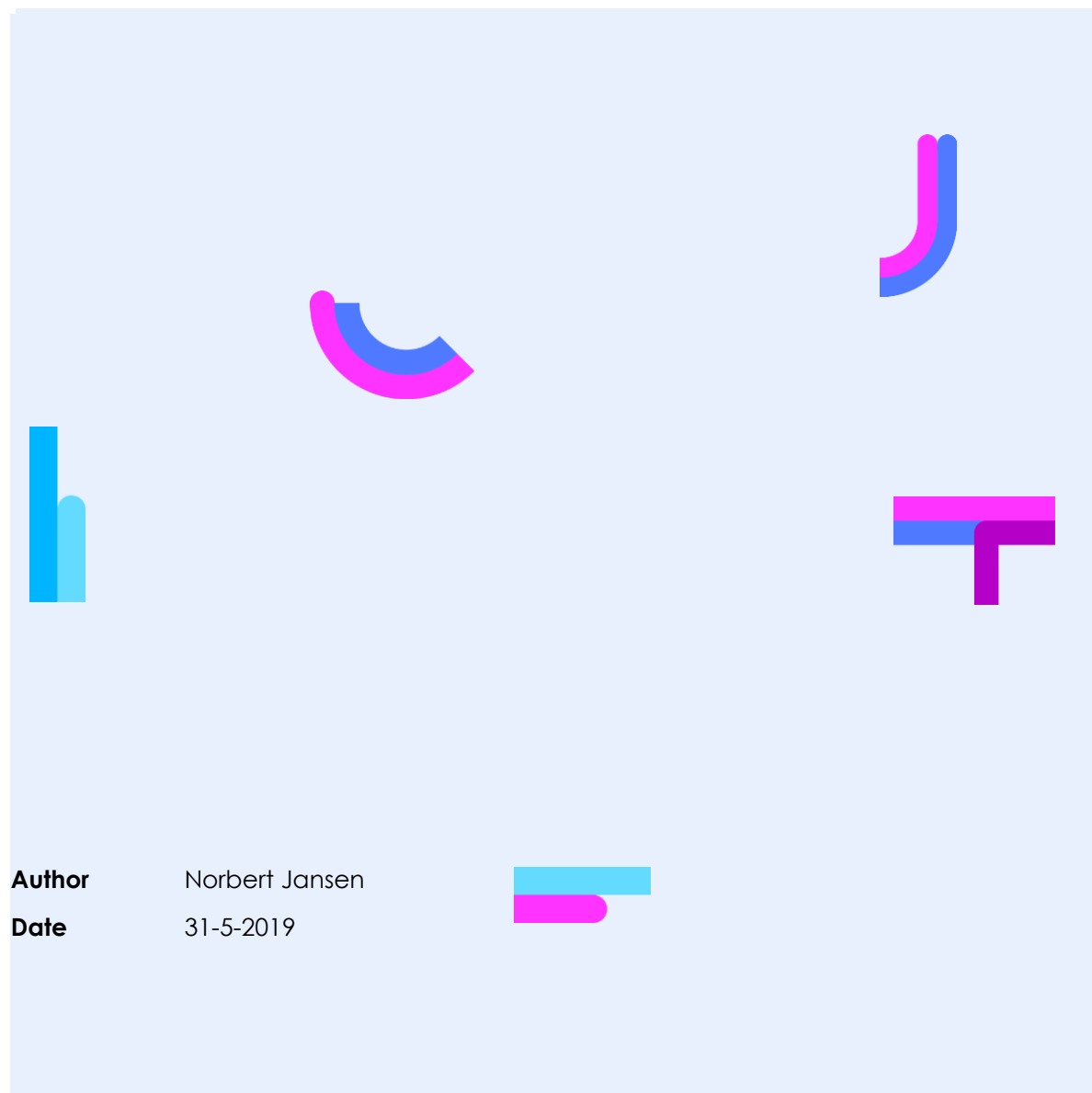


Call for submissions: On digital technology, social protection and human rights.

A report from the Netherlands



Author Norbert Jansen

Date 31-5-2019

1. Introduction

This is an entry in the call for submissions: Thematic report to the UN General Assembly on digital technology, social protection and human rights.

Scope

Specifically covered in this document is the right to social protection and to an adequate standard of living as depicted in The International Covenant on Economic, Social and Cultural Rights.

This document focuses on the Netherlands and in this document the author relates the above-mentioned human rights to the subject of fraud fighting and digitalization.

Fraud fighting is the specialization of the author.

In the Netherlands some pitfalls of digitalization are described by various organizations. Examples of side effects of digitalization for some individual citizens are well documented. This report covers some of these examples.

Before we go into fraud fighting, we look at how digitalization in the Netherlands has developed in Chapter 2. This gives some first observations regarding human rights that are depicted in Chapter 3, paragraph 1. In Chapter 3, paragraph 2 the effects of fraud fighting are described.

2. Digitalization in the Netherlands.

The Netherlands has a long history in digitalization and is well positioned in worldwide rankings in this field. Furthermore, The Netherlands has a rich history and ranks highly in the field of social protection.

The digital infrastructure system of public base registrations

In the Netherlands several decades of digitalization have passed. A digital infrastructure system of public base registries is in place covering 12 base registrations. The digital infrastructure systems aim to be the foundation of:

- a government that does not ask what is already known;
- a government that is customer focused;
- a government that cannot be fooled;
- a government that knows what it is talking about;
- a government that has its affairs in order and works cost efficient.

The public base registries cover the data of citizens, companies and organizations, addresses and buildings, topographic data, cadastral data, vehicle data, income, value of real estate, and data on underground objects.

The digital infrastructure system has legal rooting in the 'Wet digitale infrastructuur'. With this law the government wants to further digitalize public administration.



The digital infrastructure system of public base registrations helps the Netherlands to effectively introduce and enhance its services for citizens.

Building a digital government has brought huge benefits. One example is the digitalized income tax for citizens that saves citizens a lot of time and effort.

However, digitalization has not always been successful. For instance many years and millions of euros have been spend in vain to improve the base registry used by municipalities to register citizens and their addresses.

In 2012 the problems associated with the digitalization of the government led to a parliamentary enquiry [Tweede Kamer 2014] that looked into the reasons some large-scale programs failed. The enquiry also investigated how this could be improved.

3. Side effects of governmental digitalization

As stated before, digitalization of public administration has brought great advantages. Accessibility of governmental services has improved drastically, new services can be introduced that focus on the individual needs of citizens.

However, in the domain of social protection, digitalization can also have negative effects. In this chapter we will look into those faults.

3.1. Regeldruk (administrative burden) and effects that put pressure on a part of the population in Dutch society

Administrative burden and shift to self service

Before digitalization of administration started in the Netherlands, administrative burden was already a theme [Van Gestel 2006] and it still is. For example, on May 15, 2019 when participating in a panel discussion the Dutch Ombudsman has stated that for a Dutch single parent with no income from work, there are seventeen different income regulations that can apply to that person.

Digitalization of public administrations has led to a shift to self-service. Citizens are requested to apply for allowances, permits and benefits online. The eligibility, duration and amount of the service allotted to the citizen is therefore more and more determined in automated processes in back offices. Support is given in online Frequently Asked Questions-sections, online Communities, online brochures, and through a help desk. Every service has its own set of rules you have to follow. And some of these are not easy to understand, because the number of exceptions is huge and not following the rules could have one perceived as willingly misleading the government, in other words, 'a fraud'.



Digital accessibility

Around 18% of the population in the Netherlands have difficulty with reading and writing [de Greef 2018]. 1.8 million employees have difficulty reading and writing and of these 1.8 million, 80% is not able to work with computers [Baay 2015]. They have difficulty in finding the right information online, find it hard to sort through online information, or find it difficult to compare services and products online and to judge trustworthiness or quality of information online. People with low literacy have less income, more debts, a higher percentage of unemployment [de Greef 2019] and as a result are depending on social protection more than others. Thus, they have to wade through digital messages and fill in digital forms more than others. All of which is difficult, if not impossible, for someone with low literacy.

One of the reasons this group has difficulties is that the processes and IT driven interaction are developed by professionals that have at least a bachelor's degree. It is not common practice that low literacy persons are involved in the analysis, designing or testing of processes and IT systems.

Since July 2018 the 'Besluit digitale toegankelijkheid' (Resolution on digital accessibility) is in effect. This resolution forces Dutch governmental organizations to design and develop software interaction that is accessible to everybody including disabled and low literacy persons. The resolution is about the design of interaction and can help those who find it difficult to interact with the government digitally. However, the resolution doesn't cover the design of the processes, so the threat of administrative burden and complexity of processes remains. Therefore, it is likely that the low literacy group that is less able to understand the digital processes likely has fewer chances than the 'digitally abled' citizens have.

3.2. Collateral damage (Fraud and error)

Fraud industry

In the Netherlands budgets for social protection are huge: 81.8 billion euros in 2019 [Tweede Kamer 2018]. The governmental systems to make the budgets land where they are needed, are vast and complex.

This vastness and complexity can also provide ample opportunity for the bold, the resourceful and the organized to commit fraud.

As a result, fighting fraud has become an industry in itself, introducing data analysis, AI, and fraud detection algorithms to the realm of government digitalization.

With data abundant and the tools to analyze this data emerging, many governments are searching for ways to benefit from these new possibilities. Fighting fraud is one of the popular areas of data analysis. In this area governments are sharing data to intercept the behavior of fraudsters who of course do not act within the boundaries of the mandate of one or two governmental organizations.

It is not always easy to distinguish fraudsters from citizens that simply or unintendedly make mistakes.

[Fenger 2013] shows that fraud is a passive delict. In over 50% of fraud cases clients of social protection systems are not aware that they are not obeying the rules. Research shows that when clients have not personally been addressed regularly by a social protection agency,



fraud cases rise because the clients have not informed the agency about changes in their life [Fenger 2013]. Mistakes of citizens and errors of the system falsely classifying people as fraudster are called false positives.

Information quality and ownership is key

In 2011 the Wetenschappelijke Raad voor Regeringsbeleid (WRR), the national government's scientific council, already warned for three developments of digitalization that ask for a high quality of information and that ask for serious consideration of the ownership of information:

- a. Network information, i.e. shared use and shared maintenance of information by actors;
- b. Combining and enrichment of information, i.e. creation of new information and profiles on the basis of different sources from different contexts.
- c. Setting up and execution of preventive and proactive policies on the basis of information, i.e. active judgement of and acting in society grounded on information-based risk assessment.

[WRR 2011]

These three developments of digitalization can obscure the source and ownership of the data that is the basis for the information that finally arrives at the user. This can increase the chance of error in decisions made on basis of the information.

Examples of the three developments

Many examples can be given of fraud fighting initiatives of Dutch governmental organizations combining all three developments stipulated above [Olsthoorn 2016]. Many of them show when the three developments of digitalization are combined, this can achieve successful results in fraud fighting. But often it is a struggle to work on information quality in order to keep the quality of the results high.

One of the government agencies that combines the three WRR developments, is the Inlichtingenbureau, a government agency that combines information of many governmental agencies to produce information that can be used by municipalities to check welfare claims or to support their citizens. Another example is the program Landelijke Aanpak Adreskwaliteit, which focuses on the correctness of registrations on addresses by combining signals of many governmental organizations. [Olsthoorn 2016] mentions twenty initiatives of the Belastingdienst (Dutch Tax administration) sharing information with other governmental organizations from many different fields like social protection, health care, or justice. Many of the initiatives mentioned [Olsthoorn 2016] are calling to act in society on the basis of information-based risk assessment in one way or another.

Examples of false positives

A possible risk of the earlier mentioned developments by Broeders, is that through lack of understanding of the information or through failing information quality, individuals can be labeled wrongly for a longer period of time [WRR 2011].

As digitalization is always a work in progress and, as stated in Chapter 2, digitalization is not always successful, error is unavoidable.

Examples of this misinterpretation and error are available in the Netherlands.



In March 2019 Dutch parliament debated about an internal report of the Belastingdienst that investigated cases in 2014. 232 families had been wrongly accused of fraud with Kinderopvangtoeslag (Childcare benefits). This had big financial consequences for the families involved. New requests for benefits in the years after 2014 were also denied to these families. As a result, parents had to give up working or studying. In many cases the families were forced to pay back benefits from previous years. This caused many families to get into further serious financial trouble because of their debts. It took the families years to solve their dispute with Toeslagen, the department of the Belastingdienst that deals with benefits. In August 2017 the Dutch Ombudsman filed a report on the cases [Ombudsman 2017]. Instances like these strengthen the claim that with digitalization a careful government is a necessity. Careful about the information and also careful about the effect of decisions based on automated information on the individual citizen.

CJIB is the government agency from the justice department responsible of collecting fines. CJIB has been very successful in their job of digitalization. Four years ago, the Dutch ombudsman got letters from pastors about parishioners in trouble and from policemen who were fed up with incarcerating single mums because they were not able to pay their debts to government. It turned out that as a result of not paying their fine, citizens where imprisoned as a hostage until they paid their fine – even if they were not able to pay. The Ombudsman concluded that annually 120.000 citizen where held hostage on request of CJIB. [Ombudsman 2015]. Since then, CJIB started to act on the situation, allowing payment in installments, phoning citizens proactively to inform them of their fines and asking them why they did not pay them. In the year 2019 it is expected that only 1.200 citizens will be held hostage as a result of the measures of CJIB.

Example of identity fraud

In a digitalized world, the possibility to act with another person's identity can be a goldmine for criminals. Centraal Meldpunt Identiteitsfraude (CMI), a Dutch organization of the Ministry of the Interior to register and aid victims of identity fraud, files a yearly monitor on their findings. 0.4% of Dutch population suffer from financial consequences of ID fraud. Some cases are severe, with people losing their mortgage, company, or job because of the allegations they suffer coming from ID fraud.

Often, victims are not believed and have difficulty proving their innocence. Also, once they are marked in governmental databases as a fraudster, this is not easily revoked.

Revoke fraudster status of false positives

The above examples show another problem with digitalization of fraud fighting. If you are perceived as a fraudster (and for instance your benefit is blocked, or you cannot obtain a VAT number, or you have been given a fine), it is not easy to revoke the consequences even if you can prove that you are a victim. The registry of your fraudster status usually oversteps the boundaries of one organization and the mandate to undo this injustice is unknown, not present or just not implemented, making the life of the victim of false positives or ID fraud difficult for much longer than necessary.



Fraud law versus taking care of citizens

In 2012, fraud fighting in The Netherlands culminated in the 'Fraudwet' (Fraud law). Its aim was to enforce fines on citizens involved in fraud with social security, thus enabling a swift civil penalty, surpassing penology. Within a year the Dutch ombudsman reported failure of the law. Research showed that many cases were a result of error and not of fraud. In many of these cases, people who were punished already had small budgets and huge debts. It seemed that as a result of this fraud law many persons who were not able to function as usual for a period of time, were automatically perceived as fraudsters. [Fenger 2013] shows that a large part of the so-called fraudsters were temporarily irresponsible because, for example, they were in a divorce, had lost a loved one, or were suffering from depression. And when they want to pick up their lives again only to find out they are labelled as a fraudster, they do not perceive the government as very caring, thus increasing the risk to fall back, or get into even deeper trouble.

This illustrates that taking care of citizens, to know their story, is important to protect the false positives. In a fully digitalized, efficient, industrialized process, governments risk underperforming in this regard, as shown in the Dutch case of the fraud law.

Government versus Citizen

If you look at developments in data analysis that are used to prevent fraud, we can see that as a result of it, the citizens have become transparent to the government. [Ombudsman 2014]. On the other hand, the same government is not always transparent to its citizens. Its information position is very complex, and the algorithms used in fraud detection are often non-transparent. [Broeders 2017] warns for the effects of the above.

'Freedom presupposes distance – a certain amount of social space between the individual and others, including supervising bodies. In the history of the modern state, distance in relation to institutions that want to observe and direct our behavior – such as the government – has brought about an increase in personal freedom. For the government, it is only citizen behavior in relation to the law that should count. In a free society, citizens are not judged according to who they are: their intentions and emotional lives have no relevance for the law. This freedom is an important dimension of their personal security. [Broeders 2017]'

The data analysis based on combined sources of data used by governments *'is an assault on the protective function of distance [Broeders 2017]'*.



Attachment 1 Literature

- Big Data and Security Policies: Serving Security, Protecting Freedom, WRR-Policy Brief no. 6, The Hague: Wetenschappelijke Raad voor het Regeringsbeleid, 2017, Broeders, D., E. Schrijvers & E. Hirsch Ballin [Broeders, 2017]
- Geen Fraudeur toch Boete, 4 december 2014, Ombudsman of The Kingdom of The Netherlands. [Ombudsman 2014]
- Doelgericht digitaliseren – Hoe Nederland werkt aan een digitale transitie waarin mensen en waarden centraal staan, 2018, Kool, L., E. Dujso, en R. van Est Den Haag: Rathenau Instituut. [Kool 2018]
- Wat is Regeldruk?, Centrum voor Wetgevingsvraagstukken, R.A.J. van Gestel (2006), Faculteit Rechtsgeleerdheid, Universiteit van Tilburg. [van Gestel 2006]
- Final report 'Parlementair onderzoek naar ICT-projecten bij de overheid', Tweede Kamer, vergaderjaar 2014–2015, 33 326, nr. 5 [Tweede Kamer 2014]
- Uitkeringsfraude in perspectief, 2013, Menno Fenger, William [Fenger 2013]
- Feiten & cijfers laaggeletterdheid, 2018, dr. Maurice de Greef, prof. dr. Mien Segers en dr. Jan Nijhuis, Maastricht University School of Business and Economics (vakgroep Educational Research & Development), Stichting Lezen & Schrijven. [de Greef 2018]
- Laaggeletterden: achterblijvers in de digitale wereld?, 2015, Pieter Baay, Marieke Buisman & Willem Houtkoop [Baay 2015]
- De tweede Europese betaaldienstenrichtlijn (PSD2) en de risico's op fraude en witwassen, 2017, Anti Money Laundering Centre (AMLC) [AMLC 2017]
- Miljoenennota 2019, vergaderjaar 2018-2019, 35000, Tweede Kamer der Staten Generaal [Tweede Kamer 2018]
- iOverheid, 2011, Wetenschappelijke Raad voor Regeringsbeleid (WRR 2011)
- Big Data voor fraudebestrijding, 2016, Peter Olsthoorn, Wetenschappelijke Raad voor Regeringsbeleid [Olsthoorn 2016]
- Geen powerplay maar fair play, august 2017, Ombudsman of the Kingdom of The Netherlands [Ombudsman 2017]
- Make It Happen!, 2017, Information Society and Government Study Group, [BZK, 2017]
- Monitor 2017, Identiteit Centraal Meldpunt Identiteitsfraude [CMI 2017]
- GEGIJZELD DOOR HET SYSTEEM Onderzoek Nationale ombudsman over het gijzelen van mensen die boetes wel willen, maar niet kunnen betalen, november 2015, Ombudsman of the Kingdom of The Netherlands. [Ombudsman 2015]



Attachment 2 author credentials

This entry on the call for submissions is written by Norbert Jansen of ICTU, The Netherlands. Norbert Jansen is an IT graduate with over 25 years of experience in digitalization at Capgemini, Post NL and ICTU. In the last 7 years Norbert was active as a consultant in the domain of Fraud and Error at various Dutch Governments.

ICTU (www.ICTU.nl) is an independent Dutch government agency. Its mission: working on a better digital government. Founded in 2001 it has been working on digitalization in programs and projects in all ministries and all layers of public administration in the Netherlands.

