**Voorwoord Hans Frankenprijs 2021**

Sedert haar oprichting in 1989 – thans zo'n 32 jaar geleden – vervult de Stichting Geschillenoplossing Automatisering (SGOA) als onafhankelijke en onpartijdige geschilleninstantie een prominente rol in het handelsverkeer bij het oplossen, beslechten en voorkomen van ICT-conflicten. Niet alleen de 'klassieke' ICT-geschillen bij stroef lopende ICT-projecten worden ter behandeling aan de SGOA voorgelegd, maar steeds ook meer de eigentijdse civielrechtelijke vraagstukken rondom het gebruik van digitale data, privacy en cybersecurity. De instrumenten die de SGOA voor het beoordelen van ICT-gerelateerde geschillen aan de samenleving aanbiedt, omvatten onder meer arbitrage, ICT-mediation, bindend advies, ICT-conflictpreventie, Rapid Conflict Resolution en het opstellen van ICT-deskundigenberichten.

Naast het uitvoeren van haar kerntaak als geschilleninstantie vindt de SGOA het belangrijk de maatschappelijke aandacht voor het raakvlak van recht en digitale technologie te stimuleren. In verband daarmee heeft het bestuur van de SGOA in 2014 de Hans Frankenprijs in het leven geroepen. Met deze prijs, vernoemd naar de emeritus-hoogleraar die gedurende vele jaren als bestuursvoorzitter het vooraanstaande boegbeeld van de SGOA was, tracht de SGOA universitaire en hbo-studenten aan te zetten tot het schrijven van een scriptie op dit terrein. Een terrein dat volop in ontwikkeling blijft. Met trots kent de SGOA in 2021 weer de Hans Frankenprijs toe, ditmaal voor de vierde keer. Een multidisciplinaire jury, samengesteld uit de kring van de aan de SGOA verbonden deskundigen, heeft daartoe met groot plezier een groot aantal lezenswaardige scripties, afkomstig van diverse onderwijsinstellingen in Nederland, beoordeeld.

Uit de inzendingen wordt in 2021 de Hans Frankenprijs met bijzonder genoegen toegekend aan de voortreffelijke masterscriptie van Anna Keuning, getiteld: *"Correcting errors within a chain network - The allocation of responsibilities of chain actors and the legal protection against chain errors from the perspective of European and Dutch law."* Anna Keuning heeft, onder begeleiding van Professor E.F. Stamhuis, haar scriptie in het kader van haar rechtenstudie aan de Erasmus Universiteit Rotterdam in 2020 afgrond.

Ketensamenwerking in de ICT is een complex verschijnsel. Het kan je als mens of organisatie diep raken als de ene instantie in een keten van instanties onjuiste of onvolledige informatie verstrekt aan een andere instantie, die vervolgens op basis van de aldus verkregen informatie een verkeerde beslissing over jou of jouw organisatie neemt. Er zijn voorbeelden te over waarin een keten van instanties, gekenmerkt door de beduidende afwezigheid van menselijke tussenkomst bij volledig geautomatiseerd genomen beslissingen, mensen of organisatie 'vermaalt'. Laat je als burger de jou betreffende gegevens bij de ene instantie corrigeren, dan is daarmee nog niet verzekerd dat ook andere partijen in de keten onjuiste informatie en beslissingen automatisch corrigeren. Het is een blinde vlek van de wetgever: zij staat van oudsher meer stil bij verantwoordelijkheden van individuele instanties en bedrijven, dan bij die van ketens van organisaties.

In haar omvangrijke en goed gedocumenteerde juridische studie onderzoekt Anna Keuning dit verschijnsel diepgaand. Het grote maatschappelijk belang ervan is evident. Zo geeft zij bijvoorbeeld gedegen aandacht aan de vraag op welke wijze de Algemene Verordening Gegevensbescherming protectie tegen ketens van instanties aan burgers zou kunnen geven, bijvoorbeeld langs de lijnen van 'joint controllers'. De beschouwingen en visies die Anna presenteert zijn meer dan de moeite van het lezen waard. Ook andere juridische invalshoeken komen sterk aan bod, zoals het administratieve recht en de civielrechtelijke bescherming vanuit de onrechtmatige daad. Haar conclusies zetten aan tot passende vervolgstappen.

De jury van de Hans Frankenprijs 2021 spreekt haar grote waardering uit voor de bijdrage die Anne Keuning met haar Rotterdamse master-scriptie heeft geleverd aan het maatschappelijke en juridisch debat over de ICT-ketenproblematiek. Haar werkstuk smaakt naar meer en de jury hoopt daarom op nader onderzoek. De jury feliciteert Anne van harte met het winnen van deze meer dan welverdiende prijs.

Heemstede, najaar 2021

De Jury van de Hans Frankenprijs 2021

**Master Thesis**
LL.M International and European Public Law

# Correcting errors within a chain network

## *The allocation of responsibilities of chain actors and the legal protection against chain errors from the perspective of European- and Dutch law*

**ERASMUS UNIVERSITY ROTTERDAM**

Word Count (19667 including footnotes):
Student name: Anna Keuning
Student Number: 553100
Supervisor: prof. E.F Stamhuis

Date: 30 June 2020

## Index

## Introduction

Efficiency, cooperation and automation. Three key ingredients that are rapidly changing the way we interact with public bodies, how they interact with each other and how they operate. Today, it is well known that computers are a lot quicker than us when it comes to processing information, making calculations and generating outcomes. These benefits have been acknowledged and embraced by the public administration as well. A lot of administrative decisions, especially decisions with a financial character are no longer taken by civil servants anymore.[1] Decisions are data driven. Legislation is transformed into a set of algorithmic rules created by software developers that enable computers to make automated decisions. A few examples of Dutch entities that are highly automated are the Employee Insurance Agency *(*UWV*)*, the Dutch Tax and Customs Administration, (Belastingsdienst) and the Central Student Finance Directorate of the Ministry of Education, Culture and Science *(*DUO*)*. Every year, these bodies decide on millions of transactions, allowances and loans. In the exercise of their tasks, they collect massive amounts of personal information. An additional benefit of the deployment of information technology is that it possible to store all the collected data. This makes it also feasible to exchange that data. Efficiency considerations have led to an increased cooperation between several public bodies to exchange data they store amongst each other. In many occasions, persons and companies will only have to provide a certain set of personal data once, after which it will be used for multiple other goals by different bodies. This working method is believed to be more customer friendly and is also better from an informational standpoint as data only has to be included correctly into the system once.[2] As a consequence, the tasks of the employees of these public organizations have shifted: employees are no longer concerned with making decisions in the individual cases by weighing the several interests, their job focuses now on the optimization of the information processes and towards linking the information with other agencies. Bovens & Zouridis describe this development as going from *street-level* bureaucracies to *system-level* bureaucracies.[3]

[1] B.W.N. de Waard (red.), *Ervaringen met bezwaar,* Den Haag: Wetenschappelijk Onderzoek- en Documentatiecentrum (wodc) 2011 p. 43.
[2] WRR, *IOverheid,* Amsterdam: Amsterdam University Press 2011, p. 11-12.
[3] M.Bovens & S.Zouridis, 'From Street-Level to System-Level Bureaucracies: How Information and Communication Technology Is Transforming Administrative Discretion and Constitutional Control', *Public Administration Review*, vol 62 no. 2, p. 175-177.

In extent to this, the development can defined as chain informatisation: a process in which infrastructures are built to effectively transfer data in an organizational network.[4] In this way, public bodies do not have to gather all the information they need separately, they can make use of the data that is available to them in a network of chain partners. A result of this cooperation is that administrative decisions are now dependent on the data input of their own and of the other chain partners. Subsequently, decisions built upon each other. These interconnected decisions are referred to as chain decisions. An important characteristic of a chain is that there is no formal hierarchy between the several partners. In addition, the actors do not necessarily have to pursue the same aims.[5] This basic premises of chain cooperation can cause friction, because on the one hand actors within the chain operate as separate actors and emulate their own aims, but on the other hand their behaviour influences the chain because of their dependency relationship. This raises questions with regard to the responsibilities they bear, especially when processes within the chain go wrong. Errors are unavoidable. Information that travels through a chain network can be incorrect. Problems can arise due to several factors: the input information can be wrong, algorithmic rules can generate the wrong outcomes or they can be programmed in an erroneous way, for example because the legal rules were transformed into the algorithm incorrectly. Algorithms are not perfect and not neutral, and it is not that easy to sufficiently translate legal rules into 'black-and-white' computer language. As Van Eck describes it, a computer cannot do anything with legal terms that leave room for interpretation such as ''equity and reasonableness''. Computers operate in yes or no language which can result into harsh and unjust outcomes for the applicants that are faced with chain decisions.[6]

Applicants can face various troubles due to errors in a chain. A frequent problem is the difficulties people have to deal with when other people are incorrectly registered at their address. The wrong address registration can lead to applicants not being able to get certain allowances. They can also be faced with numerous erroneous bills or fines because their address is used to commit address fraud for instance.[7] A painful example that chain errors can cause very serious consequences for an applicant is the *Dolmatov*-case. Dolmatov was a

[4] J.H.A.M. Grijpink, *Keteninformatisering met toepassing op de justitiële bedrijfsketen* (diss. Eindhoven), Den Haag: SDU 1997, p. 5.
[5] T. Oosterbaan, *Architectuur als agenda. Een theoretische en empirische analyse van de rol van frames bij architectuurontwikkeling voor keteninformatisering* (diss. Rotterdam) 2012, p. 12; B.M.A van Eck, *Geautomatiseerde ketenbesluiten en rechtsbescherming (*diss. Tilburg*)* 2018, p. 44-45.
[6] Van Eck 2018, p. 189, 194-195.
[7] H.Eikenaar, 'De hardnekkige spookbewoner is groot probleem voor gemeenten', (bd.nl 2018, last accessed 23 June 2020).

Russian activist that had moved to the Netherlands, but his application for asylum was denied. His lawyer filed an appeal to this decision, but this was not included in the system of the Dutch Immigration and Naturalisation Office (IND). As a consequence, the IND registration in the system indicated incorrectly that Dolmatov resided illegally in the Netherlands and that he could be ‘’removed’’. When later, Dolmatov came into contact with the police because of suicidal tendencies, the police unjustly put Dolmatov in a deportation centre where he ultimately committed suicide.[8]

When errors travel through a chain network and are used by other bodies for their own decisions, the question arises: for what part of the chain cooperation should actors bear responsibility? Can they be held responsible if they use data of other chain partners, that turns out to be wrong? Is there a certain degree of joint responsibility for all the actors to make sure the chain is operable, and errors are corrected chain-wide? In this thesis, I will investigate the responsibilities chain actors bear amongst each other, when these types of problems arise. When an applicant is faced with an error of the chain that is a product of chain cooperation, his legal position to contest the error and get his damages compensated is mainly determined by two legal regimes. While the processing activities between the various chain actors are the necessary oil that fuel the chain and make it possible to create chain decisions, the General Data Protection Regulation (GDPR)[9] is important as it protects the data rights of the data subjects. The GDPR is directly applicable European law and offers a liability scheme for when data protection rules are breached by the actors that process the personal data. Secondly, when the chain error has resulted into an administrative decision, the applicant has the right to revise this decision and to get it corrected, on the basis of Dutch administrative law in front of the administrative court. As a complementary safety net, the applicant can claim damages under Dutch civil law for torts committed by the government that cannot be contested via administrative law. This relates to the protection of torts committed by public bodies on the basis of their factual acts.

The main research questions read as following:

1. Is the responsibility of the actor limited to the own link in the chain, even when errors are caused by others or errors have only negative effects further down the chain?

[8]AD 12 april 2013 ‘Overheid handelde onzorgvuldig in zaak Dolmatov’, https://www.ad.nl/binnenland/overheid-handelde-onzorgvuldig-in-zaak-dolmatov~a45e2b23/?referrer=https://www.google.com/

[9] Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, repealing Directive 95/46/EC (General Data Protection Regulation) OJ L119/1.

2. Does the legal system offer effective remedies to persons/companies that are in trouble as a consequence of an error somewhere in the chain?

*Sub questions:*

-Under what conditions can chain actors be defined as joint controllers under article 26 GDPR?

-How far does the responsibility of chain actor reach on the basis of the GDPR?

-What remedies does the GDPR offer an applicant?

-How far does the responsibility of a chain actor reach in Dutch administrative law?

-What remedies does Dutch administrative law offer an applicant?

-How far does the responsibility of the chain actors reach in Dutch civil law?

-What remedies does Dutch civil law offer an applicant?

**Methodology**

For this thesis, I will use the method of legal doctrinal research. Legal doctrinal research focuses on a systematic and critical analysis of the sources that constitute and interpret the law and legal concepts. The main sources of this type of analysis are legal texts, court rulings, law textbooks and journals. The goal of doctrinal research is to rearrange the available legal sources, make connections between the various rules and try to present the system as a coherent set of principles, by logically ordering the various legal principles and propositions. In this way, relationships between various rules can be assessed, certain difficulties can be explained or potential gaps in the system can be revealed. In order to obtain this goal, first the various relevant sources need to be positioned. After that, the various sources require legal interpretation, with the use of deductive, and inductive reasoning, and reasoning by analogy. After that, the researcher is able to draw normative conclusions from this synthesis.[10]

The goal of this research is to get a better view of the legal situation with regard to the responsibilities of chain actors when errors flow through a chain network. In extent to this, it will be examined how the legal system offers protection to third parties that are faced with problems due to errors of the chain. Therefore, it is necessary to get a picture of all the relevant legal schemes that influence the legal position of the chain actors and the third parties that face the consequences of their errors. In this case, it requires investigation of the GDPR,

[10] T. Hutchinson & N.Duncan, 'Defining and describing what we do: doctrinal legal research', *Deakin Law Review* 2012, vol 7 no. 1, p. 83-120.

Dutch administrative law and Dutch civil law. By making this assessment, it can be revealed how far responsibilities of chain actors reach and whether there might be certain gaps with regard to these responsibilities. In addition, the analysis opts to reveal whether there are gaps and in effective legal remedies to receive protection for chain errors.

In the first chapter, I will assess when and whether chain networks can be defined as a situation of joint control under the GDPR and if so, what the consequences of this legal definition are with regard to the responsibilities of the chain partners. In addition, I will discuss what type of protection the GDPR could offer to the applicants that suffer damages due to the chain errors and also what the limitations of the GDPR are in relation to this. For the sake of this investigation, I will use sources of European law, such as the legal text of the GDPR, the case law of the European Court of Justice (CJEU), guidelines of advisory bodies such as the Article 29 Working Party and European Journals. In the second chapter, I will investigate how administrative chain decisions are defined in Dutch administrative law and how far the responsibilities of chain partners reach when they base their administrative decisions on data that is derived from another public body. In this way, I will assess how the applicant is protected against chain errors in front of the administrative court and how the errors are opted to be solved. For this examination, I will use legal sources of Dutch administrative law, such as case law of the Dutch administrative courts, handbooks of administrative law and also the thesis of Van Eck, in which she extensively investigated legal protection in relation to chain decisions. In the third chapter, I will assess whether Dutch civil law could offer complementary protection for chain errors that do not constitute an appealable administrative decision for the applicant. I will look at how the liabilities of chain partners can be influenced if we look at it from torts committed in a multi-actor scenario on the basis of article 6:166 of the Dutch civil code. The main sources that are used for this investigation are handbooks and dissertations that concern Dutch torts law, and also handbooks that are specialized in torts committed by the government. From these findings, I opt to draw the complete combined scheme of responsibilities of chain actors when errors travel through the chain and the scheme of protection where citizens/companies can rely on when they suffer damages/problems from this chain error. In this way, I will assess whether the current legal scheme puts a sufficient level of responsibility on the various chain actors to ensure effective and complete protection against chain errors.[11]

[11] In this thesis, I will use the reference system of the *Leidraad*.

## Chapter 1: Responsibilities and legal protection of chain errors under the GDPR

### 1.1 Introduction

In this chapter, I will examine whether data chains can be qualified as joint control under article 26 of the GDPR and what this qualification means in terms of their responsibilities and the legal protection for chain errors. The General Data Protection Regulation went into force in 2018 and has revised and harmonized the European Data Protection rules. The regulation has direct effect in all the EU Member States and opts to create a same level of protection to data subjects when it comes to the processing of their personal data EU-wide.[12] This means Member States may not deviate from the GDPR articles unless the GDPR explicitly grants this discretion. Article 26 GDPR is a provision specially devoted to joint control newly introduced by the GDPR.[13] According to article 26 GDPR, joint control refers to the situation in which two or more controller jointly determine the purposes and means of the processing activities. While the special scheme dedicated to joint controllers is new, the provision can be seen as a codification of an earlier existing legal concept. Under the Data Protection Directive (DPD), the predecessor of the GDPR, joint control was already acknowledged and developed by the Article 29 Working Party (WP29)[14] and the European Court of Justice (CJEU).[15] In addition, the GDPR still handles the same scheme which distinguishes between the roles of controllers and processors to allocate their responsibilities.[16] Controllers are qualified as the main operators that make the essential decisions with regard to processing the data and carry the main responsibility to comply with the GDPR. The processors carry out processing

[12] Recital 10,11 of the GDPR.
[13] Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, repealing Directive 95/46/EC (General Data Protection Regulation) OJ L119/1.
[14] The Article 29 Working Party is an independent advisory body of the European Union, which aims to contribute to the consistent application of the European Data Protection rules EU-wide. The Article 29 Working Party is now replaced by the European Data Protection Board (EDPB). All national DPA's have a seat in the EDPB.
[15] B. van Alsenoy, 'Liability under the EU Data Protection Law: from Directive 95/46 to the General Data Protection Regulation' *Jiptec* 2016, vol. 3, p. 272.
[16] Article 29 Working Party, 'Opinion 1/2010 on the concepts of ''controller'' and ''processor'', 2010, p. 4.

activities on behalf of the controller and therefore carry less responsibilities than controllers. First, I will examine how controllers and processors are defined by the GDPR. Thereafter, I will discuss under what conditions a situation of joint control is established and whether chain network can be defined as joint control. Then, I will assess some of the novelties and new obligations the GDPR has introduced with regard to joint control and the new liability scheme of controllers and processors. After that, I will consider the limitations of the GDPR in relation to protection against errors from a chain. As the definition of joint control was predominantly developed before the enforcement of the GDPR, I will also use sources from when the DPD was still in force.

### 1.2 Controllers versus processors

Controllers are described by the GDPR as the actors determining the ‘’purposes and means’’ of the processing activities.[17] According to the WP29, controllers should be defined with a functional and factual approach. The legal status of the entity is irrelevant, and the concept has its own independent meaning in Community law to increase effective protection of data protection rules. To assess whether an actor is a controller, one should first look at the specific processing operations and ask: ‘’Why is the processing taking place?’’ ‘’Who initiated it?’’. Even if an actor is formally, for example by means of an arrangement, designated as a processor, this is not decisive in the assessment. If the actor acts a controller on the basis of the factual circumstances, he will be qualified as one.[18]

Defining the purposes and means relates to determining the necessary organisational and technical measures with regard to the substantial ‘’why and the how’’ questions of the *essential elements* of the processing activities. It relates to essential questions such as: ‘’Who will have access to the data? For how long can it be stored? When shall data be deleted?’’[19] The determination of the non-essential elements can be delegated to processors. An example is choosing the required hardware and software to take security measures.[20]

Processors are defined by pursuing processing activities based on a certain designated competence that was granted to them by a controller. A processor has to implement the instructions that are given to him by the controller, at least with regard to the essential means of the processing.[21] Therefore, the lawfulness of the processing activities by the processor

[17] Article 4(7) GDPR.
[18] Article 29 Working Party 2010, p. 9.
[19] Article 29 Working Party 2010, p. 14.
[20] Article 29 Working Party 2010, p. 15; EDPS 2018, p. 9.
[21] Article 4 (8) GDPR.

depends on the mandate that was given to him. This mandate can be given to a processor in various forms, by means of law or an arrangement. However, this does not mean that there can be no processor/controller relation without a prior contract. Again, a functional approach is handled to assess whether such a relationship exists.[22] If the processor acts outside of the mandate that is given to him, he will become a controller as well. In extent to this, the qualification of the processor is determined by the concrete activities it pursues and not by its legal status. Therefore, the same entity can simultaneously act as a processor with regard to certain processing activities on behalf of a controller and as a controller for other processing activities.[23]

## 1.3 The definition of joint control

### *1.3.1 Guidance of the Article 29 Working Party*

A situation of joint control occurs when two or more controllers determine to some extent the purposes or means of the processing activities together. Just as with defining a single controller, a situation of joint control should be determined in light of the real, factual circumstances. Arrangements between the parties can be useful but are again not decisive for this determination. The legal status of the actors is also irrelevant.[24] According to the WP29, joint control does not have to mean the controllers share all the purposes and means and determine these with equal influence. The concept can refer to various forms of pluralistic control, taking place in different combinations and forms. At one end of the spectrum there can be a very close relationship between the actors where all the purposes and means are shared, and on the other end there is the looser relationship, where only a part of the purposes or means are shared or where the cooperation is only limited to certain processing stages. Not being able to fulfil all the obligations separately from the other controllers, is not a condition to be qualified as a co-controller.[25] In more recent Guidelines, the European Data Protection Supervisor (EDPS) added that it also irrelevant whether all the involved parties have factually determined the purposes or means. Decisive is whether the actor, by entering into a specific arrangement with the other parties, was hypothetically able to influence the ‘’how and why’’ of the jointly controlled processing activities.[26]

[22] Article 29 Working Party 2010, p. 26-27.
[23] Article 29 Working Party 2010, p. 25-27.
[24] Article 29 Working Party 2010, p. 22.
[25] Article 29 Working Party 2010, p. 19.
[26] European Data Protection Supervisor, ‘EDPS Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/725’, 2018, p. 23. Although the EDPS guidelines are specifically aimed towards helping European Institutions, the guidelines are also be useful for national private and public

The mere fact that controllers exchange data through a chain, does not automatically have to mean the parties are joint controllers. However, this changes if the partners decide to set up an infrastructure to pursue their own individual or shared purposes. When the controllers decide on the essential elements of this infrastructure, they can become joint controllers, even if they use the data for their own purposes at their micro-level or if the several actors collect data for one purpose at the end of the chain. Therefore, the WP29 advocates that by assessing whether there is a situation of joint control, the micro-level and the macro-level dimension of the processing activities should be checked. While at the micro-level of the chain the activities can appear to be disconnected, the macro-level can reveal that the activities are a part of a lager ''set of operations''. A general level of unity with regard to the purpose of the chain can be sufficient to trigger joint control.[27] An example that is given of such a macro-level joint control situation is setting up an infrastructure like an E-government platform. While each public body is the controller of its own public administration and uses the data for its own purposes, the transfers of the data for further purposes between the bodies and citizens form an essential part that enables the actors to pursue their own activities. As a result, controllers of E-government platforms have to make sure the transfer of the data to the public administration is secure and operable. The WP29 stresses that the platform in itself, can also become a controller if this platform facilitates the data transfers, stores data and manages data requests.[28] Another example the WP29 gives is the use of financial service providers like SWIFT by banks in order to carry out financial transactions. At first glance both actors seem to pursue their own aims with regard to the transactions. However, when looked at it from the macro-level, the different phases of the transactions can be closely linked to each other.[29]

### *1.3.2 CJEU case law*

The CJEU handles the same functional approach to define joint control that is advocated by the WP29 and has even extended the definition of the concept further in the case *Wirtschaftakademie*. The case concerned a German private school that had created a fan page on Facebook. The visitors of the fan page did not receive notifications of the fact that Facebook placed cookies on the visitors' devices. This led to a breach of data protection

bodies as the basic explanations of the GDPR principles and matters such as controllers, processors and joint control are the same for all entities.

[27] Article 29 Working Party 2010, p. 20; EDPS 2018, p. 23.

[28] Article 29 Working Party 2010, p. 21.

[29] Article 29 Working Party 2010, p. 20.

rules.[30] The German Data Protection Authority demanded the private school to deactivate the fan page site. The school contested this decision and argued that it could not be seen as a controller, which led to the German Court making a preliminary reference to the CJEU to answer this question.[31] The Advocate General (AG) argued that the school could qualify as a controller, for three main reasons. Firstly, the school chose to use Facebook as a platform to create the fan page, which enabled Facebook to collect the specific data. Secondly, the school could also influence how Facebook would collect data, by choosing certain filters to determine to whom the fan page would be shown.[32] According to the AG, this entails de-facto influence on the processing activities of Facebook. Thirdly, he argued if the school would not be qualified as a controller, that evading liability would become too easy.[33] The CJEU agreed with the reasoning of the AG and added that this broad definition of the controller is necessary to ensure the effective and complete protection of the rights of data-subjects. The CJEU added to that it is also relevant to examine who is benefitting from the processing activities when determining whether an actor qualifies as a controller.[34] According to the Court, recognizing joint control can contribute to more complete protection of data subjects, in accordance with the requirements of data protection rules.[35]

What is interesting about this case, is that the page administrator had no factual influence on how Facebook placed cookies and how the social media platform notified this to its visitors. Facebook is the only actor that determines how the platform works and how the system can be used. Thus, the administrator was unable to the determine the ‘’why and the how’’ of the macro-level processing activities of Facebook. However, in this case the CJEU did not look at the broader macro-level set of processing activities by Facebook. The Court zoomed in on the set of individual processing activities that were taking place at the micro-level of the fan page. While the micro-level activities of the administrator influenced the way in which the data were collected, a situation of joint control occurred.[36] The WP29 stipulated that with joint control, extra attention should be put on the assessment whether at the macro-level, the activities become a set of operations that are jointly controlled. The CJEU has

[30]CJEU 5 June 2018, Case C-210/16 EU:C:2018:388, (*Wirtschaftsakademie Schleswig-Holstein* ), para 15.
[31] CJEU 5 June 2018, Case C-210/16 EU:C:2018:388(*Wirtschaftsakademie Schleswig-Holstein),* para 16.
[32] CJEU 5 June 2018, Case C-210/16 EU:C:2018:388 (*Wirtschaftsakademie Schleswig-Holstein*) Opinion AG Bot para 59.
[33] CJEU 5 June 2018, Case C-210/16 EU:C:2018:388(*Wirtschaftsakademie Schleswig-Holstein)* Opinion AG Bot para 74.
[34] CJEU 5 June 2018, Case C-210/16 ECLI:EU:C:2018:388 (*Wirtschaftsakademie Schleswig-Holstein*), para. 40.
[35] CJEU 5 June 2018, Case C-210/16 EU:C:2018:388, (*Wirtschaftsakademie Schleswig-Holstein)* paras 28, 42.
[36]R. Mahieu, J. van Hoboken & H.Asghari, ‘Responsibility for Data Protection in a networked world. On the question of the controller and effective and complete protection and its application to data access rights in Europe’, *Jiptec* 2019, vol. 10, p. 93.

expanded this vision and added that although actors may not even have determined the purpose and means of the macro-level activities, if their own micro-level activities influence the processing activities in some kind of way, a situation of joint control can be established as well. This broad definition of the controller was confirmed in the cases *Fashion-ID* and *Jehova's Witnesses*, where the Court added that to qualify as a controller, there is no condition that the actor needs to have factual access to the relevant data it controls.[37]

The CJEU remained vague in the *Wirtschaftakademie*-case when it comes to the allocation of the responsibilities when data is jointly controlled. According to the CJEU, the responsibilities of Facebook and the fan page administrator, should be assessed in light of the relevant factual circumstances.[38] Some guidance of this allocation can be derived from the *Google-Spain*-case, where the CJEU concluded that the allocation of responsibilities amongst the controllers should be limited by assessing their factual powers, responsibilities and capabilities to make sure data protection rules are complied with.[39] Mahieu, Van Hoboken and Asghari argue that this comment can be interpreted in two ways: it could mean that a controller is liable for the damages it is able to prevent without proper coordination between the controllers. It can also be interpreted in a stricter way; it could entail that controllers have to make sure that whenever they are able to prevent certain damages from occurring, they should to do so by making sure they persuade their joint controller(s) to act in line with the data protection rules or by not implementing the infringing services.[40]

### *1.3.3 Joint control and chain cooperation*

As joint control is a very broad concept defined on the basis of the factual circumstances, chain partners setting up an infrastructure to exchange data amongst each other will quite easily be conceptualized as joint control. Even though the actors of a chain network use the data for their own micro-level purposes and make decisions that can look as if they are disconnected prima-facie, when the chain cooperation is looked at from the macro-level view, it reveals that the data transfers and the decisions that derive therefrom are part of a larger ''set of operations''. This new infrastructure forms an essential part of the processing activities as it enables all the actors to pursue their own micro-level aims or for a certain aim at the end of the chain. With setting up the infrastructure, it is not necessary that all the parties

[37] EDPDS Guidelines, p. 10; CJEU 10 July 2018, Case C-25/17 ECLI:EU:C:2018, (*Jehovan todistajat)* paras. 68 to 72; CJEU 29 July 2019 Case C-40/17 ECLI:EU:C:2019:629 (*Fashion-ID).*
[38] CJEU 5 June 2018, Case C-210/16 EU:C:2018:388 (*Wirtschaftsakademie Schleswig-Holstein*) para 43.
[39] CJEU 13 May 2014, Case C-131/12 EU:C:2014:317 *(Google-Spain)* paras 38, 83.
[40] Mahieu, Van Hoboken & Asghari, *Jiptec* 2019, p. 96.

had an equal say in how this infrastructure would be designed and works. In the broad view of the CJEU, even parties that had no say at all in determining the purposes and means of the macro-level activities can be dragged into the scope, if they influence the processing activities with their own micro-level behaviour. As a result, chain partners will be jointly liable for damages due to the chain activities and will have to allocate their responsibilities amongst each other in line with article 26 GDPR. It should be noted that the chain partners do not necessarily have to be public bodies. While the legal status of the actors is irrelevant, private parties that are involved determining the purposes and means in the chain will also be dragged into the definition of joint control.

## 1.4 Novelties under the GDPR

### *1.4.1 Setting up an arrangement to allocate responsibilities*

In this paragraph, I will discuss the new features the GDPR has introduced with regard to joint control. According to article 26(1) GDPR, controllers are free to decide how they allocate their responsibilities, as long as full compliance with the GDPR is secured. This allocation has to be provided by an arrangement. The arrangement is not necessary if responsibilities are fully allocated by means of legislation. If the law leaves open certain gaps in relation to their responsibilities, a complementary arrangement has to be set up that fills these gaps.[41] The essence of the arrangement has to be communicated to the data subjects via a data notice (26(2) GDPR). The essence of the arrangement shall communicate to the data subject how the responsibilities of the multiple controllers are divided. The main goal behind this notice is that that data subjects will easily be able to know whom of the controllers to address first in case he wants to exercise his rights. The controllers can choose to create a shared notice, but they can also choose to each handle a separate notice.[42] This arrangement may also assign a central contact point to the data subject. The EDPS encourages parties to assign a central contact point to make the communication for the data-subject easier, but stresses that this does not take away the obligations of all the controllers to enable the subject to contact them separately to exercise their rights, especially with regard to the request for access, erasure or a restriction of the data.[43]

A new restriction introduced by the GDPR when it comes to the legal effects of arrangements allocating responsibilities, is that these arrangements cannot be held against the data subject when he exercises his rights. In the draft of the GDPR, the Council proposed to

[41] EDPS 2018, p. 27-28.
[42] EDPS 2018, p. 29.
[43] EDPS 2018, p. 30; article 16-18 GDPR.

limit the liabilities of the controller's vis-a-vis data subjects if the arrangement clearly reflected the allocation of their responsibilities. This would mean the data subject would have to take into account the arrangement when exercising its rights and claiming damages. This amendment was not accepted. The Commission and the Parliament found that this would lead to the undesirable situation where the data subject would be burdened with the rather difficult task to investigate which of the controllers ultimately had caused the damages. This means that once the data subject has proofed that there is an infringement of its data protection rights, he will not have to proof which one of the actors contributed to the infringement. After the damages are paid, the actors have to deal with this allocation of accountability internally. In conclusion, the arrangement to allocate responsibilities has only internal legal effect between the several actors.[44]

*1.4.2 The cumulative liability scheme of article 82 GDPR*

Article 82 of the GDPR offers a cumulative liability scheme which prescribes that any controller or processor, involved in the relevant processing activities (2), can be held severally liable for the entire amount of damages in order to ensure effective and complete protection of the data protection rules (4). While under the DPD, the controller was the designated actor that was liable for the damages that resulted from data protection breaches, processors can now be held liable under certain conditions as well. In the draft of the GDPR the Commission proposed that the mere involvement of processors would be sufficient to establish their liability. Subsequently, the Council amended the text and wanted to maintain a more clear divergence between the respective roles and responsibilities of the controllers and the processors.[45] To hold processors liable, a second condition was added: there needs to be additional proof that the processor has breached instructions of the controller or that it has breached GDPR-obligations that are specifically addressed to him. The GDPR has created an increasing number of new obligations for processors, such as the duty to notify data breaches to the controller (28 GDPR) and the duty to secure the processing activities (32 GDPR).[46] As

[44] European Commission, 'Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) -Preparation of a general approach', 2012/0011 (COD), 9565/15, p. 291; Van Alsenoy *Jiptec* 2016, p. 287.

[45] European Commission, 'Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) -Preparation of a general approach', 2012/0011 (COD), 9565/15, p. 185; Van Alsenoy *Jiptec* 2016, p. 285.

[46] Van Alsenoy *Jiptec* 2016, p. 284.

soon as this additional circumstance is established, their degree of responsibility or personal fault is irrelevant to hold them fully liable.

Thus, the controller still remains the actor that carries the primary responsibility of compliance. All the joint controllers involved in the processing activities can held liable by the data subject, due to the fact that their arrangement to allocate responsibilities of article 26(3) cannot be held against the data subject. The liability of article 82 GDPR is a strict one. Once the infringement of data protection rules is established, the controller or processor cannot evade liability simply by stating there was an absence of personal fault.[47] According to article 82(3) the only way to evade liability, is if the controller or processor can proof that the he is not in any way responsible for the damaging event. This exemption has a very tight scope and exclusively refers to event that occurs beyond their control, or in other terms: to a situation of *force majeure.* Force majeure relates to abnormal situations which could not be prevented by any reasonable measures and which does not entail the realization of risks that the party is strictly liable for.[48] When the controller or processor has paid the full damages, he is entitled to claim back a part of this compensation of the other involved controllers/processors in line with their part of the responsibility of the damage on the basis of article 82(5) GDPR.

### 1.5 GDPR limitations with regard to complete and effective chain protection

While the GDPR provides a liability scheme that has the potential to offer the data subject sufficient protection when it comes to claiming damages and offers a concrete allocation of the responsibilities of chain actors, the problem is that the applicant may need other remedies to get adequate protection from failures of the chain. When an applicant is faced with an error from the chain, the most important goal can be to stop these activities so that the error cannot cause more negative consequences by contaminating other chain decisions in the future. If an applicant for instance is constantly faced with multiple erroneous administrative fines due to a chain error, his biggest interest will be to put an end to this.[49] The GDPR does not explicitly demand that Member States should put certain specific judicial correctional remedies in place, besides the liability scheme of article 82 GDPR. It is not prescribed that the applicant should be able to judicially enforce that the error is fixed chain wide to put an end to the ongoing problems he faces from the error. Based on the principle of national procedural autonomy, a

[47] Van Alsneoy, *Jiptec* 2016, p. 282.
[48] Van Alsenoy *Jiptec* 2016, p. 283.
[49] A good example that the interest to put an end to the error can be the most important is the *Romet*-case, that I will discuss in Chapter 2.

Member State is free to determine the conditions of the national procedural rules and to establish how the applicant will receive legal protection as long it ensures the principles of effective an equivalent application of EU law. National law may not obstruct the effective application of EU law and also not treat EU remedies less favourable.[50] Thus, how the applicant will exactly be protected and what remedies are offered to him will depend on the procedural choices of the national legal system he seeks protection from.[51]

A second limitation of the GDPR is that it can only offer protection to the extent of infringements of data protection rules.[52] Errors in chains can also be caused for reasons that lay beyond matters of data protection, when a law is not sufficiently interpreted, implemented or carried out within the system for instance. If the Dutch Tax and Customs Administration does not correctly calculate the taxable income of an employee due to a mistake in tax legislation or a wrong algorithmic translation of a tax rule for example, this does not constitute a GDPR breach while nothing is wrong with the processing activities of the personal data of the applicant *an sich*. However, the inclusion of the taxable income in the Key Register of Incomes (BRI) can have negative consequences for the applicant. The application for a student loan or the application to get certain allowances for example can be influenced while other public bodies base their decision partly on the taxable income.[53] If the applicant faces troubles because the student loan or the allowances are denied or calculated at a lower sum of money for example, the applicant will not be able to rely on the GDPR.

### 1.6 Conclusion

Joint control is a very broad legal concept that refers to the situation in which controllers to some extent share purposes and means with each other. The main reason that the concept is approached broadly, is to make sure the data subject can effectively exercise his rights under the GDPR and thus to prevent gaps in responsibilities, gaps in protection and gaps in GDPR-compliance. The cooperation between the controllers can have many varying forms and has to be assessed in light of the factual circumstances. Important is that for the establishment of a joint control relationship, all the processing activities of controllers should be assessed from a macroscopic and a microscopic view. With the determination of chain networks as joint control, it is very important to make this distinction. It may seem at first hand that controllers

[50] CJEU 7 July 1981, Case 158/80 ECLI:EU:1981:163 (*Rewe-Handelsgesellschaft Nord mbH v Hauptzollamt Kiel*) para 41.
[51] Van Alsenoy, *Jiptec* 2016, p. 288.
[52] Recital 14 of the GDPR.
[53] Van Eck 2018, p. 317-321; article 21 AWR; article 8 AWIR; article 1 Wet op Studiefinanciering 2000 (''*Student Finance Act''*)

of a chain, act independently from each other because they use the exchanged data to achieve their own separate aims. However, if they choose to utilize a certain infrastructure to enable this, this infrastructure in itself becomes a crucial part of the processing activities that are carried out by the multiple controllers. As a result, the infrastructure becomes a ‘’set of operations’’ at the macro-level. All the controllers that use this infrastructure, will be obliged to make sure data the transfers are save and operable. As soon as a data chain can be qualified as joint control, the parties will have to allocate their responsibilities via an arrangement, insofar this allocation has not been established by law. For the sake of the complete and effective protection of the data subjects, the European legislators chose not to burden the data subject with the duty to assess which one of the controllers it has to address to exercise its rights and to examine which controller has ultimately caused damages. This means the internal arrangement between joint controllers only affects their internal relations. It creates no legal effects for the data subjects. When an infringement of data protection rules is established, article 82 GDPR stipulates that all the controllers and the processors that are involved in the processing activities can be held severally liable for the full amount of damages. New to the scheme is that processors can also be held liable, under the additional condition that the processor has ignored instructions of the controller or has breached GDPR obligations that are specifically addressed to him. Once the full amount of damages is paid, the actor can claim back the part of the compensation that have to be borne by the other actors based on their joint responsibilities. While the GDPR offers a clear allocation of responsibilities of joint controllers vis-à-vis the data-subject which should make it easier to claim compensation, this does not directly mean problems will be solved when an applicant is faced with an error of the chain. A judicial remedial sanction to enforce correction throughout the chain is not offered by the GDPR, which means it remains unclear how the applicant can make sure errors are corrected chain wide. This will depend on the national procedural rules of the Member State. In addition, the GDPR can only offer protection for chain failures that concern data protection breaches.

## Chapter 2: Responsibilities and legal protection of chain errors from a Dutch administrative law perspective

### 2.1 Introduction

In this chapter, the legal position of the individual addressee of a chain decision will be looked at from the perspective of administrative law. This perspective is necessary, while the legal protection of the individual is determined by a combination of directly applicable European law and Dutch administrative law. Chapter 1 stipulated that the data that is processed in the chain has to meet the requirements the GDPR sets out. Infringements of the GDPR will result in liability of the relevant actors involved in the chain. Secondly, the ultimate administrative decisions that derive from the chain are contestable via administrative law for the addressee of the decision. If the decision turns out to be incorrect, the decision can be revised. If an applicant suffers damages due to an administrative decision that is incorrect, the applicant also has the right to get the damages repaired. The liability scheme for torts of public bodies in Dutch administrative law, handles the same basic material conditions that are developed in Dutch civil law, which means there needs to be a tort, this tort needs to be attributable to a public body, there needs to be a causal link between the tort and the damages and lastly and the norm should aim to protect the applicant. Through the years, administrative courts have adopted these conditions of the civil court when determining the liability of a public body in case of an appealable decision.[54] In this chapter, I will examine how erroneous administrative decisions that derive from chains are approached from the perspective of Dutch administrative law. How are these situations dealt with from the logic of administrative law today and how does administrative law allocate the responsibilities of the chain partners amongst each other to fix chain errors throughout the network? First, I will shortly discuss the legal character chain decisions have in administrative law. Then, I will look at the legal remedies that enable applicants to contest decisions and to what extent this enables them to

[54]B.J Schueler, *Schadevergoeding en de Awb. Aansprakelijkheid voor appellabele besluiten,* Deventer: Wolters Kluwer 2005, p. 58 e.v & p. 129; article 8:73 Awb.

correct errors of the chain and the problems that derive here from. After that, I will shortly discuss what the applicant can do in case he is faced with a chain error in the absence of an administrative decision. Thereafter, I will discuss a solution for the problem with the gaps in relation to protection of the Awb and a case that can be used as an inspiration to possibly look at the responsibilities of the chain partners from another perspective.

2.2 The legal character of automated chain decisions

Automated chain decisions do not have a legal basis that was specifically designed for them. They fall under the regular denominator of all the other administrative decisions that are regulated in the Awb (*''Algemene wet Bestuursrecht''*, General act on Administrative law). Administrative decisions define themselves by creating legal consequences for its addressees. The premise of the Awb is that every decision is made by the public body that is authorized to do so based on the Awb.[55] When public bodies take decisions, they are bound by the principles of good governance.[56] One of the fundamental principles when it comes to the decision-making process is the principle of due care. The public body should take into account all the relevant information and carefully weigh the several interests that are involved with the decision. If any doubt with regard to the correctness of the information relevant for the decisions raises, the public body needs to investigate this.[57]

If the addressee of the decision does not agree with an administrative decision, he can first file for an objection at the relevant public body that has taken the decision as long as the decisions has no formal legal force yet. Then, the public body needs to review the decision.[58] After this round, the applicant can go to the administrative court, ask for a revision of the decision and for a compensation of the potential damages that were created by the unlawful decision.[59] The logic of this legal protection scheme is based on the ''traditional'' decision-making process, in which a public body does not make use of algorithmic rules or data input of a chain network to automatically generate decisions.[60] It is based on the assumption that a public body can be seen as an independent entity, where a civil servant will personally and on behalf of the public body judge from the files originating from the administration of that public body whether an applicant should get the benefit, subsidy or permission requested for

[55] Article 1:1 Awb; 1:3 Awb.
[56] Schueler 2005, p. 58.
[57] F.Çapfurt & Y.E Schuurmans, 'Blinde vlek in de Awb: data' in: T.Barkhuysen et al, *25 jaar Awb in eenheid en verscheidenheid,* Deventer: Wolters Kluwer 2019, aant. 24.3; Van Eck 2018, p. 127.
[58] Article 6:4 Awb.
[59] Article 6:4(2), 8:88 Awb; Schueler 2005, p. 11-13.
[60] De Waard 2011, p. 43.

example. From this traditional perspective, effective legal protection can be guaranteed by addressing the issue to the responsible public body. After all, the public body has access to all the relevant information and the power to change any potential misinformation in the personal file of the applicant. However, in the new reality of chain-decision making processes, where the connections and data sharing are automated, public bodies do no longer operate independently.[61] They also do not have the capability, to change information they have derived from other systems of public bodies. If data is deemed authentic by law, public bodies are obliged to use that particular information in most cases.[62]

2.3 Appealing to administrative chain decisions

When an applicant is faced with an error of a chain that has resulted into an appealable decision, he can step to the administrative court to try and get the error and the decision that builds upon this error repaired. In this paragraph I will give a few examples of cases where public bodies based their decisions on third party data and how the administrative court handled these situations with regard to fixing the problem for the applicant.

If a public body has used wrong address registrations derived from the personal records databases (BRP) which turn out to be incorrect, the administrative courts are lenient and accept that public bodies in principle may rely on this information.[63] The administrative court has argued that the consequence of the use of the BRP creates a certain duty of care for the applicants to make sure they are correctly included in the registration and to contact the source holder if this is not the case.[64] Thus, if an address registration is incorrect, this should be addressed at the source holder of the register, and not at the public body that has based its decision on it. Even if the applicant on the first hand was not aware that the address information at the source holder was incorrect and contests another chain decision that was based on the incorrect information, he will be redirected to the source holder. This means that it is not the task of the body that has based its decision on the personal records base to get the information of the record base corrected. Thus, the administrative body is then exempted of liability. However, this redirection to the source holder does not mean the problems will be resolved.

[61] P. van Delden, *Samenwerking in de publieke dienstverlening: Ontwikkelingsverloop en resultaten* (diss. Tilburg) Delft/Zutphen: Uitgeverij Eburon 2009, p. 241.
[62] Algemene Rekenkamer 'Basisregistraties vanuit het perspectief van de burger, fraudebestrijding en governance' 2014, p. 5; Van Eck 2018, p. 105.
[63] Van Eck 2018, 111-112.
[64] ABRvS, 5 september 2012, ECLI:NL:RVS:2012:BX6491 ro. 4; ABRvS 11 maart 2009, ECLI:NL:RVS:2009:BH5525, *JB* 2009/114, m.nt. G. Overkleeft-Verburg.

I will illustrate this with an example Van Eck gives in her thesis: A civilian applies for a rent allowance at the Dutch Tax and Customs Administration. After one year, the final conferment of her allowance is determined at nil, because the public record database states that a second person with an income that is too high to receive the allowance is registered at the address as well. The registration of this other person is incorrect, and the applicant never received a notice of the registration. The applicant contests the decision at the Tax Office because the registration is wrong. The applicant is then sent to the municipality to correct the registration. However, the address change only takes effect at the moment the change is implemented and has no retroactive force. This means that the applicant is still not able to receive the rent allowance over the year that the registration remains incorrect. This results into the applicant being the victim of a decision-making processes that is poorly coordinated. This practice is accepted by the administrative court, because within the scheme of the Awb logic, the interconnectivity of the separate decisions and the public bodies is not recognized.[65] As a result, the civilians becomes the victim of poor ‘’chain-protection’’.[66]

In other cases, the administrative court has been more willing to put responsibility on the public body that used the erroneous data of administrations of other public bodies. This is for example the case with residence codes in the BRP that is handed in by the IND.[67] When public bodies use this residence code, and there is a reason to believe that the code is incorrect, for example because the interested party disputes its correctness with evidence or the input of other data in the administration supports this, the public body is obliged to further investigate the correctness of the data.[68] This approach is also handled in cases when there was no option for the applicant, to contest the data that was filed in the administration of the other public body.[69] When public bodies use data from other third private parties, the same investigation obligation is advocated by the court.[70] Subsequently, when the decision in appeal thereafter is successfully annulled, this does not automatically lead to a correction of the wrongful data in the system or a revision of the other interrelated decisions, because the administrative procedure is solely focused on the particular decision in appeal. This means the other involved actors in the decision process of the chain will not be held liable for the damages and are also not under the legal duty to automatically correct the error. The applicant

[65] ABRvS, 5 september 2012, ECLI:NL:RVS:2012:BX6491, ro. 3.4.
[66] Van Eck 2018, p. 218.
[67] The IND (Immigratie- en Naturlalisatiedienst) is the Dutch public body responsible for immigrations and naturalization.
[68] ABRvS 1 juli 2009, ECLI:NL:RVS:2009:BJ1093; ABRvS 21 okotber 2009, ECLI:NL:RVS:2009:BK0811; ABRvS 6 april 2016, ECLI:NL:RVS:2016:929.
[69] ABRvS, 2 november 2011, ECLI:NL:RVS:2011:BP2823.
[70] CRvB, 19 oktober 2010, ECLI:NL:CRVB:2010:BN9985, USZ 2010/390.

shall have to try and contest the wrong registration or the wrong chain decisions at the other relevant public bodies which is a burdensome and difficult task to fulfil successfully.[71]

The applicant also has the right to file a complaint at the Dutch Data Protection Authority (AP) on the basis of article 77 GDPR when he suspects a breach of his data protection rights. However, there are some restrictions tot this procedure. A complaint will only be considered if the applicant has already complained about the processing activities at the relevant organization, or in case of public bodies; contested the decision at the public body or in appeal. This means that the applicant still will have to make sure all the actors that are involved in the decision-making process are approached first. There is not an option to combine complaints of multiple organizations; all the complaints have to be handed in separately. Next to the option to make a compliant at the AP, the applicant can go to the civil court or the administrative court[72] and claim damages for a GDPR breach on the basis of article 82 GDPR. The problem however, just as concluded in Chapter 1, is that the error of the chain that is causing ongoing issues for the applicant does not always have to constitute a breach of data protection rules. The problem can also be caused due to a wrong interpretation or execution of the law for example. In these cases, appealing to data protection rights will not offer solace.[73]

### 2.4 Contesting chain errors caused by factual acts

It is possible that an applicant is faced with an error of the chain that can produce problems for future chain decisions, without there being a contestable decision at the moment the applicant is aware of the error. If in these cases, data protection rules are breached or legislation is not executed properly, because an algorithm is not functioning right for example, these errors are defined as factual acts of the public body.[74] A factual act does not (yet) constitute an appealable decision. Strictly speaking, the Awb does not offer a legal remedy to appeal to factual acts of public bodies.[75] Only administrative decisions and the acts that connect to the decision can be contested in appeal. Recently, the administrative court did accept competence to decide on GDPR breaches in a few cases where data was unlawfully

[71] Van Eck 2018, p. 106, 432.
[72] See for further explanation, paragraph 2.4.
[73] Website of the Dutch Data protection Authority to file a complaint: <https://autoriteitpersoonsgegevens.nl/nl/meldingsformulier-klachten>
[74] G.E van Maanen & R. de Lange, *Onrechtmatige overheidsdaad,* Deventer*:* W.E.J Tjeenk Willink 2000, p. 47-49.
[75] Article 8:88 Awb.

processed by public bodies.[76] With these rulings, the court has broadened the possibility for applicants to claim damages on the basis of article 8:88 Awb in combination with article 82 GDPR. A successful appeal does require that the applicant has made use of his data protection rights under article 15-22 GDPR and that the public body has given a written reaction to the exercise of these rights. This written reaction can be viewed as an administrative decision in light of article 34 of the Dutch implementation act of the GDPR.[77] On the basis of this reaction, the applicant can claim damages for data protection breaches.[78] While it is positive that the administrative court has eye for the recent liability developments of directly applicable European law, the shortcoming of the GDPR scheme that was already pointed out in Chapter 1, is that it focuses on claiming compensation and not specifically on putting an end to errors to prevent future problems for the applicant. It also remains unclear whether the court would accept competence if a written reaction is not given after the applicant exercised his GDPR rights. In addition, the administrative court will not accept competence for factual acts that do not involve the exercise of GDPR rights, because no connection can be made to an administrative decision. This falls under the exclusive competence of the Dutch civil court that will be discussed in the next chapter.[79]

2.5 Ongoing damaging activities when data is not corrected with retroactive force

In paragraph 2.3, it became clear that a public body refusing to reverse the decision retroactively for the applicant, can have negative effects because other public decisions are built upon this decision. That the correction of a decision the applicant contests, is not an effective way to prevent further damages from occurring, can be illustrated with the ECHR case *Romet/Netherlands*. In this case, Romet was the victim of identity theft of his drivers' licence, which led to an erroneous registration of 240 vehicles at the RDW[80] on his name. Romet asked the RDW to change the registration with retroactive force, because other public bodies were constantly imposing sanctions on him for not paying taxes, speeding and driving without insurance.[81] Romet eventually ended up in debt restructuring. According to the State and the RDW, the retroactive force could not be granted to the wrong registration, because this would contaminate the purity of the register, and lead to legal uncertainty, because other

[76] ABRvS 1 april 2020,ECLI:NL:RVS:2020:898; ABRvS 1 april 2020 ELCI:RVS:2020:899; ABRvS 1 april 2020, ELCI:NL:RVS:2020:900; ABRvS 1 april 2020, ECLI:NL:RVS:2020:901.
[77] ABRvS 1 april 2020,ECLI:NL:RVS:2020:898 ro 17, 18.
[78] ABRvS 1 april 2020,ECLI:NL:RVS:2020:898 ro 22, 25.
[79] Van Maanen & De Lange 2000, p. 48-49.
[80] The RDW is the Dutch public body that is tasked with registering license plate numbers of vehicles.
[81]EHRM, 14 februari 2012, ECLI:NL:XX:2012:BW2721 (*Romet v. The Netherlands*).

public bodies based their decisions on the register as well. The administrative court accepted this practice: the court has noted in this case and other cases as well, that the interest of the users to put trust in the basic registration prevails over correcting the data with retroactive force.[82] The ECHR did not agree with this practice and blamed the State for breaching article 8 ECHR by not adequality taking administrative action at the time the driver's license was filed stolen. This means that, in the opinion of the ECHR, proactive measures should already have been deployed by the authorities at the moment they knew the license was stolen, to prevent that Romet his driver's license would be used for erroneous registrations in the first place and would cause him damages. Consequentially, the authorities were under the duty to make sure registrations were corrected even without the request of Romet to change the registration to prevent a breach of article 8 ECHR. [83]

2.6 Strict liability as an incentive to fix problems with third party data

While the administrative liability scheme is still resolved around the idea that administrative decisions are taken by public bodies separately, administrative courts are forced to use this attribution logic. This leads to a situation where the legal reality, that chain decisions are part of an interconnected and automated decision-making processes is ignored or overlooked. Public bodies in principle only have to take account for their own actions. As long as each separate public body shows, that incorrect data is the responsibility of another entity, that they had no reason to believe the data was incorrect or that they have taken the necessary steps to investigate whether the data was correct, the court will accept this. In addition, the defence that registrations cannot be changed with retroactive force, is a practice that is also tolerated. If the administrative decision is annulled, this does not have to mean other interconnected chain decisions are revised as well. Corrections do not work upstream automatically, and the administrative courts do not have the power to order this, because the procedure is solely be aimed at the particular decisions that is contested on the basis of the Awb. This results into a fragmentation of responsibilities and public bodies pointing fingers at each other when it comes to correcting the data.[84] This lack of chain protection and taking responsibility could possibly be fixed by generating stronger incentives for public bodies, to resolve issues

[82]ECHR, 14 February 2012, ECLI:NL:XX:2012:BW2721 (*Romet v. The Netherlands*), para 18; ABRvS, 11 maart 2009; ECLI:NL:RVS:2009:BH5525, JB 2009/ 114, m.n. G. Overkleeft-Verburg.
[83] ECHR, 14 February 2012, ECLI:NL:XX:2012:BW2721 (*Romet v. The Netherlands*), paras 37-44.
[84] Van Eck 2018, p. 234.

amongst each other chain-wide by looking more at the total picture of the administrative action.[85]

A starting point to fix this issue would be to multiply the internal effect of the GDPR arrangement of joint controllers when it comes to erroneous administrative chain decisions. The fact that chain actors choose to work together in the decision-making process, should mean that they can be held liable for the damaging activities of other chain partners as well. As a consequence, their internal arrangement cannot be held against the applicant which means pointing fingers in relation to responsibility is no longer an option. In this situation, the justification ground of public bodies, that the mistake does not lie with them and cannot be fixed by them, while it relates to the data of other parties, they are dependent on will no longer suffice. In this way, public bodies can be stimulated through the administrative framework to have measures in place to fix errors in the chain upstream and downstream.

Inspiration for this rationale can also be found in the tone that is set in an administrative case about a violation of recycling norms. The case concerns the following. Recycling Network, an independent environmental organization had requested the Secretary of the State to enforce the public body ‘’Afvalfonds’’ (A public body that checks the recycling process of waste) to comply with the obligation to handle a certain recycling norm for glass packages. ‘’Afvalfonds’’ was structurally violating the norms over the years. The Secretary of the State refused to impose an administrative fine, because ‘’Afvalfonds’’ was not in the position to prevent the violation from happening, due to the fact that the recycling process is dependent on the input of third parties: the more people recycle their glass, the better the recycling rate will be. In addition, Afvalfonds was dependent on the municipalities to set up a system for the collection of the glass, and of other waist companies to select and recycle glass that was not yet separated.[86] Next to that, ‘’Afvalfonds’’ had showed to the Secretary of the State that it had taken certain measures to improve the recycling process. According to the Secretary of the State, the particular dependent position of the ‘’Afvalfonds’’ made it that a warning should suffice, and a sanction would not make the situation any better.[87]

The administrative court had a completely different view on the matter than the Secretary of the State and found that the rejection of the request was poorly argued. According to the court, a punitive sanction could be the correct and necessary incentive for

[85] Van Maanen & De Lange 2000, p. 791-792.
[86] ABRvS 27 december 2017, ECLI:NL:RVS:2017:3561 ro. 6.
[87] ABRvS 23 januari 2019, ECLI:NL:RVS:2019:150 ro 4.1-4.2

‘’Afvalfonds’’ to investigate other measures to improve the recycling rate, which would eventually lead to a compliance with the norms.[88] The case lends itself for an interesting approach by analogy when handling other situations that are hard to manage for public bodies from an administrative perspective. The view is usable for the problem with the unsatisfying cycle of chain decisions and errors; even if the errors/violations occur beyond the control of the actor, this does not mean that he is not able to do something about. The actor could also choose to make an effort and try to change and improve the situation. Hence, if you choose to operate in a chain and utilize the efficiencies of the public registration of other public bodies, you have a responsibility to take action and take the necessary steps to improve the complete process and to fix the problems with the other partners involved in the process. A public body should not be able to hide behind the fact that the repeating cycle of erroneous decisions it makes lies beyond its control, because it is caused by the data input of the chain. If you fail your duties, you will have to pay for full compensation.

## 2.7 Conclusion

The traditional attribution logic of the Awb does not function properly anymore. While chain decisions are interrelated and build upon each other, the Awb still assumes that all decisions and the public bodies that make them are detached and independent from the decisions making processes and registrations of other public bodies. The responsibility of each decision is split up by the Awb and divided over each public body, which leads to a situation where every public body remains merely responsible for its own link in the complex decision-making processes of the chain network. The absence of a joint liability scheme in administrative law creates a lack of incentives for the public bodies, to actually fix the problems for the applicant and to repair the damaging situation amongst each other. This puts an increased and heavy burden on citizens or companies to get the error corrected. Contesting a single decision in appeal at the administrative court, is not a sufficient method to receive an adequate level of legal protection against government action anymore. As a result, the applicant will have to find other ways to get the error corrected and to receive legal protection for chain failures. Protection from the GDPR will also not always offer the desirable solace, while the scheme is aimed at compensation and not on correction. A first step to tackle these problems would be to transplant the logic of the liability scheme of the GDPR to administrative chain decisions. All interrelated decisions should be viewed as multi-actor

[88] ABRvS 23 januari 2019, ECLI:NL:RVS:2019:150 ro 4.7.

activities of the public bodies in which they all bear a joint responsibility to repair errors that are causing the problems for the connected decisions. With drawing inspiration from the *Afvalfonds*-case, an appeal of a public body, that the incorrectness of certain information lies beyond its control, should no longer suffice. If authorities want to benefit from chain cooperation, they should be obliged to have an arrangement in place for corrections of errors throughout the chain or network of connections; upstream and downstream.

## Chapter 3: Responsibilities and legal protection of chain errors from a Dutch civil law perspective

### 3.1 Introduction

While the legal position of the addressee of a chain decision is mainly determined by the combination of the GDPR and Dutch administrative law, Dutch civil law serves as a safety net for potential compensation of damages that are suffered due to government action that cannot be contested via administrative law and also for the legal protection of torts that do not constitute a GDPR breach.[89] In the first chapter, it became clear that protection from the GDPR is limited to infringements of data protection rights, while chain errors do not necessarily have to be caused by a breach of the GDPR. In the previous chapter, we saw that from an administrative law perspective, factual acts of the government fall under the competence of the Dutch civil court, while the administrative court only considers itself competent in cases where a connection can be made to an appealable administrative decision. In addition, the idea of multiple public actors being responsible for automated decisions as a result of chain cooperation, is not recognized, due to the fact that the Awb does not offer a legal remedy to contest multiple decisions in appeal. This means the applicant will have to make sure the error is corrected at all the different actors separately.

[89] It should be noted that the civil court is indeed also competent to judge about GDPR infringements and GDPR liability. However, when a GDPR infringement cannot be established, there is still the possibility to claim damages on the basis of Dutch tort law.

It should be stressed that the civil court will not accept competence if the applicant has the option to appeal to an administrative decision at the administrative court.[90] In addition, when there was an option for the applicant to contest an administrative decision, but he did not make use of this administrative legal procedure, the decision will have formal legal force. As a general rule, the civil court will assume that the decision and the acts of preparation that connect to the decision are lawful. Deviation from this rule to establish a tort are only possible under exceptional circumstances.[91] For this reason, Chapter 3 will only focus on legal protection for factual acts of public bodies. I will assess whether Dutch civil law could presumably offer complementary protection for chain errors. Dutch civil law does acknowledge that torts can be committed by multiple actors on the basis of article 6:166 of the Dutch Civil Code (BW). I will combine this liability scheme with the particularities of torts committed by government action in which the civil court takes into account the special position of public bodies. In this way, I will assess whether the multi actor liability scheme could potentially be successfully applied to group activities of public actors as well. First, I will examine how a group activity is defined by Dutch civil law. Then I will zoom in on the particularities of a group tort, that deviate from the scheme of torts committed individually and which actors can be held liable for a certain group activity that has caused damages. After that, I will discuss the possibility of fellow group actors holding each other liable for damages. I will constantly reflect these basic principles of group liability on the situations of joint control of data chains. Lastly, I will discuss the specialities of torts committed by the government to see whether the scheme of article 6:166 BW can also be successfully applied to public bodies.

## 3.2 A tort conducted by a group

### *3.2.1 Defintion of a group*

The liability of a tort committed in a group is regulated in article 6:166 BW. Article 6:166 BW prescribes that if one or more persons that belong to a certain group commit a tort, the whole group can be held liable, if the chance that these damages would occur should have withheld them from actively participating in the group. According to Boonekamp, acting within a group is a neutral and abstract concept, which means that all types of group activities can be dragged into the scope, as long as the group members have a certain level of awareness

[90] Van Maanen & De Lange 2000, p. 8-10.
[91] A.S Hartkamp & C.H Sieburgh, 'Formele rechtskracht' in: C.H. Sieburgh, *Mr. C. Assers Handleiding tot de beoefening van het Nederlands Burgerlijk Recht. 6. Verbintenissenrecht. Deel IV. De verbintenis uit de wet*, Deventer: Wolters Kluwer 2019 aant. 374.

that they are acting within that group setting. Although the legal text refers to a group of persons, this also includes torts conducted by legal persons.[92] A certain level of awareness of the cooperation does not have to mean however, that the actions of the group members were coordinated amongst each other.[93] In addition, it sets no further demands with regard to the legal form in which they operate together. It is also not necessary that their actions are the same or that they act together as one unit at the same time and place.[94] Actors setting up a chain network to exchange data amongst each other should therefore be qualifiable as a group activity. This also makes sense with the GDPR-logic of joint control in mind, that defines it as an activity pursued together by multiple actors. Thus, the decision to be part of a chain network and utilize its efficiencies can be seen as a clear act of awareness to be part of a group activity.[95] When it comes to torts that are committed by a group, there are some particularities in relation to the conditions which establish the liability of the group.

*3.2.2 No conditio sine qua non connection of all the actors involved*

Normally, if a tort can be attributed to a single actor, liability can only be established if there is a causal link between the conduct of the actor and the damages. The conditio sine qua non rule refers to the act that is the indispensable condition for the damages to take place. The establishment of the condictio sine qua non connection does not provide a final answer to what the real cause of the damage was, but it helps to demarcate which events could have possibly caused the damages.[96] In principle, if there is no conditio sine qua non connection, the damages cannot be attributed to the actor. To assess whether such a connection exists, the elimination method can be used. If the damages would have occurred if we think away the conduct of the actor concerned, there is no conditio sine qua non connection between the tort and the damages. Article 6:166 BW handles a special scheme with regard to the determination of the conditio sine qua non- connection. [97]

A problem with causal links in multi-actor scenario's, is that the conditio sine qua non connection does not always work sufficiently in cases where damages are caused by multiple

[92] R.J.B Boonekamp, *Onrechtmatige daad in groepsverband volgens het NWB,* Deventer: Wolters Kluwer 1990, p. 66.
[93] Rb. 's-Gravenhage 9 november 2005, ECLI:NL:RBSGR:2005:AV:2156, ro 3.2; R.J.B Boonekamp, 'artikel 166. Gedragingen in groepsverband', in: C.J.J.M. Stolker (red.), *Groene Serie Onrechtmatige daad*, Deventer: Wolters Kluwer 2019, aant. 4.2.
[94] HR 2 oktober 2015, ECLI:NL:HR:2015:2914, NJ 2016/194, m.nt. T. Hartlief; Boonekamp in: *GS Onrechtmatige daad*, art 6:166 BW, aant. 4.1.
[95] Boonekamp 1990, p. 4.
[96] Schut 1997, p. 74.
[97] Schut 1997, p. 74-75.

actors at the same time or almost at the same time.[98] An example: A has provided erroneous data to B within the data chain, but B has also solely collected erroneous data separate from the data chain on its own micro-level. B has denied an unemployment benefit based on the erroneous data of A and based on its own erroneous data. If we assume that both the erroneous data from A and B separately could have led to the denial, the following happens: If we think away the erroneous collection of data by A, the denial still occurs. Conclusion: No conditio sine qua non connection. But: if we eliminate the erroneous collection of B, the denial also still occurs. This would lead to the illogical conclusion that none of the actors have caused the damages. To solve this issue, alternative or multiple causality is used. Alternative causality assumes that at least one of the events alternatively, could have caused the damages or that the events are causing the damages at the same time.[99] Thus, an appeal to the failure of the conditio sine qua non connection will normally not suffice under article 6:166, nor under article 6:162 BW. But, article 6:166 BW goes even further than the exemption with regard to mutual causality. For the group liability to be established, article 6:166 only demands a damaging act of one of the actors. This means that it is not necessary that the other actors of the group, also factually contribute to the damages. For the other actors, it is sufficient that there is a causal link between their choice to participate in the group and the chance the damages would have occurred. The fact that these chances were foreseeable should have withheld them from participation.[100] This means that the establishment of liability of the group, is disconnected from the condictio sine qua non causality.[101]

### 3.3. The group that can be linked to the damages based on their participation

#### *3.3.2 Attribution of the torts*

To establish which group of actors can be held liable for the tort, we need to assess to which actors the tort can be attributed to. When torts are committed individually, there are two main ways a tort can be attributed. Firstly, a tort can be attributed to a party if he has caused the act due to personal fault. Next to that, a tort can be attributed to the actor as a strict liability by law or in light of the public opinion.[102] Personal fault links the perpetrator to the tort and

[98] Schut 1997, p. 75.
[99] Article 6:99 BW; K.J.O Janssen, *Onrechtmatige daad: algemene bepalingen*, Deventer: Wolters Kluwer 2009, p. 44 e.v; R.J.B Boonekamp in: A.T. Bolt (red.), *Groene Serie Schadevergoeding*, Deventer: Wolters Kluwer 2019, art 6:99 BW, aant.1; Boonekamp 1990, p. 13.
[100] Boonekamp 1990, p. 15.
[101] Boonekamp 1990, p. 18; Hof Den Haag 22 december 2015, ECLI:NL:GHDHA:2015:3515.
[102] 6:162 lid 3 BW; K.J.O Janssen in: C.J.J.M. Stolker (red.), *Groene Serie Onrechtmatige daad*, Deventer: Wolters Kluwer 2019, art. 6:162 BW, aant. 9.

relates to the question of culpability. In other words; was the tort factually committed by the actor?

With the group tort the attribution logic lies differently, because there is no condition that the tort was factually committed by all the actors or that the damages were partly caused by all the actors.[103] This result into a scheme where two different types of torts can be distinguished from each other. On the one hand we have the tort of one or more actors that have factually caused the damages. On the other hand, we have the tort that lies in breaching a duty of care by not withdrawing from participating in the group.[104] This means that the actors involved do not jointly commit one tort, but they are all on the individual level committing an individual type of tort, either by causing the damages or by failing to withdraw from participation.

For the first type of tort, attribution of the tort is linked to the factual conduct/personal fault of the actor(s) that have caused the damages to occur. For the second type of tort, attribution of the tort is a strict liability should be established with two cumulative conditions: (1) Was the actor participating in the group activity? (2) Should the probability that the damages from the tort would have occurred have withheld that actor from group participation? This second condition relates to the question whether there was a presence of a duty of care on the group participant. If an actor knows or should have known that he was participating in a group activity that could have led to the damages that eventually occurred, attribution is given. Foreseeability of the damages therefore plays a significant role in determining whether the participant should have withdrawn himself from the activity.[105]

### *3.3.3 The group activity reflected on chain activities*

Now, I will assess what these basic cumulative conditions mean for joint control activities of chain partners. The first type of actors, that ones that factually commit the tort, can logically not be eliminated from the group activity. In our case, this relates to actors that have caused the chain error for example by collecting and registering the original erroneous data (the source holders) and/or to actors that have used erroneous algorithms in which legislation is implemented or carried out incorrectly which have led to wrong automated chain decisions.

[103] Boonekamp 1990, p 71.
[104] Boonekamp 1990, p. 103.
[105] Boonekamp 1990, p. 97.

An act of participation with regard to these types of torts occurs, as soon as the relevant controllers and processors form a part of the processing activities.[106] This means that the controller has to share to some extent the purposes and means of that data with the other joint controllers. For the processor it means, that he has to be involved in processing the particular data. If a controller or a processor within a data chain are not involved in the particular processing activities, they are not participating in the group activity.

We should keep in mind that participating in the group activity, does not constitute a tort in itself. The second condition demands that there needs to be a certain duty of care to not participate in the relevant group activity, because the damages that eventually occurred were foreseeable for the actors. According to Boonekamp, this foreseeability should not be determined with the subjective knowledge of all the individual participants, but rather by looking whether there was an objective, collective foreseeability that all the group activities together, could possibly lead to the damages that have occurred. The damages that have occurred, should lie in the general line of expectation of what the group participants could have foreseen when he choose to participate.[107] Foreseeability thus relates to the question, if an actor *could have known,* these typical damages would occur by joining the group activity. Thus, the nature of the damages has to match with the nature of the activity to some extent. It is also not necessary that the actor could concretely foresee that the particular damages would occur as they did. A general foreseeability that the types of damages could happen is suffice, and not the actual, concrete damages that were suffered.[108] The fact that data can be incorrect, algorithms can be wrong or can generate wrong outcomes and can lead to damages, should lie in the general line of expectation of all the actors that operate in a chain. This means that the typical damages that can be suffered due to chain errors are objectively foreseeable for the actors that choose to work in a data chain together.

If the damages are foreseeable, the only way to evade group liability is if an actor of the group involved actively withdraws himself from the damaging group activity.[109] The question then arises whether this is possible with actors involved in the chain network and how this should take form. After all, in the case of chain cooperation, actors are by means of law or arrangement jointly involved in the decision-making process and under the legal duty to process and use certain data and to take administrative decisions. Therefore, withdrawal

[106] This viewpoint connects to the general notion of article 82(4), that all the actors involved in the processing activities can be held liable, in other words: they form part of the ‘’group activity’’.
[107] Boonekamp 1990, p. 128-129.
[108] Boonekamp, in: *GS Onrechtmatige daad*, aant. 7.1; HR 2 oktober 2015, ECLI:NL:HR:2015:2914, NJ 2016/194, m.nt. T. Hartlief.
[109] Boonekamp 1990, p. 71.

from the decision-making process (in other words; the group activity) will probably not be an option based on their legal duties. In conclusion, the only way to evade the joint liability is to take measures that opt to prevent these possible damaging activities of the group, by actively making sure errors are dealt with and fixed properly within the whole chain. When it turns out damaging activities are conceived by the group, the actors should take action against the partner(s) the error is derived from to prevent damages from happening. This means for example that incorrect data should be contested and corrected on behalf of the applicant. As a consequence, the defence of a chain actor, that he did not know the error had occurred, or the correction of data lies beyond its control for example, will not succeed from the perspective of article 6:166 BW. While the damaging activities were in the line of expectation for the actor, he is under the duty to prevent the damages from occurring in the first place. Therefore, the actor will be strictly liable for the damages.

### 3.4 Liability of the tort

Once the relevant actors involved in the tort that was committed by the group has been established, the participants of the group activity are all jointly and severally liable for the damages that have occurred according to article 6:166 (2) BW. Important is that the victim of the damages does not have to hold all the group participants liable. He may choose whom of the participants to hold accountable and then base his claim on article 6:166 BW.[110] When it comes to recourse amongst the actors, the basic rule is that all the actors involved in the group should bear the same amount of damages, unless this would be inequitable. The legislator has supported this recourse arrangement by stating that participating in a group should be characterized as an activity that comes with a general sense of solidarity. Next to that, a sole assessment of the gravity of all the actor's individual mistakes would often be unfeasible.[111]

### 3.5 Liability of damages amongst the fellow participants

Boonekamp underlines the possibility that not only a third party can suffer damages from a group activity, but also one or more of its group members. He asks whether the liability of the participant gets in the way of successfully addressing the other group members for the damages he has suffered. Boonekamp advocates that it should be possible to successfully hold the fellow participants accountable in case of damages. He argues that all the participants of the group are not only under the legal obligation to prevent damages to third parties, they are

[110] Boonekamp 1990, p. 170-171.
[111] Boonekamp 1990, p. 168-169.

also under the legal obligation to not cause any damages to their fellow participants. If this was not the case, this would result into the inequitable situation in which the group members would receive a 'free pass' to create damages vis-à-vis their group members without being sanctioned by article 6:166 BW. From this perspective, a second legal duty can be derived: participants are also under the legal duty to adequately prevent damages to their chain partners. This duty entails that partners have to pro-actively correct their own errors so that these errors will not contaminate processing activities of the other chain partners. In case the error is already processed, and a partner gets knowledge of this, it should immediately notify this to the other chain members. It is acceptable that the other participants carry the damages that were caused to another participant. In case one or more members have suffered damages from the group activity, it is reasonable that they are able to successfully claim damages from the group member(s). However, according to Boonekamp the fact that the member of the group is participating in the group activity, does mean that he presumably will have to bear a certain amount of the costs of the damages he has suffered, based on the fact that he has not withdrawn himself from the group activity. The amount of damages he has to bear, will depend on the level of his personal culpability in relation to participating in the group. The legal text of article 6:166 BW allows this interpretation, as it does not exempt members of the group in any way from action.[112]

### 3.6 The multi-actor scheme applied to torts committed by public bodies

While the government fulfils a special role in the society as the entity that represents the general interest, the position of public bodies in relation to liability diverges from the position of private actors. Torts committed by the government show some particularities compared to torts committed by private entities or persons. In principle, the same basic criteria to establish a tort apply, but the concrete specification of these conditions can be somewhat different.[113] As soon as public bodies possess legal personality they can be defined as actors that can participate in a group activity in the sense of article 6:166 BW. This means they can be summoned to appear before the civil court.[114]

Public bodies have a certain degree of margin of appreciation when it comes to executing their legal tasks. Subsequently, the civil court will handle a more reticent attitude

[112] Boonekamp 1990, p. 66-68.
[113] Van Maanen & De Lange 2000, p. 77.
[114] Article 2:1 BW declares that municipalities, the State, the water authorities, provincial authorities, and bodies that have enacting competences based on the Constitution have legal personality. According to article 2:2 BW other public bodies only possess legal personality if this is declared specifically by other law. The UWV has legal personality on the basis of article 2(2) SUWI for example.

depending on how much discretionary power a public actor has. This prevents that he will judge about political or policy-related matters that belong to the field of administrative law or politics.[115] However, today this margin of appreciation is restricted by the court because the duty of care of the government is largely defined by the principles of good governance. Since the *Ikon*-case, the Supreme Court has prescribed that the civil court should test the legitimateness of government action directly against the principles of good governance. This rule is also codified in article 3:14 BW.[116] A few examples of these principles are the principle of due care, the principle of equal treatment, the principle of legitimate expectations et cetera.[117] Thus, the government has to take into account these principles when acting within the context of civil law as well. The principles of good governance imply that the government should behave as a public example. In addition, factors that also should be taken into consideration are that public bodies possess the best recourses to know the relevant judicial and factual circumstances and have the greatest carrying capacity to cover damages.[118] It is expected from these actors that they are aware of these relevant facts and the legal consequences of their behaviour. As a result, in many cases higher demands can be required from public actors to make sure the standard of due care is complied with. This means the establishment of a tort can occur more rapidly by breaching the standard of due care. According to van Maanen & De Lange, this stricter criterion is justified in light of the special task of the government to make sure the interests and rights of the public are protected.[119] An additional notion that supports this quicker attribution is that damages caused by governments action can better be borne by the community, than by a single person that can be seen as a rather coincidental victim of the damaging public conduct.[120]

A successful appeal to a chain error will therefore depend on how the particular discretionary power of the public bodies are defined by the court and how the court relates this to the principles of good governance; did the actors have a large amount of discretionary power or not? And did the actors infringe the standard of due care by not living up to one or more principles of good governance?[121] Not adequately taking action against chain errors while this is causing damages for the applicant could be viewed as not fulfilling the principle of due care. While the government is in the position to know the factual circumstances and

[115] Van Maanen & De Lange 2000, p. 62.
[116] HR 27 maart 1987 ECLI:NL:PHR:1987:AG5565, *AB* 1987/273 (*Ikon*) ro. 3.3, 3.4.
[117] Article 3.2 Awb.
[118] Schueler 2005, p. 128-131.
[119] Van Maanen & De Lange 2000, p. 91.
[120] Schueler 2005, p. 149-151.
[121] Van Maanen & De Lange 2000, p. 58.

the consequences of their behaviour, precautionary measures can be expected to prevent damages from chain errors. Therefore, there is a viable chance for an applicant seeking protection for chain errors that the civil court will come to the conclusion that the multiple public bodies are liable for the torts committed in a group while they breached the principle of due care by not adequately preventing the damages from occurring.

## 3.7 Conclusion

In this chapter I examined whether an applicant can receive complementary protection for chain errors caused by factual government acts. The tort from a multi-actor perspective embodied in Dutch civil law has given some useful insights with regard to how this legal scheme regulates the liabilities and responsibilities of actors participating in a group activity. A tort committed in a group occurs when one or more members of the group, are factually causing damages. If the other group participants were able to foresee these damages, they were under the legal duty to withdraw themselves from the damaging group activity. This means there does not need to be a conditio sine qua non connection to their factual conduct and the concrete damages that have occurred. If the tort can be attributed to the actors of the group, they will all be jointly liable for the damages. This scheme is reflected on the activities of actors within a chain network. Once the actors form a part of the relevant processing activities, they will be accounted for as participants. If the actors could have foreseen the damaging activities, because the damages that occurred were an objectively foreseeable result of the group activities, actors are under the duty to withdraw themselves from the damaging group activity. As a result, the tort that flows from the act of participation can be attributed to them. While the chain actors will not be able to withdraw themselves from the chain process activities, the only way to evade joint liability is by making efforts to prevent or to put an end to the damaging activities. Thus, the lability scheme of torts committed in a group reflected on chain cooperation confirms the previous notion that the bodies involved in a chain network should be under the legal duty to adequately take measures to correct errors chain-wide. This last duty finds extra support in the view of Boonekamp, that participants of a group are also under the legal duty to prevent damages vis-à-vis their fellow participants. Lastly, I checked whether the special position of the government could influence the successful application of the article 6:166 BW scheme. It is expected that it should be possible to hold public bodies liable for their actions, while they also have to take into account the principles of good governance in the domain of civil law. As a consequence, the government can be held liable more quickly for its behaviour, while the civil court sets higher demands to the standard of

due care for public actors in comparison to private actors. This means that in theory, it should be possible for an applicant to receive successful complementary protection in the form of compensation for the damages he has suffered from the chain error(s) on the basis of Dutch civil law.

## Chapter 4: Conclusions and recommendations

### 4.1 Introduction

Chain informatization plays an increasing role in the administrative landscape. Public bodies deploy infrastructures together to exchange data, to make use of each other's data and to base their decisions upon each other. As a result, in a lot of cases, citizens or companies will only have to administer certain personal information at one public body. Thereafter, the data will be used a multiple time by other bodies, for a divergent range of different aims. While these chain infrastructures enable public bodies to operate quicker and more efficient, the cooperation also has a negative side. In case input data is incorrect, erroneous algorithms are deployed or legislation is carried out incorrectly, the consequences of these errors can be enormous for the applicant because of the variety of public bodies that may potentially built further upon the error. In the previous chapters, I tried to get a grasp of how the responsibilities of the various chain partners lie, when operations in the chain go wrong by looking at it from the multiple legal schemes that determine their responsibilities and that offer protection to the applicant when he is faced with a failure of the chain. In this last chapter I set out the various legal domains I examined to point out where the weaknesses and gaps in responsibilities and protection lie when chain errors occur. After that, I will make some recommendations with regard to possible solution for this lack of chain protection.

### 4.2 Responsibility and protection under the GDPR

From a GDPR-perspective, chain networks can be seen as jointly controlled by the bodies that use and exchange data amongst each other (article 26 GDPR). While at the micro-level, actors may use these data for their own purposes or collect data for a purpose at the end of the chain,

setting up an infrastructure to enable these activities creates a new ‘’set of operations’ from the macro-level perspective. As a consequence, the GDPR prescribes that the partners have a certain duty to make the transfers safe and operable.[122] The choice of the CJEU and the WP29 to define joint control very broadly, is mainly based on the rationale that the data subject should always be capable of effectively using his data protection rights and claiming damages when his data protection rights are infringed. This multi-actor approach opts to prevent that no actor can be held effectively liable for the damaging activities or that data protection rights cannot be completely utilized.[123] This goal finds extra support in the fact, that the internal allocation of the responsibilities of the joint controllers cannot be held against the data subject.[124] All the controllers and processors are strictly liable if they are involved in the processing activities for the entire amount of damages. For processors there does have to be additional proof of breaching certain GDPR-obligations or instructions of the controller. Personal fault in relation to the infringement is deemed irrelevant. Only exceptional circumstances of *force majeure* that lie completely beyond the control of the actor can form a successful way to evade liability.[125] Recourse amongst the partners, can only be claimed afterwards between the partners.[126] The strict liability scheme the GDPR prescribes is positive, while this scheme prevents that the applicant is send from pillar to post when he seeks for compensation of his damages due to the infringement of his data protection rights. The strict cumulative liability scheme can be seen as a means to obtain the effective protection with regard to the joint controlled processing activities and creates an incentive for the various chain actors, to make sure their GDPR-compliance is secured chain-wide to prevent liability.

However, the GDPR is limited in terms of offering effective and complete protection when applicants are faced with chain errors. While a part of the applicants will mainly be interested in putting an end to the ongoing problems he faces from error, so that more administrative fines or other administrative troubles in the future are prevented for example, the GDPR solely prescribes that applicants can claim damages for the infringements of their data protection rights. The GDPR does not demand that a judicial remedy is put in place so that errors that flow through a chain are fixed chain wide. How the applicant will eventually receive protection and what remedies are offered, will therefore depend on the procedural

[122] Article 29 Working Party 2010, p. 20-21.
[123] Case C-210/16 EU:C:2018:388, (*Wirtschaftsakademie Schleswig-Holstein)* para 28.
[124] Article 26(3) GDPR.
[125] Van Alsenoy *Jiptec* 2016, p.282-283.
[126] Article 82(3) GDPR.

choices of the Member State he seeks protection from.[127] Next to that, the GDPR can only be used to receive chain protection in cases of breaches of data protection rules. Chain errors can also be caused due to failures that do not constitute a data protection breach, for example when the law is interpreted incorrectly. For these cases, the applicant will not be able to rely on the liability scheme of the GDPR.

### 4.3 Responsibility and protection under Dutch administrative law

While the chain cooperation this thesis focuses on concerns a public activity, the responsibilities of chain actors and the legal position of the applicant seeking protection is for a great part determined by administrative law. However, the possibilities to contest chain errors via administrative law are limited, while the Awb in principle only allows appeals against administrative decisions that do not have formal legal force yet. When an error of the chain results into an administrative decision, the applicant can review this decision in appeal to get is revised.[128] The Awb does not provide a specific basis for interrelated, automated chain decisions. It still approaches the decisions, as a moment of an exercise of power by a separate public body. This traditional approach contradicts with the reality wherein chain decisions are only a ‘’snapshot’’ of a complex and interconnected larger decision-making process of a chain network. When public bodies base their decisions on public registrations, the general notion is that bodies may trust this information, unless there are indications that the information is incorrect. If it is possible to get the registration corrected at the source holder, the applicant will be redirected to the source holder to fix the issue. Correction of the registration at the source holder does not mean however the other decisions that were built upon the wrong registration will be revised afterwards, while registrations are not corrected with retroactive force most of the times to ensure ‘’the purity of the register’’.[129]

Even if a decision is annulled successfully in appeal, this does not result into an automatic revision of the interrelated decisions upstream and downstream of the chain as well. This is a consequence of the logic of the Awb procedure in which the judge can only decide upon the one decision the applicant appealed to. Afterwards, the applicant will have to approach the various other bodies to try and contest the error. If an applicant has complained about the problem at these bodies, but the actors do not solve the issue, he can also file for a

[127] Case 158/80 ECLI:EU:1981:163 (*Rewe-Handelsgesellschaft Nord mbH v Hauptzollamt Kiel*) para 41; Van Alsenoy, *Jiptec* 2016, p. 288.
[128] Article 6.4 Awb; Schueler 2005, p. 11-13.
[129] Van Eck 2018, 111-112; ABRvS, 5 september 2012, ECLI:NL:RVS:2012:BX6491 ro. 4; ABRvS 11 maart 2009, ECLI:NL:RVS:2009:BH5525, *JB* 2009/114, m.nt. G. Overkleeft-Verburg.

complaint at the AP if the problem concerns a data protection breach or start a legal procedure for damages on the basis of a GDPR breach. If this is not the case, the AP and protection under the GDPR are not an option. If the applicant seeks to contest a chain error that does not constitute an appealable decision, protection is limited. The administrative court recently accepted competence to decide on the compensation for liability of GDPR breaches, in case applicants exercised their GDPR rights and the public body replied to the request with a written reaction.[130] However, the protection the administrative court gave in these cases was limited to claiming compensation and not aimed at correction. Next to that, it is not clear whether the court would accept competence if such a written reaction is not given. For other factual acts that do not constitute GDPR-breaches, protection has to be sought from the civil court.

The logic of the Awb strengthens the attitude of public bodies that they can only act within the powers of their administrative tasks assigned to them. This results into pointing fingers at each other when it comes to the question who bears the ultimate responsibility for incorrect data that travels through the chain.[131] As a consequence, there is a reluctant attitude of the bodies towards citizens and companies to actually make sure the errors are dealt with properly chain-wide and to prevent potential further damages from occurring. The applicant is increasingly burdened with proofing and contesting erroneous data that flows through the chain.[132] This creates a shift in responsibility of making sure errors are corrected from the public bodies onto citizens and companies. In addition, public bodies are not eager to change data with retroactive force, because of the fact that other bodies base their decision on these registers. A painful example of this reluctant attitude is the *Romet*-case, where the RDW refused to correct the data with retroactive force because it would contaminate the register. As a result, damaging activities were still going on which put Romet in debt restructuring.[133] Consequently, citizens and companies become the victim of the choice of the government to work with the system of public registrations. According to the ECHR, the state failed to take effective measures to prevent the damages from happening on behalf of Romet as soon as they knew the driver's licence of Romet was filed stolen.[134]

### 4.4 Complementary protection under Dutch civil law

[130] RvS 1 april 2020,ECLI:NL:RVS:2020:898; RvS 1 april 2020 ELCI:RVS:2020:899; RvS 1 april 2020, ELCI:NL:RVS:2020:900; RvS 1 april 2020, ECLI:NL:RVS:2020:901.
[131] Van Eck 2018, p. 234
[132] Van Eck 2018, p. 106, 432.
[133] EHRM, 14 februari 2012, ECLI:NL:XX:2012:BW2721 (*Romet v. The Netherlands*).
[134] EHRM, 14 februari 2012, ECLI:NL:XX:2012:BW2721 (*Romet v. The Netherlands*), paras 37-44.

For the remaining category of chain failures due to factual government acts, the applicant has the option to go to the civil court. While Dutch torts law does acknowledge that torts can be committed by multiple actors on the basis of article 6:166 BW, I investigated whether an applicant could in theory successfully claim damages for chain errors of the multiple public bodies that operate in a chain together. Group torts occur when one or more actors in the group factually committed a tort that has resulted in damages. The fellow participants do not factually have to commit damaging activities, their liability will be established when they were under the legal duty to withdraw themselves from the group activity because the damages were foreseeable. This means there does not have to be a condictio sine qua non connection to their factual behaviour and the damages.[135] Chain cooperation can be defined as a group activity, while the actors consciously decide to operate together and to utilize an infrastructure to exchange data amongst each other. Thus, there is a certain level of awareness that a group activity is pursued. This level of awareness is sufficient for the qualification of the group activity. Article 6:166 BW does not demand that there needs to be effective coordination amongst the participants or that they pursue the same activities.[136] The scheme of group liability results into two types of torts: the first type is the tort that was factually causing the damages. The second tort lies in the act of participation. Participation only results into a tort if the damages that have occurred were foreseeable for the actor.[137]

To determine the relevant participating actors of the group activity that can be held liable, a connection to the logic of the GDPR can be sought. Article 82(2) GDPR prescribes that all the actors involved in the processing activities can be held liable. This means that once a tort in the chain is factually committed by one of the chain partners, the joint controllers that share the purposes or means to some extent of the particular data and the processors that process the particular data on behalf of a controller will be deemed as a part of the group activity. Foreseeability should be explained as an objective, collective foreseeability. What matters is that the participants could have known, the group activities would in general be able to cause the concrete type of damages, that eventually occurred. When the damages were objectively foreseeable, attribution is accepted based on the premise that the participant accepted the risk that the damages were able to happen.[138]

Typical damages that occur from using erroneous data or algorithms should lie in the general line of expectation when actors chose to operate in a chain network. Therefore, there

[135] Boonekamp 1990, p. 18.
[136] Boonekamp 1990, p. 4.
[137] Boonekamp 1990, p. 103.
[138] Boonekamp in: *GS Onrechtmatige daad*, art. 6:166 BW, aant. 7.1.

rests a legal duty on the actors to withdraw themselves from the damaging group activity. While the controllers and processors within the data chain will mostly be obliged to pursue certain processing activities, the only way to effectively evade liability is by actively taking measures to prevent the damaging activities from occurring or to put an end to them. If actors fail to do so, they can be held strictly liable for the entire amount of damages suffered by the victim due to the damaging group activity. This means that the defence of an actor that it did not know that the data was erroneous, or it was not able to correct the data will not succeed, because that is the risk of participating in the chain network. This risk comes for its own account.

According to Boonekamp, the group participants are not only under the legal obligation to prevent damages vis-à-vis third parties.[139] Participants have to make sure damages are prevented vis-à-vis their fellow participants. A second legal duty can be derived here from: actors should make sure that they take adequate action as soon as they are aware their own behaviour in the chain, or the behaviour of a fellow participant, is contaminating the processing activities of the other participants. If they fail to do so, their fellow participants should be able to claim damages from them.

As the government has a special position in the society, the conditions to establish a tort are specified with taking into account this position. I argued that it should be possible to appeal to a group tort of the several public bodies, while public bodies are also bound by the principles of good governance in the sphere of private law on the basis of article 3:14 BW.[140] The standard of due care to prevent a tort is subject to higher demands because of the principles of good governance, the notion that the government is the most solvable party to cover damages and in the best position to know all the relevant judicial and legal facts to prevent damages from occurring in the first place. This means the establishment of a tort due to factual government action can arise more quickly, than for private actors.

When defining the responsibilities of chain networks in light of the perspective from torts committed in a group of article 6:166 BW, a very equivalent and strict liability scheme in comparison with the GDPR is revealed. Both schemes rely on the same ground idea. When parties choose to join a group activity, or in GDPR-terms: jointly control certain data, they are also deemed to have accepted the typical risks that can be associated with joining that group activity. As a consequence, the participants are under the duty to take measures to ensure that

[139] Boonekamp 1990, p. 66-68.
[140] Van Maanen & De Lange 2000, p. 91; HR 27 maart 1987 ECLI:NL:PHR:1987:AG5565, *AB* 1987/273 (*Ikon-case*) ro. 3.3, 3.4.

damages are prevented. Every participant is strictly liable for the damages that were objectively foreseeable vis-à-vis third parties. Just as under the GDPR, when one of the participants is held liable for the damages under article 6:166 BW, he will have to pay the complete amount to the victim. Only afterwards, recourse is possible amongst the other actors.

### 4.5 Final remarks and recommendations

The current total picture of the legal schemes that determine the responsibilities and the legal protection of chain failures reveal the problems with limiting Awb protection to single administrative decisions. The most crucial and important legal remedy to revise and correct chain decisions and errors, can solely be found in administrative law. The Awb does not acknowledge that the decisions of public bodies can be connected, which results into the fragmentation of responsibilities of the chain actors with no legal mechanism in place to correct interrelated chain decisions. While the applicant will probably have the most interest in revising administrative chain decisions and in making sure other erroneous chain decisions are prevented from occurring in front of the administrative court, this type of protection is not provided by the Awb. As long as the responsibility of public bodies is mostly limited to their own link in the chain on the basis of administrative law, they will not be stimulated to put measures in place to effectively correct errors throughout the whole chain. Consequently, the applicants will remain to carry the burden of making sure the errors are corrected at all the various chain partners. Applicants potentially have to make use of other legal schemes that could offer them a different form of protection such as the GDPR and Dutch civil law. Even though the GDPR and Dutch civil law can provide complementary protection with regard to contesting chain failures and for claiming damages for these failures, protection from these schemes will not always effectively help out the applicant seeking protection. The GDPR and Dutch civil law do acknowledge that damages can be suffered due to a multi-actor activity and provide for a strict liability to prevent gaps in responsibilities and protection, but they cannot offer the correction of chain errors and decisions. In addition, it can be asked how desirable it is in the first place that a situation has been created, where the applicant is burdened to seek other forms of legal protection because the Awb fails to adequately offer chain protection. To ensure effective and adequate protection it should be possible to completely solve the issue at the administrative court.

With drawing inspiration from the strict liability schemes of the GDPR and Dutch civil law and also from the tone that was set in the *Afvalfonds*-case[141], a starting point to fix this problem would be to acknowledge in the Awb that chain decisions are connected. The chain decision-making process should be approached as a group activity in which chain actors can be held strictly responsible and liable for errors that are derived from other links within the chain. Thus, a duty of care should rest on all the chain partners to make sure their own activities do not contaminate the chain and to act proactively when they are faced with an error of another link in the chain. Consequentially, a chain actor should not be able to hide behind the fact that an error is caused by another chain actor. All the actors should bear the responsibility to prevent damages of the chain activities, which requires that a set of organizational measures is put in place to make sure such errors can be corrected completely on behalf of the applicant. If the chain actors fail to prevent damages from occurring, they should all be severally and fully liable for these damages.

To support the applicant in his appeal, it is advised that new legal remedies in administrative law are created to successfully contest and reverse all the decisions that connect to the chain error to adequately fix the error chain wide. It should be made possible that the judge is able to go beyond the contested decision in appeal and to get a look at all the relevant interrelated chain decisions, if there is an assumption the error is causing more problems somewhere upstream or downstream in the chain as well. In addition, the administrative court should have the competence to demand from the public bodies directly or indirectly via the public body in appeal that all the interconnected administrative chain decisions that built upon the error, are corrected as well.

Other potential measures to ensure adequate protection for the applicant, is that the burden of proof that a chain error is causing trouble for the applicant is revised. A current problem now is that the applicant is constantly faced with the difficulties of proofing and contesting the existence of the error at the several links of the chain. A way to reduce this burden is to accept a shift in the burden of proof, once the applicant shows prima-facie evidence of the existence of this error somewhere in the chain. After this prima-facie evidence, the involved chain actors have to proof there is no error or that the error did not cause problems or did not lead to an incorrect administrative decision on their side. In sum, when revising the administrative framework, the most important goal should be to design it in a way that stimulates all the separate chain actors to take full responsibility for their failures

[141] RvS 23 januari 2019, ECLI:NL:RVS:2019:150 ro 4.7.

as a chain. Next to that, the framework should offer effective legal remedies that aim to put a complete end to the ongoing negative consequences the chain error is causing for the applicant.

**Bibliography**


*Books and Dissertations*

**Asser/Hartkamp & Sieburgh 6-IV 2019**

A.S Hartkamp & C.H Sieburgh, 'Formele rechtskracht' in: C.H. Sieburgh, *Mr. C. Assers Handleiding tot de beoefening van het Nederlands Burgerlijk Recht. 6. Verbintenissenrecht. Deel IV. De verbintenis uit de wet*, Deventer: Wolters Kluwer 2019.

**Boonekamp: in *GS Onrechtmatige daad* 2019**

R.J.B Boonekamp, 'artikel 166. Gedragingen in groepsverband', in: C.J.J.M. Stolker (red.), *Groene Serie Onrechtmatige daad*, Deventer: Wolters Kluwer 2019.

**Boonekamp: in *GS Schadevergoeding* 2019**

R.J.B Boonekamp in: A.T. Bolt (red.), *Groene Serie Schadevergoeding*, Deventer: Wolters Kluwer 2019.

**Boonekamp 1990**

R.J.B Boonekamp, *Onrechtmatige daad in groepsverband volgens het NWB*, Deventer: Wolters Kluwer 1990.

**Çapfurt & Schuurmans in: 25 jaar Awb in eenheid en verscheidenheid**

F.Çapfurt & Y.E Schuurmans, 'Blinde vlek in de Awb: data' in: T.Barkhuysen et al, *25 jaar Awb in eenheid en verscheidenheid,* Deventer: Wolters Kluwer 2019.

**Delden, van 2009**

P. van Delden, *Samenwerking in de publieke dienstverlening: Ontwikkelingsverloop en resultaten* (diss. Tilburg) Delft/Zutphen: Uitgeverij Eburon 2009

**Eck, van 2018**

B.H.M van Eck, *Geautomatiseerde ketenbesluiten en rechtsbescherming (*diss. Tilburg*)* 2018.

**Grijpink 1997**

J.H.A.M Grijpink, *Keteninformatisering met toepassing op de justitiële bedrijfsketen* (diss. Eindhoven), Den Haag: SDU 1997.

**Janssen in: GS Onrechtmatige daad 2019**

K.J.O Janssen, 'artikel 6:162', in: C.J.J.M. Stolker (red.), *Groene Serie Onrechtmatige daad*, Deventer: Wolters Kluwer 2019.

**Janssen 2009**

K.J.O Janssen, *Onrechtmatige daad: algemene bepalingen,* Deventer: Wolters Kluwer 2009

**Maanen, van & Lange, de 2000**

G.E van Maanen & R. de Lange, *Onrechtmatige overheidsdaad,* Deventer*:* W.E.J Tjeenk Willink 2000.

**Oosterbaan 2012**

T. Oosterbaan, *Architectuur als agenda. Een theoretische en empirische analyse van de rol van frames bij architectuurontwikkeling voor keteninformatisering* (diss. Rotterdam) 2012

**Schueler 2005**

B.J Schueler, *Schadevergoeding en de Awb. Aansprakelijkheid voor appellabele besluiten,* Deventer: Wolters Kluwer 2005.

**Waard, de 2011**

B.W.N. de Waard (red.), *Ervaringen met bezwaar,* Den Haag: Wetenschappelijk Onderzoek- en Documenta- tiecentrum (wodc) 2011.

**WRR 2011**

WRR, *IOverheid,* Amsterdam: Amsterdam University Press 2011.

*Journals*

**Alsenoy, van *Jiptec* 2016**

B. van Alsenoy, 'Liability under the EU Data Protection Law: from Directive 95/46 to the General Data Protection Regulation' *Jiptec* 2016, vol. 3

**Bovens & Zouridis *Public Adminstration Review* 2002**

M.Bovens & S.Zouridis, 'From Street-Level to System-Level Bureaucracies: How Information and Communication Technology Is Transforming Administrative Discretion and Constitutional Control', *Public Administration Review* 2002, vol 62, no. 2.

**Hutchinson & Duncon *Deakin Law Review* 2012**

T. Hutchinson & N.Duncan, 'Defining and describing what we do: doctrinal legal research', *Deakin Law Review* 2012 vol 7 no. 1.

**Mahieu, Hoboken & Asghari *Jiptec* 2019**

R. Mahieu, J. van Hoboken & H.Asghari, 'Responsibility for Data Protection in a networked world. On the question of the controller and effective and complete protection and its application to data access rights in Europe ', *Jiptec* 2019, vol. 10

*Guidelines*

**Article 29 Working Party 2010**

Article 29 Working Party, 'Opinion 1/2010 on the concepts of ''controller'' and ''processor'', 2010.

**EDPS 2018**

European Data Protection Supervisor, 'EDPS Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/725', 2018.

*Reports*

**Algemene Rekenkamer 2014**

Algemene Rekenkamer 'Basisregistraties vanuit het perspectief van de burger, fraudebestrijding en governance', 2014.

*Case law*

*ECHR*

ECHR, 14 February 2012, ECLI:NL:XX:2012:BW2721 (*Romet v. The Netherlands*).

*CJEU*

CJEU 29 July 2019, Case C-40/17 ECLI:EU:C:2019:629 (*Fashion-ID).*

CJEU 10 July 2018, Case C-25/17 ECLI:EU:C:2018, (*Jehovan todistajat).*

CJEU 5 June 2018, Case C-210/16 EU:C:2018:388 (*Wirtschaftsakademie Schleswig-Holstein*).

CJEU 13 May 2014, Case C-131/12 EU:C:2014:317 *(Google-Spain).*

CJEU 7 July 1981, Case 158/80 ECLI:EU:1981:163 (*Rewe-Handelsgesellschaft Nord mbH v Hauptzollamt Kiel*).

*Dutch case law*

HR 2 oktober 2015, ECLI:NL:HR:2015:2914 *NJ* 2016/1, m.nt. T.Hartlief.

HR 27 maart 1987 ECLI:NL:PHR:1987:AG5565, *AB* 1987/273 (*Ikon*).

ABRvS 1 april 2020,ECLI:NL:RVS:2020:898.

ABRvS 1 april 2020 ELCI:RVS:2020:899.

ABRvS 1 april 2020, ELCI:NL:RVS:2020:900.

ABRvS 1 april 2020, ECLI:NL:RVS:2020:901.

ABRvS 23 januari 2019, ECLI:NL:RVS:2019:150

ABRvS 27 december 2017, ECLI:NL:RVS:2017:3561

ABRvS 6 april 2016, ECLI:NL:RVS:2016:929.

ABRvS, 5 september 2012, ECLI:NL:RVS:2012:BX6491.

ABRvS, 2 november 2011, ECLI:NL:RVS:2011:BP2823.

CRvB, 19 oktober 2010, ECLI:NL:CRVB:2010:BN9985, USZ 2010/390.

ABRvS 21 okotber 2009, ECLI:NL:RVS:2009:BK0811.

ABRvS 1 juli 2009, ECLI:NL:RVS:2009:BJ1093.

ABRvS 11 maart 2009, ECLI:NL:RVS:2009:BH5525, *JB* 2009/114, m.nt. G. Overkleeft-Verburg.

Hof Den Haag 22 december 2015, ECLI:NL:GHDHA:2015:3515.

Rb. 's-Gravenhage 9 november 2005, ECLI:NL:RBSGR:2005:AV:2156.

*News articles*

H.Eikenaar, ‘De hardnekkige spookbewoner is groot probleem voor gemeenten’, (bd.nl 2018).

AD 12 april 2013 ‘Overheid handelde onzorgvuldig in zaak Dolmatov’, https://www.ad.nl/binnenland/overheid-handelde-onzorgvuldig-in-zaak-dolmatov~a45e2b23/?referrer=https://www.google.com/