Prevention strategies, vulnerable positions and risking the ‘identity trap’

La Fors, Karolina

Published in:
Information & Communications Technology Law

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

DOI:
10.1080/13600834.2016.1183307

Publication date:
2016

Link to publication

Citation for published version (APA):
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

To cite this article: Karolina La Fors-Owczynik (2016) Prevention strategies, vulnerable positions and risking the ‘identity trap’: digitalized risk assessments and their legal and socio-technical implications on children and migrants, Information & Communications Technology Law, 25:2, 71-95, DOI: 10.1080/13600834.2016.1183307

To link to this article: http://dx.doi.org/10.1080/13600834.2016.1183307

© 2016 The Author(s). Published by Informa UK Limited, trading as Taylor & Francis Group

Published online: 26 May 2016.

Article views: 120

View related articles

View Crossmark data
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*

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

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 European Union 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

*Email: k.lafors@uvt.nl

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 European Union (EU) General Data Protection Regulation (GDPR)\(^3\) 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 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

---

\(^2\)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).

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 towards the implications of preventative technology use on children and migrants and not primarily towards the purpose of such technologies. This also includes a final plea in this article for raising awareness and stimulating reflectivity among 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’ towards 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. 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 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.


6The 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, for example, 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 signalling 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.

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. 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. 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 ProKid. 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

---

8Fors-Owczynik and Valkenburg (n 5).
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 willing-
ness 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 govern-
ments 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 impli-
cations 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.

Three technologies have been analysed in earlier research.**16** The first is the relatively
recently introduced biometric identification system for immigrants, called the immigra-
tion and naturalisation service (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 programme information supply for the criminal
justice chain (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).

---

**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.
**14**B Latour, *Science in Action: How to Follow Scientists and Engineers through Society* (1st edn
**15**La Fors-Owczynik (n 9). and K La Fors-Owczynik, ‘Monitoring Migrants or Making Migrants
“Misfit”? Data Protection and Human Rights Perspectives on Dutch Identity Management Practices
Regarding Migrants’ (2016) CLS Rev. doi:10.1016/j.clsr.2016.01.010
**16**Ibid. and see also references (n 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 in Figure 2.

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 in 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. 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 also shape immigration policies throughout Europe. Yet, as

---

**Figure 2.** The mediation process between threats and migrants involves political, legal, and socio-technical processes. Although the majority of migrants are traditionally regarded being ‘at risk’. But this perception is recently under pressure due to the current migration crisis and terrorist attacks. Beyond these politically-laden circumstances, this figure suggests and this research will show that the digitally mediated risk profiles of migrants further contribute to their vulnerable position. These systems can frame them by default ‘as a risk’ if their ‘identity’ data does not comply during an identity check, or if their ‘identity’ data matches a risk profile.

---


Philip Zimbardo argues, 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 (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 lead to reassuring Dutch media news with respect to having detected no signs of terrorism among asylum seekers to the Netherlands. 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. 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. This analysis demonstrated that the consequences of (too) sensitive biometric screening technologies and too wide variables for building a risk profile in the API 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. 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.

\[20\] Ibid.
\[24\] See (nn 4 and 14).
\[25\] La Fors-Owczynik (n 15).
\[26\] Ibid.
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 assess-
ment. 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 ‘necess-
ary’. 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
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 digi-
talized risk categories use in these systems tend to reify risks. The lengthier and more
comprehensive the screening by digital risk categories and the quicker the ‘risk’ infor-
mation 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 labour-intensive.

The fact that both children and migrants – although to differing degrees – are increas-
ingly considered and identified being either ‘at risk’ or ‘as a risk’ in the Netherlands, from
a legal perspective leads to a third commonality: they both need support to be held accoun-
table 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 dom-
estic 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,

---

27 La Fors-Owczynik and Valkenburg (n 8).
28 See (n 4).
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 then deemed to substantially increase trust with respect to the claimed 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 children29 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.

29MR Bruning and others, Kinderrechtenmonitor 2012 – Adviezen aan de Kinderombudsman (De Kinderombudsman, Den Haag 2012)
31AR Feedes, L Nicholson and B Doosje, Triggerfactoren in Het Radicaliseeringsproces (Expertise-unit Sociale Stabiliteit, Amsterdam University, Amsterdam 2015).
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 evaluation of potential side-effects. On the other hand, the policies33 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 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 – for example, false alarms rates of child abuse34- and on migrants – for example, false positives and false negatives35 – 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

---

32 Article 29 Data Protection WP. Opinion 03/2013 on Purpose Limitation (Commission of the European Union, 2013)


33 Identiteitsvaststelling in de strafrechtsketen: Wet en Protocol (Ministerie van Justitie, 2010).


to values of privacy versus security requires addressing. When doing so, particular attention will be given to two perspectives that are geared towards 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 EU 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 EU 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.

The right to privacy and data protection are two separate fundamental rights (Article 8 of the Charter of the Fundamental Rights of the EU), as the European Court of Justice also clarified in the case of Österreichischer Rundfunk 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
3.1.2.1. 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, the purpose limitation principle has remained an ‘essential first step in applying data protection laws and designing data protection safeguards for any

36 Joined cases C-465/00, C-139 & 139/01, Österreichischer Rundfunk and Others [2003] ECR I-4989.
processing operation’ ever since. 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. 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.

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. Nissenbaum even argues for the abolishment of ‘old’ data protection principles such as the purpose limitation principle. 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. 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 cases in part stemming from 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.

---

38The 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’.


40F Ferretti, ‘Data Protection and the Legitimate Interests of Data Controllers: Much Ado About Nothing or a Winter of Rights?’ (2014) 51(3) CML Rev 843.


43Ibid.

44Function creep: when data gathered for one specific purpose is also used for other purposes not indicated originally.
from the increase in use of Big Data and Open Data. 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’. 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 predefined 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’.

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’. These would strengthen and also reform the purpose limitation principle and all in all achieve improved protection of personal data and privacy.

3.1.2.2. 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 must be accepted provided this serves the purpose of security’.

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 closed-circuit television cameras (CCTV) 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 European Court of Human Rights (ECtHR) case law. Yet,

45 M Hildebrandt and K De Vries (eds), Privacy, Due Process and the Computational Turn: The Philosophy of Law Meets the Philosophy of Technology (1st edn Routledge, 2013).
47 Ibid.
scandals of breaches of privacy rights (such as issues related to the revelation of Snowden and the National Security Agency of the US) 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’. 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’. 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. Such body of case law is also essential to complement and strengthen data protection regulations.

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. 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’. 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. 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 reflected by the fact that ‘security risks proliferate and exceed the capacity for officials to fully manage or

52B Koops, ‘On Decision Transparency, or How to Enhance Data Protection After the Computational Turn’ in M Hildebrandt and K De Vries (eds), Privacy, Due Process and the Computational Turn (Routledge, Abingdon 2013).
even identify [persons], 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’ – 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. Remediing 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.

59 Ibid.
60 S Van der Hof and C Prins, ‘Personalisation and its Influence on Identities, Behaviour and Social Values’ in M Hildebrandt and S Gutwirth (eds), Profiling the European citizen Cross-disciplinary perspectives (Springer Science, 2008).
61 Hijmans (n 37) 105.
Furthermore, examples of false positives in part stemming from the broadness of variables for building risk profiles show that the API system can frame migrants ‘as a risk’ of committing identity fraud (see fn 5).

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 (see fn 5).

Furthermore, false reporting of child abuse cases by using such risk evaluation systems as the DYHR, the Reference Index High Risk Youth or ProKid are argued to have stigmatizing effects on children (see fn 29). 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.\(^\text{63}\) 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.\(^\text{64}\) All these instances would need a legal remedy and counselling 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.\(^\text{65}\) 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.\(^\text{66}\) 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.

### 3.1.3.1. 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 GDPR\(^\text{67}\) was accepted. The Police and Criminal Justice Data Protection Directive\(^\text{68}\) 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.

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 23), ‘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 EU on Fundamental Rights and the Lisbon Treaty69 came into force in 2009, ECtHR cases have been referenced less frequently by the Court of Justice of the European Union (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 European Convention on Human Rights (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

69 Art. 16 of the Lisbon Treaty specifies that everyone has the right to protect his/her data.
the cases of Peck v. United Kingdom\textsuperscript{70} and Perry v. United Kingdom\textsuperscript{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 programmes. 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 videotaping of him would take place. In both cases 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 \textit{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\textsuperscript{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

\textsuperscript{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.

\textsuperscript{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.

\textsuperscript{72}ECtHR Zakharov v. Russia, No. 47143/06, 4 December 2015; Shimovolos v. Russia, No. 30194/09, 21 June 2011.
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 favour 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’, ‘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,

73In 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 Haralambie v. Romania, No. 21737/03, 27 October 2009.

74ECtHR Khelili v. Switzerland, No. 16188/07, 18 October 2011.
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* 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’. 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 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, a law that gives

---

75ECtHR *M.M. v. United Kingdom*, No. 24029/07, 13 November 2012.
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 data protection authority 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. In the *Malone v. United Kingdom* 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 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.

80 Winner (n 1) 127.
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 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 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

---

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
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 Ph.D. thesis as a whole. For her insightful comments on this article and support (of my Ph.D.) I am very grateful to Prof Corien Prins.

Funding
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 number 201853].

Disclosure statement
No potential conflict of interest was reported by the author.

82M De Winter, Verbeter de wereld. Begin bij de opvoeding Vanachter de voordeur naar democratie en verbinding (SWP, Amsterdam 2011).