcement of human rights principles. Before discussing this combined assessment in more detail, the following section reflects upon the extent to which both the upcoming

[15] Henry Schuster & Terry Frieden (2006); 'Lawyer wrongly arrested in bombings: "We lived in 1984"'; *CNN Justice* – < http://articles.cnn.com/2006-11-29/justice/mayfield.suit_1_train-bombings-brandon-mayfield-madrid?_s=PM:LAW >.

EU Data Protection Regulation[16] and the EU Police and Criminal Justice Data Protection Directive offer by themselves (that is without an additional human rights assessment) sufficient protection and remedies for the risks described in the current use of the IDM systems (the INS and PROGIS consoles and the API system).

3. The INS console, PROGIS console and the API system within the Dutch legal and administrative landscape

Although the three applications discussed below are typical of the Dutch setting, they operate in the wider EU context and are therefore closely linked both in their design and operation to EU systems used in the policy domain of migration. They are part of a wide landscape of networked databases and digital circuits where data are shared extensively. Key EU networks that form this broader landscape are the Schengen Information Systems (SIS I and SIS II), the EU's Visa Information System (VIS) (European Commission, 2015) and Eurodac (Council Regulation (EC) No. 2725/2000), the last-mentioned being a central biometric database in which the fingerprints of asylum seekers registered in any member state are stored. The Netherlands is also required to use Europol's Secure Information Exchange Network Application (SIENA) (European Commission, 2015) as its primary channel for sharing law enforcement information, and EUROSUR[17] as a channel for exchanging surveillance information about illegal migration and cross-border crime at the EU's land, sea and air borders.

The working of all three systems will next be briefly discussed, followed by a conclusion that outlines some common features concerning their operation.

3.1. *The INS console*

Council Regulation (EC) No. 380/2008 prescribes that all member states of the EU should introduce residence permits for third-country nationals.[18] These are required to be equipped with a digital '*photograph [. . .] and two fingerprints taken flat*'. The INS console is used by the Dutch Immigration and Naturalisation Service to meet this regulation.

After a third country national is enrolled by the Dutch INS console the registered data are encrypted on the chip of the residence permit. The immigrant's identity is verified against these data and as of 1 March 2014 a photograph and the alien's ten fingerprints are registered also centrally with the Basic Facility of Aliens (BFA)[19] (2014).[20] The BFA[21] is a major database for authorised government agencies containing data about all immigrants within the Dutch immigration and border control chain.[22] The Dutch Personal Data Protection Act applies to all data gathered by the immigration and naturalisation services. Further prescriptions concerning the processing of aliens' personal data, including potentially sensitive data, for instance, of asylum seekers, are set by the Dutch Alien Act. For the retention of aliens' biometric data, including that gathered by the INS console, the Alien Act sets the limit at ten years.

The INS console is used to verify the identity of the residence permit holder as follows: the fingers of the residence permit holder are placed on a biometric fingerprint reader; the recorded images are then verified against those encrypted in the permit. If there is a match, the identity verification indicates that the identity of the residence permit holder is correct, and that residence permit belongs to the bearer. The direct scanning of fingerprints by the INS console fingerprint reader system had been envisioned to provide a much greater degree of certainty[23] (Teveen, 2013) as to the residence holder's identity than dactyslips (sheets of inked fingerprints) provide. All third country nationals will be enrolled using the INS console. However, when the interviews providing empirical data were taken, the INS had started by only enrolling asylum seekers. Although not all immigrants have yet been registered using the INS console, officials using the system have expressed their concerns relating to the right to privacy and even to the right to asylum. For instance, when the fingerprint reader displayed a false negative result for an asylum seeker during verification processes, a professional responded as follows:

I: How about the lady for whom it went wrong?

P: [. . .] the system showed 'no match' for her fingers [. . .] Are we going to refuse that lady a residence permit, because the prints might not be hers? [. . .] The lady was a Somali national, and

[16] In December 2015 the text of the new General Data Protection Regulation reached its fairly final form. This can be regarded as quite a substantial achievement within the data protection history of Europe. The new prescriptions will provide a much stricter and also more 'human rights-minded' legal remedy for private citizens, such as the rules related to 'breach notification'; 'privacy by design' or 'data protection impact assessments' also demonstrate this. At the same time, the new legal instruments are also promising as they provide comprehensive legal guidance, including fines in case data protection prescriptions are violated, for public, commercial and other parties involved in processing personal data.

[17] Regulation (EU) No. 1052/2013 of the European Parliament and of the Council of 22 October 2013 establishing the European Border Surveillance System (Eurosur), OJ 2013 L 295.

[18] Aliens are all citizens, not having Dutch, EU, Norwegian, Icelandic, or Swiss nationality.

[19] The regulation allows for more than 30 authorities within the Dutch immigration and border control chain to verify the identity of third country national immigrants.

[20] *Besluit van 21 januari 2014 tot wijziging van het Vreemdelingenbesluit 2000[. . .]:* Due to parliamentary protests, the D66 Party achieved that this law will be valid for seven years and then a new vote shall take place whether to continue with the central registration of biometric data of aliens. After five years, an evaluation of this law shall take place.

[21] Any Dutch immigration or border control authority can check the identity of an enrolled immigrant against INS console data in the BFA.

[22] The BFA traditionally also contains copies of inked fingerprints, also called as dactyslips, of third country national asylum seekers. A copy of each asylum seeker immigrant's dactyslip is prescribed by the EU's Dublin Convention (Council Regulation (EC) No 2725/2000) to be submitted to the Eurodac central database.

[23] This was explained by eliminating a step in the process which during the production of dactyslips was seen to decrease the verifiability of fingerprints. Dactyslips are produced from inked fingerprints by digitising the paper sheets bearing the inked prints, yet the direct scanning eliminates the digitization step.

*although Somalis do that, she had not mutilated her fingerprints [. . .], I checked her fingers myself. Then I took her prints and got a 40 % result. I was like: what is this? [. . .] if you clean your fingers, then the prints are worse, if they are greasy, you gain better prints. What are the oily spots on your skin? It is here [points to side of nose] and on your forehead. So, to get good prints we ask people to rub these spots [. . .]. But, these techniques were not helpful. Finally, the project manager asked her to put her four fingers on the scanner and fold them a little around the table, and then the pressure was right. It was not easy, but we improved the fingerprint quality. We achieved 80 %; that was good quality. (INS officer, city A)**[24]

3.2. The PROGIS console

Identity fraud is a major concern within the Dutch law enforcement chain, and the prominence of the problem has grown every time a person has been reported as being different to the one originally sentenced for a particular crime. In 2009 the Dutch Act on Identification of Suspects, Convicts and Witnesses[25] was introduced to harmonise data with respect to the identity of criminal suspects, victims and witnesses. The Act requires law enforcement and justice authorities to obtain ten digital fingerprints and a facial photograph of suspects and convicts and thereby to construct harmonised, verifiable identity of a person available to every authority within the law enforcement chain.[26] The Dutch Decision on Establishing the Identity of Suspects and Victims[27] of 2009 explains in detail that only the biometric features of suspects, convicts, former suspects, unknown convicts and deceased persons are registered. Being part of the information provision program of the Dutch criminal law chain (PROGIS, in Dutch: *Programma Informatievoorziening Strafrechtsketen*), the PROGIS console is used for law enforcement purposes. Hence, PROGIS data fall under the data protection prescriptions of the Dutch Police Data Act. The registered fingerprints and photographs are called the 'ID state' of the person, the aim of which is two-fold. First, the use of the ID state by law enforcement authorities allows for them to verify persons against 'integrated identity' data (2011) and prevents each authority from separately establishing identity data about a criminal, witness or suspect. Second, the Dutch Ministry of Security and Justice intends the ID state to ensure that the person incarcerated is the same person as was sentenced ('Politie: grondige identificatie voorkomt identiteitsfraude – Security.NL, 2012). Associated with each PROGIS ID state is a criminal justice chain number (CJCN, in Dutch: *strafrechtsketennummer* – SKN) and a biometric number. Both numbers are registered centrally in the Criminal Justice Chain Database (CJCD). A biometric number is associated with an ID state, and a CJCN is associated with the criminal person.

The Dutch Alien Police operates the PROGIS console, and the biometric information gained by enrolment using the system is shared only among agencies within the Dutch law enforcement and justice chain. If an immigrant is suspected of a crime (for instance, a visa overstay, which is a crime in the Netherlands), the immigrant is identified by the PROGIS console as a criminal suspect in the Netherlands. Although the purpose of PROGIS is to improve identity verification and consequently certainty about the identity of a person standing in front of the police officer, PROGIS often produces negative results (La Fors-Owczynik and Van der Ploeg, 2015) in practice. This raises severe privacy concerns:

*Webfit is the predecessor of PROGIS, and was the first program to use fingerprints that were taken digitally. In Ter Apel, the Alien Police said: "we tried out Webfit, but it did not work for us and it took too much time to work with it." The Webfit program was actually installed in such a way that it always delivered negative results for asylum seekers when verifying their fingerprints. Webfit turned out to have only been tested on Dutch fingers [. . .]; despite updates, Webfit is still the basis for PROGIS, and we still often get negative results. (INS professional about PROGIS)**

3.3. Advanced passenger information system

The Advanced Passenger Information (API) system exemplifies a smart border system that the guidelines for which were set up according to the latest standards of the International Civil Aviation Organization (ICAO), the World Customs Organization (WCO) and the International Air Transport Association (IATA). Given that the Netherlands is signatory party to the Schengen Agreement and the corresponding Schengen Border Code, the introduction of the API system at Schiphol Airport constitutes part of the control of the extensive European 'smart-border' network, the set-up of which was heavily advocated by the European Commission (2011).

The sole aim and purpose of the API system at Schiphol Airport is to prevent illegal entry into the Netherlands, whereas the API Directive 2004/82/EC allows for this purpose to be combined with others, such as preventing international crime, such as stopping those involved in human trafficking (2004). Therefore, Dutch border management and immigration authorities operate the system to sort out travellers according to risk profiles registered in API system. These profiles contain attributes of delinquent passengers that range from behavioural and bodily attributes, to accessories or clothing, to flight information from the departure control system of air carriers, to data from the machine readable zones of travel documents. Specifically to prevent illegal migration to the EU, API Directive 2004/82/EC prescribes that member states, including the Netherlands, exchange passenger data on incoming and outbound flights prior to departure. The retention period for such data is 24 hours, within which period such data shall also be cross-checked against API profiles. Receiving such information on

[24] The quotes with an '*' can also be found in La Fors-Owczynik. and Van der Ploeg (2015) '*Migrants at/as risk: Identity verification and risk assessment technologies in The Netherlands*' in Digitizing identities: Doing identity in a networked world (eds. Van der Ploeg, I. & Pridmore, J.), Routledge.

[25] *Wet identiteitsvaststelling verdachten, veroordeelden en getuigen*, 2009.

[26] The introduction of the PROGIS console kept the police's routine in fingerprinting suspects in remand and convicted criminals by ink and the production of dactyslips, digital scans of the inked fingerprint sheets. These sheets are still produced and transferred to the Facility for Verification and Identification (FVI, in Dutch: *Voorziening voor Verificatie en Identificatie*) (Min. van Veiligheid en Justitie, 2011).

[27] *Besluit identiteitsvaststelling verdachten en veroordeelden*, 2009.

passengers before their flight departs was seen essential to prevent not only illegal entry, but also such broader threats as terrorism or international crime (Leers, 2012). Consequently, as of January 2012, air carriers departing from 28 airports[28] that are considered to be high risk are obliged to submit passenger data without prior request to relevant border control agencies before their departure. The type of passenger data is laid down by the Dutch Alien Order 2000 (in Dutch: *Vreemdelingenbesluit*, 2000; Korthals & Cohen).

Legal prescriptions related to the processing of API data fall under the Dutch Police Data Act. This is because border control tasks are assigned by the Dutch Police Act 1993 to the Dutch Royal Military Police. The Dutch Data Protection Authority (DPA) in a letter to the Minister of Immigration, Integration and Asylum expressed its concerns over privacy regarding the government's intention to extend the set of API data (Kohnstamm, 2012) that the Dutch Royal Military Police can request for the detection of illegal immigrants and prevention of related criminality. The main concern expressed by the DPA was that the purpose and effectiveness of broadening the scope of API profiles have been insufficiently demonstrated by the Dutch government. In a subsequent letter the DPA also shared its concerns about whether the processing of API data meets the requirements of the Dutch Data Protection Act. Moreover, concerns relating to the question of which authority (INS, KMar or others) at the border will be responsible for the processed passenger data before data from air carriers are sent to border control authorities (Tomesen, 2012). These concerns are further aggravated by the fact that in practice API profiles often produce false positives (La Fors-Owczynik and Van der Ploeg, 2015) and unnecessary detention of passengers:

> *[. . .] we were informed by Madrid that a gang was trafficking women from South and Central America for prostitution. [. . .] We learnt that these women use Amsterdam as a transit; therefore we built a profile on flights from South and Central America. We wanted to check all women in the age group of 18–24 years travelling through Amsterdam to Madrid. If a match emerged on these criteria, then the system flagged that passenger. Since not all female passengers were being trafficked, you had to ask what a passenger's purpose of travel was. [. . .] there was often no reason to stop the passenger, but these are indicators you base your profile on. (Royal Military Police officer about API)**

3.4. *Interim conclusion*

The above discussion shows that the three systems are clearly different, not only in their operation, but also in their technological, legal and administrative environment. However, what makes them comparable are their effect on travellers, immigrants, refugees and asylum seekers. In particular, all three systems function on the basis of design and operational features that frame migrants as constituting a risk (for identity fraud, illegal immigration, etc.). One could say that the default for the identification process is a mindset of suspicion. As such this is not problematic. However, given the accuracy problems that all three systems face (producing false positives, unnecessary detention of passengers, etc.), migrants see themselves confronted with a situation in which they are digitally framed as a potential risk to society. The empirical examples and findings presented in this article demonstrate that an immigrant can much more easily be framed 'as a risk' (La Fors-Owczynik and Van der Ploeg, 2015) by the PROGIS console identification and verification process, than a regular citizen. Moreover, empirical data also show that when using the API system, the potential for a match between attributes in a risk profile and attributes of the traveller renders travellers being viewed as increasingly suspicious of posing a risk, or 'as being a risk'. Also, empirical details show that the use of these profiles can lead to false accusations against travellers and to infringements of their right to privacy (Article 8 of the ECHR), eventually also the right to liberty (Article 5 of the ECHR) and in some cases even the right to asylum.

A key question at this point is then whether the current legislative framework offers an adequate mechanism for addressing situations where migrants are unjustifiably framed as a risk, for instance facing unjustified criminal accusations at airports. Or, in other cases even being potentially sent back to their home country, thus not receiving the protection that our society ought to provide them, given they are at risk in their home country. Section 4 therefore looks at the European Convention on Human Rights, followed by a discussion in Section 5 of the new EU data protection regime.

4. The European convention on human rights

The ECHR contains a wide range of provisions relevant for the protection of migrants. Article 8 of the ECHR on the right to respect for private life and family life is of critical relevance. Although the ECHR does not contain this right explicitly, the human right to asylum is also crucial for this analysis. The right to privacy requires that each person shall be protected from physical and also digital threats to their privacy. In this sense the right to privacy can be regarded as a pre-requisite to other rights, such as the right to liberty (Article 5), the right not to be discriminated against or the right to data protection (as laid down by the Charter of Fundamental Rights and Freedoms of the European Union[29]).

4.1. *Human right to privacy*

Immigrants and travellers are exposed to intensified mechanisms of security control. These groups regularly find themselves in the middle of public safety versus privacy dichotomies, although in different ways. The case law of the European Court of Human Rights (ECtHR)[30] demonstrates that public safety interests often override the individual privacy interests of a migrant. To make the potential privacy right limitations of the use of digital systems for all citizens,

[28] The risk of illegal migration from these 28 locations is deemed to be very high.

[29] Charter of Fundamental Rights of the European Union [1999] OJ C364/01.

[30] App. No. 35753/03, ECtHR, 11 January 2005 and App. No. 26625/02, ECtHR, 24 January 2006.

including migrants, transparent is set out by law. Therefore, to assess how the human right to privacy can strengthen the position of migrants with respect to the negative consequences that biometric identification and risk profiling practices can cause them is critical.[31]

The ECHR sets out the fundamental right to a private and family life (Article 8). The Convention also defines conditions of exception under which government agencies are allowed to infringe this fundamental right. ECtHR jurisprudence[32] also specifies that any form of infringement of this right shall be in accordance with the principles of proportionality (the infringement shall not imbalance the pursued objective) and subsidiarity (the pursued objective cannot be achieved with less intrusion on the citizens' privacy). The collection and storage of data must comply with these principles and the infringement of the right to privacy must be legitimised by law, must pursue a legitimate aim and must be necessary in a democratic society. Although migrants have travelled from beyond the legal borders over which the Convention applies, the enforcement of the human right to privacy by EU border control, immigration and law enforcement authorities is essential as these migrants' aim is to enter the EU. For such authorities to set an example how human rights are enacted in practice, while operating digital identification or risk profiling systems, is of the utmost importance.

Over the years, the ECtHR has ruled several times on issues where the privacy or private life of migrants in the broadest sense was at stake. Several of these cases are of relevance for the protection of migrants when technology is used to process them and thus frame their position.

On 16 July 2009, for example, the Grand Chamber of the ECtHR issued a judgment in the case of *Féret v. Belgium*[33] in which it strictly condemned the state for its use of language on its internet publications, which incited discrimination and racial hatred against immigrants:

> *Political discourse which incites hatred based on religious, ethnical or cultural prejudices represents a danger for social peace and political stability in democratic States.*

Furthermore, the ECtHR:

> *attaches particular weight to the medium [the Internet] used and the context in which the impugned remarks were expressed in the present case, and consequently their potential impact on public order and social cohesion.*[34]

This case is relevant to our discussion as among other things it requires the agency using the technological application to mediate and therefore address the potentially negative implications of a particular government communication that is technology-based. Given that both biometric identification and risk profiling systems have mediating and therefore potentially aggravating effects (e.g. when they distribute wrongful, potentially discriminative information on migrants), the above judgment offers an indication that the potential harmful effects of a specific technology used should be considered and if necessary addressed by the state.

On 4 December 2008, in the case of *S. and Marper v. UK*, the Court ruled on the situation of an 11-year old applicant who was accused of attempted robbery. His fingerprints and DNA were registered with the UK DNA database. After the charges against him were dropped, he requested the removal of his registered data. This was turned down. Subsequently, he filed charges against the UK police at the ECtHR, and stressed that the retention of his data by the police violated his right to privacy (Article 8 of the ECHR). The Court indicated that:

> *the retention at issue constitutes a disproportionate interference with the applicants' right to respect for private life and cannot be regarded as necessary in a democratic society.*

This judgment is important in light of this article's theme, given that it relates to the retention of biometric data on innocent persons by police authorities. It is therefore of relevance for biometric identification practices of law enforcement authorities using the PROGIS console. The ECtHR ruled in favour of the right to privacy when fingerprints are retained non-proportionately by law enforcement authorities:

> *The Court accordingly considers that the retention of fingerprints on the authorities' records in connection with an identified or identifiable individual may in itself give rise, notwithstanding their objective and irrefutable character, to important private-life concerns. [. . .]the Court [. . .] considers that, while it may be necessary to distinguish between the taking, use and storage of fingerprints, on the one hand, and samples and profiles, on the other, in determining the question of justification, the retention of fingerprints constitutes an interference with the right to respect for private life.*

A final example of a ruling relevant to our discussion is the case of *Thlimmenos v. Greece*[35] in which the ECtHR ruled specifically in favour of the right not to be discriminated against:

> *the right not to be discriminated against in the enjoyment of the rights guaranteed under the Convention is also violated when States without an objective and reasonable justification fail to treat differently persons whose situations are significantly different.*

This judgment is of vital importance in light of profiling practices by Dutch border control and immigration authorities. Its importance is particularly relevant when it comes to potential

[31] On this, see the United Nations Human Rights Committee (CCPR) General Comment No. 16 (8-04-1988): The right to respect of privacy, family, home and correspondence, and protection of honour and reputation (Art. 17). See also Council of Europe (2005), *Human Rights and the Fight against Terrorism – The Guidelines of the Council of Europe*, Guideline VI: 'Measures used in the fight against terrorism that interfere with privacy [. . .] must be provided for by law'.

[32] App. No. 28341/95, ECtHR, 4 May 2000 and App. No. 30562/04 & 30566/04, 4 December 2008.

[33] App. No. 15615/07, ECtHR, 16 July 2009.

[34] Ibid.

[35] App. No. 34369/97, ECtHR, 6 April 2000.

false negatives produced by biometric registration and verification via the INS or PROGIS consoles.

4.2. *Human right to asylum*

Given the problems with the working of the three systems (false positives, false negatives) outlined earlier, migrants are at risk in that they can potentially be digitally framed as posing a risk, thus giving them the status of *persona non grata*. This categorisation can indirectly contribute to the rejection of their asylum request and to their deportation, and consequently can lead to further exposure to torture and inhuman treatment in their home or a transit land. Although the ECHR does not contain an explicit right to asylum in itself, the Court has created an opening for such a right given that it has established the right to asylum as a fundamental human right, which will have positive implications for future asylum cases. A number of such cases will be briefly described below. It should be noted that the Charter of Fundamental Rights and Freedoms of the European Union,[36] which was introduced to harmonise and enforce (ECHR) human rights law within the context of the EU, also introduced the right to asylum as a separate fundamental right.

On 17 July 2008, the ECtHR ruled in *NA. v. United Kingdom*[37] that the United Kingdom could not expel an applicant (of Tamil origin) because that would breach Article 3 of the ECHR. If expulsion were to take place, there was sufficient evidence to prove that the applicant would be exposed to inhuman treatment in his home country, Sri Lanka, due to his ethnic origin.

In another judgment, the Court went even further by finding violations of the ECHR by EU member states. On 21 January 2011, in the case of *M.S.S. v. Belgium and Greece*,[38] the ECHR reprehended both Belgium and Greece for automatically applying the Dublin Convention to an asylum seeker. The applicant, an Afghan national, claimed that his rights under Articles 3 and 5 would be infringed.

The third judgment with respect to the right to asylum is unique of its kind. On 23 February 2012, in the case of *Hirsi Jamaa and others v. Italy*,[39] the Court ruled for the first time against an EU member state on immigrants' interception at sea. The applicants, 24 Somali and Eritrean nationals, alleged that Italy violated their right to be protected from torture as laid down by Article 3 of the ECHR, when Italy attempted to deport them back to Libya. The Court found that Italy violated Article 3 and Article 4 of Protocol No. 4,[40] which prohibit collective expulsion. Furthermore, the Court found the Italian government guilty of breaching Article 13 of the ECHR and required the government to pay fines amounting to more than EUR 15,000 per applicant. Apart from the unique precedent this judgment set concerning seaborne immigration to the EU, the decision established crucial extraterritorial relevance for the European Convention on Human Rights. This judgment strengthens human rights remedies for all asylum seekers.

4.3. *Interim conclusion*

The above Court rulings on both privacy and asylum provide useful guidance for cases in which biometric identity management and risk profiling systems on migrants, including immigrants and travellers, are used. In the specific situation of asylum-seeking immigrants, the right to asylum and the right to privacy are closely intertwined. This is because the negative consequences that digital enrolment and verification mechanisms by the three systems can have on asylum seekers could result in infringement of both their right to privacy as well as their right to asylum. This only further emphasises the need for strengthening the legal position of this group.

The ECtHR cases on the right to privacy enshrine the necessity for states to give utmost priority to the enforcement of such rights within the contexts where the INS console, PROGIS console or API system are used. To enforce these rights in practice is essential as they provide immigrants and travellers with a broader protective legal environment against the downsides of identification and profiling practices than the existing, and in part also the proposed, data protection regime.

5. The new European data protection regime: identification and risk profiling of migrants

All three technologies discussed in Section 3 target individuals either directly or indirectly. Whereas the INS and PROGIS consoles are aimed at establishing and verifying a person's identity, the API system is geared towards sorting out persons based on the characteristics built into a risk profile. Although the INS and PROGIS consoles are both identification systems, because of their legally and administratively strictly separated settings, they deal with persons differently. The consequences of using these systems are useful in assessing the provisions of the new EU data protection regime that are related to identification and profiling. The new regime will replace Directive 95/46/EC, and Framework Decision 2008/977/JHA on policing related personal data will provide substantially broader legal protection and remedies for citizens from the effects of digital technology use. The immense growth in digitalisation within all aspects of citizens' lives in the past 25 years has necessitated new data protection prescriptions. The new General Data Protection Regulation (GDPR)[41] and the Police and Criminal Justice Data Protection Directive[42] will be in effect as of the end of 2017.

[36] Charter of Fundamental Rights of the European Union [1999] OJ C364/01.

[37] App. No. 25904/07, ECtHR, 17 July 2008.

[38] App. No. 30696/09, 2011, ECtHR 108.

[39] App. No. 27765/09, ECtHR, 23 February 2012.

[40] N. Frenzen, 'Hirsi v. Italy: Prohibition of collective expulsion Extends to Extra-territorial actions' *Migrants at sea* (Los Angeles, 23 February 2012), retrieved on 10 May 2015 from <http://migrantsatsea.org/tag/european-court-of-human-rights/>.

[41] In this article I use the latest version of the GDPR accepted on 15 June 2015 by the European Council and the European Parliament.

[42] In this article I use the version from 2012 of the Police and Criminal Justice Data Protection Directive.

5.1. *Data protection and human rights controversies in day-to-day use of the INS and PROGIS consoles and API system*

5.1.1. *Establishing 'accurate identity'*

5.1.1.1. . . . using the INS console. Data protection regulations, including the new GDPR, do not deal extensively with issues preceding the digital enrolment of persons into identity registration processes. However, this omission is highly influential in determining the reliability and quality of digital data, which are supposed to prove the accuracy of an immigrant's identity. Biometric information datasets, as also generated by the INS console, are claimed to be more trustworthy as persons cannot easily fake their biometric features (La Fors-Owczynik and Van der Ploeg, 2015). Yet, paradoxically, within the immigration chain, this information is often based on quite weak credentials. An INS officer operating a mobile version of the new INS console in a refugee camp related the following:

> *I: How can you be sure that an [undocumented] person you want to identify using the INS console is who he/she claims to be?*
>
> *P: That you never know. To give you a simple answer: I can only hope that a person who says something about him/herself to me, says the same thing to our UNHCR colleagues. It could be a lie both times, but since I cannot figure this out otherwise, I must be satisfied with the consistency of the refugee's story. (INS professional, city D)**

This quote demonstrates that such an easily falsified credential as the same personal history told twice can routinely provide a basis for enrolment by the INS console. Certainly, the difficulty for refugees to provide more trustworthy credentials to INS officers shall not be underestimated. Yet, it is worth discussing whether this significant deficit in relation to the reliability of the registered identity data on an immigrant does not undermine the 'principle of data quality' as set out in Article 6 of the 95/46/EC Directive. If similar cases emerge in the future and the new GDPR is already in effect, evaluating the implications of weak credentials on the 'accuracy' principle as set out in Article 5(d) during digital identification would be essential.

The above example also demonstrates the trust INS officers must place in the immigrant's personal history. Furthermore, this shows how a migrant's right to asylum becomes enforced in daily practice and it also provides a positive example for framing migrants as being 'at risk'.

5.1.1.2. . . . using a PROGIS profile. Establishing a PROGIS profile should serve to increase the accuracy in identifying a person, including a migrant. However, the diversity of consoles and the network of systems PROGIS is built up from often require multiple attempts to enrol a migrant or criminal, and produce verifiable fingerprints:

> *I: How about the standard criteria? I also saw that when a fingerprint is indicated as green, this means a reasonably good quality, right?*
>
> *P: Yes, but the fingerprints read by the scanner are linked to another system [than those which are registered in the CJCD]. It may happen that one scanner on a console will do everything neatly and display fingerprints as green. But the systems behind the scenes, which actually read the fingerprint, need a higher quality, because they need to display images as clearly as possible. So, a fingerprint that looks good at first glance may sometimes be still rejected.*
>
> *I: How does this happen?*
>
> *P: The Royal Military Police has many such problems. They also have PROGIS consoles. [. . .] Their systems are based on WebFIT stations (a system behind the scenes in PROGIS) which are only for aliens. But because the WebFIT stations had only been tested on Dutch fingerprints, the fingerprints of aliens were always rejected, and the Royal Military Police had to retake fingerprints four or five times from the same alien. Since fingerprints are tagged with a barcode, the system says: this barcode is already known, retake the fingerprint. (PROGIS police officer, city B)*

The above problem cannot be addressed through the existing 2008 Framework Decision. However, in future, Article 4 of the Police and Criminal Justice Data Protection Directive will provide better remedy for migrants should a border guard requests migrants to retake their fingerprints. This Article prescribes such 'principles relating to personal data processing' as whether the data have been obtained fairly and lawfully. Besides, what 'Dutchness' shall mean in the context of PROGIS, the fact that a migrant being 'non-Dutch' has to be enrolled more often than a Dutch citizen challenges the prohibition of discrimination as set by Article 14 of the European Convention on Human Rights and by Article 21 of the Charter on Fundamental Rights of the EU.

5.1.2. *False negatives during verifications*

5.1.2.1. . . . using the INS console. The case highlighted in Section 3.1 of a female asylum seeker is not unique, but occurs relatively frequently within the Dutch immigration system. Since the accuracy rate of the INS console is 79% (Ministerie van Veiligheid en Jusititie, 2014) this means that in 21% of the cases, the INS console would categorise an asylum seeker as posing a risk of identity fraud. Article 6(e) of Directive 95/46/EC and Article 5 of the new GDPR both specify that personal data 'must be kept in a form which permits identification of a data subject'. Yet, Directive 95/46/EC has no requirements as to how this 'form' shall be achieved, or how the data are to be obtained, only that the data have to be processed fairly and lawfully. Neither does it state what conditions apply if persons (in our case, asylum seekers) are confronted of being framed as potential identity fraudsters just because their fingerprints cannot be verified. Article 6(e) of the new GDPR is very clear that data processing shall be 'necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller'. This purpose in the case of identification by the INS console is of course beyond doubt. When the Regulation takes effect and cases similar to the false negatives generated during identification processing of asylum seekers using the INS console emerge, Article 33 of the GDPR lays down a potential legal

remedy. It prescribes for data controllers to carry out data protection impact assessments, if the introduction of a high technology system and its purpose is '*likely to result in a high risk for the rights and freedoms of individuals, such as discrimination, identity theft or fraud*'. Moreover, if the new Regulation was in force, the additional requirements regarding female asylum seekers (see Section 3.1) to produce 'verifiable' fingerprints could have also been assessed against Article 5 of the GDPR. The latter sets out that the processing of data shall be made transparent for the data subject.

Both migrants and the new data protection regulation could furthermore profit from provisions of the ECHR – Article 8 on the right to a private life, and Article 14 on the '*prohibition of discrimination amongst others on grounds of race, ethnic origin, genetic features and religion*'. In addition, relevant ECtHR case law can provide a useful remedy. The Schengen Border Code could also be of help, as this prohibits discrimination by immigration and border control authorities throughout the EU. Consultation of these legal documents is essential, as the INS console can clearly frame an asylum seeker who is regarded being 'at risk' as someone who poses 'a risk' (of identity fraud). Consequently, such a digitally mediated framing and categorisation can relatively easily put the legal status of an asylum seeker in jeopardy.

5.1.2.2. . . . using the PROGIS console. During identity verification processes using the PROGIS console, false negative rates are also around 21% (Ministerie van Veiligheid en Jusititie, 2014). Given that only suspects, criminals (and deceased victims) are registered, all (living) persons identified via PROGIS are regarded being 'as a risk'. Apart from the crime that usually frames and categorises a person within law enforcement as being a risk for society, the high sensitivity of the PROGIS fingerprint reader can also lead to frame someone as posing a(n additional) risk: identity fraud.

> *Imagine that a man is accused of a crime a month later and he has no ID on him than we consult this database (CJCD). If he is known, than there is a possibility for verification on the PROGIS console and we will identify him through two of his fingers. If he is identified then the criminal justice chain number is used, because according to the database he is the person he says he is. The database then displays additional information about him. Subsequently, two fingers are placed separately on the reader. This will check where the digital fingerprints are registered. If the fingerprints match, then that is displayed. In case there is no match then a red cross appears. In such a case, either there is something wrong with the fingerprints, which could be the case at that moment, or we identify the person a second time using two other fingerprints. If the fingerprints are rejected again, then this man will be accused of having given a false name. (PROGIS operating police officer, city D)*

The 2008 Framework Decision on Policing does not deal with issues related to the quality of data or how that data have been obtained. Therefore, it cannot provide a remedy for when a migrant is accused of identity fraud due to non-verifiable fingerprints. The Police and Criminal Justice Directive, however, specifies in Article 6 the principles for data accuracy and reliability, and in Article 7 the provisions for the lawfulness of data processing. After the Directive comes into effect, these provisions could provide a legal remedy against unjust, digitally mediated accusations against anyone. Such accusations can be regarded as an infringement on one's right to privacy as set by Article 8 ECHR, and one's right not to be discriminated against as set by Article 14 ECHR. For asylum seekers, ECHR case law on the right to asylum can also provide assistance.

5.1.3. *False positives via API profiles*

When the criteria in the API profiles are set up and risk profiles are used, false positive results for passengers are unfortunately a common occurrence (Hoogstrate and Veenman, 2012). Consequently, unnecessary detention of passengers regularly occurs as this has also been demonstrated in Section 3.3 by the empirical example on API.

Whereas the purposes for installing the API system and risk profiles are covered by EU and national laws, there is no legal permission for producing false positives and for stopping and interrogating persons just because their personal characteristics match a risk profile. Hence, any passenger wrongly detained could ask for a proportionality check from a border guard. This principle is laid down by Article 3 of the Framework Decision and if similar cases occur in the future, after the Police and Criminal Justice Data Protection Directive comes into force, Article 4(a) relating to fair and lawful processing, and also Article 7 on conditions for lawful processing also provide remedies. Furthermore, wrongly detained (accused) persons could also seek a remedy through their fundamental right to a private life as set by Article 8 of the ECHR, and through their right not to be discriminated against as laid down by Article 14 of the ECHR.

Cases of 'ad-hoc' detention using the API system are also on the increase:

> *Airlines are obliged to supply data for API. We put together what they need to deliver [. . .] This data comes to us in a system and in that system we build in such items as watch lists. [. . .] In fact, a watch list means that you search with known information for known persons. [. . .] In addition, manual assessment or operational analysis also takes place. Basically a trained border guard officer assesses the information on the complete passenger list with his own eyes. He looks at the list of a flight from China, and on that flight from China there are three Nigerians. That might be illogical on that route. This could require some extra attention paid to that flight. This will then be a filter for that particular flight, but will not become an additional profile on other flights. This simply exemplifies how a filter can be applied because certain people became interesting and merit further investigation. The use of such filters is much more in the direction, for example, of preventing terrorism, or things like that. Because you always look for unknown data on unknown persons: someone who, for whatever reason, is simply conspicuous. (Royal Military Police officer, city A)*

Although the aims of the API system are legitimate and founded in both EU and national laws, 'ad-hoc' detention of passengers referred to in the above two quotes could be assessed from the perspective of Article 3 of the Framework Decision. This provision prescribes that during data collection, principles of lawfulness, proportionality and legitimate

purpose shall be defined prior to the collection. As the quoted example and also other criticisms (Van Brakel and De Hert, 2011) demonstrate, police forces often rely on their gut instincts when identifying suspicious citizens, in the above case, selecting 'conspicuous' passengers. Such ad-hoc selections however challenge the principles of proportionality and also question the extent to which the prescriptions of lawfulness, proportionality and legitimate purpose, as set out in Article 3 of the Framework Decision, are enforced. The extent to which an ad-hoc selection, which aims to filter out terrorists or serious criminals, can be regarded necessary and proportionate in a democratic society is highly contentious. In a recent letter to the Dutch government, the Meijers Committee[43] underlined the need to assess whether the API system achieves its purpose. The Committee strongly questioned the necessity and proportionality of introducing any filtering activity on passenger data for the purposes of fighting international terrorism and serious crime (Meijers Committee, 2011). These principles are also enshrined by the new Police and Criminal Justice Data Protection Directive, and therefore in future cases the Directive can also be consulted. The implications of 'ad-hoc' detention on passengers' fundamental right to a private life as laid down by Article 8 of ECHR would also be worth assessing. Stopping regular travellers can easily frame travellers as posing a risk. In cases of false accusations, Article 8 can provide a broader scope for protection than either the existing or the drafted data protection rules.

5.2. *Interim conclusion*

Unintended, discriminative consequences are inherent in socio-technical practices (Prins, Broeders, Griffioen, Keizer, and Keymolen, 2011). The above section also demonstrates that such discriminative consequences are also inherent in the use of the INS and PROGIS consoles and the API system.

Despite the quite different legal, organisational and administrative settings in which these three technologies are embedded, empirical examples demonstrate how a migrant subjected to digital identification and verification practices via the INS or PROGIS consoles, and to risk monitoring practices via the API system are very much prone to be framed 'as a risk' (on this, see also La Fors-Owczynik and Van der Ploeg, 2015) or be viewed as a 'misfit'. This is quite worrying, especially because generating data using these systems has become extremely simple. Both the threshold for achieving high quality in biometric identification and the extensive and easily variable markers, for instance, in API risk profiles have meant an exponential growth in cases of false positives and false negatives occurring. Consequently, occurrences of false accusations of immigrants and travellers will become more frequent in the future. If we put this into perspective, currently one out of every five persons can already be falsely accused using INS or PROGIS consoles because good data quality in these systems is measured at 79%. Thus, the greater the risk categories become, the easier is to frame someone being risky. Another aspect of the problem relates to the fact that in a time where big data increasingly became common resource, to find and erase data that have led to wrongful accusations would be extremely labour-intensive and complicated, and at times even impossible to accomplish. The implications of such accusations and the existence of wrongful data is unpredictable; therefore it is better explored, for instance, through scenario-building by the new data protection regime. Article 33 of the GDPR could inspire a legal practice that is more directed towards the implications of technologies.

The issues raised call for new forms of data protection. In comparison to the relevant, already existing data protection rights and principles, the potential of the new GDPR and Police and Criminal Justice Data Protection Directive has been assessed. First, in light of empirical details, the question of data accuracy and reliability has proved to be a recurring issue in all cases. The new GDPR in its Article 5(d) and the Police and Criminal Justice Data Protection Directive in its Article 6 provide significantly improved safeguards with respect to data quality.

Second, in all cases where migrants' lives are adversely affected, the principles relating to the lawfulness of data processing in the new data protection regime provide more extensive safeguards than in the already existing legislation. Article 5(a) of the GDPR and Article 7 of the Police and Criminal Justice Data Protection regime prescribe a wide set of principles for the lawfulness of data processing. Given that the existing Framework Decision applies only to cross-border data processing, the prescriptions of the new data protection regulations provide a far more encompassing legal remedy. By the time the GDPR comes into force, the prescription to carry out data protection impact assessment (Article 33) prior to the introduction of technologies could help to prevent or limit the recurrence of wrongful, digitally mediated accusations of migrants.

Third, the proportionality principle is also enshrined in the current data protection regime (see Article 13 of the 95/46/EC and Article 17 of the Framework Decision). However, the new data protection rules, when ratified, will enforce this principle and the subsidiarity principle more thoroughly than current provisions. Given that these principles are also human rights principles, their improved enforcement within the new data protection regime can be seen as a win–win situation also for those migrants adversely affected by the Dutch government's use of technology.

6. Discussion: what can data protection and human rights regulations do for migrants framed digitally as a 'risk'?

> *The enjoyment of any right set forth by law shall be secured without discrimination on any ground such as sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or other status. No one shall be discriminated against by any public authority on any ground such as those mentioned in paragraph. (Protocol No. 12 to the Convention for the Protection of Human Rights and Fundamental Freedoms)*

The Netherlands ratified the European Convention on Human Rights in 1954. In addition, in 2005, the Netherlands also ratified Protocol No. 12 to the Convention for the

[43] Meijers Committee: a Dutch standing committee of experts on international immigration, refugee and criminal law – <http://commissie-meijers.nl>.

Protection of Human Rights and Fundamental Freedoms, which is an anti-discrimination treaty. Article 21 of the Treaty on the Functioning of the European Union also clearly prohibits discriminative practices. Based on all these instruments, the new data protection regime will have great potential in offering remedies against government practices that have discriminative and other privacy-invasive effects on migrants in the Netherlands.

The above analysis has however shown, first, that despite the advantages of digital systems in government use, the fundamental right to privacy and the right not to be discriminated against are at times put under pressure. Monitoring practices of migrants by the INS and PROGIS consoles and the API system can by default make certain innocent immigrants be viewed as a 'misfit', 'as a risk' for the society of the hosting country. The current data protection regime has been shown to provide unsatisfactory protection when it comes to such negative effects as a consequence of the use of these three systems.

Second, empirical insight sheds light onto an important deficiency of the new data protection regime, as mentioned in Section 2.4. The new regime allows for the blurring of boundaries between the definitions of the fundamental right to data protection and the fundamental right to privacy. Notably, the regulation (still) 'translates' (Latour, 1987) broader problems of privacy into issues of data protection. Such an approach leaves only limited room for discussion on other fundamental values related to privacy such as non-discrimination and autonomy, or on the enforcement of democratic principles such as proportionality. This is also evident in how the enforcement of the right to privacy tends to be evaluated. In practice, as far as data protection rules are concerned, this often implies that the right to privacy is enforced. Privacy impact assessments (PIAs) exemplify this (La Fors-Owczynik, 2015). PIAs are intended to assess implications on the fundamental right to privacy, yet what they in fact evaluate are implications on the right to data protection, when dealing with the processing of data. The fact that PIAs are rather focusing on data protection issues than on various aspects of privacy has also been raised by other scholars (Milaj, 2015; Wright, 2012; Wright and De Hert, 2012).

Because the definition of the right to privacy in the ECHR is much broader than many of the definitions set by data protection rules, complementing data protection assessments by evaluation against Article 8 of the ECHR can provide a very useful remedy for migrants who are subject to the unpredictable privacy implications of systems such as the INS and PROGIS consoles or the API system. Complementing data protection assessments with human rights evaluations is much needed, especially for immigrants, who have a more vulnerable legal position than regular citizens. These legal tools have the potential to clear migrants who have been falsely accused. Moreover, they can allow migrants to be regarded being 'at risk' (e.g., an asylum seeker can be regarded being 'at risk') or simply not being viewed as posing a threat (e.g., a traveller matching a risk profile is not necessarily a criminal).

A third issue concerns the potential long-term implication of false risk profiles on migrants' lives. Time limits for retaining data on migrants vary, depending on whether the data derive from INS consoles (10 years), PROGIS consoles (5 years) and especially from the API system (retention rules set different limitations of 24 hours, a month or a number of years, depending on the purpose of retention). Although prescriptions concerning the erasure of false data in the new data protection regulation are strict, it is essential to provide the data subject with transparency as to how long the false data are retained and when, where and how such data can be erased, especially in light of a recent ECJ judgement. The European Court of Justice (2014) rendered the EU Data Retention Directive 2006/24/EC invalid and argued that the retention of massive amounts of commercial communications data and the possibility for law enforcement authorities to access the data seriously interferes with such fundamental rights as the right to data protection and the right to privacy of citizens. Although in the case of the INS and PROGIS consoles and the API system, the amount of data involved is not extensive, caution shall be taken as the downside of using these technologies puts not only the privacy, but also the autonomy of immigrants and travellers under pressure.

For professionals and policy makers to stress the importance of privacy and autonomy to citizens – in this case to migrants – and take account of these concepts in their broad, human rights-oriented sense requires them to reflect upon what the pitfalls of using these technologies can be. Breaking with schemes in which virtual data are regularly separated from the actual person is a prerequisite to developing such a reflective approach. As the empirical examples have also shown, virtual data and the actual person are constitutive of each other and this becomes clear when looking at the implications of these technologies.

To conclude, the insights gained by this analysis were intended to prompt greater awareness of the new data protection rules and the potential of the European Convention on Human Rights for practitioners using such and similar identification and risk profiling systems internationally as those evaluated in this article. This analysis advocates the reopening of political and public debate within the Netherlands and the EU as to what degree of false positives during risk assessment practices and false negatives during identity verification practices can be regarded as 'necessary in a democratic society'. Such discussion should evaluate whether the price we pay, for instance, for framing immigrants and regular travellers digitally 'as a risk' does not lead to the slow erosion of such fundamental principles as proportionality, subsidiarity and even such democratic values held high in Europe as liberty and equality.

Acknowledgements

This article is based on research conducted during the DigIDeas project. Funding for this project was granted to Dr. Irma van der Ploeg by the European Research Council under the European Union's Seventh Framework Programme (FP7 2007–2013)/ Grant No. 201853/. Prof. Corien Prins has provided great support and very insightful comments on this article, for this I am particularly grateful for her.

REFERENCES

Ajana B. Recombinant identities: biometrics and narrative bioethics. *J Bioeth Inq* 2010;7(2):237–58.

Akrich M. The de-scription of technical objects. In: Bijker W, Law J, editors. *Shaping technology/building society: studies in sociotechnical change*. Cambridge, MA: MIT Press; 1992. p. 205–24.
Amoore L. Biometric borders: governing mobilities in the war on terror. *Polit Geogr* 2006;25:336–51.
Amoore L. Algorithmic war: everyday geographies of the war on terror. *Antipode* 2009;41:49–69.
Aradau C, van Munster R. (2005). Governing terrorism and the (non-) politics of risk. Political Science Publications, University of Southern Denmark, (11).
Aradau C, van Munster R. Insuring terrorism, assuring subjects, ensuring normality: the politics of risk after 9/11. *Alternatives/Boulder*. 2008;33(2):191–210. <http://doi.org/10.1177/030437540803300205>.
Besluit identiteitsvaststelling verdachten en veroordeelden (2009), <http://wetten.overheid.nl/BWBR0026302/geldigheidsdatum_21-09-2015>.
Besluit van 21 januari 2014 tot wijziging van het Vreemdelingenbesluit 2000 In verband met de uitbreiding van het gebruik van biometrische kenmerken in de vreemdelingenketen in verband met het verbeteren van de identiteitsvaststelling van de vreemdeling (2014) [accessed 22.02.11].
Bigo D. (2013). When Montesquieu goes transnational: the Roma as an excuse, visas as preventive logic, judges as sites of resistance. In: D Bigo, S Carrera, & E Guild editors. *Foreigners, refugees or minorities? Rethinking people in the contexts of border controls and visas*.
Bowker GC, Leigh Star S. *Sorting things out classification and its consequences*. Cambridge (US), London (UK): MIT Press; 1999.
Broeders D. (2009). *Breaking down anonymity. Digital surveillance on irregular migrants in Germany and the Netherlands*. Erasmus University of Rotterdam.
Caplan J, Torpey J, editors. *Documenting individual identity: the development of state practices in the modern world*. Princeton, NJ: Princeton University Press; 2001.
Ceyhan A. Technologization of security: management of uncertainty and risk in the age of biometrics. *Surveill Stud* 2008;5(2):102–23.
Clark R. Human identification in information systems: management challenges and public policy issues. *Inf Technol People* 1994;7(4):6–37.
Council of the European Union. Council directive 2004/82/EC on the obligation of carriers to communicate passenger data. *OJEU* 2004;6(1):24–7.
Council Regulation (EC) No 2725/2000. Concerning the establishment of "Eurodac" for the comparison of fingerprints for the effective application of the Dublin Convention. *OJEU* 2000;*OJ L316*:1–10.
De Hert P, Sprokkereef A. *The use of privacy enhancing aspects of biometrics as a PET (privacy enhancing technology) in the Dutch private and semi-public domain ("Allientie Vitaal Bestuur" project)*. Tilburg: Tilburg Institute for Law and Technology; 2009.
De Vries K. Identity, profiling algorithms and a world of ambient intelligence. *Ethics Inf Technol* 2010;12(1):71–85. <http://doi.org/10.1007/s10676-009-9215-9>.
Dijstelbloem H, Broeders D. Border surveillance, mobility management and the shaping of non-publics in Europe. *Eur J Soc Theor* 2014;18(1):21–38. <http://doi.org/10.1177/1368431014534353>.
Dijstelbloem H, Meijer A, editors. *Migration and the new technological borders of Europe*. Basingstoke, UK: Palgrave Macmillan; 2011.
Dodge M, Kitchin R. *Codes of Life: Identification Codes and the Machine-Readable World; pp. 1–47*. London. Retrieved on 10th October 2010 from <http://www.casa.ucl.ac.uk/working_papers/paper82.pdf>; 2004 [accessed 10.10.10].
European Commission. (2011). *Communication from the Commission to the European Parliament and the Council "Smart Borders – options and the way ahead." Communication*, <http://ec.europa.eu/dgs/home-affairs/news/intro/docs/20111025/20111025-680_en.pdf>. [accessed 23.03.11].
European Commission. (2015). Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions The European Agenda on Security. Strasbourg, <http://ec.europa.eu/dgs/home-affairs/e-library/documents/basic-documents/docs/eu_agenda_on_security_en.pdf>. [accessed 14.10.15].
Foucault M. *Discipline and punish: the birth of the prison*. New York: Vintage; 1977 by A. S.
Germany presses for quota system for EU migrant distribution. (2015). *The Guardian*, <http://www.theguardian.com/world/2015/apr/29/germany-quota-system-eu-migrant-distribution>. [accessed 15.05.15].
Haggerty KD, Ericson RV. The surveillant assemblage. *Bri J Sociol* 2000;51(4):605–22.
Hildebrandt M. Defining profiling: a new type of knowledge? In: Hildebrandt M, Gutwirth S, editors. *Profiling the European citizen cross-disciplinary perspectives*. Berlin, Germany: Springer Science; 2008.
Hoogstrate AJ, Veenman CJ. *Informatiegestuurde grenscontrole Verkenning ten behoeve van het gebruik van selectieprofielen in het kader van grensbeheer*. Den Haag: Nederlands Forensich Instituut; 2012.
Inzet van Analytics bespaart douane kosten en brengt effectiviteit in grenscontrole. (2015), <http://www.business-analytics.biz/blogs/inzet-van-analytics-bespaart-douane-kosten-en-brengt-effectiviteit-in-grenscontrole/>. [accessed 14.07.15].
Kohnstamm J. (2012). *Advies op het ontwerpwijzigingsbesluit Vreemdelingenbesluit 2000*, <https://cbpweb.nl/sites/default/files/atoms/files/z2012-00458.pdf>. [accessed 05.04.13].
Korthals AH, Cohen MJ. Besluit van 23 november 2000 tot uitvoering van de Vreemdelingenwet 2000 (Vreemdelingenbesluit 2000). *Stb.* 2000;497:1–222.
La Fors-Owczynik K. Minor protection or major injustice? Children's rights and digital preventions directed at youth in the Dutch justice system. *Comput Law Secur Rev* 2015;31(5):651–67.
La Fors-Owczynik K, Van der Ploeg I. Migrants at/as risk: Identity verification and risk assessment technologies in The Netherlands. In: Van der Ploeg I, Pridmore J, editors. *Digitizing identities: doing identity in a networked world*. London: Routledge; 2015.
Latour B. *Science in action: how to follow scientists and engineers through society*. Cambridge, Massachusetts. Cambridge, MA: Harvard University Press; 1987.
Latour B. Where are the missing masses? The sociology of a few mundane artifacts. In: Bijker WE, Law J, editors. *Shaping Technology/Building Society: Studies in Sociotechnical Change*. Cambridge, Mass.: MIT Press; 1992 from: <http://www.bruno-latour.fr/sites/default/files/50-MISSING-MASSES-GB.pdf>; Retrieved on 13 May 2015.
Law J. Actor network theory and material semiotics. In: Turner BS, editor. *The New Blackwell Companion of Social Theory*. Hoboken, NJ: John Wiley and Sons Ltd; 2009.
Leers G. (2012). Kamerbrief over het gebruik van passagiergegevens in het grensbeheer, <http://www.rijksoverheid.nl/documenten-en-publicaties/kamerstukken/2012/03/12/kamerbrief-over-het-gebruik-van-passagiersgegevens-in-het-grensbeheer.html>. [accessed 03.03.13].
Lips M, Taylor M, Morgan J. *Identification practices in government: citizen surveillance and the quest for public service improvement*.

Rotterdam: Identity in the Information Society, Springer Netherlands; 2009.
Lyon D. *Surveillance as social sorting: privacy, risk and digital discrimination*. London: Routledge; 2002.
Lyon D. *Identifying citizens: ID cards as surveillance*. Cambridge (UK); Malden (USA): Polity Press; 2009.
Magnet SA. *When biometrics fail: gender, race, and the technology of identity*. Durham, NC: Duke University Press; 2011.
McNeil JB, Carafano JJ, Zuckerman J. (2011). *39 Terror Plots Foiled: Examining Counterterrorism's Success Stories* (Vol. 4999), <http://www.heritage.org/research/reports/2011/05/39-terror-plots-foiled-since-911-examining-counterterrorisms-success-stories>. [accessed 10.04.13].
Meijers Committee. (2011). *Brief betreffende "Richtlijn betreffende het gebruik van persoonsgegevens van passagiers voor het voorkomen, opsporen, onderzoeken en vervolgen van terroristische misdrijven en zware" criminaliteit*. Retrieved on 12th May 2015 from www.commissie-meijers.nl.
Milaj J. Privacy, surveillance, and the proportionality principle: the need for a method of assessing privacy implications of technologies used for surveillance. *Int Rev Law Com Technol* 2015;0869(November):1–16. <http://doi.org/10.1080/13600869.2015.1076993>.
Mininisterie van Veiligheid en Justitie. (2011). *Protocol identiteitsvaststelling (strafrechtsketen)*, <http://www.rijksoverheid.nl/documenten-en-publicaties/brochures/2011/12/22/protocol-identiteitsvaststelling.html>. [accessed 12.03.12].
Ministerie van Veiligheid en Justitie. (2011). Het Fundament Progis. (M. van V. en Justitie, Ed.).
Ministerie van Velighied en Jusitie. (2014). Aan de Voorzitter van de Tweede Kamer der Staten-Generaal Postbus 20018 2500 EA Den Haag Datum: 23 december 2011 Betreft: Camaraondersteuning MTV-controles.
Muller B. (Dis)qualified bodies: securitization, citizenship and 'identity management. *Citizensh Stud* 2004;8:279–94.
Politie: grondige identificatie voorkomt identiteitsfraude – Security.NL. (2012). Retrieved September 3, 2012, from <http://www.security.nl/artikel/42902/1/Politie:_grondige_identificatie_voorkomt_identiteitsfraude.html>.
Prins C, Broeders D, Griffioen H, Keizer A-G, Keymolen E. (2011). *iGovernment Synthesis of WRR Report 86*.
Prins JEJ. Privacy in geding: expliciteren, wegen en beperken van belangen. In: Groenhuijsen MS, Soeteman A, editors. *Recht in geding*. Boom Juridische Uitgevers; 2014. p. 51–9.
Regeringspartijen tegen Europees database vluchtgegevens. (2015). *Nos*, <http://nos.nl/artikel/2061690-regeringspartijen-tegen-europese-database-vluchtgegevens.html>. [accessed 27.10.12].
Regulation (EU) No 1052/2013 of the European Parliament and of the Council of 22 October 2013 establishing the European Border Surveillance System (Eurosur), OJEU (2013).
Rijksdienst. (2013). *Toetsmodel Privacy Impact Assessment (PIA)*, <https://www.rijksoverheid.nl/documenten/publicaties/2013/06/24/toetsmodel-privacy-impact-assessment-pia-rijksdienst>. [accessed 05.02.14].
Salter M. *The rights of passage: passports in international relations*. Colorado (US), London (UK): Lynne Rienner Publisher; 2003.
Salter M. Governmentalities of an airport: heterotopia and confession. *Int Polit Soc* 2007;1(1):49–66.
Schouten P. Security as controversy: reassembling security at Amsterdam Airport. *Secur Dialogue* 2014;45(1):23–42.
Schreuder E. (2014). *Privacy Impact Assessment (PIA) deelproject Justitiële Keteninformatisering "Risico" s en Privacy by Design bij de justitiële ketenberichten voor de Jeugdwet'*.
Schwartz PM. (2013). The EU-U.S. Privacy Collision: A Turn To Institutions and Procedures. *126 Harvard Law Review 1966*, 1966–2009.
Suchman L. Do categories have politics? The language/action perspective reconsidered. *Comput Support Coop Work* 1994;2:177–90.
Taylor M, Morgan J, Lips M. Information-intensive government and the layering and sorting of citizenship. *Public Money Manage* 2007;27(2):161–4.
Teveen F. (2013). *JBZ-Raad; Brief regering; Reactie op de brief van de Commissie Meijers van 24 januari 2013 over het EURODAC-voorstel*.
Tomesen WBM. (2012). *Advies over het Wetsvoorstel houdende wijziging van de Vreemdelingenwet 2000 en de Algemene Douanewet met het oog op het structureel verwerken van gegevens ten behoeve van het verbeteren van grenscontrole en het bestrijden van illegale immigratie alsmede*, <https://cbpweb.nl/sites/default/files/downloads/adv/z2012-00631.pdf>. [accessed 02.12.12].
Van Brakel R, De Hert P. Policing, surveillance and law in a pre-crime society: Understanding the consequences of technology based strategies. *Journal of Police Studies* 2011;3(20).
Van der Ploeg I. *The machine – readable body: essays on biometrics and the informatization of the body*. Maastricht: Shaker Publishing; 2005a.
Van der Ploeg I. (2005b). *The politics of biometric identification normative aspects of automated social categorization*.
Van der Ploeg I, Sprenkels I. Migration and the machine-readable body. In: Dijstelbloem H, Meijer A, editors. *Migration and the new technological borders of Europe*. Basingstoke, UK: Palgrave Macmillan; 2011. p. 68–104.
Wet Aanpak Fraude Toeslagen (2014), <https://www.eerstekamer.nl/wetsvoorstel/33754_wet_aanpak_fraude_toeslagen>. [accessed 05.05.15].
Wet modernmigratiebeleid (2013), <http://wetten.overheid.nl/BWBR0027930/geldigheidsdatum_10-09-2015>. [accessed 02.04.14].
Wet van 18 juli 2009 tot wijziging van het Wetboek van Strafvordering, het Wetboek van Strafrecht en enige andere wetten in verband met het verbeteren en versterken van de vaststelling van de identiteit van verdachten, veroordeelden en getuigen (2009).
Wilson D, Weber L. Surveillance, risk and preemption on the Australian border. *Surveill Soc* 2008;5(2):124–41. <http://library.queensu.ca/ojs/index.php/surveillance-and-society/article/view/3431>. [accessed 09.10].
Wright D. The state of the art in privacy impact assessment. *Comput Law Secur Rev* 2012;28(1):54–61. <http://doi.org/10.1016/j.clsr.2011.11.007>.
Wright D, De Hert P. Introduction to privacy impact assessment. In: Wright D, De Hert P, editors. *Privacy impact assessment*. Rotterdam: Springer Netherlands; 2012. p. 3–32.
Zedner L. Security, the state, the citizen: the changing architecture of crime control. *New Crim. L. Rev.*2010;13(2):379–403. <http://doi.org/10.1525/nclr.2010.13.2.379>.

Accepted and published in Information and Communications Technology Law, 2016, Vol. 25, No. 2 (pp. 71-95)

Thesis Chapter VII.

Prevention strategies, vulnerable positions and risking the 'identity trap': Digitalized risk assessments and their legal and socio-technical implications on children and migrants

Karolina La Fors-Owczynik

Abstract

At first sight, the prevention of abuse of children, anti-social behaviour of children or migrants' identity fraud or illegal entry are quite different objectives which require different professional skills and legislative background. Even the digital technologies introduced to boost the prevention of the above problems are quite different. However, this article, aims to show that the implications of the design and use of these systems cast quite similar 'risk shadows' on both children and migrants that can be conceived as an 'identity trap' risk. The aim of this article is therefore to look for similarities and acquire a better insight into the use and implications of digital tools within policy areas that focus on vulnerable groups in our society such as children and migrants. A second aim is to explore how the legal framework, in particular the new EU data protection regime soon to be formally adopted, can assist actors involved to remedy the negative implications on children and migrants' positions, which stem from the use of preventative identity management systems. In addition, the article also pursues possibilities of guiding professionals in becoming reflexive about the detrimental implications of digital technologies and testing the normative potential of the legal framework regarding the vulnerable position of children and migrants. For finding ways in which professionals can become more reflexive about the potential negative implications of preventative identity management technologies is critical in order to create a context that is much more than merely law on the books.

Keywords: prevention, children, migrants, vulnerability, data protection, human rights, risks

1. Introduction

> "*The issues that divide or unite people in society are settled not only in the institutions and practices of politics proper, but also, and less obviously, in tangible arrangements of steel and concrete, wires, and transistors, nuts and bolts.*"[1]

Langdon Winner came up with this provocative statement thirty five years ago. These lines also succinctly cover many salient points about the implications of the use of digital technologies today. The current use of the so-called preventative identity management technologies[2] is illustrative of this, for instance, within youth care, law enforcement, border control and immigration. Besides the good-willed intentions and protective purposes behind these tools, potential negative implications of these technologies on children's and migrants' lives are also evident. The objectives and implications of these systems differ significantly depending on their specific targeted groups, for example young people or migrants. However, at a more general level, important similarities in the implications of using such systems can be discerned.

The aim of this article is first to look for such similarities in order to acquire a better insight into the use and implications of digital tools within policy areas that focus on vulnerable groups in our society. A second aim is to explore how the legal framework, in particular the new EU General Data Protection Regulation[3] and the new EU Police and Criminal Justice Data Protection Directive[4] soon to be formally adopted, can assist actors involved to remedy the negative implications on children and migrants' positions which stem from the use of preventative identity management systems. Also, the following analyses aim to determine to what extent differences arise in the position of the individuals involved, given youth care is primarily a national policy domain, whereas immigration is addressed at EU level. Finally, the article pursues the possibilities of guiding professionals in becoming reflexive about the detrimental implications of digital technologies and testing the normative potential of the legal framework regarding the vulnerable position of children and migrants. For professionals to improve their legal awareness and become more reflexive about the potential negative implications of preventative identity management technologies is critical in creating a context that is much more than merely law on the books.

Given these aims, the following sections focus on identity management systems that are used for prevention in youth care, law enforcement, immigration and border control. First, the discussion will bring the commonalities between the systems used in these domains to the fore and assess the extent to which the legal framework properly addresses the implications of risk assessment technologies on the lives of children and migrants. The analysis also sheds light on how the combined context of technologies, laws, policy areas and issues emerging in professional practices influence and shape the ways in which children and migrants are regarded as being 'at risk' and increasingly 'as a risk.' These insights are helpful in assessing what conditions contribute to their vulnerable position and what kind of legal remedies could address the vulnerabilities.

Secondly, the analysis deals with the question of whether the legal framework reinforces or mitigates the vulnerable position of the individuals affected by the use of these systems. Subsequently the discussion investigates whether differences in the position of both groups emerge as a consequence of differing policy ambitions. Challenges within the area of immigration are primarily EU-wide concerns, whereas those in youth care are primarily addressed at national level. To research the

[1] Winner, L. 'Do artefacts have politics?' Daedalus, 109(1) (MIT Press, 1980) 128

[2] Identity management technologies (IDM) discussed in this article are technologies used for the registration and processing of personal data within citizen-state relations.

[3] General Data Protection Regulation, (COM)2015

[4] Police and Criminal Justice Data Protection Directive, COM(2012) 10

implications of preventative identity management technologies on those subjected to these systems in national policy domains, the systems used in The Netherlands are taken as an illustrative example.

Finally, in order to assess whether the normative potential of the legal framework can provide adequate remedy against the vulnerable position of children and migrants, the following analysis assesses and conceptualizes the validity of certain data protection and human rights principles. Here, insights into how identity management systems affect the lives of children and migrants in day-to-day life are used by way of illustration. These insights intend to further establish the need for a legal framework which is much more oriented toward the implications of preventative technology use on children and migrants and not primarily toward the purpose of such technologies. This also includes a final plea in this article for raising awareness and stimulating reflexivity amongst professionals regarding the potential side-effects and detrimental implications of using these systems on children and migrants and especially regarding the potential of the legal framework to address these effects.

2. Commonalities between migrants and children: identity management to ease their vulnerable positions?

The key reasons for the vulnerable position of children and migrants can be viewed in the dynamic changes their lives go through from being 'at the peripheries of citizenship' toward becoming full-fledged citizens. These changes involve their increase in knowledge, the phases in which they gain more legal entitlements, claiming a position within society and being no longer dependent on the aid, assistance as well as formal intervention of others. For instance, after passing a certain legal age limit, children can earn entitlements to vote, drive or use other services that adult citizens are already entitled to use. Migrants can become entitled to hold a residence permit in a host country only after passing exams and administrative immigration checks. Putting this *in-between* position of these groups against a background of a substantial reliance on digital risk evaluation procedures by governments is illustrative of a certain multifaceted concept of 'security.' This is characterized by the diverse modes within which both children and migrants are increasingly considered, identified and framed being either 'at risk' or 'as a risk' in The Netherlands[5] The connection between being 'at risk' and being perceived 'as a risk' constitutes a conceptual symmetry between these groups in the research that provides the foundation for this paper. The following two sections specify some forms of how this symmetry plays out through the ways in which risks are increasingly digitally mediated in relation to these groups. In this paper the notion of mediation is conceptualized as something encompassing technologies, laws, policies, professional practices and specifically both the rather purpose-oriented[6] perception of data protection rules as well as the more implication-oriented perception of human rights perspectives on modes of personal data processing. The notion of mediation allows better framing of how human rights perspectives can enrich data protection assessments regarding the technologies in question in this paper.

[5] La Fors-Owczynik, K., & Valkenburg, G. (2015). Risk identities: constructing actionable problems in Dutch youth. In I. Van der Ploeg & J. Pridmore (Eds.), *Digitizing Identities: Doing Identity in a Networked World*. New York: Routledge.
La Fors-Owczynik, K., & Van der Ploeg, I. (2015). Migrants at/as risk: Identity verification and risk assessment technologies in The Netherlands. In I. Van der Ploeg & J. Pridmore (Eds.), *Digitizing Identities: Doing Identity in a Networked World*. Routledge.

[6] The new data protection regime incorporates a handful of new principles that go beyond purpose-oriented data protection, such as privacy by design, privacy by default, data minimization. Yet, an era of Big Data and arising necessities for digitalized prevention in more and more policy areas to some extent undermine the practical enforcement of these more 'technological implication-oriented' principles.

2.1. Securing children, securing citizens: Digitalized risk evaluations in youth care

As mentioned in the Introduction, the situation in The Netherlands will be used by way of example in this article. An initial relevant observation here is that the Dutch policy domain of youth care increasingly shapes and is shaped by public safety. This inter-relationship has become technically enabled by recently introduced systems to secure children in the first place and indirectly also to secure citizens. A series of dramatic cases, e.g. the tragic death of Savanna,[7] stirred particular interest in concerns about children being 'at risk.' In this case, youth healthcare workers and other agencies involved with the 3 year old girl were blamed for not having shared data on the child adequately, and if they had done so the fatality could have been prevented. Not only this dramatic event, but also various other examples of child abuse and anti-social behaviour towards children were translated in the political debate that followed into problems of information-sharing, for the prevention of which digital information sharing systems were seen as important facilitators.

The first of these systems is the Digital Youth Healthcare Registry (hereinafter, DYHR). DYHR is an information management system for the registration and processing of children's data within the youth healthcare sector. The second system, the so-called Reference Index High Risk Youth (hereinafter, RI), is a risk-profiling, public safety system connected to a large variety of Dutch youth care institutions that is introduced for evaluating risks against youths. The third system is a preventative system of the Dutch police, called ProKid 12- SI (hereinafter, ProKid), which is aimed at scoring children and their direct living environment against a set of risk categories. The established connections and overlapping concerns between policy domains of youth healthcare, youth care and public safety are visible in the convergence of these three initiatives. Through the combined use of the DYHR, the RI and ProKid, risks are projected for all children nationwide, and these children become understood in light of these risks. There is an overlap in function between the DYHR and the RI. In the RI, risk signals are sent in from other, linked technological registration systems youth care institutions. The DYHR's section of risk registration is connected to the RI and upon registration, risk signals are automatically sent from the DYHR to the RI. Information based on ProKid risk signaling by the police is shared manually with youth care workers. The three means of technology-based intervention and the means for mediation within the processes of prevention are graphically depicted in Figure 1.

'Gezinsvoogd Savanna vervolgd' - [7] http://www.nu.nl/algemeen/911116/gezinsvoogd-savanna-vervolgd-video.html

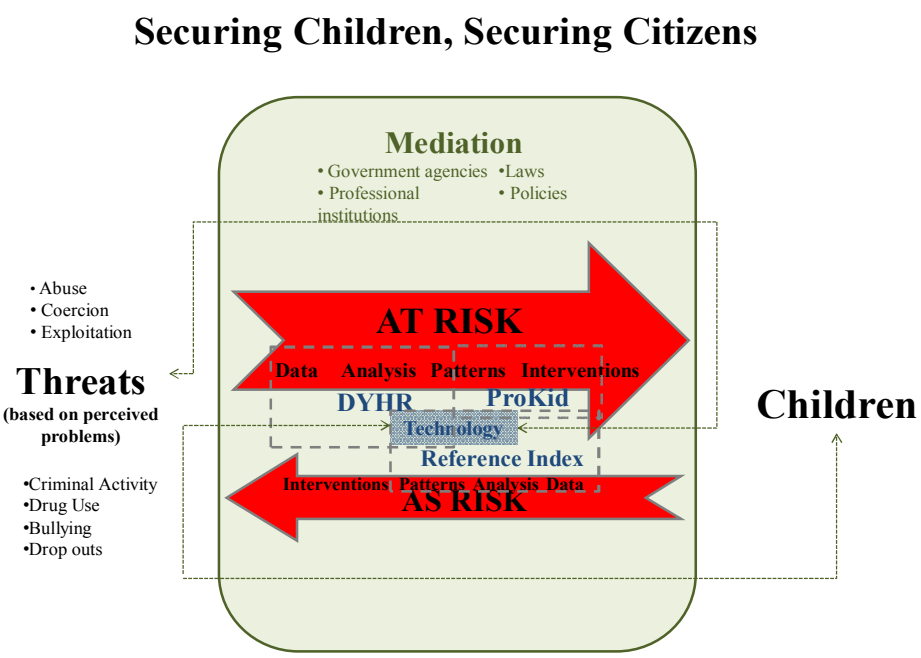

Figure 1.

On the far left of Figure 1, the threats children face or the threats that children may cause are intertwined with what it means to be 'at risk' or 'as a risk.' These are intimately connected with extensive media attention, specifically in relation to child abuse cases and instances of criminal activity performed by children. As the Figure demonstrates, children are largely considered being 'at risk' because they are seen as vulnerable to persons who may have hostile intentions towards them. To a lesser extent children are also perceived 'as a risk' based on their potential involvement in criminal activities, drug use, bullying or dropping out of school. The section on mediation demonstrates the means by which the government agencies and other organizations engage with prevention practices in The Netherlands. The mediation involves, for instance, personal data gathering on threats; and data analysis by youth healthcare, care and police professionals using the DYHR, the RI or ProKid. The manner in which certain problems are framed is significant for children's lives, since these problems become referential to the type of intervention process that will be imposed on them. The extent to which the notions of being 'at risk' and 'as a risk' are interrelated within the digital arrangements of the DYHR, the RI and ProKid have been demonstrated in earlier work[8]. Furthermore, in the abovementioned work the ways in which 'risks' - in various forms of negative implications on children's lives - can emerge from digitalized mechanisms of prevention have also been shown. The extent to which the current as well as upcoming personal data and fundamental children's rights instruments can provide adequate normative protection from the pitfalls of digitalized risk assessment by the DYHR, the RI and ProKid have also been analysed earlier[9]. Pitfalls demonstrated in this analysis involve, first, that the same colour-code is used for victims, witnesses and perpetrators which thus blurs boundaries between these categories in

[8] La Fors-Owczynik, K., & Valkenburg, G. (2015). Risk identities: constructing actionable problems in Dutch youth. In I. Van der Ploeg & J. Pridmore (Eds.), *Digitizing Identities: Doing Identity in a Networked World*. New York: Routledge.
[9] *Ibid,* and K. La Fors-Owczynik 'Profiling anomalies and the anomalies of profiling: Digitalized risk assessments on Dutch youth and the new European data protection regime' In R. Leenes, N. Purtova, & S. Adams (Eds.), *Under Observation: The Interplay between eHealth and surveillance.* (Springer Netherlands, 2016, forthcoming).

ProKid[10]. Secondly, relations between children their relatives, friends and animals are rendered available for risk evaluation in ProKid, meaning that not only the privacy of individual children is at stake, but also all others related to them. Thirdly, inherent in the *modus operandi* of the DYHR is that 'good deeds' and positive developments are not registered and thus not used in the analyses. The system merely focuses on risks concerning children. Moreover, potential negative effects on children's lives also emerge from the obscurity of the decision making process by professionals with respect to what can lead up to a 'simple' digital flag and to the difficulty for professionals in deciding whether or not to register issues under the banner of risk[11]. Fourthly, insights into the practices using the DYHR, the RI and ProKid have also shown that the ease by which information can be shared among professionals by the help of these systems results in extremely lengthy and labour-intensive procedures to deal with incorrect data on risks, which can consequently have long-term stigmatizing effects.

2.2. Securing Citizens, Securing Migrants: Identification and risk profiling of migrants[12]

The current political discourse within The Netherlands and the EU concerning migration, and the unprecedented flow of migrants in particular, shows both positivism and willingness to help the crowds of immigrants fleeing injustice, but also confusion. In a recent report of Human Rights Watch[13] on the developments concerning immigration to Europe in the previous year it has even been pointed out that: "The politics of fear led governments around the globe to roll back human rights during 2015." Beyond these large, very important political and democracy affecting questions, the digital identification and risk profiling practices present less visible issues that can have detrimental implications on migrants' lives as well as on the force of fundamental rights in a democratic society such as The Netherlands. When we look at the daily work involved in digital identification, verification and risk evaluation systems, we see that extensive standards embedded in digital systems in professional practice allow for spotting deviance among migrants earlier than among citizens who do not have to submit themselves to evaluation by these technologies. Threats such as identity fraud, illegal migration and related crime constitute problems for which digital identity management technologies are presented as the best answers. Consequently these threats are 'translated'[14] into digital forms of information-sharing[15].

Three technologies have been analysed in earlier research[16]. The first is the relatively recently introduced biometric identification system for immigrants, called the INS console within the Dutch immigration and border control sector. The second is the biometric identification system for suspects, criminals and (deceased) victims, called the PROGIS console within the Dutch law enforcement sector. The third system is the Advanced Passenger Information (hereinafter, API) system operated at Schiphol Airport by border control and immigration agencies in order to improve the sorting out of dangerous travellers by profiling them against a set of risk categories (API risk profiles).

---

[10] La Fors-Owczynik, K. 'Minor protection or major injustice? Children's rights and digital preventions directed at youth in the Dutch justice system' (2015) 31(5) Computer Law and Security Review, 651.

[11] *Ibid*.

[12] By the term *migrants* in this article, I refer both to immigrants and regular travellers who cross over the Dutch border or pass a check-point for Dutch immigration or law enforcement.

[13] Human Rights Watch, *World Report 2016* (New York, 2016)

[14] Latour, B., *Science in action: How to follow scientists and engineers through society*. (1st edn, Cambridge, Massachusetts: Harvard University Press, 1987)

[15] *Ibid* footnote 9. and
La Fors-Owczynik, K. 'Monitoring Migrants or Making Migrants "Misfit"? Data protoction and human rights perspectives on Dutch identity management practices regarding migrants' (2016) Computer Law and Security Review, doi:10.1016/j.clsr.2016.01.010

[16] *Ibid*. and see also references in footnote 4.

Upon entry into the EU, a first priority is to establish the status of immigrants (e.g. distinguishing asylum seekers from legal immigrants). This is done by means of the aforementioned systems by projecting risks of identity fraud and illegal migration on all immigrants within the context of the INS console. Within the context of the API system this is done by projecting these risks on all travellers passing through API check-points. The relationships between migrants being considered 'as a risk' and 'at risk' for the three IDM technologies and other means for mediation within the processes of prevention are graphically depicted below in Figure 2.

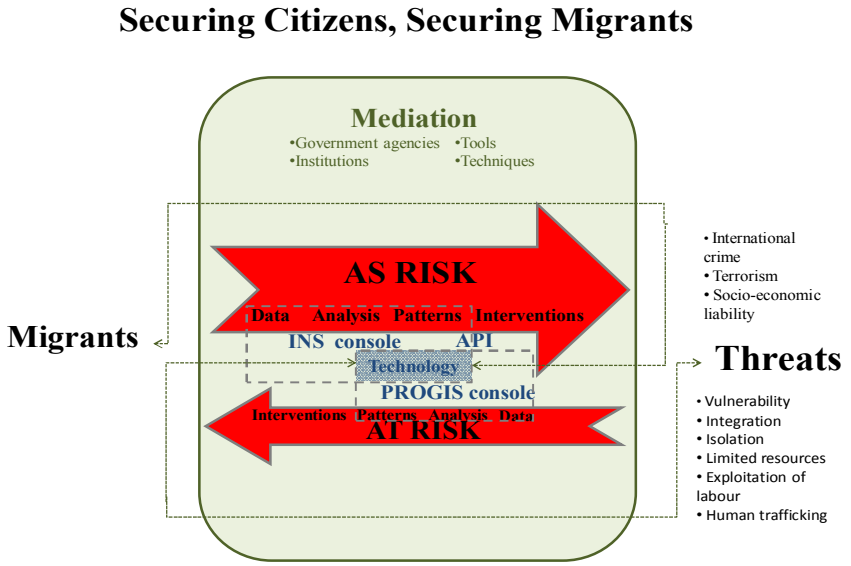

Figure 2.

On the far right of Figure 2, the threats faced by migrants or the threats that migrants are perceived to constitute, continuously shape and are shaped by what it means to be 'at risk' or 'as a risk.' The perception of who is regarded 'as a risk' is influenced by political intervention such as the recent comments by the EU Vice-President about 60% of all immigrants to the EU from last year having been economic migrants who need to be returned[17]. Furthermore, extensive media attention and the political rhetoric specifically in relation to terrorism and instances of criminal activity, such as the instances of assault against women in Cologne on New Year's Eve[18] also shape immigration policies throughout Europe. Yet, as Philip Zimbardo argues[19], the fear that terrorist attacks evoke conveys the message that all citizens in the threatened societies are vulnerable. As a reaction to these negative emotions, enemies have to be identified, rendered visible and even named. As Zimbardo infers, this can often lead to prejudice towards groups of society, including migrants[20] (the abovementioned Cologne attacks also exemplify this). Media information about the fact that, for instance, two immigrants who were involved in the attacks in Paris in November had been registered earlier as asylum seekers in Greece[21] lead to

[17] Euractiv.nl, European Commission: Schengen suspension could be extended, 60% of migrants should be sent back. (2016). Retrieved on 22 of January 2016 from http://www.euractiv.com/sections/global-europe/commission-schengen-suspension-could-be-extended-60-migrants-should-be-sent

[18] Connolly, K. (2016). 'Cologne inquiry into "coordinated" New Year's Eve sex attacks' *The Guardian*. (London, January 5th, 2016)

[19] Zimbardo, P. G. 'The Political Psychology of Terrorist Alarms' (2003), 1–7, available online: <http://zimbardo.com/downloads/2002%20Political%20Psychology%20of%20Terrorist%20Alarms.pdf>

[20] *Ibid.*

[21] Nos.nl, 'Twee zelfmoordterroristen waren geregistreerd in Griekenland'. (2015). Retrieved on 10th December 2015 from http://nos.nl/artikel/2070392-twee-zelfmoordterroristen-waren-geregistreerd-in-griekenland.html

reassuring Dutch media news with respect to having detected no signs of terrorism amongst asylum seekers to The Netherlands[22]. As Figure 2 depicts, evidence of certain migrants having been involved in terrorism allows for a picture that migrants can constitute a risk. Political rhetoric stresses that asylum seekers are indeed persons who need shelter because they are 'at risk' in their home country. The latter view of migrants is based on their vulnerability to human trafficking, exploitation of labour, integration problems, isolation, their limited financial resources and other conditions. Yet, in practice, identification and identity verification methods are strengthened and digital technologies only gain prominence in facilitating this[23]. The extent to which certain automatically enabled processes contribute to the construction of new risks, such as the false accusation of certain immigrants, has been demonstrated in earlier work[24]. This analysis demonstrated that the consequences of (too) sensitive biometric screening technologies and too wide variables for building a risk profile in the Advanced Passenger Information systems allow for false accusations of migrants. Furthermore, research based on empirical details assessed the data protection and human rights implications of the design and daily use of the INS and PROGIS consoles and the risk profiling system of API at Schiphol airport[25]. The analysis showed that the current legal framework is failing, and the proposed new data protection framework, although having greater potential, would also fall short of providing sufficient normative protection for migrants from the downsides of monitoring by these systems. Unintended implications of the use of these systems often contribute to frame migrants as 'misfits' in society even though they do not pose a risk or in more severe cases they would need the opposite: assistance and protection because they are 'at risk' of violence. False accusations of identity fraud can emerge as a consequence of mismatching fingerprints on the biometric reader of the INS and PROGIS consoles, and false perceptions of illegal migration can emerge because certain characteristics of a(n innocent) traveller match an API risk profile[26].

2.3. Interim conclusion

The previous two sections have shown that technologies as means by which government agencies engage in prevention practices, on the one hand frame children and migrants through the lens of constituting 'a risk,' and on the other hand, this framing can reinforce the vulnerability of both of these groups and can even put them into vulnerable positions. This constitutes a commonality between children and migrants that requires critical assessment. If the negative implications of using these technologies on the lives of these groups reinforces their vulnerable position then that can also frame a (less democratic) image of the society where the use of such technologies is seen as being 'fair,' 'acceptable' and 'necessary.' Furthermore, the previous two sections also demonstrated that commonalities between children and immigrants emerge not only based on their vulnerable position or potentially endangering attitude towards others. Such extremes could certainly also characterize regular citizens. But, it is far more their in-between status of becoming a full-fledged citizen but not yet being one legally that brings their first important commonality to the fore. For instance, a child whose digital record shows a risk of domestic abuse (in which the involvement of parents or guardians is implicit) and therefore he/she cannot rely on legal aid by his/her parents or guardians, or for instance an unenrolled asylum seeker who is practically without a status up until the token of his/her legality, a resident permit

[22] Nos.nl, 'Medewerkers asielzoekerscentra kunnen terrorisme herkennen'. (2015). Retrieved on 12th December 2015 from http://nos.nl/artikel/2059507-medewerkers-asielzoekerscentra-kunnen-terrorisme-herkennen.html
[23] EUObserver, Tusk: "Wave of migrants too big not to to be stopped." (2015). Retrieved on 2nd February 2016 from https://euobserver.com/migration/131363
[24] See footnote 4 and 14.
[25] La Fors-Owczynik, K. 'Monitoring Migrants or Making Migrants "Misfit"? Data protoction and human rights perspectives on Dutch identity management practices regarding migrants' (2016) Computer Law and Security Review, doi:10.1016/j.clsr.2016.01.010
[26] *Ibid.*

would have been issued, for these persons creates a vulnerable position in themselves. (To this position I refer later on in this section as an 'accountability vacuum.')

A second commonality is that both children and migrants are exposed to a broad variety of digital risk evaluation. Earlier research about children and digital risk assessment within youth care demonstrated that, despite the noble intentions behind digital systems, the digitalized risk categories use in these systems tend to reify risks[27]. The lengthier and more comprehensive the screening by digital risk categories and the quicker the 'risk' information exchange on a person, the higher the likelihood that the identity of a person - in our case of a child or migrant - becomes 'trapped' in a potential 'tunnel vision of risk' or a certain 'risk identity' provided by these assessments. Furthermore, the correction of false information is extremely lengthy and labor-intensive.

The fact that both children and migrants - although to differing degrees - are increasingly considered and identified being either 'at risk' or 'as a risk' in The Netherlands[28], from a legal perspective leads to a third commonality: they both need support to be held accountable for their deeds. Full-fledged citizens do not need that. Under the age of 18, children can be held accountable for their deeds only via their parents or guardians, and under the age of 12, children cannot be prosecuted according to Dutch law. Yet, given events of domestic violence or child abuse, all parents registered in ProKid, for instance, are also digitally codified and checked against standard risk categories for constituting potential threats to children. This has been demonstrated earlier through examples of the RI and ProKid. This digitally codified change in assessing all parents or guardians in practice as a potential actor with a negative influence on the development of children can also weaken the position of children themselves. By framing a parent or guardian as a potential threat to children results in a situation where children have no direct (legal) support in enhancing their accountability and to some extent also their rights. This is especially worrying when it comes to traumatized child victims. More or less the same applies to immigrants. They are also, in particular before and during the process of receiving their residence permit, in a weak position as a consequence of their status. Migrants have less legal support in terms of being accountable for their deeds and more importantly for the suspected deeds authorities of receiving states can confront them with, as compared to local citizens. This can be thought of as an 'accountability vacuum' regarding children and migrants. In practice, through the use of digital risk assessment systems, both groups are held more accountable for their deeds, for their potential deeds and often even for the deeds of their relatives, friends or traveling companions by government authorities, than regular citizens who are not subjected to such systems. This clearly constitutes a pressure. Stemming from this pressure, another commonality can be defined between the two categories. This commonality is that - because of their in-between position – those children and migrants in particular who are exposed to digital risk assessments have insufficient mechanisms to shape their position within society and often cannot stand up for their rights. From a legal perspective they are either dependent on their parents, or on an assigned lawyer in order to effectuate their rights. Hence, paradoxically this lack of practical autonomy in standing up for their rights renders them vulnerable and consequently more exposed and often regarded as being prone to 'problems' such as anti-social or delinquent behaviour, identity fraud or illegal entry.

Therefore, given the example of Dutch residence permits, they are currently established by highly sensitive biometric readers through the help of the mentioned INS consoles. The sensitive features in these consoles are than deemed to substantially increase trust with respect to the claimed

[27] La Fors-Owczynik, K., & Valkenburg, G. (2015). Risk identities: constructing actionable problems in Dutch youth. In I. Van der Ploeg & J. Pridmore (Eds.), *Digitizing Identities: Doing Identity in a Networked World*. New York: Routledge.
[28] See footnote 4.

identity of a person. The digitalized path for identification, including risk assessment against potential identity fraud, can in practice further jeopardize the legal position of immigrants in a hosting country. Because on the one hand, any mismatching of fingerprints frames disbelief in the claimed identity of an immigrant and on the other hand this also prompts a request for explanation and proof of their identity claim. Given that full-fledged citizens are not exposed to such practices and consequently do not end up in a position where they have to prove their identity, or worse, their innocence, both children[29] and migrants exposed to false accusations by these risk assessment systems can experience discrimination. Furthermore, detrimental implications can be what Schermer calls issues of "de-individualisation"[30], in other words that an individual who is accused of being a member of a certain group can personally suffer from the negative implications of the risk profile of the whole group. In a recent report to the Dutch government, researchers from the University Amsterdam warned about creating day-to-day situations in society, where some persons might feel they are treated unfairly or discriminated against, because this can trigger radical reactions[31]. Radical reactions are often coupled with a lack of belief in such basic democratic principles as liberty and equality and can undermine openness, mutual respect and the importance of and need for diversity in society. Therefore, to redress these principles and values by diminishing the vulnerable position that children and migrants can experience as a consequence of the pitfalls of identification and risk assessment practices is pivotal. In line with this, the next section looks into certain data protection and human rights principles and scenarios as potential counter measures against such vulnerability.

3. Data protection and human rights principles as counter measures against the vulnerability of children and migrants

The vulnerable position of children and migrants is often reinforced by the fact that these technologies are designed and used with a somewhat purpose-oriented stance and not with one that is primarily concerned with the implications of using these systems on the lives of those persons subjected to them. Given the pace of current technological developments (e.g. the rise of Big Data and Open Data) this is problematic in itself.

Preventative technologies or security enhancing technologies always have legitimate purposes in a democratic society, in other words if they infringe upon the right to privacy, that infringement is legitimized by law[32]. Despite this question of legitimacy, the design and introduction of such technologies in the majority of cases is never accompanied by a democratic legitimization process, such as the processes accompanying legislation. A legitimization process would optimally include an

[29] Bruning, M. R. et al.. *Kinderrechtenmonitor 2012 - Adviezen aan de Kinderombudsman* (2012) (De Kinderombudsman, Den Haag)

[30] Schermer, B. W. 'The limits of privacy in automated profiling and data mining' Computer Law and Security Review, (2011) *27*(1), 45

[31] Feedes, A. R., Nicholson, L., & Doosje, B. *Triggerfactoren in het radicaliseeringsproces.* (2015) (Expertise-unit Sociale Stabiliteit, Amsterdam University, Amsterdam)

[32] Article 29 Data Protection Working Party. *Opinion 03/2013 on purpose limitation.* (Commission of the European Union, 2013)

Bellanova, R., & De Hert, P. 'Le cas S. et Marper et les données personnelles : l'horloge de la stigmatisation stoppée par un arrêt européen'. (2009) 4(76) Cultures & Conflits, 101; *Handbook on European data protection law.* (Publication Office of the European Union, Luxembourg, 2014); Prins, J. E. J. 'Digital Diversity : Protecting Identities Instead of Individual Data' In L. Mommers & A. Schmidt (Eds.), *Het binnenste buiten: Liber amicorum ter gelegenheid van het emeritaat van prof. dr. Aernout Schmidt.* (eLaw Leiden, 2010)

evaluation of potential side-effects. On the other hand, the policies[33] and laws serving to legitimize these systems are also somewhat purpose-oriented. One of the main principles of the Data Protection Directive (95/46/EC), the 'purpose limitation' principle, also exemplifies this. This principle remains prominent in the new General Data Protection Regulation (hereinafter, GDPR). The text of the new GDPR had already been finalized in December 2015. In this section, I focus on the normative potential of the GDPR, more specifically on some of its most essential principles, such as the purpose limitation principle. Furthermore, I explore the validity of human rights principles that are relevant from the perspective of both the purposes and the implications of technologies. I investigate these legal instruments regarding whether they can provide sufficient counter measures to remedy the vulnerable position of these two groups or whether they reify their vulnerable position.

This is essential because governments, including in The Netherlands, are empowered by their citizens to maintain security, yet in their monopolistic positions government authorities often miss out on adequately redressing the downsides of preventative security measures. Even though the error rates of identification and risk assessment technologies on children – e.g. false alarms rates of child abuse[34]- and on migrants – e.g. false positives and false negatives[35] - are relatively high, counter measures to compensate those persons exposed to the negative implications of these systems are still scarce.

3.1. Purpose versus Implication?

3.1.1. The right to data protection and the right to privacy

By directing attention towards the vulnerability of children and migrants and the implications of preventative risk assessment systems on this vulnerability, the debate related to values of privacy versus security requires addressing. When doing so, particular attention will be given to two perspectives that are geared toward how legal prescriptions related to identity management technologies shall be enforced: either by focusing on the purpose(s) of technology or on the implication(s) of it.

The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (hereinafter, Convention 108) of the European Union as a pioneer legal instrument paved the way for implementing the protection of personal data in different legal frameworks and mechanisms in the EU. Through the introduction of Directive 95/46/EC, the right to data protection became implemented into secondary law within the EU. Later on, the Treaty of Amsterdam introduced data protection also into the EU's primary law by its Article 286. The Treaty of Lisbon (hereinafter, TFEU) also brought significant changes regarding data protection in the EU. It abolished the three pillar structure of the EU by which the direct relevance of EU legislation for national laws of member states became codified. Since then, Article 16 of the TFEU introduced the right to data protection as a fundamental right that also became a direct influence on national legislation. With the introduction of the TFEU, the right to data protection has also been strengthened because the Charter of the Fundamental Rights of the European Union came also into force, Article 8 of which codified the right to data protection as a fundamental right. On the road to establish data protection as a fundamental right of everyone in Europe, Directive 95/46/EC has been of great influence. To improve the enforcement of this right and also the right to privacy, among other things, the new data protection regime provides an up-dated, technology-informed set of new legal tools and measures.

---

[33] Identiteitsvaststelling in de strafrechtsketen: Wet en Protocol (2010). Ministerie van Justitie.

[34] Pronk, I. 'Het gezin is helemaal weg.' (2010) *Trouw,* Retrieved on 22nd January 2016 from http://www.trouw.nl/tr/nl/4324/Nieuws/article/detail/1583323/2010/02/09/Het-gezin-is-helemaal-weg.dhtml

[35] Hoogstrate, A. J., & Veenman, C. J. *Informatiegestuurde grenscontrole Verkenning ten behoeve van het gebruik van selectieprofielen in het kader van grensbeheer* (2012) (Nederlands Forensich Instituut, Den Haag)

The right to privacy and data protection are two separate fundamental rights (Article 8 of the Charter of the Fundamental Rights of the European Union), as the European Court of Justice also clarified in the case of *Osterreichischer Rundfunk*[36] by inferring that "data processing does not by definition fall within the scope of private life of Article 8 of ECHR." Privacy and data protection are, however, intertwined concepts especially if we look at the implications of monitoring technologies on citizens' lives. To remedy the often detrimental implications of such digital practices and to foster the enforcement of both the right to privacy and the right to data protection, the potential of data protection legislation should not be underestimated. Therefore, the next section explores whether a focus on the purpose of technology from a data protection perspective can strengthen the legal position of children and migrants exposed to preventative digital monitoring.

3.1.2. The purpose limitation principle and security

Purpose limitation

One of the cornerstones of the Data Protection Directive and also of the new Data Protection Regulation is the principle of purpose limitation. Given that the legal framework was initially meant to allow for the free flow of personal data and secondly meant to protect individual citizens[37], the purpose limitation principle has remained an "essential first step in applying data protection laws and designing data protection safeguards for any processing operation" ever since.[38] This had in particular been the case during the most recent, comprehensive data protection reforms. The purpose limitation principle is also a crucial pre-requisite for other principles such as transparency, fairness, lawfulness or legitimacy in data processing, therefore its effective enforcement is pivotal. Yet, criticism arose concerning loopholes in the new regulation[39] (De Hert & Papakonstantinou, 2012; Gonzalez Fuster, 2014). For instance, with respect to the purpose limitation principle, Ferretti criticized the new regulation for allowing data controllers far greater potential for justifying data processing than the earlier rules. Article 7(f) GDPR states that "processing is necessary for the purposes of legitimate interests pursued by the controller or a third party." Yet Ferretti argues that the "*current provision should be narrowly interpreted in light of the case law of the Court of Justice, so as to give effect to the Charter which provides that any limitation of the rights it contains must be provided for by law*"[40]. This criticism is especially relevant when it comes to preventative data aggregation regarding children within areas of youth care, law enforcement and regarding migrants within immigration and border control practices. The Article 29 Data Protection Working Party (hereinafter, WP) shared its concerns in relation to the future of the purpose limitation principle, especially at a time where the growing use of Big Data - including its use by government authorities - seems unstoppable. The WP expressed its concerns about the unfolding trend within which "the elasticity of purposes for which personal data are being collected" and the eagerness for "data maximization" provide significant risks both to the private life of citizens and the enforcement of data protection rules[41]. Nissenbaum even argues for the abolishment of 'old' data

[36] Joined cases C-465/00, C-139 & 139/01, *Osterreichischer Rundfunk and Others* [2003] ECR I-4989.

[37] Hijmans, H. *The European Union as a Constitutional Guardian of Internet Privacy and Data Protection : the Story of Article What the European Union does and should do to make Article 16.* (2016) (PhD thesis, University of Amsterdam, Free University of Brussels)

[38] The introduction of the ePrivacy Directive (2002/58/EC) also fostered this principle as it had set out that the processing of data should be "strictly proportionate" and "necessary in a democratic society."

[39] De Hert, P., & Papakonstantinou, V. 'The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals' (2012) 28(2) Computer Law & Security Review, 130; Gonzalez Fuster, G. *The Emergence of Personal Data Protection as a Fundamental Right of the EU* (Springer International Publishing, 2014)

[40] Ferretti, F. 'Data protection and the legitimate interests of data controllers: Much ado about nothing or a winter of rights?' (2014) 51(3) Common Market Law Review, 843

[41] Article 29 Data Protection Working Party *Opinion 02/2013 on apps and smart devices* (Commission of the European Union, 2013)

protection principles such as the purpose limitation principle[42]. She advocates data protection measures that would assess the contextual implications of digital technology use in relation to how technology use can reshape the context. For instance, how technology use can rearrange social norms that had earlier been regarded as part of the mutual respect for those sharing the relationship. Nissenbaum gives the example of information shared between a doctor and a patient being sold to a commercial company being a severe infringement of (the norms underlying the concept of) privacy in that context[43]. Aside from the legal challenges of attempting to frame and interpret privacy and data protection through contexts, the principle of purpose limitation will remain part of the current data protection regulation. Hildebrandt and De Vries argue however, that the purpose limitation principle, even in its new form in the regulation, has to be to give redress, for instance in the anticipated growth in function creep[44] cases in part stemming from the increase in use of Big Data and Open Data[45]. Moerel and Prins also advocate a reformative perspective on the purpose limitation principle. They argue that "*this principle is still relevant, but […] it should be tied in with the interest served rather than with the original purpose for data collection*"[46]. In this way they argue that a 'legitimate interest test' would much better suit how data should be processed in the age of Big Data rather than purely testing whether data has been collected and processed according to the pre-defined purpose(s): "*The time has come to recognise the legitimate interest ground as the main legal ground for each and every phase of the data lifecycle*"[47](Moerel & Prins, 2015).

However, the new data protection regulation with its broadened scope specifies that data processing shall be lawful and legitimate and consequently limits the purpose of data processing. For instance, *via* Article 23 it prescribes new principles that are also relevant for limiting the purpose of data processing. The principles of privacy by design and by default inscribe the de facto protection of a person's privacy into a fundamental pre-requisite of any data processing. Yet, Koops and Leenes critically point out the downsides of taking a strict 'code' view of these concepts. They argue for a perspective on 'privacy by design' and 'privacy by default' that much rather takes the form of 'communication strategies' than the form of strict 'codes'[48]. These would strengthen and also reform the purpose limitation principle and all in all achieve improved protection of personal data and privacy.

Security

Security as a goal and a value often presents a strong means of legitimization when it comes to violating the purpose limitation principle and the right to data protection and indirectly the right to privacy in general. This trade-off model is still the formula for balancing between these values. The fact that privacy is often framed as a trade-off against security can be traced back to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of the Council of Europe (also called Convention 108). The first legal instrument to protect individuals against the detrimental effects of data processing, this stated that "restrictions on the rights laid down in the Convention are only possible when overriding interests (e.g. state security, defence, etc.) are at stake." In legal scholarship, this trade-off between privacy and security is further reinforced: "restrictions on privacy

[42] Nissenbaum, H. 'Privacy as contextual integrity' (2004) 79 Washington Law Review 119
[43] *Ibid.*
[44] Function creep: when data gathered for one specific purpose is also used for other purposes not indicated originally.
[45] Hildebrandt, M., & De Vries, K. (Eds.). *Privacy, due process and the Computational Turn: the Philosophy of Law meets the Philosphy of Technology*. (1st edn, Routledge, 2013)
[46] Moerel, L., & Prins, C. 'On the death of purpose limitation' *Privacy Perspectives Where the Real Conversation in Privacy Happens* (2, June, 2015)
[47] *Ibid.*
[48] Koops, B.-J., & Leenes, R. 'Privacy regulation cannot be hardcoded. A critical comment on the "privacy by design" provision in data-protection law' (2014) 28(2) International Review of Law, Computer and Technology, 159

must be accepted provided this serves the purpose of security"[49]. However, citizens also desire security and expect that state authorities will protect them from threats. According to surveys, citizens are willing to give up their privacy and subject themselves to scrutinizing surveillance modes, such as security checks at airports or CCTV cameras in different public spaces, in order to increase their security. Despite the legal framework, notions of security are not by definition in opposition to notions of privacy. The fact that private interests can often equate to security interests is also demonstrated by ECtHR case law.[50] Yet, scandals of breaches of privacy rights (such as issues related to the revelation of Snowden and the NSA) shake up any balance between privacy and security and tend to undermine citizens' trust. As Hijmans and Kranenborg state: "the restoration of this trust is the most pressing challenge"[51]. A crucial element of difficulty in restoring this trust is what Koops points out concerning the new data protection regulation as "the fact that people have little over how their digital personae and data shadows are being treated"[52]. To tackle this challenge, a handful of cases that condemned signatory states of the European Convention on Human Rights for having breached the fundamental right to privacy of citizens are pivotal in attempting to restore such trust.[53] Such body of case law is also essential to complement and strengthen data protection regulations[54].

Yet, the vast amount of data that can be made available for algorithmic purposes presents new challenges and also shifts the perspective of a trade-off model between security and privacy to unknown territory. Scholars from different disciplines have criticized and pointed out the pitfalls of this opposition[55]. For instance, Solove argues that the 'zero-sum' game type of policy and legal stance taken regarding security and privacy forces a choice between these values and he furthermore asserts that "protecting privacy is not fatal to security measures"[56]. Furthermore, Valkenburg, from empirical details on body scanner use, shows that the purpose of security is in practice often achieved by a far more comprehensive infringement of the right to privacy of a traveller than anticipated within the processes legitimizing the purpose and use of these technologies[57]. Besides the more severe implications on the right to privacy in order to achieve the purpose of security, as Boyle and Haggerty assert, in practice these technologies are far from being silver bullets. They argue that many security officials believe that the potential for "zero risk is unattainable" given the vulnerabilities of security itself. This is also

[49] Hijmans, H., & Scirocco, A. 'Shortcomings in EU data protection in the third and the second pillars. Can the lisbon treaty be expected to help?' (2009) 45(6) Common Market Law Review, 1485

[50] ECtHR *Klass v. Germany*, No. 5029/71, 6 September 1978; ECtHR *Malone v. United Kingdom*, No. 8691/79, 2 August 1984; ECtHR *Leander v. Sweden*, No. 9248/81, 26 March 1987, ECtHR; *Gaskin v. United Kingdom*, No. 10454/83, 7 July 1989.

[51] Hijmans, H., & Kranenborg, H. (Eds.). *Data Protection anno 2014: How to Restore Trust? Contribution in honour of Peter Hustinx, European Data Protection Supervisor*. (1st edn, Intersentia, 2014).

[52] Koops, B. 'On decision transparency, or how to enhance data protection after the computational turn'. In M. Hildebrandt & K. De Vries (Eds.), *Privacy, Due Process and the Computational Turn* (Abingdon: Routledge, 2013)

[53] ECtHR *Niemietz v. Germany*, No. 13710/88, 16 December 1992; ECtHR *Halford v. United Kingdom*, No. 20605/92, 25 June 1997; ECtHR *Amann v. Switzerland*, No. 27798/95, 16 February 2000; ECtHR *Rotaru v. Romania*, No. 28341/95, 4 May 2000; ECtHR *Soro v. Estonia*, No. 22588/08, 16 September 2015.

[54] Hustinx, P. J.'EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation' *Collected Courses of the European University Institute's Academy of European Law*, *24*(January 2013), 1, Retrieved on the 22nd of January from https://secure.edps.europa.eu/EDPSWEB/edps/EDPS/Publications/SpeechArticle/SA2014

[55] Costa, L., & Poullet, Y. 'Privacy and the regulation of 2012.' (2012) 28(3) Computer Law & Security Review, 251; Milaj, J. 'Privacy, surveillance, and the proportionality principle: The need for a method of assessing privacy implications of technologies used for surveillance.' (2015) 8(69) International Review of Law, Computers & Technology, 1; Mironenko, O. Body scanners versus privacy and data protection. (2011) 27(3) Computer Law and Security Review, 232; Nissenbaum, H. 'Privacy as contextual integrity' (2004) 79 Washington Law Review 119; Prins, J. E. J. Digital Diversity : Protecting Identities Instead of Individual Data. In L. Mommers & A. Schmidt (Eds.), *Het binnenste buiten: Liber amicorum ter gelegenheid van het emeritaat van prof. dr. Aernout Schmidt*. (eLaw, Leiden, 2010); Schermer, B. W. 'The limits of privacy in automated profiling and data mining' (2011).27(1) Computer Law and Security Review, 45

[56] Solove, D. J. *Nothing to hide: The False Tradeoff between Privacy and Security*. (Yale University Press, 2011).

[57] Valkenburg, G. 'Privacy Versus Security: Problems and Possibilities of the Trade-Off Model' In. Gutwirth, S., Leenes, R.; De Hert, P. (Eds.) Reforming European Data Protection Law (Springer Science, 2015)

reflected by the fact that "security risks proliferate and exceed the capacity for officials to fully manage or even identify [persons]"[58] , and ultimately it "becomes a pressing challenge to maintain the appearance of absolute security"[59].

In light of the recent terrorist attacks and humanitarian crisis, answering the classical question of 'How much privacy shall be given up to gain how much security?' seems even more ill-judged than ever before. Mostly, because whereas surveillance methods geared toward forecasting and acting against 'particular types of individuals'[60] - also common in practice in Dutch youth care, law enforcement, immigration and border control - are advancing rapidly, there is little assessment of the actual outcome of these security practices. Ex ante assessment could put the trade-off model under critical scrutiny by asking, for instance, whether it was worth giving up 'that much' privacy for gaining 'that much' security. For instance, the data protection impact assessment requirement set out by Article 33 of the new GDPR could be inspirational. It demonstrates not only a stronger orientation towards exploring the implications of technology use on values such as privacy, but it does not frame this as being in opposition to security. Although conducting data processing for preventative or security purposes falls under the scope of the 2008 Police and Criminal Justice Directive and therefore Article 33 of GDPR is not applicable, this Article could still be inspirational for public authorities in processing citizens' data to evaluate the impact of these measures on both security and the privacy of citizens. Moreover, to evaluate whether there is any threat to society that justifies any security measure in the first place, the proportionality test of the European Court of Justice could also be used as a strong legal tool. Furthermore, as Hijmans points out: "*the absence of a connection between a threat to public security and the retention of data was an element in the ruling of the Court in* Digital Rights Ireland and Seitlinger *leading to the annulment of Directive 2006/24 on data retention.*"[61]

To conclude, the new data protection regime provides a far more comprehensive set of tools to enforce the right to data protection and privacy. However, as long as certain modes of reflection are not codified and institutionalized concerning the effectiveness of digital security measures, preventative digital technologies will remain widely used silver bullets to maximize security[62].

3.1.3. Remedying negative implications on privacy by enforcing data protection principles?

False accusation of migrants as a consequence of identity verification through the INS and PROGIS consoles often occurs, as the 79% accuracy rate of these systems indicates. Furthermore, examples of false positives in part stemming from the broadness of variables for building risk profiles show that the Advanced Passenger Information system can frame migrants 'as a risk' of committing identity fraud (La Fors-Owczynik, 2016).

---

[58] Boyle, P., Haggerty, K. 'Spectacular Security: Mega-Events and the Security Complex' International Political Sociology (2009) 3(3) 257 (263)

[59] *Ibid*.

[60] Van der Hof, S., & Prins, C. 'Personalisation and its Influence on Identities, Behaviour and Social Values' In *Profiling the European citizen Cross-disciplinary perspectives* (Springer Science, 2008)

[61] Hijmans, H. *The European Union as a Constitutional Guardian of Internet Privacy and Data Protection : the Story of Article What the European Union does and should do to make Article 16*. (2016) (PhD thesis, University of Amsterdam, Free University of Brussels) 105

[62] Amoore, L., & Hall, A. 'Border theatre: on the arts of security and resistance' (2010) 17(3) Cultural Geographies, 299; Broeders, D. *Breaking down anonymity. Digital surveillance on irregular migrants in Germany and the Netherlands*. (PhD thesis, Erasmus University of Rotterdam, 2009); Ceyhan, A. Technologization of Security : Management of Uncertainty and Risk in the Age of Biometrics. (2008) 5(2) Surveillance Studies, 102; Salter, M. 'Governmentalities of an Airport: Heterotopia and Confession' (2007) 1(1) International Political Sociology, 49; Thomas, R. (2005). 'Biometrics, International Migration and Human Rights' (2005) 7 European Journal of Migration and Law, 377; Van der Ploeg, I. 'Security in the Danger Zone: Normative Issues of Next Generation Biometrics' In E. Mordini & D. Tzovaras (Eds.), *Second generation biometrics: The ethical, legal and social context* (Springer, 2010)

Forecasting problems of anti-social behaviour towards children on the basis of 'deviant' parents or friends and on the basis that a child had already been a victim of abuse according to the ProKid system raises questions of children's rights (La Fors-Owczynik, 2015).

Furthermore, false reporting of child abuse cases by using such risk evaluation systems as the Digital Youth Healthcare Registry, the Reference Index High Risk Youth or ProKid are argued to have stigmatizing effects on children (Bruning, Van den Brink, de Jong – de Kruijf, Olthof, & Van der Zon, 2012). Various examples demonstrate that false reporting of child abuse cases can have devastating effects. According to certain victims, such reporting can put them into a highly vulnerable position and even render them "paranoid" about and "mistrusting" of the youth care institutions and risk registration systems to which these institutions are linked[63]. Yet, the director of a main organ responsible for the reporting of child abuse cases in The Netherlands, called Advice and Reporting Centre Child Abuse, admitted in an interview that, for instance, 10% of false positive reporting of child abuse cases should be regarded as the price we must pay for the 90% of cases when reporting was adequate and necessary[64]. All these instances would need a legal remedy and counseling to compensate those who were victims of false accusations by these systems and whose position became vulnerable as a consequence of using these systems.

When it comes to digital data exchange, the right to data protection and the right to privacy are two separate fundamental rights, and the implications of technology use on persons' lives are often not covered in their broadest sense within data protection regulations[65]. As De Hert and Gutwirth argue, this springs from the two main reasons behind the underlying rationale of the Directive – one being the achievement of an Internal Market, and the other being the enforcement of fundamental rights – so that in practice not human rights but rather economic interests prevail[66]. As they further infer, the introduction of the right to data protection can be regarded as remedying this deficiency in general. However, when it comes to mitigating the vulnerable position of children and migrants who are exposed to digitalized risk monitoring, ECtHR case law enforcing main principles of the data protection regulation in its broad human rights-oriented sense can be viewed as more useful in offering more specific, practical and also technical legal aid.

Data protection principles as fundamental values

The immense growth in digitalization within all aspects of citizens' lives in the past 25 years has provided an urge for new data protection prescriptions. An important event within this process, in December 2015, the final version of the text of the new General Data Protection Regulation (GDPR) [67] was accepted. The Police and Criminal Justice Data Protection Directive[68] will replace Framework Decision 2008/977/JHA on policing-related personal data. Until the Directive comes into force, Directive 95/46/EC implemented by the Dutch Personal Data Protection Act (2001) will remain in force in The Netherlands. Yet the new regime provides substantially broader legal protection and remedies for citizens against the side-effects of digital identification and risk profiling practices than the earlier data protection tools. Therefore, the extent to which the normative potential of the new regulative principles is effective in mitigating the vulnerable position of children and migrants is worth assessing.

[63] Van der Meer, M. (2013). Ik ben bang van vantrouwend geworden. *Oudersonline.nl*. Retrieved on 18th December 2015 from http://www.ouders.nl/artikelen/ik-ben-bang-en-wantrouwend-geworden

[64] See footnote 4.

[65] See footnote 53.

[66] De Hert, P., & Gutwirth, S. Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalism in Action. In Gutwirth, S. et. al. (Eds.) *Reinventing Data Protection?* (Springer Science, Dordrecht 2009)

[67] The latest version of the GDPR was accepted on 15 December 2015 by the European Council and the European Parliament (Council of the European Union, 2015) and I use this version in this article.

[68] In this article, I use the version from 2012 of the Police and Criminal Justice Data Protection Directive.

A crucial, positive effect of the new data protection regime compared to the earlier data protection rules is that it has significantly broadened its orientation towards the potential implications of the use of digital technology. Beyond expanding upon such essential principles as already enshrined by Directive 95/46/EC, such as proportionality, fairness, lawfulness and transparency (Articles 10, 11), the new regime introduces additional principles that are anchored in fundamental rights traditions. For instance, prescriptions such as those regarding 'consent and lawful authority' (Articles 7, 8), specification as to the 'retention period of the data' (Article 13), 'right to erasure / right to be forgotten' (Article 17), 'data protection by design and by default' (Article 23), 'data breach notification: when, how and to whom?' (Article 32), and 'data protection impact assessment' (Article 33 of GDPR).

The principles that are reflected upon more thoroughly later in this section will also be assessed in light of relevant ECtHR case law. This is important, because since the Charter of the European Union on Fundamental Rights and the Lisbon Treaty[69] came into force in 2009, ECtHR cases have been referenced less frequently by the CJEU. The CJEU became the judicial guardian by which the prescriptions of the Charter would be enforced within the EU. Given that the EU as such is not a signatory to the European Convention on Human Rights, the Convention does not directly apply to the EU. However, the Convention applies to all individual member states as they have individually signed up to it. Referring to ECtHR cases is important as the Court often uses a broader definition of private life when it comes to the implications of digital technologies. Furthermore, all the case law referred to in the following section has the commonality of being based on a broad human rights-oriented interpretation of current data protection principles, and specific surveillance practices condemned by the ECtHR, including preventative surveillance practices by state authorities as violating a person's fundamental right to privacy as laid down by Article 8 of the ECHR. This case law therefore provides a useful basis showing how the right to privacy and data protection rules in general can be strengthened through a stance that is oriented towards the implications of technology use on citizens' rights, including the lives of children and migrants.

The first principle set out by Article 6 (GDPR), which was also enshrined in Directive 95/46/EC, is an explicitly purpose-oriented one: the *purpose limitation principle.* According to this principle, data should be processed for one or more specific purposes and used only for those purposes which are compatible with the original purpose(s) and a check against this principle also entails determining whether the processing of data is legitimate or against the law. The purpose limitation principle does not prohibit data processing for other purposes and the use of data within analytics as long as this activity is fair. Fairness entails, for instance, that the data processing has proportionate implications on one's right to privacy. The importance of this principle has also been strengthened by ECtHR case law, as the cases of *Peck v. United Kingdom*[70] and *Perry v. United Kingdom*[71] also demonstrate. In the case of *Peck v. United Kingdom*, the applicant complained of having suffered infringement of privacy as he was recognizable in CCTV footage that had been broadcasted on BBC news and other television programs. Whereas the national authorities did not recognize that the disclosure of the given video footage entailed a breach of the applicant's privacy, the ECtHR ruled that the disclosure of video footage violated the privacy of the applicants. In the case of *Perry v. UK*, the applicant complained of having been the victim of covert surveillance during a police investigation in which he has been accused of robbery. The applicant claimed that this surveillance practice was illegal and infringed his right to privacy as he had not previously received information any that such video-taping of him would take place. In both cases

[69] Art. 16 of the Lisbon Treaty specifies that everyone has the right to protect his/her data.
[70] This case concerned the disclosure of video footage data gathered in public spaces for broadcasting use by the media. The applicant could not foresee the purpose of such data processing. For more information about this case, please see the court case ECtHR *Peck v. United Kingdom*, No. 44647/98, 28 April 2003.
[71] This case concerned the recording of video footage of the applicant in his place of custody, and use of this information by presenting it to witnesses within criminal investigations. For more, please see *Perry v. United Kingdom*, No. 63737/00, 17 July 2003.

the Court found that the purpose of data aggregation and processing was illegitimate, violated the right to privacy of the applicants and was not "necessary in a democratic society." All this underlines further the pivotal necessity of the purpose limitation principle. The second principle is the *transparency principle*, Article 5 (GDPR), which is closely linked to the purpose limitation principle as this prescribes that the subject shall receive information about the purpose of the data processing, who the data controller is and any other information to ensure the processing is fair and lawful. If information is not collected for law enforcement purposes, the GDPR specifies that information shall be made more easily accessible for citizens. Furthermore, the GDPR specifies that all data processors are obliged to ask citizens for their consent and 'demonstrate' by providing evidence that they have asked for consent (Article 7) before they started to process the subject's data. The GDPR broadened the form of the 'consent' principle in Directive 95/46/EC, as the Regulation provides greater control for individual citizens including a set of specified criteria (e.g. 'informed,' 'freely given') for consent (Article 7) and also through including specifications about consent when it comes to the processing of such sensitive personal data as that of children (Article 8). A legal means to enhance transparency is also guaranteed by Article 13 GDPR as it prescribes that the 'retention period of the data' shall be clearly stated. Yet, the definition of retention period remains ambiguous when it comes, for instance, to Big Data. In the current form of the regulation to interpret retention periods pertaining to Big Data could even lead to more confusion than transparency. To clarify this is necessary because the prescriptions relating to how long data can be retained has essential implications on the quality of data, which is another principle closely linked to transparency.

Enforcing transparency also often remains an issue for the ECtHR. The cases of *Roman Zakharov v. Russia* and *Shimovolos v. Russia*[72] also demonstrate that the practical enforcement of the transparency principle and the right to data protection is often under great pressure and the ECtHR can provide significant help by its condemnatory judgments in order to assist in the practical enforcement of this right. In the case of *Zakharov v. Russia*, the applicant, who was editor-in chief of an NGO that monitors whether the Russian state fosters freedom of expression in the country, complained of having been subjected to illegal, permanent mobile phone interception by the Russian Federal Security Service. After his case had been dismissed several times at national level, the ECtHR ruled that his right to privacy had been violated and the Court condemned in general all non-transparent practices of state surveillance. In the *Shimovolos v. Russia* case the applicant was a human rights activist, and such activism is considered extremism by Russian state practices. The applicant complained that the state authorities kept a secret record of him in order to prevent him joining social gatherings that were related to human rights related protests.

In both cases the ECtHR stressed that transparency of state surveillance practices shall be upheld and the legitimacy of such practices shall not be exhausted by a simple compliance check with domestic laws. Such checks are not sufficient to decide whether the human rights prescriptions of the European Convention of Human Rights are enforced. A compliance check shall entail whether the rule of law as enshrined by the preamble of the Convention is respected. The transparency of data processing is pivotal to uphold and the ECtHR enforces this, for instance, also by ruling in favor of fostering citizens' access to information about themselves.[73]

A third important principle is the *data quality principle*. Article 5 of the new GDPR specifies that data shall be processed 'fairly' and 'lawfully' and collected data must be 'adequate,' 'necessary,'

[72] ECtHR *Zakharov v. Russia*, No. 47143/06, 4 December 2015; *Shimovolos v. Russia*, No. 30194/09, 21 June 2011.
[73] In the ECtHR case *Gaskin v. United Kingdom* the Court held that access to records which relate to a person's family life must be secured by state authorities and this was not granted to Gaskin when he requested access to his personal data. In the *Haralambie v. Romania* case the ECtHR ruled that the right of access to information was not properly enforced by the Romanian state authorities and this resulted in detrimental implications on the private life of the applicant. ECtHR *Gaskin v. United Kingdom*, No. 10454/83 07 July 1989 ; ECtHR *Haramblie v. Romania*, No. 21737/03, 27 October 2009.

'accurate,' 'kept up to date' and 'kept in a from which permits the identification of the data subject no longer than is necessary.' Yet, by their various definitions and the possibilities to interpret them, these a priori specifications are ambiguous. Taking a broad human rights-based definition and interpretation could assist in solving these ambiguities. Hence, the data quality principle can only be tested when the implications of data processing on the subject are assessed in their broadest human rights sense.

The 'right to erasure' or the 'right to be forgotten' (Article 17) and 'data protection by design' and 'data protection by default' (Article 23) entail such technical specifications as anonymization, pseudonimization and encryption. Therefore, these rights and principles are unprecedented legal requirements and guarantees that can assist in the practical enforcement of the right to data protection and also the right to privacy. When put into practice, these new rights could provide also clarification with respect to the ambiguities around such terms as, for instance, 'adequate, accurate or up to date' as set out by Article 5. These novel legal requirements put the data quality principle (also known from Article 6 of the earlier Directive) in a new dimension, as before its registration data shall comply both by design and default with privacy and data protection rules.

Until the GDPR is in force, and also afterwards, ECtHR cases, such as *Khelili v. Switzerland*,[74] demonstrate how the data quality principle can be enforced. The judgment in the *Khelili v. Switzerland* case is explicit about how the registration and retention of wrongful information by state authorities can have significant detrimental effects on a person's private life. In *Khelili v. Switzerland* a French woman complained of having been wrongly classified by the Swiss police authorities as a prostitute and that this wrong information remained in the Geneva police's database for five years. Consequently, the ECtHR ruled that the wrongful and prolonged retention of such data constituted a violation of her right to private life.

In the ECtHR case *M.M. v. United Kingdom*[75] the applicant disappeared with his baby grandson for a day in order to prevent his son moving to Australia after his marriage had broken down. The police, after having investigated the case, only registered a caution in the grandfather's records. Yet, this registration remained for a prolonged period of time and resulted in the applicant being denied a job due to his criminal record. This case also underlines that the retention of 'caution' or risk-related information by state authorities can indeed have detrimental effects on a person's life, which state authorities should adequately compensate for.

The latter two cases are especially useful to demonstrate preventative risk assessment modes by state authorities on children, since the registration and retention of wrongful, risk-related information and the non-proportionate, extended retention of risk data in police databases about children could also significantly hamper their life chances.

The fourth principle that deserves attention is the *data protection impact assessment* (Article 33 GDPR). Given that data protection impact assessments are codified, their implementation will be fundamentally different from earlier assessments as the supervisory authority can directly screen the results. Yet, the inclusion of this new principle also created controversies around its interpretation and practical implementation. Controversies include, for instance, risks stemming from the data processing to the rights of a data subject. Van Dijk, Gellert and Rommeveit argue, for instance, that "*merging risks and rights in the proposed fashion could change their meanings into something hardly predictable*"[76]. Such controversies could also have implications on the enforcement of the closely linked *rights of access, rectification and opposition* of the subject, which prescribe that to those subjected to digital surveillance shall be granted the right to receive a copy of all data processed about them. In some cases the right to object to the processing of their data shall also be granted. The clarification of ambiguities

[74] ECtHR *Khelili v. Switzerland*, No. 16188/07, 18 October 2011.
[75] ECtHR *M.M. v. United Kingdom*, No. 24029/07, 13 November 2012.
[76] Van Dijk, N., Gellert, R., & Rommetveit, K. 'A Risk to a Right? Beyond Data Protection Risk Assessments' (2016) 32(2) Computer Law & Security Review, 31

around the practical enforcement of Article 33 of GDPR will be a time-consuming process, yet the principle in itself is a great addition to enforce the human right to privacy in a broad sense.

A fifth important principle is *the security principle*. Article 32 GDPR codifies that data controllers shall issue 'data breach notifications' including when and how data breaches happened and to whom. Given that data breaches shall be communicated within 72 hours and the data protection authorities have the power to issue significant fines if companies commit a 'data breach,' this also codified their direct liability for any personal data collected by them. The data controller shall implement appropriate technical and organizational measures to prevent accidental loss or destruction of data. Furthermore, the processor shall have "sufficient guarantees in respect of the technical security measures and organizational measures governing the processing." Although specific ECtHR case law is quite limited on this principle, a recent development by the Dutch government is significant. In May 2015 the Dutch government introduced the Bill on Notification of Data Leaks[77], a law that gives significantly higher authority to the Dutch Data Protection Authority. By obliging data controllers to notify the Data Protection Authority of each case of a data leak, the DPA can impose substantial fines on parties guilty of personal data leaks. By this new Bill, the Dutch government has established also a strong precursor for the new EU data protection regime.

3.1.4. Legality and democracy

The specific negative implications of risk assessment technologies on children's lives detailed in section 2.1., and the drawbacks of identification and risk profiling systems on migrants' lives detailed in section 2.2. beyond the assessed relevant data protection principles and ECtHR case law, could also be checked against a rule of law test, meaning whether the existing domestic legislation provides sufficient safeguards to maintain the 'rule of law' in a given (in this case Dutch) democratic society.

When the human rights and also the new and past data protection framework define legal exceptions that allow for infringement on the right to privacy (as laid down by Article 8 of the ECHR) - in its broad sense – this is again framed as an opposition to security. In Articles 8, 9, 10 and 11 of ECHR, conditions for arbitrary tampering with the right to privacy, freedom of thought, conscience and religion (Article 9), freedom of expression (Article 10) and freedom of assembly and association (Article 11) are, first of all covered by the legality principle. This means that any infringement of these rights (Articles 8, 9, 10 and 11) shall be made "in accordance with the law." However, a number of ECtHR cases show how state authorities have been condemned because the Court found that domestic legislation provided insufficient safeguards to maintain, beyond the right to privacy, also such democratic values as legitimacy and legality[78]. In the *Malone v. United Kingdom*[79] case, the applicant asserted that he has been a victim of telephone wire tapping on the authority of a warrant issued by the Secretary of State. He further argued that there was no supervision of how such warrants are executed, therefore they should be considered illegal. In the ECtHR judgment, the Court held that UK law did not provide sufficient safeguards to protect the applicant's right to privacy. Furthermore, it stated that: "*the minimum degree of legal protection to which citizens are entitled under the rule of law in a democratic society is lacking.*" Certainly such a conclusion requires careful assessment of all legal, societal, technological and other

[77] Wijziging van de Wet bescherming persoonsgegevens en enige andere wetten in verband met de invoering van een meldplicht bij de doorbreking van maatregelen voor de beveiliging van persoonsgegevens alsmede uitbreiding van de bevoegdheid van het College bescherming persoonsgevens, Eerste Kamer (2015) 33662. Retrieved on 16th January 2016 from https://www.eerstekamer.nl/behandeling/20150210/gewijzigd_voorstel_van_wet

[78] ECtHR *Huvig v. France*, No. 11105/84, 24 April 1990; ECtHR *Halford v. United Kingdom*, No. 20605/92, 25 June 1997, ECtHR *Leander v. Sweden*, No. 9248/81, 26 March 1987.

[79] ECtHR *Malone v. United Kingdom*, No. 8691/79, 2 August 1984.

conditions. The fact that the Court can give such a judgment underlines however the potential of the ECtHR in enforcing and guaranteeing fundamental rights and democratic values.

3.2. Interim conclusion: incorporating data protection and human rights principles into professional work

The decision to reflect upon the negative implications of the use of Dutch identity management technologies on children and migrants' lives in light of the current Dutch data protection principles, and to also reflect upon these principles via ECtHR case law and the principles of the new EU Data Protection regime was taken for a number of reasons. First, given the relative novelty of these technologies, and their implications, rendered children and migrants comparatively vulnerable groups. The second reason is that many of the consequences of these systems on children's and migrants' lives are long-term and could be better addressed from a combined data protection and human rights perspective. In light of these developments, to evaluate the abovementioned negative implications of the DYHR, the RI and ProKid on children's lives, and of the INS and PROGIS consoles and the API system on migrants' lives, via the relevant prescriptions of the principles of the new EU data protection regime is not only timely but it is useful to discuss options offered by more advanced data protection and human rights remedies for children and migrants in order to mitigate their vulnerable position as a consequence of digitalized risk assessments. Assessing a selection of data protection principles and human rights case law has also been useful in order to test the normative state of the current and future EU data protection regime. Yet, more importantly, this analysis was meant to help to draw the attention of professionals who use preventative digital systems for the assessment of children and migrants to the drawbacks of these systems. The analysis also intended to highlight for professionals what data protection principles and ECtHR case law can offer in order to mitigate the vulnerable position of children and migrants assessed by these systems. Furthermore, this research would like to clearly acknowledge the high workload of professionals in the relevant fields, and their genuine interest in conducting their work well and avoiding the drawbacks when operating these systems. For professionals, however, employing a mindset that is inspired by Article 33 of GDPR, for instance, and carrying out their assessment work while bearing in mind the implications of the use of technology on data protection and human rights principles is crucial. To remain proportionate, not to discriminate, and perhaps even more importantly to reevaluate priorities between privacy and security interests on a case-by-case basis could help prevent children and migrants becoming trapped in a digitalized 'risk identity' that is imposed upon them and retained for a long period of time. Why? Because each time a violation of the right to privacy, autonomy or non-discrimination against citizens occurs these fundamental rights, although upheld in the statute books, are not enacted in practice as universal rights. Since children and migrants, partly as a consequence of the use of preventative identity management systems, are placed in a certain 'accountability vacuum' and would perhaps be in most need of their human rights, privacy, dignity and equality being respected, to evaluate whether risk-based monitoring practices comply with principles of proportionality, legality and democracy is essential.

4. Conclusion

> "*By far the greatest latitude of choice exists at the very first time a particular instrument, system, or technique is introduced. Because choices tend to become strongly fixed in material equipment, economic investment, and social habit, the original flexibility vanishes for all practical purposes once the initial commitments are made. In that sense technological innovations are similar to legislative acts or political foundings that establish a framework for public order that will endure...*"[80])

The status of democracy in a society is never absolute but continuously changing: democracy after the Second World War or in the 1960s, 1970s and 1980s was quite different than it is today. Yet, despite its imperfections, to keep its fundamental principles such as liberty, equality and non-discrimination intact in day-to-day practice is perhaps the most important goal to strive for in order to allow democracy endure, even in a highly digitalized society.

This is especially crucial for novel forms of digitalized prevention practices. The possibility of a threat within digital prevention mechanisms often becomes a real expectation of a threat. Risk profiling criteria in digital systems are regularly based on threats that have happened in the past, and when such projections of past experiences prove not to constitute sufficient basis for risk calculations because of the emergence of new threats, as a reaction these new threats should also be incorporated into the risk calculation as new(ly experienced) possibilities of threats for the future. This often results in the introduction of new systems or the improvement of old ones. However, the possibilities of extending such a 'threat-response' cycle and allowing for the implementation of more and more digital technologies in order to perform forms of prevention without proper legal countermeasures seem to be almost infinite.

Therefore, despite the noble purposes behind each of the abovementioned digital systems, the detrimental implications of the current use of the six identity management technologies in The Netherlands in order to protect children and migrants against a variety of risks can also be regarded as experimenting with the day-to-day value of the right to privacy, the right not to be discriminated against, but also with the right to liberty and security. Hence, these implications should be taken seriously. Article 5 of the ECHR allows for infringing upon the right to liberty of a person 'subject to lawful arrest' such as 'arrest of reasonable suspicion of a crime or imprisonment.' Yet, the current preventative modus of digitalized identity monitoring of children and migrants by typifying bodily and behavioural characteristics as 'risk indicators' in the name of security put the boundaries of 'reasonableness' in our current society to the test. Terrorist attacks exemplify events which are often unpredictable and irrational. The preventative measures introduced to prevent such attacks are mostly based on incidents that are incomparable perhaps only except for their devastating implications. Consequently, prevention techniques are not based on statistics but on random data, which leads to profiling practices using such stretched scales that are geared toward searching for the infamous "unknown unknowns." The orchestrated digital techniques that are used to identify the potential perpetrators better and faster in practice gradually cut the boundaries and limit the extensions of diversity under the banner of security measures that are considered and believed being 'acceptable and necessary in a democratic society.' Despite the proven imperfections of risk profiling[81] and identity management technologies in maintaining security, these systems remain successful in sustaining the impression of security, at least until a new event occurs that these systems were supposed to prevent. The worry is that in the long run

[80] Winner, L. 'Do artefacts have politics?' Daedalus, 109(1) (MIT Press, 1980) 127

[81] Lecluijze, I. The wrong tool for the job. The introduction of the Child Index in Dutch child welfare. (PhD thesis, Maastricht University, 2015)

democratic society might just lose its democracy. This is something Dutch sociologists are also concerned with when it comes to the digital risk profiling of children's behaviour:

> "*Education [in The Netherlands] became an individual project, a type of behaviour therapy. But is a child actually well educated if he has not become a criminal or, if he has not fallen prey to a pimp? […] education, training and youth policy should be about much more than dealing with behaviour. It should, for instance, much rather be about how to learn, understand and internalize democratic citizenship, humanity and freedom and about what it means to live in a democratic society in which you are entitled to your own identity, but where you also have to grant others the same right. How do you offer alternatives to the tempting 'us-and-them' way of thinking, which on the one hand provides a secure sense of belonging, but on the other bears the risk of dehumanizing and excluding the other?*"[82]

Although children and immigrants differ significantly, the first experiences of children in their social relationships to others and how they begin to understand and practice democratic values such as mutual respect and human dignity can be compared with how immigrants gather their first impressions of others in their new home country and how they learn to internalize democratic rights and values. The principle of treating others well because we would also like to be treated well can be regarded in general as a crucial precept to live by. However, when it comes to assessing children and migrants against risks, being cautious and attentive of potential discriminative effects is essential, because each of those practices which result in detrimental implications on children and migrants can have prevailing implications. Because children will become grown-ups and migrants will become integrated citizens who together form a future society that has to care about bringing up new children and integrating new immigrants. Therefore, for youth care, law enforcement and immigration professionals to orchestrate and perhaps re-prioritize digitalized prevention techniques with other methods such as education and more social cooperation and to balance and compensate the negative legal and societal implications of digital identification and risk assessment techniques on these groups in day-to-day practice is crucial and something to strive for. This is the case because the fundamental values of democracy, human rights and also those values enshrined by the new data protection regime, beyond national and international court decisions, are much rather enforced by setting examples in daily practice.

Acknowledgements

This article greatly benefited from the research conducted under the realm of the DigIDeas project, which project was awarded to Dr. Irma van der Ploeg by the European Research Council under the European Union's Seven Framework Programme (FP7 2007–2013)/Grant No. 201853/. The DigIDeas project allowed for conducting empirical research and gaining insights from Science and Technology Studies (STS) and surveillance studies in an interdisciplinary environment. The gained insights assisted in informing the legal analysis in this article and in my PhD thesis as a whole. For her insightful comments on this article and support (of my PhD) I am very grateful to Prof Corien Prins.

[82] De Winter, M. *Verbeter de wereld. Begin bij de opvoeding Vanachter de voordeur naar democratie en verbinding.* (Amsterdam, SWP, 2011)

Summary of PhD thesis

Title:

Digitizing risks and risking citizen rights: Prevention practices and their legal and socio-technical implications on children's and migrants' lives

Karolina La Fors-Owczynik

The digitalized prevention of threats and risks has earned growing prominence within different Dutch government policy areas in the past decades. Youth care, law enforcement, immigration and border control are policy areas where such technological developments have emerged rapidly and extensively. The consequences for citizens' lives are regularly underestimated. Therefore these areas necessitate careful legal and socio-technical analysis.

The focus of these policy areas are among others children and migrants. Both can be considered as vulnerable groups with respect to their social status, legal position and often awareness of 'threats'. Digital technologies have been implemented to prevent or react upon such threats, given these systems facilitate generating proactive knowledge on situations and circumstances that might become a threat for them. However, risks might also stem from the very design and daily use of such systems. For in implementing and using these systems, to different degrees both groups can be regarded being at the 'peripheries of citizenship' and to some extent these groups might even fall prey to unintended exclusions. To conduct research about these potential 'peripheries' is therefore pivotal, as this can provide useful reflections upon the conditions of citizens' rights within society as a whole. As a conceptual symmetry, I analyzed the regulatory framework that applies to the use of personal data of children as well as migrants and assessed the implications of preventative identity management systems on their lives, especially how they have been digitally framed as being 'at risk' or 'as a risk'. This particular symmetry assisted in unpacking the modes in which digital mechanisms of exclusion and inclusion regarding these quite vulnerable groups take place.

In focusing on children, it becomes clear that, on the national level several well-mediated incidents of child-abuse and anti-social behaviour of youth have been catalysts for the introduction of a variety of digital, risk prevention systems. The introduction of these systems also coincided with the historical transformation of Dutch youth care in terms of comprehensive changes in the legal framework regarding youth care and the redistribution of tasks among government and youth care authorities. The following three systems introduced and used within this period constituted part of the analysis in this thesis: the Digital Youth Healthcare Registry(DYHR) within youth healthcare, the Reference Index High Risk Youth(RI) within youth care in general and the preventative system used by the Dutch police: ProKid 12-SI(ProKid). Each of these systems are geared toward preventing risks related to violence towards children and to varying degrees also toward preventing violence committed by children. The DYHR is a system used uniquely by youth healthcare professionals, where

professionals can register risk data about children below the age of 19 and can also signal their concern within the connected Reference Index High Risk Youth. The Reference Index is a certain safety net of alarm bells among professionals in youth care. The prerequisite of professionals to inform each other and co-operate regarding a child case is digitally wired within the web of RI. In its set up a broad variety of institutions involved with youth are linked to each other via risk signal submission to RI. A so-called 'match' is triggered if more risks have been registered about the same child under the age of 23 by different youth care workers. The ProKid system is unique on its own, as by its use the police took up for the first time a systematic prevention task by monitoring, signaling and registering risks with respect to children under the age of 12 as well as their families and friends.

In looking at the second group – migrants – it becomes clear that border control and immigration, both on the EU level and the national level, as well as combatting illegal entry, identity fraud and related crimes committed by migrants have been regarded as high priorities during the past decade. The randomness and consequently difficult anticipation of international terrorism has paradoxically contributed to an exponential growth in highly sensitive identity management technologies in order to filter terrorists from travellers and immigrants Digital identity management and risk profiling technologies for screening immigrants and travellers have been regarded as 'ultimate promises' to fight and prevent such 'deviances' as illegal entry, identity fraud and related crime or even terrorism. Three technologies used in the Netherlands have been analyzed in this thesis. One is the biometric identification and identity verification system called INS console used by the Dutch immigration services to identify immigrants. The second technology is the PROGIS console used by Dutch authorities within the law enforcement chain. Instances of identity fraud among criminals prompted this biometric system, which serves to establish trustworthy and verifiable identity for suspects, criminals and also deceased victims. Furthermore, this system is intended to provide coherence about the identity data of registered persons among authorities within the justice system. The third system is the Advanced Passenger Information (API) system, which serves to profile travellers against international and national risk profiles that are related to a variety of delinquencies. Personal characteristics, travel and baggage information in combination with international delinquency data are regularly projected on travellers by this system to filter those who 'misfit'.

The methodological set up of the thesis is legal desk research, whereby STS and in particular actor network theory is used to assist in drawing empirically-based, informed legal conclusions. One of the main perceptions of STS is that technology is not neutral and technology and persons mutually shape and implicate each other. This has been considered helpful for this thesis when encroaching on the boundaries of such legal definitions as privacy, data protection and related human rights issues. Insights into professional practices have been gained by semi-structured interviews with professionals (15 professionals concerning children and 12 professionals concerning migrants) having been involved either in the design or the use of one of these systems in different Dutch cities. When selecting professionals, I kept a diversity ranging from professionals who took part in the design of systems to those who were only users. With respect to the case study on children, this involved that I interviewed doctors and nurses using the Digital Youth Healthcare Registry and who also transmitted risk signals to the Reference Index. As to the Reference Index, I interviewed system designers and managers on different levels in municipalities who were responsible for the operational management of risk signals and the risk

signaling by professionals via the Reference Index. Concerning ProKid SI 12-, I interviewed police officers who took part in the technical and policy related design of the system, and also field officers who carried out the digital risk profiling of children via ProKid. With respect to the case study on migrants, I interviewed immigration, alien police, Royal Marechaussee officers who took part either in the design or use of INS console, PROGIS console and the API system. In some cases a designer has also participated in operating the system. The experience from the user-perspective often proved to be helpful for these stakeholders as in this manner they could suggest practice-based improvements.

This empirically-based approach towards technology and its daily use helped to provide more comprehensive legal conclusions about digital risk assessments and identity verifications. The legal research has been centered around examining the implications of technology use in the light of the normative framework provided by the existing and newly drafted data protection rules of the EU as well as in light of fundamental human rights and children's rights principles.

In light of the above the main research questions of this thesis are defined as follows:

What are the implications of the design and use of preventative IDM systems for the legal and societal position of citizens within different contexts of citizen-government relations in The Netherlands; and what is the potential of the EU data protection as well as the ECHR fundamental rights regime to prevent and remedy the potential risks of such system-use for the lives of citizens?

In answering this question, the second, third and fourth chapters focused on the youth care domain. Chapters five and six deal with the relevant issues related to migrants. Chapter seven presents lessons that can be learnt from the two case studies by providing an analytical comparison between digitalised risk profiling and identification practices of children and migrants.

As to youth care, chapter two dived into the implications of the DYHR, RI and ProKid systems by STS methods. This chapter explored the mechanisms leading up to a risk profile of a child within these systems. It concluded that the extensiveness of risk categories, the broadness of the 'social radius' around a child, can figure in the risk qualification of a child. In combination with the time span within which risk data can remain relevant, children can easily be assigned a high risk category. On the other hand, however, to erase such a risk profile and even a wrong risk profile is an extremely work-intensive process. All this raises ethical and social concerns about the implications of these systems for the position of children within society, which also serves to prompt discussion about the 'acceptability' of using these systems.

Chapter three explored the normative potential of the current and proposed data protection regime[1] in light of the implications of the DYHR, RI and ProKid on children's lives. In addition to an analysis of the data protection regime, the analysis looked at the role the United Nations Convention on the Rights of the Child could play. The analysis explored how the proposed data protection rules will impact present profiling practices of children by requiring more tailor-made risk assessments for them. Although the digital applications as such are meant to prevent problems and serve in the 'best interest' of the child, the empirical examples show that the very use of these systems is what often puts this 'best interest' into jeopardy in various forms of potentially discriminative profiling. Furthermore, although the new data protection rules will provide far better protection for children than the current ones, the new regime alone appears not sufficient to prevent or mitigate the sketched risks stemming from the use of these systems. Therefore, the chapter concluded that reframing the data protection

[1] Concerning the new data protection regime, in this thesis I refer to the new EU General Data Protection Regulation (version from 15th December 2015) and the EU Police and Criminal Justice Data Protection Directive (version 2016/680).

regime in order to better protect "the best interest of the child" as established by the United Nations Convention on the Rights of the Child is necessary, when it comes to the risk profiling of children.

Chapter four, investigated current digitalised preventative practices directed at children that oddly are carried out by the Dutch police using ProKid. The analysis investigated the implications of the day-to-day use of this system on children's lives according to prescriptions of the United Nations CRC. The analysis has shown first, that a variety of ambiguities surround this system. For instance, one relates to that by using ProKid the police carries out a new task of prevention directed at children under the age of 12. However, the police by law is not allowed to conduct (law enforcement) investigations on children under the age of 12. The analysis also shed a light on the policy goals behind the system. What appears problematic is that the system is employed for two highly different policy goals: preventing 'crimes against children' as well as 'crimes committed by children'. Both are held up as equal priorities within the policy discourse ProKid is employed in by the Dutch police. The analysis in this chapter shows however, that risk profiling practices in order to meet such diverging goals clash with a set of CRC rights and principles, as the profiling by ProKid often frames children as potential perpetrators even when they are registered as victims of violence.

Chapters five and six focused on the implications of the INS, PROGIS console and API system on migrants' lives. Chapter five analysed how immigrants and travellers are increasingly framed as posing a risk to the Netherlands. More specifically, by STS methods it is shown how prevention modes and their associated risk assessment systems have come to focus on translating specific problems around migrants into problems of illegal entry, identity fraud and related crimes. The chapter describes that the quest for 'accurate identity' and the technologies used to tackle this goal transform the problem and create new uncertainties and risks for those subjected to monitoring by these systems. For instance, the high sensitivity of biometric readers and the density of inbuilt standards bring with them that the verification of fingerprints require extensive work-arounds, because the verification of fingerprints on these readers can easily produce false results. The analysis concluded that these systems can result in a shift that increasingly produces an image of migrants *posing* a risk. Clearly this raises ethical concerns.

From chapter six, it becomes clear that beyond the politics of the current humanitarian migration crisis, digitalised professional practices of immigration and border control increasingly frame migrants being viewed as a risk. This in particular can decrease the chances, for instance, for asylum seekers to become and remain to be seen as being 'at risk'. The chapter discusses the normative implications of such practices on migrants' lives by assessing these examples against the background of relevant prescriptions of the current and the proposed EU data protection regime, as well as of fundamental rights and principles of the EU human rights framework. It concluded that the capacity of the current data protection regime in protecting migrants from being framed 'as a risk' or a 'misfit' via digital prevention practices is insufficient. Moreover, although the new data protection rules provide a much broader set of protective prescriptions, the normative potential of the new rules would highly benefit from the European Convention on Human Rights as its prescriptions can provide additional legal remedy for migrants from the detrimental implications of digitalised identification and risk profiling.

Chapter seven brings the domains of children and migrants together and sets out to search for similarities between risk profiling practices on children and migrants and thus acquire better insights in the use and implications of digital tools within policy areas that focus on vulnerable groups in our society. The chapter thus aims to determine the extent to which differences emerge in the position of individuals involved, among others given that youth care is addressed primarily on the a national policy level and immigration on the EU level. The analysis also entailed the pursuit of normative and broader societal options that can guide professionals in becoming reflective about the detrimental implications

of digital technologies. Furthermore, this pursuit included testing possible differences in the normative potential of the data protection and human rights' framework regarding the vulnerable position of children on the one hand and migrants on the other hand. The findings of the chapter show that for youth care, law enforcement and immigration, professionals need to orchestrate and perhaps re-prioritise digitalised prevention techniques with other methods such as education and social cooperation. Secondly, to balance and find adequate legal remedy against the negative effects of digital identification and risk assessment techniques on these groups in day-to-day practices remains an essential requirement for professionals.

A key motive behind this is raising better insights and awareness about the possible detrimental consequences of using identity management systems by government authorities in order to forecast and prevent risks regarding children and migrants. By informing the theoretical analysis with empirical examples from youth care it becomes clear that although these systems are meant to serve the best interest of the child", in practice their very use can potentially result in infringing upon this interest. The fact that migrants can also suffer the detrimental effects of such technology use relates to flaws in the set policy goals. Notably, profiling practices and identity verification practices are geared towards achieving the policy goal to render children and migrants 'more and more transparent'. However, as the analysis in this thesis shows, the particular 'transparency' gained by these digital practices is not neutral. For if only risk related data is deemed interesting for registration about a child or a migrant, the lens through which professionals need to look and register issues becomes much more a transforming prism as to the identity of the subjected child or migrant. The conclusions and recommendations in each of the chapters in this thesis have issued a plea for a more human rights and children's rights-minded approaches in professional practices. An approach that gives recognition of the applicable regulatory framework on data protection as well as human rights is in particular crucial given risk related predictions shape the future of citizens already in the present. On the policy level a discussion on how potential detrimental effects (such as stigmatization and discrimination) can be addressed by giving recognition to the regulatory framework (as early as in the design process of the digital tools) appears therefore crucial. In line with this, the analysis in this thesis demonstrated that using IDM systems within the context of Dutch youth care and law enforcement and in the context of Dutch border control and immigration can render the positions of children and migrants vulnerable. The analysis furthermore highlighted that the potential of the new European data protection regime in providing protection and remedy for children and migrants compared to the 95/EC/46 Directive is significantly stronger which is highly beneficial for these groups. Yet, the thesis also pointed out that the challenges posed by the daily use of preventative IDM systems to screen children and migrants require the consideration of broader fundamental children's and human rights prescriptions. These prescriptions proved to be indispensable not only in order to prevent and remedy unnecessary intrusions into the private lives of the scrutinized citizens, but also to prevent and remedy the detrimental, long-term implications of such intrusions on children's and migrants' lives, such as for instance the stigmatizing effects of false accusations demonstrated.